某局点本体CPU达到100%问题处理案例

终结者 张燃 2019-10-18 发表

组网及说明

无

问题描述

现场组网特殊，采用的是adcampus组网，AP是终结者的本体和分体，同时现场的vlan划分不合理，全校只有两个vlan，一个是学生vlan，一个是老师vlan。同时在分体的下行口还有有线接入，有线无线采用同一个vlan。同时现场采用的是全vlan免认证。所以现场的终端数量很大。

过程分析

基于现场的组网、环境情况，现场的组网规划不合理，首先有线无线必须要划分开，用单独的vlan进行数据转发；其次无线的业务vlan要合理划分，可以根据终端数量级、业务分类等进行划分，尽量不要让一个vlan过大。查看本体CPU进程，发现evHndl_6进程高，这个进程表示收包线程，目前整机收包线程cpu高。收包线程cpu高一般首先怀疑是广播量大或者存在不正常的报文复制。 现场有线抓包发现确实有大量的arp请求，源地址基本为各种终端。基本是由于大量的广播报文达到AP有线口，导致的CPU达到100%。

解决方法

根据现场的情况，解决方法如下：

1、网络规划必须要有线无线分开，无线vlan划分要合理。

2、现网所有设备下行口开启端口隔离，无线vlan开启vlan内用户隔离。

3、现网环境尽量做认证，不要全vlan免认证上网。

4、由于现场存在大量的终端广播大量的arp请求，所以配置arp攻击检测（该配置要在终端的转发点上配置才有效，现场是直通模式本地转发，通过map文件下发到分体上。）

配置限制和指导

切换源MAC地址固定的ARP攻击检查模式时，如果从监控模式切换到过滤模式，过滤模式马上生效；如果从过滤模式切换到监控模式，已生成的攻击检测表项，到表项老化前还会继续按照过滤模式处理。

对于网关或一些重要的服务器，可能会发送大量ARP报文，为了使这些ARP报文不被过滤掉，可以将这类设备的MAC地址配置成保护MAC地址，这样，即使该设备存在攻击也不会被检测或过滤。

配置步骤

(1) 进入系统视图。

system-view

(2) 开启源MAC地址固定的ARP攻击检测功能，并选择检查模式。

arp source-mac { filter（过滤） | monitor（监控） }

缺省情况下，源MAC地址固定的ARP攻击检测功能处于关闭状态。

(3) 配置源MAC地址固定的ARP报文攻击检测的阈值。

arp source-mac threshold threshold-value

本命令的缺省情况与设备的型号有关，请以设备的实际情况为准。

(4) 配置源MAC地址固定的ARP攻击检测表项的老化时间。

arp source-mac aging-time time

缺省情况下，源MAC地址固定的ARP攻击检测表项的老化时间为300秒，即5分钟。

(5) （可选）配置保护MAC地址。

arp source-mac exclude-mac mac-address&<1-n>

缺省情况下，未配置任何保护MAC地址。