目 录

1 WLAN IDS配置

说明

本文所指的 AP 和 FAT AP 代表了 MSR 900 和 MSR 20-1X 无线款型，以及安装了 SIC-WLAN 模块的 MSR 系列路由器。

1.1 WLAN IDS功能简介

802.11 网络很容易受到各种网络威胁的影响，如未经授权的 AP 用户、Ad-hoc 网络、拒绝服务型攻击等。Rogue 设备对于企业网络安全来说是一个很严重的威胁。WIDS（Wireless Intrusion Detection System，无线入侵检测系统）用于对有恶意的用户攻击和入侵无线网络进行早期检测。WIPS（Wireless Intrusion Prevention System，无线入侵防御系统）可以保护企业网络和用户不被无线网络上未经授权的设备访问。Rogue 设备检测功能是 WIDS/WIPS 功能的一部分，它用于检测 WLAN 网络中的 Rogue 设备，并对它们采取反制措施，以阻止其工作。

1.1.1 常用术语

- WIDS：WIDS 用于放置到已有的无线网络中，它可以对网络外恶意的攻击和入侵无线网络进行检测。
- Rogue AP：网络中未经授权或者有恶意的 AP，它可以是私自接入到网络中的 AP、未配置的 AP、邻居 AP 或者攻击者操作的 AP。如果在这些 AP 上存在漏洞的话，黑客就有机会危害你的网络安全。
- Rogue Client：非法客户端，网络中未经授权或者有恶意的客户端，类似于 rogue AP。
- Rogue Wireless Bridge：非法无线网桥，网络中未经授权或者有恶意的网桥。
- Monitor AP：网络中用于扫描或监听无线介质，并试图检测无线网络中的攻击。
- Ad-hoc mode：把无线客户端的工作模式设置为 Ad-hoc 模式，Ad-hoc 终端可以不需要任何设备支持而直接进行通讯。
- Passive Scanning：在被动扫描模式下，monitor AP 监听该信道下空气介质中所有的 802.11 帧。
- Active Scanning：在监听 802.11 帧的同时，monitor AP 发送广播探查请求并在该信道上等待所有的探查响应消息。每一个在 monitor AP 附近的 AP 都将回应探查请求，这样就可以通过处理探查响应帧来分辨 friend AP 和 rogue AP。在发送探查请求时，Monitor AP 是伪装成客户端的。

1.1.2 检测IDS攻击

为了及时发现 WLAN 网络的恶意或者无意的攻击，通过记录信息或者发送日志信息的方式通知网络管理者。目前设备支持的入侵检测主要包括泛洪攻击检测、Spoof 检测以及 Weak IV 检测。

1. 泛洪攻击检测

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合法无线客户端的报文。

攻击检测通过持续地监控每台无线客户端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，该无线客户端将被认定在实施泛洪攻击。如果在 WLAN 设备上开启动态黑名单功能，此时被检测到的攻击设备将被加入黑名单，在后续一段时间内将被禁止接入 WLAN 网络。

入侵检测支持对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）
- 802.11 Null 数据帧
- 802.11 Action 帧

2. Spoofing攻击检测

Spoofing 攻击是指潜在的攻击者会仿冒其他设备的名义发送攻击报文，以达到破坏无线网络正常工作的目的。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报文就可能导致客户端下线，同样如果攻击者仿冒客户端的名义给 AP 发送解除认证报文也会影响无线网络的正常工作。

目前，Spoofing 攻击检测支持对仿冒 AP 名义发送的广播解除认证和广播解除关联报文进行检测。当接收到这两种报文时，设备会将其定义为 Spoofing 攻击并被记录到日志中。

3. Weak IV攻击检测

使用 WEP 加密的时候，WLAN 设备对于每一个报文都会使用 IV（Initialization Vector，初始化向量），IV 和 Key 一起作为输入来生成 Key Stream，使相同密钥产生不同加密效果。当一个 WEP 报文被发送时，用于加密报文的 IV 也作为报文头的一部分被发送。如果 WLAN 设备使用不安全的方法生成 IV，例如始终使用固定的 IV，就可能会暴露共享的密钥，如果潜在的攻击者获得了共享的密钥，攻击者将能够控制网络资源。

检测 IDS 攻击可以通过识别每个 WEP 报文的 IV 来预防这种攻击，当一个有 Weak IV 的报文被检测到时，这个检测将立刻被记录到日志中。

1.1.3 黑白名单

1. 黑白名单列表

在 WLAN 网络环境中，可以通过黑白名单功能设定一定的规则过滤无线客户端，实现对无线客户端的接入控制。

黑白名单维护三种类型的列表。

- 白名单列表：该列表包含允许接入的无线客户端的 MAC 地址。如果使用了白名单，则只有白名单中指定的无线客户端可以接入到 WLAN 网络中，其他的无线客户端将被拒绝接入。
- 静态黑名单列表：该列表包含拒绝接入的无线客户端的 MAC 地址。
- 动态黑名单列表：当 WLAN 设备检测到来自某一设备的非法攻击时，可以选择将该设备动态加入到黑名单中，拒绝接收任何来自于该设备的报文，直至该动态黑名单表项老化为止，从而实现对 WLAN 网络的安全保护。

2. 黑白名单的处理过程

黑白名单按照以下步骤对接收到的 802.11 报文进行过滤，只有满足条件的报文允许通过，其他的所有的报文都会被丢弃。

(1) 当 AP 接收到一个 802.11 帧时，将针对该 802.11 帧的源 MAC 进行过滤；

(2) 如果设置了白名单列表，但接收帧的源 MAC 不在白名单列表内，该帧将被丢弃；

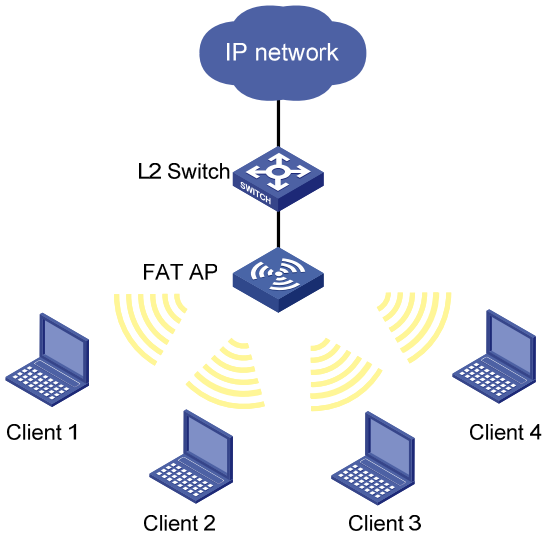
(3) 如果源 MAC 在白名单内，该帧将被作为合法帧进一步处理；

(4) 如果没有设置白名单列表，则继续搜索静态和动态的黑名单列表。如果源 MAC 在静态或动态黑名单列表内，该帧将被丢弃；

(5) 如果源 MAC 没有在静态或动态黑名单列表内，或者黑名单列表为空，则该帧将被作为合法帧进一步处理。

3. 黑白名单的作用范围

图1-1 无线用户接入控制组网图



在 FAT AP 组网图中，假设 Client 1 的 MAC 地址存在于黑名单列表中，则 Client 1 不能与 FAT AP 发生关联。当 Client 1 的 MAC 地址存在于白名单列表中时，它可以接入无线网络。

1.2 WLAN IDS配置任务简介

表1-1 WLAN IDS 配置任务简介

配置任务		说明	详细配置
配置AP的工作模式		可选	1.3
配置IDS攻击检测	配置IDS攻击检测	可选	1.4
	IDS攻击检测显示和维护		
配置黑白名单		可选	1.5

1.3 配置AP的工作模式

WLAN 网络由跨越建筑物提供不同 WLAN 服务的 AP 组成，由于 rogue 设备的存在，管理员需要其中的一些 AP 监视 WLAN。AP 可以工作在 Normal、Monitor 或 Hybrid 三种模式之一。

- 标准（Normal）模式：AP 仅传输 WLAN 用户的数据，不进行任何监测。
- 监控（Monitor）模式：在这种模式下，AP 需要扫描 WLAN 中的设备，此时 AP 仅做监测 AP，不做接入 AP。当 AP 工作在 Monitor 模式时，该 AP 提供的所有 WLAN 服务都将关闭。Monitor 模式的 AP，监听所有 802.11 帧。
- 混合（Hybrid）模式：在这种模式下，AP 可以在监测无线环境的同时可以提供无线服务。

表1-2 配置 AP 的工作模式

配置	命令	说明
进入系统视图	**system-view**	-
配置AP工作在Monitor模式	**wlan work-mode monitor**	两者选择其一 缺省情况下，AP工作在Normal模式，仅提供WLAN服务 需要注意的是： • 当 AP 从 Normal 模式切换到 Monitor 模式时，AP 不会重启 • 当 AP 从 Monitor 模式切换到 Normal 模式时，AP 会重启
配置AP工作在Hybrid模式	**wlan device-detection enable**	

说明

- 如果 AP 工作模式为 Hybrid 模式，需要配置服务模板，AP 可以在监测无线环境的同时可以提供无线服务。
- 如果 AP 工作模式为 Monitor 模式，那么 AP 不需要提供无线服务，不需要配置服务模板。

1.4 配置检测IDS攻击

1.4.1 配置检测IDS攻击

表1-3 配置 IDS 攻击检测

配置	命令	说明
进入系统视图	**system-view**	-
进入IDS视图	**wlan ids**	-
配置IDS攻击检测	**attack-detection enable** { **all** | **flood** | **spoof** | **weak-iv** }	必选 缺省情况下，攻击检测功能处于关闭状态

1.4.2 IDS攻击检测显示和维护

在完成上述配置后，在任意视图下执行 **display** 命令可以显示 IDS 攻击检测配置后的运行情况，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 IDS 攻击检测统计信息。

表1-4 IDS 攻击检测显示和维护

配置	命令
显示WLAN系统的攻击检测历史信息	**display wlan ids history** [**|** { **begin** | **exclude** | **include** } *regular-expression*]
显示检测到的攻击数	**display wlan ids statistics** [**|** { **begin** | **exclude** | **include** } *regular-expression*]
清除WLAN系统攻击检测的历史信息	**reset wlan ids history**

配置	命令
清除WLAN系统攻击检测的统计信息	**reset wlan ids statistics**

1.5 配置黑白名单

各种名单列表的特性如下：

- 切换到 IDS 视图下可以配置静态黑名单列表、白名单列表、使能动态黑名单列表功能以及动态黑名单中的对应列表的生存时间。
- 只有当表项存在于白名单列表中时，对应的客户端才能通过帧过滤。用户可以通过命令行添加或删除表项。
- 当输入表项存在于黑名单列表中时将被拒绝通过，当 WIDS 检测到泛洪攻击时，该表项将被动态添加到动态黑名单列表中。对于存在于动态黑名单中的表项，用户可以通过命令行设置生存时间。在该时间超时后，该设备接口将被从动态列表中删除。

1.5.1 配置静态列表

表1-5 配置静态列表

操作	命令	说明
进入系统视图	**system-view**	-
进入ids视图	**wlan ids**	-
配置白名单列表	**whitelist mac-address** *mac-address*	可选 缺省情况下，不存在静态白名单
配置静态黑名单列表	**static-blacklist mac-address** *mac-address*	可选 缺省情况下，不存在静态黑名单

1.5.2 配置动态黑名单

表1-6 配置动态黑名单

操作	命令	说明
进入系统视图	**system-view**	-
进入ids视图	**wlan ids**	-
使能动态黑名单列表功能	**dynamic-blacklist enable**	可选 缺省情况下，动态黑名单功能处于关闭状态
设置动态黑名单中的对应列表的生存时间	**dynamic-blacklist lifetime** *lifetime*	可选 缺省情况下，生存时间为300秒

1.5.3 黑白名单显示和维护

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黑白名单的运行情况，通过查看显示信息验证配置的效果。

在用户视图下执行 **reset** 命令清除黑白名单的相关信息。

表1-7 黑白名单显示和维护

操作	命令
显示黑名单列表	**display wlan blacklist** { **static** | **dynamic** } [**|** { **begin** | **exclude** | **include** } *regular-expression*]
显示白名单列表	**display wlan whitelist** [**|** { **begin** | **exclude** | **include** } *regular-expression*]
清除动态黑名单列表选项	**reset wlan dynamic-blacklist** { **mac-address** *mac-address* | **all** }

1.6 WLAN IDS配置举例

1.6.1 WLAN IDS配置举例

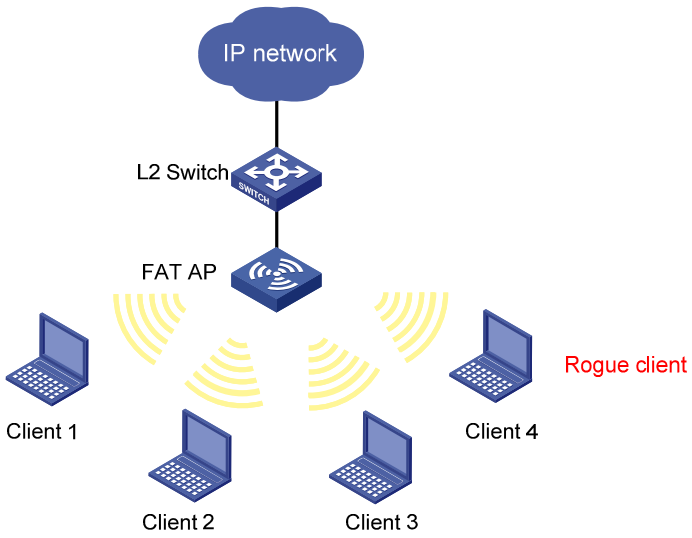
1. 组网需求

FAT AP 通过二层交换机接入网络。

- Client 1（MAC 地址为 000f-e215-1515）、Client 2（MAC 地址为 000f-e215-1530）、Client 3（MAC 地址为 000f-e213-1235）连接到无线网络中，享受 FAT AP 提供的 WLAN 服务。
- 通过配置 FAT AP 的工作模式为 Hybrid 模式达到其在提供 WLAN 服务的同时，检测网络中非法客户端的目的。

2. 组网图

图1-2 WIDS 配置组网图



3. 配置步骤

创建 WLAN BSS 接口。

```
<AP> system-view
[AP] interface wlan-bss 1
[AP-WLAN-BSS1] quit
```

配置 WLAN 服务模板为 clear 模式，配置 SSID 为 service，不配置认证方式。

```
[AP] wlan service-template 1 clear
[AP-wlan-st-1] ssid service
[AP-wlan-st-1] authentication-method open-system
[AP-wlan-st-1] service-template enable
[AP-wlan-st-1] quit
```

在 Wlan-radio 2/0 上绑定无线服务模板 1 和 WLAN-BSS 1

```
[AP] interface Wlan-radio 2/0
[AP-Wlan-radio2/0] service-template 1 interface WLAN-BSS 1
[AP-Wlan-radio2/0] quit
```

配置 AP 工作为 Hybrid 模式，使其提供无线服务的同时对非法设备进行检测。

```
[AP] wlan device-detection enable
```

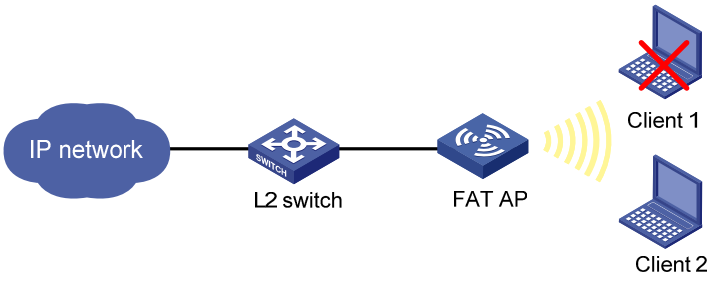
1.6.2 黑名单配置举例

1. 组网需求

客户端通过 FAT AP 接入无线网络。其中 Client 1（0000-000f-1211）为已知非法客户端，为了保证无线网络的安全性，网络管理员需要将其的 MAC 地址加入到设备的黑名单列表中，使其无法接入网络。

2. 组网图

图1-3 黑名单配置组网图



3. 配置步骤

将 Client 1 的 MAC 地址 0000-000f-1211 添加到静态黑名单列表。

```
<Sysname> system-view
[Sysname] wlan ids
[Sysname-wlan-ids] static-blacklist mac-address 0000-000f-1211
```

完成配置后，非法客户端 Client 1（0000-000f-1211）无法接入 AP，其它客户端正常接入网络。