# 接口NAT outbound与IPsec出方向报文冲突处理办法

NAT IPSec VPN **曾招维** 2022-05-10 发表

## 问题描述

在一个接口上同时配置了IPsec与NAT的情况下，对于出方向报文，设备先进行NAT转换，再进行IPsec处理。若接口上需要进行NAT转换的流量与需要进行IPsec处理的流量未能通过配置准确的区分，将会导致接口上的报文不能按照预期进行IPsec处理。

错误配置导致IPSEC异常：

```
#
interface GigabitEthernet0/1
 port link-mode route
 combo enable copper
 ip address 1.1.1.1 255.255.255.0
 nat outbound///所有出设备流量进行nat转换
 ipsec apply policy policy1
#
```

可通过定义ACL只对非IPsec感兴趣流进行NAT地址转换：

```
#
interface GigabitEthernet0/1
 port link-mode route
 combo enable copper
 ip address 1.1.1.1 255.255.255.0
 nat outbound 3010
 ipsec apply policy policy1
#
#
acl advanced 3010
 rule 0 deny ip source 192.168.1.0 0.0.0.255 destination 192.168.2.0 0.0.0.255///假设NAT侧私网感兴趣流为这个
 rule 5 permit ip
#
```

但IPsec感兴趣流较多或者不好定义NAT流量特征时，直接通过开启ipsec no-nat-process功能后，当前接口上需要进行IPsec处理的流量将不会进行NAT转换，减轻划分NAT与IPsec流量的工作量，进而降低接口上IPsec与NAT共存时配置的复杂度。

```
#
interface GigabitEthernet0/1
 port link-mode route
 combo enable copper
 ip address 1.1.1.1 255.255.255.0
 nat outbound
 ipsec apply policy policy1
 ipsec no-nat-process enable
#
```

## 解决方法

两种方法均可，但ipsec no-nat-process功能配置更为简单。