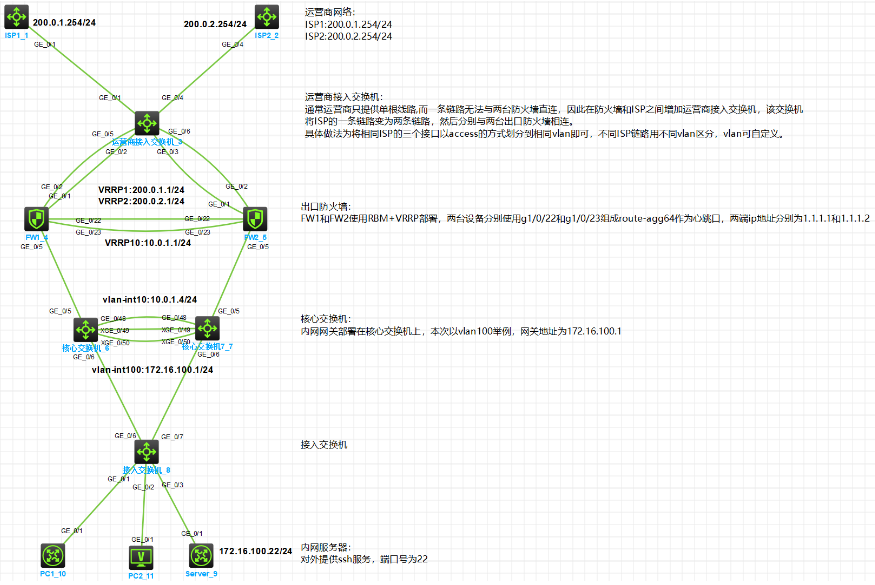
知 V7防火墙RBM+VRRP主备部署作为园区出口(下行交换机使用IRF或单机)

域间策略/安全域 VRRP 双机热备 NAT 保存上一跳 **薛佳宇** 2023-02-26 发表

组网及说明

一、拓扑



运营商网络:
ISP1:200.0.1.254/24
ISP2:200.0.2.254/24

运营商接入交换机:
通常运营商只提供单根线路,而一条链路无法与两台防火墙直连，因此在防火墙和ISP之间增加运营商接入交换机，该交换机将ISP的一条链路变为两条链路，然后分别与两台出口防火墙相连。
具体做法为将相同ISP的三个接口以access的方式划分到相同vlan即可，不同ISP链路用不同vlan区分，vlan可自定义。

出口防火墙:
FW1和FW2使用RBM+VRRP部署，两台设备分别使用g1/0/22和g1/0/23组成route-agg64作为心跳口，两端ip地址分别为1.1.1.1和1.1.1.2

核心交换机:
内网网关部署在核心交换机上，本次以vlan100举例，网关地址为172.16.100.1

接入交换机

内网服务器:
对外提供ssh服务，端口号为22

二、需求

1、 园区出口部署两台防火墙，使用RBM+VRRP方式实现主备

2、 从运营商租借两条ISP链路，要求两条链路同时使用，互为备份

3、 如运营商接入交换机上行链路出现故障，防火墙路由需快速感知到并切换

4、 内网核心交换机使用IRF实现高可靠性

5、 内网vlan 100:172.16.100.0/24可通过任意出口访问运营商网络

6、 内网和公网侧访问防火墙上任意ISP地址的TCP 2222端口都能访问到内网Server提供的ssh服务

7、 内网Server手工配置地址172.16.100.22，该地址不可分配给其他终端；PC1固定获取172.16.100.15地址，PC2随机获取地址。

三、配置思路

1、 运营商提供的单根线路无法与两台防火墙直连，因此在防火墙和ISP之间增加运营商接入交换机，该交换机将ISP的一条链路变为两条链路，然后分别与两台出口防火墙相连。具体做法为将相同ISP的三个接口以access的方式划分到相同vlan即可，不同ISP链路用不同vlan区分，vlan可自定义。

2、 每个ISP只提供了1个公网ip，所以防火墙上行连接到同一组ISP的接口可配置同网段的私网ip地址，将vrrp虚拟地址配置为ISP的ip地址即可，注意配置虚拟IP时需要配置掩码，掩码以ISP给的为准。

3、 为保证防火墙可快速感知到运营商接入交换机上行链路的状况，可配置nqa探测到ISP网关地址的状态，同时与track联动，防火墙配置的到各ISP的缺省路由再分别与track关联。

4、 为保证内网vlan100可以访问运营商网络，以及公网侧可以访问内网Server的服务，需在防火墙分别配置SNAT和DNAT。内网使用ISP地址访问Server的服务需配置双向NAT。

5、 防火墙各接口加入安全域并放行安全策略。

四、接口及地址规划

本端接口	vlan/ip	补充	对端
		运营商接入交换机	
G1/0/1	VLAN10	ISP1	ISP1
G1/0/2	VLAN10		FW1:G1/0/1
G1/0/3	VLAN10		FW2:G1/0/1
G1/0/4	VLAN20	ISP2	
G1/0/5	VLAN20		FW1:G1/0/2
G1/0/6	VLAN20		FW2:G1/0/2
		出口防火墙FW1	
G1/0/1	10.0.0.1/30	VRRP1:200.0.1.1/24 active	
G1/0/2	10.0.0.5/30	VRRP2:200.0.2.1/24 active	
G1/0/5	10.0.1.2/24	VRRP10:10.0.1.1/24 active	核心交换机6:G1/0/5
G1/0/22	Route-agg64，1.1.1.1/30	HA接口	FW2:G1/0/22
G1/0/23			FW2:G1/0/23
		出口防火墙FW2	
G1/0/1	10.0.0.2/30	VRRP1:200.0.1.1/24 standby	

G1/0/2	10.0.0.6/30	VRRP2:200.0.2.1/24 standby	
G1/0/5	10.0.1.3/24	VRRP10:10.0.1.1/24 standby	核心交换机7:G2/0/5
G1/0/22	Route-agg64，1.1.1.2/30	HA接口	FW1:G1/0/22
G1/0/23			FW1:G1/0/23
核心交换机6-slot1/核心交换机7-slot2(IRF)			
[illegible]	VLAN10	Vlan-int:10:10.0.1.4/24	FW1:G1/0/5
G2/0/5	VLAN10		FW2:G2/0/5
G1/0/48	VLAN4000	BFD MAD检测，1.1.1.5/30	核心交换机7:G2/0/48
G2/0/48	VLAN4000	BFD MAD检测，1.1.1.6/30	核心交换机6:G1/0/48
XG1/0/49	IRF-PORT1/1	IRF接口	核心交换机7:XG2/0/49
XG1/0/50			核心交换机7:XG2/0/50
XG2/0/49	IRF-PORT2/2	IRF接口	核心交换机6:XG1/0/49
XG2/0/50			核心交换机6:XG1/0/50
G1/0/6	Bridge-agg100 VLAN100	Trunk Vlan-int100:172.16.100.1/24	接入交换机:G1/0/6
G2/0/6			接入交换机:G1/0/7
接入交换机			
G1/0/6	Bridge-agg100	Trunk	核心交换机6:G1/0/6
G1/0/7	VLAN100		核心交换机7:G2/0/6
G1/0/1	Access		PC1
G1/0/2	Vlan100		PC2
G1/0/3			Server
终端			
PC1	Dhcp自动获取	获取固定ip 172.16.100.15	接入交换机:G1/0/1
PC2	Dhcp自动获取	自动分配	接入交换机:G1/0/2
Server	172.16.100.22	对外提供ssh服务	接入交换机:G1/0/3

配置步骤

HCL模拟器工程文件已上传至HCLhub：http://hclhub.h3c.com/project/9466/summary/master?path=README.md&type=text

如链接失效可登录http://hclhub.h3c.com/ 搜索：v7_防火墙_rbm_双机主备

(1) 运营商接入交换机

1、配置将IPS1的三个接口划分到vlan 10，将ISP2的三个接口划分到vlan20

```
#创建vlan10，并将接口g1/0/1~g1/0/3划分到vlan10
#
system-view
#
vlan 10
port GigabitEthernet 1/0/1 GigabitEthernet 1/0/2 GigabitEthernet 1/0/3
quit
#
#创建vlan20，并将接口g1/0/4~g1/0/6划分到vlan20
#
vlan 20
port GigabitEthernet 1/0/4 GigabitEthernet 1/0/5 GigabitEthernet 1/0/6
quit
#
#保存配置
save force
```

(2) 出口防火墙

1、 完成FW1和FW2的RBM基础配置

```
#创建三层聚合口64，并将接口g1/0/22和接口g1/0/23加入该聚合口。该聚合口将作为FW之间RBM的数据/控制通道，同时为接口配置控制通道IP。
#
system-view
#
sysname FW1
#
interface Route-Aggregation64
ip address 1.1.1.1 255.255.255.252
#
interface GigabitEthernet1/0/22
port link-aggregation group 64
#
interface GigabitEthernet1/0/23
port link-aggregation group 64
#完成RBM配置，指定数据通道为Route-Aggregation64，HA回切时间为10分钟，控制通道本段ip地址为1.1.1.1，对端ip地址为1.1.1.2，本设备作为主管理设备。
remote-backup group
 data-channel interface Route-Aggregation64
 delay-time 10
 local-ip 1.1.1.1
 remote-ip 1.1.1.2
 device-role primary
#
```

```
#FW2此部分配置与FW1类似。
#
system-view
#
sysname FW2
#
interface Route-Aggregation64
ip address 1.1.1.2 255.255.255.252
#
interface GigabitEthernet1/0/22
port link-aggregation group 64
#
interface GigabitEthernet1/0/23
port link-aggregation group 64
#
remote-backup group
 data-channel interface Route-Aggregation64
 delay-time 10
 local-ip 1.1.1.2
 remote-ip 1.1.1.1
 device-role secondary
#
```

2、 完成FW1和FW2的VRRP配置

```
#ISP只提供了1个公网ip，所以防火墙上行连接到同一组ISP的接口可配置同网段的
私网ip地址，将vrrp虚拟地址配置为ISP的ip地址即可，注意配置虚拟IP时需要配置掩
码，掩码以ISP给的为准。
#配置VRRP时需要与RBM关联(主设备命令后增加active，反之standby)
#因防火墙为双出口，为了保证源进源出，在公网口配置ip last-hop hold。
#
interface GigabitEthernet1/0/1
port link-mode route
ip address 10.0.0.1 255.255.255.252
vrrp vrid 1 virtual-ip 200.0.1.1 255.255.255.0 active
ip last-hop hold
#
interface GigabitEthernet1/0/2
port link-mode route
ip address 10.0.0.5 255.255.255.252
vrrp vrid 2 virtual-ip 200.0.2.1 255.255.255.0 active
ip last-hop hold
#
interface GigabitEthernet1/0/5
port link-mode route
ip address 10.0.1.2 255.255.255.0
vrrp vrid 10 virtual-ip 10.0.1.1 255.255.255.0 active
#
#FW2的部分配置与FW1类似。
#
interface GigabitEthernet1/0/1
port link-mode route
ip address 10.0.0.2 255.255.255.252
vrrp vrid 1 virtual-ip 200.0.1.1 255.255.255.0 standby
ip last-hop hold
#
interface GigabitEthernet1/0/2
port link-mode route
ip address 10.0.0.6 255.255.255.252
vrrp vrid 2 virtual-ip 200.0.2.1 255.255.255.0 standby
ip last-hop hold
#
interface GigabitEthernet1/0/5
port link-mode route
ip address 10.0.1.3 255.255.255.0
vrrp vrid 10 virtual-ip 10.0.1.1 255.255.255.0 standby
#
```

3、完成FW1和FW2的track和路由配置

```
#完成nqa配置，用于探测防火墙到各ISP网关地址的连通性，探测方式为icmp，探
测间隔为100ms，超时时间为500ms，连续5次不通即探测失败。
#
nqa entry isp1 main
type icmp-echo
destination ip 200.0.1.254
frequency 100
next-hop ip 200.0.1.254
probe timeout 500
reaction 1 checked-element probe-fail threshold-type consecutive 5 action-type trigg
er-only
#
nqa entry isp2 main
type icmp-echo
destination ip 200.0.2.254
frequency 100
next-hop ip 200.0.2.254
probe timeout 500
reaction 1 checked-element probe-fail threshold-type consecutive 5 action-type trigg
er-only
#
#启动nqa探测，并配置track与nqa联动
#
nqa schedule isp1 main start-time now lifetime forever
nqa schedule isp2 main start-time now lifetime forever
#
track 1 nqa entry isp1 main reaction 1
#
track 2 nqa entry isp2 main reaction 1
#
#配置缺省路由与track项关联，同时配置去往内网vlan100的回程路由
#
ip route-static 0.0.0.0 0 200.0.1.254 track 1
ip route-static 0.0.0.0 0 200.0.2.254 track 2
ip route-static 172.16.100.0 24 10.0.1.100
#
```

配置关键点

1、 防火墙查看RBM和VRRP状态，FW1为主，FW2为备

```
#FW1
RBM_P<FW1>dis remote-backup-group status
Remote backup group information:
  Backup mode: Active/standby   -----------备份组模式为主/备
  Device management role: Primary-----------设备管理状态为主
  Device running status: Active -----------设备运行状态为主
  Data channel interface: Route-Aggregation64
  Local IP: 1.1.1.1
  Remote IP: 1.1.1.2    Destination port: 60064
  Control channel status: Connected
  Keepalive interval: 1s
  Keepalive count: 10
  Configuration consistency check interval: 24 hour
  Configuration consistency check result: Not Performed
  Configuration backup status: Auto sync enabled
  Session backup status: Hot backup enabled
  Delay-time: 10 min
  Uptime since last switchover: 0 days, 15 hours, 29 minutes
  Switchover records:
    Time                    Status change        Cause
    2023-02-25 22:31:08   Standby to Active    Interface status changed
RBM_P<FW1>
RBM_P<FW1>dis vrrp
IPv4 Virtual Router Information:
 Running mode       : Standard
 RBM control channel is established
   VRRP active group status : Master
   VRRP standby group status: Master
 Total number of virtual routers : 3
 Interface          VRID  State       Running Adver   Auth          Virtual
                                       Pri     Timer   Type          IP
 ---------------------------------------------------------------------------
 GE1/0/1            1     Master      100     100     Not supported    200.0.1.1
 GE1/0/2            2     Master      100     100     Not supported    200.0.2.1
 GE1/0/5            10    Master      100     100     Not supported    10.0.1.1
RBM_P<FW1>
```

```
#FW2
RBM_S<FW2>dis remote-backup-group status
Remote backup group information:
  Backup mode: Active/standby
  Device management role: Secondary
  Device running status: Standby
  Data channel interface: Route-Aggregation64
  Local IP: 1.1.1.2
  Remote IP: 1.1.1.1    Destination port: 60064
  Control channel status: Connected
  Keepalive interval: 1s
  Keepalive count: 10
  Configuration consistency check interval: 24 hour
  Configuration consistency check result: Not Performed
  Configuration backup status: Auto sync enabled
  Session backup status: Hot backup enabled
  Delay-time: 10 min
  Uptime since last switchover: 0 days, 15 hours, 32 minutes
  Switchover records:
    Time                    Status change        Cause
    2023-02-25 22:31:08   Active to Standby    Interface status changed
RBM_S<FW2>
RBM_S<FW2>dis vrrp
IPv4 Virtual Router Information:
 Running mode       : Standard
 RBM control channel is established
   VRRP active group status : Backup
   VRRP standby group status: Backup
 Total number of virtual routers : 3
 Interface          VRID  State       Running Adver   Auth          Virtual
                                       Pri     Timer   Type          IP
 ---------------------------------------------------------------------------
 GE1/0/1            1     Backup      100     100     Not supported    200.0.1.1
 GE1/0/2            2     Backup      100     100     Not supported    200.0.2.1
 GE1/0/5            10    Backup      100     100     Not supported    10.0.1.1
RBM_S<FW2>
```

2、 核心交换机IRF状态正常

```
<CORE>dis irf
MemberID    Role    Priority  CPU-Mac         Description
 *+1        Master  1         902f-b99b-0604  ---
   2        Standby 1         9035-7748-0704  ---
--------------------------------------------------------
 * indicates the device is the master.
 + indicates the device through which the user logs in.

 The bridge MAC of the IRF is: 902f-b99b-0600
```

```
#FW2此部分配置与FW1类似。
#
nqa entry isp1 main
 type icmp-echo
  destination ip 200.0.1.254
  frequency 1000
  next-hop ip 200.0.1.254
  probe timeout 500
  reaction 1 checked-element probe-fail threshold-type consecutive 5 action-type trigg
```