某局点fw 板卡tracert 下一跳显示*号问题处理经验案例

Tracert 刘文峰 2016-09-14 发表

某局点S12510-F上插了一块fw 板卡，通过内联口互ping 都能ping 通，从12510-f 上tracert 到fw 板卡显示正常下一跳，但是从fw 板卡tracert S12510-f 结果显示*号，tracert 交换机上的其他服务器，也都显示*号，通过在交换机上镜像抓包查看，交换机收到tracert 报文，ttl 也正常，同时也回应了icmp 不可达报文，感觉问题就出在fw 上。

交换机tracert fw 结果：

tracert 111.1.28.34

traceroute to 111.1.28.34(111.1.28.34) 30 hops max,40 bytes packet, press CTRL_C to break

1 111.1.28.34 1 ms 1 ms 1 ms

fw 板卡tracert 交换机结果：

tracert 111.1.28.38

traceroute to 111.1.28.38(111.1.28.38) 30 hops max,40 bytes packet, press CTRL_C to break

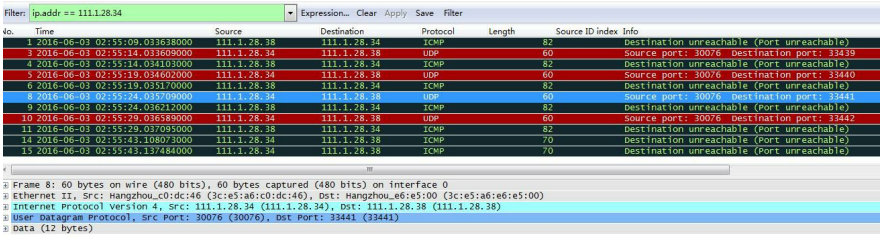
1 * * *

2 * * *

3 * * *

4 * *

交换机上镜像抓包结果：能看到交换回应了icmp 不可达报文



通过远程登入设备测试，发现从fw tracert 出去，icmp 不可达报文被识别为攻击，

traceroute to 111.1.31.220(111.1.31.220) 30 hops max,40 bytes packet, press CTRL_C to break

%Jun 3 13:32:34:868 2016 ZJJXI-MS-IDCQT-FW01-A19 ATTACK/6/ATK_ATTACK_REPORT: atck Type(1016)=(9)ICMP Unreachable;rcvIfName(1023)=Ten-GigabitEthernet0/0.1001;srcIPAddr(1017)=111.1.31.220;srcMacAddr(1021)= ;destIPAddr(1019)=111.1.31.130;destMacAddr(1022)= ;atckSpeed(1047)=0;atckTime_cn(1048)=20160603133234

登入web界面查看配置，发现在报文异常检测里面勾选了“icmp 不可达报文攻击检测”，在开启了“icmp 不可达攻击”设备会检测进入到防火墙的报文类型是否为icmp 不可达报文，如果是，则根据用户配置选择对报文进行丢弃或者转发，同时记录日志。

取消勾选“icmp 不可达报文攻击检测”后，问题解决，从fw tracert 交换机或者其他设备恢复正常。

目前防火墙支持以下基于特征识别的防攻击，可以在所有安全区域开启攻击防范，但建议不启用“ICMP 不可达报文攻击检测”，否则会引起大量的主机操作系统正常发送的ICMP协议报文被阻断。另外，在需要通过防火墙执行Tracert操作时，不启用“Tracert报文攻击检测”。