AC跨公网对接IMC因服务器无法获取终端IP地址导致portal认证失败问题

Portal 谭奇伟 2024-10-01 发表

组网及说明

AC跨公网对接IMC认证服务器，AC纳管的AP和接入的无线终端与IMC认证服务器之间也跨越公网，无线终端的地址在出口经过NAT转换，AC服务模板下配置远程portal认证。

告警信息

无

问题描述

故障AC下无线终端均无法通过portal认证，在AC和核心交换机上直连接口镜像抓包发现，IMC的req-info报文发送给AC，但是AC没有回复IMC的ack-info报文，也没有回复其它报文，导致认证失败。

	Protocol	Time	Source	Destination	Vlan	Lengt	Info
4022	Portal	2024-08-27 15:12:22.651298	10.	10.		76	REQ_INFO

过程分析

根据上述故障描述，IMC应当将portal的req-info报文发给了AC，但是AC却没有回复，这就需要在AC上通过debug等方法进一步查看。

首先在AC上开启如下debug命令，同时复现故障：

<AC> debug portal error

<AC> debug portal event

<AC> debug portal packet

<AC> debug radius all

<AC> debug radius error

[AC] info-center enable

<AC> t m

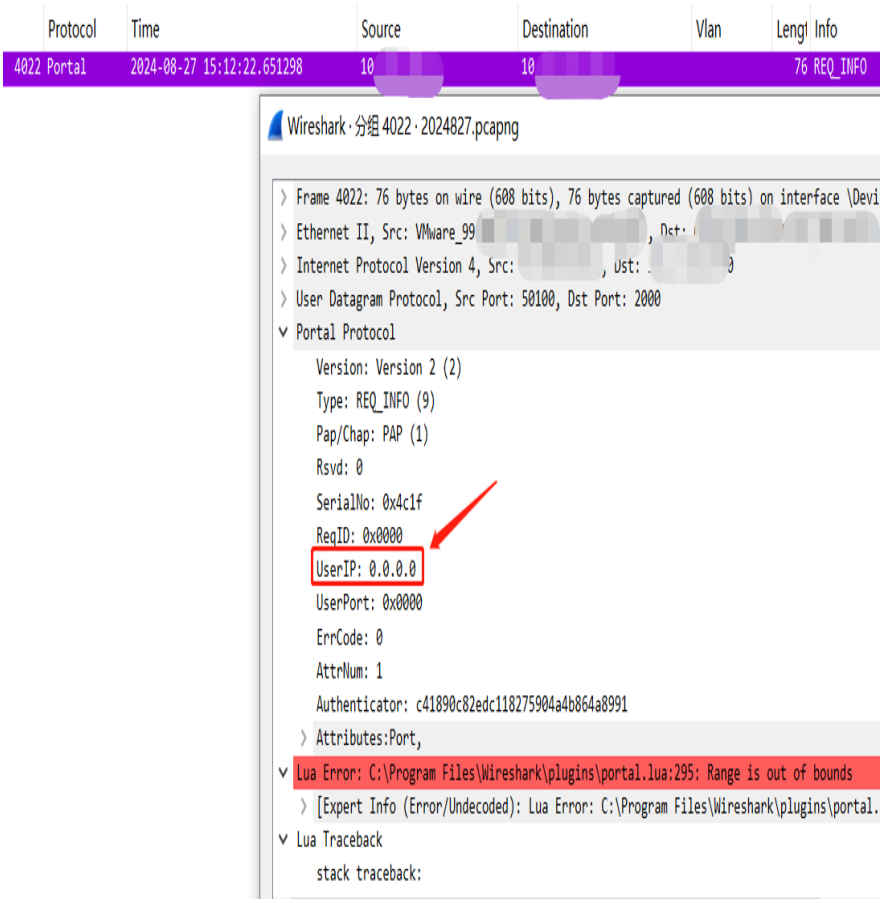
<AC> t d

复现故障后发现，尽管抓包发现IMC将req-info发送给了AC，但是AC上仍然没有任何portal报文的debug记录打印，那么是否IMC发送给AC的req-info报文在AC内部被丢弃了呢？

在AC上通过：display portal packet statistics server xxx 查看，发现经过再次的portal认证故障复现后，只有Invalid packets计数有增长，这说明IMC发给AC的req-info报文被AC认为是无效的。

参考知了案例：https://zhiliao.h3c.com/theme/details/223494

检查IMC发送给AC的req-info报文，发现req-info报文中没有填写userip（终端的IP地址）字段，该字段没有填写导致AC将此报文识别为无效报文，因此需要找IMC确认为什么没有IMC发送给AC的req-info报文没有填写userip字段。



经IMC侧排查，这是由于portal服务器没有获取到认证无线终端的IP地址，这与近期修改了IMC portal server的安全策略有关。

在修改安全策略后，IMC portal server通过无线终端发送给服务器HTTP报文中的userip字段（AC上portal web-server下的url-parameter userip xxx属性携带）来获取终端私网IP地址，而当前AC的portal web-server下配置的是：url-parameter wlanuserip source-address，IMC portal server在新的安全策略下无法识别wlanuserip字段，因此portal server会继续尝试从终端HTTP请求的源地址获取终端IP地址，而HTTP请求的源地址是经过NAT转换后的地址，因此portal server就拿不到终端的私网IP地址，导致req-info和ack-info握手失败，从而导致认证失败。

解决方法

在AC的portal web-server newpt下的把

url-parameter wlanuserip source-address

改成：

url-parameter userip source-address用来在终端给IMC portal server的HTTP报文中携带终端的私网IP地址。