

知 iMC EIA和无线WX5510E配合进行Portal集中认证+本地转发特性时提示设备拒绝请求

Portal 罗孝晨 2015-12-25 发表

iMC和WX5510E配合配置本地转发集中portal认证的时候提示设备拒绝请求，在portal的调试日志里面看设备在回应ACK_INFO的时候是设备拒绝请求

无

1.根据之前处理过的Portal认证提示“向设备发送请求超时”处理经验，首先判断是否是iMC侧配置有问题，检查端口组，IP地址组，接入设备密钥和Portal设备密钥是否与设备侧保持一致，Netstat -aon |findstr 50100检查portal端口是否被占用。

修改端口组信息

端口组名 *	192.168.65.0 x	提示语言 *	动态检测
开始端口 *	0	终止端口 *	ZZZZZ
协议类型 *	HTTP	快速认证 *	否
是否NAT *	否	错误透传 *	是
认证方式 *	CHAP认证	IP地址组 *	yiche-29
心跳间隔(分钟) *	0	心跳超时(分钟) *	0
用户域名		端口组描述	
无感知认证	不支持	客户端防破解 *	否
页面推送策略	portal	缺省认证页面	PHONE - 手机

用户 > 接入策略管理 > Portal服务管理 > 设备配置 > 设备详细信息

设备详细信息

设备名	ac	业务分组	未分组
版本	Portal 2.0	IP地址	172.20.2.250
监听端口	2000	本地Challenge	否
认证重发次数	0	下线重发次数	1
支持逃生心跳	否	支持用户心跳	否
密钥	*****	组网方式	直连
最近一次下发时间	2015-12-22 15:57:47	下发结果	失败
下发失败原因	Telnet登录失败。		
设备描述			

IP地址组详细信息

IP地址组名	yiche-29
业务分组	未分组
起始地址	192.168.65.1
终止地址	192.168.65.253
类型	普通
使用此IP地址组的设备名	ac

2、收集Portal调试级别日志进行分析：

2015-12-23 10:23:51.768[Portal服务器][调试(0)][24][ProxyResponseDeviceHandler::run]
192.168.65.4;REQ_INFO(9);128;172.20.2.250:2000;报文处理成功

Packet Type:REQ_INFO(9)
SerialNo:128
Address:192.168.70.174
Port:50300
RemoteIp:172.20.2.250
RemotePort:2000
Version:portal 2.0//IPV4 版本
Auth Type:CHAP
ErrorID:0
UserIP:192.168.65.4
UserPort:0

ReqID:0
Rsvd:0
attriNum:1

Port:

2015-12-23 10:23:51.771[Portal服务器][调试(0)][21][ProxyRequestHandler::run]192.168.65.4 ; ACK_I
NFO(10) ; 128 ; 172.20.2.250:2000 ; 设备拒绝请求(1)

Packet Type:ACK_INFO(10)
SerialNo:128
Address:192.168.70.174
Port:50908
RemoteIp:172.20.2.250
RemotePort:2000
Version:portal 2.0
Auth Type:CHAP
ErrorID:1 \\这个错误值是设备侧回应给iMC服务器的
UserIP:192.168.65.4
UserPort:0
ReqID:0
Rsvd:0
attriNum:1

Device Time Stamp:1445179866

597	10:28:15.318579000	172.20.2.250	192.168.70.174	PORTAL	76	Portal type Unknown (0x30)
598	10:28:15.322392000	192.168.70.174	172.20.2.250	PORTAL	58	Portal type Unknown (0x31)
841	10:28:21.318077000	192.168.70.174	172.20.2.250	PORTAL	76	Portal type REQ_INFO
842	10:28:21.320735000	172.20.2.250	192.168.70.174	PORTAL	80	Portal type ACK_INFO
893	10:28:21.324531000	192.168.70.174	172.20.2.250	PORTAL	74	Portal type REQ_CHALLENGE
844	10:28:21.325381000	172.20.2.250	192.168.70.174	PORTAL	80	Portal type ACK_CHALLENGE
1153	10:28:23.497485000	172.20.2.250	192.168.70.174	PORTAL	76	Portal type Unknown (0x30)
1154	10:28:23.503411000	192.168.70.174	172.20.2.250	PORTAL	58	Portal type Unknown (0x31)
1535	10:28:28.376273000	192.168.70.174	172.20.2.250	PORTAL	76	Portal type REQ_INFO
1536	10:28:28.379799000	172.20.2.250	192.168.70.174	PORTAL	80	Portal type ACK_INFO
1537	10:28:28.381634000	192.168.70.174	172.20.2.250	PORTAL	74	Portal type REQ_CHALLENGE

User Datagram Protocol, Src Port: cisco-sccp (2000), Dst Port: 50100 (50100)
Source port: cisco-sccp (2000)
Destination port: 50100 (50100)
Length: 46
Checksum: 0xd0c1 [validation disabled]

PORTAL Protocol
VERSION: 2
Type: ACK_INFO (0x0a)
Pap/Chap: 0x00
Reserve: 0
Serial Number: 136
Request ID: 0
User IP: 192.168.65.4 (192.168.65.4)
User Port: 0
Error Code: 0x01
Attribute Number: 0x01

0000	00 1d d8 b7 1e 69 00 26	99 00 0f 45 08 00 45 00	i.& ...E..E.
0010	00 42 90 e2 00 00 fc 11	77 63 ac 14 02 fa c0 a8	.B..... WC.....
0020	46 ae 07 d0 c3 b4 00 2e	d0 c1 02 0a 00 00 00 88	F..... ..
0030	00 00 c0 a8 41 04 00 00	01 01 b6 27 0f dc b2 76	...A... ..V
0040	bb ea 7f 56 6a 3a ad df	ad cc 26 06 56 23 b1 da	...vj:... ..&.V..

通过抓包中红色标注的信息可以分析出,设备所有的回应报文中都包含Error Code: 0X01, 这和iMC的portal日志中ErrorID=1对应起来。整个portal报文交互过程中, iMC给接入设备发送的报文内容没有错误, 所以要分析为什么iMC给接入设备发送的REQ报文后, 设备都给iMC回应了设备拒绝请求。因此需要进一步分析设备侧给iMC回应的Error Code: 0X01的触发原因。

3、关于设备拒绝请求的原因, 从设备回应的ACK-CHALLENGE报文携带的ErrorID=1, 根据经验可能是设备侧没有该终端对应的ARP表项或者设备队列满导致, 建议设备侧进行排查。后通过主网络工程师对AC的配置进行分析后, 发现在使用本地转发+集中认证模式进行portal认证时, AC侧需要在全局模式下增加一条命令为:wlan client learn-ipaddr enable, 通过此命令来开启无线客户端IP地址窥探功能。如果没有配置此命令, 会导致设备回应iMC报文中携带ErrorID=1的错误值。

1、设备侧排查后发现, 分析是无线侧没有配置learn-ipaddr功能, 需要在AC上配置wlan client learn-ipaddr enable

【描述】

wlan client learn-ipaddr enable 命令用来开启无线客户端IP地址窥探功能。**undo wlan client learn-ipaddr enable**命令用来关闭无线客户端IP地址窥探功能。

缺省情况下，无线客户端IP地址窥探功能处于关闭状态。

【举例】

开启无线客户端IP地址窥探功能。

```
<Sysname> system-view
```

```
[Sysname] wlan client learn-ipaddr enable
```

- 1、抓包分析进行判断portal报文有无错误
- 2、分析认证过程进行到哪一步出现问题
- 3、重点检查设备侧和iMC侧配置
- 4、对于设备侧给iMC回应的报文中含有ErrorID，需要设备侧进行定位，该报文为设备侧发送给iMC服务器。