Layer4流量监控如何阻塞流量？

问题：

如果只接收被反映的流量， Layer4流量监控如何阻塞流量？

环境：

Layer4流量监控-配置的L4TM阻塞可疑流量

解决方案：

思科Web安全工具(WSA)有能阻塞在所有网络端口的一内置的Layer4流量监控(L4TM)服务(TCP/UDP 0-65535)间的可疑会话。

通过使用TAPS (测验接入端口)设备，必须重定向要能监控或阻塞这些会话流量到WSA，或者通过配置网络设备的(Cisco设备的SPAN端口一个镜像端口)。不支持L4TM轴向模式。

即使流量从设备的原始会话只被反映(复制)， WSA能通过休息TCP会话或发送ICMP “UDP会话的主机不可及”消息仍然阻塞可疑流量。

对于TCP会话

当WSA L4TM收到数据包到/从服务器，并且流量匹配块操作， L4TM将发送TCP RST (重置)数据包到客户端或服务器根据方案。TCP RST数据包是有TCP RST标志设置的一正常数据包到1。

RST的接收方首先验证它，然后更改状态。如果接收方是在监听状态，忽略它。如果接收方在SYN-RECEIVED状态和以前是在监听状态，则接收方回到监听状态，否则接收方中止连接并且去闭合状态。如果接收方在其他状态，它中止连接并且建议用户并且去闭合状态。

有要考虑的两个案件(在两种情况下用户/客户端是在防火墙后) ：

第一个是，当可疑数据包从往一个客户端的防火墙外面来内部网络的时。RST将发送到服务器，并且在这种情况下将达到通常不会转发RST的防火墙，但是将终止会话，因为相信RST实际上来自客户端。在这种情况下RST的来源IP将是客户端的伪装的IP。客户端将终止会话。

第二个案件是，当数据包自内部网络的客户端来和去外部服务器时(防火墙的外部)。RST然后发送给客户端，并且RST来源IP将是服务器的伪装的IP。

对于UDP会话

一种相似的行为由WSA进行，当可疑流量是从UDP会话时，但是而不是发送TCP RST， L4TM将传送ICMP主机不可及信息(ICMP对客户端或服务器的type3代码1)。然而，在这些情况下没有IP伪装作为ICMP信息阐明，主机是不可得到的，因此不能发送数据包。来源IP在这种情况下将是WSA的IP。

使用数据路由表，这些RSTs和ICMP数据包从WSA被发送，通过M1， P1或者P2，根据部署。