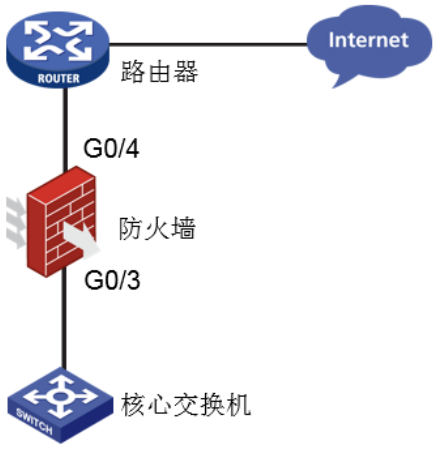
某局点SecPath F1080 虚墙的安全策略看不到匹配次数故障排查经验案例

Context 王周华 2020-08-31 发表

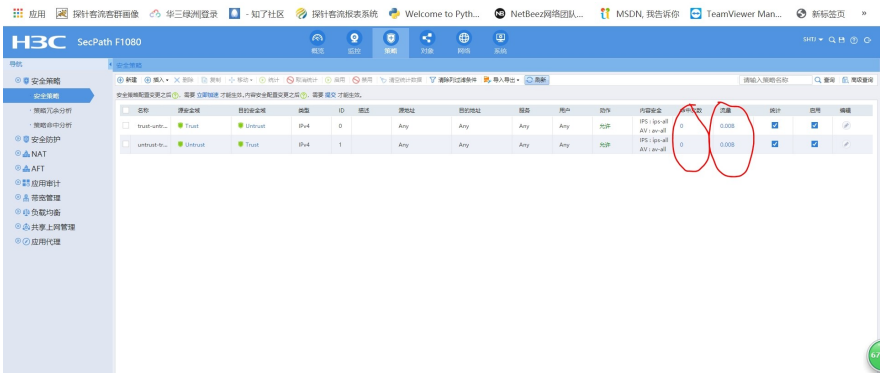
组网及说明

现场将防火墙二层部署在网络中，并且在防火墙上创建了虚墙，想要通过虚墙放通业务流量。组网大致拓扑图如下：



问题描述

现场反馈现在业务流量已经正常运行了，但是在虚墙的安全策略中看不到命中次数和流量。



过程分析

1、定位下流量是否上送到了虚墙上，可以在虚墙上查看是否有对应流量的会话或者开启debugging security-policy all查看是否有命中安全策略的日志输出，现场在虚墙上开启debugging security-policy all发现没有G1/0/3口和G1/0/4口对应的debug输出，那么流量应该没有上送到虚拟防火墙上。

2、和现场确认根墙上有匹配相同接口的安全策略，且该安全策略有流量以及命中次数。将根墙上的安全策略禁用后，启用虚拟防火墙的安全策略发现流量不通了，说明流量命中的是根墙的安全策略。

3、检查根墙上虚墙的配置，G1/0/3口和G1/0/4口是二层口，通过共享接口的方式将接口共享到虚拟防火墙上，但是没有将vlan共享到虚墙上，要将流量引入到虚墙上，需要将vlan也分配给虚墙。

解决方法

在根墙上创建vlan并且通过**allocate vlan**将vlan分配给虚墙，虚墙看不到vlan，也不能创建vlan。共享vlan的时候需要注意：

1、VLAN 1不能被共享。

2、端口的缺省VLAN不能被共享。

3、已经创建了VLAN接口的VLAN不能被共享。