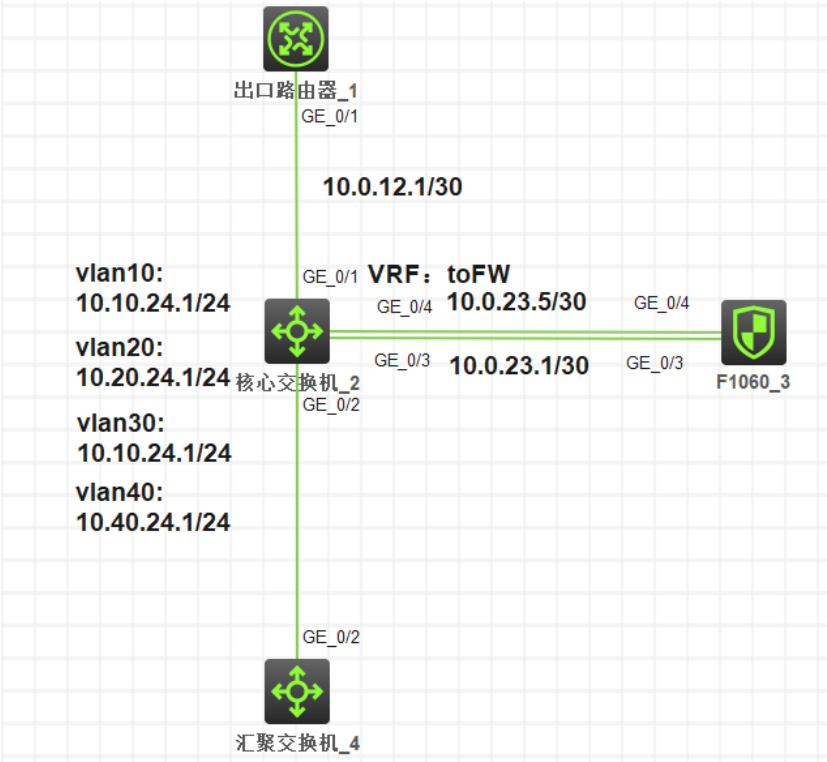
V7防火墙三层旁路部署(VRF方式)

BYPASS NQA VRF 设备部署方式 Track 薛佳宇 2021-12-18 发表

组网及说明



出口路由器	G0/1	10.0.12.1/30
核心交换机	G1/0/1(VRF:tofw)	10.0.12.2/30
	G1/0/4(VRF:tofw)	10.0.23.5/30
	G1/0/3	10.0.23.1/30
	Vlan-int10	10.10.24.1/24
防火墙	G1/0/4	10.0.23.6/30
	G1/0/3	10.0.23.2/30

要求：

1、 防火墙三层旁路部署在核心交换机上

2、 内网所有网段网关都在核心交换机上，要求所有访问外网的正反向流量都经过防火墙处理

3、 当防火墙与核心交换机互联的任意链路故障，流量依旧可以由交换机正常转发

配置步骤

Ps：内网以vlan 10为例，其他内网网段配置过程一样

一、出口路由器配置

```
<H3C>system-view
[H3C]sysname Router
[Router]
#配置下行接口IP地址
[Router]inter GigabitEthernet 0/1
[Router-GigabitEthernet0/1]ip address 10.0.12.1 30
[Router-GigabitEthernet0/1]qu
[Router]
#配置内网网段的回程路由，下一跳为核心交换机与路由器互联接口的地址
[Router]ip route-static 10.10.24.0 24 10.0.12.2
#保存配置
 Router]save force
 Validating file. Please wait...
 Configuration is saved to device successfully.
```

二、汇聚交换机配置

```
<H3C>system-view
[H3C]sysname L2 SW
[L2 SW]
#创建业务vlan10
[L2 SW]vlan 10
[L2 SW-vlan10]quit
[L2 SW]
#配置上行接口为trunk模式，允许vlan10通过，禁止vlan1通过(非必配)
[L2 SW]inter GigabitEthernet 1/0/2
[L2 SW-GigabitEthernet1/0/2]port trunk permit vlan 10
[L2 SW-GigabitEthernet1/0/2]undo port trunk permit vlan 1
[L2 SW-GigabitEthernet1/0/2]qu
[L2 SW]
#保存配置
[L2 SW]save force
Validating file. Please wait...
 Saved the current configuration to mainboard device successfully.
```

三、核心交换机配置

```
<H3C>system-view
#创建VRF，名称为tofw
[Core]ip vpn-instance tofw
[Core-vpn-instance-tofw]qu
[Core]
#创建业务vlan10
[Core]vlan 10
[Core-vlan10]qu
[Core]
#配置连接汇聚交换机的接口为trunk模式，允许vlan10通过，禁止vlan1通过(非必配)
[Core]inter GigabitEthernet 1/0/2
[Core-GigabitEthernet1/0/2]port link-type trunk
[Core-GigabitEthernet1/0/2]port trunk permit vlan 10
[Core-GigabitEthernet1/0/2]undo port trunk permit vlan 1
[Core-GigabitEthernet1/0/2]qu
[Core]
#创建vlan-interface 10作为业务网关，地址为10.10.24.1/24
[Core]inter vlan 10
[Core-Vlan-interface10]ip address 10.10.24.1 24
[Core-Vlan-interface10]qu
[Core]
#配置连接防火墙的第一个接口为三层模式，地址为10.0.23.1/30，这个接口作为内网流量出交换
```

机进入防火墙的接口

[Core]inter GigabitEthernet 1/0/3

[Core-GigabitEthernet1/0/3]port link-mode route

[Core-GigabitEthernet1/0/3]ip address 10.0.23.1 30

配置关键点

[Core-GigabitEthernet1/0/3]qu

#为了防止防火墙与核心交换机的任意互联链路故障，回程流量无法正常发送到内网，所以需要保证在故障场景，VRF fw中有到内网网段的路由，下面通过路由复制+EAA策略的方式来实现故障期间复制缺省public实例的内网路由，非故障期间使用手动的静态路由

[Core]inter GigabitEthernet 1/0/4

[Core-GigabitEthernet1/0/4]port link-mode route