ACE客户端和服务器击中同样VIP

目录

简介

本文档为客户端和服务器抵达相同虚拟 IP 地址 (VIP) 的应用控制模块 (ACE) 提供了一个配置范例。客户端在服务器上进行了负载均衡，并且未使用网络地址转换 (NAT)，但抵达 VIP 的服务器使用了源 NAT。

此范例使用两个上下文；管理上下文用于远程管理和容错 (FT) 配置，第二个上下文 C1 用于负载均衡。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档不限于特定的软件和硬件版本。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

背景信息

- 单臂模式 - 当进行 VIP 连接的设备进入服务器所在的相同 VLAN 上的 ACE 时使用此拓扑。服务器答复流量必须返回 ACE，然后才能发送到启动该连接的设备。可以使用源 NAT 或基于策略的路由完成此操作。
- 双臂模式 – 当进行 VIP 连接的设备进入与服务器所在的 VLAN 不同的 VLAN 上的 ACE 时使用此拓扑。如果服务器的默认网关设置为该 ACE，则不需要源 NAT。答复流量将返回 ACE，然后再发送回客户端。

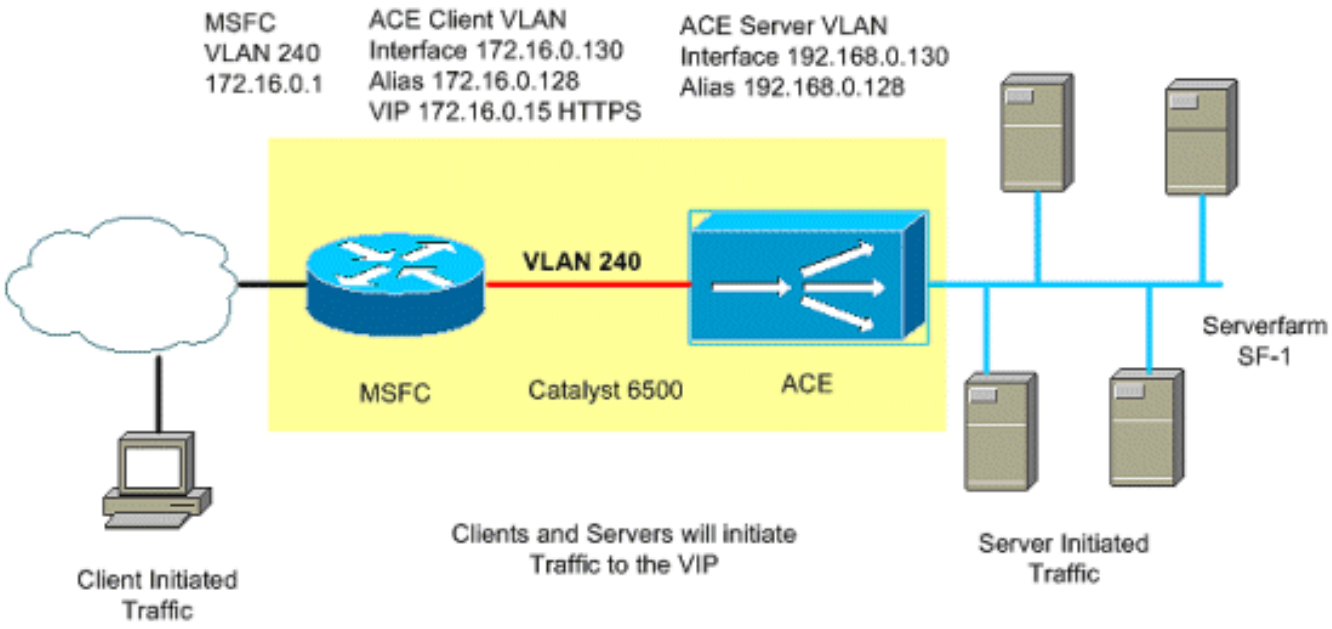
配置

本部分提供有关如何配置本文档所述功能的信息。

注意： 使用命令查找工具（仅限注册用户）可获取有关本部分所使用命令的详细信息。

网络图

本文档使用以下网络设置：



配置

本文档使用以下配置：

- Catalyst 6500 - ACE 插槽 2 C1 上下文
- Catalyst 6500 - ACE 插槽 2 管理上下文
- Catalyst 6500 - MSFC 配置

ACE C1 上下文
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 管理上下文

```
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 domai n
default-domain username www password 5
$1$UZIiwUk7$QMVYN1JASaycabrHkhGcS/ role Admin domain
default-domain switch/Admin#
```

路由器配置

```
!--- 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#
```

验证

使用本部分可确认配置能否正常运行。

- **Show serverfarm 名称** — 显示有关服务器群和 rserver 的状态的信息。此示例提供输出示例:

```
：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 ----------------------
---------- ----------connections---------- real weight state 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** — 显示有关多匹配策略的信息。使用此命令验证 VIP 是否获得连接以及是否断开连接。此示例提供输出示例：：`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** — 显示有关 ACE 上的当前连接的信息。此示例提供输出示例：：`switch/C1#show conn total current connections : 8 conn-id np dir proto vlan source destination state ------ ----+--+---+-----+----+---------------------+--------------- -+ 11 1 in TCP 511 192.168.0.200:1380 172.16.0.15:80 ESTAB 9 1 out TCP 511 192.168.0.203:80 192.168.0.254:1065 ESTAB 12 2 in TCP 240 130.10.96.221:2446 172.16.0.15:80 ESTAB 9 2 out TCP 511 192.168.0.200:80 130.10.96.221:2446 ESTAB switch/C1# *!--- Top two lines are the server connecting to the VIP. !--- 192.168.0.254 is the natpool address. !--- Bottom two lines are a client making a connection to the VIP.*`

故障排除

目前没有针对此配置的故障排除信息。

相关信息

- 技术支持和文档 - Cisco Systems