

Configure ACE in Routed Mode with L7 Policies

Document ID: 107400

Introduction

Prerequisites

Requirements

Components Used

Conventions

Configure

Network Diagram

Configurations

Verify

Troubleshoot

Related Information

Introduction

This document provides a sample configuration for the Application Control Module (ACE) configured in routed mode with Layer 7 (L7) policies. The ACE makes a load balancing decision based on specific content in the URL.

This sample uses two contexts:

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

Prerequisites

Requirements

There are no specific requirements for this document.

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

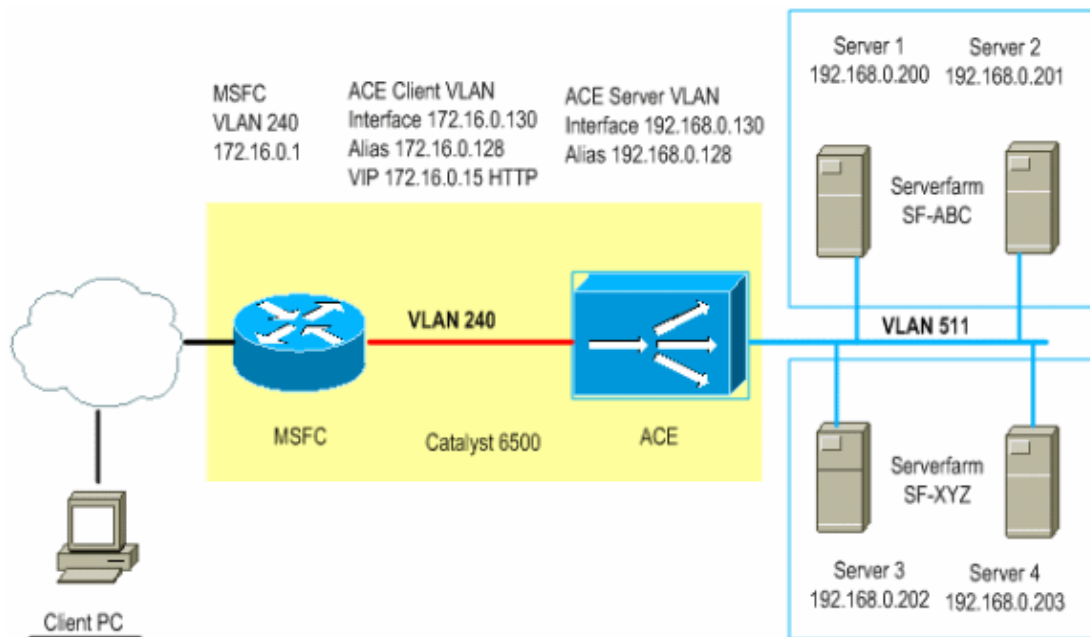
In this section, you are presented with the information to configure the features described in this document.

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 configuration

```
ACE C1 Context

switch/C1#show running-config
Generating configuration....

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
```

```
!--- http probe used to detect the status of the web servers.
```

```
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
```

```
serverfarm host SF-1  
  probe WEB_SERVERS  
  rserver S1  
    inservice  
  rserver S2  
    inservice  
  rserver S3  
    inservice  
  rserver S4  
    inservice
```

```
!--- Serverfarm used for traffic that matches the default class-map.  
!--- Client traffic that does not match /abc* or /xyz*  
!--- uses this serverfarm.
```

```
serverfarm host SF-ABC  
  probe WEB_SERVERS  
  rserver S1  
    inservice  
  rserver S2  
    inservice
```

```
!--- Serverfarm used to match traffic for /abc* content.
```

```
serverfarm host SF-XYZ  
  probe WEB_SERVERS  
  rserver S3  
    inservice  
  rserver S4  
    inservice
```

```
!--- Serverfarm used to match traffic for /xyz* content.
```

```
class-map match-all L4VIPCLASS  
  2 match virtual-address 172.16.0.15 tcp eq www
```

```
!--- Layer 4 class-map that defines the IP address and port.
```

```
class-map type http loadbalance match-all L7CLASS-ABC  
  2 match http url /abc/*  
class-map type http loadbalance match-all L7CLASS-XYZ  
  2 match http url /xyz/*
```

```
!--- 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 WEB_L7_POLICY  
  class L7CLASS-ABC  
    serverfarm SF-ABC  
  class L7CLASS-XYZ  
    serverfarm SF-XYZ  
  class class-default  
    serverfarm SF-1
```

```
!--- 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 L4VIPCLASS  
    loadbalance vip inservice  
    loadbalance policy WEB_L7_POLICY  
    loadbalance vip icmp-reply active  
    loadbalance vip advertise active
```

```
!--- 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 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 that defines 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 C1 context uses.

ft group 2
 peer 1
 no preempt
 associate-context C1
 inservice

!--- FT group used for the load balancing C1 context.

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 Ommited.

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** Displays information about the serverfarm and the state of the rservers.

This example provides sample output:

```
switch/C1# show serverfarm SF-1
serverfarm      : SF-1, type: HOST
total rservers : 4

-----
--                                     -----connections-----
--      real          weight state      current   total     failure
--      +-----+-----+-----+-----+-----+-----+
--
-- rserver: S1
--   192.168.0.200:0      8     OPERATIONAL  0         57        0
-- rserver: S2
--   192.168.0.201:0      8     OPERATIONAL  0         57        0
-- rserver: S3
--   192.168.0.202:0      8     OPERATIONAL  0         56        0
-- rserver: S4
--   192.168.0.203:0      8     OPERATIONAL  0         56        0
```

- **Show service-policy name detail** Displays information about the multi-match policy that includes state of the VIP, hit count for layer 7 class-maps, and dropped connections.

This example provides sample output:

```
switch/C1#show service-policy VIPs detail
-----
Interface: vlan 240
service-policy: VIPs
class: L4VIPCLASS
VIP Address:      Protocol:  Port:
172.16.0.15      tcp          eq      80
loadbalance:
L7 loadbalance policy: WEB_L7_POLICY
VIP Route Metric  : 77
VIP Route Advertise : ENABLED-WHEN-ACTIVE
VIP ICMP Reply    : ENABLED-WHEN-ACTIVE
VIP State: INSERVICE

!--- VIP State: Inservice shows the policy is ready
!--- to accept traffic.
```

```
!--- There must be at least one rserver inservice for the policy
!--- to show Inservice .
```

```
curr conns      : 1          , hit count      : 233
dropped conns   : 0
client pkt count : 1202      , client byte count: 142327
server pkt count : 1213      , server byte count: 1206796
conn-rate-limit  : 0          , drop-count : 0
bandwidth-rate-limit : 0      , drop-count : 0
L7 Loadbalance policy : WEB_L7_POLICY
class/match : L7CLASS-ABC
LB action :
  primary serverfarm: SF-ABC
  state: UP
  backup serverfarm : -
hit count      : 3
dropped conns   : 0
```

```
!--- Client traffic that matches the layer7 class-map matching /abc*
```

```
class/match : L7CLASS-XYZ
LB action :
  primary serverfarm: SF-XYZ
  state: UP
  backup serverfarm : -
hit count      : 3
dropped conns   : 0
```

```
!--- Client traffic that matches the layer7 class-map matching /yx*
```

```
class/match : class-default
LB action :
  primary serverfarm: SF-1
  state: UP
  backup serverfarm : -
hit count      : 226
dropped conns   : 0
```

```
!--- Client traffic that matches the default class-map.
```

```
switch/C1#
```

- **Show conn** Displays current connections on the ACE.

This example provides sample output:

```
switch/C1#show conn
```

```
total current connections : 2
```

conn-id	np	dir	proto	vlan	source	destination	state
11	2	in	TCP	240	172.16.1.10:2142	172.16.0.15:80	ESTAB
10	2	out	TCP	511	192.168.0.203:80	172.16.1.10:2142	ESTAB

```
switch/C1#
```

Troubleshoot

There is currently no specific troubleshooting information available for this configuration.

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: 107400
