F5030 IPSEC起来，访问ipsec业务不通

IPSec VPN　zhiliao_l9hSOv　2023-05-28 发表

组网及说明

F5030----10.1.1.1----20.2.2.2---- F1000-AI-60 起ipsec。

问题描述

测试连通性公网地址可达，通过display ike sa 、display ipsec sa 查看 ipsec已起来，查看配置无问题，访问2侧本端业务都正常，但是访问对端web业务（走ipsec）时一直转圈圈

过程分析

通过display ipsec statistics 查看报文被MTU 丢弃。

```
 display ipsec statistics
    Received/sent packet rate: 5/5 packets/sec
    Received/sent byte rate: 290/290 bytes/sec
    Dropped packets (received/sent): 0/45
    Dropped packets statistics
      No available SA: 0
      Wrong SA: 0
      ACL check failure: 0
      MTU check failure: 45
```

后续通过display ipsec sa 查看 路径MTU 1424

```
 display ipsec sa
-------------------------------
Interface: GigabitEthernet1/0/1
    Tunnel id: 3
    Encapsulation mode: tunnel
    Perfect Forward Secrecy:
    Inside VPN: vp1
    Extended Sequence Numbers enable: Y
    Traffic Flow Confidentiality enable: N
    Transmitting entity: Initiator
    Path MTU: 1424
```

解决方法

由于display ipsec sa 查看的 通道MTU值无法修改（path mtu），此时修改内网接口（感兴趣流上来的接口）tcp mss 值，修改的幅度：每次减30的进行调整。 后续修改内网接口tcp mss 后业务访问正常