安全产品配置BFD MAD检测的经典方法

IRF 张泷文 2016-04-28 发表

V7防火墙和负载均衡往往需要配置IRF堆叠，那么BFD MAD检测就必须要配置。
BFD MAD配置比较单一，对于可以配置二层接口的设备，可以使用vlan虚接口；对于无法配置二层口的设备，就使用聚合口配置。

方法一、使用二层口配置

创建VLAN 3，并将Firewall A（成员编号为1）上的端口GigabitEthernet1/0/1和Firewall B（成员编号为2）上的端口GigabitEthernet2/0/1加入VLAN 3中。
[Sysname] vlan 3
[Sysname-vlan3] quit
[Sysname]interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1]port link-mode bridge
[Sysname-GigabitEthernet1/0/1]port access vlan 3
[Sysname-GigabitEthernet1/0/1]quit
[Sysname]interface GigabitEthernet 2/0/1
[Sysname-GigabitEthernet2/0/1]port link-mode bridge
[Sysname-GigabitEthernet2/0/1]port access vlan
[Sysname-GigabitEthernet2/0/1]quit
创建VLAN接口3，并配置MAD IP地址。
[Sysname] interface vlan-interface 3
[Sysname-Vlan-interface3] mad bfd enable
[Sysname-Vlan-interface3] mad ip address 192.168.2.1 24 member 1
[Sysname-Vlan-interface3] mad ip address 192.168.2.2 24 member 2
[Sysname-Vlan-interface3] quit

因为BFD MAD和生成树功能互斥，所以在GigabitEthernet1/0/1和GigabitEthernet2/0/1上关闭生成树协议。
[Sysname] interface gigabitethernet 1/0/1
[Sysname-gigabitethernet-1/0/1] undo stp enable
[Sysname-gigabitethernet-1/0/1] quit
[Sysname] interface gigabitethernet 2/0/1
[Sysname-gigabitethernet-2/0/1] undo stp enable

#防火墙设备需要配置域间策略，因为bfd报文是到设备本地，因此要配置local到接口的域间策略。
将接口vlan-interface 3加入安全域Trust（步骤略）。
创建对象组。
[Sysname] object-group ip address mad
[Sysname-obj-grp-ip-mad] 0 network subnet 192.168.2.0 255.255.255.0
[Sysname-obj-grp-ip-mad] quit
创建域间策略对象。
[Sysname] object-policy ip local-trust
[Sysname-object-policy-ip-local-trust] rule 1 pass source-ip mad destination-ip mad
[Sysname-object-policy-ip-local-trust] quit
创建源域为local，目的为trust的域间策略，并引用域间策略对象。
[Sysname] zone-pair security source local destination trust
[Sysname-zone-pair-security-Local-Trust] object-policy apply ip local-trust
[Sysname-zone-pair-security-Local-Trust] quit

方法二、使用三层口配置
配置聚合口，并在聚合口上下MAD BFD
interface Route-Aggregation64
mad bfd enable
mad ip address 192.168.200.5 255.255.255.252 member 1
mad ip address 192.168.200.6 255.255.255.252 member 2
#
interface GigabitEthernet1/0/11
port link-mode route

```
 port link-aggregation group 64
 #
 interface GigabitEthernet2/0/11
 port link-mode route
 port link-aggregation group 64
```

防火墙需要配置接口安全域和域间策略

1、对于防火墙，需要配置BFD MAD接口的安全域和域间策略
2、当出现arp冲突时，需要看bfd session是否down，down为正常，up为设备分裂。如果down的情况下arp冲突，尝试绑定mac地址。
3、BFD地址应该在同一个网段。二层接口方法下bfd vlan不能它用。