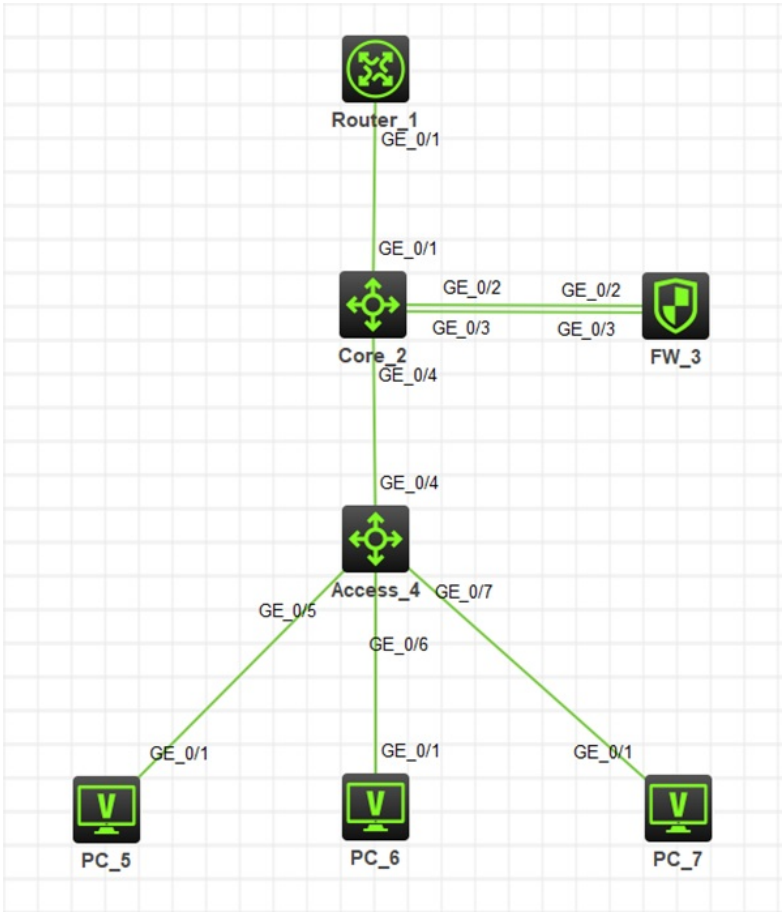
V7 防火墙单机旁路部署(网关在防火墙)

域间策略/安全域 **薛佳宇** 2022-07-12 发表

组网及说明

防火墙旁路部署在核心交换机上，内网有三个网段vlan 10：172.16.10.1/24、vlan 20：172.16.20.1/24、vlan30：172.16.30.1。要求内网网关在防火墙设备上，由防火墙作为DHCP服务器给终端下发地址，同时由防火墙来控制禁止vlan10访问vlan 20，禁止vlan20访问vlan30，其他不做限制。



配置思路：

1、 接入交换机根据业务需求，将不同的接口划入指定vlan

2、 接入交换机和核心交换机互联接口配置成trunk模式，放行三个业务vlan

3、 核心交换机与防火墙互联的链路1(G1/0/3)的接口配置成trunk模式，放行三个业务vlan，内网流量通过这跟线路进入防火墙

4、 核心交换机与防火墙互联的链路2(G1/0/2)，交换机侧接口工作在access模式，划入vlan5。防火墙侧接口工作在三层模式，链路2三层互联，防火墙处理完的流量经过这跟链路回到核心交换机

5、 核心交换机与出口路由器配置互联地址，核心交换机写默认路由指向出口路由器，出口路由器针对内网网段写回程路由指向核心交换机,核心交换机写回程路由指向防火墙

6、 防火墙配置DHCP及安全策略

配置步骤

1、 配置接入交换机Access

```
<Access>sys
#创建业务vlan
[Access]vlan 10
[Access-vlan10]quit
[Access]vlan 20
[Access-vlan20]quit
[Access]vlan 30
[Access-vlan30]quit
[Access]
#根据业务需要将不同的终端接口划分到不同的vlan
[Access]inter GigabitEthernet 1/0/5
[Access-GigabitEthernet1/0/5]port access vlan 10
[Access-GigabitEthernet1/0/5]quit
[Access]
[Access]inter GigabitEthernet 1/0/6
[Access-GigabitEthernet1/0/6]port access vlan 20
[Access-GigabitEthernet1/0/6]quit
[Access]
[Access]inter GigabitEthernet 1/0/7
[Access-GigabitEthernet1/0/7]port access vlan 30
[Access-GigabitEthernet1/0/7]quit
[Access]
#将接入交换机上行口配置成trunk模式，允许vlan10、20、30通过，禁止vlan1通行
[Access]inter GigabitEthernet 1/0/4
[Access-GigabitEthernet1/0/4]port link-type trunk
[Access-GigabitEthernet1/0/4]port trunk permit vlan 10 20 30
[Access-GigabitEthernet1/0/4]undo port trunk permit vlan 1
[Access-GigabitEthernet1/0/4]qu
#保存配置
[Access] save force
```

2、 配置核心交换机Core

```
<Core>system-view
#创建业务vlan
[Core]vlan 10
[Core-vlan10]quit
[Core]vlan 20
[Core-vlan20]quit
[Core]vlan 30
[Core-vlan30]quit
[Core]vlan 5
[Core-vlan5]quit
[Core]vlan 6
[Core-vlan6]quit
[Core]
#配置连接接入交换机下行口为trunk模式，允许vlan10、20、30通过，禁止vlan1通行
[Core]inter GigabitEthernet 1/0/4
[Core-GigabitEthernet1/0/4]port link-type trunk
[Core-GigabitEthernet1/0/4]port trunk permit vlan 10 20 30
[Core-GigabitEthernet1/0/4]undo port trunk permit vlan 1
[Core-GigabitEthernet1/0/4]qu
[Core]
#配置连接防火墙的接口(链路1)为trunk模式，允许vlan10、20、30通过，禁止vlan1通行
[Core]inter GigabitEthernet 1/0/3
[Core-GigabitEthernet1/0/3]port link-type trunk
[Core-GigabitEthernet1/0/3]port trunk permit vlan 10 20 30
[Core-GigabitEthernet1/0/3]undo port trunk permit vlan 1
[Core-GigabitEthernet1/0/3]quit
```

[Core]
#配置连接防火墙的接口(链路2)属于vlan5
[Core]inter GigabitEthernet 1/0/2
[Core-GigabitEthernet1/0/2]port access vlan 5
[Core-GigabitEthernet1/0/2]quit
[Core]
#配置连接路由器的接口属于vlan6
[Core]inter g 1/0/1
[Core-GigabitEthernet1/0/1]port access vlan 6
[Core-GigabitEthernet1/0/1]quit
[Core]
#配置交换机和防火墙的互联地址10.0.23.2/24
[Core]inter vlan 5
[Core-Vlan-interface5]ip address 10.0.23.2 24
[Core-Vlan-interface5]qu
[Core]
#配置交换机和路由器的互联地址10.0.12.2/24
[Core]inter vlan 6
[Core-Vlan-interface6]ip address 10.0.12.2 24
[Core-Vlan-interface6]quit
[Core]
#配置默认路由指向出口路由器
[Core]ip route-static 0.0.0.0 0 10.0.12.1
#配置内网网段回程路由指向防火墙
[Core]ip route-static 172.16.10.0 24 10.0.23.3
[Core]ip route-static 172.16.20.0 24 10.0.23.3
[Core]ip route-static 172.16.30.0 24 10.0.23.3
#保存配置
[Core] save force

3、 配置防火墙，默认登陆用户名和密码均为admin
Login: admin
Password: admin
<H3C>sys
[H3C]sysname FW
#创建业务vlan
[FW]vlan 10
[FW-vlan10]quit
[FW]vlan 20
[FW-vlan20]quit
[FW]vlan 30
[FW-vlan30]quit
[FW]
#配置连接交换机的接口(链路1)为trunk模式，允许vlan10、20、30通过，禁止vlan1通行
[FW]inter GigabitEthernet 1/0/3
[FW-GigabitEthernet1/0/3]port link-mode bridge
[FW-GigabitEthernet1/0/3]port link-type trunk
[FW-GigabitEthernet1/0/3]port trunk permit vlan 10 20 30
[FW-GigabitEthernet1/0/3]undo port trunk permit vlan 1
[FW-GigabitEthernet1/0/3]quit
[FW]
#配置连接交换机的接口(链路2)互联地址10.0.23.3/24
[FW]inter GigabitEthernet 1/0/2
[FW-GigabitEthernet1/0/2]ip address 10.0.23.3 24
[FW-GigabitEthernet1/0/2]quit
[FW]
#创建业务vlan的网关接口
[FW]inter vlan 10
[FW-Vlan-interface10]ip address 172.16.10.1 24
[FW-Vlan-interface10]quit
[FW]
[FW]inter vlan 20
[FW-Vlan-interface20]ip address 172.16.20.1 24
[FW-Vlan-interface20]quit

配置关键点
1、安全策略按照由上往下policy-ip看到的顺序从上往下匹配
2、配置安全策略前，先想一下流量走向，即流量从哪个接口进，又从哪个接口出，这样就可以根据接口确定源/目安全域了

[FW]
[FW]inter vlan 30
[FW-Vlan-interface30]ip address 172.16.30.1 24
[FW-Vlan-interface30]quit
[FW]
#创建业务vlan的dhcp地址池
[FW]dhcp server ip-pool vlan10