ipsec vpn和nat server之间的冲突

张旭A 2017-08-06 发表

跨公网的私网网段互访，通过IPsec VPN建立连接，实现私网间的访问，一般情况会在公网口进行ipsec的封装，而公网出口一般都会配置nat outbound，nat的优先级又要高于ipsec，如果nat的acl中没有拒绝vpn私网的用户互访，该数据到达公网口，进行nat的转换后直接就发送到公网设备，由于没有进行ipsec封装，导致ipsec vpn无法建立而不通。排除nat outbound的干扰，nat sever对于内网的ipsec互访的用户是否会有干扰呢？通过下面某个用户的案例来看下：
某局点客户反馈在公网口配置nat sever后导致映射的内网服务器无法通过ipsec vpn互访，删除nat sever后，通信正常，说明nat sever已经影响到ipsec vpn的建立了，为此模拟了客户的环境。
如图：202.1.1.0/24网段和202.1.3.0/24网段模拟公网环境，1.1.1.1和3.3.3.3模拟通过vpn互访的私网用户。为了排除nat outbound的干扰，公网口均不配置nat outbound。
组网：

首先先配置ipsec保证私网能够互访。
在msr36-20_1上测试

```
[MSR36-20_1]ping -a 1.1.1.1 3.3.3.3
Ping 3.3.3.3 (3.3.3.3) from 1.1.1.1: 56 data bytes, press CTRL_C to break
Request time out
56 bytes from 3.3.3.3: icmp_seq=1 ttl=255 time=2.000 ms
56 bytes from 3.3.3.3: icmp_seq=2 ttl=255 time=2.000 ms
56 bytes from 3.3.3.3: icmp_seq=3 ttl=255 time=1.000 ms
56 bytes from 3.3.3.3: icmp_seq=4 ttl=255 time=0.000 ms
```

```
[MSR36-20_1]dis ike sa
    Connection-ID   Remote                Flag         DOI
-------------------------------------------------------------------------
    1               202.1.3.3             RD           IPsec
Flags:
RD--READY RL--REPLACED FD-FADING RK-REKEY
```

```
[MSR36-20_1]dis ipsec sa
-------------------------------
Interface: GigabitEthernet0/0
-------------------------------

  -----------------------------
  IPsec policy: map1
  Sequence number: 10
  Mode: ISAKMP
  -----------------------------
    Tunnel id: 0
    Encapsulation mode: tunnel
    Perfect Forward Secrecy:
    Inside VPN:
    Extended Sequence Numbers enable: N
    Traffic Flow Confidentiality enable: N
    Path MTU: 1428
    Tunnel:
        local  address: 202.1.1.1
        remote address: 202.1.3.3
    Flow:
        sour addr: 1.1.1.1/255.255.255.255  port: 0  protocol: ip
        dest addr: 3.3.3.3/255.255.255.255  port: 0  protocol: ip
```

清除ipsec sa 和ike sa 在接口配置nat sever看是否影响ipsec建立后，在接口配置natsever后观察1.1.1.1和3.3.3.3访问是否收到影响。

```
#
interface GigabitEthernet0/0
 port link-mode route
 combo enable copper
 ip address 202.1.1.1 255.255.255.0
 nat server global current-interface inside 1.1.1.1
 ipsec apply policy map1
#
```

测试发现：私网仍然能够互访，ipsec sa和ike sa 也正常建立

```
<MSR36-20_1>ping -a 1.1.1.1 3.3.3.3
Ping 3.3.3.3 (3.3.3.3) from 1.1.1.1: 56 data bytes, press CTRL_C to break
Request time out
56 bytes from 3.3.3.3: icmp_seq=1 ttl=255 time=2.000 ms
56 bytes from 3.3.3.3: icmp_seq=2 ttl=255 time=2.000 ms
56 bytes from 3.3.3.3: icmp_seq=3 ttl=255 time=2.000 ms
56 bytes from 3.3.3.3: icmp_seq=4 ttl=255 time=2.000 ms
```

```
[MSR36-20_1]dis ike sa
    Connection-ID   Remote                Flag         DOI
-------------------------------------------------------------------------
    1               202.1.3.3             RD           IPsec
Flags:
RD--READY RL--REPLACED FD-FADING RK-REKEY
```

```
[MSR36-20_1]dis ipsec sa
-------------------------------
Interface: GigabitEthernet0/0
-------------------------------

  -----------------------------
  IPsec policy: map1
  Sequence number: 10
  Mode: ISAKMP
  -----------------------------
    Tunnel id: 0
    Encapsulation mode: tunnel
    Perfect Forward Secrecy:
    Inside VPN:
    Extended Sequence Numbers enable: N
    Traffic Flow Confidentiality enable: N
    Path MTU: 1428
    Tunnel:
        local  address: 202.1.1.1
        remote address: 202.1.3.3
    Flow:
        sour addr: 1.1.1.1/255.255.255.255  port: 0  protocol: ip
        dest addr: 3.3.3.3/255.255.255.255  port: 0  protocol: ip
```

通过排查客户配置发现客户nat sever的配置最后添加了命令reversible，于是修改测试环境配置

```
#
interface GigabitEthernet0/0
 port link-mode route
 combo enable copper
 ip address 202.1.1.1 255.255.255.0
 nat server global current-interface inside 1.1.1.1 reversible
 ipsec apply policy map1
#
return
```

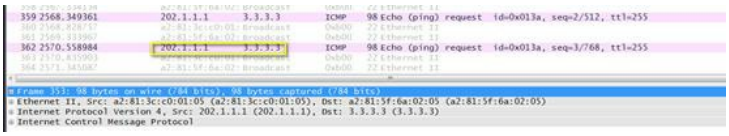
测试发现：私网无法互访，ipsec和ike sa无法正常建立。

```
<MSR36-20_1>ping -a 1.1.1.1 3.3.3.3
Ping 3.3.3.3 (3.3.3.3) from 1.1.1.1: 56 data bytes, press CTRL_C to break
Request time out
Request time out
Request time out
Request time out
Request time out
```

```
% Unrecognized command found at     position.
<MSR36-20_1>dis ike sa
    Connection-ID   Remote                Flag         DOI
-------------------------------------------------------------------------
<MSR36-20_1>
```

```
<MSR36-20_1>dis ipsec sa
<MSR36-20_1>
```

说明没有触发ipsec进行封装，通过msr36-20_1公网口抓包查看到，ping包的源地址经过nat转换封装为公网口202.1.1.1。



再来看reversible的含义 //经测试当前版本并不是对已经建立了地址转换的表项进行地址转换，而是针对于映射的内网服务器发起公网访问时都进行源地址转换。

Reversible	是否允许反向地址转换。若其值为“Y”，则表示在某方向上发起的连接已成功建立地址转换表项的情况下，允许反方向发起的连接使用已建立的地址转换表项进行地址转换；否则，不允许

由此可以看见，配置此命令后反向表项的连接生效，导致数据匹配nat转发，ipsec无法建立。

需要配置ipsec和nat sever的内网用户接口上配置nat sever后面不能添加reversible：reversiblenat server global current-interface inside 1.1.1.1 reversible