

知 v7 对终端重定向攻击的处理方法

wlan接入

AAA

协议报文限速

陆启隆

2019-04-04 发表

组网及说明

集中转发，典型Portal认证组网

问题描述

现场发现有攻击终端，一直在大量发送https的重定向报文，导致ac的某个转发核资源耗尽，进而影响了连接到该转发核上用户报文的转发，导致部分终端无法上网。

过程分析

对于该问题最终的解决方法是找到问题终端，从根本上解决攻击报文的来源。但在找到该终端之前可以在设备上配置命令，暂时规避。

portal redirect max-session per-user命令用来配置单用户Portal 重定向的最大会话数。后面的数值可根据现场的情况进行调整。

【使用指导】当用户客户端装了恶意软件或遭到病毒攻击时，会发起大量Portal 重定向会话。本命令用来同时配置设备上单个Portal 用户的HTTP 和HTTPS 重定向的最大会话数，即单个Portal 用户的HTTP 重定向的最大会话数和HTTPS 重定向会话数均为设置值，Portal 重定向的总最大会话数为二者之和。对于无线应用，仅集中转发模式生效。

【举例】# 配置单用户 Portal 重定向的最大会话数为128。

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

```
[Sysname] portal redirect max-session per-user 128
```

解决方法

配置该命令，现场调整参数为10，观察一段时间，用户可以正常上网，该问题解决。