FortiADC SLB Virtual Server L4 方式部署详解

版本	1.0
时间	2015 年 10 月
支持的版本	FortiADC v4.3.x
作者	刘康明
状态	已审核
反馈	support_cn@fortinet.com

目录

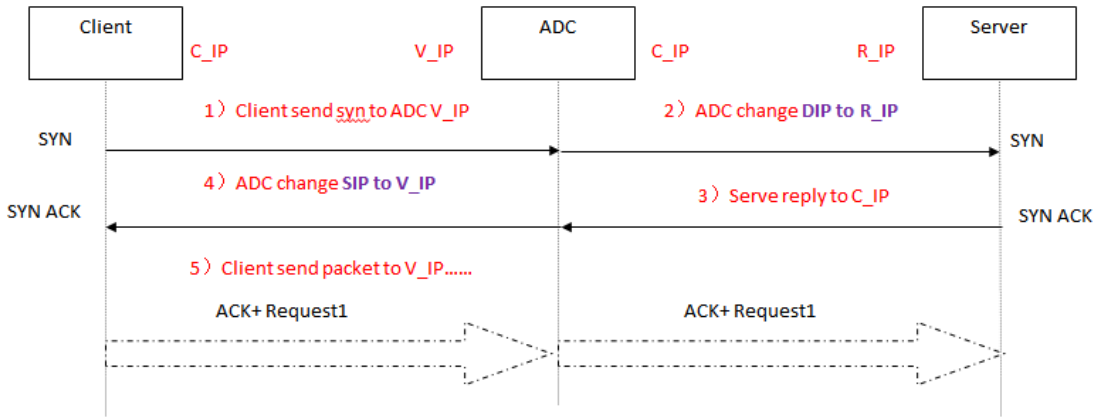
简介

FortiADC SLB 在实际的应用中可采取 Layer4、Layer7、Layer2 的部署方式，其中 FortiADC 的负载处理又包含数据转发模式和代理模式，同时支持 IPv4 和 IPv6 的双栈协议。看似复杂多变的各种部署方式，实际上都是为了更好的实现不同应用场景下的服务器负载均衡功能，本文将针对 FortiADC 常用的三种 L4 负载均衡服务实现类型进行说明：

- DNAT
- FULLNAT
- DR

Virtual Server L4 DNAT 转发部署方式介绍

- 过程类似于 DNAT 的处理方式，具体转换过程如下图所示：

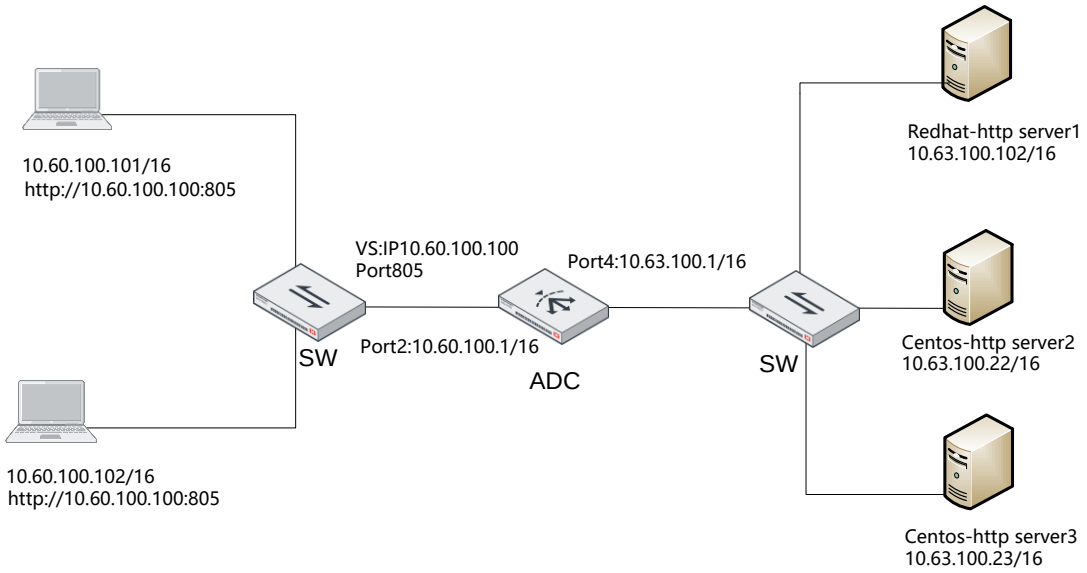


客户端只需要知道 ADC 的 Virtual IP（V_IP）和 Port 并发起访问，ADC 将客户端所访问的 DIP（即 V_IP）转换为内部的真实 IP（即 R_IP），类似于 DNAT 设备的处理方式。

真实服务器回复客户端（C_IP）的时候，ADC 将真实服务器的 SIP 还原成虚拟 IP（即 V_IP），然后再转发给客户端。

整个过程对于 Client 和 Sevrer 都是透明的，ADC 在 DNAT 方式的转换过程中实现业务的负载调度。

- 配置举例



1.config ADC intetface :

FortiADC# config system interface

FortiADC (interface) # edit port2

FortiADC (port2) # set ip 10.60.100.1/16（clientside）

FortiADC (port2) # next

FortiADC (interface) # edit port4

FortiADC (port2) # set ip 10.63.100.1/16 （serverside）

FortiADC (port4) # end

2.config pool:（RealServer pool with 3 members）

FortiADC # config load-balance pool

FortiADC (pool) # edit pool-4

FortiADC (pool-4) # config pool_member

FortiADC (pool_member) # edit 1

FortiADC (4) # set ip 10.63.100.102

FortiADC (4) # next

FortiADC (pool_member) # edit 2

FortiADC (1) # set ip 10.63.100.22

FortiADC (1) # next

FortiADC (pool_member) # edit 3

FortiADC (1) # set ip 10.63.100.23

FortiADC (1) # next

3.config method： can use default

4.config profile： can use default

5.config virtual-server：

```
FortiADC # config load-balance virtual-server
FortiADC (virtual-server) # edit vs4                                  (add virtual-server)
FortiADC (vs4) # set type l4-load-balance                             (set type L4)
FortiADC (vs4) # set packet-forwarding-method NAT                     (by default)
FortiADC (vs4) # set interface port2                                  (set interface)
FortiADC (vs4) # set ip 10.60.100.100                                 (virtual-server IP)
FortiADC (vs4) # set port 805                                         (virtual-server port)
FortiADC (vs4) # set load-balance-method LB_METHOD_ROUND_ROBIN    (轮询调度)
FortiADC (vs4) # set load-balance-pool pool-4                         (调用 Real Server Pool)
FortiADC (vs4) # set load-balance-profile LB_PROF_TCP                 (选择 profile L4 协议)
FortiADC (vs4) # end
```

6.server config route:

```
route add -net 10.60.0.0 netmask 255.255.0.0 gw 10.63.100.1
```

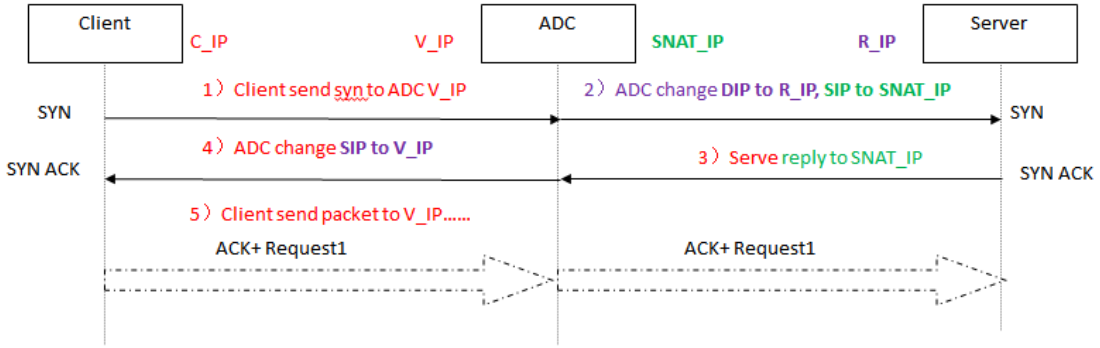
当多个客户端发起 http://10.60.100.100:805 访问，将打开 Web 页面并在 server1、server2、server3 之间轮询调度。

Virtual Server L4 FULLNAT 转发部署方式介绍

- 类似于 DNAT+SNAT 的处理方式

Virtual Server L4 FULLNAT 转发方式类似于 DNAT+SNAT 的处理方式，FULLNAT 方式与 DNAT 方式相比只是在虚服务器 IP(V_IP)转换为真实服务器 IP(R_IP)之后，再在出接口方向做了一次源 NAT 转换，此时源目 IP 均被转换，故而称作 FULLNAT，这样设计的好处是内部的 SW 和 RealServer 可以减少路由的配置，同时更加方便的实现跨 vlan 之间的访问，缺点是 RealServer 无法获得用户的真实 IP，而解决的办法是通过在 TCP Option 选项中携带客户端的真实 IP 发给 RealServer。

具体转换过程如下图所示：

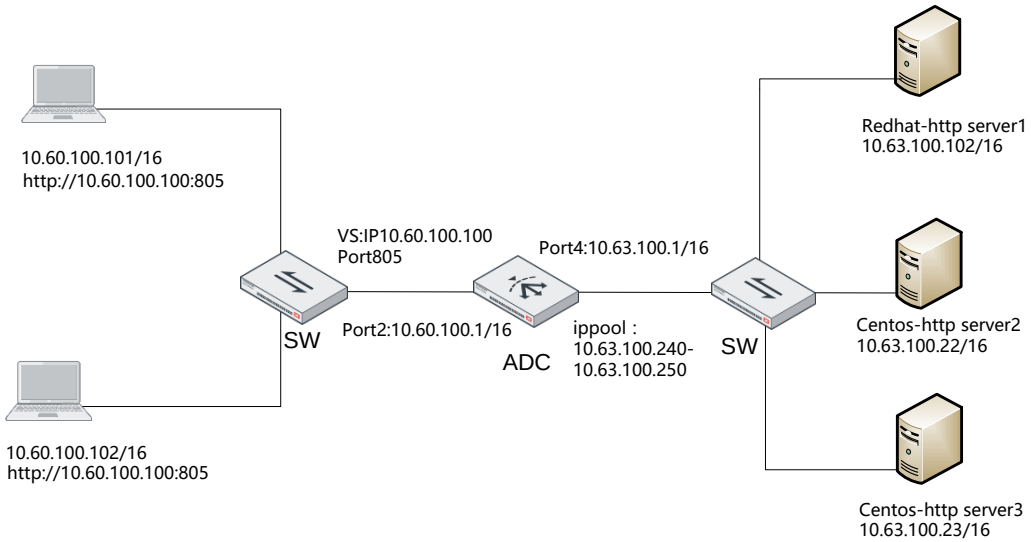


客户端只需要知道 ADC 的 Virtual IP（V_IP）和 Port 并发起访问，ADC 将客户端所访问的 DIP（即 V_IP）转换为内部的真实 IP（即 R_IP），类似于 DNAT 的处理方式，同时在出接口又将客户端 IP（C_IP）做源 NAT 转换为 ADC 的 SNAT_IP，客户端访问服务器的数据同时做了 DNAT 和 SNAT 转换。

真实服务器将回复 SNAT_IP，ADC 将真实服务器的 SIP 还原成虚拟 IP（即 V_IP），同时将 SNAT_IP 还原成客户端 IP(C_IP)，然后再转发给客户端。

整个过程对于 Client 和 Sevrer 都是透明的，ADC 在 FULLNAT 方式的转换过程中实现业务的负载调度。

- 配置举例



以下只摘取关键配置，其中接口配置、config pool、config method、config profile 与 DNAT 方式举例中的配置相同：

config ippool (SNAT Pool)

FortiADC # config load-balance ippool

FortiADC (ippool) # edit snat-pool (add ippool)

FortiADC (snat-pool) # set addr-type ipv4

FortiADC (snat-pool) # set interface port4 (snat out interface)

FortiADC (snat-pool) # set ip-min 10.63.100.240
FortiADC (snat-pool) # set ip-max 10.63.100.250

config virtual-server：

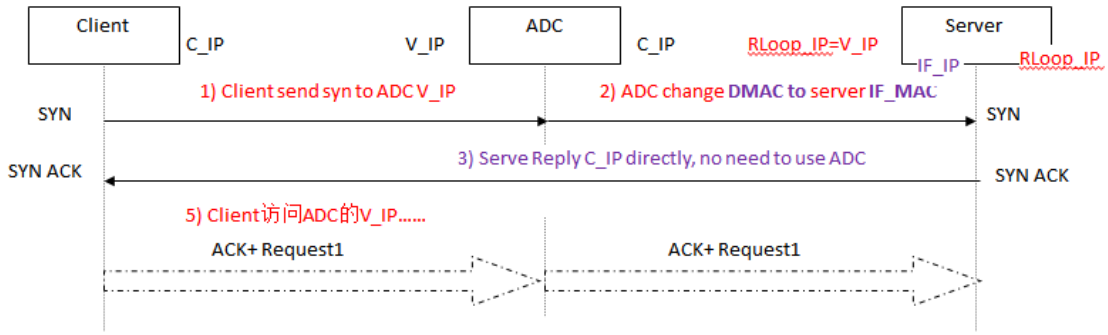
FortiADC # config load-balance virtual-server
FortiADC (virtual-server) # edit vs4 (add virtual-server)
FortiADC (vs4) # set type l4-load-balance (set type L4)
FortiADC (vs4) # set packet-forwarding-method FullNAT (FULLNAT)
FortiADC (vs4) # set interface port2 (set interface)
FortiADC (vs4) # set ip 10.60.100.100 (virtual-server IP)
FortiADC (vs4) # set port 805 (virtual-server port)
FortiADC (vs4) # set ippool snat-pool (snat-pool)
FortiADC (vs4) # set load-balance-method LB_METHOD_ROUND_ROBIN (轮询调度)
FortiADC (vs4) # set load-balance-pool pool-4 (调用 Real Server Pool)
FortiADC (vs4) # set load-balance-profile LB_PROF_TCP (选择 profile L4 协议)
FortiADC (vs4) # end

当多个客户端发起 http://10.60.100.100:805 访问，将打开 Web 页面并在 server1、server2、server3 之间轮询调度。

Virtual Server L4 DR 转发部署方式介绍

DR 的效率是所有模式中最高的，它只需要修改目的 MAC，但部署上必须要求 FortiADC 和后端服务器在同一个 VLAN 中，DR 非常适合应用于小规模网络中。

具体工作过程如下图所示：

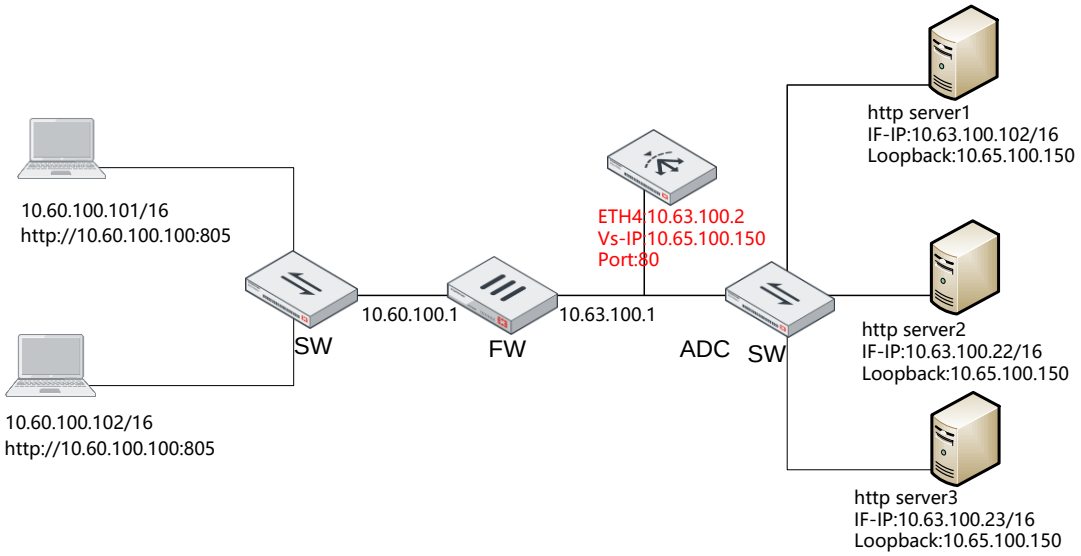


虚拟 IP：FortiADC 上配置的虚拟 IP(V_IP) == 服务器上的本地 RLoop_IP，RLoop_IP 是防火墙的本地回环地址。真实 IP：Pool-member IP == 真实服务器连接 FortiADC 的接口 IP（IF_IP）。

FortiADC 在处理过程中只将客户端访问服务器报文中的目的 MAC(DMAC)转

换为真实服务器的接口 MAC(IF_MAC)，而服务器回复客户端的时候流量将不再走 FortiADC，由服务器直接回复给客户端(C_IP)。FortiADC 的 DR 部署要求与内部真实服务器位于同一个广播域内。

- 配置举例



V_IP==RLoop_IP, RLoop_IP 是服务器的 loopback 接口地址
Real-server 使用 server if_ip

config pool:（RealServer）

FortiADC # config load-balance pool
FortiADC (pool) # edit pool-DR
FortiADC (pool-DR) # config pool_member
FortiADC (pool_member) # edit 1
FortiADC (4) # set ip 10.63.100.102
FortiADC (4) # next
FortiADC (pool_member) # edit 2
FortiADC (1) # set ip 10.63.100.22
FortiADC (1) # next
FortiADC (pool_member) # edit 3
FortiADC (1) # set ip 10.63.100.23
FortiADC (1) # next

config virtual-server:

FortiADC # config load-balance virtual-server
FortiADC (virtual-server) # edit vs-DR
FortiADC (vs-DR) # set type l4-load-balance
FortiADC (vs-DR) # set packet-forwarding-method direct_routing
FortiADC (vs-DR) # set interface port4
FortiADC (vs-DR) # set ip 10.65.100.150 (V_IP==服务器的 loopback 地址)

FortiADC (vs-DR) # set port 80 (virtual-server port, must 80)

当多个客户端发起 http://10.60.100.150 访问，将打开 Web 页面并在 server1、server2、server3 之间轮询调度，请求方向的流量将在 ADC 上进行负载调度，而服务器回复的流量则不再经过 ADC 处理直接就发送给了客户端。