

ACE Client and Servers Hitting the Same VIP

Document ID: 107398

Introduction

Prerequisites

Requirements

Components Used

Conventions

Background Information

Configure

Network Diagram

Configurations

Verify

Troubleshoot

Related Information

Introduction

This document provides a sample configuration for the Application Control Module (ACE) with Clients and Servers that hit the same Virtual IP Address (VIP). Clients are load balanced to the servers with no Network Address Translation (NAT) while servers that hit the VIP use source NAT.

This sample uses two contexts; the Admin context is used for remote management and Fault Tolerant (FT) configuration, and the second context C1 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.

Background Information

- **One Armed Mode** This topology is used when the device that makes the connection to the VIP enters the ACE on the same VLAN on which the servers reside. The server reply traffic must return to the ACE before it is sent to the device that initiated the connection. This can be done with either source NAT or policy based routing.

- **Two Armed Mode** This topology is used when the device that makes the connection to the VIP enters the ACE on a different VLAN than that on which the servers reside. If the servers have the default gateway set to the ACE, there is no need for source NAT. The reply traffic returns to the ACE before it is sent back to the client.

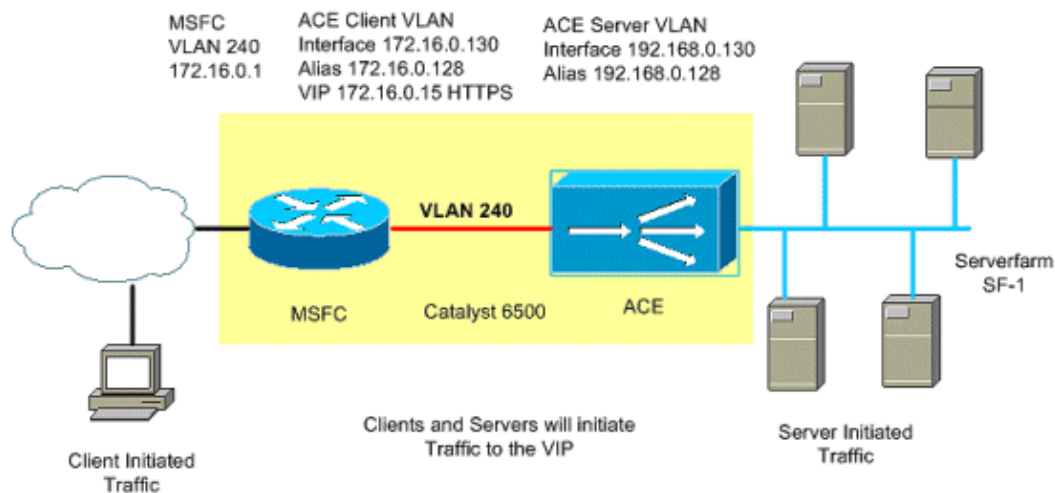
Configure

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 run
Generating configuration....

access-list any line 8 extended permit icmp any any
access-list any line 16 extended permit ip any any

!--- Access-list used 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 used to detect the status
!--- of the servers in the serverfarm.
```

```
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
```

```
!--- Traffic hitting the VIP
!--- will be load balanced to these servers.
```

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

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

```
class-map match-all REAL_SERVERS
  2 match source-address 192.168.0.0 255.255.255.0
```

```
!--- Layer 3 class-map defining source traffic.
!--- This traffic matches server initiated.
```

```
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

!--- Management class-map defining
!--- 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 class-default
    serverfarm SF-1

!--- Layer 4 policy-map defining
!--- the serverfarm that will be used.

policy-map multi-match VIPs
  class L4VIPCLASS
    loadbalance vip inservice
    loadbalance policy WEB_L7_POLICY
    loadbalance vip icmp-reply active
    loadbalance vip advertise active
  class REAL_SERVERS
    nat dynamic 1 vlan 511

!--- Traffic originating from clients
!--- will only match class L4VIPCLASS.
!--- This traffic will not use source NAT.
!--- Servers that make a connection to the
!--- VIP will match both classes and will use
!--- natpool 1 to change the source address
!--- of the server to 192.168.0.254 before
!--- it is loadbalanced.

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

!--- Apply access-lists and service policies
!--- to the client side VLAN.
```

```
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
 access-group input any
 nat-pool 1 192.168.0.254 192.168.0.254 netmask 255.255.255.0 pat
 service-policy input VIPs
 no shutdown

!--- For servers to be able to hit the VIP
!--- the service-policy VIPs will also need to be applied here.

ip route 0.0.0.0 0.0.0.0 172.16.0.1

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 R1
```

!--- 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 Configuration

```
!--- 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.

- **Show serverfarm name** 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
```

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

```
-----
```

real	weight	state	connections		
			current	total	failures
rserver: S1					
192.168.0.200:0	8	OPERATIONAL	0	31	0
rserver: S2					
192.168.0.201:0	8	OPERATIONAL	0	30	0
rserver: S3					
192.168.0.202:0	8	OPERATIONAL	0	30	0
rserver: S4					
192.168.0.203:0	8	OPERATIONAL	0	29	0

```
switch/C1#
```

- **Show service-policy name** Displays information about the multi-match policy. Use this command to verify if the VIP gets connections and if they are dropped.

This example provides sample output:

```
switch/C1#show service-policy VIPs
```

```
Status      : ACTIVE
```

```
-----
Interface: vlan 240 511
service-policy: VIPs
class: L4VIPCLASS
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
  curr conns           : 0 , hit count           : 120
  dropped conns        : 0
  client pkt count     : 1007 , client byte count: 139433
  server pkt count     : 1122 , server byte count: 1237658
  conn-rate-limit      : 0 , drop-count       : 0
  bandwidth-rate-limit : 0 , drop-count       : 0
class: REAL_SERVERS
nat:
  nat dynamic 1 vlan 511
  curr conns           : 0 , hit count           : 41
  dropped conns        : 0
  client pkt count     : 514 , client byte count: 78758
  server pkt count     : 608 , server byte count: 708319
  conn-rate-limit      : 0 , drop-count       : 0
  bandwidth-rate-limit : 0 , drop-count       : 0
```

```
switch/C1#
```

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

This example provides sample output:

