目 录

1 WIPS

1.1 WIPS简介

WIPS（Wireless Intrusion Prevention System，无线入侵防御系统）是针对 802.11 协议开发的二层协议检测和防护功能。WIPS 通过对信道进行监听及分析处理，从中检测出威胁网络安全、干扰网络服务、影响网络性能的无线行为或设备，并提供对入侵的无线设备的反制，为无线网络提供一套完整的安全解决方案。

WIPS 由 Sensor 以及网管软件组成。开启 WIPS 功能的 AP 称为 Sensor，Sensor 负责监听无线信道，并将收集的信息进行综合分析。AP 会分析攻击源并对其实施反制，同时向网管软件输出日志信息。网管软件提供丰富的图形界面，提供系统控制、报表输出、告警日志管理功能。

WIPS 支持以下功能：

- 攻击检测：提供多种攻击方式的攻击检测功能。
- 设备分类：通过侦听无线信道的 802.11 报文来识别无线设备，并对其进行分类。
- 反制：对非法设备进行攻击，使其它设备无法关联到非法设备，从而保护用户网络的安全。

1.2 攻击检测

WIPS 通过分析侦听到的 802.11 报文，来检测针对 WLAN 网络的无意或者恶意的攻击，并以告警的方式通知网络管理员。

1.2.1 泛洪攻击检测

泛洪攻击是指通过向无线设备发送大量同类型的报文，使无线设备会被泛洪攻击报文淹没而无法处理合法报文。WIPS 通过持续地监控 AP 或客户端的流量来检测泛洪攻击。当大量同类型的报文超出上限时，认为无线网络正受到泛洪攻击。

目前 WIPS 能够防范的泛洪攻击包括：

1. 鉴权请求帧泛洪攻击

攻击者通过模拟大量的客户端向 AP 发送鉴权请求帧，AP 收到大量攻击报文后无法处理合法客户端的鉴权请求帧。

2. 探查请求/关联/重关联泛洪攻击

攻击者通过模拟大量的客户端向 AP 发送探查请求/关联请求/重关联请求帧，AP 收到大量攻击报文后无法处理合法客户端的探测请求/关联请求/重关联请求帧。

3. EAPOL-Start泛洪攻击

IEEE 802.1X 标准定义了一种基于 EAPOL（EAP over LAN，局域网上的可扩展认证协议）的认证协议，该协议通过客户端发送 EAPOL-Start 帧开始一次认证流程。AP 接收到 EAPOL-Start 后会回复一个 EAP-Identity-Request，并为该客户端分配一些内部资源来记录认证状态。攻击者可以通过模拟大量的客户端向 AP 发送 EAPOL-Start 来耗尽该 AP 的资源，使 AP 无法处理合法客户端的认证请求。

4. 广播/单播解除鉴权泛洪攻击

攻击者通过仿冒 AP 向与其关联的客户端发送广播/单播的解除鉴权帧，使得被攻击的客户端与 AP 的关联断开。这种攻击非常突然且难以防范。单播取消鉴权攻击是针对某一个客户端，而广播取消鉴权攻击是针对与该 AP 关联的所有客户端。

5. 广播/单播解除关联泛洪攻击

攻击原理同广播/单播解除鉴权泛洪攻击。攻击者是通过仿冒 AP 向与其关联的客户端发送广播/单播解除关联帧，使得被攻击的客户端与 AP 的关联断开。这种攻击同样非常突然且难以防范。

6. RTS/CTS泛洪攻击

在无线网络中，通信双方需要遵循虚拟载波侦听机制，通过 RTS（Request to Send，发送请求）/CTS（Clear to Send，清除发送请求）交互过程来预留无线媒介，通信范围内的其它无线设备在收到 RTS 和（或）CTS 后，将根据其中携带的信息来延迟发送数据帧。RTS/CTS 泛洪攻击利用了虚拟载波侦听机制的漏洞，攻击者能通过泛洪发送 RTS 和（或）CTS 来阻塞 WLAN 网络中合法无线设备的通信。

7. Block ACK泛洪攻击

该攻击通过仿冒客户端发送伪造的 Block ACK 帧来影响 Block ACK 机制的正常运行，导致通信双方丢包。

8. Null-Data泛洪攻击

该攻击通过仿冒合法客户端向与其关联的 AP 发送 Null-Data 帧，并且将 Null-Data 帧的节电位置位，使得 AP 误认为合法的客户端进入省电模式，将发往该客户端的数据帧进行暂存。如果攻击者持续发送 Null-Data 帧，当暂存帧的存储时间超过 AP 暂存帧老化时间后，AP 会将暂存帧丢弃，妨害了合法客户端的正常通信。

9. Beacon泛洪攻击

该攻击是通过发送大量的 Beacon 帧使客户端检测到多个虚假 AP，导致客户端选择正常的 AP 进行连接时受阻。

10. EAPOL-Logoff泛洪攻击

在 EAPOL 认证环境中，当通过认证的客户端需要断开连接时，会发送一个 EAPOL-Logoff 帧来关闭与 AP 间的会话。但 AP 对接收到的 EAPOL-Logoff 帧不会进行认证，因此攻击者通过仿冒合法客户端向 AP 发送 EAPOL-Logoff 帧，可以使 AP 关闭与该客户端的连接。如果攻击者持续发送仿冒的 EAPOL-Logoff 帧，将使被攻击的客户端无法保持同 AP 间的连接。

11. EAP-Success/Failure泛洪攻击

在使用 802.1X 认证的 WLAN 环境中，当客户端认证成功时，AP 会向客户端发送一个 EAP-Success 帧（code 字段为 success 的 EAP 帧）；当客户端认证失败时，AP 会向客户端发送一个 EAP-Failure 帧（code 字段为 failure 的 EAP 帧）。攻击者通过仿冒 AP 向请求认证的客户端发送 EAP-Failure 帧或 EAP-Success 帧来破坏该客户端的认证过程，通过持续发送仿冒的 EAP-Failure 帧或 EAP-Success 帧，可以阻止被攻击的客户端与 AP 间的认证。

1.2.2 畸形报文检测

畸形报文攻击是指攻击者向受害客户端发送有缺陷的报文，使得客户端在处理这样的报文时会出现崩溃。WIPS 利用 Sensor 监听无线信道来获取无线报文，通过报文解析检测出具有某些畸形类型特征的畸形报文，并发送告警。

目前支持的畸形报文检测包括：

1. IE长度非法检测

该检测是针对所有管理帧的检测。信息元素（Information Element，简称 IE）是管理帧的组成元件，每种类型的管理帧包含特定的几种 IE。报文解析过程中，当检测到该报文包含的某个 IE 的长度为非法时，该报文被判定为 IE 长度非法的畸形报文。

2. 重复IE检测

该检测是针对所有管理帧的检测。当解析某报文时，该报文所包含的某 IE 重复出现时，则判断该报文为重复 IE 畸形报文。因为厂商自定义 IE 是允许重复的，所以检测 IE 重复时，不检测厂商自定义 IE。

3. 多余IE检测

该检测是针对所有管理帧的检测。报文解析过程中，当检测到既不属于报文应包含的 IE，也不属于 reserved IE 时，判断该 IE 为多余 IE，则该报文被判定为多余 IE 的畸形报文。

4. 报文长度非法检测

该检测是针对所有管理帧的检测。当解析完报文主体后，IE 的剩余长度不等于 0 时，则该报文被判定为报文长度非法的畸形报文。

5. IBSS和ESS置位异常检测

该检测是针对 Beacon 帧和探查响应帧进行的检测。当报文中的 IBSS 和 ESS 都置位为 1 时，由于此种情况在协议中没有定义，所以该报文被判定为 IBSS 和 ESS 置位异常的畸形报文。

6. 畸形Authentication帧检测

该检测是针对认证帧的检测。当检测到以下情况时请求认证过程失败，会被判断为认证畸形报文。

- 当对认证帧的身份认证算法编号（Authentication algorithm number）的值不符合协议规定，并且其值大于 3 时；
- 当标记客户端和 AP 之间的身份认证的进度的 Authentication Transaction Sequence Number 的值等于 1，且状态代码 status code 不为 0 时；
- 当标记客户端和 AP 之间的身份认证的进度的 Authentication Transaction Sequence Number 的值大于 4 时。

7. 畸形Association-Request帧检测

该检测是针对关联请求帧的检测。当收到关联请求帧中的 SSID 的长度等于 0 时，判定该报文为畸形关联请求报文。

8. 畸形的HT IE检测

该检测是针对 Beacon、探查响应帧、关联响应帧、重关联请求帧的检测。当检测到以下情况时，判定为 HT IE 的畸形报文，发出告警，在静默时间内不再告警。

- 解析出 HT Capabilities IE 的 SM Power Save 值为 2 时；

- 解析出 HT Operation IE 的 Secondary Channel Offset 值等于 2 时。

9. Duration超大检测

该检测是针对单播管理帧、单播数据帧以及 RTS、CTS、ACK 帧的检测。如果报文解析结果中该报文的 Duration 值大于指定的门限值，则为 Duration 超大的畸形报文。

10. Null-probe-Response检测

该检测是针对探查响应报文。当检测到该帧为非 Mesh 帧，但同时该帧的 SSID Length 等于 0，这种情况不符合协议（协议规定 SSID Length 等于 0 的情况是 Mesh 帧），则判定为无效探查响应报文。

11. Invalid-Deauth-Code检测

该检测是针对解除认证畸形帧的检测。当解除认证畸形帧携带的 Reason code 的值属于集合[0，67～65535]时，则属于协议中的保留值，此时判定该帧为含有无效原因值的解除认证畸形报文。

12. Invalid-Disassoc-Code检测

该检测是针对解除关联帧的检测。当解除关联帧携带的 Reason code 的值属于集合[0，67～65535]时，则属于协议中的保留值，此时判定该帧为含有无效原因值的解除关联畸形报文。

13. SSID超长检测

该检测是针对 Beacon、探查请求、探查响应、关联请求帧的检测。当解析报文的 SSID length 大于 32 字节时，不符合协议规定的 0～32 字节的范围，则判定该帧为 SSID 超长的畸形报文。

14. Fata-Jack检测

该检测是针对认证帧的检测。Fata-Jack 畸形类型规定，当身份认证算法编号即 Authentication algorithm number 的值等于 2 时，则判定该帧为 Fata-Jack 畸形报文。

15. Invalid-Source-Address检测

该检测是针对所有管理帧的检测。当检测到该帧的 TO DS 等于 1 时，表明该帧为客户端发给 AP 的，如果同时又检测到该帧的源 MAC 地址为广播或组播，则该帧被判定为 Invalid-Source-Address 畸形报文。

16. Overflow-EAPOL-Key检测

该检测是针对 EAPOL-Key 帧的检测。当检测到该帧的 TO DS 等于 1 且其 Key Length 大于 0 时，则判定该帧为 Key 长度超长的 EAPOL 报文。Key length 长度异常的恶意的 EAPOL-Key 帧可能会导致 DOS 攻击。

1.2.3 Spoofing检测

Spoofing 攻击是指攻击者仿冒其他设备，从而威胁无线网络的安全。例如：无线网络中的客户端已经和 AP 关联，并处于正常工作状态，此时如果有攻击者仿冒 AP 的名义给客户端发送解除认证/解除关联报文就可能导致客户端下线，从而达到破坏无线网络正常工作的目的；又或者攻击者仿冒成合法的 AP 来诱使合法的客户端关联，攻击者仿冒成合法的客户端与 AP 关联等，从而可能导致用户账户信息泄露。

目前支持的 Spoofing 检测包括：

1. AP仿冒AP

该仿冒是指攻击者使用 AP 仿冒正常工作的 AP 的 MAC 地址，向客户端发送报文的行为。WIPS 通过报文的接收时间和报文中的时间戳计算出 AP 的启动时间，并与之前记录的该 AP 的启动时间进行比较来判断是否发生仿冒。如果计算出的本次 AP 启动时间早于之前计算出的 AP 启动时间，则判定为发生 AP 仿冒 AP 攻击。

WIPS 通过侦听无线网络内的 Beacon 或探查响应帧报文来检测 AP 仿冒 AP 行为。

2. AP仿冒客户端

该仿冒是指攻击者使用 AP 仿冒合法客户端的 MAC 地址发送报文。WIPS 通过检测 AP 发送的报文中的 MAC 地址是否存在于客户端列表中来判断是否有仿冒发生。如果该 AP 的 MAC 地址存在于客户端列表中，则判定为发生了 AP 仿冒客户端。

3. 客户端仿冒AP

该仿冒是指攻击者使用客户端仿冒合法 AP 的 MAC 地址发送报文。WIPS 通过检测客户端发送的报文中发送端的 MAC 地址是否存在于 AP 列表中来判断是否有仿冒发生。如果该客户端的 MAC 地址存在于 AP 列表中，则判定为发生了客户端仿冒 AP。

1.2.4 Weak IV检测

WEP 安全协议使用的 RC4 加密算法存在一定程度的缺陷，当其所用的 IV 值不安全时会大大增加其密钥被破解的可能性，当 IV 值的第一个字节小于 16（10 进制）且第二个字节为 FF 时，该类 IV 值即被称为 Weak IV。WIPS 特性通过检测每个 WEP 报文的 IV 值来预防这种攻击。

1.2.5 Omerta检测

Omerta 是一个基于 802.11 协议的 DoS 攻击工具，它通过向信道上所有发送数据帧的客户端回应解除关联帧，使客户端中断与 AP 的关联。Omerta 发送的解除关联帧中的原因代码字段为 0x01，表示未指定。由于正常情况下不会出现此类解除关联帧，因此 WIPS 可以通过检测每个解除关联帧的原因代码字段来检测这种攻击。

1.2.6 广播解除关联帧/解除认证帧攻击检测

当攻击者仿冒成合法的 AP，发送目的 MAC 地址为广播地址的解除关联帧或者解除认证帧时，会使合法 AP 下关联的客户端下线，对无线网络造成攻击。

1.2.7 客户端禁用 802.11n 40MHz检测

支持 802.11n 标准无线设备可以支持 20MHz 和 40MHz 两种带宽模式。在无线环境中，如果与 AP 关联的某个无线客户端禁用了 40MHz 带宽模式，会导致 AP 与该 AP 关联的其它无线客户端也降低无线通信带宽到 20MHz，从而影响到整个网络的通信能力。WIPS 通过检测无线客户端发送的探测请求帧来发现禁用 40MHz 带宽模式的无线客户端。

1.2.8 节电攻击检测

对于处于非节电模式下的无线客户端，攻击者可以通过发送节电模式开启报文（Null 帧），诱使 AP 相信与其关联的无线客户端始终处于睡眠状态，并为该无线客户端暂存帧。被攻击的无线客户端因

为处于非节电模式而无法获取这些暂存帧，在一定的时间之后暂存帧会被自动丢弃。WIPS 通过检测节电模式开启/关闭报文的比例判断是否存在节电攻击。

1.2.9 非法信道检测

用户可以设置合法信道集合，并开启非法信道检测，如果 WIPS 在合法信道集合之外的其它信道上监听到无线通信，则认为在监听到无线通信的信道上存在入侵行为。

1.2.10 软AP检测

软 AP 是指客户端上的无线网卡在应用软件的控制下对外提供 AP 的功能。攻击者可以利用这些软 AP 所在的客户端接入公司网络，并发起网络攻击。WIPS 通过检测某个 MAC 地址在无线客户端和 AP 这两个角色上的持续活跃时长来判断其是否是软 AP，不对游离的无线客户端进行软 AP 检测。

1.2.11 Windows网桥检测

当一个连接到有线网络的无线客户端使用有线网卡建立了 Windows 网桥时，该无线客户端就可以通过连接外部 AP 将外部 AP 与内部有线网络进行桥接。此组网方式会使外部 AP 对内部的有线网络造成威胁。WIPS 会对已关联的无线客户端发出的数据帧进行分析，来判断其是否存在于 Windows 网桥中。

1.2.12 未加密设备检测

在无线网络中，如果有授权 AP 或信任的无线客户端使用的配置是未加密的，网络攻击者很容易通过监听来获取无线网络中的数据，从而导致网络信息泄露。WIPS 会对信任的无线客户端或授权 AP 发出的管理帧或数据帧进行分析，来判断其是否使用了加密配置。

1.2.13 热点攻击检测

热点攻击指恶意 AP 使用热点 SSID 来吸引周围的无线客户端来关联自己。攻击者通过伪装成公共热点来引诱这些无线客户端关联自己。一旦无线客户端与恶意 AP 关联上，攻击者就会发起一系列的安全攻击，获取用户的信息。用户通过在 WIPS 中配置热点文件，来指定 WIPS 对使用这些热点的 AP 和信任的无线客户端进行热点攻击检测。

1.2.14 AP扮演者攻击检测

在 AP 扮演者攻击中，攻击者会安装一台恶意 AP 设备，该 AP 设备的 BSSID 和 ESSID 与真实 AP 一样。当该恶意 AP 设备在无线环境中成功扮演了真实 AP 的身份后，就可以发起热点攻击，或欺骗检测系统。WIPS 通过检测收到 Beacon 帧的间隔是否小于 Beacon 帧中携带的间隔值来判断其是否为攻击者扮演的恶意 AP。

1.2.15 绿野模式检测

当无线设备使用 802.11n 绿野模式时，不可以和其他 802.11a/b/g 设备共享同一个信道。通常当一台设备侦听到有其他设备占用信道发送和接收报文的时候，会延迟报文的发送直到信道空闲时再发

送。但是 802.11a/b/g 设备不能和绿野模式的 AP 进行通信，无法被告知绿野模式的 AP 当前信道是否空闲，会立刻发送自己的报文。这可能会导致报文发送冲突、差错和重传。

1.2.16 蜜罐AP检测

攻击者在合法 AP 附近搭建一个蜜罐 AP，通过该 AP 发送与合法 AP SSID 相似的 Beacon 帧或 Probe Response 帧，蜜罐 AP 的发送信号可能被调得很大以诱使某些授权客户端与之关联。当有客户端连接到蜜罐 AP，蜜罐 AP 便可以向客户端发起某些安全攻击，如端口扫描或推送虚假的认证页面来骗取客户端的用户名及密码信息等。因此，需要检测无线环境中对合法设备构成威胁的蜜罐 AP。WIPS 系统通过对外部 AP 使用的 SSID 进行分析，若与合法 SSID 的相似度值达到一定阈值就发送蜜罐 AP 告警。

1.2.17 中间人攻击检测

在中间人攻击中，攻击者在合法 AP 和合法客户端的数据通路中间架设自己的设备，并引诱合法客户端下线并关联到攻击者的设备上，此时攻击者就可以劫持合法客户端和合法 AP 之间的会话。在这种情况下，攻击者可以删除，添加或者修改数据包内的信息，获取验证密钥、用户密码等机密信息。中间人攻击是一种组合攻击，客户端在关联到蜜罐 AP 后攻击者才会发起中间人攻击，所以在配置中间人攻击检测之前需要开启蜜罐 AP 检测。

1.2.18 无线网桥检测

攻击者可以通过接入无线网桥侵入公司网络的内部，对网络安全造成隐患。WIPS 通过检测无线网络环境中是否存在无线网桥数据以确定周围环境中是否存在无线网桥。当检测到无线网桥时，WIPS 系统即产生告警，提示当前无线网络环境存在安全隐患。如果该无线网桥是 Mesh 网络时，则记录该 Mesh 链路。

1.2.19 关联/重关联DoS攻击检测

关联/重关联 DoS 攻击通过模拟大量的客户端向 AP 发送关联请求/重关联请求帧，使 AP 的关联列表中存在大量虚假的客户端，达到拒绝合法客户端接入的目的。

1.2.20 AP泛洪攻击检测

AP 设备在完成部署后通常是固定不动的，正常情况下 WIPS 通过检测发现网络环境中的 AP 设备的数目达到稳定后不会大量增加。当检测到 AP 的数目超出预期的数量时， WIPS 系统即产生告警，提示当前无线网络环境存在安全隐患。

1.2.21 WIPS学习表项的攻击检测

如果攻击者通过发送大量报文来增加 WIPS 的处理开销等。通过检测周期内学习到设备的表项来判断是否需要对表项学习进行限速处理。设备在统计周期内学习到的 AP 或客户端表项达到触发告警阈值，设备会发送告警信息，并停止学习 AP 表项和客户端表项。

1.2.22 Signature检测

Signature 检测是指用户可以根据实际的网络状况来配置 Signature 规则，并通过该规则来实现自定义攻击行为的检测。WIPS 利用 Sensor 监听无线信道来获取无线报文，通过报文解析，检测出具有某些自定义类型特征的报文，并将分析检测的结果进行归类处理。

每个 Signature 检测规则中最多支持配置 6 条子规则，分别对报文的 6 种特征进行定义和匹配。当 AC 解析报文时，如果发现报文的特征能够与已配置的子规则全部匹配，则认为该报文匹配该自定义检测规则，AC 将发送告警信息或记录日志。

可以通过子规则定义的 6 种报文特征包括：

- 帧类型；
- MAC 地址；
- 序列号；
- SSID 长度；
- SSID；
- 报文中指定位置的字段取值。

1.3 设备分类

1.3.1 AP的分类类别

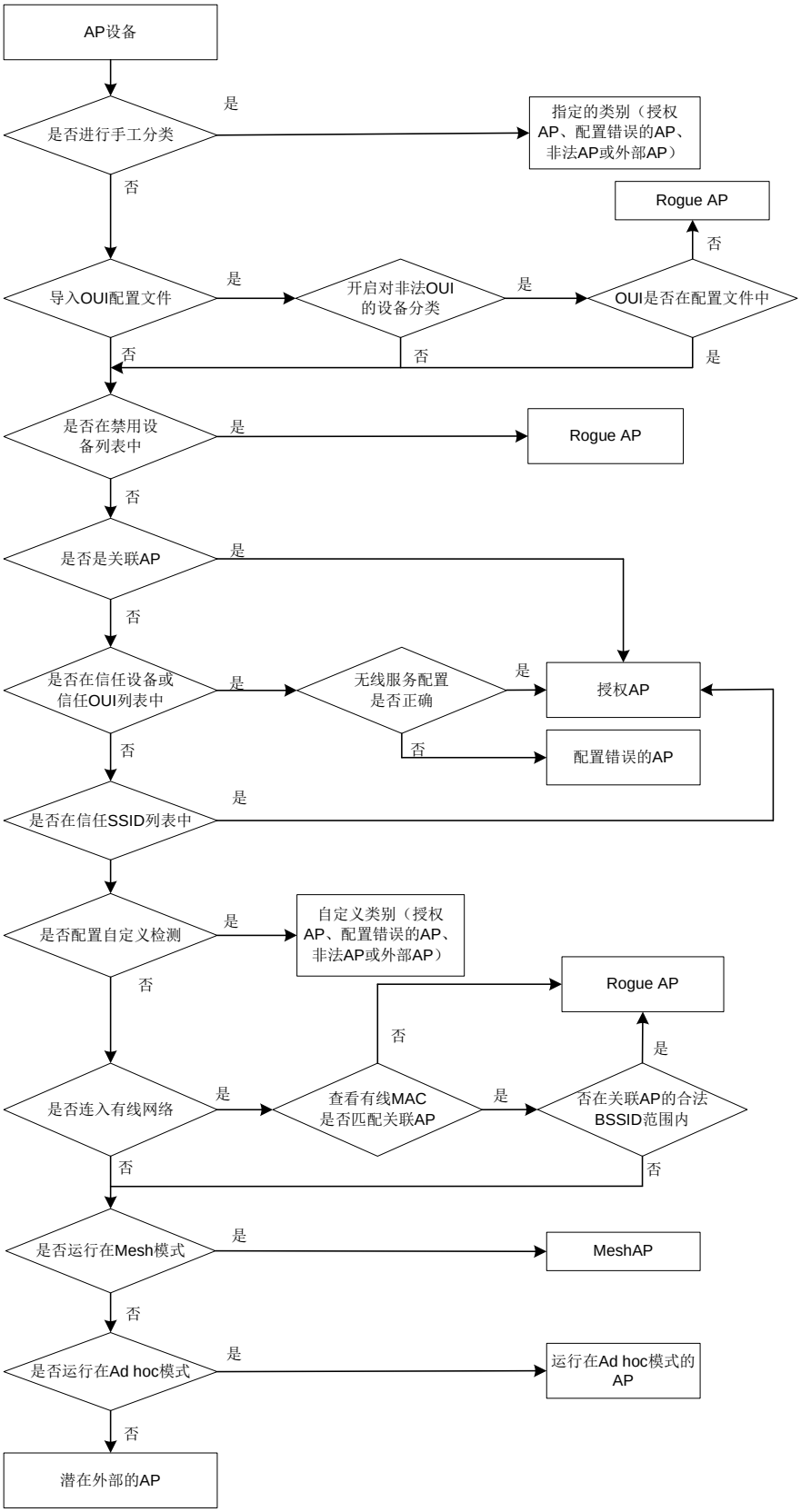
WIPS 将检测到的 AP 分为以下几类：

- 授权 AP（Authorized AP）：允许在无线网络中使用的 AP。包括已经关联到 AC 上且不在禁用列表中的 AP、手动指定的授权 AP、添加到信任列表中的 AP 和通过自定义规则分类的授权 AP；
- 非法 AP（Rouge AP）：不允许在无线网络中使用的 AP。包括禁用设备列表中的 AP、不在 OUI 配置文件中的 AP、手动指定的非法 AP 和通过自定义规则分类的非法 AP。有线接入但是未关联的 AP 有可能是非法 AP；
- 配置错误的 AP（Misconfigured AP）：无线服务配置错误，但是允许在无线网络中使用的 AP。包括手动指定的配置错误的 AP 和通过自定义规则分类的配置错误的 AP；
- 外部 AP（External AP）：其他无线网络中的 AP。WIPS 可能会检测到邻近网络中的 AP，例如邻近公司或个人住宅中的 AP。目前仅支持手工指定的外部 AP 和通过自定义规则分类的外部 AP；
- Ad hoc：运行在 Ad hoc 模式的 AP。WIPS 通过检测 Beacon 帧将其分类为 Ad hoc；
- Mesh：运行在 Mesh 模式的 AP。WIPS 通过检测 Beacon 帧将其分类为 Mesh；
- 潜在授权的 AP（Potential-authorized AP）：无法确定但可能是授权的 AP。如果 AP 既不在信任设备、信任 OUI 列表、信任 SSID 列表和禁用设备列表中，也不是未关联 AP，并且未对其进行手工分类和符合自定义规则分类，那么该 AP 很可能是授权的 AP，如 Remote AP；
- 潜在非法的 AP（Potential-rogue AP）：无法确定但可能是非法的 AP。如果 AP 既不在信任设备或信任 OUI 列表中也不在禁用设备列表中，而且它的无线服务配置也不正确，那么，如果检测到它的有线端口可能连接到网络中，则认为其为潜在非法的 AP；如果能确定其有线端口连接到网络中，则认为其为非法 AP，如恶意入侵者私自接入网络的 AP；

- 潜在外部的 AP（Potential-external AP）：无法确定但可能是外部的 AP。如果 AP 既不在信任设备或信任 OUI 列表中也不在禁用设备列表中，而且它的无线服务配置也不正确，同时也没有检测到它的有线端口连接到网络中，则该 AP 很可能是外部的 AP；
- 未分类 AP（Uncategorized AP）：无法确定归属类别的 AP。

WIPS对检测到的AP的分类处理流程如 图 1-1 所示：

图1-1 WIPS 对检测到的 AP 设备的分类处理流程示意图



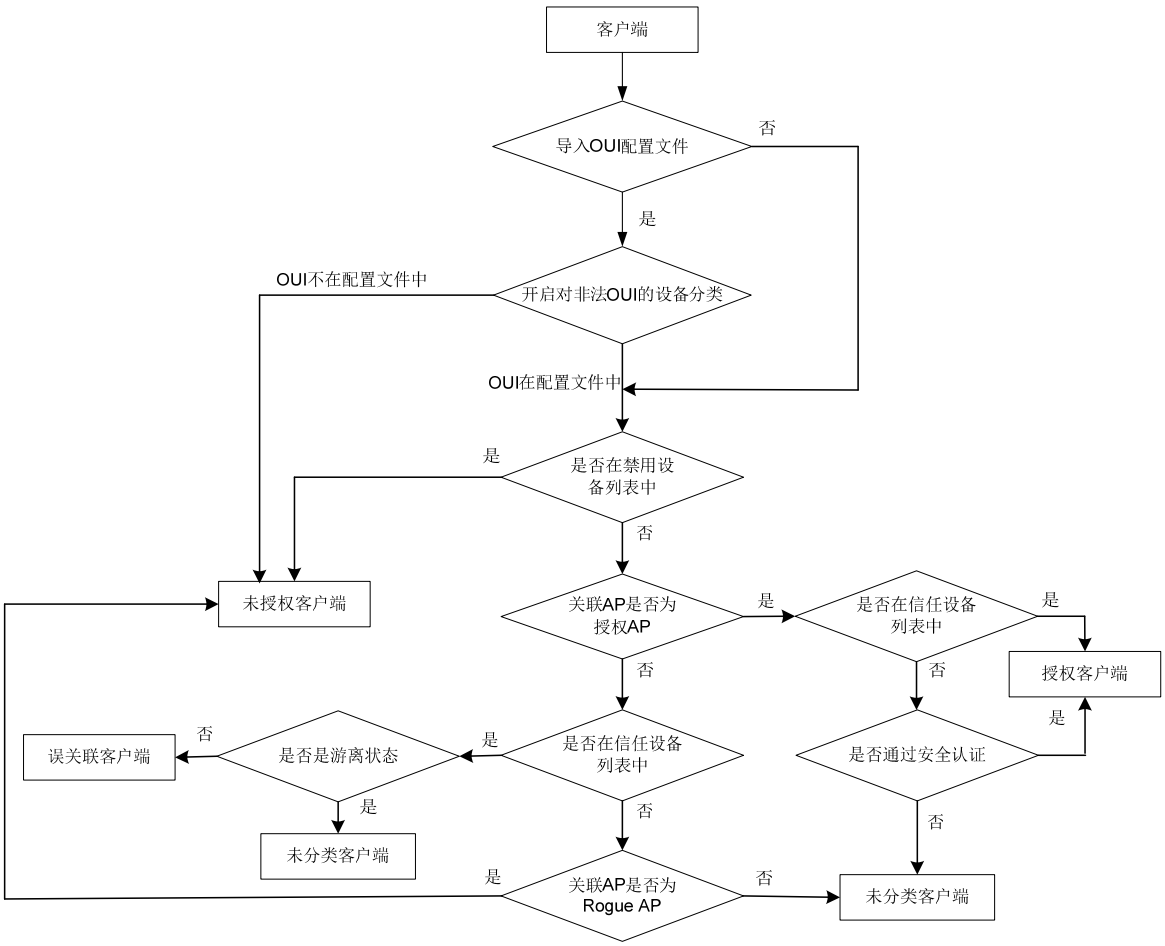
1.3.2 客户端的分类类别

WIPS 将检测到的客户端分为以下几类：

- 授权客户端（Authorized Client）：允许使用的客户端，如关联到授权 AP 上的受信任的客户端或通过加密认证方式关联到授权 AP 上的客户端都是授权的客户端；
- 未授权客户端（Unauthorized Client）：不允许使用的客户端。如在禁用设备列表中的客户端、连接到 Rogue AP 上的客户端以及不在 OUI 配置文件中的客户端都是未授权客户端；
- 错误关联客户端（Misassociation Client）：信任设备列表中的客户端关联到非授权 AP 上。错误关联的客户端可能会对网络信息安全带来隐患；
- 未分类客户端（Uncategorized Client）：无法确定归属类别的客户端。

WIPS对检测到的客户端的分类处理流程如 图 1-2 所示：

图1-2 WIPS 对检测到的客户端的分类处理流程示意图



1.4 反制

在无线网络中设备分为两种类型：非法设备和合法设备。非法设备可能存在安全漏洞或被攻击者操纵，因此会对用户网络的安全造成严重威胁或危害。反制功能可以对这些设备进行攻击使其他无线终端无法关联到非法设备。

1.5 WIPS配置任务简介

表1-1 WIPS 配置任务简介

配置任务		说明	详细配置
开启WIPS功能		必选	1.6
配置攻击检测	配置泛洪攻击检测	各类型的攻击检测之间没有先后顺序，可根据实际组网需求，配置其中的一种或多种	1.7.1
	配置畸形报文检测		1.7.2
	配置攻击检测策略		1.7.3
	配置WIPS学习表项的攻击检测		1.7.4
	应用攻击检测策略		1.7.5
	配置Signature规则		1.7.6
	应用Signature规则		1.7.7
	应用Signature策略		1.7.8
	配置忽略告警信息的MAC地址列表		1.7.9
配置设备分类	配置分类策略	根据实际组网需求进行配置	1.8.1
	应用分类策略		1.8.2
配置反制	配置反制策略	根据实际组网需求进行配置	1.9.1
	应用反制策略		1.9.2

1.6 配置WIPS功能

WLAN 网络在组网过程中可以根据职能不同在逻辑上划分成多个区域，每个区域对接入服务的安全性、安全级别、无线设备的无线行为要求不同，我们称这些不同的区域为 VSD（Virtual Security Domain，虚拟安全域），用户可以对无线接入网络的各个 VSD 采用不同的安全检测策略。开启 WIPS 功能前，需要将 AP 加入到指定 VSD 中。

表1-2 配置 WIPS 功能

操作	命令	说明
进入系统视图	**system-view**	-
将AP加入到指定的VSD中	**wips virtual-security-domain** *vsd-name*	缺省情况下，没有将AP加入到指定的VSD中
退出VSD视图	**quit**	-
进入Radio接口视图	**interface wlan-radio** *interface-number*	-
配置WIPS功能	**wips enable**	缺省情况下，WIPS功能处于关闭状态

1.7 配置攻击检测

创建一个攻击检测策略，定义一个或多个用于攻击检测的特征项。

1.7.1 配置泛洪攻击检测

表1-3 配置泛洪攻击检测

操作	命令	说明
进入系统视图	**system-view**	-
进入WIPS视图	**wips**	缺省情况下，没有配置WIPS视图
创建攻击检测策略，并进入攻击检测策略视图	**detect policy** *policy-name*	缺省情况下，不存在攻击检测策略
配置关联请求帧泛洪攻击检测功能	**flood association-request** [**interval** *interval-value* | **quiet** *quiet-value* | **threshold** *threshold-value*] *	缺省情况下，关联请求帧泛洪攻击检测功能处于关闭状态
配置认证请求帧泛洪攻击检测功能	**flood authentication** [**interval** *interval-value* | **quiet** *quiet-value* | **threshold** *threshold-value*] *	缺省情况下，认证请求帧泛洪攻击检测功能处于关闭状态
配置Beacon帧泛洪攻击检测功能	**flood beacon** [**interval** *interval-value* | **quiet** *quiet-value* | **threshold** *threshold-value*] *	缺省情况下，Beacon帧泛洪攻击检测功能处于关闭状态
配置Block ACK帧泛洪攻击检测功能	**flood block-ack** [**interval** *interval-value* | **quiet** *quiet-value* | **threshold** *threshold-value*] *	缺省情况下，Block ACK帧泛洪攻击检测功能处于关闭状态
配置RTS帧泛洪攻击检测功能	**flood rts** [**interval** *interval-value* | **quiet** *quiet-value* | **threshold** *threshold-value*] *	缺省情况下，RTS帧泛洪攻击检测功能处于关闭状态
配置CTS帧泛洪攻击检测功能	**flood cts** [**interval** *interval-value* | **quiet** *quiet-value* | **threshold** *threshold-value*] *	缺省情况下，CTS帧泛洪攻击检测功能处于关闭状态
配置解除认证帧泛洪攻击检测功能	**flood deauthentication** [**interval** *interval-value* | **quiet** *quiet-value* | **threshold** *threshold-value*] *	缺省情况下，解除认证帧泛洪攻击检测功能处于关闭状态
配置解除关联帧泛洪攻击检测功能	**flood disassociation** [**interval** *interval-value* | **quiet** *quiet-value* | **threshold** *threshold-value*] *	缺省情况下，解除关联帧泛洪攻击检测功能处于关闭状态
配置EAPOL-Start帧泛洪攻击检测功能	**flood eapol-start** [**interval** *interval-value* | **quiet** *quiet-value* | **threshold** *threshold-value*] *	缺省情况下，EAPOL-Start帧泛洪攻击检测功能处于关闭状态
配置Null-Data帧泛洪攻击检测功能	**flood null-data** [**interval** *interval-value* | **quiet** *quiet-value* | **threshold** *threshold-value*] *	缺省情况下，Null-Data帧泛洪攻击检测功能处于关闭状态
配置探查请求帧泛洪攻击检测功能	**flood probe-request** [**interval** *interval-value* | **quiet** *quiet-value* | **threshold** *threshold-value*] *	缺省情况下，探查请求帧泛洪攻击检测功能处于关闭状态
配置重关联帧泛洪攻击检测功能	**flood reassociation-request** [**interval** *interval-value* | **quiet** *quiet-value* | **threshold** *threshold-value*] *	缺省情况下，重关联帧泛洪攻击检测功能处于关闭状态

操作	命令	说明
配置EAPOL-Logoff帧泛洪攻击检测功能	**flood eapol-logoff** [**interval** *interval-value* | **quiet** *quiet-value* | **threshold** *threshold-value*] *	缺省情况下，EAPOL-Logoff帧泛洪攻击检测功能处于关闭状态
配置EAP-Failure帧泛洪攻击检测功能	**flood eap-failure** [**interval** *interval-value* | **quiet** *quiet-value* | **threshold** *threshold-value*] *	缺省情况下，EAP-Failure帧泛洪攻击检测功能处于关闭状态
配置EAP-Success帧泛洪攻击检测功能	**flood eap-success** [**interval** *interval-value* | **quiet** *quiet-value* | **threshold** *threshold-value*] *	缺省情况下，EAP-Success帧泛洪攻击检测功能处于关闭状态

1.7.2 配置畸形报文检测

表1-4 配置畸形报文检测

操作	命令	说明
进入系统视图	**system-view**	-
进入WIPS视图	**wips**	-
创建攻击检测策略，并进入攻击检测策略视图	**detect policy** *policy-name*	缺省情况下，不存在攻击检测策略
配置IE重复的畸形报文检测功能	**malformed duplicated-ie** [**quiet** *quiet-value*]	缺省情况下，IE重复的畸形报文检测功能处于关闭状态
配置Fata-Jack畸形报文检测功能	**malformed fata-jack** [**quiet** *quiet-value*]	缺省情况下，Fata-Jack畸形报文检测功能处于关闭状态
配置IBSS和ESS置位异常的畸形报文检测功能	**malformed illegal-ibss-ess** [**quiet** *quiet-value*]	缺省情况下，IBSS和ESS置位异常的畸形报文检测功能处于关闭状态
配置源地址为广播或者组播的认证和关联畸形报文检测功能	**malformed invalid-address-combination** [**quiet** *quiet-value*]	缺省情况下，源地址为广播或者组播的认证和关联畸形报文检测功能处于关闭状态
配置畸形关联请求报文检测功能	**malformed invalid-assoc-req** [**quiet** *quiet-value*]	缺省情况下，畸形关联请求报文检测功能处于关闭状态
配置畸形认证请求报文检测功能	**malformed invalid-auth** [**quiet** *quiet-value*]	缺省情况下，畸形认证请求报文检测功能处于关闭状态
配置含有无效原因值的解除认证畸形报文检测功能	**malformed invalid-deauth-code** [**quiet** *quiet-value*]	缺省情况下，含有无效原因值的解除认证畸形报文检测功能处于关闭状态
配置含有无效原因值的解除关联畸形报文检测功能	**malformed invalid-disassoc-code** [**quiet** *quiet-value*]	缺省情况下，含有无效原因值的解除关联畸形报文检测功能处于关闭状态
配置IE长度非法的畸形报文检测功能	**malformed invalid-ie-length** [**quiet** *quiet-value*]	缺省情况下，IE长度非法的畸形报文检测功能处于关闭状态
配置畸形HT IE报文检测功能	**malformed invalid-ht-ie** [**quiet** *quiet-value*]	缺省情况下，畸形HT IE报文检测功能处于关闭状态

操作	命令	说明
配置报文长度非法的畸形报文检测功能	**malformed invalid-pkt-length** [**quiet** *quiet-value*]	缺省情况下，报文长度非法的畸形报文检测功能处于关闭状态
配置Duration字段超大的畸形报文检测功能	**malformed large-duration** [**quiet** *quiet-value* | **threshold** *value*]	缺省情况下，Duration字段超大的畸形报文检测功能处于关闭状态
配置无效探查响应报文检测功能	**malformed null-probe-resp** [**quiet** *quiet-value*]	缺省情况下，无效探查响应报文检测功能处于关闭状态
配置key长度超长的EAPOL报文检测功能	**malformed overflow-eapol-key** [**quiet** *quiet-value*]	缺省情况下，key长度超长的EAPOL报文检测功能处于关闭状态
配置SSID长度超长的畸形报文检测功能	**malformed overflow-ssid** [**quiet** *quiet-value*]	缺省情况下，SSID长度超长的畸形报文检测功能处于关闭状态
配置多余IE畸形报文检测功能	**malformed redundant-ie** [**quiet** *quiet-value*]	缺省情况下，多余IE畸形报文检测功能处于关闭状态

1.7.3 配置攻击检测策略

表1-5 配置攻击检测策略

操作	命令	说明
进入系统视图	**system-view**	-
进入WIPS视图	**wips**	-
创建攻击检测策略，并进入攻击检测策略视图	**detect policy** *policy-name*	缺省情况下，不存在攻击检测策略
配置客户端地址仿冒检测功能	**client-spoofing** [**quiet** *quiet-value*]	缺省情况下，客户端地址仿冒检测功能处于关闭状态
配置AP地址仿冒检测功能	**ap-spoofing** [**quiet** *quiet-value*]	缺省情况下，AP地址仿冒检测功能处于关闭状态
配置Weak IV检测功能	**weak-iv** [**quiet** *quiet-value*]	缺省情况下，Weak IV检测功能处于关闭状态
配置Omerta攻击检测功能	**omerta** [**quiet** *quiet-value*]	缺省情况下，Omerta攻击检测功能处于关闭状态
配置广播解除关联帧检测功能	**disassociation-broadcast** [**interval** *interval-value* | **quiet** *quiet-value* | **threshold** *threshold-value*] *	缺省情况下，广播解除关联帧检测功能处于关闭状态
配置广播解除认证帧检测功能	**deauthentication-broadcast** [**interval** *interval-value* | **quiet** *quiet-value* | **threshold** *threshold-value*] *	缺省情况下，广播解除认证帧检测功能处于关闭状态
配置客户端是否开启了禁用802.11n 40MHz模式检测功能	**ht-40mhz-intolerance** [**quiet** *quiet-value*]	缺省情况下，客户端是否开启了禁用802.11n 40MHz模式检测功能处于关闭状态
配置节电攻击检测功能	**power-save** [**interval** *interval-value* | **minoffpacket** *packet-value* **| onoffpercent** *percent-value* **| quiet** *quiet-value*] *	缺省情况下，节电攻击检测功能处于关闭状态

操作	命令	说明
配置合法信道集	**permit-channel** *channel-id-list*	缺省情况下，未配置合法信道集
配置非法信道检测功能	**prohibited-channel** [**quiet** *quiet-value*]	缺省情况下，非法信道检测功能处于关闭状态
配置Windows网桥检测功能	**windows-bridge** [**quiet** *quiet-value*]	缺省情况下，Windows网桥检测功能处于关闭状态
配置未加密授权AP检测功能	**unencrypted-authorized-ap** [**quiet** *quiet-value*]	缺省情况下，未加密授权AP检测功能处于关闭状态
配置未加密信任客户端检测功能	**unencrypted-trust-client** [**quiet** *quiet-value*]	缺省情况下，未加密的信任客户端检测功能处于关闭状态
配置软AP检测功能	**soft-ap** [**convert-time** *time-value*]	缺省情况下，软AP检测功能处于关闭状态
配置AP扮演者攻击检测功能	**ap-impersonation** [**quiet** *quiet-value*]	缺省情况下，AP扮演者攻击检测功能处于关闭状态
配置绿野模式检测功能	**ht-greenfield** [**quiet** *quiet-value*]	缺省情况下，绿野模式检测功能处于关闭状态
配置关联/重关联DoS攻击检测功能	**association-table-overflow** [**quiet** *quiet-value*]	缺省情况下，关联/重关联DoS攻击检测功能处于关闭状态
配置无线网桥检测功能	**wireless-bridge** [**quiet** *quiet-value*]	缺省情况下，无线网桥检测功能处于关闭状态
配置AP泛洪攻击检测功能	**ap-flood** [**apnum** *apnum-value* | **exceed** *exceed-value* | **quiet** *quiet-value*] *	缺省情况下，AP泛洪攻击检测功能处于关闭状态
配置蜜罐AP检测功能	**honeypot-ap** [**similarity** *similarity-value* | **quiet** *quiet-value*] *	缺省情况下，蜜罐AP检测功能处于关闭状态
配置中间人攻击检测功能	**man-in-the-middle** [**quiet** *quiet-value*]	缺省情况下，中间人攻击检测功能处于关闭状态
配置AP信道变化检测功能	**ap-channel-change** [**quiet** *quiet-value*]	缺省情况下，AP信道变化检测功能处于关闭状态
退出到WIPS视图	**quit**	-
导入热点信息的配置文件	**import hotspot** *file-name*	缺省情况下，未导入热点信息的配置文件
创建攻击检测策略，并进入攻击检测策略视图	**detect policy** *policy-name*	缺省情况下，不存在攻击检测策略
配置热点攻击检测功能	**hotspot-attack** [**quiet** *quiet-value*]	缺省情况下，热点攻击检测功能处于关闭状态

1.7.4 配置WIPS学习表项的攻击检测

当 WIPS 检测到某个无线设备在设定的时间内没有收发报文，则会将该无线设备的状态从 active 切换到 inactive，这段时间即为非活跃时间。如果该无线设备在设定的老化时间内没有收发报文，则会删除该无线设备的表项。

表1-6 配置 WIPS 学习表项的攻击检测

操作	命令	说明
进入系统视图	**system-view**	-
进入WIPS视图	**wips**	-
创建攻击检测策略，并进入攻击检测策略视图	**detect policy** *policy-name*	缺省情况下，不存在攻击检测策略
配置客户端表项学习的速率	**client-rate-limit** [**interval** *interval-value* | **quiet** *quiet-value* | **threshold** *threshold-value*] *	缺省情况下，学习客户端表项的统计周期为60秒，发送告警信息后的静默时间为1200秒，客户端表项的阈值为512
配置客户端表项的时间参数	**client-timer inactive** *inactive-value* **aging** *aging-value*	缺省情况下，客户端表项的非活跃时间为300秒，老化时间为600秒
配置AP表项学习的速率	**ap-rate-limit** [**interval** *interval-value* | **quiet** *quiet-value* | **threshold** *threshold-value*] *	缺省情况下，学习AP表项的统计周期为60秒，发送告警信息后的静默时间为1200秒，AP表项的阈值为64
配置AP表项的时间参数	**ap-timer inactive** *inactive-value* **aging** *aging-value*	缺省情况下，AP表项的非活跃时间为300秒，老化时间为600秒

1.7.5 应用攻击检测策略

通过在虚拟安全域上应用攻击检测策略，使已配置的攻击检测策略在虚拟安全域内的Radio上生效。

表1-7 应用攻击检测策略

操作	命令	说明
进入系统视图	**system-view**	-
进入WIPS视图	**wips**	-
创建VSD，并进入VSD视图	**virtual-security-domain** *vsd-name*	缺省情况下，不存在VSD
在VSD上应用攻击检测策略	**apply detect policy** *policy-name*	缺省情况下，没有在VSD上应用攻击检测策略

1.7.6 配置Signature规则

在配置 Signature 检测时，首先要创建一个 Signature 规则，并进入 Signature 规则视图。在该视图下，可以定义一条或多条用于 Signature 检测的子规则。

当配置了多个Signature检测规则时，设备会根据Signature检测规则的ID编号由小到大依次匹配，匹配上一条 Signature 检测规则后，将不再继续匹配其它 Signature 检测规则。

表1-8 配置 Signature 规则

操作	命令	说明
进入系统视图	**system-view**	-

操作	命令	说明
进入WIPS视图	**wips**	-
创建Signature规则，并进入Signature规则视图	**signature rule** *rule-id*	缺省情况下，不存在Signature规则
配置Signature规则中匹配帧类型的子规则	**frame-type** { **control** | **data** | **management** [**frame-subtype** { **association-request** | **association-response** | **authentication** | **beacon** | **deauthentication** | **disassociation** | **probe-request** }] }	缺省情况下，未配置Signature规则中匹配帧类型的子规则
配置Signature规则中匹配报文中携带的MAC地址的子规则	**mac-address** { **bssid** | **destination** | **source** } *mac-address*	缺省情况下，未配置Signature规则中匹配报文中携带的MAC地址的子规则
配置Signature规则中匹配序列号的子规则	**seq-number** *seq-value1* [**to** *seq-value2*]	缺省情况下，未配置Signature规则中匹配序列号的子规则
配置Signature规则中匹配SSID长度的子规则	**ssid-length** *length-value1* [**to** *length-value2*]	缺省情况下，未配置Signature规则中匹配SSID长度的子规则
配置Signature规则中匹配SSID的子规则	**ssid** [**case-sensitive**] [**not**] { **equal** | **include** } *string*	缺省情况下，未配置Signature规则中匹配SSID的子规则
配置Signature规则中匹配报文中指定位置的字段的子规则	**pattern** *pattern-number* **offset** *offset-value* **mask** *hex-value value1* [**to** *value2*] [**from-payload**]	缺省情况下，未配置Signature规则中匹配报文中指定位置的字段的子规则

1.7.7 应用Signature规则

通过在 Signature 策略上应用 Signature 规则，使已配置的 Signature 规则在 Signature 策略内生效。

表1-9 应用 Signature 规则

操作	命令	说明
进入系统视图	**system-view**	-
进入WIPS视图	**wips**	-
创建Signature策略，并进入Signature策略视图	**signature policy** *policy-name*	缺省情况下，不存在Signature策略
应用Signature规则	**apply signature rule** *rule-id*	缺省情况下，Signature策略中没有应用Signature规则
配置对符合Signature规则的报文检测功能	**detect signature** [**interval** *interval-value* | **quiet** *quiet-value* | **threshold** *threshold-value*] *	缺省情况下，对符合Signature规则的报文检测功能处于开启状态，统计周期为60秒，发送告警日志后的静默时间为600秒，触发告警阈值为50

1.7.8 应用Signature策略

通过在虚拟安全域上应用 Signature 策略，使已配置的 Signature 策略在虚拟安全域内的 Radio 上生效。

表1-10 应用 Signature 策略

操作	命令	说明
进入系统视图	**system-view**	-
进入WIPS视图	**wips**	-
创建VSD，并进入VSD视图	**virtual-security-domain** *vsd-name*	缺省情况下，不存在VSD
在VSD上应用Signature策略	**apply signature policy** *policy-name*	缺省情况下，VSD内没有应用Signature策略

1.7.9 配置忽略告警信息的MAC地址列表

对于可以忽略 WIPS 告警信息的设备列表中的无线设备，WIPS 仍然会对其做正常的监测，但是不会产生与该设备相关的任何 WIPS 告警信息。

表1-11 配置忽略列表

操作	命令	说明
进入系统视图	**system-view**	-
进入WIPS视图	**wips**	-
配置忽略WIPS告警信息的设备列表	**ignorelist mac-address** *mac-address*	缺省情况下，未配置忽略WIPS告警信息的设备列表

1.8 配置设备分类

创建一个分类策略，对设备进行分类。

1.8.1 配置分类策略

可以通过两种配置方式实现设备分类，其中手工分类的优先级高于自动分类。

- 自动分类：通过信任设备列表、信任 OUI 列表和静态禁用设备列表对所有设备进行分类；或通过自定义的 AP 分类规则对 AP 设备进行分类。
- 手工分类：通过手动指定 AP 的类型对设备进行分类。

具体分类处理流程请参见 图 1-1 和 图 1-2。

1. 配置自动分类

表1-12 配置分类策略（自动分类）

操作	命令	说明
进入系统视图	**system-view**	-
进入WIPS视图	**wips**	-
指定导入配置文件中的OUI信息	**import oui** *file-name*	缺省情况下，未导入配置文件的OUI信息
创建分类策略，并进入分类策略视图	**classification policy** *policy-name*	缺省情况下，没有创建分类策略
配置对非法OUI的设备进行分类	**invalid-oui-classify illegal**	缺省情况下，不对非法OUI的设备进行分类
将指定的MAC地址添加到信任设备列表中	**trust mac-address** *mac-address*	缺省情况下，信任设备列表中不存在MAC地址
将指定的OUI添加到信任OUI列表中	**trust oui** *oui*	缺省情况下，信任OUI列表中不存在OUI 该命令只能对AP进行分类
将指定的SSID添加到信任设备列表中	**trust ssid** *ssid-name*	缺省情况下，信任设备列表中不存在SSID
将指定的MAC地址添加到静态禁用设备列表中	**block mac-address** *mac-address*	缺省情况下，静态禁用设备列表中不存在MAC地址
在设备分类策略上应用AP分类规则	**apply ap-classification rule** *rule-id* { **authorized-ap** | { { **external-ap** | **misconfigured-ap** | **rogue-ap** } [**severity-level** *level*] } }	缺省情况下，分类策略中没有应用AP分类规则

表1-13 配置 AP 分类规则

操作	命令	说明
进入系统视图	**system-view**	-
进入WIPS视图	**wips**	-
创建AP分类规则，并进入AP分类规则视图	**ap-classification rule** *rule-id*	缺省情况下，没有创建AP分类规则
配置自定义AP信号RSSI规则	**rssi** *value1* [**to** *value2*]	缺省情况下，没有在AP分类规则中对AP信号的信号强度进行匹配
配置自定义SSID规则	**ssid** [**case-sensitive**] [**not**] { **equal** | **include** } *ssid-string*	缺省情况下，没有在AP分类规则中对AP使用无线服务的SSID进行匹配
配置自定义AP运行时间规则	**up-duration** *value1* [**to** *value2*]	缺省情况下，没有在AP分类规则中对AP的运行时间进行匹配
配置自定义AP关联客户端数量规则	**client-online** *value1* [**to** *value2*]	缺省情况下，没有在AP分类规则中对AP上已关联的无线客户端数量进行匹配

操作	命令	说明
配置自定义发现AP的Sensor数量规则	**discovered-ap** *value1* [**to** *value2*]	缺省情况下，没有在AP分类规则中对发现AP的sensor数量进行匹配
配置自定义安全方式规则	**security** { **equal** | **include** } { **clear** | **wep** | **wpa** | **wpa2** }	缺省情况下，没有在AP分类规则中对AP使用无线服务的数据安全方式进行匹配
配置自定义认证方式规则	**authentication** { **equal** | **include** } { **802.1x** | **none** | **other** | **psk** }	缺省情况下，没有在AP分类规则中对AP使用无线服务的安全认证方式进行匹配
配置自定义OUI信息规则	**oui** *oui-info*	缺省情况下，没有在AP分类规则中对AP设备的OUI信息进行匹配

2. 配置手工分类

表1-14 配置分类策略（手工分类）

操作	命令	说明
进入系统视图	**system-view**	-
进入WIPS视图	**wips**	-
创建分类策略，并进入分类策略视图	**classification policy** *policy-name*	缺省情况下，不存在分类策略
配置AP手工分类	**manual-classify mac-address** *mac-address* { **authorized-ap** | **external-ap** | **misconfigured-ap** | **rogue-ap** }	缺省情况下，没有对AP进行手工分类

1.8.2 应用分类策略

通过在虚拟安全域上应用分类策略，使已配置的分类策略在虚拟安全域内的 Radio 上生效。

表1-15 应用分类策略

操作	命令	说明
进入系统视图	**system-view**	-
进入WIPS视图	**wips**	-
创建VSD，并进入VSD视图	**virtual-security-domain** *vsd-name*	缺省情况下，不存在VSD
在VSD上应用分类策略	**apply classification policy** *policy-name*	缺省情况下，没有在VSD上应用分类策略

1.9 配置反制

创建一个反制策略，配置对一个或多个反制设备类型进行反制。

1.9.1 配置反制策略

表1-16 配置反制策略

操作	命令	说明
进入系统视图	**system-view**	-
进入WIPS视图	**wips**	-
创建反制策略，并进入反制策略视图	**countermeasure policy** *policy-name*	缺省情况下，不存在反制策略
配置对外部AP进行反制	**countermeasure external-ap**	缺省情况下，未配置对外部AP进行反制
配置对配置错误的AP进行反制	**countermeasure misconfigured-ap**	缺省情况下，未配置对配置错误的AP进行反制
配置对关联错误的客户端进行反制	**countermeasure misassociation-client**	缺省情况下，未配置对关联错误的客户端进行反制
配置对潜在授权AP进行反制	**countermeasure potential-authorized-ap**	缺省情况下，未配置对潜在授权AP进行反制
配置对潜在外部AP进行反制	**countermeasure potential-external-ap**	缺省情况下，未配置对潜在外部AP进行反制
配置对潜在Rogue AP进行反制	**countermeasure potential-rogue-ap**	缺省情况下，未配置对潜在Rogue AP进行反制
配置对Rogue AP进行反制	**countermeasure rogue-ap**	缺省情况下，未配置对Rogue AP进行反制
配置对未授权的客户端进行反制	**countermeasure unauthorized-client**	缺省情况下，未配置对未授权的客户端进行反制
配置对未确定分类的AP进行反制	**countermeasure uncategorized-ap**	缺省情况下，未配置对未确定分类的AP进行反制
配置对未确定分类的客户端进行反制	**countermeasure uncategorized-client**	缺省情况下，未配置对未确定分类的客户端进行反制
配置根据指定的MAC地址对设备进行手工反制	**countermeasure mac-address** *mac-address*	缺省情况下，未配置根据指定的MAC地址对设备进行手工反制
配置对ad hoc设备进行反制	**countermeasure adhoc**	缺省情况下，未配置对ad hoc设备进行反制
配置对发起广播解除认证帧攻击的设备进行反制	**countermeasure attack deauth-broadcast**	缺省情况下，未配置对发起广播解除认证帧攻击的设备进行反制
配置对发起广播解除关联帧攻击的设备进行反制	**countermeasure attack disassoc-broadcast**	缺省情况下，未配置对发起广播解除关联帧攻击的设备进行反制
配置对发起蜜罐AP攻击的设备进行反制	**countermeasure attack honeypot-ap**	缺省情况下，未配置对发起蜜罐AP攻击的设备进行反制
配置对发起热点攻击的设备进行反制	**countermeasure attack hotspot-attack**	缺省情况下，未配置对发起热点攻击的设备进行反制

操作	命令	说明
配置对禁用802.11n 40MHz模式的设备进行反制	**countermeasure attack ht-40-mhz-intolerance**	缺省情况下，未配置对禁用802.11n 40MHz模式的设备进行反制
配置对发起畸形报文攻击的设备进行反制	**countermeasure attack malformed-packet**	缺省情况下，未配置对发起畸形报文攻击的设备进行反制
配置对发起中间人攻击的设备进行反制	**countermeasure attack man-in-the-middle**	缺省情况下，未配置对发起中间人攻击的设备进行反制
配置对发起Omerta攻击的设备进行反制	**countermeasure attack omerta**	缺省情况下，未配置对发起Omerta攻击的设备进行反制
配置对发起节电攻击的设备进行反制	**countermeasure attack power-save**	缺省情况下，未配置对发起节电攻击的设备进行反制
配置对发起软AP攻击的设备进行反制	**countermeasure attack soft-ap**	缺省情况下，未配置对发起软AP攻击的设备进行反制
配置对未加密的信任客户端进行反制	**countermeasure attack unencrypted-trust-client**	缺省情况下，未配置对未加密的信任客户端进行反制
配置对Weak IV设备进行反制	**countermeasure attack weak-iv**	缺省情况下，未配置对Weak IV设备进行反制
配置对Windows网桥的设备进行反制	**countermeasure attack windows-bridge**	缺省情况下，未配置对Windows网桥设备进行反制
配置对所有发起攻击的设备进行反制	**countermeasure attack all**	缺省情况下，未配置对所有发起攻击的设备进行反制
配置所有Sensor进行反制功能	**select sensor all**	缺省情况下，所有Sensor进行反制功能处于关闭状态

1.9.2 应用反制策略

通过在虚拟安全域上应用反制策略，使已配置的反制策略在虚拟安全域内的 Radio 上生效。

表1-17 应用反制策略

操作	命令	说明
进入系统视图	**system-view**	-
进入WIPS视图	**wips**	-
创建VSD，并进入VSD视图	**virtual-security-domain** *vsd-name*	缺省情况下，不存在VSD
在VSD上应用反制策略	**apply countermeasure policy** *policy-name*	缺省情况下，没有在VSD上应用反制策略

1.10 配置探针功能

在 AP 的 Radio 接口上开启探针功能后，AP 通过对信道进行扫描，收集无线设备的信息并生成表项，同时将收集到的无线设备信息上传至指定的服务器。

表1-18 配置探针功能

操作	命令	说明
进入系统视图	**system-view**	-
配置探针AP上报无线设备信息的HTTPS服务器	**client-proximity-sensor server** *string* [**window-time** *window-time-value* | **partner** *partner-value*] *	缺省情况下，未配置探针AP上报无线设备信息的HTTPS服务器
配置探针AP上报无线设备信息的UDP服务器	**client-proximity-sensor udp-server** *ip-address* **port** *port-number* [**interval** *interval* | **preshared-key** [**cipher** | **simple**] *key-string*] *	缺省情况下，未配置探针AP上报无线设备信息的UDP服务器
配置AP表项的时间参数	**client-proximity-sensor ap-timer inactive** *inactive-value* **aging** *aging-value*	缺省情况下，AP表项的非活跃时间为300秒，老化时间为600秒
配置客户端表项的时间参数	**client-proximity-sensor client-timer inactive** *inactive-value* **aging** *aging-value*	缺省情况下，客户端表项的非活跃时间为300秒，老化时间为600秒
配置探针AP上报的MAC地址过滤列表	**client-proximity-sensor filter-list** *list*	缺省情况下，未配置探针AP上报的MAC地址过滤列表
配置探针AP检测无线设备信号强度的阈值	**client-proximity-sensor rssi-threshold** { **ap** *ap-rssi-value* | **client** *client-rssi-value* }	缺省情况下，未配置探针AP检测无线设备信号强度的阈值
配置探针AP上报苹果终端随机MAC地址功能	**client-proximity-sensor random-mac-report enable**	缺省情况下，探针AP上报苹果终端随机MAC地址功能处于关闭状态
配置探针AP将AP设备信息上报UDP服务器	**client-proximity-sensor report-ap enable**	缺省情况下，AP设备信息不上报UDP服务器
配置探针AP快速上报UDP服务器功能	**client-proximity-sensor rt-report enable**	缺省情况下，探针AP快速上报UDP服务器功能处于关闭状态
进入Radio接口视图	**interface wlan-radio** *interface-number*	-
配置探针功能	**client-proximity-sensor enable**	缺省情况下，探针功能处于关闭状态

1.11 私接代理检测功能

私接代理是指无线客户端为非法的用户共享网络的行为，在 AP 上开启私接代理检测功能后，可以检测到有非法网络共享行为的无线客户端信息并生成表项。

表1-19 配置私接代理检测功能

操作	命令	说明
进入系统视图	**system-view**	-
开启私接代理检测功能	**wlan nat-detect enable**	缺省情况下，私接代理检测功能处于关闭状态

1.12 WIPS显示和维护

在完成上述配置后，在任意视图下执行 **display** 命令可以显示配置后 WIPS 的运行情况，通过查看显示信息验证配置的效果。

在用户视图下执行 **reset** 命令可以清除 WIPS 的信息。

表1-20 WIPS 显示和维护

操作	命令
显示所有Sensor信息	**display wips sensor**
显示AC收到Sensor上报的攻击检测信息	**display wips statistics** [**receive | virtual-security-domain** *vsd-name*]
显示在指定VSD内检测到的无线设备的信息	**display wips virtual-security-domain** *vsd-name* **device** [**ap** [**adhoc** | **authorized** | **external** | **mesh** | **misconfigured** | **potential-authorized** | **potential-external** | **potential-rogue** | **rogue** | **uncategorized**] | **client** [[**dissociative-client**] [**authorized** | **misassociation** | **unauthorized** | **uncategorized**]] | **mac-address** *mac-address*] [**verbose**]
显示被反制过设备的信息	**display wips virtual-security-domain** *vsd-name* **countermeasure record**
显示探针AP检测到的无线设备信息	**display client-proximity-sensor device** [**ap** | **client** | **mac-address** *mac-address*] [**verbose**]
显示AC收到探针AP上报的检测统计信息	**display client-proximity-sensor statistics receive**
显示所有探针AP的信息	**display client-proximity-sensor sensor**
显示私接代理检测信息	**display wlan nat-detect** [**mac-address** *mac-address*]
清除所有Sensor上报的信息	**reset wips statistics**
清除指定VSD内内学习到的AP表项和客户端表项	**reset wips virtual-security-domain** *vsd-name* { **ap** { **all** | **mac-address** *mac-address*} | **client** { **all** | **mac-address** *mac-address* } | **all** }
清除指定VSD内所有被反制过的设备信息	**reset wips virtual-security-domain** *vsd-name* **countermeasure record**
清除无线设备表项	**reset client-proximity-sensor device** { **ap** | **client** | **mac-address** *mac-address* | **all** }
清除所有探针AP上报的信息	**reset client-proximity-sensor statistics**
清除私接代理检测信息表项	**reset wlan nat-detect**

1.13 WIPS典型配置举例

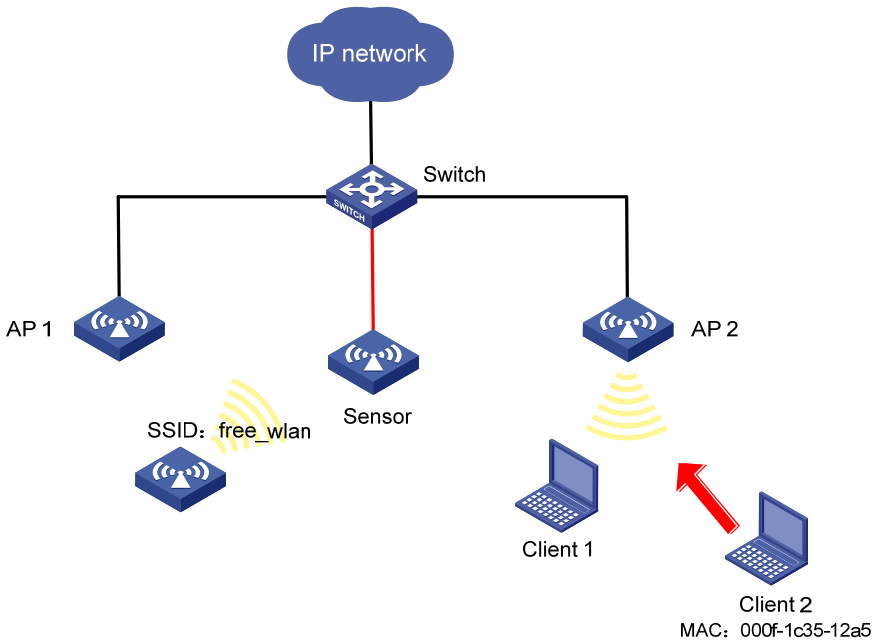
1.13.1 WIPS分类与反制配置举例

1. 组网需求

如 图 1-3 所示，AP1 和AP2 为Client提供无线服务，SSID为“abc”，在Sensor上开启WIPS功能，配置分类策略，将非法客户端的MAC地址（000f-1c35-12a5）添加到静态禁用列表中，将SSID“abc”添加到静态信任列表中，要求对检测到的潜在外部AP和未授权客户端进行反制。

2. 组网图

图1-3 WIPS 分类与反制组网图



3. 配置步骤

在 AP1 和 AP2 上完成无线服务的相关配置，具体配置步骤可参见“WLAN 配置指导”中的“WLAN 接入”，此处不再重复。

配置虚拟安全域 vsd1。

```
<Sensor> system-view
[Sensor] wips
[Sensor-wips] virtual-security-domain vsd1
[Sensor-wips-vsd-vsd1] quit
[Sensor-wips] quit
```

开启 WIPS 功能。

```
[Sensor] interface WLAN-Radio 1/0/1
[Sensor-WLAN-Radio1/0/1] wips enable
[Sensor-WLAN-Radio1/0/1] quit
[Sensor] interface WLAN-Radio 1/0/2
[Sensor-WLAN-Radio1/0/2] wips enable
```

```
[Sensor-WLAN-Radio1/0/2] quit
[Sensor] interface WLAN-Radio 1/0/3
[Sensor-WLAN-Radio1/0/3] wips enable
[Sensor-WLAN-Radio1/0/3] quit
```

配置 Sensor 加入虚拟安全域 vsd1。

```
[Sensor] wips virtual-security-domain vsd1
```

配置分类策略 class1，将 Client 2 的 MAC 地址配置禁用 MAC 地址，并且将名为“abc”的 SSID 配置为信任 SSID。

```
[Sensor] wips
[Sensor-wips] classification policy class1
[Sensor-wips-cls-class1] block mac-address 000f-1c35-12a5
[Sensor-wips-cls-class1] trust ssid abc
[Sensor-wips-cls-class1] quit
```

虚拟安全域 vsd1 应用分类策略 class1。

```
[Sensor-wips] virtual-security-domain vsd1
[Sensor-wips-vsd-vsd1] apply classification policy class1
[Sensor-wips-vsd-vsd1] quit
```

配置反制策略 protect，反制未授权客户端和潜在外部 AP。

```
[Sensor-wips] countermeasure policy protect
[Sensor-wips-cms-protect] countermeasure unauthorized-client
[Sensor-wips-cms-protect] countermeasure potential-external-ap
[Sensor-wips-cms-protect] quit
```

虚拟安全域 vsd1 应用反制策略 protect。

```
[Sensor-wips] virtual-security-domain vsd1
[Sensor-wips-vsd-vsd1] apply countermeasure policy protect
[Sensor-wips-vsd-vsd1] quit
[Sensor-wips] quit
```

4. 验证配置

(1) 通过 **display wips virtual-security-domain** 命令查看无线设备的分类结果。

```
[Sensor] display wips virtual-security-domain vsd1 device
Total 3 detected devices in virtual-security-domain vsd1

Class: Auth - authorization; Ext - extern; Mis - mistake;
       Unauth - unauthorized; Uncate - uncategorized;
       (A) - associate; (C) - config; (P) - potential

MAC address    Type   Class    Duration    Sensors Channel Status
00e0-fc00-5829 AP     Auth     00h 10m 24s 1       11      Active
000f-e228-2528 AP     Auth     00h 10m 04s 1       11      Active
000f-e223-1616 AP     Ext(P)   00h 10m 46s 1       11      Active
000f-1c35-12a5 Client Unauth   00h 10m 02s 1       11      Active
000f-e201-0102 Client Auth     00h 10m 02s 1       11      Active
```

在虚拟安全域 vsd1，MAC 地址为 000f-e223-1616 的 AP 被分类成潜在外部 AP，MAC 地址为 000f-1c35-12a5 的客户端被分类为未授权的客户端。

(2) 通过命令行 **display wips virtual-security-domain vsd1 countermeasure record** 命令查看反制过的设备记录信息。

```
[Sensor] display wips virtual-security-domain vsd1 countermeasure record
Total 2 times countermeasure, current 2 countermeasure record in virtual-security-domain vsd1

Reason: Attack; Ass - associated; Black - blacklist;
        Class - classification; Manu - manual;

MAC address    Type   Reason   Countermeasure AP      Radio ID   Time
000f-e223-1616 AP     Class    Sensor                 1          2014-06-03/10:30:36
000f-1c35-12a5 Client Class    Sensor                 1          2014-06-03/09:13:26
```

在虚拟安全域 vsd1，MAC 地址为 000f-1c35-12a5 的未授权客户端和 MAC 地址为 000f-e223-1616 的潜在外部 AP 被反制。

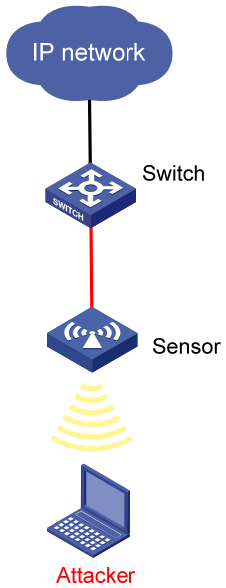
1.13.2 WIPS畸形报文检测和泛洪攻击检测配置举例

1. 组网需求

如 图 1-4 所示，将AP配置为Sensor，配置虚拟安全域VSD_1，并配置Sensor属于这个虚拟安全域，当检测到攻击者对无线网络进行IE重复的畸形报文或Beacon帧泛洪攻击时，AP打印告警信息。

2. 组网图

图1-4 畸形报文检测和泛洪攻击检测组网图



3. 配置步骤

在 Sensor 上完成无线服务的相关配置，具体配置步骤可参见“WLAN 配置指导”中的“WLAN 接入”，此处不再重复。

配置虚拟安全域 vsd1。

```
<Sensor> system-view
[Sensor] wips
[Sensor-wips] virtual-security-domain vsd1
```

```
[Sensor-wips-vsd-vsd1] quit
[Sensor-wips] quit
```
开启 WIPS 功能。
```
[Sensor] interface WLAN-Radio 1/0/1
[Sensor-WLAN-Radio1/0/1] wips enable
[Sensor-WLAN-Radio1/0/1] quit
[Sensor] interface WLAN-Radio 1/0/2
[Sensor-WLAN-Radio1/0/2] wips enable
[Sensor-WLAN-Radio1/0/2] quit
[Sensor] interface WLAN-Radio 1/0/3
[Sensor-WLAN-Radio1/0/3] wips enable
[Sensor-WLAN-Radio1/0/3] quit
```
配置 Sensor 加入虚拟安全域 vsd1。
```
[Sensor] wips virtual-security-domain vsd1
```
创建攻击检测策略，当检测到 IE 重复的畸形报文和 Beacon 帧泛洪攻击时，向 AC 发送日志信息或告警信息。检测 IE 重复的畸形报文的静默时间为 50 秒，检测 Beacon 帧的统计周期为 100 秒，触发阈值为 200，静默时间为 50 秒。
```
[Sensor] wips
[Sensor-wips] detect policy dtc1
[Sensor-wips-dtc-dtc1] malformed duplicated-ie quiet 50
[Sensor-wips-dtc-dtc1] flood beacon interval 100 quiet 50 threshold 200
[Sensor-wips-dtc-dtc1] quit
```
在虚拟安全域 VSD_1 上应用攻击检测策略。
```
[Sensor-wips] virtual-security-domain VSD_1
[Sensor-wips-vsd-VSD_1] apply detect policy dtc1
[Sensor-wips-vsd-VSD_1] quit
[Sensor-wips] quit
```
4. 验证结果

(1) 当网络中没有攻击者时，在 Sensor 上通过命令行 **display wips statistics receive** 命令查看收到报文的统计信息，畸形报文和泛洪报文的统计个数为 0。
```
[Sensor] display wips statistics receive
Information from sensor 1
Information about attack statistics:
Detected association-request flood messages: 0
Detected authentication flood messages: 0
Detected beacon flood messages: 0
Detected block-ack flood messages: 0
Detected cts flood messages: 0
Detected deauthentication flood messages: 0
Detected disassociation flood messages: 0
Detected eapol-start flood messages: 0
Detected null-data flood messages: 0
Detected probe-request flood messages: 0
Detected reassociation-request flood messages: 0
Detected rts flood messages: 0
Detected duplicated-ie messages: 0
```

```
Detected fata-jack messages: 0
Detected illegal-ibss-ess messages: 0
Detected invalid-address-combination messages: 0
Detected invalid-assoc-req messages: 0
Detected invalid-auth messages: 0
Detected invalid-deauth-code messages: 0
Detected invalid-disassoc-code messages: 0
Detected invalid-ht-ie messages: 0
Detected invalid-ie-length messages: 0
Detected invalid-pkt-length messages: 0
Detected large-duration messages: 0
Detected null-probe-resp messages: 0
Detected overflow-eapol-key messages: 0
Detected overflow-ssid messages: 0
Detected redundant-ie messages: 0
Detected AP spoof AP messages: 0
Detected AP spoof client messages: 0
Detected AP spoof ad-hoc messages: 0
Detected ad-hoc spoof AP messages: 0
Detected client spoof AP messages: 0
Detected weak IV messages: 0
Detected excess AP messages: 0
Detected excess client messages: 0
Detected sig rule messages: 0
Information from sensor 2
Information about attack statistics:
Detected association-request flood messages: 0
Detected authentication flood messages: 0
Detected beacon flood messages: 0
Detected block-ack flood messages: 0
Detected cts flood messages: 0
Detected deauthentication flood messages: 0
Detected disassociation flood messages: 0
Detected eapol-start flood messages: 0
Detected null-data flood messages: 0
Detected probe-request flood messages: 0
Detected reassociation-request flood messages: 0
Detected rts flood messages: 0
Detected duplicated-ie messages: 0
Detected fata-jack messages: 0
Detected illegal-ibss-ess messages: 0
Detected invalid-address-combination messages: 0
Detected invalid-assoc-req messages: 0
Detected invalid-auth messages: 0
Detected invalid-deauth-code messages: 0
Detected invalid-disassoc-code messages: 0
Detected invalid-ht-ie messages: 0
Detected invalid-ie-length messages: 0
```

```
Detected invalid-pkt-length messages: 0
Detected large-duration messages: 0
Detected null-probe-resp messages: 0
Detected overflow-eapol-key messages: 0
Detected overflow-ssid messages: 0
Detected redundant-ie messages: 0
Detected AP spoof AP messages: 0
Detected AP spoof client messages: 0
Detected AP spoof ad-hoc messages: 0
Detected ad-hoc spoof AP messages: 0
Detected client spoof AP messages: 0
Detected weak IV messages: 0
Detected excess AP messages: 0
Detected excess client messages: 0
Detected sig rule messages: 0
```

(2) 当检测到IE重复的畸形报文和Beacon帧泛洪攻击时，在Sensor上通过命令行 **display wips statistics receive** 查看收到报文的统计信息，IE重复的畸形报文的统计个数为28和Beacon帧泛洪攻击的统计个数为18。

```
[Sensor] display wips statistics receive
Information from sensor 1
Information about attack statistics:
Detected association-request flood messages: 0
Detected authentication flood messages: 0
Detected beacon flood messages: 18
Detected block-ack flood messages: 0
Detected cts flood messages: 0
Detected deauthentication flood messages: 0
Detected disassociation flood messages: 0
Detected eapol-start flood messages: 0
Detected null-data flood messages: 0
Detected probe-request flood messages: 0
Detected reassociation-request flood messages: 0
Detected rts flood messages: 0
Detected duplicated-ie messages: 0
Detected fata-jack messages: 0
Detected illegal-ibss-ess messages: 0
Detected invalid-address-combination messages: 0
Detected invalid-assoc-req messages: 0
Detected invalid-auth messages: 0
Detected invalid-deauth-code messages: 0
Detected invalid-disassoc-code messages: 0
Detected invalid-ht-ie messages: 0
Detected invalid-ie-length messages: 0
Detected invalid-pkt-length messages: 0
Detected large-duration messages: 0
Detected null-probe-resp messages: 0
Detected overflow-eapol-key messages: 0
Detected overflow-ssid messages: 0
```

```
Detected redundant-ie messages: 0
Detected AP spoof AP messages: 0
Detected AP spoof client messages: 0
Detected AP spoof ad-hoc messages: 0
Detected ad-hoc spoof AP messages: 0
Detected client spoof AP messages: 0
Detected weak IV messages: 0
Detected excess AP messages: 0
Detected excess client messages: 0
Detected sig rule messages: 0
Information from sensor 2
Information about attack statistics:
Detected association-request flood messages: 0
Detected authentication flood messages: 0
Detected beacon flood messages: 0
Detected block-ack flood messages: 0
Detected cts flood messages: 0
Detected deauthentication flood messages: 0
Detected disassociation flood messages: 0
Detected eapol-start flood messages: 0
Detected null-data flood messages: 0
Detected probe-request flood messages: 0
Detected reassociation-request flood messages: 0
Detected rts flood messages: 0
Detected duplicated-ie messages: 28
Detected fata-jack messages: 0
Detected illegal-ibss-ess messages: 0
Detected invalid-address-combination messages: 0
Detected invalid-assoc-req messages: 0
Detected invalid-auth messages: 0
Detected invalid-deauth-code messages: 0
Detected invalid-disassoc-code messages: 0
Detected invalid-ht-ie messages: 0
Detected invalid-ie-length messages: 0
Detected invalid-pkt-length messages: 0
Detected large-duration messages: 0
Detected null-probe-resp messages: 0
Detected overflow-eapol-key messages: 0
Detected overflow-ssid messages: 0
Detected redundant-ie messages: 0
Detected AP spoof AP messages: 0
Detected AP spoof client messages: 0
Detected AP spoof ad-hoc messages: 0
Detected ad-hoc spoof AP messages: 0
Detected client spoof AP messages: 0
Detected weak IV messages: 0
Detected excess AP messages: 0
Detected excess client messages: 0
```

```
Detected sig rule messages: 0
```

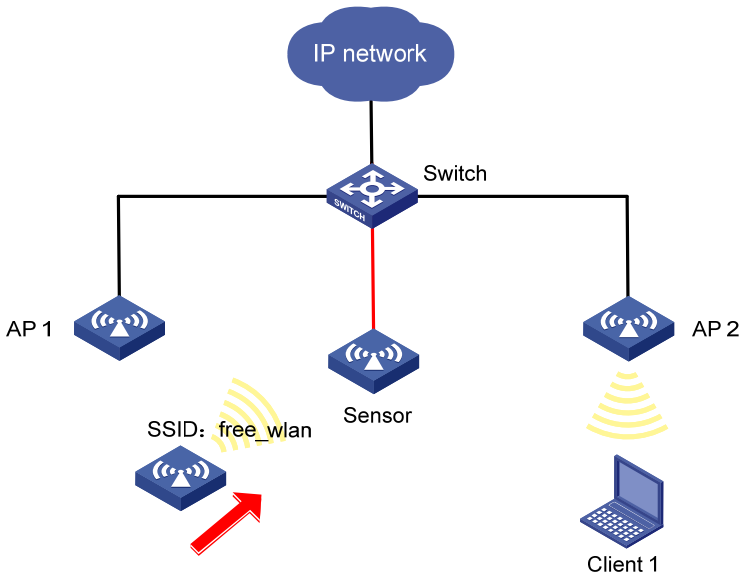
1.13.3 Signature检测配置举例

1. 组网需求

如 图 1-5 所示，AP1 和AP2 为Client提供无线服务，SSID为“abc”，在Sensor上开启WIPS功能，配置Signature检测，检测无线环境中是否存在其他的无线服务，对SSID不是abc的Beacon帧进行检测，并打印告警信息。

2. 组网图

图1-5 WIPS 的攻击检测组网图



3. 配置步骤

在 Sensor 上完成无线服务的相关配置，具体配置步骤可参见“WLAN 配置指导”中的“WLAN 接入”，此处不再重复。

配置虚拟安全域 vsd1。

```
<Sensor> system-view
[Sensor] wips
[Sensor-wips] virtual-security-domain vsd1
[Sensor-wips-vsd-vsd1] quit
[Sensor-wips] quit
```

开启 WIPS 功能。

```
[Sensor] interface WLAN-Radio 1/0/1
[Sensor-WLAN-Radio1/0/1] wips enable
[Sensor-WLAN-Radio1/0/1] quit
[Sensor] interface WLAN-Radio 1/0/2
[Sensor-WLAN-Radio1/0/2] wips enable
[Sensor-WLAN-Radio1/0/2] quit
[Sensor] interface WLAN-Radio 1/0/3
[Sensor-WLAN-Radio1/0/3] wips enable
```

```
[Sensor-WLAN-Radio1/0/3] quit
```

配置 Sensor 加入虚拟安全域 vsd1。

```
[Sensor] wips virtual-security-domain vsd1
```

Signature 规则 1，配置子规则对 SSID 不是 abc 的 Beacon 帧进行检测。

```
[Sensor] wips
[Sensor-wips] signature rule 1
[Sensor-wips-sig-rule-1] frame-type management frame-subtype beacon
[Sensor-wips-sig-rule-1] ssid not equal abc
[Sensor-wips-sig-rule-1] quit
```

创建 Signature 策略 sig1，应用 Signature 规则 1，配置统计周期为 5 秒，发出告警后的静默时间为 60 秒，统计次数的阈值为 60。

```
[Sensor-wips] signature policy sig1
[Sensor-wips-sig-sig1] apply signature rule 1
[Sensor-wips-sig-sig1] detect signature interval 5 quiet 60 threshold 60
[Sensor-wips-sig-sig1] quit
```

配置虚拟安全域 vsd1，应用 Signature 策略。

```
[Sensor] wips
[Sensor-wips] virtual-security-domain vsd1
[Sensor-wips-vsd-vsd1] apply signature policy sig1
[Sensor-wips-vsd-vsd1] quit
```

4. 验证结果

(1) 当检测到 SSID 为“free_wlan”的无线服务后， Sensor 会打印告警信息。

```
WIPS/5/WIPS_SIGNATURE: -VSD=vsd1-RuleID=1; Signature rule matched.
```

(2) 在 Sensor 上通过命令行 **display wips statistics receive** 查看 Signature 检测统计信息，Signature 检测统计计数为 26。

```
[Sensor] display wips statistics receive
Information from sensor
Information about attack statistics:
Detected association-request flood messages: 0
Detected authentication flood messages: 0
Detected beacon flood messages: 0
Detected block-ack flood messages: 0
Detected cts flood messages: 0
Detected deauthentication flood messages: 0
Detected disassociation flood messages: 0
Detected eapol-start flood messages: 0
Detected null-data flood messages: 0
Detected probe-request flood messages: 0
Detected reassociation-request flood messages: 0
Detected rts flood messages: 0
Detected duplicated-ie messages: 0
Detected fata-jack messages: 0
Detected illegal-ibss-ess messages: 0
Detected invalid-address-combination messages: 0
Detected invalid-assoc-req messages: 0
Detected invalid-auth messages: 0
```

```
Detected invalid-deauth-code messages: 0
Detected invalid-disassoc-code messages: 0
Detected invalid-ht-ie messages: 0
Detected invalid-ie-length messages: 0
Detected invalid-pkt-length messages: 0
Detected large-duration messages: 0
Detected null-probe-resp messages: 0
Detected overflow-eapol-key messages: 0
Detected overflow-ssid messages: 0
Detected redundant-ie messages: 0
Detected AP spoof AP messages: 0
Detected AP spoof client messages: 0
Detected AP spoof ad-hoc messages: 0
Detected ad-hoc spoof AP messages: 0
Detected client spoof AP messages: 0
Detected weak IV messages: 0
Detected excess AP messages: 0
Detected excess client messages: 0
Detected sig rule messages: 26
```