

使用iNode 进行SSLVPN认证，上线1分钟左右后掉线

iNode

Radius

iMC

张兴龙

2020-06-23 发表

组网及说明

不涉及

问题描述

现场客户使用iNode 做SSLVPN认证，3A服务器用IMC，现场反馈iNode拨号上线后，出现1分钟左右就会下线的现象，下线原因为user-request



用户 > 用户接入日志 > test > 接入明细 > 接入明细详细信息			
接入明细详细信息			
基本信息			
帐号名	test	用户名	test
服务器名	bij	用户分组	未分组
登录名	test	接入策略名	bij
接入信息			
接入开始时间	2020-06-17 15:49:21	接入结束时间	2020-06-17 15:50:21
接入时长	1分钟0秒	下线原因	User Request (用户自动下线)
设备IP地址	192.160.128.34	设备端口号	66535
设备槽号		设备子槽号	
设备序列号		IMSI号码	
上传字节数	0	下载字节数	0
VLAN ID/内网VLAN ID		外网VLAN ID	

过程分析

问题分析和定位

一 收集UAM debug日志，通过查看日志可以看到设备侧主动发起了计费结束报文

下线原因为1，代表用户请求下线，因为这个是设备侧主动发起的下线报文

%% 2020-06-17 15:50:21.886 ; [LDBG] ; [18128] ; LAN ; test ; 4 ;

1113afb94bbf4ff99a05bbbc475073ea ; ; Received message from 192.160.128.34:

CODE = 4 ID = 213.

User-Name(1) = test

NAS-Identifier(32) = L01_F3F4_ZWW_FW_F5000M

NAS-IP-Address(4) = 3231744034.

Calling-Station-Id(31) = 70-1c-e7-4a-62-94

Acct-Session-Id(44) = 0000001120200617074335000000fb081296749

Acct-Session-Time(46) = 60.

Acct-Terminate-Cause(49) = 1. 设备发来主动下线，下线原因为user-request

Class(25) = i66HUNHT

hw_IP_Host_Addr(60) = 0.0.0.0 70:1c:e7:4a:62:94

hw_ISP_ID(17) = imc

Acct-Authentic(45) = 1.

Acct-Status-Type(40) = 2. 结束计费

Acct-Delay-Time(41) = 0.

Event-Timestamp(55) = 1592379875.

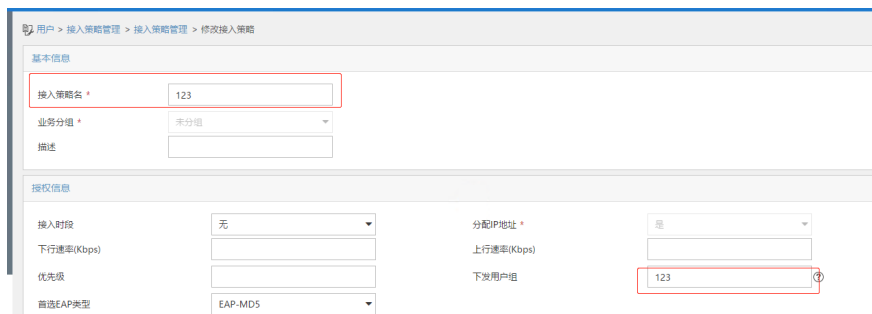
hw_Product_ID(255) = H3C SecPath F5000-M

hw_Nas_Startup_Timetamp(59) = 1591372538.

二、因为是设备侧主动发起的下线，联系设备侧进行定位，设备侧定位原因是iNode侧主动发送了下线的请求给设备，然后设备侧发送了下线请求给IMC，之后IMC侧将用户下线。

但是现场这个用户关联123的策略是可以认证成功，关联bij策略是不能认证成功的

1) 如下截图，test 用户关联认证策略123是可以上线成功，且上线后不掉线



用户 > 接入策略管理 > 接入策略管理 > 修改接入策略

基本信息

接入策略 * 123

业务分组 * 未分组

描述

授权信息

接入时段 无

下行速率(Kbps)

优先级

首选EAP类型 EAP-MD5

分配IP地址 * 是

上行速率(Kbps)

下发用户组 123

2) test 账号关联接入策略bij上线成功后，1分钟会下线

用户 > 接入策略管理 > 接入策略管理 > 修改接入策略

基本信息

接入策略名 *

bij

业务分组 *

未分组

描述

授权信息

接入时段

无

分配IP地址 *

否

下行速率(Kbps)

上行速率(Kbps)

优先级

下发用户组

bij

通过对比发现，这两个地方，接入策略种下发的用户组是不一样的，对比终端的配置可以看到，当使用接入策略123时，终端会有一个到策略服务器的路由（即终端可以正常和策略服务器通信）；当使用接入策略bij时，终端没有到策略服务器的路由（终端不可以和策略服务器通信）。

三、进一步分析iNode侧的日志，查看iNode报文可以看到，在用户test上线后，终端发送了很多out-pkt[1]报文，但是没有任何回复，这个报文是发给策略服务器的，目前iNode的机制就是在服务侧启用了策略服务器的情况下，如果iNode无法和策略服务器正常通信的情况下，会主动让终端下线。

```
<i n="userName">test</i>
[2020-06-17 15:49:50] [Dt1Cmn] [3bf0] SecPkt secPushInner: out-pkt [1] <data><i n="userName">test</i><i n="hwAddr">70:1C:E7:4A:62:94</i><i n="ev
[2020-06-17 15:49:55] [Dt1Cmn] [3bf0] SecPkt secPushInner: out-pkt [1] <data><i n="userName">test</i><i n="hwAddr">70:1C:E7:4A:62:94</i><i n="ev
[2020-06-17 15:50:01] [Dt1Cmn] [3bf0] SecPkt secPushInner: out-pkt [1] <data><i n="userName">test</i><i n="hwAddr">70:1C:E7:4A:62:94</i><i n="ev
[2020-06-17 15:50:06] [Dt1Cmn] [3bf0] SecPkt secPushInner: out-pkt [1] <data><i n="userName">test</i><i n="hwAddr">70:1C:E7:4A:62:94</i><i n="ev
[2020-06-17 15:50:12] [Dt1Cmn] [3bf0] SecPkt secPushInner: out-pkt [1] <data><i n="userName">test</i><i n="hwAddr">70:1C:E7:4A:62:94</i><i n="ev
[2020-06-17 15:50:17] [Dt1Cmn] [3bf0] SecPkt secPushInner: out-pkt [1] <data><i n="userName">test</i><i n="hwAddr">70:1C:E7:4A:62:94</i><i n="ev
[2020-06-17 15:50:23] [Dt1Cmn] [3bf0] SecPkt secPushInner: out-pkt [1] <data><i n="userName">test</i><i n="hwAddr">70:1C:E7:4A:62:94</i><i n="ev
[2020-06-17 15:50:29] [Dt1Cmn] [3bf0] SecPkt secPushInner: out-pkt [1] <data><i n="userName">test</i><i n="hwAddr">70:1C:E7:4A:62:94</i><i n="ev
[2020-06-17 15:50:34] [Dt1Cmn] [3bf0] SecPkt secPushInner: out-pkt [1] <data><i n="userName">test</i><i n="hwAddr">70:1C:E7:4A:62:94</i><i n="ev
```

解决方法

解决方案：

1) 如果现场不使用安全检查等相关功能项的话，可以关闭策略服务器

用户 > 接入策略管理 > 业务参数配置 > 系统配置 > 策略服务器参数配置

策略服务器参数配置

☐ 启用策略服务器

策略服务器配置端口 *

9013

策略服务器日志级别

提示

心跳间隔时长(秒) *

720

报文的压缩和加密

启用

☐ 在IPv6网络启用策略服务器

代理服务监听端口 *

9019

iNode管理中心IP

心跳超时次数(次) *

3

确定

返回

2) 配置终端路由，保证终端侧可以正常和策略服务器通信，本案例中，下发的用户组在设备侧有相关的配置，不通用户组终端上线后可以拿到不通的路由，保证终端上线的用户可以拿到到策略服务器的路由即可。