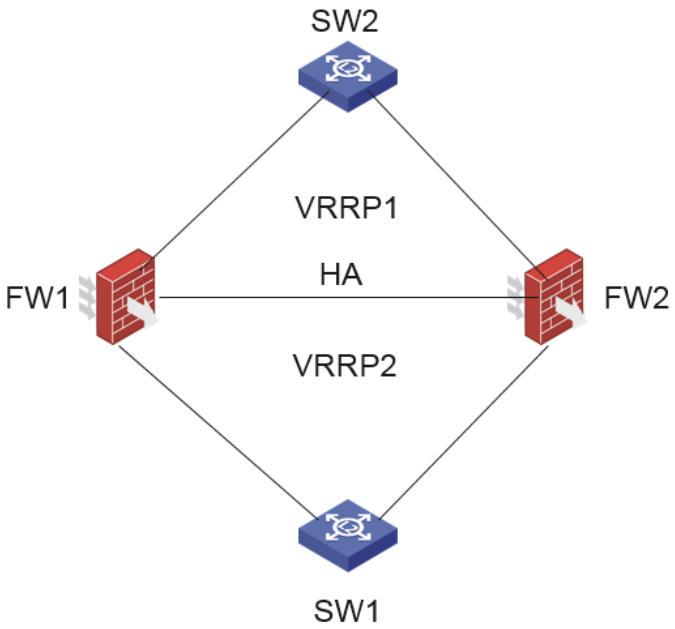
某局点 F5000使能NAT后日志报地址冲突的经验案例

VRRP NAT 张腾 2019-06-24 发表

组网及说明



2台V5防火墙做HA，同时针对上下行设备分别做VRRP;VRRP组1和组2的master都为FW1；

问题描述

由于业务需要，和现场HA的组网环境，两台防火墙在与SW2互联的接口使能相同配置的静态NAT；使能后，2台防火墙日志报IP地址冲突:

%Apr 3 14:59:24:023 2019 JP-7F-AB07-H3CFW-01 ARP/5/ARP_DUPGLOBALIP: IP address 10.32.66.153 conflicts with global or imported IP address, sourced from XXXX-00d8-72c2.

过程分析

一、从日志看是IP地址冲突，而且在2台设备上报冲突的IP地址都为静态NAT的global地址，并且冲突来源的MAC分别为2台防火墙的上行口MAC；

nat static 172.30.254.10 **10.32.66.153**

二、2台防火墙的上行口地址分别为10.32.66.5、10.32.66.6，VRRP虚地址为10.32.66.4，为什么设备上不存在的global地址10.32.66.153会响应ARP导致IP地址冲突?

[10.32.66.5]display ip routing-table

Destinations : 19 Routes : 19

Destination/Mask	Proto	Pre	Cost	NextHop	Interface
0.0.0.0/32	Direct	0	0	127.0.0.1	InLoop0
10.32.66.0/24	Direct	0	0	10.32.66.5	GE1/0/13
10.32.66.0/32	Direct	0	0	10.32.66.5	GE1/0/13
10.32.66.4/32	Direct	1	0	127.0.0.1	InLoop0
10.32.66.5/32	Direct	0	0	127.0.0.1	InLoop0
10.32.66.153/32	**Direct**	**1**	**0**	**0.0.0.0**	**NULL0**

查看2台设备的路由表会发现，在配置了静态NAT后会生成一条目的地址为global地址10.32.66.153的null0路由；**其实不只是静态NAT的公网地址，包括NAT SERVER的公网地址，源地址转换的地址池地址；只要在接口使能后，这些地址都会生成一条null0路由；目的就是为了让设备能够响应公网的ARP请求，因为不可能在设备上把这些涉及的地址都配上；**

原理： 这些地址全部会进入地址管理模块进行统一地址管理，并由地址管理模块通知路由管理模块将这些IP地址加入路由表。当外部设备向这些地址发起ARP请求，设备便会将ARP请求送到地址管理模块检查ARP报文的合法性，地址管理发现ARP所请求的IP地址为NAT地址池地址，则通知NAT模块判断是否需要回应ARP，NAT模块会检查ARP所请求的IP地址是否是收到ARP接口下配置的NAT的地址，如果是则通知ARP模块进行ARP应答。

三、现场组网有这种需求，应该如何规避?

V5设备针对这种场景开发了NAT TRACK VRRP的功能；当NAT联动VRRP后，只有VRRP主设备上才会生成上述地址的null0路由，而VRRP备设备是不会生成null0路由的，这样只有VRRP主设备会响应ARP请求，就不会出现IP地址冲突了；

四、规避方法：
1、针对静态nat场景：
在接口使能静态NAT时联动VRRP
nat outbound static track vrrp 1
2、针对源地址转换的address-group场景：
除了在接口联动VRRP
nat outbound 3000 address-group 0 track vrrp 1
还需要保证2台设备的地址池优先级不同
[FW1]nat address-group 0 X.X.X.10 X.X.X.10 **level 0**
[FW2]nat address-group 0 X.X.X.10 X.X.X.10 **level 1**
3、针对NAT SERVER场景
在接口使能NAT SERVER时联动VRRP
nat server protocol tcp global X.X.X.X www inside 172.16.100.20 www track vrrp 1
五、注意事项：
如果设备上存在多个VRRP组，NAT联动的VRRP组**必须是配置NAT的接口所在的VRRP组**，否则2个设备都不会生成null0路由；

解决方法

配置NAT联动VRRP解决；