Secpath T200E新特性导致网络间隙性中断案例

姜洪杰 2008-03-14 发表

Secpath T200E新特性导致网络间隙性中断案例

某用户测试SECPATH IPS T200E,导致用户网络间隙性丢包，服务器无法访问。

1、组网图：

部署方式：在CISCO6500上做端口SPAN，将从广域网上进入流量镜像到我司secpath T200E连接的端口上。Secpath T200E做旁路模式部署（相当于IDS使用）。

为了保证测试效果，在secpath T200E上把过滤器动作设置为了block + notify，但是我司设备部署上去后客户网络发生了振荡，cisco 7500 ping cisco 6500严重丢包，但是一旦把我司sepath T200E拔出，客户网络就恢复正常，客户认为我司设备有极大问题。

为定位这个问题，在我司设备与cisco6500间连接hub抓包，抓包显示网络中有大量的tcp reset 报文，但是把我司ips T200E网线拔离后再抓包显示tcp reset 报文没有了。

再查看T200E的接口信息显示：

T200E是在发送报文，难道是这个报文导致了客户网络不正常?

经过研发分析：

我司T系列IPS即使做IDS使用时也具有通过发送TCP Reset报文实现攻击阻断的特性。

我司T系列IPS的这个个攻击阻断的特性，正是这个特性导致以上的问题产生。

我司IPS在block + notify的情况下默认对block的流会发送tcp reset报文，重置tcp连接，这样即使在旁路模式（IDS）下也可以阻断部分攻击，但是在这次测试中由于管理口没有连接客户网络导致IPS使用业务口（连接镜像的口）发送了tcp reset报文，并且报文中的mac地址就是原来接受到的报文的mac地址。

如下图所示：

原本客户网络中从端口2接收到了攻击报文，并从端口1出去，这个报文并镜像到了T200E上后，T200E就发送一个tcp reset 报文，由于管理口没有连接到网络，T200E就使用业务口发送，并使用了原来的mac地址，镜像口一旦具有mac地址学习功能的话，导致交换设备mac地址漂移，网络间隙中断。

咨询了研发朱毅泉，如果使用管理口的话，发送tcp reset报文就使用T200E管理口的mac 了，这样也就没有问题。

解决方案一：把T200E的管理口接入用户网络，使用管理口发送TCP reset 报文。

解决方案二：当旁路部署时尽量使用permit + notify的方式，这样使用效果就和IDS完全一样了。

解决方案三：可以修改block的动作，设置不发送tcp reset 报文。

当然建议今后使用旁路模式部署的话，尽量使用permit + notify，或者修改block的动作，设置不发送tcp reset 报文，防止由于意外原因客户把管理口网线断了，导致类似问题发生。