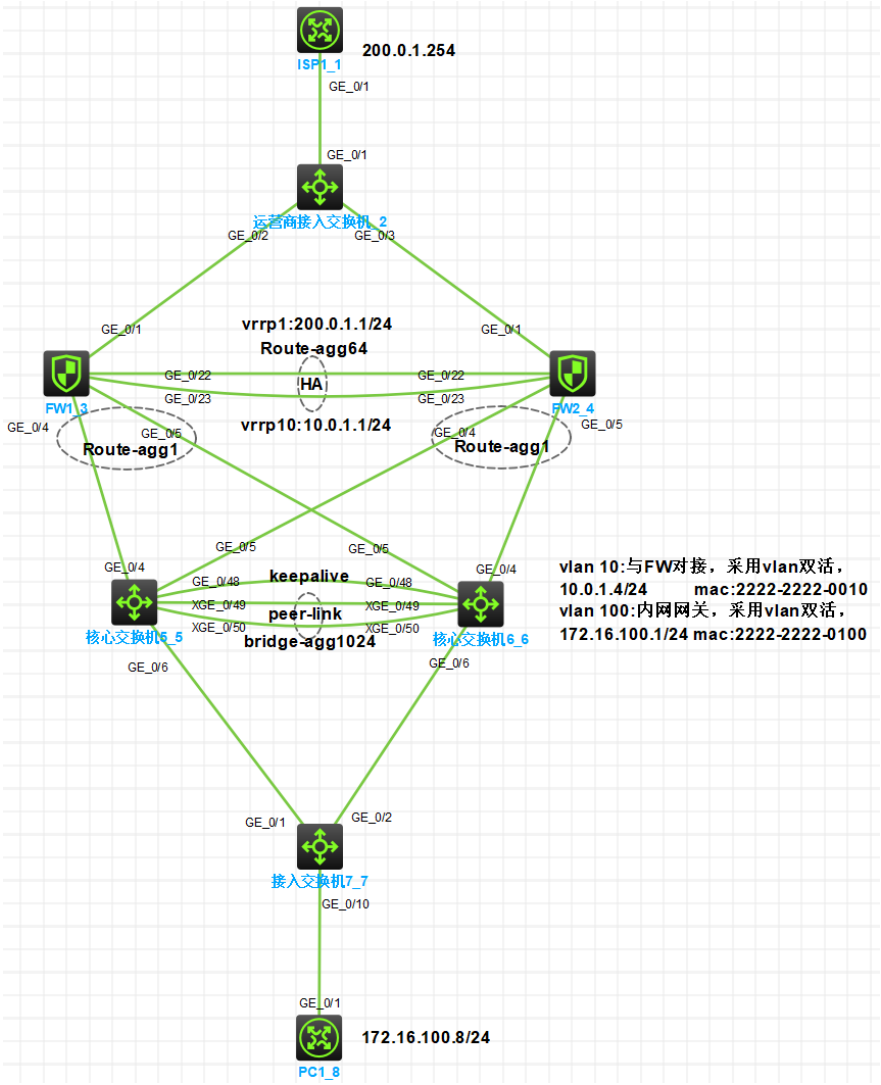
V7防火墙RBM+VRRP主备部署作为园区出口(下行交换机使用M-LAG)

VRRP 双机热备 NAT 薛佳宇 2023-02-27 发表

组网及说明

一、拓扑



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、 从运营商租借一条ISP链路，要求两条链路同时使用，互为备份
3、 内网核心交换机使用M-LAG实现高可靠性
4、 内网vlan 100:172.16.100.0/24可通过任意出口访问运营商网络
5、 内网PC可访问ISP网络。

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、 为保证内网vlan100可以访问运营商网络，需在防火墙分别配置SNAT。
4、 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
出口防火墙FW1			

G1/0/1	10.0.0.1/30	VRRP1:200.0.1.1/24 active	运营商接入:G1/0/2
G1/0/4	Route-agg1	VRRP10:10.0.1.1/24 active	核心交换机5G1/0/4
G1/0/5	10.0.1.2/24		核心交换机6:G1/0/5
G1/0/22	Route-agg64，1	HA接口	FW2:G1/0/22
G1/0/23	.1.1.1/30		FW2:G1/0/23
出口防火墙FW2			
G1/0/1	10.0.0.2/30	VRRP1:200.0.1.1/24 active	运营商接入:G1/0/3
G1/0/4	Route-agg1	VRRP10:10.0.1.1/24 active	核心交换机5G1/0/5
G1/0/5	10.0.1.3/24		核心交换机6:G1/0/4
G1/0/22	Route-agg64，1	HA接口	FW1:G1/0/22
G1/0/23	.1.1.2/30		FW1:G1/0/23
核心交换机5			
XG1/0/49	Bridge-agg100	Peer-link	核心交换机6:XG1/0/49
XG1/0/52			核心交换机6:XG1/0/50
G1/0/48	1.1.1.5/30	VRF:mlag keepalive	核心交换机6:G1/0/48
G1/0/4	Bridge-agg1	Vlan-int10:	FW1:G1/0/4
G1/0/5	Bridge-agg2	10.0.1.4/24 2222-2222-0010	FW2:G1/0/4
G1/0/6	Bridge-agg100	Vlan-int100:	接入交换机:G1/0/1
	m-lag group100	172.16.100.1/24 2222-2222-0100	
核心交换机6			
XG1/0/49	Bridge-agg100	Peer-link	核心交换机5:XG1/0/49
XG1/0/52			核心交换机5:XG1/0/50
G1/0/48	1.1.1.6/30	VRF:mlag keepalive	核心交换机5:G1/0/48
G1/0/4	Bridge-agg2	Vlan-int10:	FW2:G1/0/5
	m-lag group2	10.0.1.4/24 2222-2222-0010	
G1/0/5	Bridge-agg1		FW1:G1/0/5
G1/0/6	Bridge-agg100	Vlan-int100:	接入交换机:G1/0/2
	m-lag group100	172.16.100.1/24 2222-2222-0100	
接入交换机			
G1/0/1	Bridge-agg	Trunk	核心交换机5:G1/0/6
G1/0/2	VLAN100		核心交换机6:G1/0/6
G1/0/10	Access Vlan100		PC1
终端			
PC1	172.16.100.8/24		接入交换机:G1/0/10

配置步骤

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

如连接失效可登录http://hclhub.h3c.com/，搜索：yzfw_rbm_vrrp_主备_to_mlag

配置步骤

(1) 运营商接入交换机

1、 配置将IP S1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
#
vlan 10
port GigabitEthernet 1/0/1 GigabitEthernet 1/0/2 GigabitEthernet 1/0/3
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。
#
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)
#
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
#
interface Route-Aggregation1
 ip address 10.0.1.2 255.255.255.0
 link-aggregation mode dynamic
 vrrp vrid 10 virtual-ip 10.0.1.1 255.255.255.0 active
#
interface GigabitEthernet1/0/4
port link-aggregation group 1
#
interface GigabitEthernet1/0/5
port link-aggregation group 1
#
```

配置关键点

1、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。

2、配置VRRP时需要与RBM关联(主设备命令后增加active，反之standby)

```
#FW2此部分配置与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
#
#
interface Route-Aggregation1
 ip address 10.0.1.2 255.255.255.0
 link-aggregation mode dynamic
 vrrp vrid 10 virtual-ip 10.0.1.1 255.255.255.0 standby
#
interface GigabitEthernet1/0/4
port link-aggregation group 1
#
interface GigabitEthernet1/0/5
port link-aggregation group 1
#
```

3、 完成FW1和FW2的nqa、track和路由配置

```
#配置缺省路由，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
ip route-static 172.16.100.0 24 10.0.1.4
#
```

```
#FW2此部分配置与FW1类似。
#
ip route-static 0.0.0.0 0 200.0.1.254
ip route-static 172.16.100.0 24 10.0.1.4
#
```

4、 完成FW的安全域配置(此部分配置主管理设备会实时同步给备管理设备)

```
#配置将内网接口Route-Aggregation1加入trust区域，将ISP1接口g1/0/1加入untrust
区域。
#
security-zone name Trust
import interface Route-Aggregation1
quit
#
security-zone name Untrust
import interface GigabitEthernet1/0/1
quit
#
```

5、 完成FW的全局NAT配置(此部分配置主管理设备会实时同步给备管理设备)

```
#配置nat地址组，用于源地址转换，同时各地址组与接口的VRRP备份组关联
#
nat address-group 1 name isp1
address 200.0.1.1 200.0.1.1
vrrp vrid 1
quit
#
nat global-policy
#配置名为trust2isp的规则，用于匹配由trust域访问untrust域，源地址是172.16.100.
0/24的流量，匹配上后执行源地址转换，转换后的源ip为nat地址组1 中的地址。
  rule name trust2isp
  source-zone trust
  destination-zone untrust
  source-ip subnet 172.16.100.0 24
  action snat address-group 1 vrrp 1
```

6、 完成FW的安全策略配置(此部分配置主管理设备会实时同步给备管理设备)

```
#
security-policy ip
#创建名为trust2untrust的安全策略规则rule 5，匹配源域为trust，目的域为untrust或untrust2，源地址为172.16.100.0/24的流量，动作为允许。（对应内网vlan100访问互联网的需求）
 rule 5 name trust2untrust
  action pass
  source-zone trust
  destination-zone untrust
```