nat server命令配置reversible参数可能会导致ipsec隧道流量不通（单通）的说明

IPSec VPN 徐猛 2021-12-30 发表

问题描述

两个局点之间建立ipsec隧道进行通信的时候。正常需要对保护的感兴趣流量在nat outbound中进行deny处理，如下这样配置正常能够保护192.168.2.0/23 去往192.168.0.0/16的流量走ipsec隧道。但是如果本端的源地址作为映射后的地址使用，且映射时添加了**reversible参数，将会导致映射的私网地址无法匹配ipsec隧道进行转发。**

```
#
interface GigabitEthernet1/0/15
port link-mode route
ip address *.246.43.18 255.255.255.248
ip last-hop hold
nat outbound 3000
nat server protocol tcp global *.246.43.19 80 inside 192.168.2.182 80 reversible
ipsec apply policy 1
#
acl advanced 3000
 description nat
 rule 0 deny ip source 192.168.2.0 0.0.1.255 destination 192.168.0.0 0.0.255.255
 rule 4 permit ip
#
```

解决方法

添加了reverse参数后，nat outbound中添加的acl 3000参数对**192.168.2.182就不生效了。因为添加reversible参数后，内部服务器主动访问外网时，将私网地址转换为内部服务器向外提供服务的外网IP地址。如果需要该地址的流量能走ipsec隧道，需要关闭reversible参数。**

#
interface GigabitEthernet1/0/15
port link-mode route
ip address *.246.43.18 255.255.255.248
ip last-hop hold
nat outbound 3000
nat server protocol tcp global *.246.43.19 80 inside 192.168.2.182 80 reversible
ipsec apply policy 1
#

reversible：表示支持私网侧内部服务器主动访问外网。内部服务器主动访问外网时，将私网地址转换为内部服务器向外提供服务的外网IP地址。