# 中低端防火墙HA联动VRRP主备模式中NAT功能典型配置（公网地址只有一个）

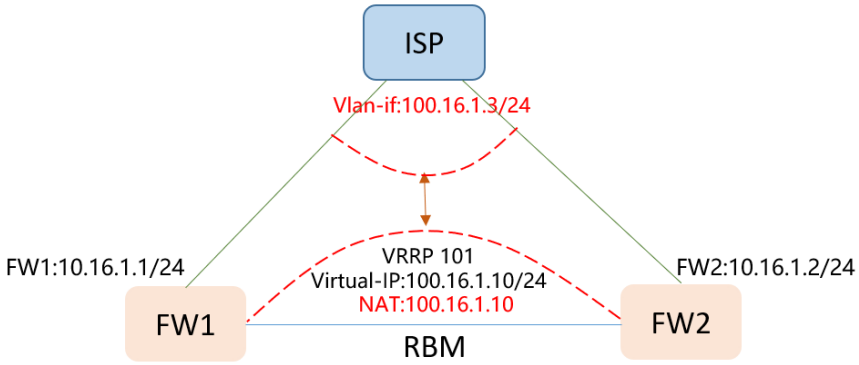
双机热备 VRRP VRRP NAT **孔凡安** 2023-12-27 发表

## 组网及说明

安全产品全新RBM特性HA组网方案，紧随业界潮流，组网灵活，规避了双机部署时横向链路的带宽限制，两台设备控制平面分离，升级操作简单，可以实现双机配置自动同步和业务的平滑切换。
设备部署在公网出口场景下，典型的RBM+VRRP场景下最少需要3个公网地址。但是有时候客户仅有1个公网地址，无法参考典配完成部署。此时可以利用**RBM支持VRRP虚拟地址和接口地址配置不同网段**的特性解决现场需求。

该特性说明见链接：RBM结合VRRP场景下支持VRRP虚拟地址和接口地址不在同一网段

**组网如下：**




## 配置步骤

**FW配置：**

| | FW1 | FW2 |
|---|---|---|
| RBM部分 | #<br>remote-backup group<br> data-channel interface Route-Aggregation 64<br> local-ip 192.60.12.1<br> remote-ip 192.60.12.2<br> device-role primary<br>#| #<br>remote-backup group<br> data-channel interface Route-Aggregation64<br> local-ip 192.60.12.2<br> remote-ip 192.60.12.1<br> device-role secondary<br>#|
| VRRP+NAT部分 | #<br>interface Route-Aggregation1.10<br> ip address 10.16.1.1 255.255.255.0<br> vrrp vrid 101 virtual-ip 100.16.1.10 255.255.255.0 active<br> **nat outbound address-group 1**<br> vlan-type dot1q vid 101<br>#<br>nat address-group 1<br> **address 100.16.1.10 100.16.1.10**<br>#| #<br>interface Route-Aggregation1.10<br> ip address 10.16.1.2 255.255.255.0<br> vrrp vrid 101 virtual-ip 100.16.1.10 255.255.255.0 standby<br> **nat outbound address-group 1**<br> vlan-type dot1q vid 101<br>#<br>nat address-group 1<br> **address 100.16.1.10 100.16.1.10**<br>#|

## 配置关键点

**Q1.** NAT地址池是否需要绑定VRRP VRID?
**A1：**不需要，RBM主设备地址池地址才响应ARP，**备机NAT地址池不响应ARP**。

**Q2：**FW发出报文源MAC是接口MAC，但是对端回应报文目的MAC是虚拟MAC（0000-5e00-01**xx**）。公网侧设备有MAC校验，收到MAC不一致的报文会丢弃。能否解决?
**A2：**暂时没有方案解决。如果是**最新版本（90分支）**可以尝试关闭虚拟MAC地址发布功能，但是**不保证一定可以解决。**目前软件侧针对该命令实现的效果是：可以保证VRRP虚拟地址以接口MAC响应对端ARP请求；但是涉及到NAT，NAT地址池还是以VRRP虚MAC响应ARP。

查看ISP学到的地址池地址对应MAC：

```
<ISP>disp arp
  Type: S-Static   D-Dynamic   O-Openflow   R-Rule   M-Multiport  I-Invalid
IP address      MAC address    SVLAN/VSI  Interface/Link ID       Aging Type
100.16.1.10     0000-5e00-0165 101        BAGG11                  12    D
```

vrrp virtual-mac enable命令用来开启虚拟MAC地址发布功能。

undo vrrp virtual-mac enable命令用来关闭虚拟MAC地址发布功能。

【命令】

vrrp virtual-mac enable

undo vrrp virtual-mac enable

【缺省情况】

虚拟MAC地址发布功能处于开启状态。

【视图】

系统视图

【缺省用户角色】

network-admin

mdc-admin

【使用指导】

缺省情况下，VRRP虚拟路由器使用虚拟MAC地址和上下游设备通信。虚拟MAC地址由Master路由器动态生成，如果虚拟路由器重启，生成的虚拟MAC地址可能不同。所以，虚拟MAC地址不能用来标识一台VRRP虚拟路由器。如果在上下游设备配置静态ARP表项时使用虚拟MAC地址，可能会因为虚拟MAC地址变化，导致通信失败。

关闭虚拟MAC地址发布功能后，VRRP虚拟路由器将使用配置VRRP功能的接口的真实MAC地址和上下游设备通信。Master路由器对外发布免费ARP报文时，宣告的是虚拟IP地址和真实MAC地址的组合；Master路由器收到ARP请求时，也会使用真实MAC地址应答。真实MAC地址具有固定不变的属性，适用于配置静态ARP表项等使用场景。

本命令仅在VRRP工作在标准模式时生效，工作在负载均衡模式时不生效。

【举例】

# 关闭虚拟MAC地址发布功能。

<Sysname> system-view

[Sysname] undo vrrp virtual-mac enable

【相关命令】

· vrrp mode