某局点MS4320V2 ipsec访问不通

IPSec VPN　张猛　2021-12-22 发表

组网及说明

设备：MS4320V2
版本：R6319
组网：不涉及

问题描述

MS4320V2设备和对端友商设备建立ipsec隧道，隧道建立后设备下联终端访问对端设备不通。且本端display ike sa显示的flow源地址与配置地址段不同。本端地址10.250.0.1ping对端设备是通的，但是同网段下的终端10.250.0.10ping对端地址不通。

过程分析

```
[H3C]dis ike sa
   Connection-ID   Remote              Flag        DOI
-----------------------------------------------------------------------
   73              10.205.232.92       RD          IPse
   Tunnel:
      local  address: 192.168.1.254
      remote address: 10.205.232.92
   Flow:
      sour addr: 10.0.0.0/255.255.255.128  port: 0  protocol: ip
      dest addr: 10.240.9.128/255.255.255.128  port: 0  protocol: ip
```

显示的Flow流源IP为10.0.0.0/25网段

但是设备上配置的流保护源网段为10.0.0.0/8网段：

```
acl advanced 3001
rule 15 permit ip source 10.0.0.0 0.255.255.255 destination 10.240.9.128 0.0.0.127
ipsec policy mapycs 10 isakmp
transform-set ycs
 security acl 3001
```

1.观察发现display中源ip的掩码变成了配置的目的网段的掩码，后确认为已知显示问题，设备上显示的源ip掩码位数会自动和目的ip的掩码同步，导致显示错误，实际不影响ipsec业务，因此本端的10.250.0.1属于10.0.0.0/8网段，可以正常访问对端设备。

2.设备下联同网段终端ping不通对端设备的原因在于，ipsec的封装是需要cpu来进行，而下联设备的ping报文在交换机上直接硬件转发，并不会上送cpu，因此无法进行ipsec封装，也自然无法和对端通信。目前设备只支持对上送cpu的各类协议报文进行ipsec封装。

解决方法

1.显示的已知问题已经合入新版本，即将发布。

2.对业务报文进行ipsec封装，目前只能通过qos将业务流量trap to cpu来实现，但是报文转发会变慢，且报文过多的话会加大cpu的负载，少量业务可用此方法暂时规避。