S5820V2-52QF交换机ipsec问题说明

IPSec VPN　夏威　2019-11-24 发表

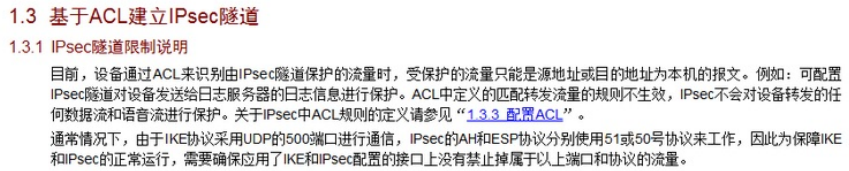
问题描述

S5820V2-52QF交换机ipsec说明

解决方法

交换机上IPsec不能封装转发流量，原因是交换机会通过硬件直接转发，报文不上CPU。IPsec业务必须在CPU处理。

1. 因为交换机上IPsec不能封装转发流量，因此不会有转发性能的数据。目前交换机上IPsec主要用户保护log等本机报文。
2. 用GRE over IPsec应该是不行的。因为交换机上GRE也是走硬件，不上CPU是没有机会走IPsec的。



1.3 基于ACL建立IPsec隧道

1.3.1 IPsec隧道限制说明

目前，设备通过ACL来识别由IPsec隧道保护的流量时，受保护的流量只能是源地址或目的地址为本机的报文。例如：可配置IPsec隧道对设备发送给日志服务器的日志信息进行保护。ACL中定义的匹配转发流量的规则不生效，IPsec不会对设备转发的任何数据流和语音流进行保护。关于IPsec中ACL规则的定义请参见“1.3.3 配置ACL”。

通常情况下，由于IKE协议采用UDP的500端口进行通信，IPsec的AH和ESP协议分别使用51或50号协议来工作，因此为保障IKE和IPsec的正常运行，需要确保应用了IKE和IPsec配置的接口上没有禁止掉属于以上端口和协议的流量。