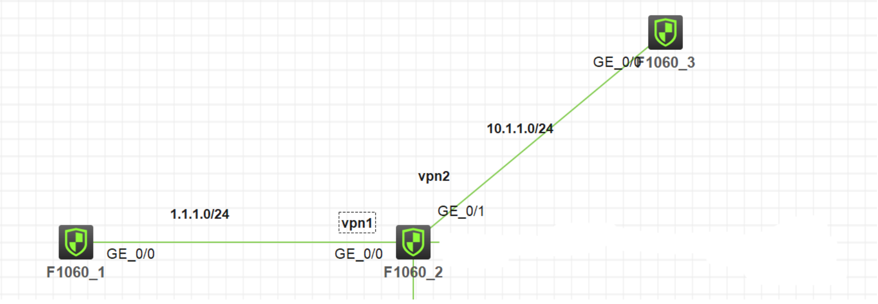
VRF场景下DNAT+SNAT典型配置举例

VRF NAT 孔凡安 2022-10-05 发表

组网及说明



注：如无特别说明，描述中的 FW1 或 MSR1 对应拓扑中设备名称末尾数字为 1 的设备，FW2 或 MSR2 对应拓扑中设备名称末尾数字为 2 的设备，以此类推；另外，同一网段中，IP 地址的主机位为其设备编号，如 FW1 的 g0/0 接口若在 1.1.1.0/24 网段，则其 IP 地址为 1.1.1.1/24，以此类推。

实验说明：

1. FW1位于公网侧，通过SSH访问内网服务器（FW3代替）。
2. FW2未NAT设备，GE1/0/0位于untrust安全域，vpn实例为v1；GE1/0/1位于trust安全域，vpn实例为v2。
3. FW上GE1/0/0配置内部服务器映射DNAT，GE1/0/1配置SNAT。
4. FW1和FW3的配置略过。

配置步骤

1. VPN实例

```
#
ip vpn-instance v1
#
ip vpn-instance v2
```

2. NAT相关配置

```
#
nat address-group 1 address 10.1.1.12 10.1.1.12
#
acl advanced 3001
 rule 0 permit ip vpn-instance v1 source 1.1.1.1 0
```

3. 接口配置

```
#
interface GigabitEthernet1/0/0
 port link-mode route
 combo enable copper
 ip binding vpn-instance v1
 ip address 1.1.1.2 255.255.255.0
 nat server protocol tcp global 1.1.1.12 22 vpn-instance v1 inside 10.1.1.3 22 vpn-instance v2
#
interface GigabitEthernet1/0/1
 port link-mode route
 combo enable copper
 ip binding vpn-instance v2
 ip address 10.1.1.2 255.255.255.0
 nat outbound 3001 address-group 1 vpn-instance v2
```

4. 安全策略

```
security-policy ip
 rule 1 name u2t
  action pass
  vrf v2
  source-zone untrust
  destination-zone trust
  source-ip src
  destination-ip dst-v2
#
object-group ip address dst-v2
 0 network host address 10.1.1.3
#
object-group ip address src
 0 network host address 1.1.1.1
#
security-zone name Trust
 import interface GigabitEthernet1/0/1
#
security-zone name Untrust
 import interface GigabitEthernet1/0/0
```

会话信息：

```
Slot 1:
Initiator:
  Source      IP/port: 1.1.1.1/3078
  Destination IP/port: 1.1.1.12/22
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: v1/-/-
  Protocol: TCP(6)
  Inbound interface: GigabitEthernet1/0/0
  Source security zone: Untrust
Responder:
  Source      IP/port: 10.1.1.3/22
  Destination IP/port: 10.1.1.12/1029
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: v2/-/-
  Protocol: TCP(6)
  Inbound interface: GigabitEthernet1/0/1
  Source security zone: Trust
State: TCP_ESTABLISHED
Application: SSH
Rule ID: 1
Rule name: u2t
Start time: 2022-10-05 12:25:44  TTL: 1186s
Initiator->Responder:          8 packets       1241 bytes
Responder->Initiator:          7 packets       1413 bytes
```

配置关键点

正常情况下，如果只配置了DNAT，需要添加VRF路由：

ip route-static vpn-instance v2 1.1.1.0 24 vpn-instance v1 1.1.1.1

配置了SNAT后，该路由可以取消。

注意事项：接口下NAT映射配置，以及SNAT对应的acl配置。

Debug信息：

```
*Oct  5 12:25:44:786 2022 H3C IPFW/7/IPFW_PACKET: -COntext=1;
Receiving, interface = GigabitEthernet1/0/0
version = 4, headlen = 20, tos = 192
pktlen = 60, pktid = 51, offset = 0, ttl = 255, protocol = 6
checksum = 46778, s = 1.1.1.1, d = 1.1.1.12
channelID = 0, vpn-InstanceIn = 1, vpn-InstanceOut = 1.
prompt: Receiving IP packet from interface GigabitEthernet1/0/0.
Payload: TCP
  source port = 3078, destination port = 22
  sequence num = 0x048f6653, acknowledgement num = 0x00000000, flags = 0x2
  window size = 64512, checksum = 0x1a70, header length = 40.


*Oct  5 12:25:44:787 2022 H3C NAT/7/COMMON: -COntext=1;
 PACKET: (GigabitEthernet1/0/0-in-config) Protocol: TCP
         1.1.1.1: 3078 -        1.1.1.12:   22(VPN:    1) ------>
         1.1.1.1: 3078 -        10.1.1.3:   22(VPN:    2)
*Oct  5 12:25:44:787 2022 H3C NAT/7/COMMON: -COntext=1;
 PACKET: (GigabitEthernet1/0/1-out-config) Protocol: TCP
         1.1.1.1: 3078 -        10.1.1.3:   22(VPN:    1) ------>
       10.1.1.12: 1029 -        10.1.1.3:   22(VPN:    2)
*Oct  5 12:25:44:787 2022 H3C IPFW/7/IPFW_PACKET: -COntext=1;
Sending, interface = GigabitEthernet1/0/1
version = 4, headlen = 20, tos = 192
pktlen = 60, pktid = 51, offset = 0, ttl = 254, protocol = 6
checksum = 42424, s = 10.1.1.12, d = 10.1.1.3
channelID = 0, vpn-InstanceIn = 2, vpn-InstanceOut = 2.
prompt: Sending IP packet received from interface GigabitEthernet1/0/0 at interface
GigabitEthernet1/0/1.
Payload: TCP
  source port = 1029, destination port = 22
  sequence num = 0x048f6653, acknowledgement num = 0x00000000, flags = 0x2
  window size = 64512, checksum = 0x106f, header length = 40.


*Oct  5 12:25:44:787 2022 H3C IPFW/7/IPFW_PACKET: -COntext=1;
Receiving, interface = GigabitEthernet1/0/1
version = 4, headlen = 20, tos = 192
pktlen = 60, pktid = 49, offset = 0, ttl = 255, protocol = 6
checksum = 42170, s = 10.1.1.3, d = 10.1.1.12
channelID = 0, vpn-InstanceIn = 2, vpn-InstanceOut = 2.
prompt: Receiving IP packet from interface GigabitEthernet1/0/1.
Payload: TCP
  source port = 22, destination port = 1029
  sequence num = 0x7fd759cc, acknowledgement num = 0x048f6654, flags = 0x12
 window size = 64512, checksum = 0x9270, header length = 40.


*Oct  5 12:25:44:787 2022 H3C NAT/7/COMMON: -COntext=1;
 PACKET: (GigabitEthernet1/0/1-in-session) Protocol: TCP
        10.1.1.3:   22 -       10.1.1.12: 1029(VPN:    2) ------>
        10.1.1.3:   22           1.1.1.1: 3078(VPN:    1)
```