WA系列FAT AP动态黑名单功能的配置

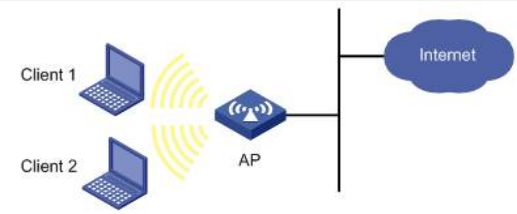
wlan接入 wlan安全 攻击检测及防范 **宋斌** 2011-10-13 发表

WA系列FAT AP动态黑名单功能的配置

一、 组网需求：

WA系列FAT AP（如WA2220-AG）、交换机、便携机（安装有11b/g无线网卡）

二、 组网图：



本配置举例中Client 1和Client 2是两个无线用户，当他们对AP发起泛洪攻击时，AP就可以把他们添加到动态黑名单里。

三、 特性介绍：

泛洪攻击（Flooding攻击）是指WLAN设备会在短时间内接收了大量的同种类型的报文。此时WLAN设备会被泛洪攻击报文淹没而无法处理真正的无线终端的报文。

IDS攻击检测通过持续的监控每台设备的流量大小来预防这种泛洪攻击。当流量超出可容忍的上限时，该设备将被认为要在网络内泛洪从而被锁定，此时如果使能了动态黑名单，检查到的攻击设备将被加入动态黑名单。

IDS支持下列报文的泛洪攻击检测：

- 认证请求/解除认证请求（Authentication / De-authentication）
- 关联请求/解除关联请求/重新关联请求（Association / Disassociation / Reassociation）
- 探查请求（Probe request）
- 空数据帧
- Action帧

当一个AP支持超过一个BSSID时，无线终端会发送探查请求报文到每个单独的BSSID。所以在报文为探查请求报文的情况下，需要考虑源端和目的端的共同流量，而对于其它类型的报文，只需要考虑源端的流量即可。

动态黑名单功能作为一种防护手段，有效地应对了网络中潜在存在的客户端对AP发起的泛洪攻击，保障AP正常工作。

四、 主要配置步骤

配置WIDS。

```
[AP] wlan ids
```

使能泛洪攻击入侵检测。

```
[AP-wlan-ids] attack-detection enable flood
```

使能动态黑名单功能。

```
[AP-wlan-ids] dynamic-blacklist enable
```

#设置动态黑名单表项生命周期。

```
[AP-wlan-ids] dynamic-blacklist lifetime 500
```

当Client被加入到动态黑名单中时，Client将被“管制”所设置的lifetime的时间。Client从黑名单中“释放”的条件是lifetime时间到期且Client不再发攻击报文。这个lifetime时长可以根据要求设置，范围是1分钟到1小时，设备默认时长是300秒。

五、 结果验证：

当Client 发起对AP泛洪攻击时（例如：Client向AP发送大量攻击性关联帧报文，或者向AP发送大量攻击性去关联帧报文），AP将该Client 加入到动态黑名单中，在一段时间

内该Client将不能与AP发生关联。

```
display wlan blacklist dynamic
Total Number of Entries: 2
                        Dynamic Blacklist
------------------------------------------------------------------------------
 MAC-Address    Lifetime(s) Last Updated Since(hh:mm:ss)     Reason
------------------------------------------------------------------------------
 000e-35b2-8be9 500         00:02:11                      Assoc-Flood
 0000-0000-0002 500         00:01:17                      Deauth-Flood
```

Assoc-Flood指该Client因发送关联帧攻击而被加入黑名单；Deauth-Flood是指该Client因发送去关联帧攻击而被加入到黑名单中。