F5000-X系列防火墙堆叠后BFD MAD检测配置举例

IRF　程咪　2019-09-03 发表

组网及说明

1 配置需求及说明

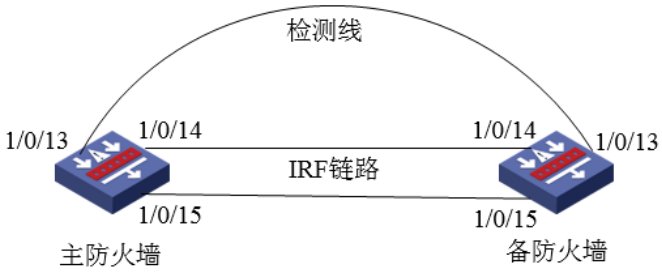
1.1 适用的产品系列

本案例适用于如F5080、F5060、F5030、F5000-M等F5000、F5000-X系列的防火墙。

1.2 配置需求及实现的效果

某单位购买两台防火墙用于防护内网服务器使用，为了简化网络架构和增强组网可靠性需要将两台防火墙虚拟化为一台防火墙使用。但是考虑到如果中间堆叠线出现故障造成堆叠分裂，那么用户在流量依旧会转给备设备，为了防止这一问题出现需要增加BFD MAD检测，实现当堆叠分裂后备设备除IRF端口以外的所有端口关闭。

2 组网图



组网说明：将主防火墙的14与15接口和备用防火墙14与15接口互联组成IRF链路，将主设备13与备设备13接口使用网线互联组成检测链路。

配置步骤

3 配置步骤

3.1 主防火墙配置

3.1.1 配置主防火墙的优先级为10

system-view

[H3C]irf member 1 priority 10

3.1.2 将需要进行堆叠配置的端口1/0/14与1/0/15接口加入IRF端口

物理端口加入IRF端口时需要先关闭端口，添加到IRF端口后再开启端口。

[H3C]interface range GigabitEthernet 1/0/14 to GigabitEthernet 1/0/15

[H3C-if-range]shutdown

[H3C-if-range]quit

[H3C]irf-port 1/2

[H3C-irf-port1/2]port group interface GigabitEthernet 1/0/14

[H3C-irf-port1/2]port group interface GigabitEthernet 1/0/15

[H3C-irf-port1/2]quit

[H3C]interface range GigabitEthernet 1/0/14 to GigabitEthernet 1/0/15

[H3C-if-range]undo shutdown

[H3C-if-range]quit

3.1.3 配置完成后激活IRF配置

[H3C]irf-port-configuration active

3.2 备防火墙配置

3.2.1 进入备设备命令行将备设备成员ID修改为2

将备设备成员ID配置为2，出现是否切换的提示后输入“Y”。

system-view

[H3C]irf member 1 renumber 2

Renumbering the member ID may result in configuration change or loss. Continue?[Y/N]:Y

[H3C]quit

3.2.2 成员ID修改为2后需要重启设备才能生效

输入reboot命令后设备会提示是否保存配置，输入“Y”，后面会出现是否重启设备提示，输入“Y”。

reboot

Start to check configuration with next startup configuration file, please wait.....DONE!

Current configuration may be lost after the reboot, save current configuration? [Y/N]:Y

This command will reboot the device. Continue? [Y/N]:Y

3.2.3 将需要进行堆叠配置的端口,2/0/14与2/0/15接口加入IRF端口

重启后设备成员ID变为2，物理端口加入IRF端口时需要先关闭端口，添加到IRF端口后再开启端口。

[H3C]interface range GigabitEthernet 2/0/14 to GigabitEthernet 2/0/15
[H3C-if-range]shutdown
[H3C-if-range]quit
[H3C]irf-port 2/1
[H3C-irf-port2/1]port group interface GigabitEthernet 2/0/14
[H3C-irf-port2/1]port group interface GigabitEthernet 2/0/15
[H3C-irf-port2/1]quit
[H3C]interface range GigabitEthernet 2/0/14 to GigabitEthernet 2/0/15
[H3C-if-range]undo shutdown
[H3C-if-range]quit

3.2.4 配置完成后激活IRF配置

使用“irf-port-configuration active”命令激活IRF配置，激活后备防火墙将重启，重启后加入堆叠组成为主防火墙的一部分。

[H3C]irf-port-configuration active

3.3 堆叠建立后配置BFD MAD检测

3.3.1 创建聚合组1并将物理端口接入聚合组

[H3C] interface route-aggregation 1
[H3C-Route-Aggregation1] quit
[H3C] interface gigabitethernet 1/0/13
[H3C-GigabitEthernet1/0/13] port link-aggregation group 1
[H3C-GigabitEthernet1/0/13] quit
[H3C] interface gigabitethernet 2/0/13
[H3C-GigabitEthernet2/0/13] port link-aggregation group 1
[H3C -GigabitEthernet2/0/13] quit

3.3.2 BFD MAD配置

进入聚合组1开启BFD检测并配置MAD检测IP地址。

[H3C] interface route-aggregation 1
[H3C-Route-Aggregation1] mad bfd enable
[H3C-Route-Aggregation1] mad ip address 192.168.10.1 24 member 1
[H3C-Route-Aggregation1] mad ip address 192.168.10.2 24 member 2
[H3C-Route-Aggregation1] quit

3.3.3 安全域配置

将route-aggregation 1接口加入“trust”区域

[H3C] security-zone name trust
[H3C-security-zone-Trust] import interface route-aggregation 1
[H3C-security-zone-Trust] quit

3.3.4 放通安全策略配置

防火墙目前版本存在两套安全策略，请在放通安全策略前确认设备运行那种类型的安全策略？以下配置任选其一。

1. 通过命令“display cu | in security-policy”如果查到命令行存在“security-policy disable”或者没有查到任何信息，则使用下面策略配置。

[H3C]display cu | in security-policy
security-policy disable

#创建对象策略pass。

[H3C]object-policy ip pass
[H3C-object-policy-ip-pass] rule 0 pass
[H3C-object-policy-ip-pass]quit

#创建Trust到Untrust域的域间策略调用pass策略。

[H3C]zone-pair security source Trust destination local
[H3C-zone-pair-security-Trust- local]object-policy apply ip pass
[H3C-zone-pair-security-Trust- local]quit
[H3C]zone-pair security source local destination Trust
[H3C-zone-pair-security-local -trust]object-policy apply ip pass
[H3C-zone-pair-security-local -trust]quit

2. 通过命令“display cu | in security-policy”如果查到命令行存在“security-policy ip”并且没有查到“security-policy disable”，则使用下面策略配置。

[H3C]display cu | in security-policy
security-policy ip

创建安全策略并放通local到trust和trust到local的安全策略。

[H3C]security-policy ip
[H3C-security-policy-ip]rule 10 name test
[H3C-security-policy-ip-10-test]action pass
[H3C-security-policy-ip-10-test]source-zone local
[H3C-security-policy-ip-10-test]source-zone Trust

[H3C-security-policy-ip-10-test]destination-zone local
[H3C-security-policy-ip-10-test]destination-zone Trust
[H3C-security-policy-ip-10-test]quit

4 检验配置结果

4.1.1 堆叠正常时查看MAD状态

看到BFD MAD已经开启

[H3C]display mad
MAD ARP disabled.
MAD ND disabled.
MAD LACP disabled.
MAD BFD enabled.

查看MAD状态

[H3C]display mad verbose
Multi-active recovery state: No
Excluded ports (user-configured):
Excluded ports (system-configured):
  GigabitEthernet1/0/14
  GigabitEthernet1/0/15
  GigabitEthernet2/0/14
  GigabitEthernet2/0/15
MAD ARP disabled.
MAD ND disabled.
MAD LACP disabled.
MAD BFD enabled interface: Route-Aggregation1
  MAD status   : Normal   \\MAD检测状态正常
  Member ID   MAD IP address   Neighbor   MAD status
  1   192.168.10.1/24   2   Normal
  2   192.168.10.2/24   1   Normal

4.1.2 堆叠分裂后时查看MAD状态

[H3C]display mad verbose
Multi-active recovery state: No
Excluded ports (user-configured):
Excluded ports (system-configured):
  GigabitEthernet1/0/14
  GigabitEthernet1/0/15
MAD ARP disabled.
MAD ND disabled.
MAD LACP disabled.
MAD BFD enabled interface: Route-Aggregation1
  MAD status   : Faulty   \\MAD状态为:Faulty状态说明堆叠分裂
  Member ID   MAD IP address   Neighbor   MAD status
  1   192.168.10.1/24   2   Faulty

此时使用“display interface brief down”查看端口时发现所有端口全部被关闭。

display interface brief down
Brief information on interfaces in route mode:
Link: ADM - administratively down; Stby - standby
Interface   Link   Cause
GE2/0/0   DOWN   MAD ShutDown
GE2/0/1   DOWN   MAD ShutDown
GE2/0/2   DOWN   MAD ShutDown
GE2/0/3   DOWN   MAD ShutDown
GE2/0/4   DOWN   MAD ShutDown
GE2/0/5   DOWN   MAD ShutDown
GE2/0/6   DOWN   MAD ShutDown
GE2/0/7   DOWN   MAD ShutDown
GE2/0/8   DOWN   MAD ShutDown
GE2/0/9   DOWN   MAD ShutDown
GE2/0/10   DOWN   MAD ShutDown
GE2/0/11   DOWN   MAD ShutDown
GE2/0/12   DOWN   MAD ShutDown
GE2/0/13   DOWN   DOWN (Link-Aggregation interface down)
GE2/0/16   DOWN   MAD ShutDown

配置关键点

4.1.3 注意事项

1、 MAD检测与BFD Session无关，堆叠建立或者堆叠分裂时通过“display bfd session”查看BFD状态都是DOWN状态。

```
[H3C]display bfd session
 Total Session Num: 1     Up Session Num: 0     Init Mode: Active
 IPv4 session working in control packet mode:
 LD/RD          SourceAddr      DestAddr        State    Holdtime    Interface
 97/0           192.168.10.1    192.168.10.2    Down     0ms         RAGG1
```