ASA对Traceroute报文的处理问题

目录

技术领域

ASA 5500 Series, ICMP, Traceroute

问题描述

ASA丢弃某些LINUX主机的traceroute报文。

ASA对于Traceroute报文的处理机制

Traceroute报文工作机制分为两种：基于UDP端口以及基于ICMP。
基于UDP端口的traceroute需要在ACL中打开相应UDP端口。
基于ICMP的traceroute稍显复杂。ASA默认情况下将ICMP报文看做无状态的连接，因此如果需要通过ICMP报文，例如在traceroute中，其反方向的回包为ICMP的time-exceeded包，因此需在接口用ACL允许该报文，否则traceroute将失败。另一种方法是配置ICMP Inspection. 一旦配置了ICMP Inspection,ASA会将ICMP会话看做有状态的连接，从而允许返回流量。而由于traceroute报文利用了ICMP的time-exceeded错误作为其工作机制，因此需要同时打开ICMP ERROR的Inspection.

故障排除步骤

1. 检查主机使用的是基于UDP端口的traceroute还是基于ICMP time-exceeded的traceroute。
2. 如果是基于UDP端口的traceroute，需要在ACL中打开相应端口，从UDP的33434开始，每次加1。一般LINUX主机用的是基于UDP的traceroute，而微软的操作系统大多用基于ICMP的traceroute。如果要修改LINUX主机的traceroute成为基于ICMP的，可在trace时加上-I 关键字：

```
traceroute -I 192.168.1.1
```

3. 如果是基于ICMP的traceroute，则推荐打开icmp以及icmp error的inspection：

```
ciscoasa(config)#policy-map    global_policy
ciscoasa(config-pmap)#class    inspection_default
ciscoasa(config-pmap-c)#inspect icmp
ciscoasa(config-pmap-c)#inspect icmp error
ciscoasa(config-pmap-c)#end
```

总结

1. 首先需要弄清主机使用何种机制traceroute，是基于ICMP的还是UDP端口的。
2. 在ACL中允许相应的流量通过，必要时将ICMP连接看做有状态的连接。
3. 查看log，并进行抓包分析。

相关文档

1. ASA/PIX/FWSM: Handling ICMP Pings and Traceroute
   http://www.cisco.com/en/US/products/hw/vpndevc/ps2030/products_tech_note09186a0080094e8a.shtml#trace
2. RFC 792 INTERNET CONTROL MESSAGE PROTOCOL
   http://tools.ietf.org/html/rfc792