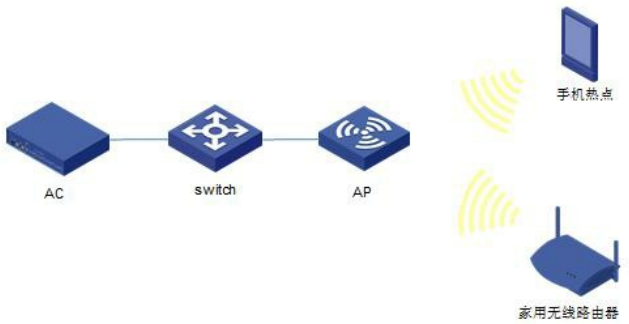
WIPS扫描无线热点干扰典型配置举例

WIPS wlan优化 殷俊 2017-09-28 发表

在公共wifi使用场景中，考虑到无线接入安全问题，防止其他无线厂商、私设无线路由设备等配置与我司相同SSID来做钓鱼攻击，需要对此类仿冒SSID进行监控，但考虑到无线网络的可接入性，在未检测到私设SSID时不进行反制行为，只做监控。这类场景特别是安全级别较高的大型会展、新闻中心、重要会议中心等场所。此类场所一般现场wifi信号数量不可控，存在大量wifi信号，特别是新闻记者较多时，对wifi的依赖更高，现场可能存在非常多的私设无线路由器、手机热点等。大量wifi信号的存在，不仅容易引发钓鱼攻击行为，更导致无线干扰严重，影响用户体验。特别是在无线WLAN网络高密覆盖场景，此类行为更为紧张。

对于这种wifi信号较多的场景，大多数客户是通过在现场通过wifi扫描软件采集现场存在的wifi信号信息，而这些信息可能随着用户实际使用行为动态变化，不可能时时刻刻守在现场扫描。因此，我司无线可以通过WIPS模块让AP对周遭环境进行无线网络扫描，只需远程监控就可采集现场实际存在的wifi信号，评估干扰源。

WIPS相对于WIDS作为扫描监控的优势在于，数据采集更精细话，更容易精确定位扫描终端位置，并且更容易精确判断或反制恶意干扰源。



1.配置WIDS扫描监控

#进入系统视图

<AC> system-view

配置AP开启WIPS功能，并设置为带外sensor，即此时AP仅做监测AP（对非法设备进行检测），不做接入AP。

[AC] wlan ap ap model WA4620i-ACN

[AC-wlan-ap-ap] serial-id 210235A29G007C000022

[AC-wlan-ap-ap] radio 1

[AC-wlan-ap-ap-radio-1] wips detect mode detect-only

[AC-wlan-ap-ap-radio-1] radio enable

[AC-wlan-ap-ap-radio-1] radio 2

[AC-wlan-ap-ap-radio-2] wips detect mode detect-only

[AC-wlan-ap-ap-radio-2] radio enable

进入WIPS视图，开启WIPS模块功能。

[AC]wlan ips

[AC-wlan-ips]wips enable

创建新的自定义AP分类规则“1”

[AC-wlan-ips]ap-classification-rule 1

设置匹配上该自定义AP分类规则的AP为rouge AP

[AC-wlan-ips-class-1]classify-type rogue-ap

自定义AP分类规则的匹配条件为SSID，SSID为H3C

[AC-wlan-ips-class-1]sub-rule ssid equal H3C

添加指定无线设备的MAC地址到静态信任设备列表已知合法AP的MAC

[AC-wlan-ips]static-trustlist 000f-e45d-fa00

若不知则可以使用厂商来区分static-trustoui

[AC-wlan-ips] static-trustoui 3891d5

[AC-wlan-ips] static-trustoui vendor h3c

WIPS纯扫描不接入情况下（detect-only），是每个信道60ms，即信道与信道之间间隔60ms。扫到最后一个信道直接再回头扫第一个信道，间隔也是60ms。例如13个信道加起来也就780ms，不到1s。那么扫到rouge-ap之后，在AC上看状态status是active。所以扫到一个rogue-ap，从这个rouge-ap消失开始算，缺省情况下，最大780ms一个轮询周期扫不到后，过300s会从active状态置为inactive，这期

间要最多要等20s，AC上才能刷新一次表项。所以从AC上看，最多320s后可以从AC上看到终端置为inactive。然后再过86400s后，表项自动删除。除非在这期间这个rogue-ap又启动了，则从启动开始算，最多在780ms内扫到，并置为active状态。所以要做到扫描最敏感的话，以上三个时间周期都要改短。但不能改的太短，怕扫到的信号多的情况下更新压力大，而且更新的太快的话，可能还没及时发现某些信号，表项就被清掉了。

AC上显示信息缺省每隔20s更新一次，可修改，默认20s，建议改为10s。

[AC-wlan-ips] timer device-update 10

如果Rouge AP如果不在了，active置为inactive状态，默认是300s，可修改，建议改为120s。

[AC-wlan-ips] timer ap-inactivity 120

置为inactive状态后，表项老化删除时间默认是86400s（24h），可修改，建议修改为900s。

[AC-wlan-ips] timer device-aging 900

2.验证WIPS扫描监控结果

显示所有虚拟安全域中的无线接入服务的信息，可以比较直观的看到监控扫描AP在部署区域内可扫描到现场有多少私设SSID，或者说可以扫描到有多少无线设备。

<AC> display wlan ips network

#AP = number of APs, VSD = virtual security domain

Detected Wireless Networks

SSID	Security	Auth-Method	Encrypt-Method	#AP

VSD default: 83

	Clear	None	-NA-	3
	WPA2	PSK	CCMP	1
Linus&＃39;s ASUS	WPA2	PSK	CCMP	1
HUAWEI-E5573-710C	WPA2	PSK	CCMP	1
island-0E8D90	WPA2	PSK	CCMP	1
ZMI_CC76	WPA2/WPA	PSK	TKIP/CCMP	1
ChinaNet-1D43	WPA2/WPA	PSK	TKIP/CCMP	1
ChinaNet-3C16	WPA2/WPA	PSK	TKIP/CCMP	1
ChinaNet-1D19	WPA2/WPA	PSK	TKIP/CCMP	1

……

显示所有虚拟安全域中的所有设备的详细信息。可以通过详细信息，查看到对应的这个干扰SSID是被哪台监控AP扫到的，并且这台监控AP扫到的干扰信号的RSSI值，可以大概判断这台设备所处的位置。

<AC> display wlan ips devices verbose

[AC]dis wlan ips devices verbose

Detected Wireless Devices

VSD: default

Total Number of APs: 599

BSSID : 60da-83b6-4c10

Vendor: -NA-

SSID : BRICS2017

Hide SSID : No

Status : Active

Classification : Authorized

Severity Level : 0

Security : Clear

Encrypt Method : -NA-

Authentication Method : None

Radio Type : 802.11ac

Channel : 36

In Countermeasure List : No

Up Time : 2017-08-09/20:26:46

First Reported Time : 2017-09-03/08:13:50

Last Reported Time : 2017-09-04/09:32:40

Reporting Sensor : 3

Sensor 1 : hcxw030

Mac Address : 60da-83b6-1480

RadioId : 1

RSSI : 8

Last Reported Time : 2017-09-04/09:31:42

Sensor 2 : hcxw117

```
    Mac Address          : 60da-83b6-a420
    RadioId              : 1
    RSSI                 : 35
    Last Reported Time   : 2017-09-04/09:32:33
  Sensor 3               : hcxw149
    Mac Address          : 60da-83b6-3190
    RadioId              : 1
    RSSI                 : 56
    Last Reported Time   : 2017-09-04/09:32:40
 Attached Clients        : 15
  Client 1               : 0c1d-afde-597c
  Client 2               : 145f-94b0-4e71
  Client 3               : 14a5-1a0c-5de9
  Client 4               : 203c-ae55-b4b9
  Client 5               : 28f0-76e0-c616
 Detected Attacks        : -NA-
--------------------------------------------------------------------------------
```

WIPS模块与WIDS模块不能在一台AP上同时运行，功能模块会冲突。即不能在一台AP下同时开启work-mode monitor和wips detect mode

为了保证WIPS模块扫描到的干扰信号信息的时效性，建议修改相应表项的计时器。

在功能一般用在无线wifi信号较多的高密部署场景，AP在做扫描监控时不建议同时作为无线业务接入，同时运行时对无线接入性能影响较大。一般建议在这类场景单独部署一台AP用来做扫描监控。

在配置WIPS允许列表时，需要提前搜集当前已部署的我司无线设备OUI以及可能涉及到的其他厂商OUI或者mac，配置到允许列表，以防止误扫为rogue ap。