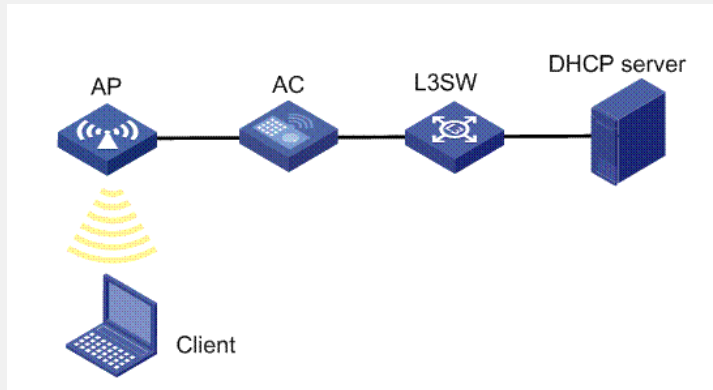


WX系列AC实现动态黑名单典型配置

一、组网需求

WX系列AC、FIT AP、交换机、便携机2台（安装有无线网卡）、

二、组网图



本配置举例中的AC使用的是WX6103无线控制器，AP使用的是WA2200系列无线局域网接入点设备，Client上线后通过DHCP服务器获取IP地址。

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设备会被泛洪的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：

- 1) 认证请求/解除认证请求（Authentication / De-authentication）；
- 2) 关联请求/解除关联请求/重新关联请求（Association / Disassociation / Reassociation）；
- 3) 探查请求（Probe request）；
- 4) 空数据帧；
- 5) 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地的共同流量，而对于其它类型的报文，只需要考虑源端的流量即可。

四、配置信息

```
display current-configuration
#
version 5.20, Release 2108
#
sysname AC
#
domain default enable system
#
vlan 1
#
domain system
access-limit disable
state active
idle-cut disable
self-service-url disable
#
wlan rrm
11a mandatory-rate 6 12 24
11a supported-rate 9 18 36 48 54
```

```

11b mandatory-rate 1 2
11b supported-rate 5.5 11
11g mandatory-rate 1 2 5.5 11
11g supported-rate 6 9 12 18 24 36 48 54
#
wlan service-template 1 clear
ssid wmm
bind WLAN-ESS 1
authentication-method open-system
service-template enable
#
interface NULL0
#
interface Vlan-interface1
ip address 63.1.1.20 255.255.0.0
#
interface M-GigabitEthernet1/0/1
#
interface Ten-GigabitEthernet1/0/1
port link-type trunk
port trunk permit vlan all
#
interface WLAN-ESS1
#
wlan ap ap model WA2220E-AG
serial-id 210235A29F007C000177
radio 1
channel 157
service-template 1
radio enable
radio 2
#
wlan ids
dynamic-blacklist enable
attack-detection enable flood
#
user-interface con 0
user-interface aux 0
user-interface vty 0 4
#
return

```

五、 主要配置步骤

```

# 在WLAN IDS视图下使能动态黑名单功能
[AC] wlan ids
[AC-wlan-ids] dynamic-blacklist enable
[AC-wlan-ids] attack-detection enable flood

```

六、 验证结果

当检测到洪攻击后（可以使用模拟工具每秒发送100个管理帧给AP），攻击源被加入动态黑名单，在动态黑名单老化期内，AC拒绝攻击源关联请求。

```
display wlan ids statistics
```

```
Current attack tracking since: 2008-08-29/10:22:07
```

Type	Current	Total
Probe Request Frame Flood Attack	0	0
Authentication Request Frame Flood Attack	0	0
Deauthentication Frame Flood Attack	1	1
Association Request Frame Flood Attack	0	0
Disassociation Request Frame Flood Attack	0	0
Reassociation Request Frame Flood Attack	0	0
Action Frame Flood Attack	0	0
Null Data Frame Flood Attack	0	0
Weak IVs Detected	0	0

Spoofed Deauthentication Frame Attack	0	0
Spoofed Disassociation Frame Attack	0	0

display wlan blacklist dynamic

Total Number of Entries : 1

Dynamic Blacklist

MAC-Address Lifetime(s) Last Updated Since(hh:mm:ss) Reason

000f-e2cc-ff01 300 00:00:04 Deauth-Flood
