BGP路由协议下静态NAT444跨VPN实例的路由引入

NAT444 孔德飞 2024-03-29 发表

组网及说明

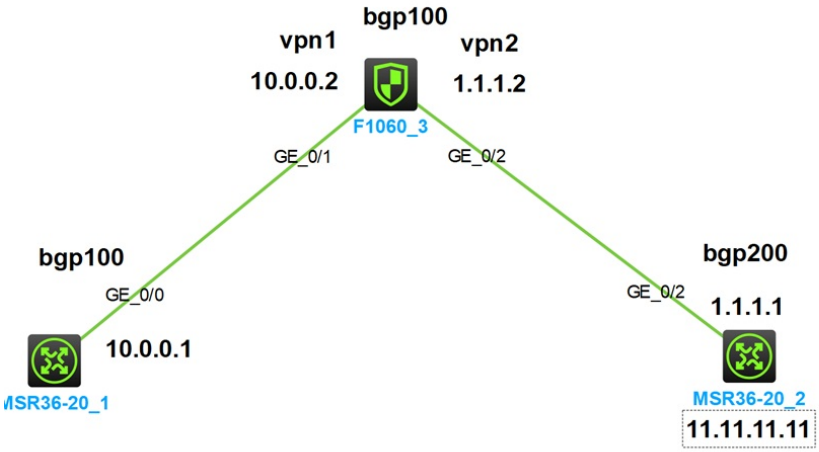
组网如下：

FW与MSR建立IBGP，FW与MSR2建立EBGP

G1/0/1属于VPN1，G1/0/2属于VPN2

FW上配置BGP实现跨VPN实例的路由引入

并且FW配置静态NAT444，实现MSR1的10.0.0.1可以访问MSR2的11.11.11.11



配置步骤

关键配置：

MSR1与MSR2配置忽略，主要讲FW的配置

接口加入安全域

```
security-zone name Trust
 import interface GigabitEthernet1/0/1
security-zone name Untrust
 import interface GigabitEthernet1/0/2
```

本案例主要讲解路由相互引入问题，安全策略全通

```
security-policy ip
 rule 0 name 0
  action pass
  vrf vpn1
 rule 1 name 1
  action pass
  vrf vpn2
```

配置VPN实例

```
ip vpn-instance vpn1
 route-distinguisher 10:11

ip vpn-instance vpn2
 route-distinguisher 20:11


interface GigabitEthernet1/0/1
 port link-mode route
```

```
 combo enable copper
 ip binding vpn-instance vpn1
 ip address 10.0.0.2 255.255.255.0
#
interface GigabitEthernet1/0/2
 port link-mode route
 combo enable copper
 ip binding vpn-instance vpn2
 ip address 1.1.1.2 255.255.255.0
```

配置静态NAT444

```
nat port-block-group 1
 local-ip-address 10.0.0.1 10.0.0.10 vpn-instance vpn1
 global-ip-pool 2.2.2.2 2.2.2.2
 block-size 500
 port-range 10001 15000
```

接口g1/0/2配置静态nat 444

```
interface GigabitEthernet1/0/2
  nat outbound port-block-group 1
```

手工写一条VPN1到VPN2的跨VPN实例的静态默认路由

```
ip route-static vpn-instance vpn1 0.0.0.0 0 vpn-instance vpn2 1.1.1.1
```

BGP对下行MSR1发布默认路由0.0.0.0.对上发布NAT黑洞路由2.2.2.2

```
[H3C]display  ip routing-table vpn-instance vpn2

Destinations : 12       Routes : 12

Destination/Mask   Proto   Pre Cost        NextHop         Interface
0.0.0.0/32         Direct  0   0           127.0.0.1       InLoop0
1.1.1.0/24         Direct  0   0           1.1.1.2         GE1/0/2
1.1.1.2/32         Direct  0   0           127.0.0.1       InLoop0
1.1.1.255/32       Direct  0   0           1.1.1.2         GE1/0/2
2.2.2.2/32         Direct  1   0           0.0.0.0         NULL0
11.11.11.11/32     BGP     255 0           1.1.1.1         GE1/0/2
127.0.0.0/8        Direct  0   0           127.0.0.1       InLoop0
127.0.0.1/32       Direct  0   0           127.0.0.1       InLoop0
127.255.255.255/32 Direct  0   0           127.0.0.1       InLoop0
224.0.0.0/4        Direct  0   0           0.0.0.0         NULL0
224.0.0.0/24       Direct  0   0           0.0.0.0         NULL0
255.255.255.255/32 Direct  0   0           127.0.0.1       InLoop0
bgp 100
 #
 ip vpn-instance vpn1
  router-id 11.11.11.11
  peer 10.0.0.1 as-number 100
  #
  address-family ipv4 unicast
   network 0.0.0.0 0.0.0.0（对下发布默认）
   peer 10.0.0.1 enable
 #
 ip vpn-instance vpn2
  router-id 33.33.33.33
  peer 1.1.1.1 as-number 200
  #
  address-family ipv4 unicast
   network 2.2.2.2 255.255.255.255（对上发布黑洞路由）
   peer 1.1.1.1 enable
```

配完成之后，在MSR1上可以看到默认路由

<H3C>display ip routing-table

Destinations : 11 Routes : 11

Destination/Mask Proto Pre Cost NextHop Interface
0.0.0.0/0 BGP 255 0 10.0.0.2 GE0/0
0.0.0.0/32 Direct 0 0 127.0.0.1 InLoop0
10.0.0.0/24 Direct 0 0 10.0.0.1 GE0/0
10.0.0.1/32 Direct 0 0 127.0.0.1 InLoop0
10.0.0.255/32 Direct 0 0 10.0.0.1 GE0/0
127.0.0.0/8 Direct 0 0 127.0.0.1 InLoop0
127.0.0.1/32 Direct 0 0 127.0.0.1 InLoop0
127.255.255.255/32 Direct 0 0 127.0.0.1 InLoop0
224.0.0.0/4 Direct 0 0 0.0.0.0 NULL0
224.0.0.0/24 Direct 0 0 0.0.0.0 NULL0
255.255.255.255/32 Direct 0 0 127.0.0.1 InLoop0

在MSR2上可以看到NAT地址池2.2.2.2的路由

<H3C>display ip routing-table

Destinations : 12 Routes : 12

Destination/Mask Proto Pre Cost NextHop Interface
0.0.0.0/32 Direct 0 0 127.0.0.1 InLoop0
1.1.1.0/24 Direct 0 0 1.1.1.1 GE0/2
1.1.1.1/32 Direct 0 0 127.0.0.1 InLoop0
1.1.1.255/32 Direct 0 0 1.1.1.1 GE0/2
2.2.2.2/32 BGP 255 0 1.1.1.2 GE0/2
11.11.11.11/32 Direct 0 0 127.0.0.1 InLoop0
127.0.0.0/8 Direct 0 0 127.0.0.1 InLoop0
127.0.0.1/32 Direct 0 0 127.0.0.1 InLoop0
127.255.255.255/32 Direct 0 0 127.0.0.1 InLoop0
224.0.0.0/4 Direct 0 0 0.0.0.0 NULL0
224.0.0.0/24 Direct 0 0 0.0.0.0 NULL0
255.255.255.255/32 Direct 0 0 127.0.0.1 InLoop0

并且MSR1可以ping通MSR2

<H3C>ping 11.11.11.11
Ping 11.11.11.11 (11.11.11.11): 56 data bytes, press CTRL+C to break
56 bytes from 11.11.11.11: icmp_seq=0 ttl=254 time=0.790 ms
56 bytes from 11.11.11.11: icmp_seq=1 ttl=254 time=0.563 ms
56 bytes from 11.11.11.11: icmp_seq=2 ttl=254 time=0.346 ms
56 bytes from 11.11.11.11: icmp_seq=3 ttl=254 time=0.604 ms
56 bytes from 11.11.11.11: icmp_seq=4 ttl=254 time=0.679 ms

FW的会话如下

[H3C]display nat session verbose
Slot 1:
Initiator:
  Source IP/port: 10.0.0.1/10984
  Destination IP/port: 1.1.1.1/2048
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: vpn1/-/-
  Protocol: ICMP(1)
  Inbound interface: GigabitEthernet1/0/1
  Source security zone: Trust
Responder:
  Source IP/port: 1.1.1.1/10009

  Destination IP/port: 2.2.2.2/0
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: vpn2/-/-
  Protocol: ICMP(1)
  Inbound interface: GigabitEthernet1/0/2
  Source security zone: Untrust
State: ICMP_REPLY
Application: ICMP
Rule ID: 0
Rule name: 0
Start time: 2024-03-29 15:13:16 TTL: 22s
Initiator->Responder: 5 packets 420 bytes
Responder->Initiator: 5 packets 420 bytes