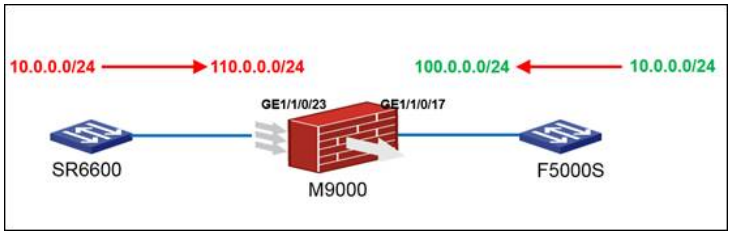
M9000跨VPN实例地址重叠双向NAT互访配置举例

金山 2016-01-06 发表

客户采购M9000设备，用于互联两个业务网络（以两台三层设备为例），由于前期规划原因，两个业务网络地址完全重叠，为实现在不修改业务网络IP地址的前提下，业务能够双向互防，需要在M9000设备上部署跨VPN实例的NAT策略。
本案例主要描述上述需求的关键配置项，其它配置功能简略。
本配置案例在M9000 CMW710-D9118P07版本中测试验证。



如图所示，M9000与两个业务网络互联，分别以SR6600和F5000S代表，两个业务网段的IP地址完全重叠，均为10.0.0.0/24。为实现不修改地址前提的双向互访，现拟SR6600侧客户端以目标IP地址110.0.0.0/24一对一访问F5000S侧服务器端，反之F5000S侧客户端以目标IP地址100.0.0.0/24一对一访问SR6600侧服务器端，NAT转换在M9000上完成。

1、M9000配置业务端口、管理相关等基础配置。若为两台M9000，则正常配置IRFII、MAD等基础配置。（略）
2、在系统视图下配置VPN实例，用于和两端业务网络互联。

```
#
ip vpn-instance F5K
 route-distinguisher 2:1
#
ip vpn-instance SR66
 route-distinguisher 1:1
#
```

3、在系统视图下配置静态NAT策略

```
#
nat static inbound net-to-net 10.0.0.0 10.0.0.255 vpn-instance F5K local 110.0.0.0 255.255.255.0 vpn-instance SR66
nat static outbound net-to-net 10.0.0.0 10.0.0.255 vpn-instance SR66 global 100.0.0.0 255.255.255.0 vpn-instance F5K
#
```

4、在系统视图下配置NAT策略相关路由

```
#
ip route-static vpn-instance SR66 10.0.0.0 24 172.20.10.1
ip route-static vpn-instance SR66 110.0.0.0 24 vpn-instance F5K 172.20.20.2
ip route-static vpn-instance F5K 10.0.0.0 24 172.20.20.2
#
```

5、配置接口所属安全区域及域间策略，本案例中简化为全通策略。

```
#
security-zone name F5K
 import interface GigabitEthernet1/1/0/17
#
security-zone name SR66
 import interface GigabitEthernet1/1/0/23
#
zone-pair security source F5K destination SR66
 packet-filter 3920
 packet-filter 3910
#
zone-pair security source SR66 destination F5K
 packet-filter 3910
 packet-filter 3920
#
acl advanced 3910
 rule 10 permit ip vpn-instance SR66
#
```

```
acl advanced 3920
 rule 20 permit ip vpn-instance F5K
#
```
6、配置互联接口
```
#
interface GigabitEthernet1/1/0/17
 port link-mode route
 combo enable copper
 ip binding vpn-instance F5K
 ip address 172.20.20.1 255.255.255.0
 nat static enable
#
interface GigabitEthernet1/1/0/23
 port link-mode route
 combo enable copper
 ip binding vpn-instance SR66
 ip address 172.20.10.2 255.255.255.0
#
```
7、功能验证

a、从SR6600侧客户端10.0.0.10以目标IP地址110.0.0.10访问F5000S侧的服务器端10.0.0.10。
```
<SR6602>ping -c 100 -a 10.0.0.10 110.0.0.10
  PING 110.0.0.10: 56  data bytes, press CTRL_C to break
    Reply from 110.0.0.10: bytes=56 Sequence=0 ttl=254 time=1 ms
    Reply from 110.0.0.10: bytes=56 Sequence=1 ttl=254 time=1 ms
    Reply from 110.0.0.10: bytes=56 Sequence=2 ttl=254 time=1 ms
    Reply from 110.0.0.10: bytes=56 Sequence=3 ttl=254 time=5 ms
    ……
  --- 110.0.0.10 ping statistics ---
    100 packet(s) transmitted
    100 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 1/1/34 ms
```
b、从F5000S侧客户端10.0.0.10以目标IP地址100.0.0.10访问F5000S侧的服务器端10.0.0.10。
```
<F5000-S>ping -c 100 -a 10.0.0.10 100.0.0.10
  PING 100.0.0.10: 56  data bytes, press CTRL_C to break
    Reply from 100.0.0.10: bytes=56 Sequence=0 ttl=254 time=1 ms
    Reply from 100.0.0.10: bytes=56 Sequence=1 ttl=254 time=1 ms
    Reply from 100.0.0.10: bytes=56 Sequence=2 ttl=254 time=1 ms
    Reply from 100.0.0.10: bytes=56 Sequence=3 ttl=254 time=1 ms
  ……
  --- 100.0.0.10 ping statistics ---
    100 packet(s) transmitted
    100 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 1/1/3 ms
```
c、在M9000设备上查看会话表项，可以观察到NAT策略的执行结果：
```
CPU 1 on slot 7 in chassis 1:
Initiator:
  Source      IP/port: 10.0.0.10/25
  Destination IP/port: 110.0.0.10/2048
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: SR66/-/-
  Protocol: ICMP(1)
  Inbound interface: GigabitEthernet1/1/0/23
  Source security zone: SR66
Responder:
  Source      IP/port: 10.0.0.10/25
  Destination IP/port: 100.0.0.10/0
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: F5K/-/-
  Protocol: ICMP(1)
  Inbound interface: GigabitEthernet1/1/0/17
  Source security zone: F5K
State: ICMP_REPLY
```

Application: OTHER
Start time: 2015-12-04 21:58:43 TTL: 27s
Initiator->Responder: 100 packets 8400 bytes
Responder->Initiator: 100 packets 8400 bytes

Initiator:
  Source IP/port: 10.0.0.10/12
  Destination IP/port: 100.0.0.10/2048
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: F5K/-/-
  Protocol: ICMP(1)
  Inbound interface: GigabitEthernet1/1/0/17
  Source security zone: F5K
Responder:
  Source IP/port: 10.0.0.10/12
  Destination IP/port: 110.0.0.10/0
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: SR66/-/-
  Protocol: ICMP(1)
  Inbound interface: GigabitEthernet1/1/0/23
  Source security zone: SR66
State: ICMP_REPLY
Application: OTHER
Start time: 2015-12-04 21:58:37 TTL: 20s
Initiator->Responder: 100 packets 8400 bytes
Responder->Initiator: 100 packets 8400 bytes

1、配置NAT Inbound策略后注意配置指向Local地址的路由表项。
2、路由表和域间策略配置时注意添加VPN实例。