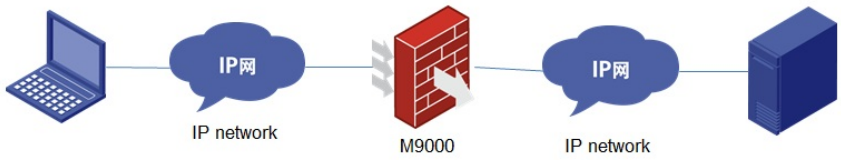
M9000 SSL VPN引流原理及典型配置

SSL VPN 孙兆强 2018-09-30 发表

组网及说明



M9000有多快FW插卡

配置步骤

M9000存在多块业务板卡时，会通过内部引流分到到不同板卡上，SSLVPN模块本身没有下发openflow流表的功能，需要借助其他模块（如nat）来实现。

引流方法一、借助nat模块实现自动引流

创建IPv4高级ACL3000，允许所有IP报文通过。

[Device] acl advanced 3000

[Device-acl-ipv4-adv-3000] rule permit ip

[Device-acl-ipv4-adv-3000] quit

创建地址池ippool，指定IP地址范围为10.1.1.1～10.1.1.10。

[Device] sslvpn ip address-pool ippool 10.1.1.1 10.1.1.10

创建SSL VPN AC接口1，配置该接口绑定VPN实例VPN1，并配置接口的IP地址为10.1.1.100/24。

[Device] interface sslvpn-ac 1

[Device-SSLVPN-AC1] ip address 10.1.1.100 24

[Device-SSLVPN-AC1] quit

创建NAT地址组，配置出方向NAT地址转换。

[Device] nat address-group 1

[Device-nat-address-group-1] address 2.2.2.10 2.2.2.20//这个地址随便用一个不用段就可以，但是内网设备要把这个段的路由指回m9k，一般内外都有默认路由指回来了

[Device-nat-address-group-1] quit

[Device] interface GigabitEthernet1/0/2//内网口

[Device-GigabitEthernet1/0/2] nat outbound 3000 address-group 1

[Device-GigabitEthernet1/0/2] quit

nat引流方式ssl vpn拨入后访问内网的其他网段是没有问题的。到本地的报文（比如ping M9006的接口地址）是没有这个nat的openflow引流的，所以进行hash，hash的结果就是ping M9000的接口地址，有的地址能通有的不通。这时候就要采用手动引流的方式。

引流方法二、手动引流

以下配置以到该接口地址172.16.254.1 的手工引流为例供参考：

sslvpn ip address-pool sslvpnpool 172.16.248.1 172.16.251.90

#

acl advanced 3999

description SSL_VPN_MQC

rule 0 permit ip source 172.16.248.0 0.0.1.255 destination 172.16.254.1 0

rule 5 permit ip source 172.16.250.0 0.0.0.255 destination 172.16.254.1 0

rule 10 permit ip source 172.16.251.0 0.0.0.63 destination 172.16.254.1 0

rule 15 permit ip source 172.16.251.64 0.0.0.15 destination 172.16.254.1 0

rule 20 permit ip source 172.16.251.80 0.0.0.7 destination 172.16.254.1 0

rule 25 permit ip source 172.16.251.88 0.0.0.1 destination 172.16.254.1 0

rule 30 permit ip source 172.16.251.90 0 destination 172.16.254.1 0

rule 35 permit ip source 172.16.254.1 0 destination 172.16.248.0 0.0.1.255

rule 40 permit ip source 172.16.254.1 0 destination 172.16.250.0 0.0.0.255

rule 45 permit ip source 172.16.254.1 0 destination 172.16.251.0 0.0.0.63

rule 50 permit ip source 172.16.254.1 0 destination 172.16.251.64 0.0.0.15

rule 55 permit ip source 172.16.254.1 0 destination 172.16.251.80 0.0.0.7

rule 60 permit ip source 172.16.254.1 0 destination 172.16.251.88 0.0.0.1

rule 65 permit ip source 172.16.254.1 0 destination 172.16.251.90 0

```
#
traffic classifier sslvpn operator and
if-match acl 3999
#
traffic behavior sslvpn
redirect interface Blade2/0/1
#
qos policy sslvpn
classifier sslvpn behavior sslvpn
#
qos apply policy sslvpn global inbound enhancement
```

为保证到其他接口地址能ping通，其他的接口地址也要做相似配置（或加到此acl里）。

配置关键点

1、地址池随便用一个不用段就可以，但是内网设备要把这个段的路由指回m9k，一般内外都有默认路由指回来了

2、可以采用手工引流方式，将sslvpn的流量和到防火墙本地的流量引到同一块防火墙板卡，但是操作和维护起来比较麻烦，在现网不影响功能使用的情况下，可以不用采取措施。