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

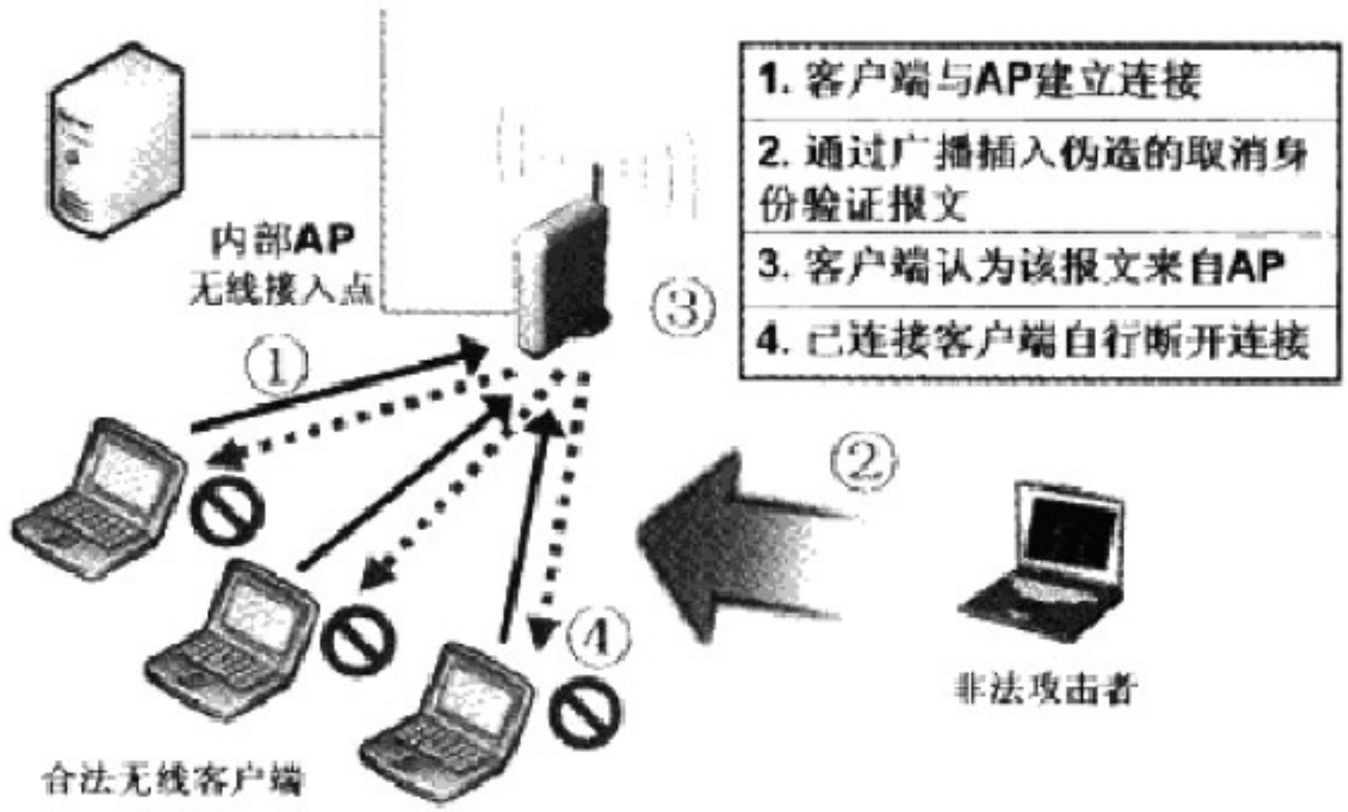
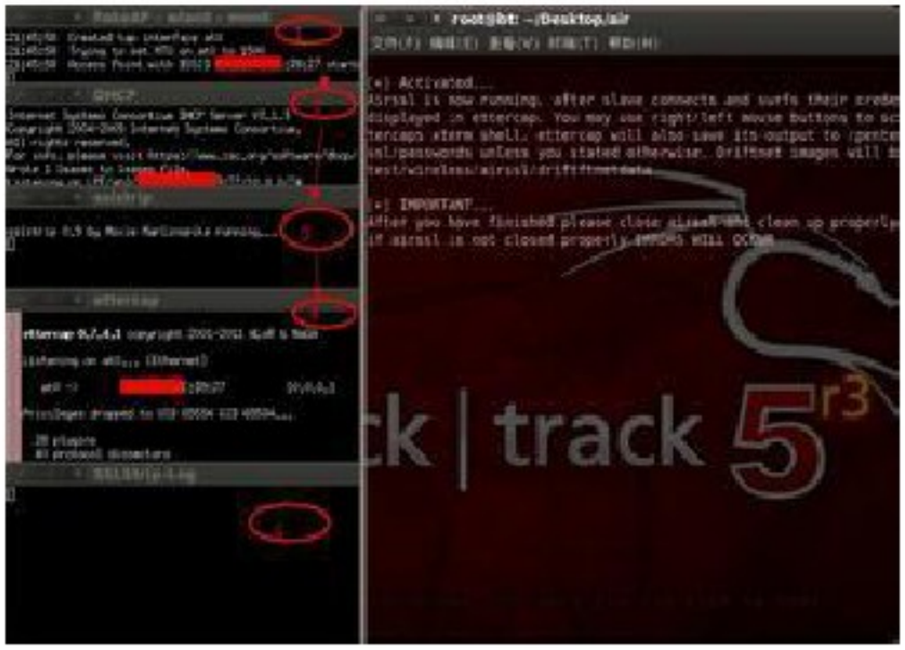


图 8-10 取消身份验证洪水攻击原理图

安全隐患

- 多种针对WiFi热点的攻击手段
  - 伪造AP攻击



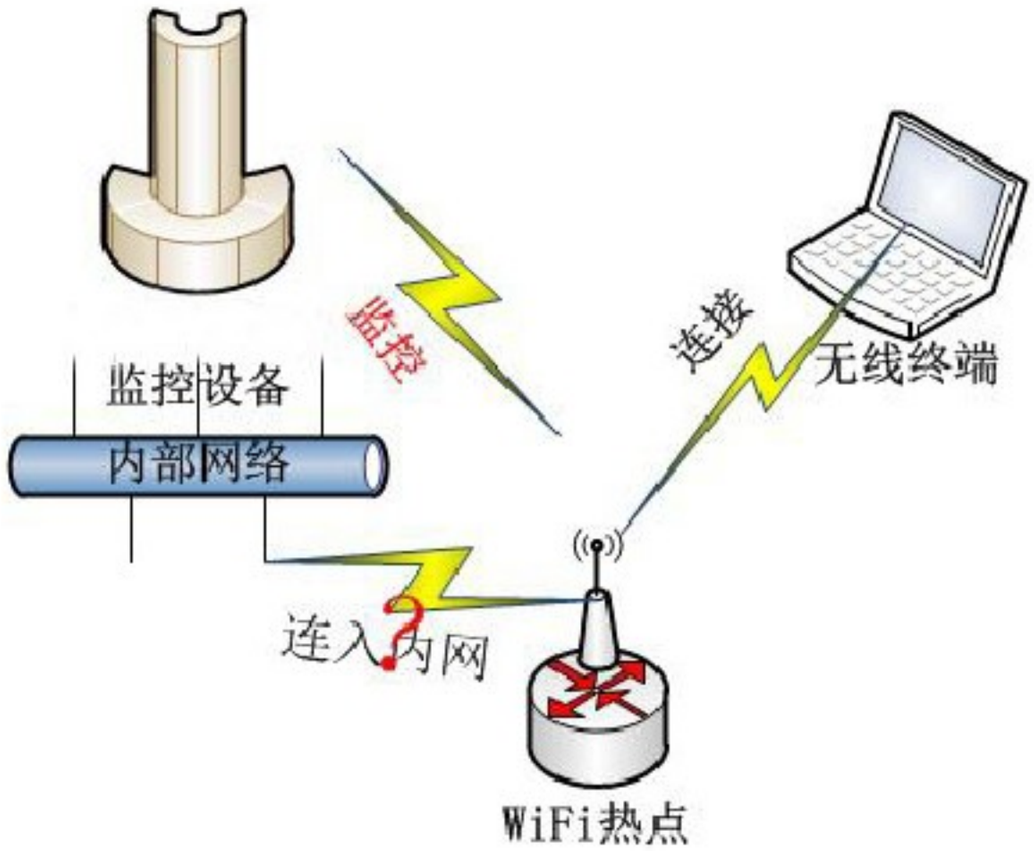
所有无线网络攻击要么是为了获得连接WiFi热点的授权、要么是连入WiFi热点以后继续攻击

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）

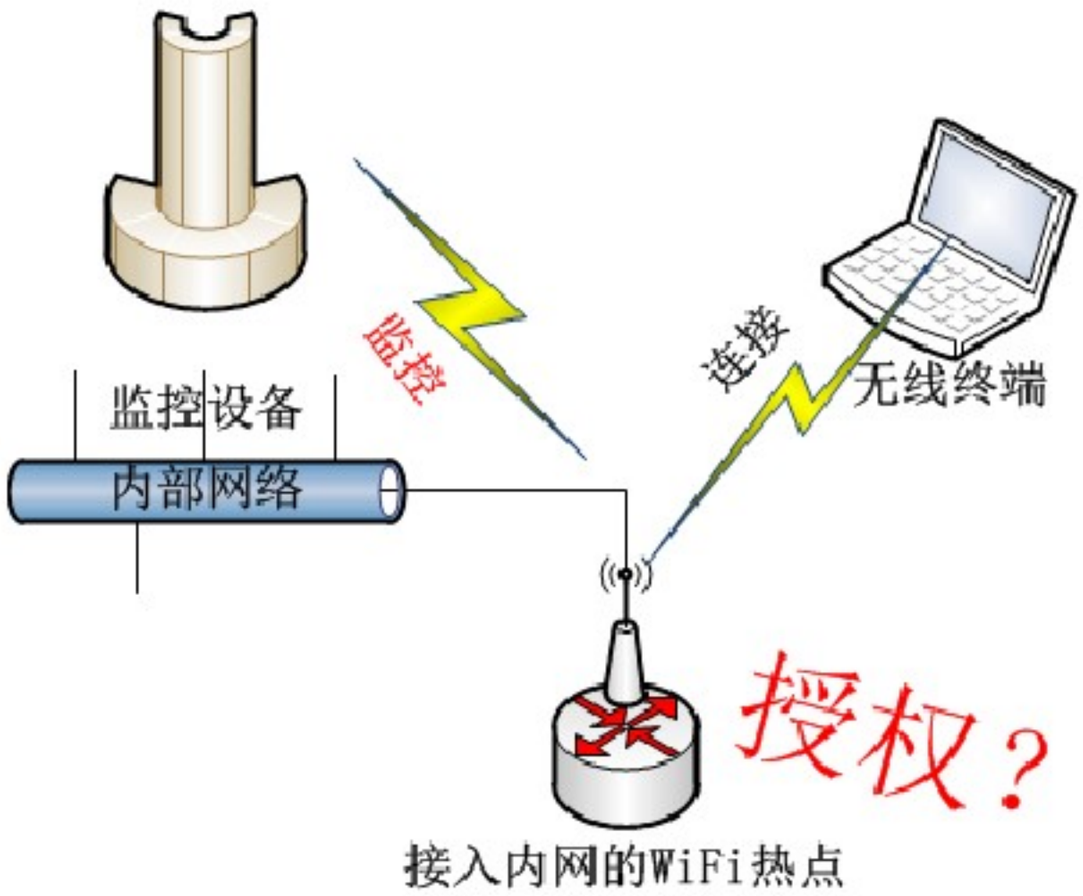
功能需求

- 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



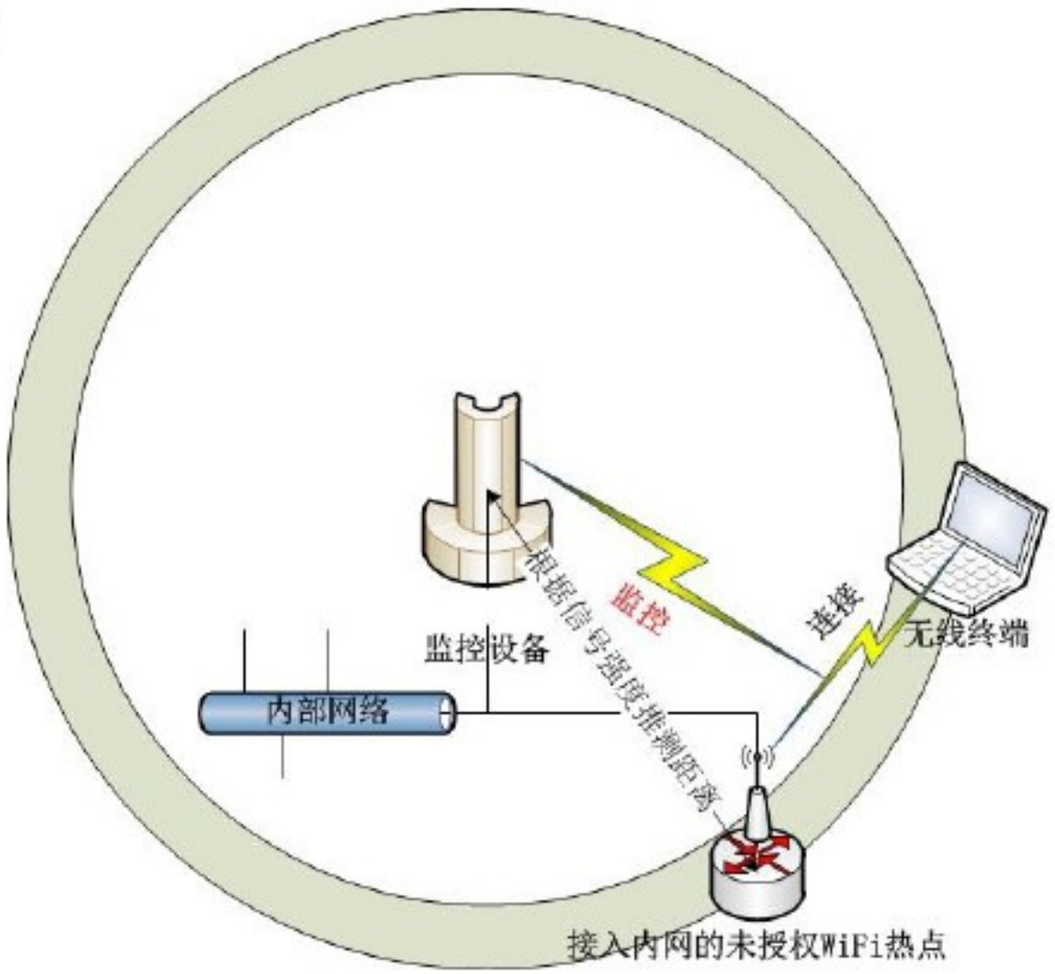
功能需求

- 对于接入内网的WiFi热点，区分出授权和未授权的WiFi热点



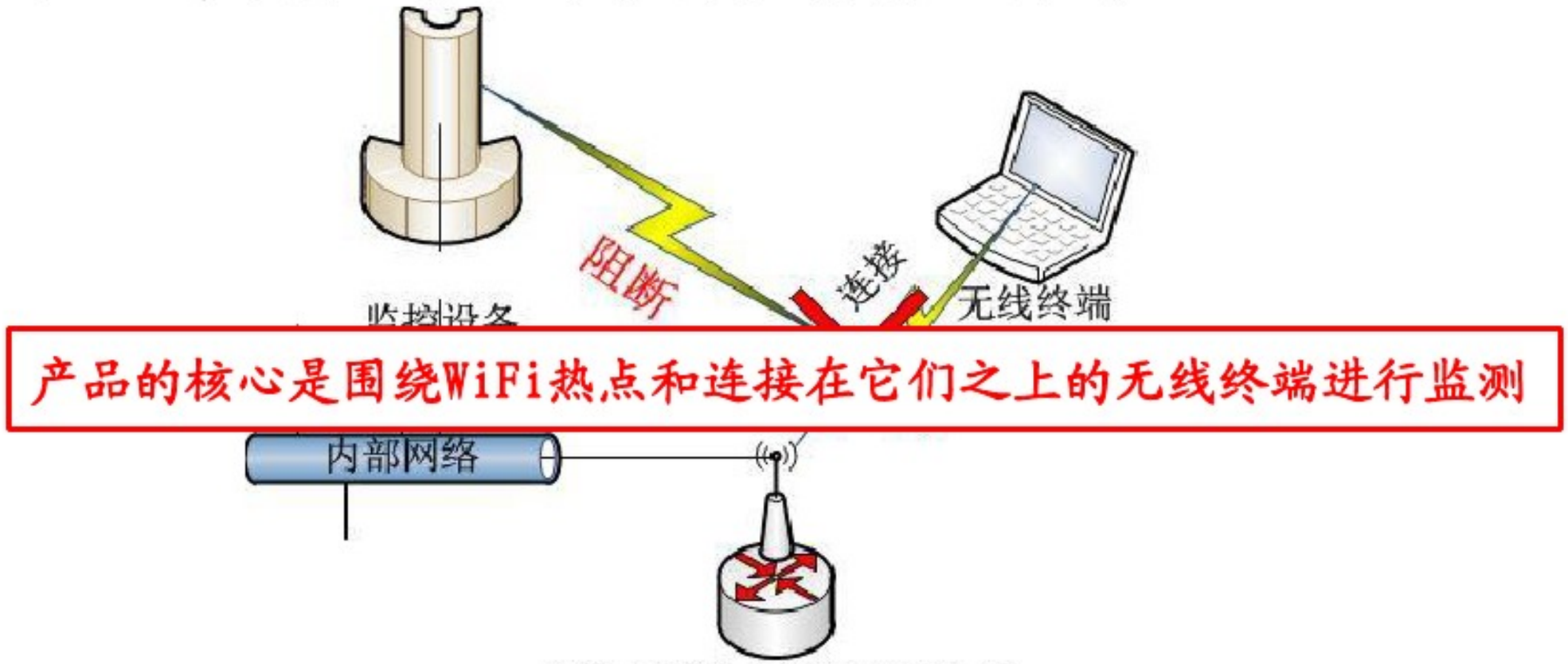
功能需求

- 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

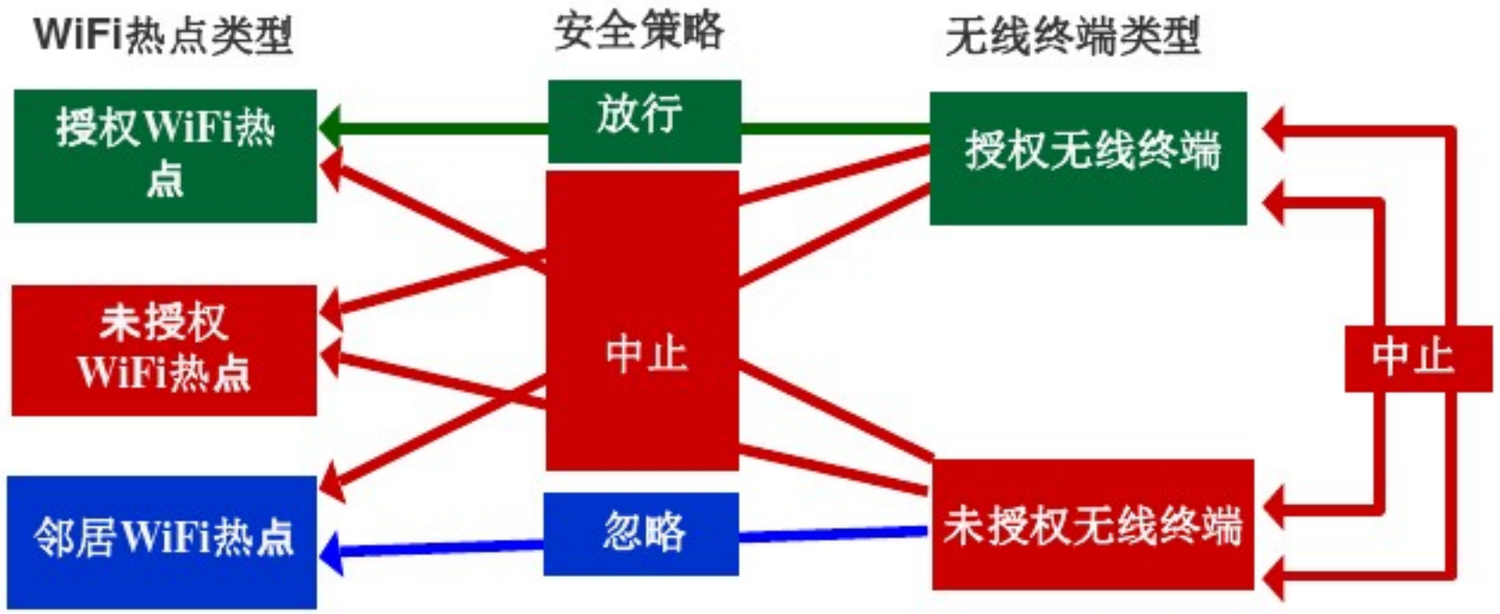


BlueSecurity

- 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

BlueSecurity—无线设备管理

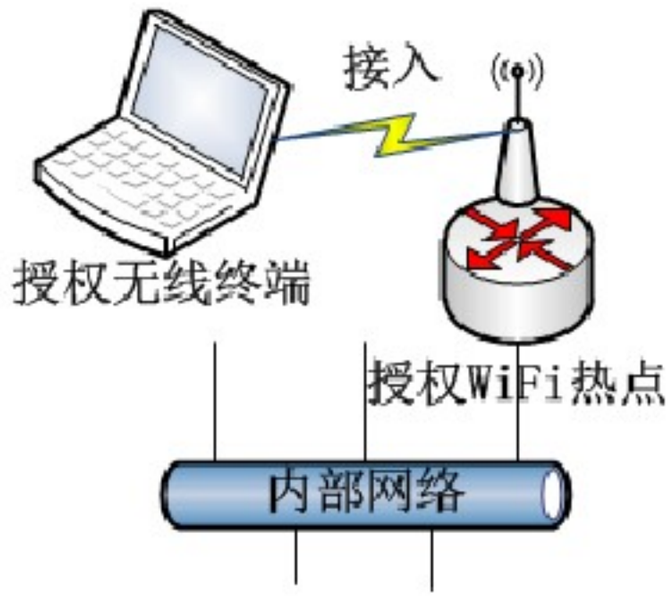
- 自动对检测到的WiFi热点和无线终端作出分类
- 围绕无线终端与WiFi热点的连接进行管理



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

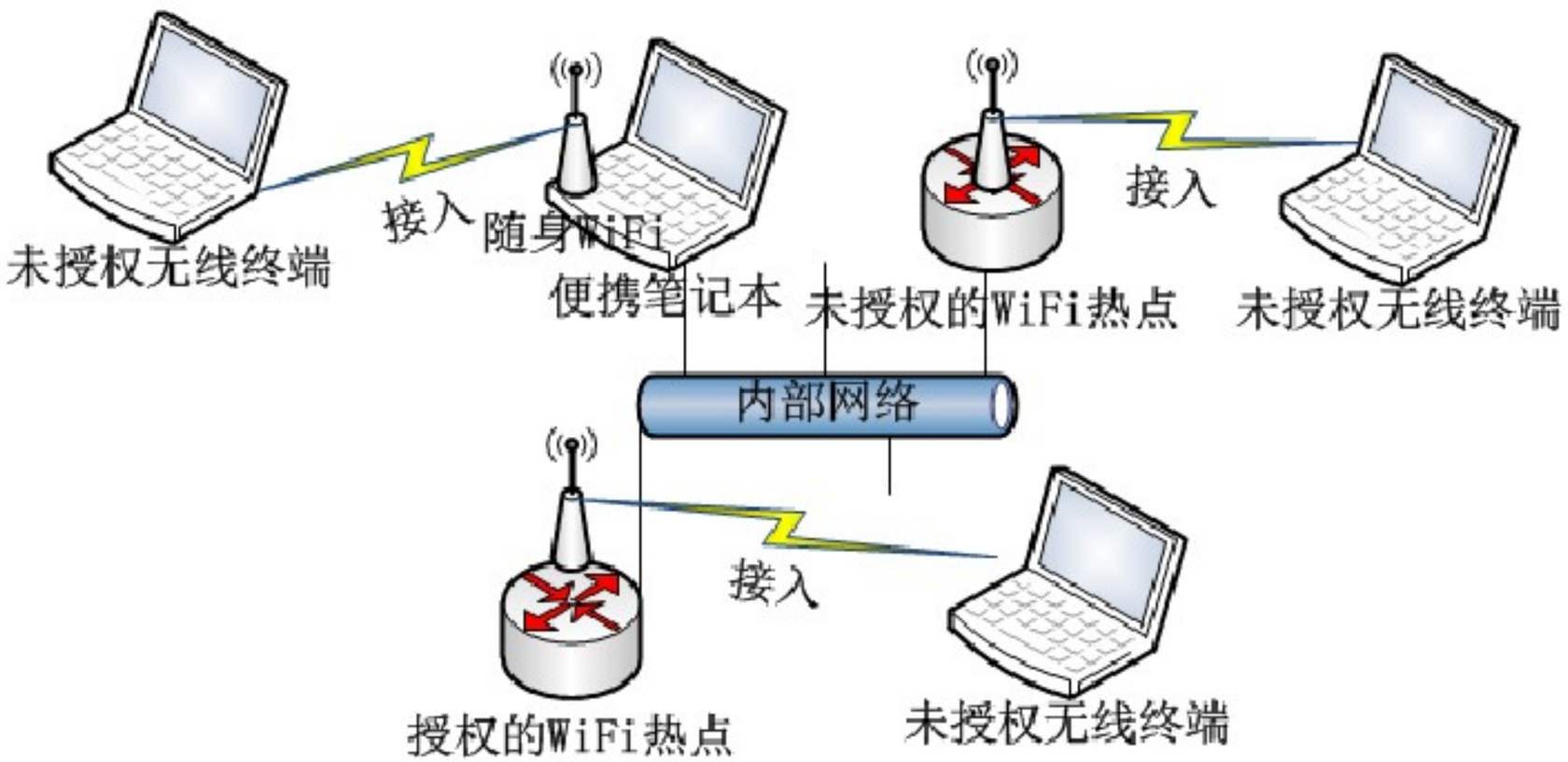


BlueSecurity—异常事件检测

- 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

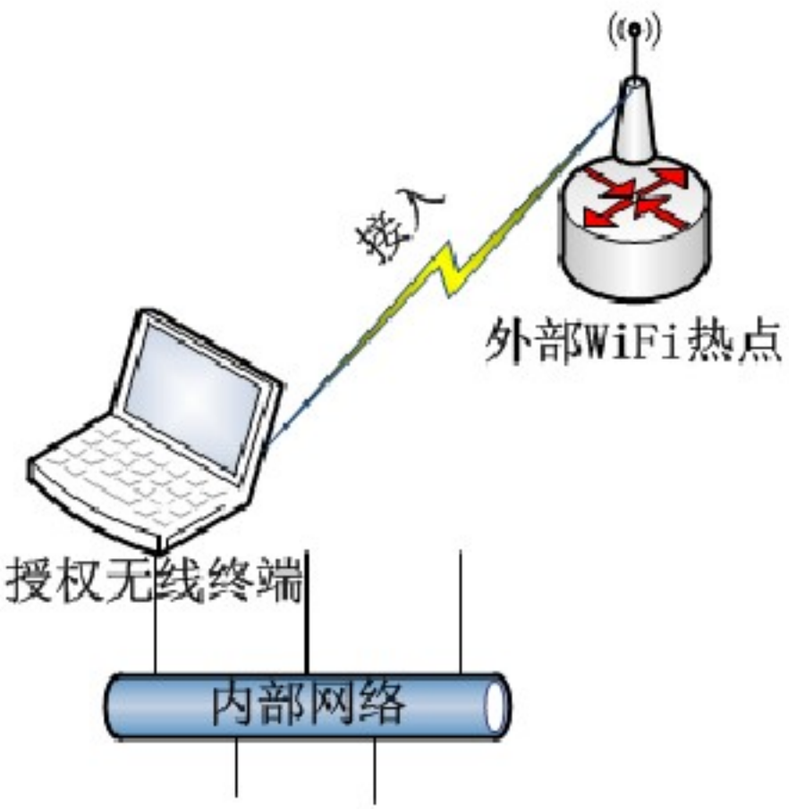
BlueSecurity—异常事件检测

- 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



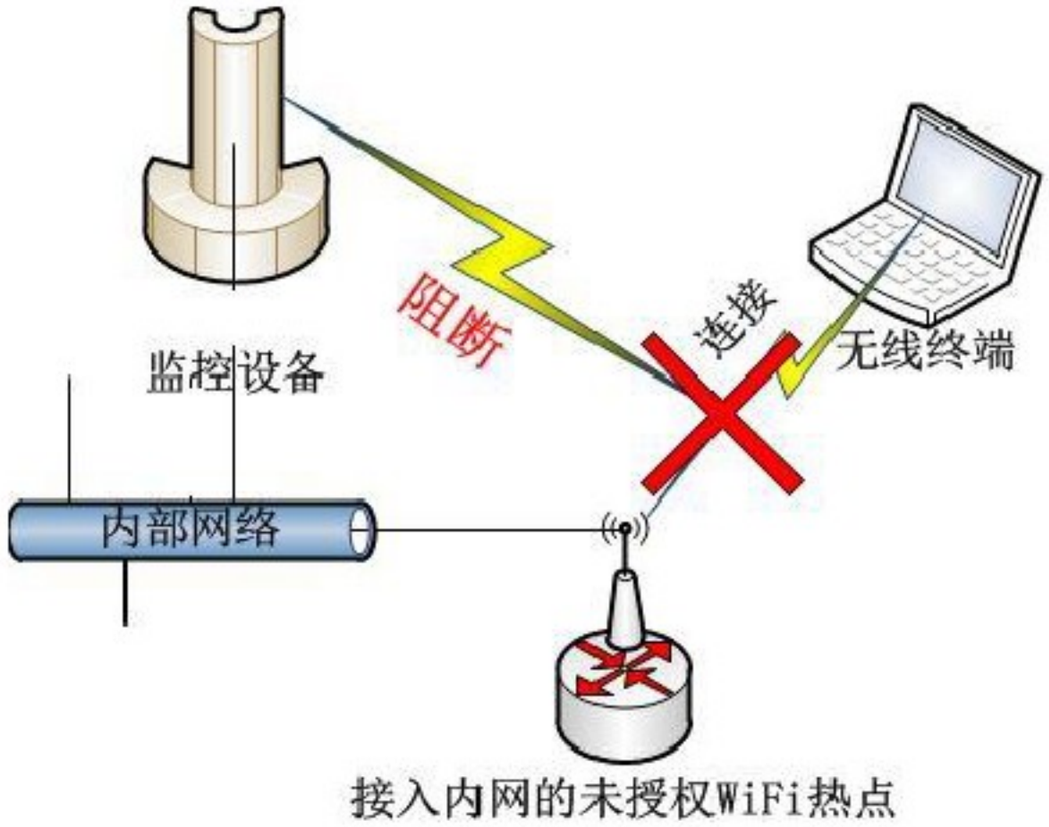
BlueSecurity—异常事件检测

- 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



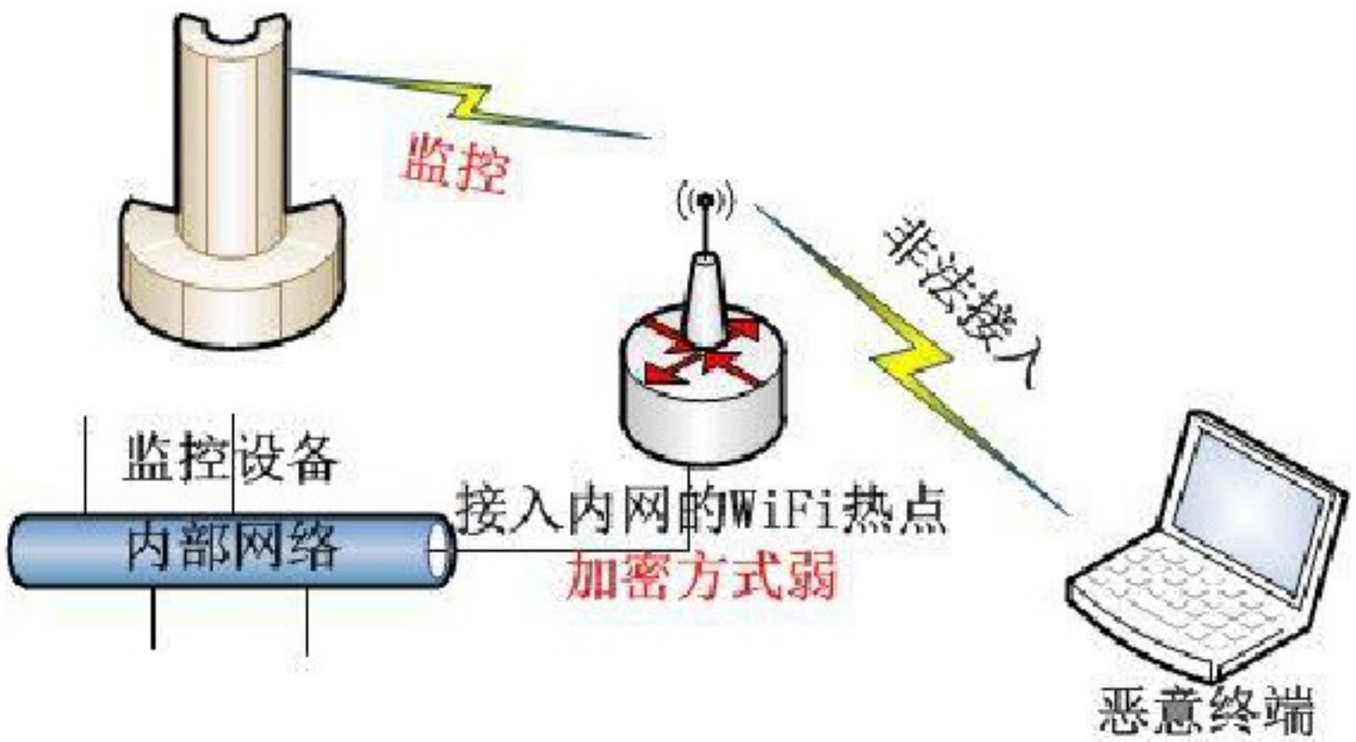
BlueSecurity—异常事件检测

- 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



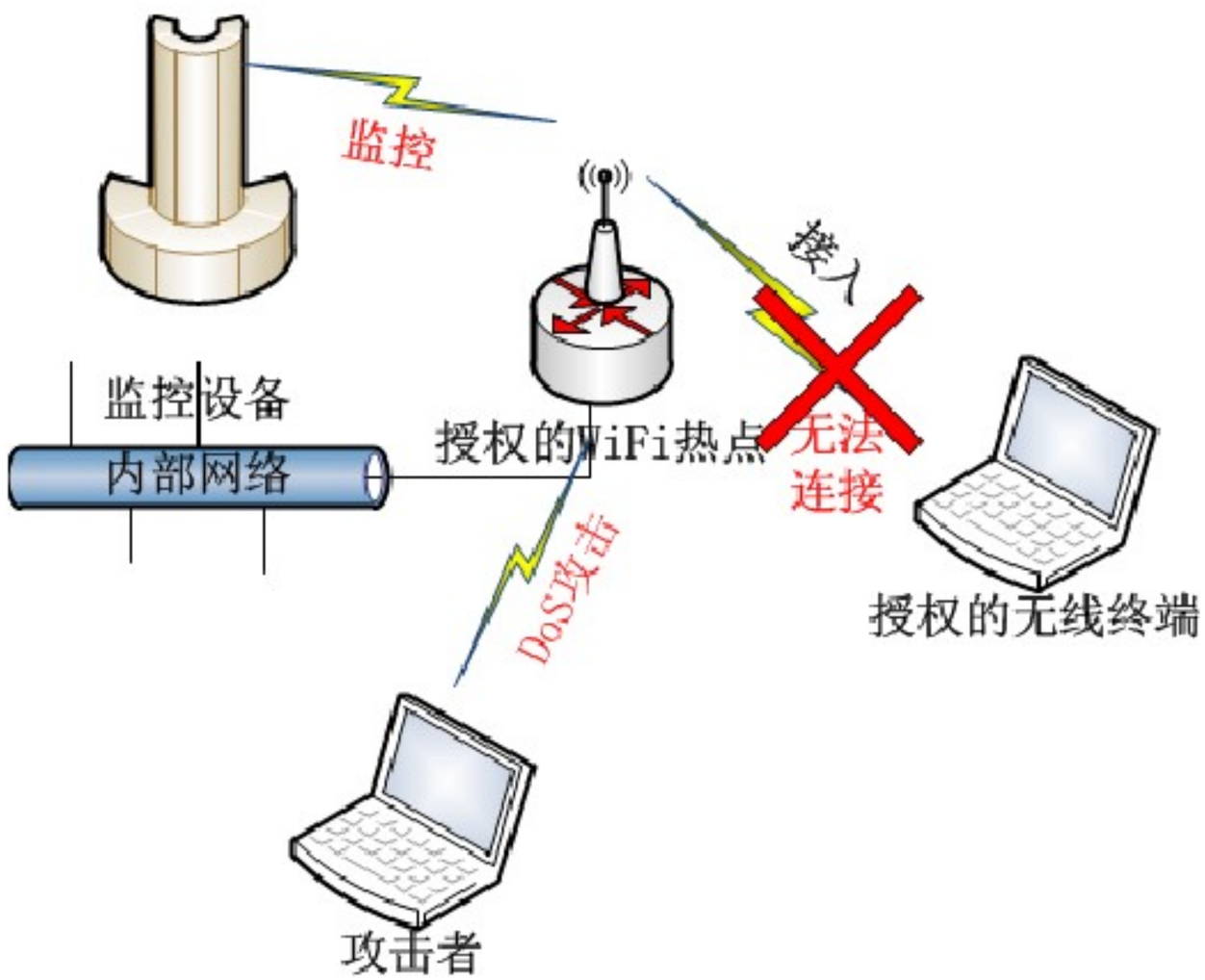
BlueSecurity—异常事件检测

- 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



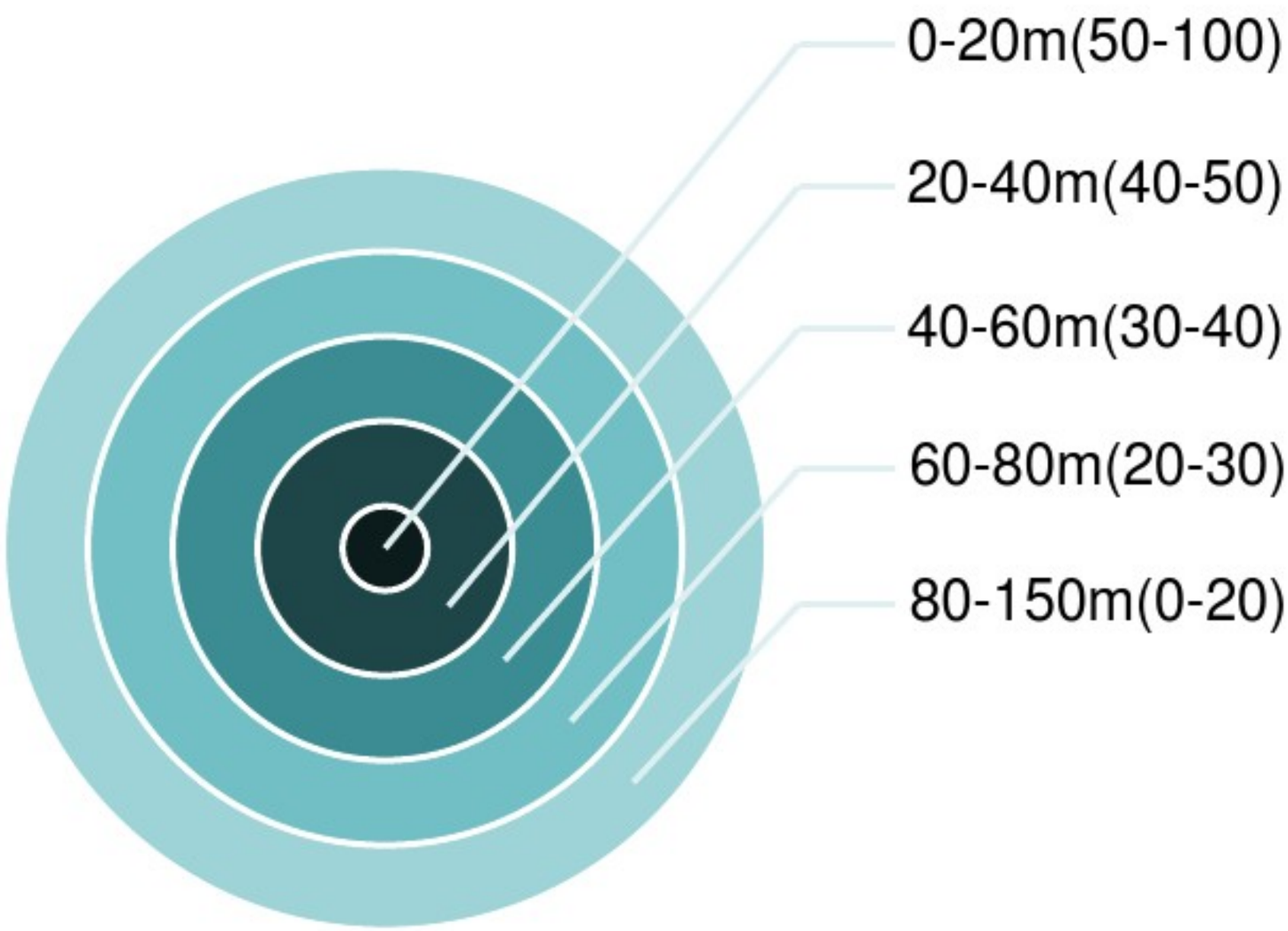
BlueSecurity—异常事件检测

- 攻击警报
  - 发现DoS攻击发出警报
  - 可以瘫痪WiFi热点



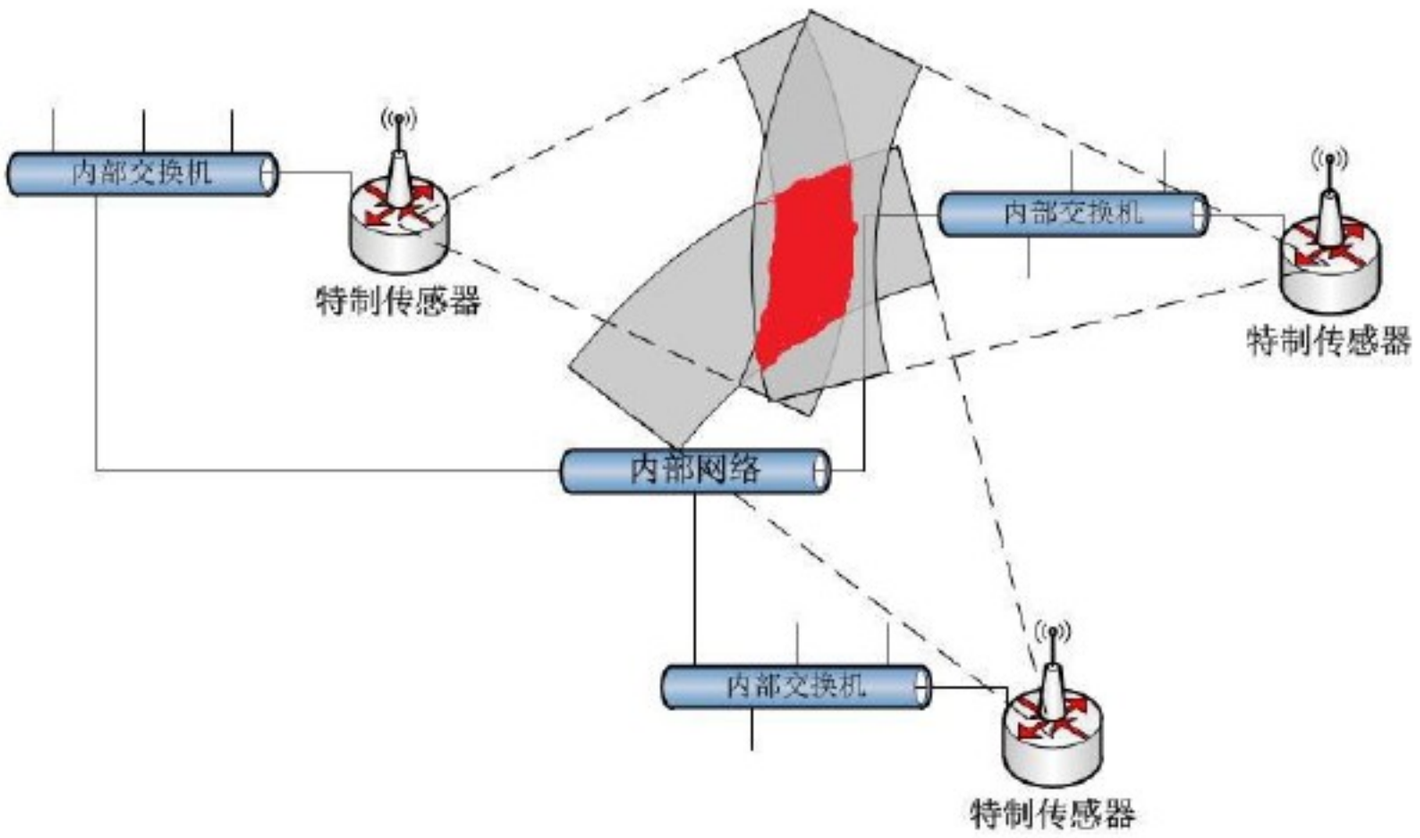
BlueSecurity—定位

- 在单点模式下通过信号强度计算大致的距离范围



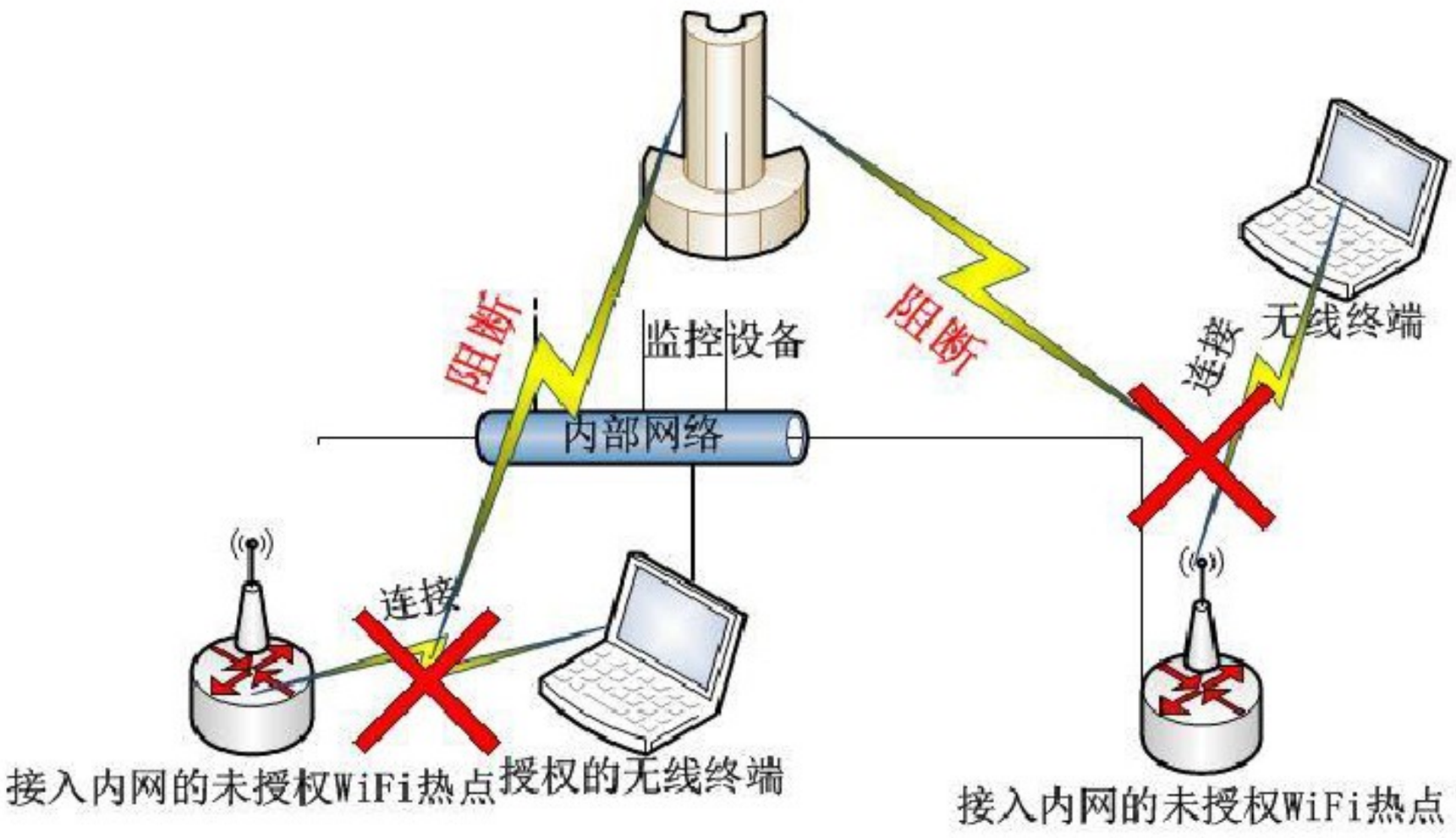
BlueSecurity—定位

- 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



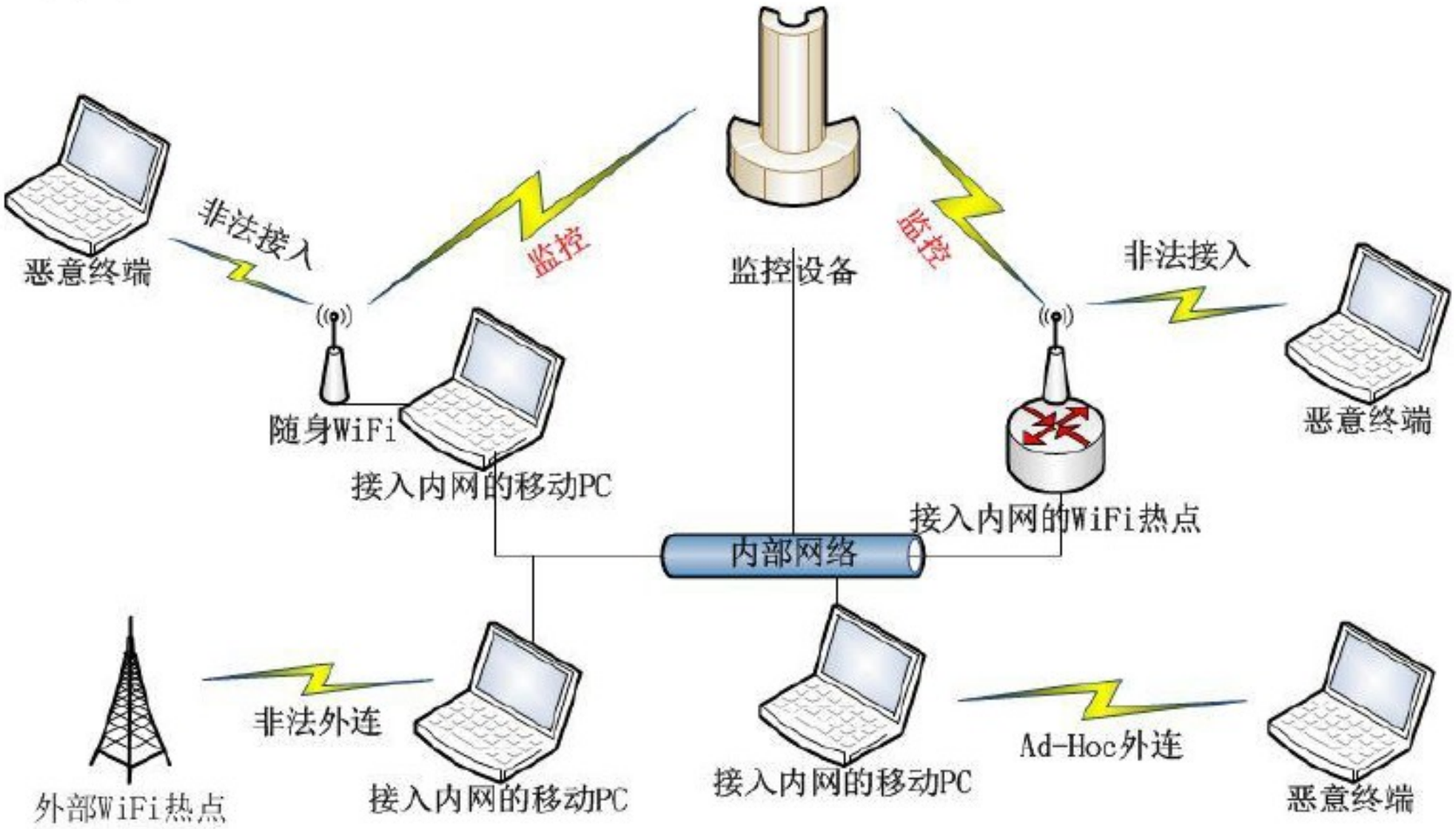
BlueSecurity—阻断

- 阻断是针对无线终端与WiFi热点的连接来实现的



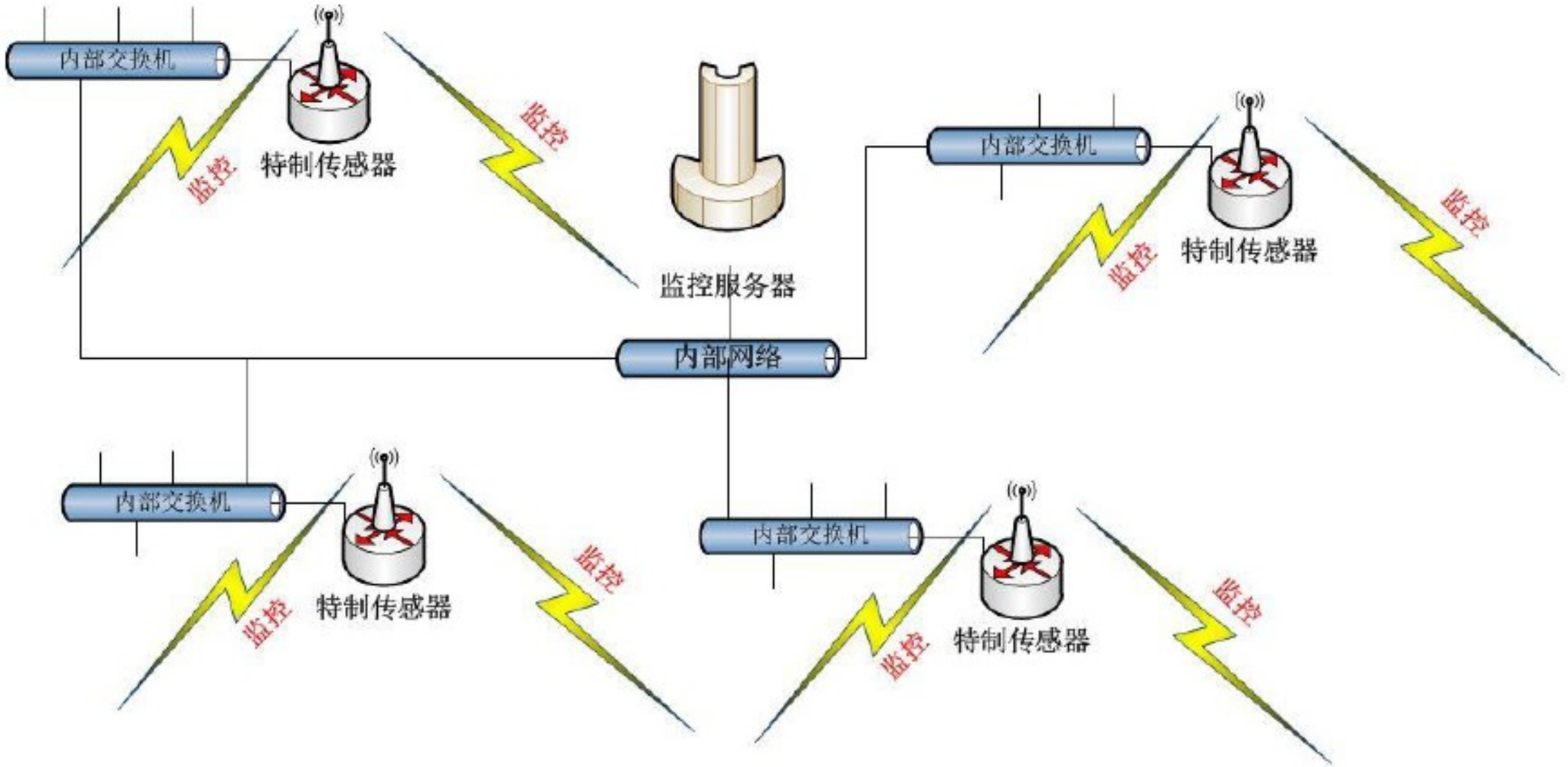
BlueSecurity—部署模式

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

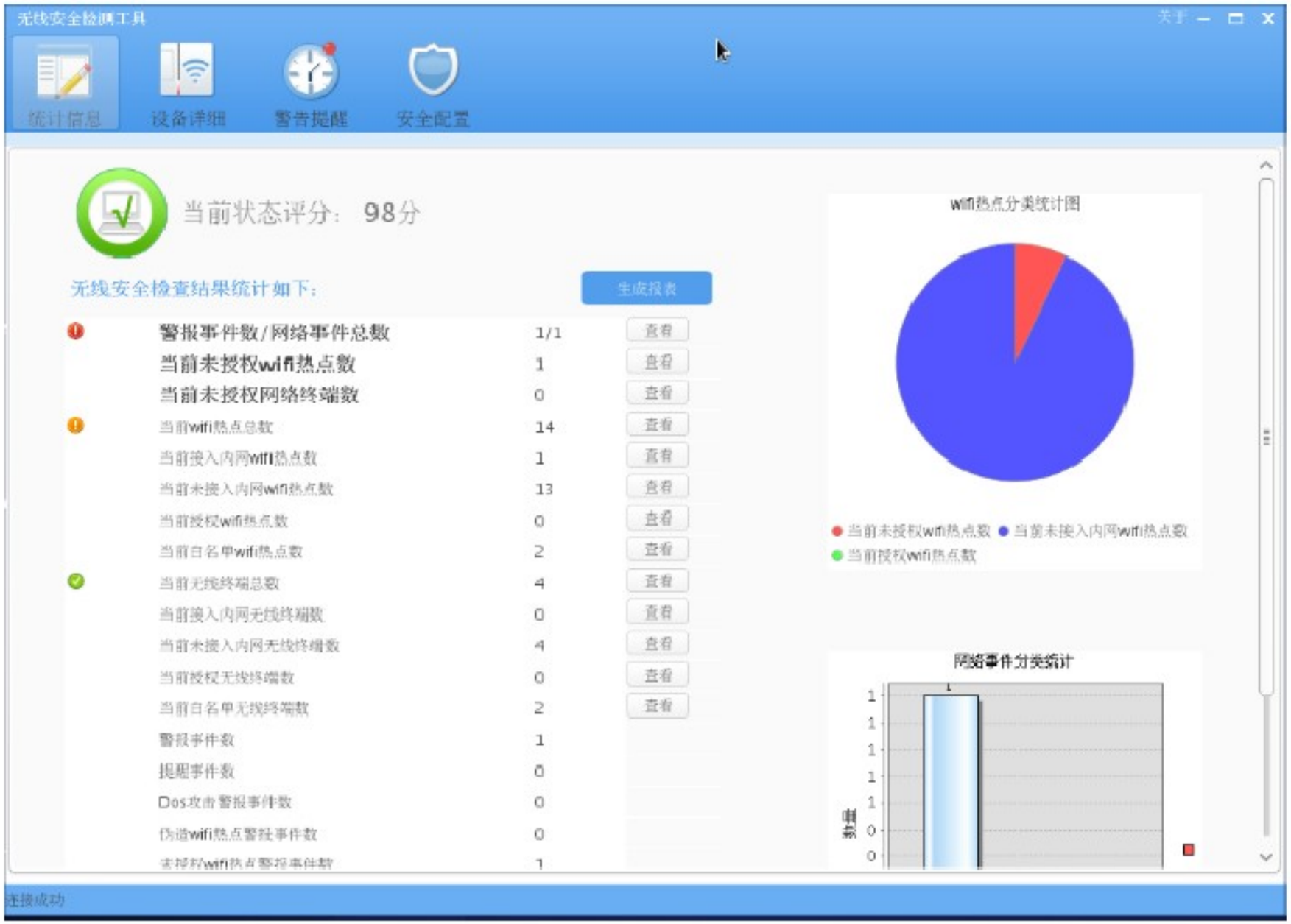
定位功能

- 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

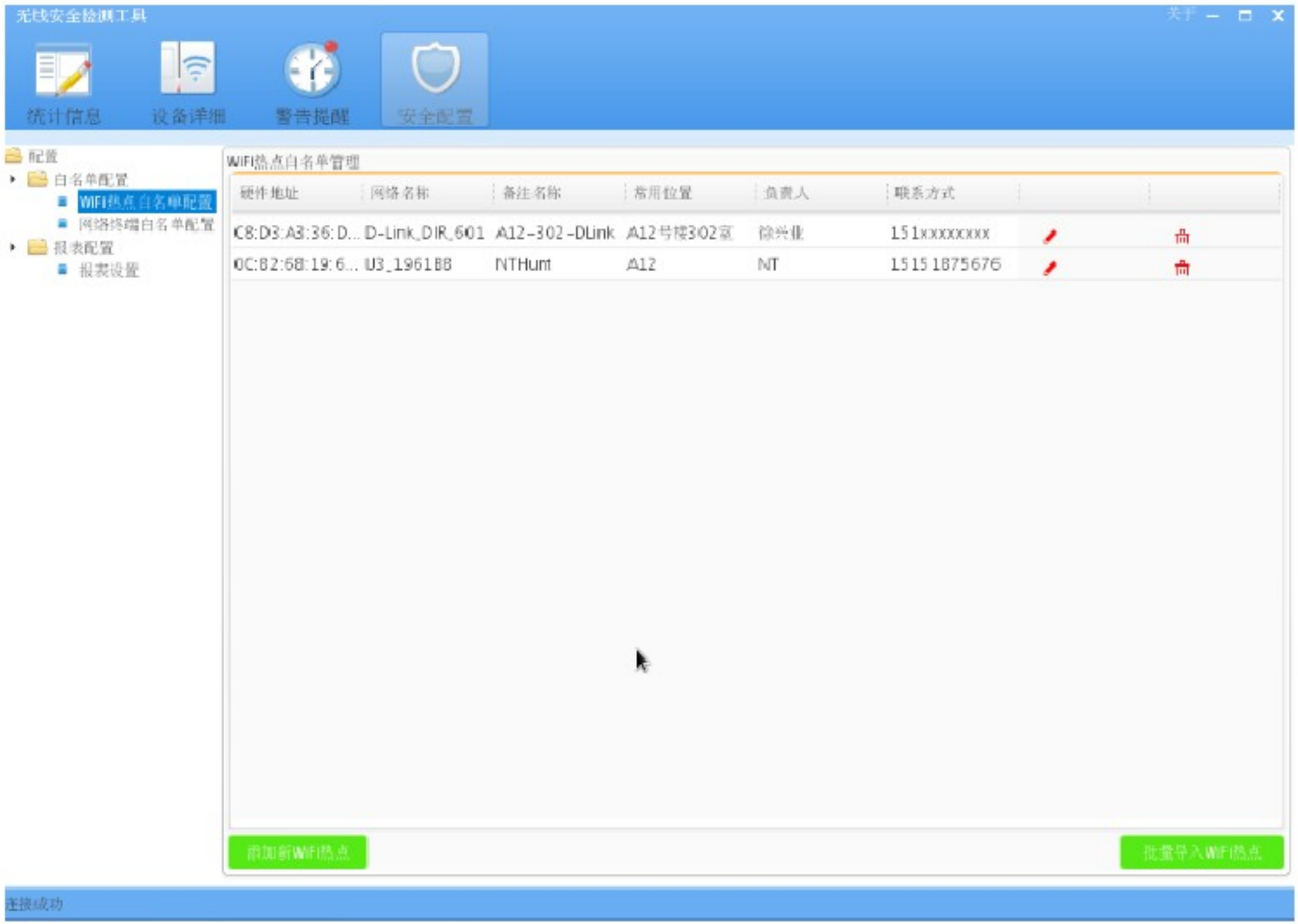
阻断功能

- 对随身WiFi发动阻断
- 无线终端无法连接到网络

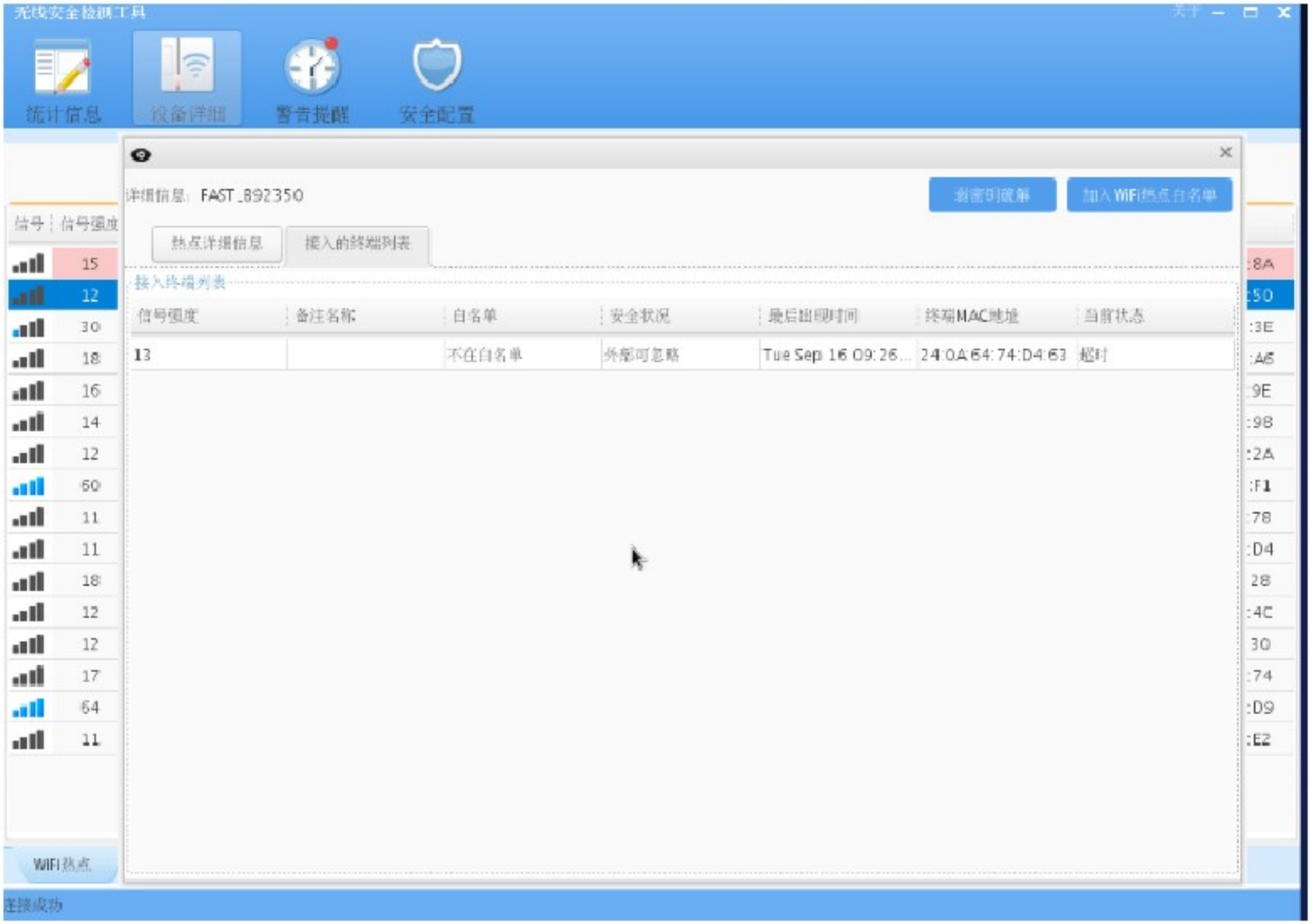
运行抓图-主界面


无线安全检测工具
关于
统计信息
设备详细
警告提醒
安全配置
当前状态评分： 98分
无线安全检查结果统计如下：
生成报表
警报事件数/网络事件总数 1/1 查看
当前未授权wifi热点数 1 查看
当前未授权网络终端数 0 查看
当前wifi热点总数 14 查看
当前接入内网wifi热点数 1 查看
当前未接入内网wifi热点数 13 查看
当前授权wifi热点数 0 查看
当前白名单wifi热点数 2 查看
当前无线终端总数 4 查看
当前接入内网无线终端数 0 查看
当前未接入内网无线终端数 4 查看
当前授权无线终端数 0 查看
当前白名单无线终端数 2 查看
警报事件数 1
提醒事件数 0
Dos攻击警报事件数 0
伪造wifi热点警报事件数 0
wifi热点分类统计图
当前未授权wifi热点数
当前未接入内网wifi热点数
当前授权wifi热点数
网络事件分类统计
连接成功

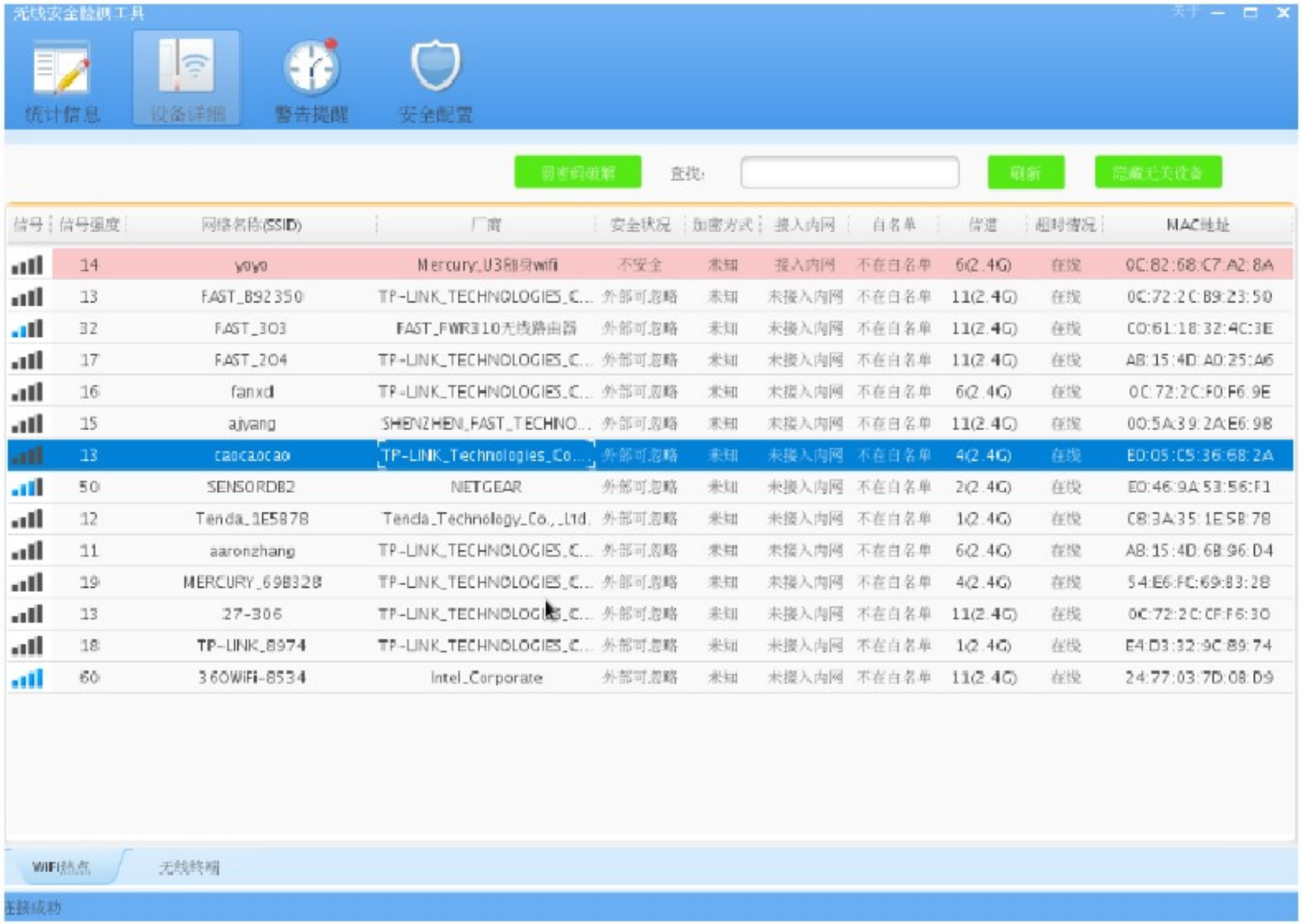
运行抓图-安全配置


无线安全检测工具
关于
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
151xxxxxxxx
0C:82:68:19:6...
U3_1961B8
NTHum
A12
NT
15151875676
添加新WIFI热点
批量导入WIFI热点
连接成功

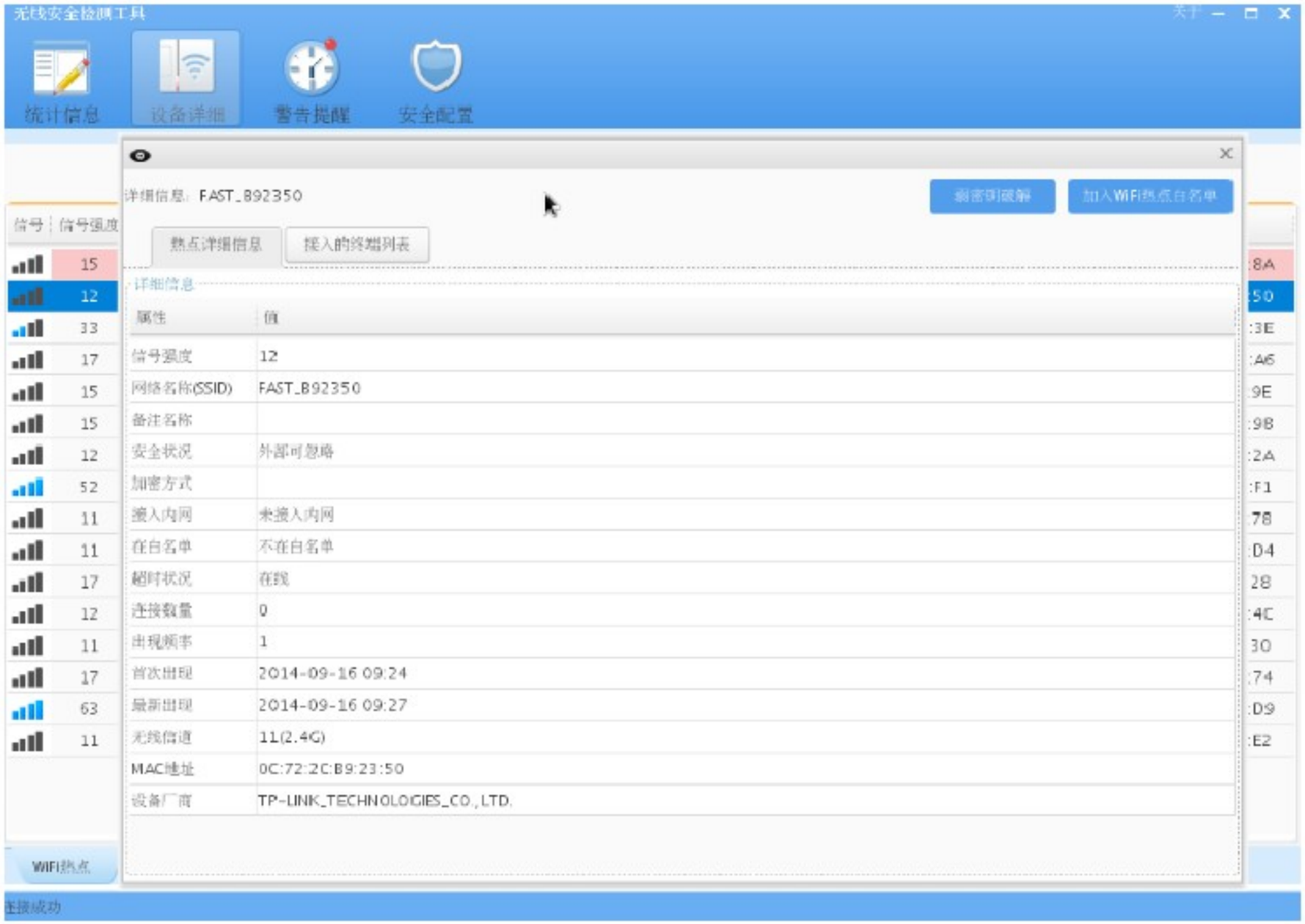
运行抓图-热点接入的终端列表



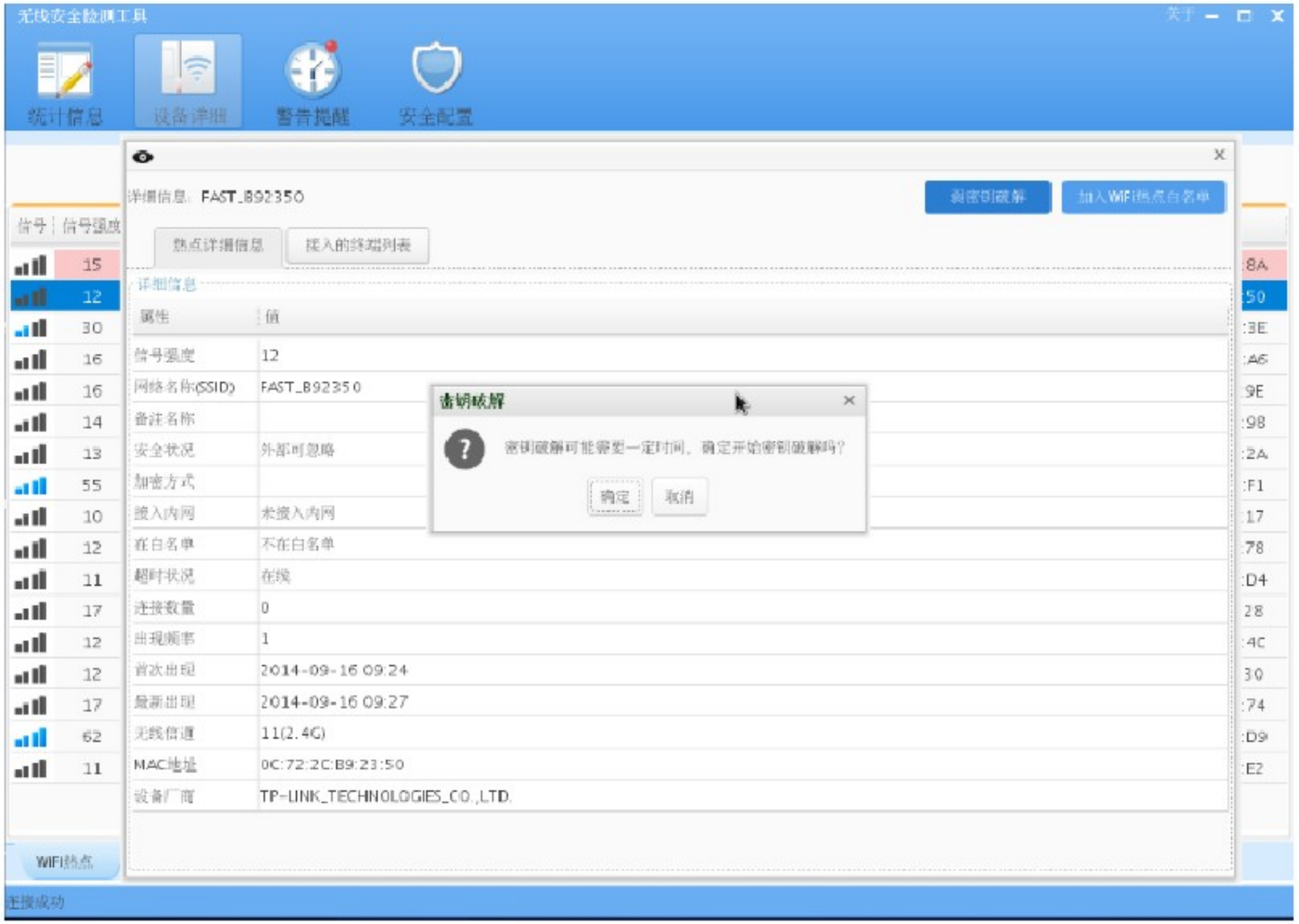
运行抓图-热点设备的详情列表



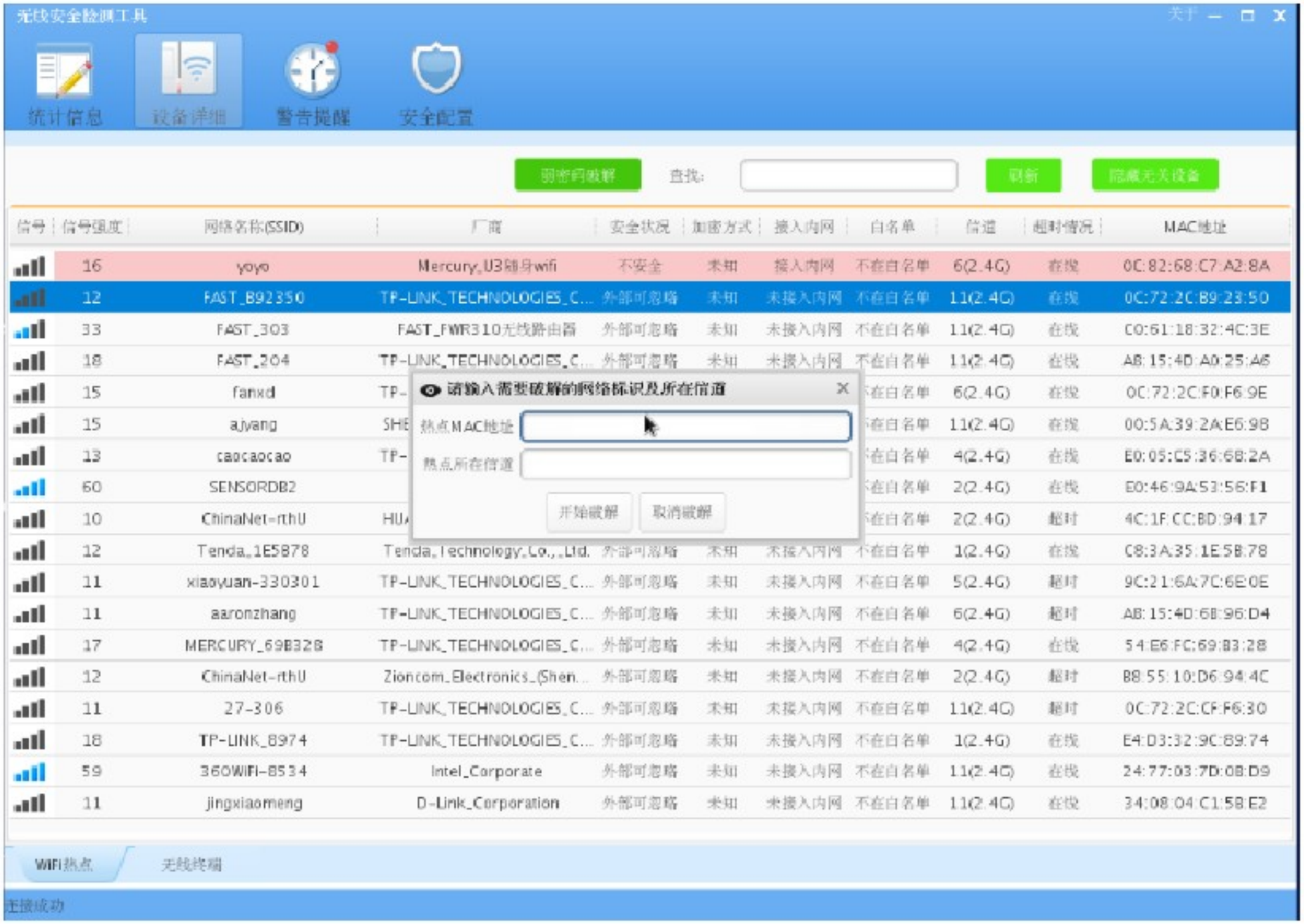
运行抓图-热点的详情信息



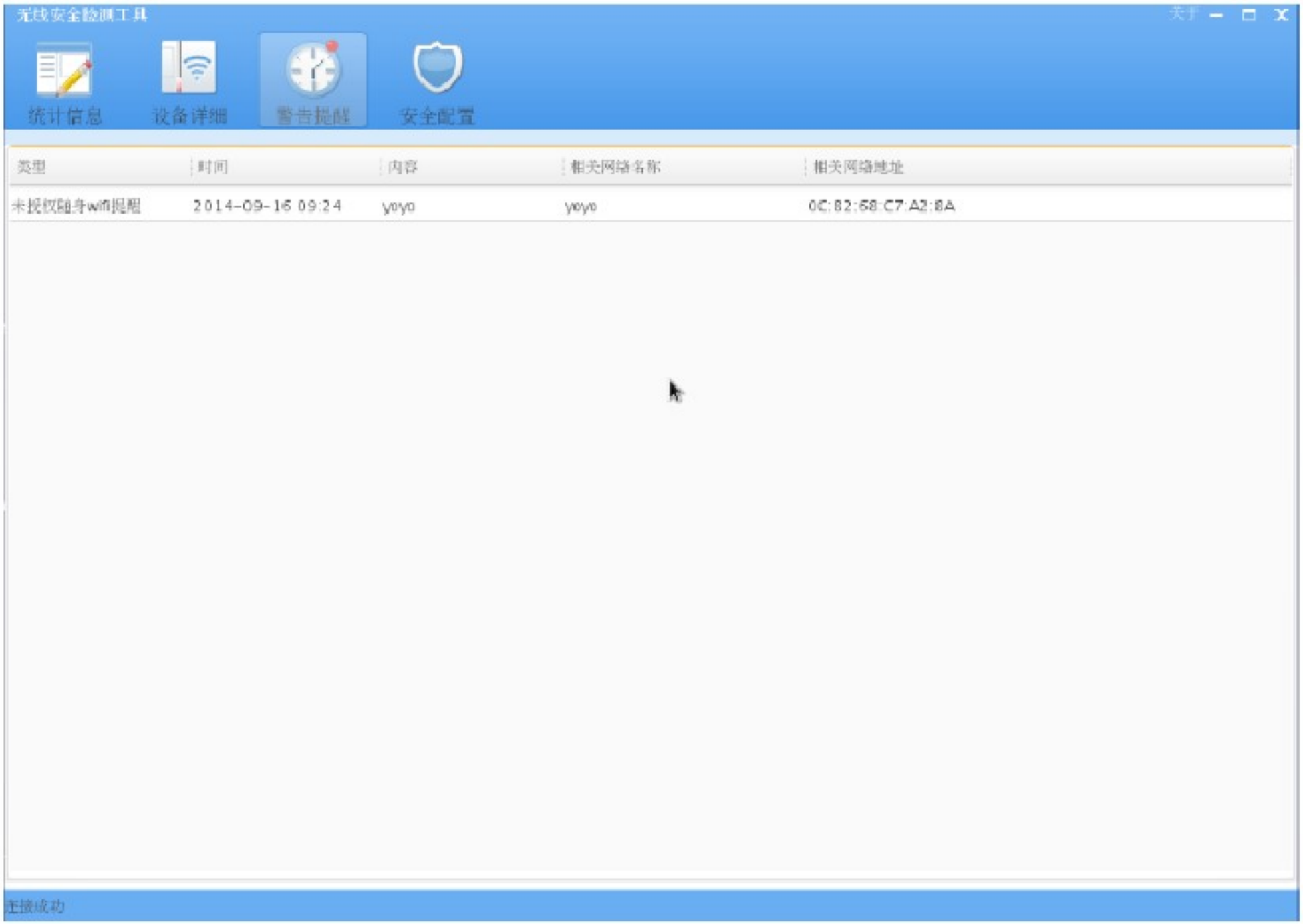
运行抓图-弱秘钥破解的界面



运行抓图-自定义弱秘钥的破解界面



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