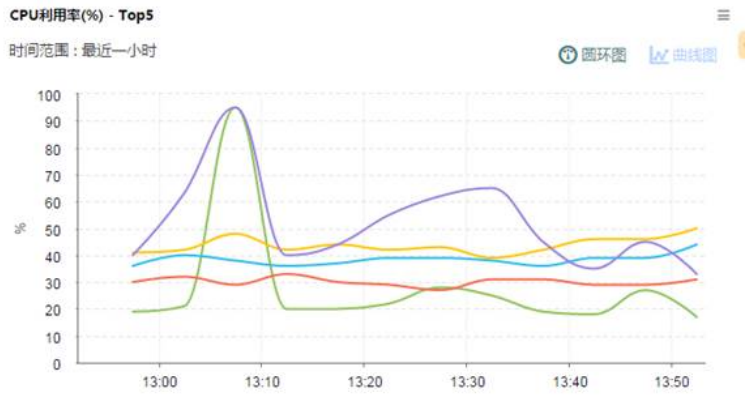
防御无线终端DOS（泛洪）攻击

wlan接入 攻击检测及防范 **殷俊** 2016-01-11 发表

无线DOS攻击会导致AP繁忙，报文处理不过来，报文上送AC后 CPU上升到95%以上，导致受攻击的AP，AC无法正常工作，数据转发甚至设备运行情况收到很大程度的影响。

AC CPU利用率达到95%以上



通过协议报文统计查看，发现CPU利用率瞬时升高时，终端关联认证请求报文（auth request）突然异常增多，与历史数据统计相比，并非一个数量级。该种行为在用户正常无线接入是不可能出现，判断为终端恶意攻击，报文统计信息如下：

协议号	时间	丢弃	已处理
4955 dot11_auth	13:01:56 12/16/2015	609	2407
4956 dot11_auth	13:02:56 12/16/2015	609	2179
4957 dot11_auth	13:03:57 12/16/2015	609	2320
4958 dot11_auth	13:04:57 12/16/2015	609	2329
4959 dot11_auth	13:05:58 12/16/2015	609	2431
4960 dot11_auth	13:06:58 12/16/2015	609	2540
4961 dot11_auth	13:08:04 12/16/2015	9074	19368
4962 dot11_auth	13:09:06 12/16/2015	10447	8185
4963 dot11_auth	13:10:07 12/16/2015	10447	1991
4964 dot11_auth	13:11:07 12/16/2015	10447	2259
4965 dot11_auth	13:12:08 12/16/2015	10447	2148
4966 dot11_auth	13:13:08 12/16/2015	10447	2064
4967 dot11_auth	13:14:08 12/16/2015	10447	2046
4968 dot11_auth	13:15:09 12/16/2015	10447	2263
4969 dot11_auth	13:16:09 12/16/2015	10447	2237
4970 dot11_auth	13:17:09 12/16/2015	10447	2316
4971 dot11_auth	13:18:10 12/16/2015	10447	2316
4972 dot11_auth	13:19:10 12/16/2015	10447	2378
4973 dot11_auth	13:20:11 12/16/2015	10447	2315

配置方法：

#使能终端关联认证请求报文（auth request）协议的总带宽限速功能

anti-attack protocol dot11_auth enable

#配置协议限速速率，限速速率是协议所能拥有的总带宽，超过该带宽的流量都会被限速模块限制并丢弃掉，取值范围为0～102400，单位为包每秒（pps）。

anti-attack protocol dot11_auth threshold 40

#协议按流限速速率，按流限速速率是指用户的某类协议报文所能拥有的最大带宽。超过该带宽的流量都会被限速模块限制并丢弃掉，取值范围为0～102400，单位为包每秒（pps）。

anti-attack protocol dot11_auth flow-threshold 20

对于大型公共wifi场景，实时监测网络运行情况，对于该类攻击实施有效的防御措施。

该类攻击源地址分为两种：

1.静态mac地址模拟协议报文攻击。这种情况对于攻击终端的mac比较容易定位，突发的流量较高，发包速率较高，可以通过WIDS配置静态黑名单的方法限制。

2.动态mac地址模拟协议报文攻击。这种情况比较难于定位到攻击终端，因为攻击终端每个攻击报文都是随机生成mac地址作为源去发送，建议通过限制报文发送速率来控制