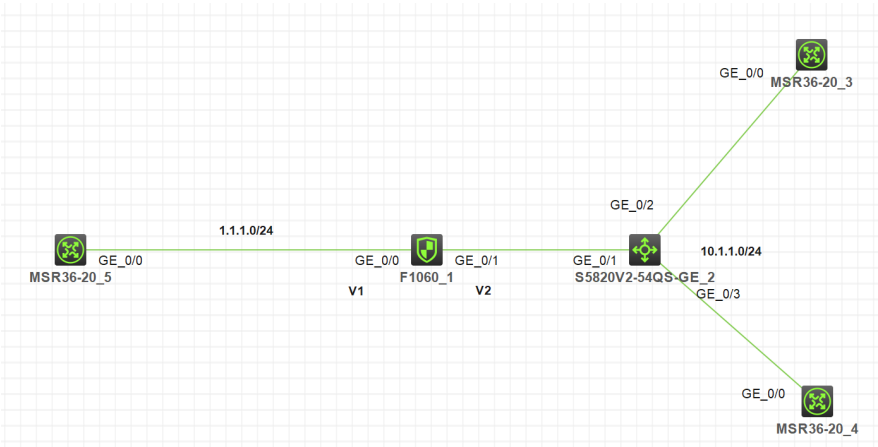
跨VPN实例的NAT hairpin功能的实现

NAT 孔凡安 2022-02-19 发表

组网及说明



注：如无特别说明，描述中的FW1或R1对应拓扑中设备名称末尾数字为1的设备，R2对应拓扑中设备名称末尾数字为2的设备，以此类推。

组网说明：R5模拟外网设备，FW1作为出口防火墙，外网口G1/0/0做了nat outbound和nat server（映射内网服务器R3,ip.addr = 10.1.1.3）。交换机作为纯二层设备。FW上对应两个VPN实例，v1和v2,分别绑定外网口和内网口。

要求：

1. R5能通过公网地址(ip.addr = 1.1.1.11)访问到内网服务器R3
2. R4能通过公网地址（ip.addr =1.1.1.11）访问到R3

配置步骤

路由器相关配置：
配置IP地址和相应的路由，保证内网路由器网关在FW上。

防火墙配置：

```
#
ip vpn-instance v1
#
ip vpn-instance v2
#
interface GigabitEthernet1/0/0
 port link-mode route
 combo enable copper
 ip binding vpn-instance v1        //配置该条命令时，接口下配置会清空，需要先绑定VPN实例
 ip address 1.1.1.1 255.255.255.0
 nat outbound vpn-instance v1
 nat server global 1.1.1.11 vpn-instance v1 inside 10.1.1.3 vpn-instance v2            //注意绑定VPN实例
#
interface GigabitEthernet1/0/1
 port link-mode route
 combo enable copper
 ip binding vpn-instance v2
 ip address 10.1.1.1 255.255.255.0
 nat hairpin enable        //nat hairpin下发在内网口
#
security-zone name Trust
 import interface GigabitEthernet1/0/1
#
security-zone name Untrust
 import interface GigabitEthernet1/0/0

#
 ip route-static vpn-instance v2 0.0.0.0 0 vpn-instance v1 1.1.1.5    //一定要配置，不然无法触发nat hairpin的功能
#
security-policy ip
 rule 0 name v1
  action pass
  vrf v2            //安全策略处于简单考虑，作了全通配置，需要绑定源安全域所在的vpn实例
```

分析：由于跨了VPN实例，所以查看会话会有两条。

```
<H3C>dis session ta ipv4 v
Slot 1:
Total sessions found: 0
<H3C>dis session ta ipv4 v
Slot 1:
Initiator:
  Source      IP/port: 1.1.1.1/17
  Destination IP/port: 1.1.1.11/2048
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: v1/-/-
  Protocol: ICMP(1)
  Inbound interface: GigabitEthernet1/0/0
  Source security zone: Untrust
Responder:
  Source      IP/port: 10.1.1.3/17
  Destination IP/port: 1.1.1.1/0
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: v2/-/-
```

Protocol: ICMP(1)

Inbound interface: GigabitEthernet1/0/1

Source security zone: Trust

State: ICMP_REPLY

Application: ICMP

Rule ID: 0

Rule name: v1

Start time: 2022-02-19 01:30:56 TTL: 26s

Initiator->Responder: 1 packets 84 bytes

配置关键点

需要在防火墙上配置跨VPN实例的缺省路由。

ip route-static vpn-instance v2 0.0.0.0 0 vpn-instance v1 1.1.1.5