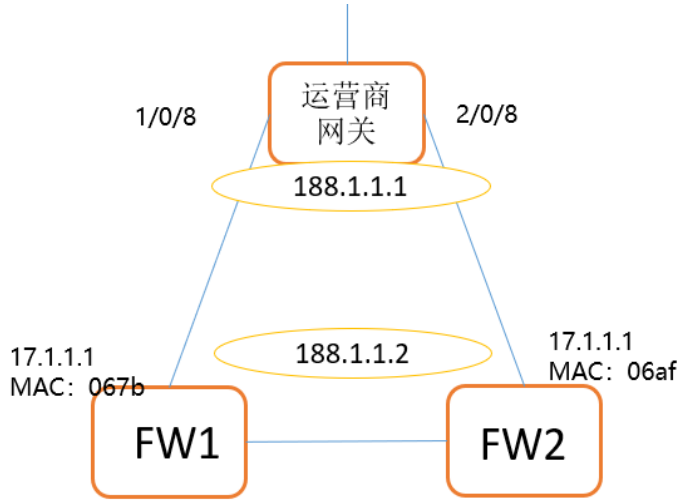
安全V7防火墙使用RBM主备+VRRP时候的MAC转发情况（VRRP虚地址和NAT地址池地址同网段，VRRP接口地址是私网）

VRRP　孔梦龙　2023-12-27 发表

组网及说明

组网如下：



配置步骤

RBM：P

#

interface GigabitEthernet1/0/5

 port link-mode route

 ip address 17.1.1.1 255.255.255.252

 vrrp vrid 3 virtual-ip 188.1.1.2 255.255.255.0 active

 nat outbound address-group 2

#

RBM：S

#

interface GigabitEthernet1/0/5

 port link-mode route

 ip address 17.1.1.2 255.255.255.252

 vrrp vrid 3 virtual-ip 188.1.1.2 255.255.255.0 standby

 nat outbound address-group 2

#

#

nat address-group 2

 address 188.1.1.10 188.1.1.11

#

配置关键点

此时：

查看运营商网关设备上的ARP，是可以学到地址池的ARP的：

188.1.1.2　0000-5e00-0103 55　GE1/0/8　17　D

188.1.1.10　9023-b46c-067b 55　GE1/0/8　20　D

188.1.1.11　9023-b46c-067b 55　GE1/0/8　20　D

down掉P设备上的VRRP接口后，运营商网关从备框学到：

188.1.1.2　0000-5e00-0103 55　GE2/0/8　20　D

188.1.1.10　9023-b46c-06af 55　GE2/0/8　20　D

188.1.1.11　9023-b46c-06af 55　GE2/0/8　20　D

up起来P设备上的口子，delay-time以后，切换：

188.1.1.2 0000-5e00-0103 55 GE1/0/8 20 D

188.1.1.10 9023-b46c-06af 55 GE2/0/8 17 D

188.1.1.11 9023-b46c-06af 55 GE2/0/8 17 D

上行设备上的ARP不刷新，此时业务中断，需要等到ARP老化；

此时解决办法：

方式一、运营商上设备需要清理一下ARP

方式二、地址池绑定vrrp

#

nat address-group 2

address 188.1.1.10 188.1.1.11

vrrp vrid 3

#

但是由此延伸出一个问题

地址池没有绑定VRRP的时候，对端学到地址池地址使用的是我们的接口MAC，绑定以后学到的全是虚MAC

188.1.1.2 0000-5e00-0103 55 GE1/0/8 20 D

188.1.1.10 0000-5e00-0103 55 GE1/0/8 20 D

188.1.1.11 0000-5e00-0103 55 GE1/0/8 20 D

此时运营商正向过来的请求目的MAC是虚MAC，我们回应的时候源MAC是接口实际MAC，此时会可能会被运营商限制；