某局点结合第三方认证服务器portal认证失败的处理经验案例

wlan接入 丁佳欣 2020-06-09 发表

组网及说明

null

问题描述

某局点开局部署结合第三方认证服务器的portal认证，现场出现用户终端能够成功弹出portal页面后，输入用户名和密码认证失败的问题，于是我们对此原因展开分析。

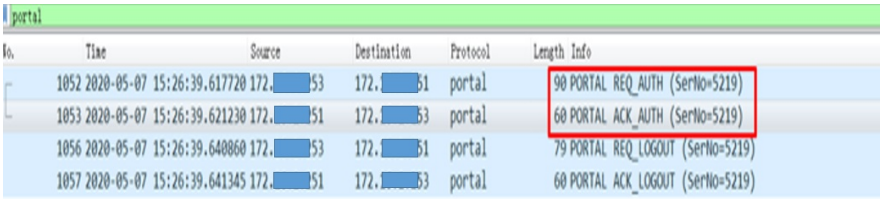
过程分析

（1） 首先检查配置，暂时没有发现问题

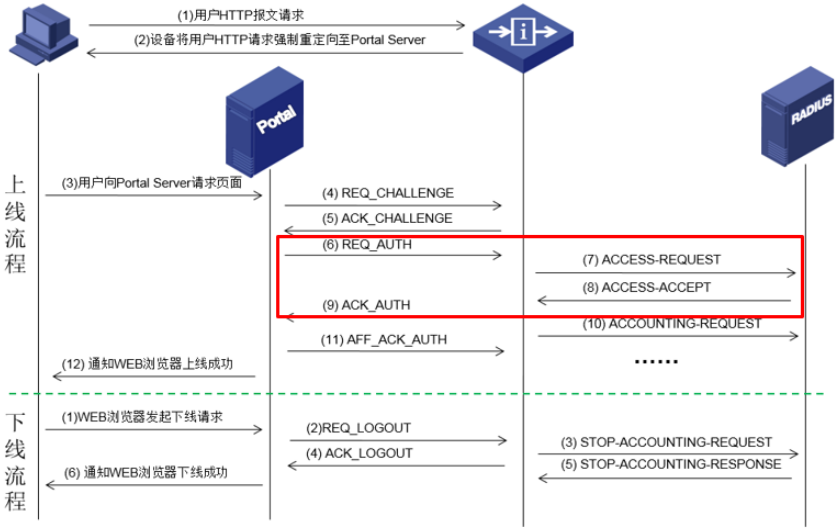
Portal的主要配置如下：

```
radius scheme portal
 primary authentication 172.X.X.253
 primary accounting 172.X.X.253
 key authentication cipher $c$3$5jlgF2ZY0MbHWGKx/MAkWLWBu1FuGIU=
 key accounting cipher $c$3$nIOLVsSE8ReppFfnSI5Eo9UPrjjqe6o=
 user-name-format without-domain
 nas-ip 172.X.X.251
#
domain portal
 authorization-attribute idle-cut 15 1024
 authentication portal radius-scheme portal
 authorization portal radius-scheme portal
 accounting portal radius-scheme portal
#
portal host-check enable
 portal free-rule 0 destination ip 172.X.X.0 255.255.255.0
 portal free-rule 1 destination ip X.X.X.66 255.255.255.255
 portal free-rule 2 destination ip X.X.X.X 255.255.255.255
#
portal web-server portal
 url http://172.X.X.253/cid/8264/portal.html
 url-parameter bssid ssid
 url-parameter redirect original-url
 url-parameter staip source-address
 url-parameter stamac source-mac
 url-parameter vlan1 vlan
#
portal server portal
 ip 172.X.X.253 key cipher $c$3$Wqd9HodvO33bkT8gNBSqeZcU5icxESo=
```

（2） 在AC上进行抓包分析：



Portal认证原理：



从抓包结果结合portal认证原理进行分析，我们可以看出portal服务器向AC发送认证请求REQ_AUTH报文后AC直接回复了认证应答的ACK_AUTH报文，跳过了本应该向radius服务器发起的接入请求和radius服务器允许接入应答的过程，即下图中过程（7）、（8）。

在终端即表现为用户向portal server请求页面成功后，输入用户名和密码无法认证成功。

（3） 为什么AC未向radius服务器发起接入请求呢，我们结合radius和portal的debug信息进一步分析，下面分开说明：

Radius的debug信息：

Debugging radius all:

May 7 15:10:06:136 2020 无线PORTAL/7/FSM: User-SM [172.X.X.100]: State changed from Initial to Authenticating.

*May 7 15:10:06:136 2020 无线RADIUS/7/EVENT:

Got RADIUS server info successfully.

*May 7 15:10:06:136 2020无线 RADIUS/7/EVENT:

Created request context successfully.

*May 7 15:10:06:136 2020 无线RADIUS/7/EVENT:

Created request packet successfully, dstIP: 172.X.X.253, dstPort: 1812, VPN instance: --(public), socketFd: 85, pktID: 16.

*May 7 15:10:06:137 2020 无线RADIUS/7/EVENT:

Added packet socketfd to epoll successfully, socketFd: 85.

*May 7 15:10:06:137 2020 RADIUS/7/EVENT:

Mapped PAM item to无线RADIUS attribute successfully.

*May 7 15:10:06:137 2020 无线RADIUS/7/ERROR:

Failed to fill RADIUS attribute in packet. //填充radius属性失败

*May 7 15:10:06:137 2020 无线RADIUS/7/ERROR:

Failed to compose request packet. //无法构成请求包

*May 7 15:10:06:137 2020无线 RADIUS/7/ERROR:

Failed to send request packet and create request context. //发送请求包失败

*May 7 15:10:06:137 2020 无线RADIUS/7/EVENT:

Sent reply message successfully.

*May 7 15:10:06:137 2020 RADIUS/7/EVENT:

PAM_RADIUS: Processing 无线RADIUS authentication.

*May 7 15:10:06:138 2020 无线RADIUS/7/EVENT:

PAM_RADIUS: Fetched authentication reply-data successfully, resultCode: 4

*May 7 15:10:06:138 2020 无线RADIUS/7/EVENT:

Processing AAA request data.

从radius的debug信息，我们得知Radius 报文封装失败。

Portal的debug信息：

Debugging portal all:

*May 8 17:30:15:201 2020 无线PORTAL/7/ERROR: Packet validity check failed due to invalid authenticator. //认证发起者无效导致认证包的合法性检查失败

*May 8 17:30:15:201 2020无线 PORTAL/7/EVENT: Success to get info from wlan snooping, vlan:100. mac:c498-8038-70cf,userip:172.X.X.100

*May 8 17:30:15:201 2020 无线PORTAL/7/EVENT: Success to get ifindex(628) and vlan(100) from IPCIM, user IP=172.X.1.100

*May 8 17:30:15:201 2020 无线PORTAL/7/ERROR: The packet is invalid. //认证包无效

从以上portal的debug信息，我们得知认证发起者和认证包都是无效

解决方法

出现以上报错一般是由于AC上配置的portal服务器密钥与认证服务器上配置的portal服务器密钥不一致导致。

因此我们怀疑是由于现场的共享密钥配置错误导致认证失败。后续让现场修改密钥后问题解决。