

*BlueSecurity*无线网络入侵检测系统

蓝云信息

无线网络蓬勃发展

- 移动互联网正在爆炸式增长
- 习惯于WiFi热点的覆盖
- 在工作场所自己架设WiFi热点



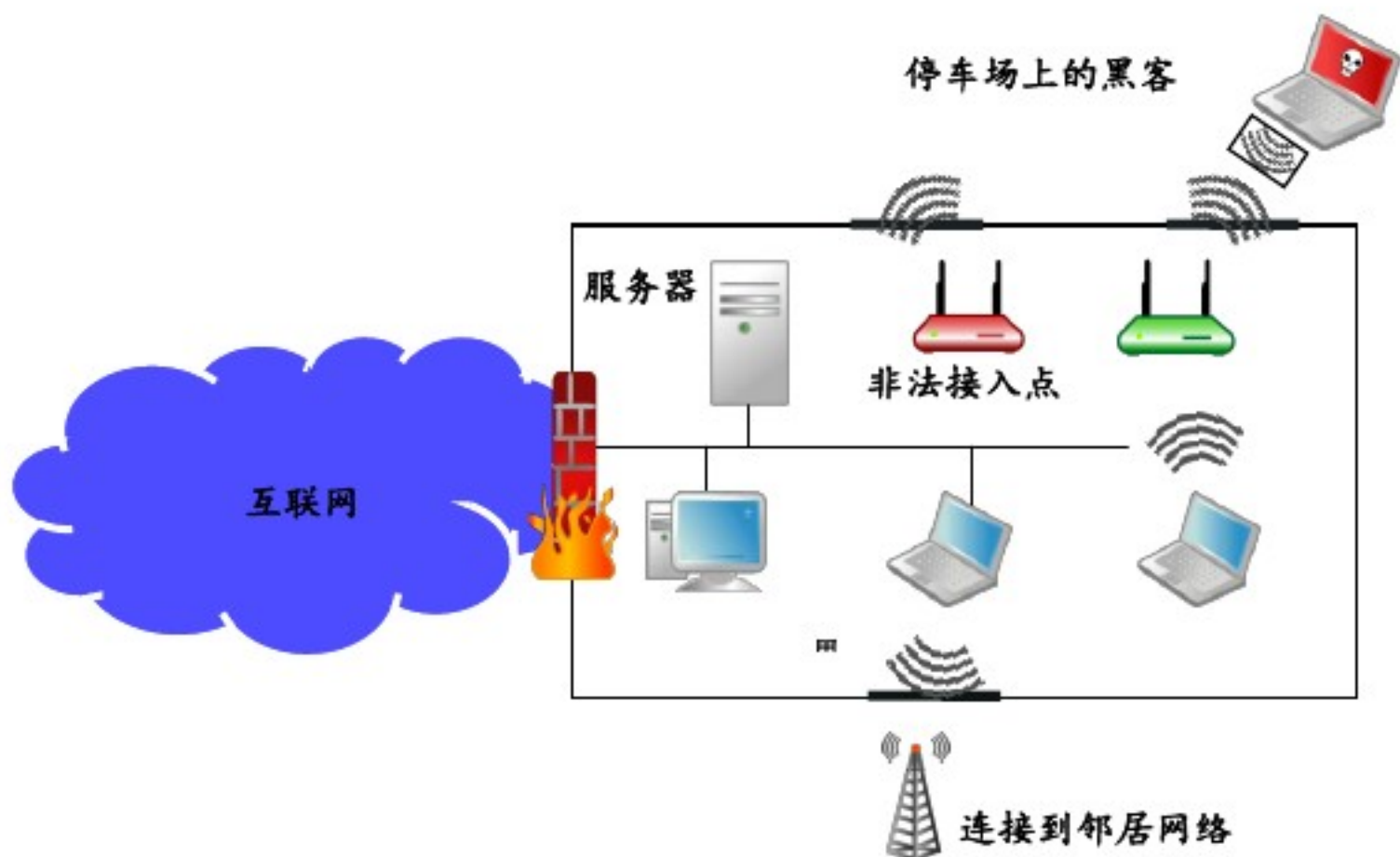
安全隐患

- WiFi热点可能是邪恶的



安全隐患

- 工作场所架设的WiFi热点开放了内网的接入口，绕过了有线网络的防火墙



安全隐患

- 多种针对WiFi热点的攻击手段
 - DoS攻击

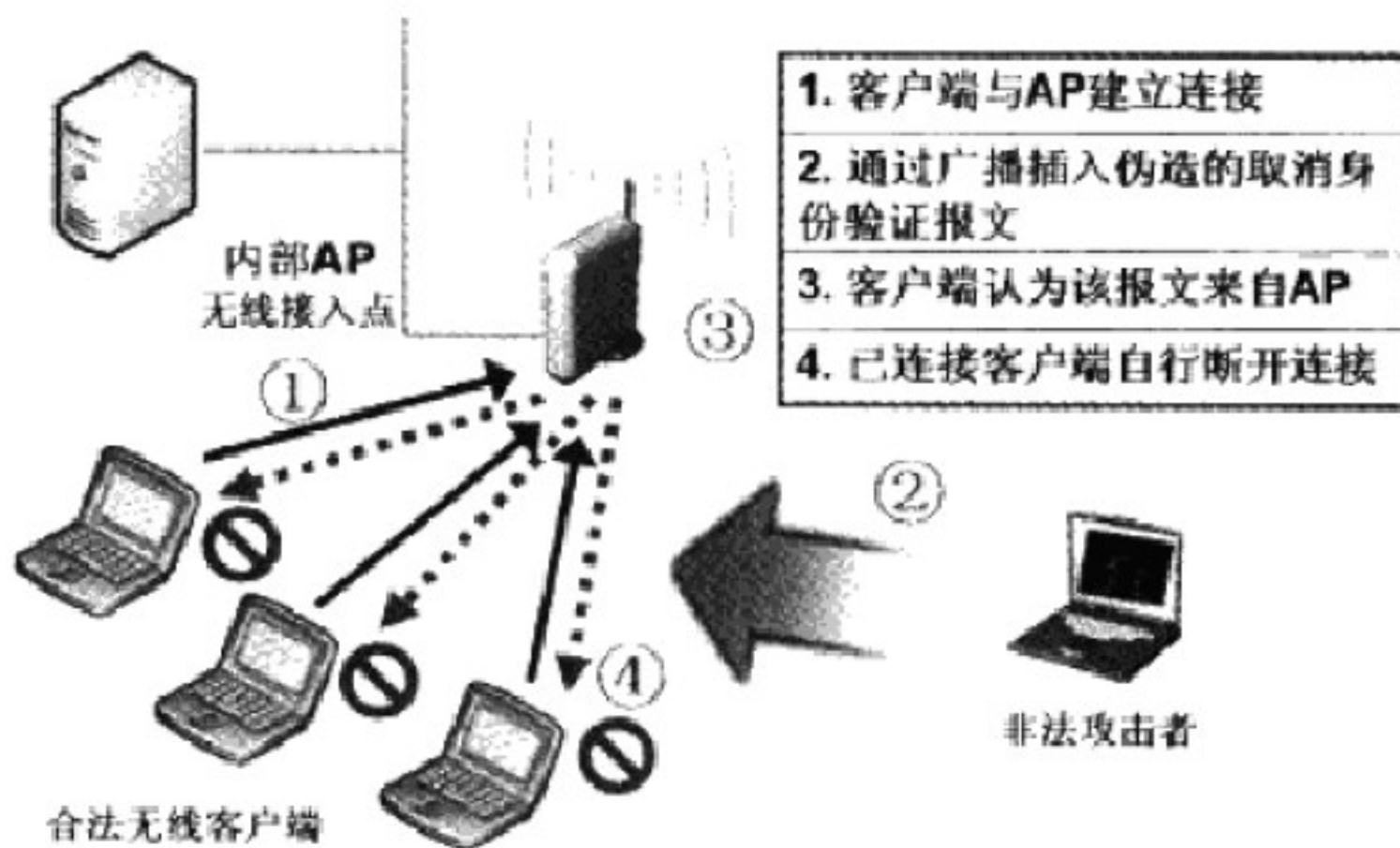
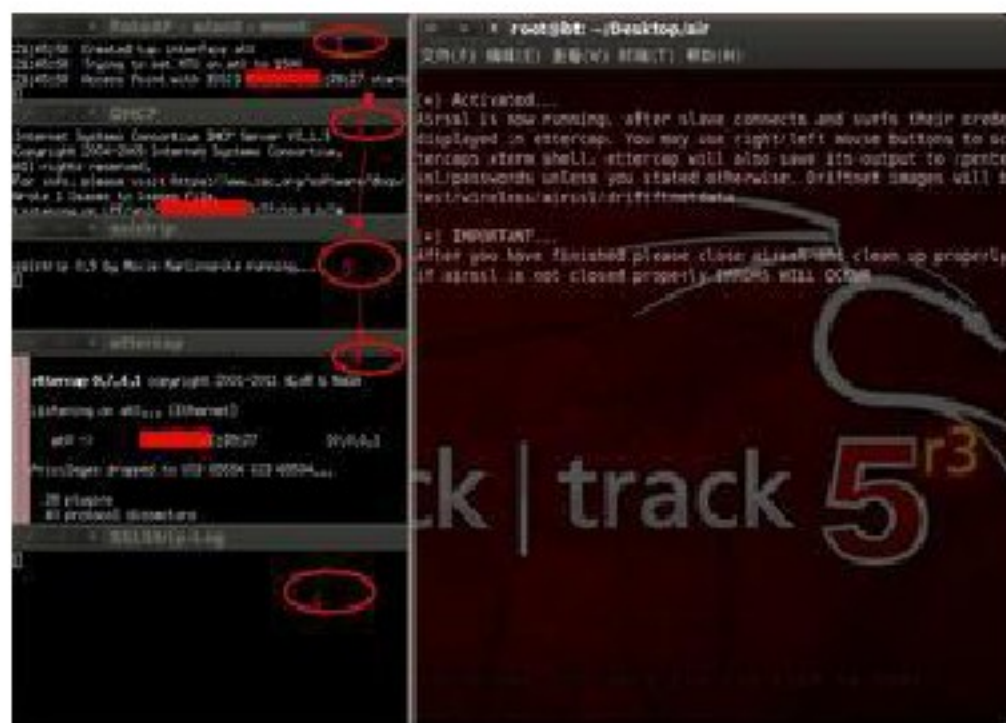


图 8-10 取消身份验证洪水攻击原理图

安全隐患

- 多种针对WiFi热点的攻击手段
 - 伪造AP攻击



Attacker



Wireless AP
+ Honeypot



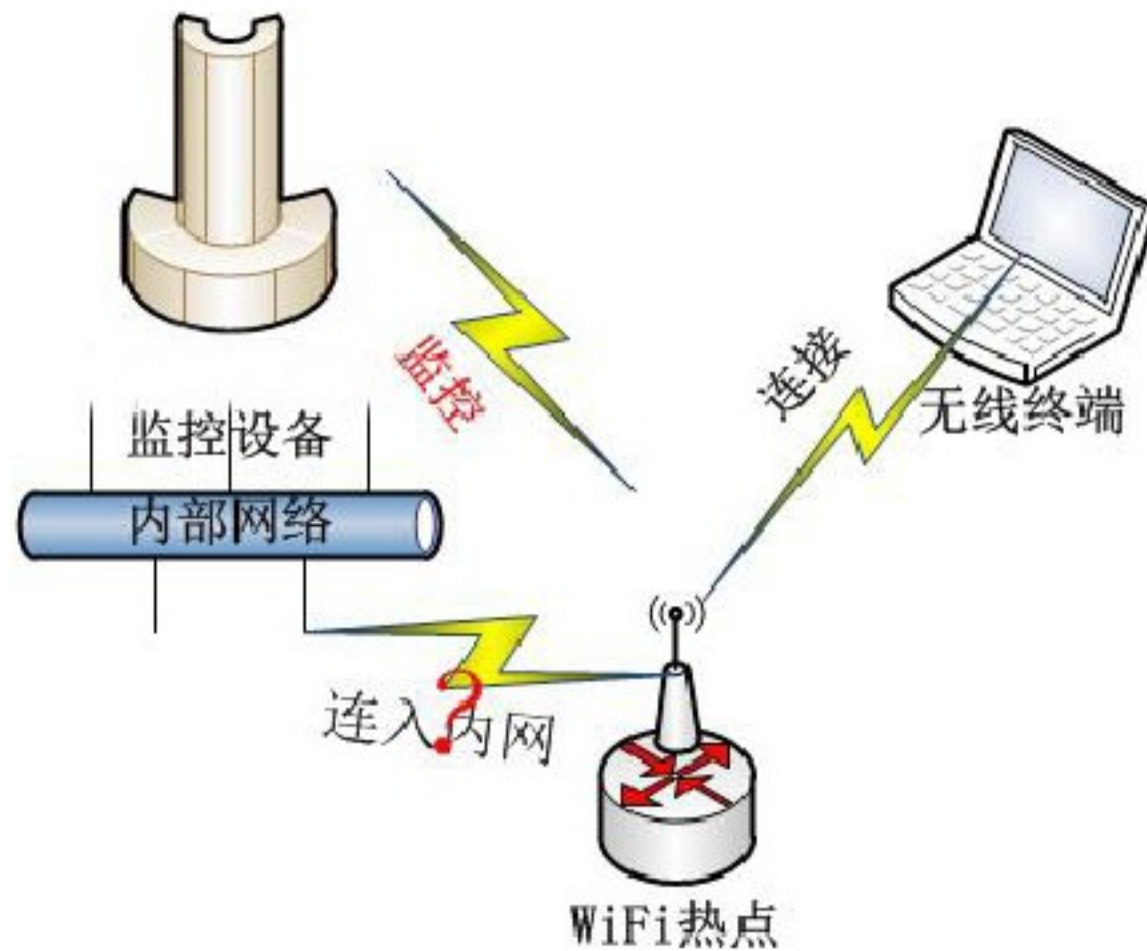
所有无线网络攻击要么是为了获得连接WiFi热点的授权、要么是连入WiFi热点以后继续攻击

应用场景

- 绝对禁止WiFi使用的安全区域（保密区域）
- 允许授权的WiFi热点开放，但不允许未授权无线终端接入网络的办公区域（一般有内外网分离的政府机构和公司）
- 允许安全的WiFi热点开放，但不允许不安全的WiFi热点开放的公共场所（机场、火车站等）

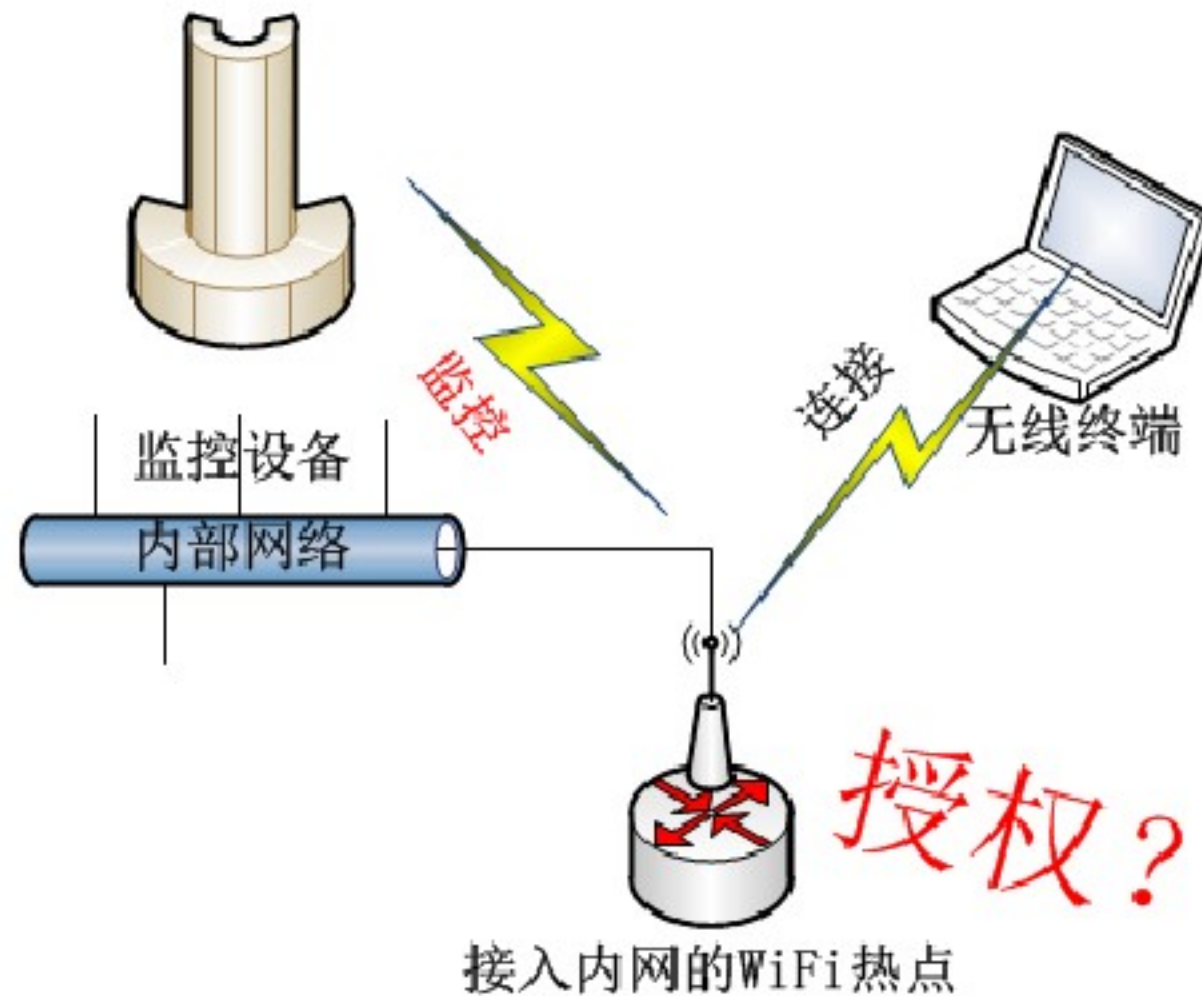
功能需求

- 判断WiFi热点是否接入内网，是否有无线终端通过WiFi热点接入内网



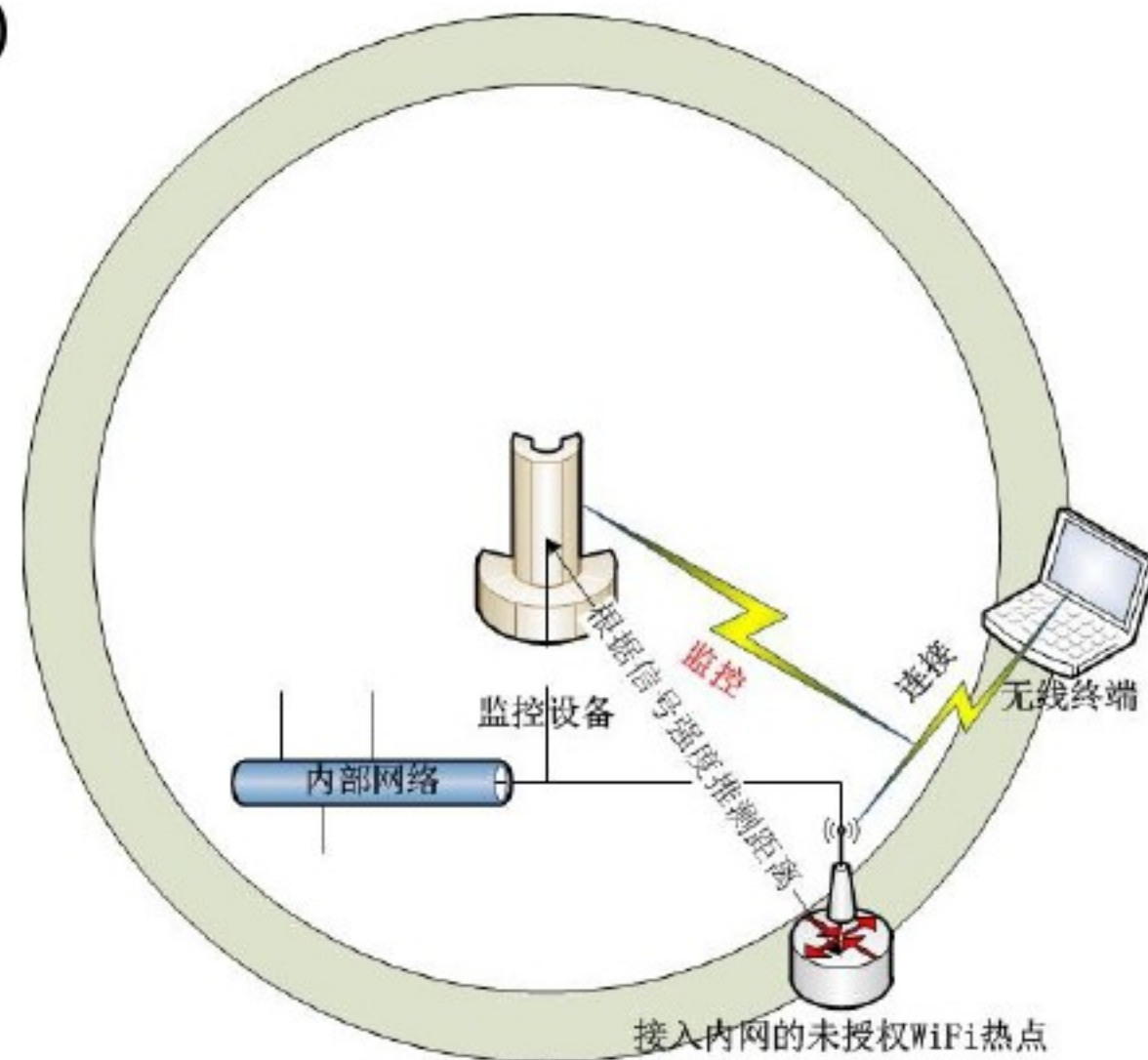
功能需求

- 对于接入内网的WiFi热点，区分出授权和未授权的WiFi热点



功能需求

- 定位未授权的WiFi热点（在极端情况下指所有接入内网的WiFi热点）



功能需求

- 阻止未授权的无线终端继续接入内网



产品的核心是围绕WiFi热点和连接在它们之上的无线终端进行监测



BlueSecurity

- **核心**: WiFi热点和无线终端管理
- **独创**非法接入内网的WiFi热点与随身WiFi检测技术
- **定位**: WiFi热点、无线终端和警报事件
- **阻断**: 断开未授权无线连接

监测

- 异常连接

定位

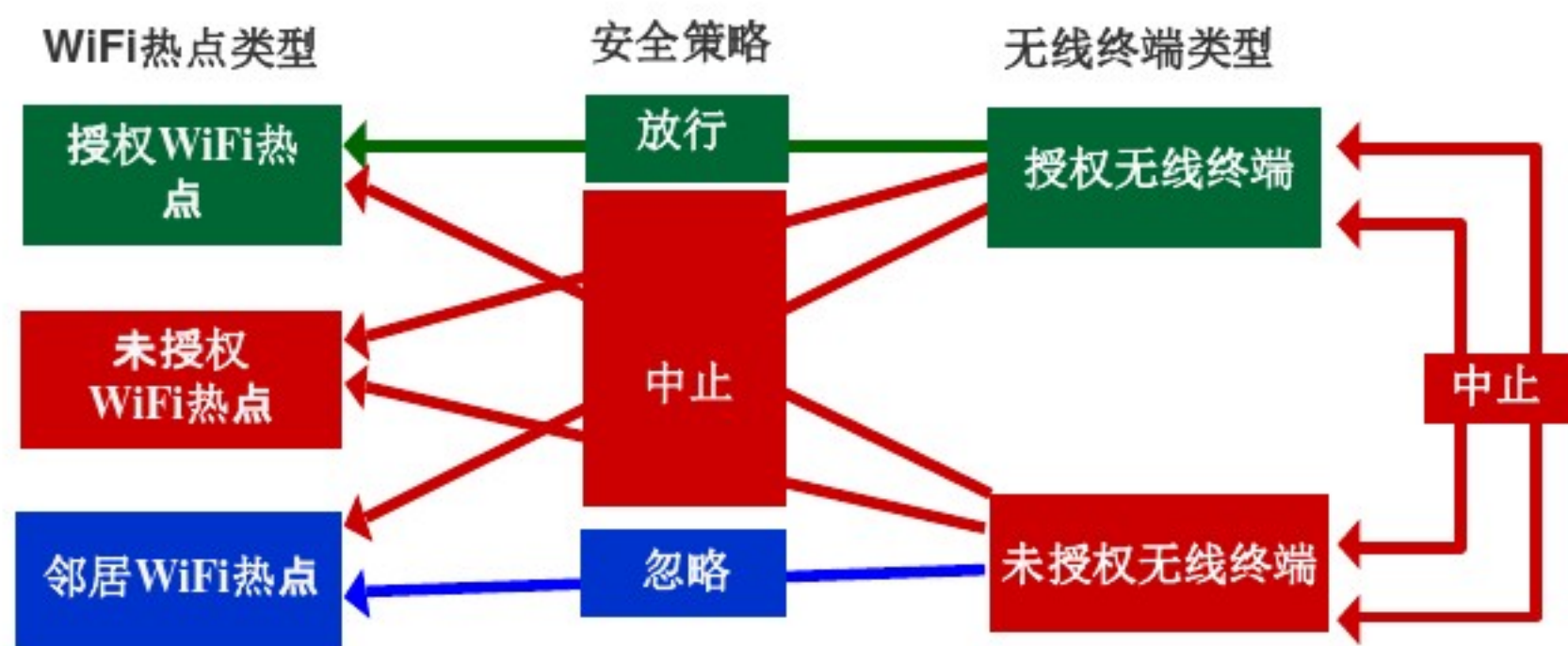
- 定位警报

阻断

- 自动阻断

BlueSecurity—无线设备管理

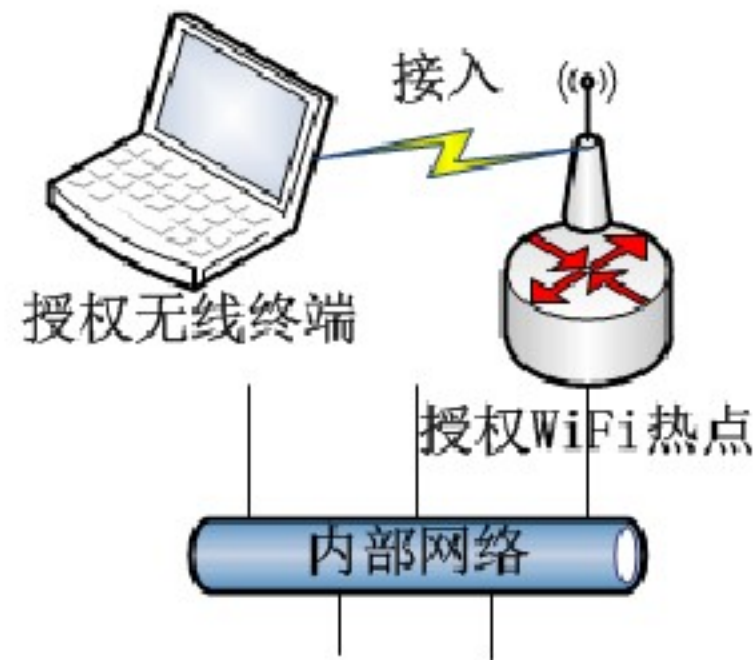
- 自动对检测到的WiFi热点和无线终端作出分类
- 围绕无线终端与WiFi热点的连接进行管理



BlueSecurity—异常事件检测

- 安全连接
 - 发现授权的WiFi热点连入内网发出提醒
 - 发现授权的无线终端连接授权的WiFi热点发出提醒

即使是安全连接，接入内网也需要提醒用户



BlueSecurity—异常事件检测

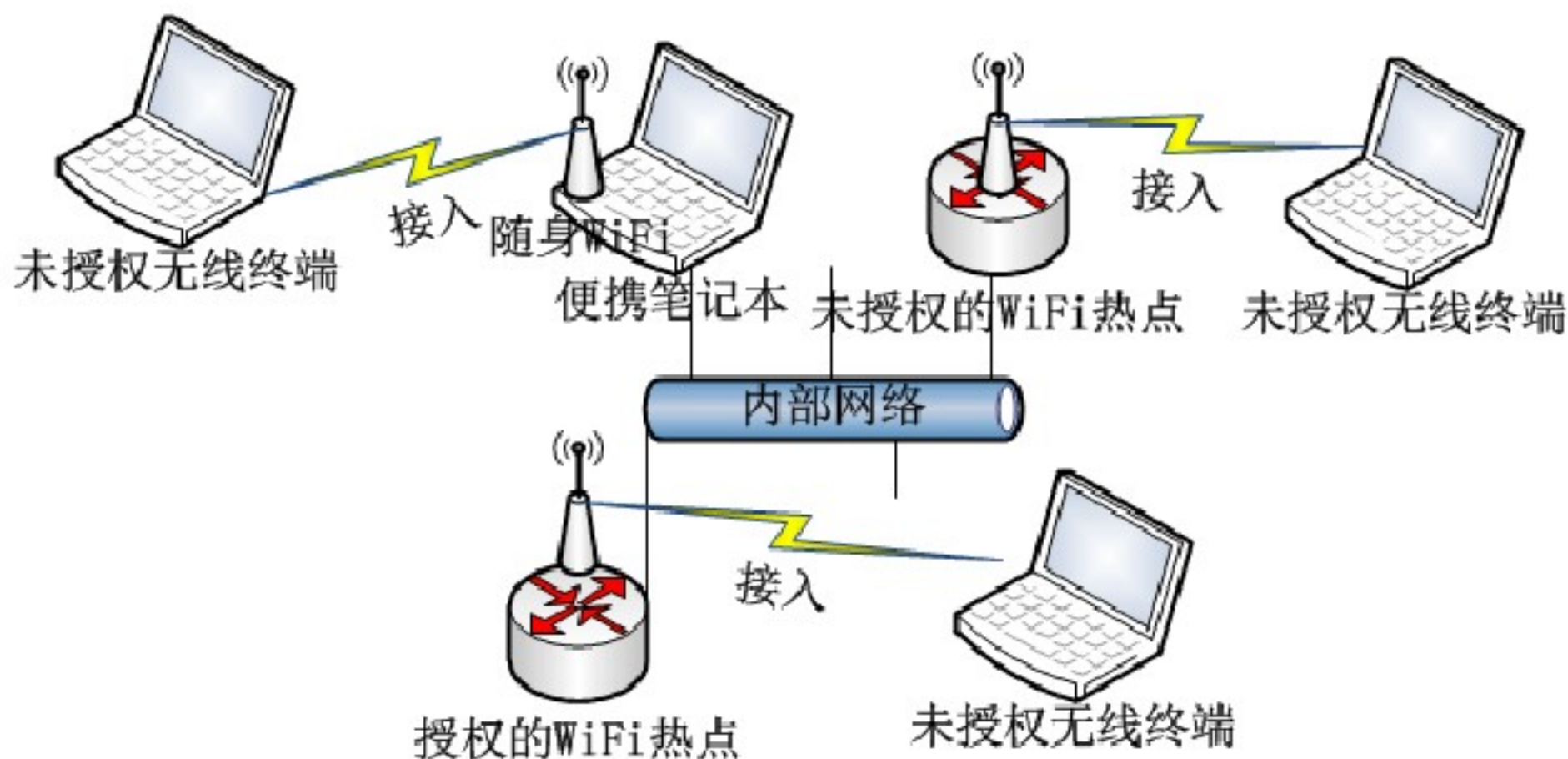
- 异常连接
 - 发现非授权的WiFi热点连入内网发出警报
 - NAT方式的WiFi热点和随身WiFi都可以隐藏内部网络信息
 - 独创的随身WiFi检测技术



BlueSecurity—异常事件检测

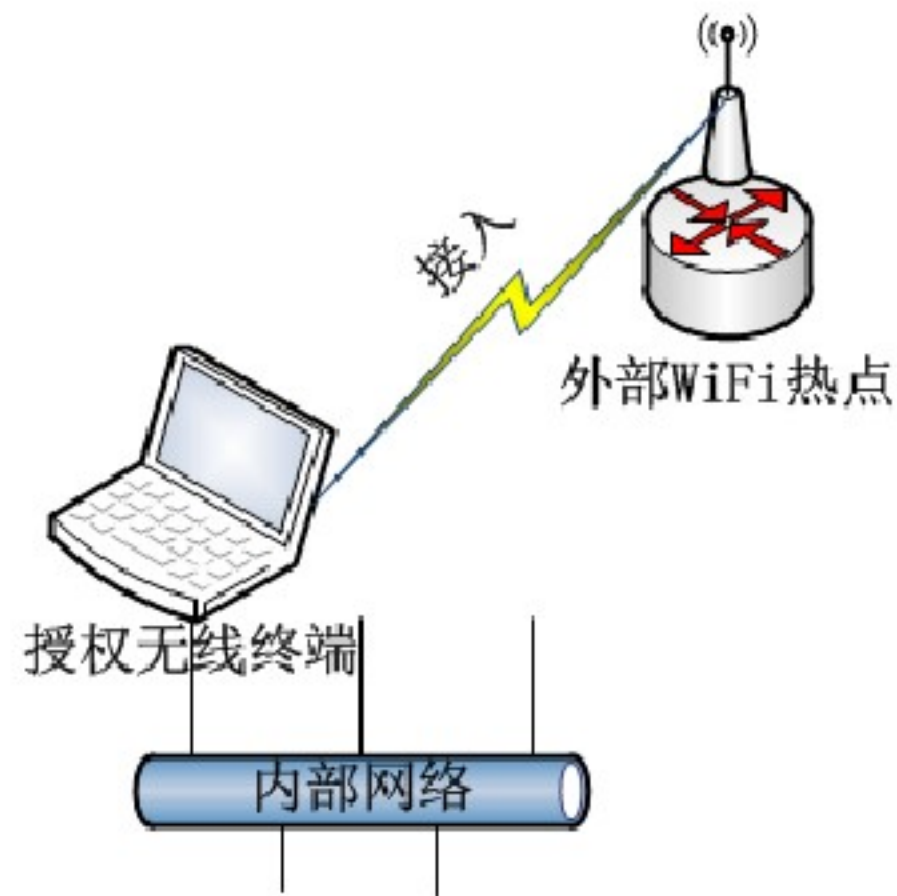
- 异常连接

- 发现非授权的无线终端连接已连入内网的WiFi热点发出警报
- 无论WiFi热点授权与否，都需要警报



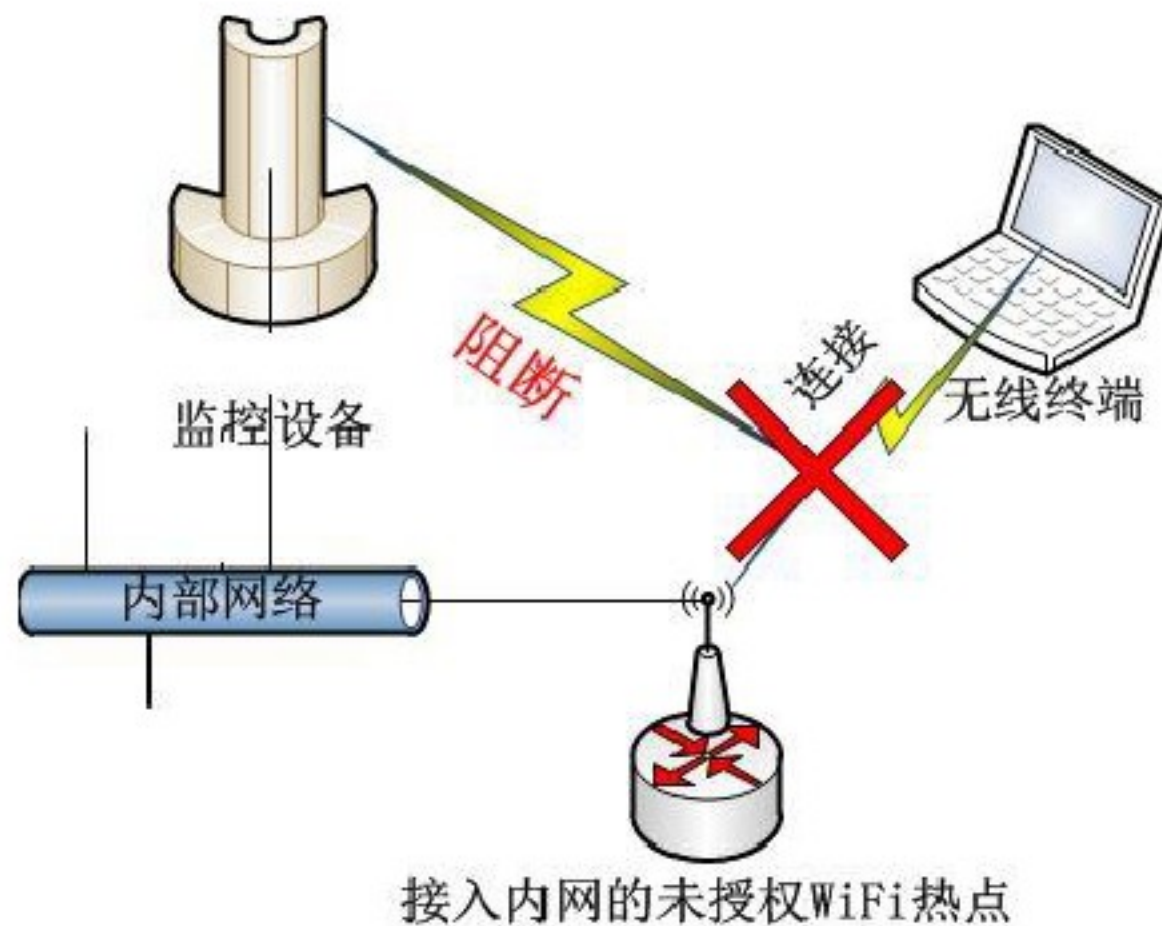
BlueSecurity—异常事件检测

- 异常连接
 - 发现授权的无线终端连接未授权的WiFi热点发出警报
 - 遭遇钓鱼攻击会出现此类情况



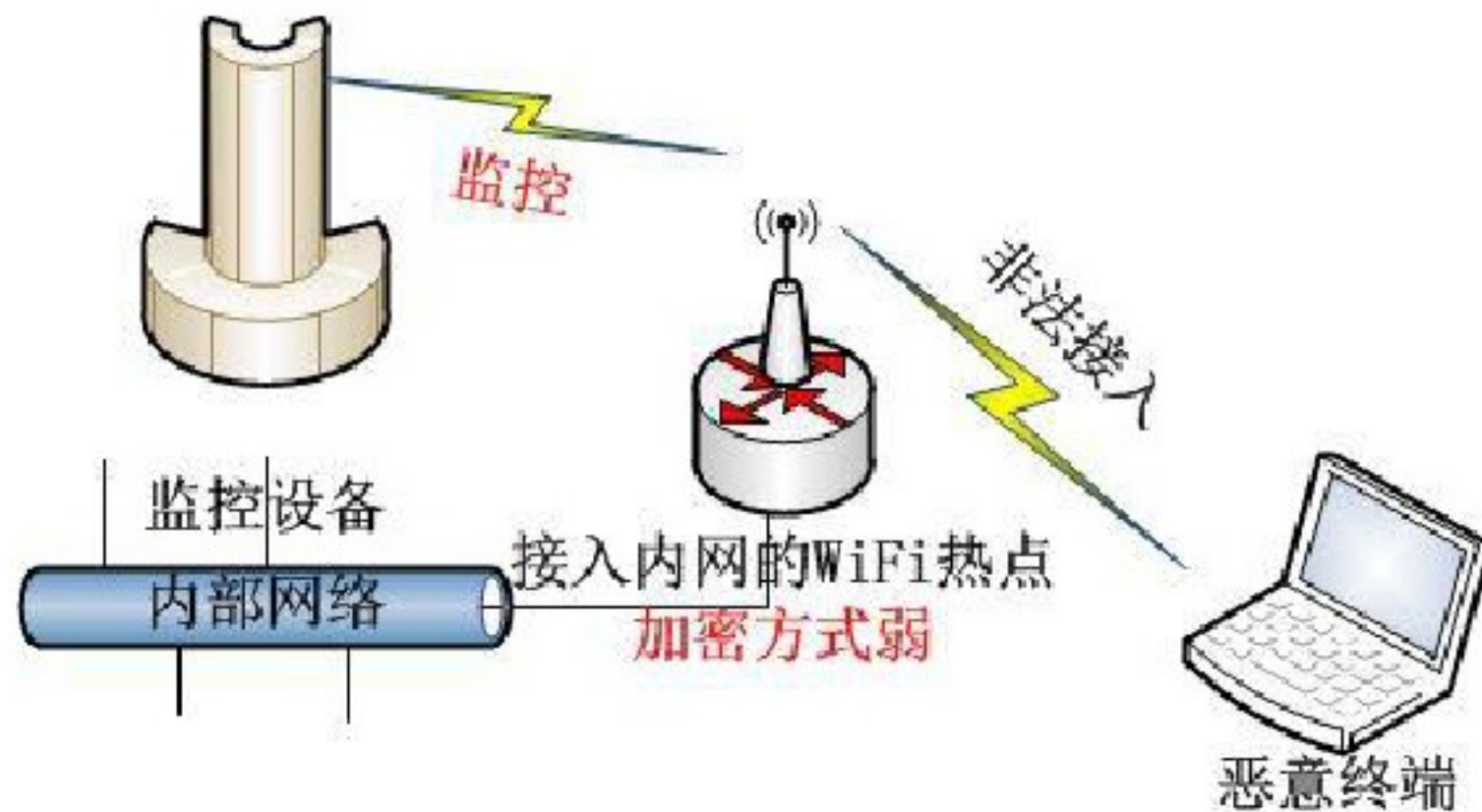
BlueSecurity—异常事件检测

- 漏洞提醒
 - 发现有弱加密的接入内网WiFi热点发出提醒
 - 易被破解，成为网络的漏洞



BlueSecurity—异常事件检测

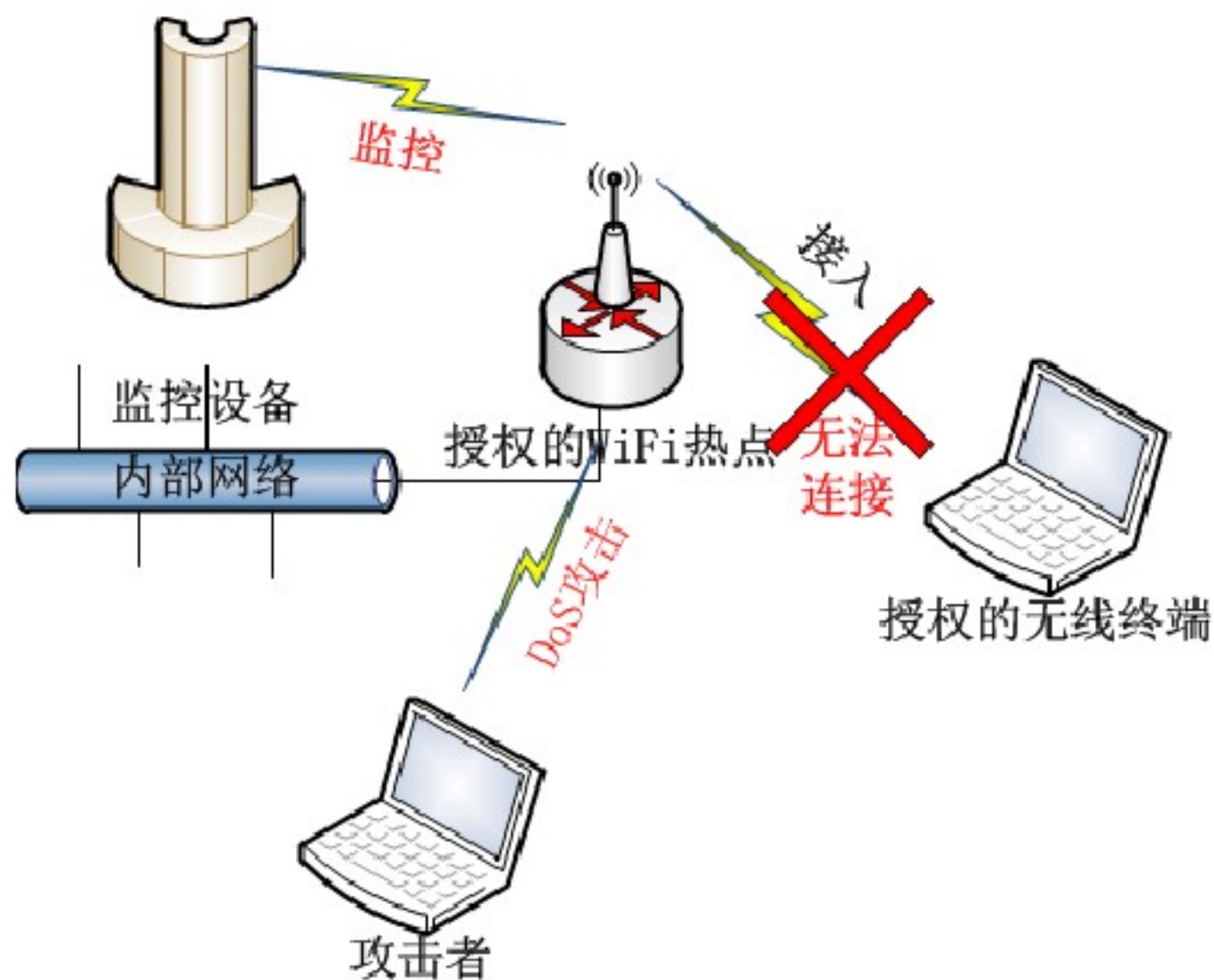
- 攻击警报
 - 发现有伪造的WiFi热点发出警报
 - 典型的钓鱼攻击场景



BlueSecurity—异常事件检测

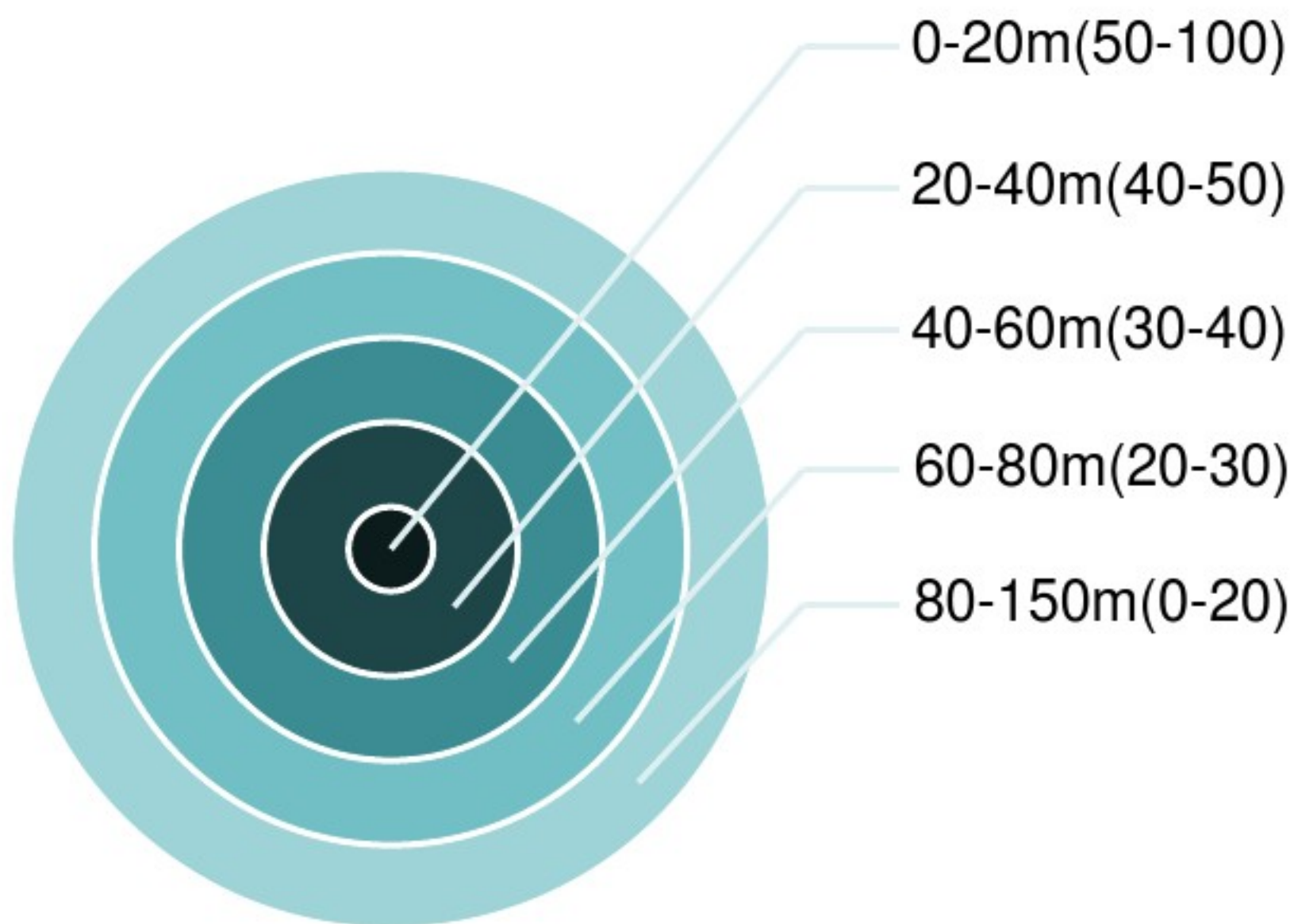
- 攻击警报

- 发现DoS攻击发出警报
- 可以瘫痪WiFi热点



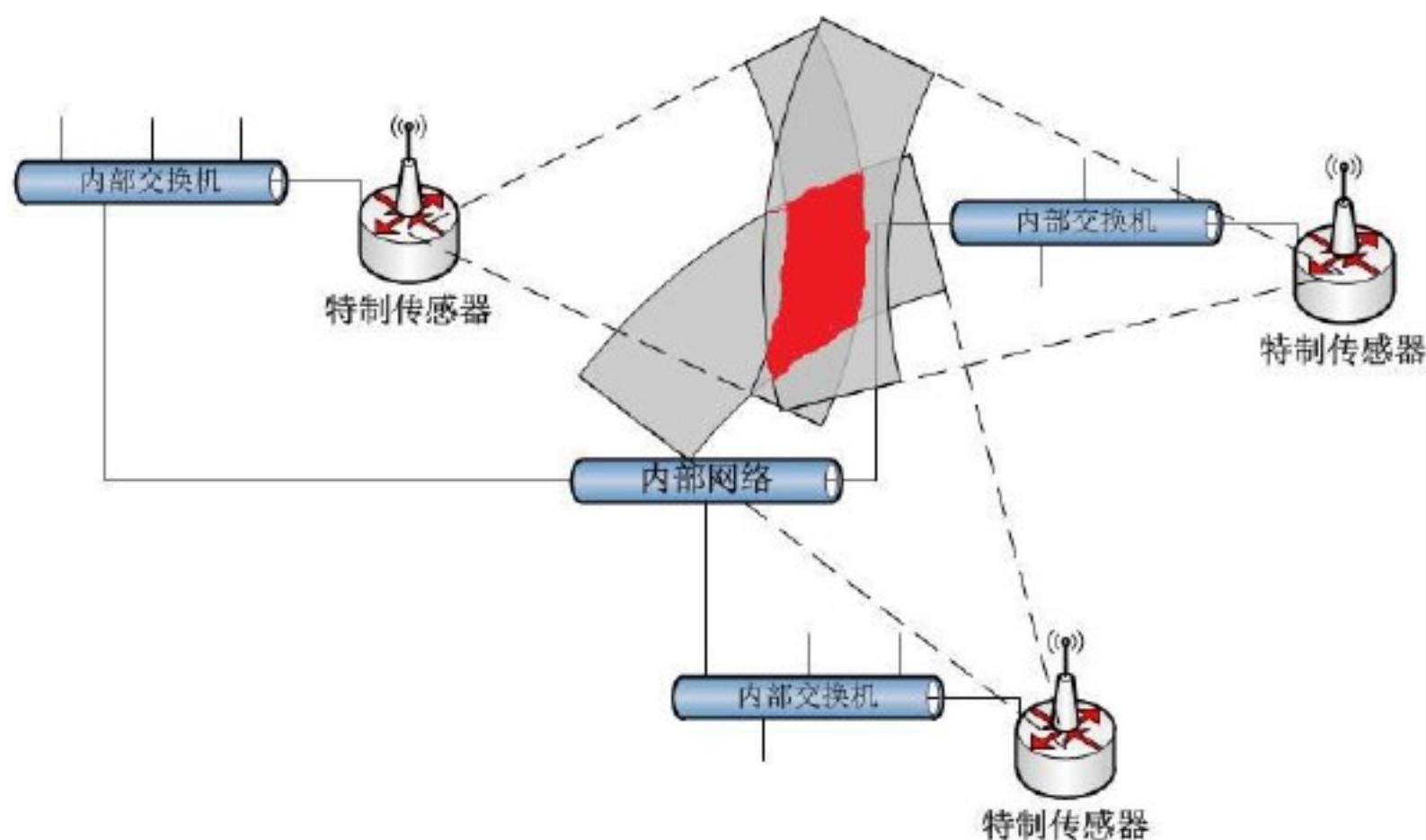
BlueSecurity—定位

- 在单点模式下通过信号强度计算大致的距离范围



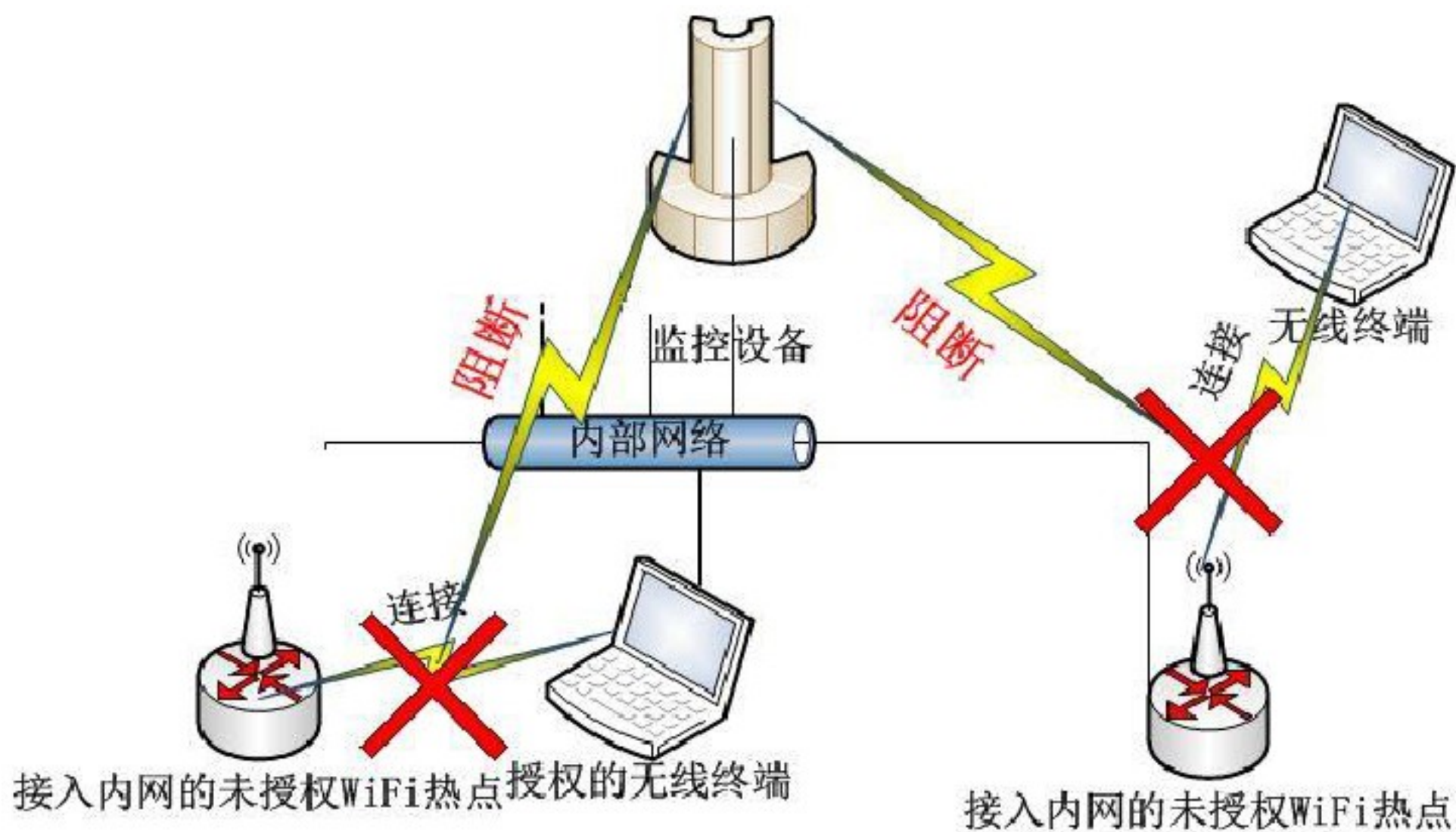
BlueSecurity—定位

- 在多点模式下综合计算进行定位
- 多个特制传感器测算距离范围得到结果进行重叠



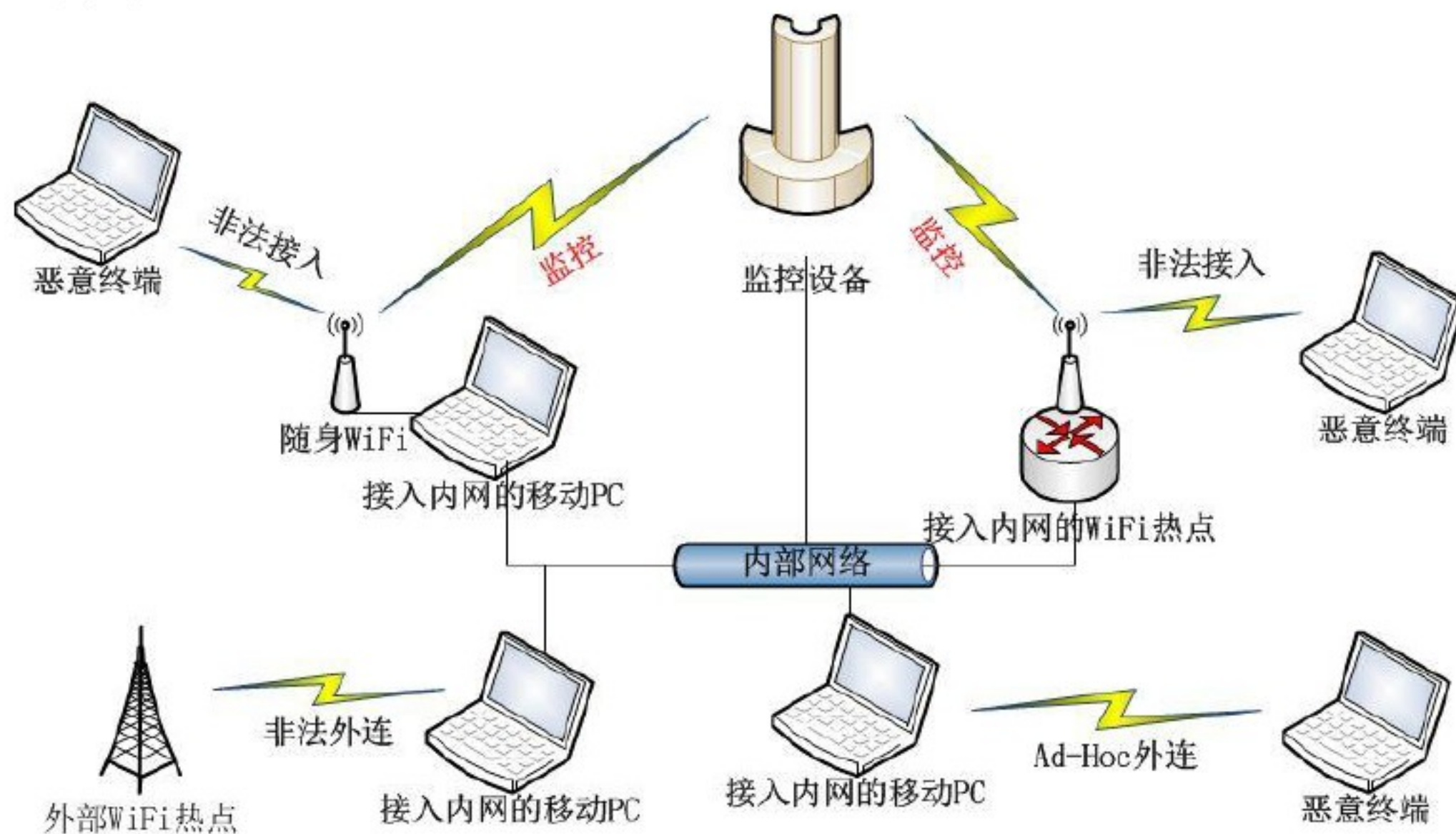
BlueSecurity—阻断

- 阻断是针对无线终端与WiFi热点的连接来实现的



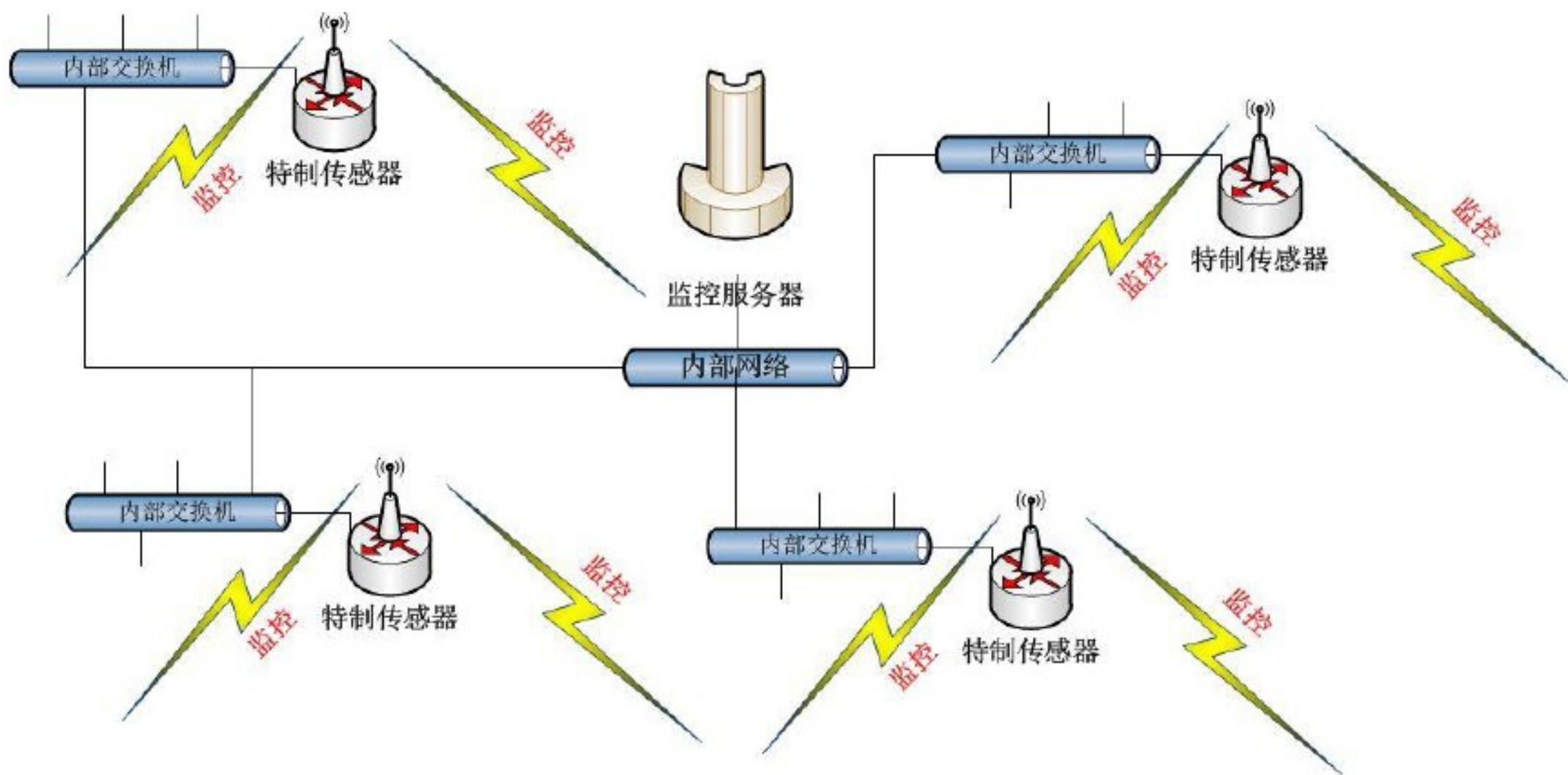
BlueSecurity—部署模式

单点模式是针对轻量级的应用环境，管理的空间小，设备少（如较大的空旷房间或者机密的小空间）



BlueSecurity—部署模式

多点模式将使用服务器处理信息，使用特制的传感器监测无线空间，可以弹性扩展，适合整个楼宇或者大面积室内区域的监控



BlueSecurity应用功能

- 检测接入内网的WiFi热点
- 检测随身WiFi
- 检测接入内网的无线终端
- 白名单
- 定位
- 阻断

检测接入内网WiFi

- 将WiFi热点A插入内网，配置IP地址
- 非法WiFi热点接入内网警报
- 使用无线终端，如手机接入WiFi热点A，
- 非法客户端接入内网警报

检测随身WiFi

- 将携带的随身WiFi B接入一台PC（已接入内网）
- 非法WiFi热点侵入报警
- 使用无线终端，如手机接入WiFi B，
- 非法客户端侵入提示报警

白名单功能

- 将WiFi热点A加入白名单
- 停止报警，且WiFi热点列表中归类发生变化
- 将接入WiFi热点A的终端加入白名单
- 提示新接入内网终端，不报警，无线终端列表发生变化

定位功能

- 将随身WiFi插入一台较远处的电脑
- 根据详细信息窗口中的信号强度和距离判断追踪
- 移动探测设备寻找随身WiFi

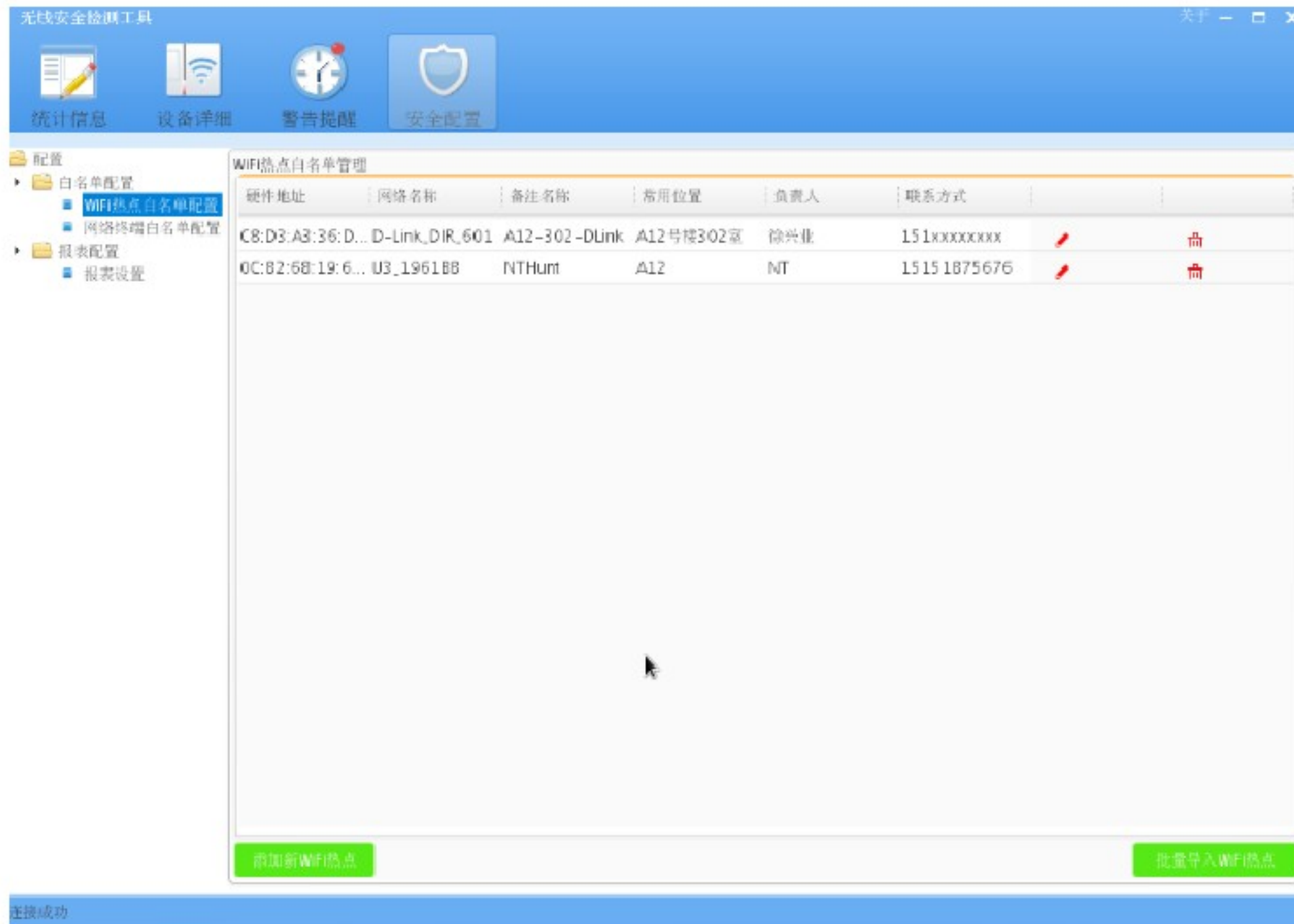
阻断功能

- 对随身WiFi发动阻断
- 无线终端无法连接到网络

运行抓图-主界面



运行抓图-安全配置



无线安全检测工具

统计信息 设备详细 警告提醒 安全配置

配置

- 白名单配置
 - WIFI热点白名单配置
 - 网络终端白名单配置
- 报表配置
 - 报表设置

WIFI热点白名单管理

硬件地址	网络名称	备注名称	常用位置	负责人	联系方式		
C8:D3:A3:36:D...	D-Link_DIR_601	A12-302-DLink	A12号楼302室	徐兴业	151xxxxxxx	✎	🔔
0C:82:68:19:6...	U3_1961BB	NTHum	A12	NT	1515 1875676	✎	🔔

添加新WIFI热点 批量导入WIFI热点

连接成功

运行抓图-热点接入的终端列表

The screenshot displays a software interface for wireless security. The main window is titled "无线安全检测工具" (Wireless Security Detection Tool). It features a top navigation bar with icons for "统计信息" (Statistics), "设备详细" (Device Details), "警告提醒" (Warning Alerts), and "安全配置" (Security Configuration). The central area shows a detailed view for a specific hotspot, "FAST_892350". Below this, there is a section titled "接入终端列表" (Connected Terminal List) which contains a table with the following data:

信号强度	备注名称	白名单	安全状况	最后出现时间	终端MAC地址	当前状态
13		不在白名单	外部可忽略	Tue Sep 16 09:26...	24:0A:64:74:D4:63	超时

On the left side of the interface, there is a vertical list of signal strength indicators, each represented by a bar chart and a numerical value. At the bottom left, a status bar indicates "连接成功" (Connection Successful). On the right side, there is a vertical list of MAC addresses, including :8A, :50, :3E, :A5, :9E, :98, :2A, :F1, :78, :D4, 28, :4C, 30, :74, :D9, and :E2.

运行抓图-热点设备的详情列表

无线安全检测工具

统计信息 设备详细 警告提醒 安全配置

刷新 查找: 刷新 隐藏无关设备

信号	信号强度	网络名称(SSID)	厂商	安全状况	加密方式	接入内网	白名单	信道	超时情况	MAC地址
	14	yoyo	Mercury_U3随身wifi	不安全	未知	接入内网	不在白名单	6(2.4G)	在线	0C:82:68:C7:A2:8A
	13	FAST_B92350	TP-LINK_TECHNOLOGIES_C...	外部可忽略	未知	未接入内网	不在白名单	11(2.4G)	在线	0C:72:2C:B9:23:50
	32	FAST_303	FAST_FWR310无线路由器	外部可忽略	未知	未接入内网	不在白名单	11(2.4G)	在线	C0:61:18:32:4C:3E
	17	FAST_204	TP-LINK_TECHNOLOGIES_C...	外部可忽略	未知	未接入内网	不在白名单	11(2.4G)	在线	AB:15:4D:A0:25:A6
	16	fanxd	TP-LINK_TECHNOLOGIES_C...	外部可忽略	未知	未接入内网	不在白名单	6(2.4G)	在线	0C:72:2C:F0:F6:9E
	15	ajyang	SHENZHEN_FAST_TECHNO...	外部可忽略	未知	未接入内网	不在白名单	11(2.4G)	在线	00:5A:39:2A:E6:98
	13	caocaocao	TP-LINK_Technologies_Co...	外部可忽略	未知	未接入内网	不在白名单	4(2.4G)	在线	E0:05:C5:36:68:2A
	50	SENSORDB2	NETGEAR	外部可忽略	未知	未接入内网	不在白名单	2(2.4G)	在线	E0:46:9A:53:56:F1
	32	Tenda_1E5878	Tenda_Technology_Co.,_Ltd.	外部可忽略	未知	未接入内网	不在白名单	1(2.4G)	在线	C8:3A:35:1E:5B:78
	31	aaronzhang	TP-LINK_TECHNOLOGIES_C...	外部可忽略	未知	未接入内网	不在白名单	6(2.4G)	在线	AB:15:4D:6B:96:D4
	19	MERCURY_69B328	TP-LINK_TECHNOLOGIES_C...	外部可忽略	未知	未接入内网	不在白名单	4(2.4G)	在线	54:E6:FC:69:83:28
	13	27-306	TP-LINK_TECHNOLOGIES_C...	外部可忽略	未知	未接入内网	不在白名单	11(2.4G)	在线	0C:72:2C:CF:F6:30
	18	TP-LINK_8974	TP-LINK_TECHNOLOGIES_C...	外部可忽略	未知	未接入内网	不在白名单	1(2.4G)	在线	E4:D3:32:9C:89:74
	60	360WIFI-8534	Intel_Corporate	外部可忽略	未知	未接入内网	不在白名单	11(2.4G)	在线	24:77:03:7D:08:D9

WIFI热点 无线终端

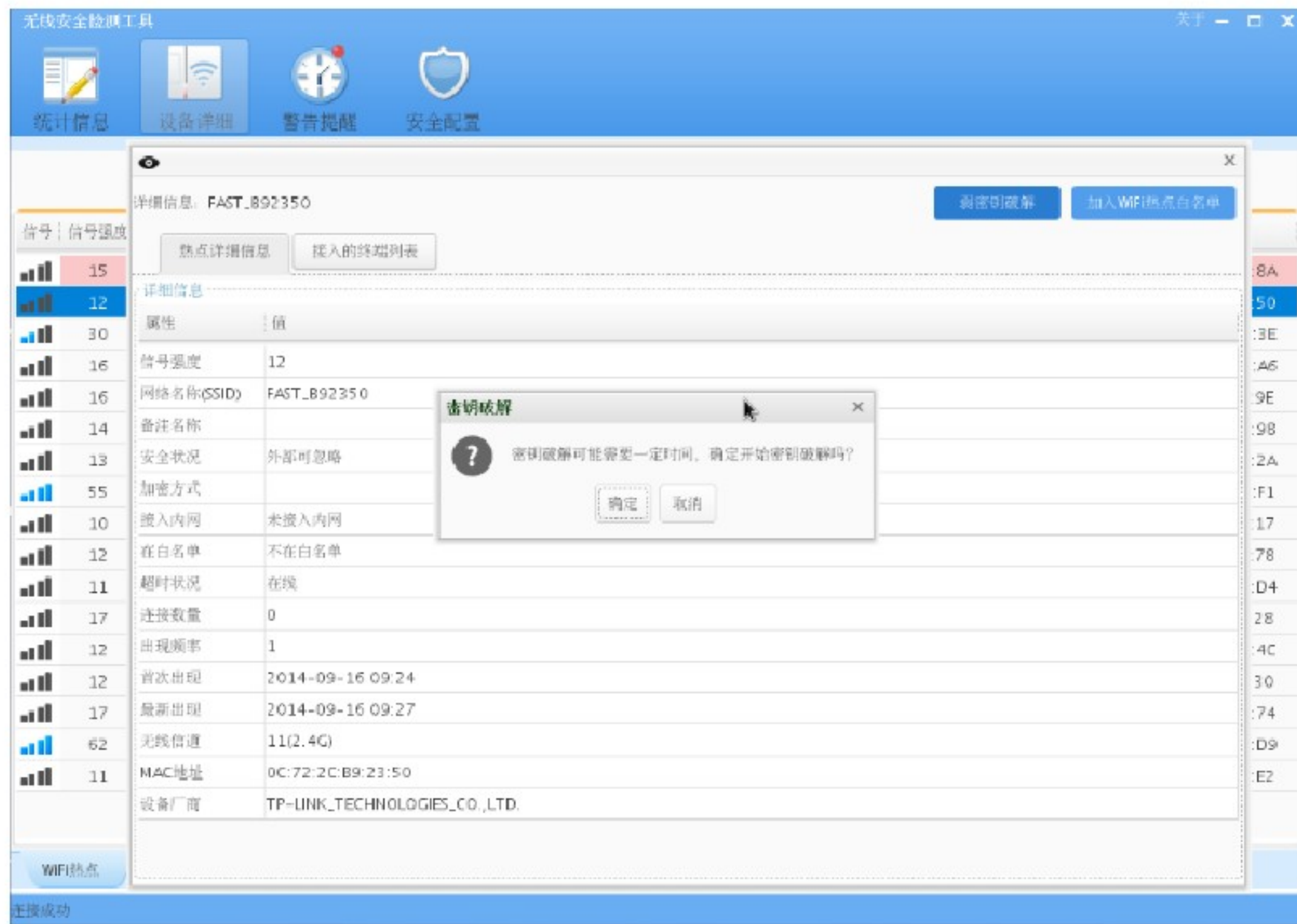
连接成功

运行抓图-热点的详情信息

The screenshot displays a software interface for wireless security analysis. The main window is titled '无线安全检测工具' (Wireless Security Detection Tool). It features a top navigation bar with icons for '统计信息' (Statistics), '设备详细' (Device Details), '警告提醒' (Warning Alerts), and '安全配置' (Security Configuration). A central pane shows the '详细信息: FAST_B92350' (Detailed Information: FAST_B92350) for a selected hotspot. This pane includes buttons for '热点详细信息' (Hotspot Detailed Information) and '接入的终端列表' (List of Connected Devices). A table below provides specific details for the hotspot, such as signal strength, SSID, security status, and MAC address. On the left, a '信号 | 信号强度' (Signal | Signal Strength) section shows a list of detected hotspots with their respective signal levels. On the right, a vertical list of MAC addresses is visible. At the bottom, a blue bar indicates '连接成功' (Connection Successful).

属性	值
信号强度	12
网络名称(SSID)	FAST_B92350
备注名称	
安全状况	外部可忽略
加密方式	
接入内网	未接入内网
在白名单	不在白名单
超时状况	在线
连接数量	0
出现频率	1
首次出现	2014-09-16 09:24
最新出现	2014-09-16 09:27
无线信道	11(2.4G)
MAC地址	0C:72:2C:B9:23:50
设备厂商	TP-LINK_TECHNOLOGIES_CO.,LTD.

运行抓图-弱密钥破解的界面



运行抓图-自定义弱密钥的破解界面

The screenshot displays a software interface for wireless security testing. At the top, there are navigation icons for '统计信息' (Statistics), '设备详细' (Device Details), '警告提醒' (Warning Alerts), and '安全配置' (Security Configuration). Below these is a search bar with a '弱密钥破解' (Weak Password Cracking) button and a '隐藏无关设备' (Hide Irrelevant Devices) button. The main area is a table listing detected wireless networks with columns for signal strength, SSID, manufacturer, security status, encryption, network type, whitelist status, channel, timeout, and MAC address. A dialog box is overlaid on the table, prompting the user to enter the network name and channel for password cracking. The dialog box contains the following text and fields:

请输入需要破解的网络标识及所在信道

热点MAC地址:

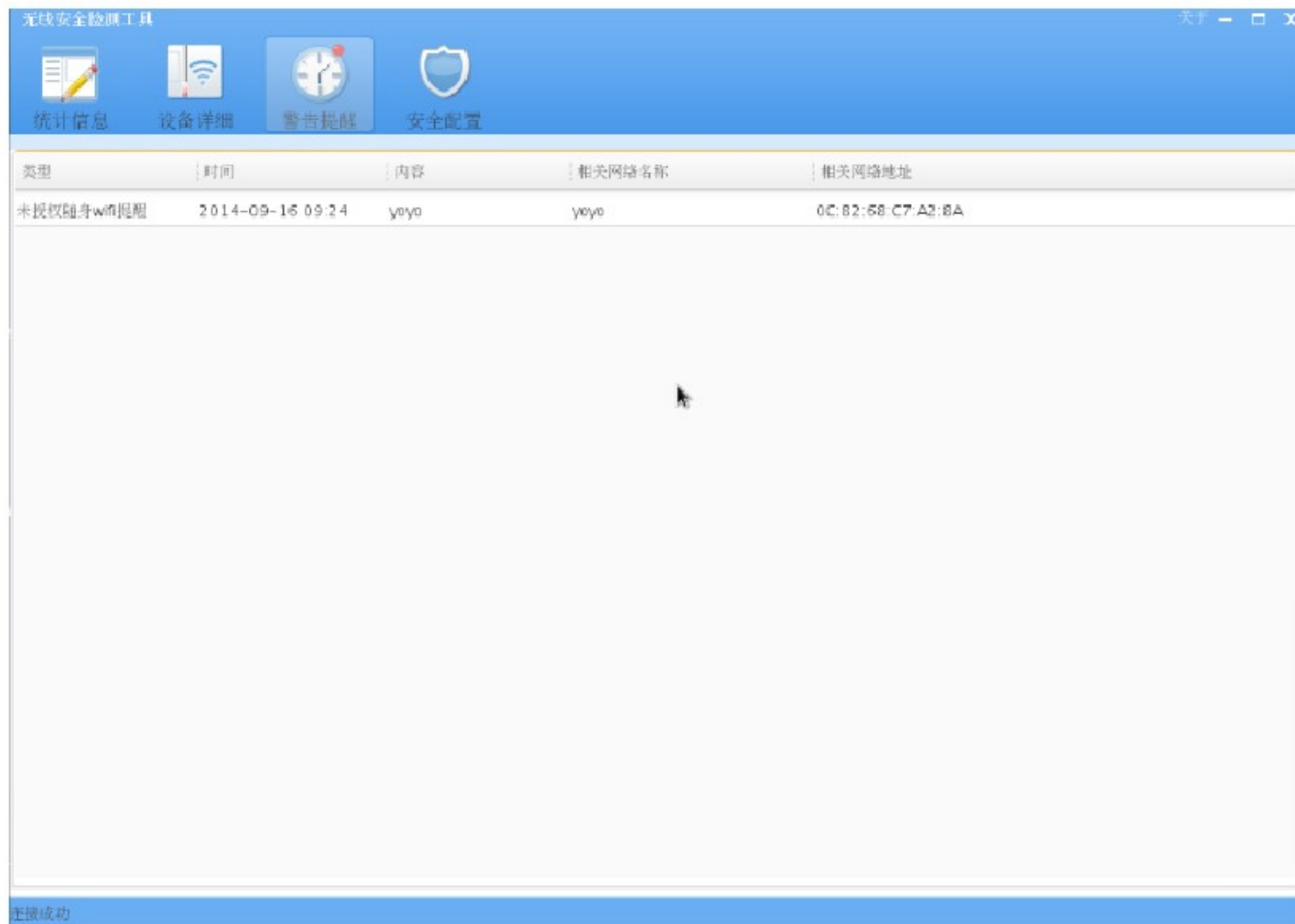
热点所在信道:

开始破解 取消破解

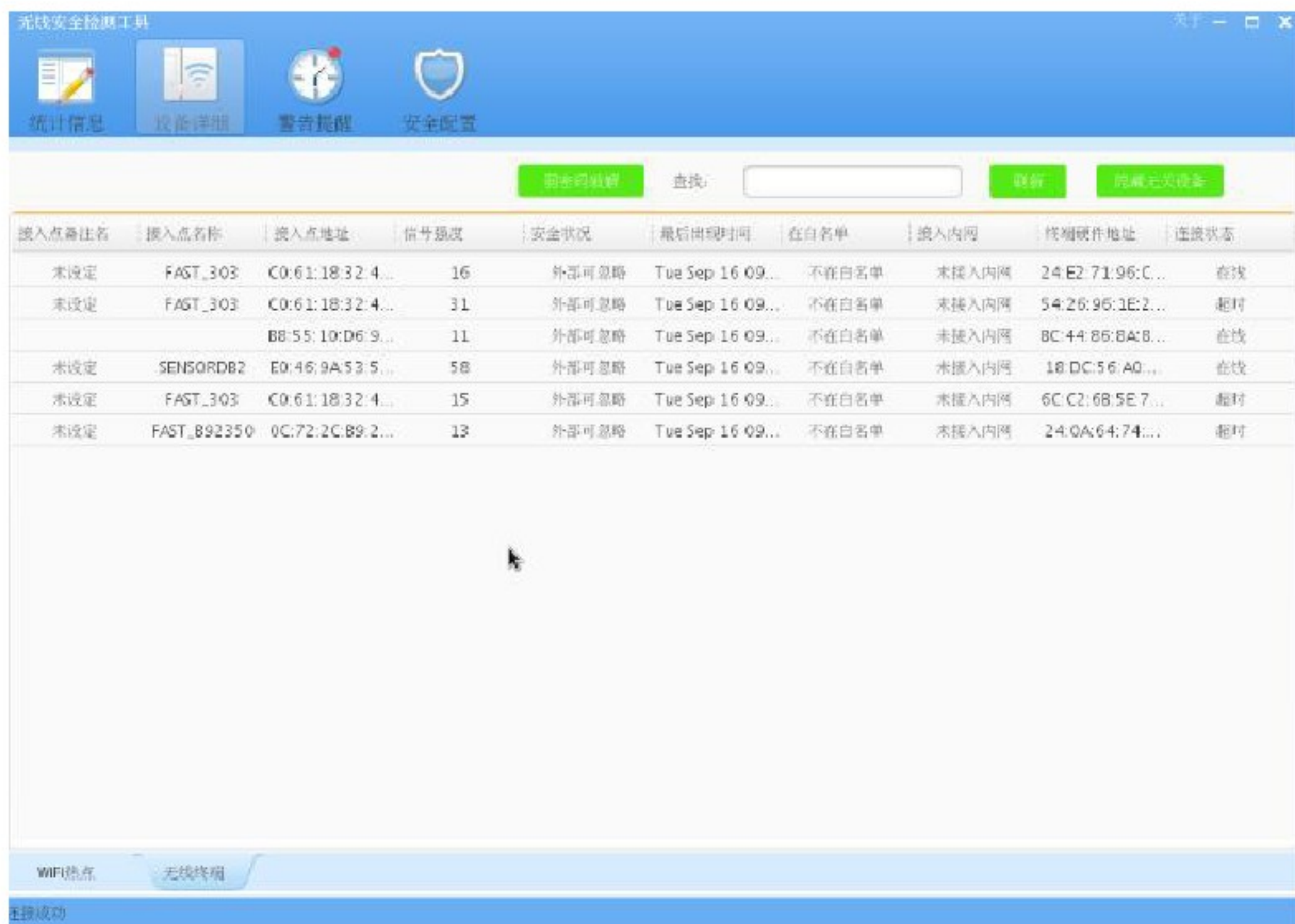
信号	信号强度	网络名称(SSID)	厂商	安全状况	加密方式	接入内网	白名单	信道	超时情况	MAC地址
📶	16	yoyo	Mercury_U3随身wifi	不安全	未知	接入内网	不在白名单	6(2.4G)	在线	0C:82:68:C7:A2:8A
📶	12	FAST_B92350	TP-LINK_TECHNOLOGIES_C...	外部可忽略	未知	未接入内网	不在白名单	11(2.4G)	在线	0C:72:2C:B9:23:50
📶	33	FAST_303	FAST_FWR310无线路由器	外部可忽略	未知	未接入内网	不在白名单	11(2.4G)	在线	00:61:18:32:4C:3E
📶	18	FAST_204	TP-LINK_TECHNOLOGIES_C...	外部可忽略	未知	未接入内网	不在白名单	11(2.4G)	在线	AB:15:4D:A0:25:A6
📶	15	fanxd	TP-				不在白名单	6(2.4G)	在线	0C:72:2C:F0:F6:9E
📶	15	ajyang	SHE				不在白名单	11(2.4G)	在线	00:5A:39:2A:E6:9B
📶	13	caocaocao	TP-				不在白名单	4(2.4G)	在线	E0:05:C5:36:68:2A
📶	60	SENSORDB2					不在白名单	2(2.4G)	在线	E0:46:9A:53:56:F1
📶	10	ChinaNet-rthU	HUA				不在白名单	2(2.4G)	超时	4C:1F:CC:BD:94:17
📶	12	Tenda_1E5878	Tenda_Technology,Co.,,Ltd.	外部可忽略	未知	未接入内网	不在白名单	1(2.4G)	在线	C8:3A:35:1E:58:78
📶	11	xiaoyuan-330301	TP-LINK_TECHNOLOGIES_C...	外部可忽略	未知	未接入内网	不在白名单	5(2.4G)	超时	9C:21:6A:7C:6E:0E
📶	11	aaronzhang	TP-LINK_TECHNOLOGIES_C...	外部可忽略	未知	未接入内网	不在白名单	6(2.4G)	超时	AB:15:4D:6B:96:D4
📶	17	MERCURY_69B32B	TP-LINK_TECHNOLOGIES_C...	外部可忽略	未知	未接入内网	不在白名单	4(2.4G)	在线	54:E6:FC:69:83:28
📶	12	ChinaNet-rthU	Zioncom_Electronics_(Shen...	外部可忽略	未知	未接入内网	不在白名单	2(2.4G)	超时	B8:55:10:D6:94:4C
📶	11	27-306	TP-LINK_TECHNOLOGIES_C...	外部可忽略	未知	未接入内网	不在白名单	11(2.4G)	超时	0C:72:2C:CF:F6:30
📶	18	TP-LINK_8974	TP-LINK_TECHNOLOGIES_C...	外部可忽略	未知	未接入内网	不在白名单	1(2.4G)	在线	E4:D3:32:9C:89:74
📶	59	360WIFI-8534	Intel_Corporate	外部可忽略	未知	未接入内网	不在白名单	11(2.4G)	在线	24:77:03:7D:08:D9
📶	11	jingxiaomeng	D-Link_Corporation	外部可忽略	未知	未接入内网	不在白名单	11(2.4G)	在线	34:08:04:C1:58:E2

At the bottom of the interface, there are tabs for 'WIFI热点' (WIFI Hotspots) and '无线终端' (Wireless Terminals), and a status bar indicating '连接成功' (Connection Successful).

运行抓图-未授权随身WiFi接入警告



运行抓图-无线网络终端的设备详情



The screenshot shows a software interface titled "无线安全检测工具" (Wireless Security Detection Tool). It features a navigation bar with icons for "统计信息" (Statistics), "设备详情" (Device Details), "警告提醒" (Warning Alerts), and "安全配置" (Security Configuration). Below the navigation bar, there are buttons for "刷新数据" (Refresh Data), a search input field, and buttons for "刷新" (Refresh) and "隐藏无关设备" (Hide Irrelevant Devices). The main area contains a table with the following columns: "接入点备注名" (Access Point Remark Name), "接入点名称" (Access Point Name), "接入点地址" (Access Point Address), "信号强度" (Signal Strength), "安全状况" (Security Status), "最后出现时间" (Last Appearance Time), "在白名单" (In Whitelist), "接入内网" (Access Intranet), "物理硬件地址" (Physical Hardware Address), and "连接状态" (Connection Status). The table lists several devices with their respective details.

接入点备注名	接入点名称	接入点地址	信号强度	安全状况	最后出现时间	在白名单	接入内网	物理硬件地址	连接状态
未设定	FAST_303	C0:61:18:32:4...	16	外部可忽略	Tue Sep 16 09...	不在白名单	未接入内网	24:E2:71:96:C...	在线
未设定	FAST_303	C0:61:18:32:4...	31	外部可忽略	Tue Sep 16 09...	不在白名单	未接入内网	54:26:95:1E:2...	离线
		B8:55:10:D6:9...	11	外部可忽略	Tue Sep 16 09...	不在白名单	未接入内网	BC:44:86:8A:8...	在线
未设定	SENSORDB2	E0:46:9A:53:5...	58	外部可忽略	Tue Sep 16 09...	不在白名单	未接入内网	18:DC:56:A0...	在线
未设定	FAST_303	C0:61:18:32:4...	15	外部可忽略	Tue Sep 16 09...	不在白名单	未接入内网	6C:C2:68:5E:7...	离线
未设定	FAST_B92350	0C:72:2C:89:2...	13	外部可忽略	Tue Sep 16 09...	不在白名单	未接入内网	24:0A:64:74...	离线

At the bottom of the interface, there are tabs for "WiFi热点" (WiFi Hotspot) and "无线终端" (Wireless Terminal), with "无线终端" currently selected. A status bar at the very bottom indicates "连接成功" (Connection Successful).