某局点通过Radius 登录S5800设备认证失败故障处理案例

Radius Telnet/SSH 赵国卫 2013-10-30 发表

某局点通过Radius 登录S5800设备认证失败故障处理案例

一、 组网：

无。

二、 问题描述：

客户采用telnet的方式对网络内的S5800设备进行管理，登录设备时需要到远端Radius服务器进行Radius认证，之前telnet正常，某天突然无法telnet登录其中一台S5800设备，而同样配置的另外一台S5800则可以正常登录。

三、 过程分析：

针对客户反馈问题，首先查看设备配置，确认设备配置不存在问题。

在设备上开启debug radius packet ，然后进行认证，发现有下面的debug输出：

*Sep 27 10:09:52:537 2011 DMZ-5800A RDS/7/DEBUG: Recv MSG,[MsgType=Auth request Index = 43, ulParam3=471469200]

*Sep 27 10:09:55:534 2011 DMZ-5800A RDS/7/DEBUG: Recv MSG,[MsgType=PKT auth timeout Index = 43, ulParam3=0]

*Sep 27 10:09:58:537 2011 DMZ-5800A RDS/7/DEBUG: Recv MSG,[MsgType=PKT auth timeout Index = 43, ulParam3=0]

*Sep 27 10:10:01:533 2011 DMZ-5800A RDS/7/DEBUG: Recv MSG,[MsgType=PKT auth timeout Index = 43, ulParam3=0]

*Sep 27 10:09:52:541 2011 DMZ-5800A RDS/7/DEBUG: Send: IP=[10.27.255.1], UserIndex=[43], ID=[0], RetryTimes=[0], Code=[1], Length=[208]

*Sep 27 10:09:55:534 2011 DMZ-5800A RDS/7/DEBUG: Send: IP=[10.27.255.1], UserIndex=[43], ID=[0], RetryTimes=[1], Code=[1], Length=[208]

*Sep 27 10:09:58:537 2011 DMZ-5800A RDS/7/DEBUG: Send: IP=[10.27.255.1], UserIndex=[43], ID=[0], RetryTimes=[2], Code=[1], Length=[208]

*Sep 27 10:10:01:535 2011 DMZ-5800A RDS/7/DEBUG:

Error: Auth server no response.(AAAID = 43, Req-ID = 0)

*Sep 27 10:10:01:535 2011 DMZ-5800A RDS/7/DEBUG: RADIUS Server No Response

*Sep 27 10:10:01:541 2011 DMZ-5800A SC/7/Error: Local user: yuchen666 does not exist.

从debug信息来看，认证失败的原因是认证超时，而且没有配置本地用户导致远程认证失败的时候转本地认证也失败，最终导致了用户无法telnet设备。从“RADIUS Server No Response ”信息来判断，有两种情况会导致此现象：

1．Radius Server没有响应设备的Radius Request报文；

2．Radius Server响应了设备Radius Response但是设备没有正常处理。

从现场现象来看，因为网络内其他同样配置的设备可以正常登录而且使用的是同一个Radius Server，那么第一点可能性基本可以排除。那就要进一步看看设备CPU有没有正常处理Radius Response报文了。通过在设备上debug上CPU的报文发现，聚合组端口有大量的ICMP攻击报文冲上CPU，报文内容如下面的debug输出。其源MAC地址是固定的：0001-d7db-0089， 但是源IP是变化的，报文上CPU的速率大概有400-500个/秒，这些ICMP报文会进入CPU的0队列，而Radius Response报文也入CPU的0队列，因为CPU对各个队列的报文有CAR限制，这样radius的报文就会被挤掉。

*Sep 29 17:36:33:568 2011 DMZ-5800A RXTX/7/pkt:

From board 1: received packet from chip1,port24,reason=0x80000,cos=0,sMod=6,sPort=24,len=74, Matched=0

*Sep 29 17:36:33:569 2011 DMZ-5800A RXTX/7/pkt:

0000 38 22 d6 68 d6 33 00 01 d7 db 00 89 81 00 00 05

0010 08 00 45 00 00 38 eb dd 40 00 ff 01 1e 10 0a 22

0020 3e 0a 0a 14 1f 97 0b 00 c7 ba 00 00 00 00 45 68

0030 00 93 49 ce 00 00 01 11 16 ff 0a 14 1f 97 0a 1d

这样就会导致CPU丢弃掉Radius Response报文，从而导致了认证失败。

四、 解决方法：

移除网络里的攻击主机之后，认证恢复正常。本案例主要是给大家提供一种认证思路，要掌握的重点在于如何查看Radius的debug信息，并且掌握对“Radius Server no response”问题的排查思路。