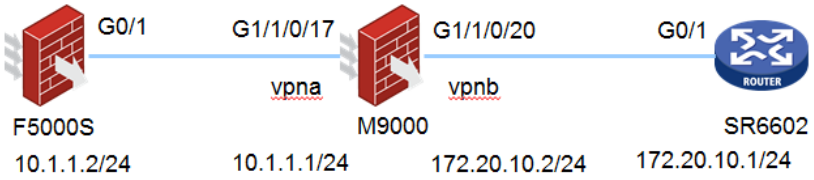
V7防火墙通过acl实现跨vpn的静态nat转换

VRF NAT 李超 2016-07-04 发表

客户采购V7防火墙，两个业务带有不同的vpn实例，客户想要实现只有访问特定地址时才进行nat地址转换。



以F5000S作为客户一个网络，SR6602为另外一个网络，现在想要实现访问172.20.10.1的时候做nat转换。
注：由于涉及到vpn，所以在实验室验证。

F5000S侧配置：

```
#
interface GigabitEthernet0/1
 port link-mode route
 ip address 10.1.1.2 255.255.255.0
#
zone name Trust id 2
 priority 85
 import interface GigabitEthernet0/1
#
ip route-static 172.20.10.0 255.255.255.0 10.1.1.1
#
```

SR6602侧配置：

```
#
interface GigabitEthernet0/1
 description M9000_1
 ip address 172.20.10.1 255.255.255.0
#
ip route-static 10.1.1.0 255.255.255.0 172.20.10.2
#
```

M9000侧配置：

```
  #
zone-pair security source Untrust destination Trust
 packet-filter 3100
#
zone-pair security source Trust destination Untrust
 packet-filter 3200
#
security-zone name Trust
 import interface GigabitEthernet1/1/0/17
#

   security-zone name Untrust
 import interface GigabitEthernet1/1/0/20

#
interface GigabitEthernet1/1/0/17
 port link-mode route
 combo enable copper
 ip binding vpn-instance vpna
 ip address 10.1.1.1 255.255.255.0
#
interface GigabitEthernet1/1/0/20
```

```
 port link-mode route
 combo enable copper
 ip binding vpn-instance vpnb
 ip address 172.20.10.2 255.255.255.0
 nat outbound 3020 vpn-instance vpnb
#
//配置vpna的静态路由，指向vpnb的一个地址172.20.10.1
ip route-static vpn-instance vpna 0.0.0.0 0 vpn-instance vpnb 172.20.10.1
//配置vpnb的静态路由，指向vpna的一个地址10.1.1.2
ip route-static vpn-instance vpnb 0.0.0.0 0 vpn-instance vpna 10.1.1.2
#
acl advanced 3100
 rule 10 permit ip vpn-instance vpnb
#
acl advanced 3200
 rule 20 permit ip vpn-instance vpna  //此处的vpn是针对源的
#
acl advanced 3020
 rule 0 permit ip vpn-instance vpna source 10.1.1.0 0.0.0.255 destination 172.20.10.3 0
#
ip vpn-instance vpna
 route-distinguisher 1:1
#
ip vpn-instance vpnb
 route-distinguisher 2:2
#
```

功能验证：

当M9000上面G1/1/0/20 的nat outbound的acl为

```
acl advanced 3020
 rule 0 permit ip vpn-instance vpna source 10.1.1.0 0.0.0.255 destination 172.20.10.1 0
```

定义目的地址的是ping的目的地址时，匹配该acl

```
Initiator:
  Source      IP/port: 10.1.1.2/40
  Destination IP/port: 172.20.10.1/2048
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: vpna/-/-
  Protocol: ICMP(1)
  Inbound interface: GigabitEthernet1/1/0/17
  Source security zone: F5000S
Responder:
  Source      IP/port: 172.20.10.1/2
  Destination IP/port: 172.20.10.2/0
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: vpnb/-/-
  Protocol: ICMP(1)
  Inbound interface: GigabitEthernet1/1/0/20
  Source security zone: SR6602
State: ICMP_REPLY
Application: OTHER
Start time: 2016-04-14 05:21:21  TTL: 25s
Initiator->Responder:          5 packets       420 bytes
Responder->Initiator:          5 packets       420 bytes
```