第4层流量监控器如何阻止流量？

问题：

如果第4层流量监控器仅接收镜像流量，它如何阻止流量？

环境：

第4层流量监控器 — 配置为阻止可疑流量的L4TM

解决方案：

思科网络安全设备(WSA)具有内置的第4层流量监控器(L4TM)服务，可阻止所有网络端口(TCP/UDP 0-65535)上的可疑会话。

要能够监控或阻止这些会话流量，必须通过使用TAP（测试接入端口）设备或在网络设备上配置镜像端口（思科设备上的SPAN端口）将流量重定向到WSA。L4TM串接模式尚不支持。

即使流量仅从原始会话镜像（复制）到设备，WSA仍可以通过暂停TCP会话或发送UDP会话的ICMP“主机不可达”消息来阻止可疑流量。

对于TCP会话

当WSA L4TM接收到发往或来自服务器的数据包，且流量与阻止操作匹配时，L4TM将根据场景向客户端或服务器发送TCP RST（重置）数据报。TCP RST数据报只是TCP RST标志设置为1的常规数据包。

RST的接收方首先验证它，然后更改状态。如果接收方处于LISTEN状态，则它会忽略它。如果接收方处于SYN-RECEIVED状态，并且之前处于LISTEN状态，则接收方返回LISTEN状态，否则接收方将中止连接并进入CLOSED状态。如果接收方处于任何其他状态，它将中止连接并建议用户进入CLOSED状态。

需要考虑两种情况（两种情况下用户/客户端都位于防火墙后面）：

第一种情况是可疑数据包从防火墙外部传输到内部网络中的客户端。RST将发送到服务器，在这种情况下，它将到达通常不会转发RST的防火墙，但会终止会话，因为它认为RST实际上来自客户端。在这种情况下，RST的源IP将是客户端的欺骗IP。客户端将终止会话。

第二种情况是数据包来自内部网络中的客户端，并且要发往外部服务器（防火墙外）。 然后，RST将发送到客户端，而RST源IP将是服务器的欺骗IP。

对于UDP会话

当可疑流量来自UDP会话时，WSA会执行类似行为，但L4TM不会发送TCP RST(TCP RST)，而是会向客户端或服务器发送ICMP主机不可达消息（ICMP第3类代码1）。但是，在这些情况下，不会出现IP欺骗，因为ICMP消息表明主机无法访问，因此无法发送数据包。在本例中，源IP将是WSA的IP。

这些RST和ICMP数据包是使用数据路由表从WSA通过M1、P1或P2发送的，具体取决于部署。