360 无线入侵防御系统

产品白皮书

360

360

目 录 | Contents

一. 前言

二. 无线安全问题分析

2.1 企业自建热点

2.2 非企业自建热点

2.2.1 其他企业热点

2.2.2 员工自建热点

2.2.3 恶意热点

三. 无线安全防护的必要性

四. 当前防护手段不足

4.1 缺少持续的检测工具

4.2 缺少有效的防护措施

4.3 缺少必要的审计手段

五. 无线网络防护的基本要求

5.1 安全情况评估

5.2 及时发现热点

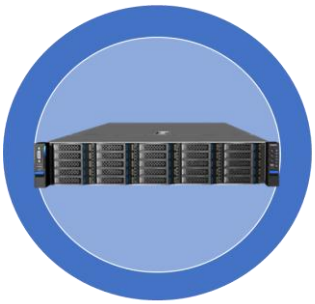
5.3 热点精确阻断

5.4 攻击行为检测

六. 360 天巡无线入侵防御系统

6.1 产品概述

6.2 产品架构



MGR2000系列
中控服务器

WHM200
室内型无线收发引擎

WHM300
室外型无线收发引擎

6.3 产品优势

6.3.1 无线入侵实时监测

6.3.2 恶意热点精确阻断

6.3.3 安全事件智能告警

6.3.4 黑白名单智能管控

-
-

6.3.5 安全审计报表

6.3.6 无线网络状况展示

6.3.7 多区域分级管理

6.3.8 精确定位跟踪

6.3.9 产品独立部署

6.4 主要功能

6.4.1 无线热点阻断

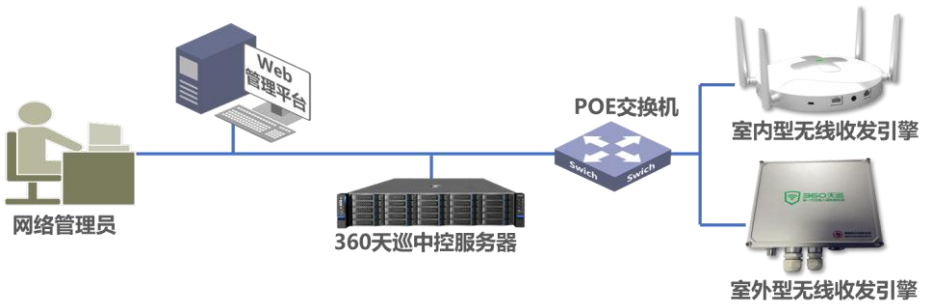
6.4.2 无线攻击检测

6.4.3 安全策略设置

6.4.4 无线安全评估

6.5 产品部署

6.5.1 部署架构



6.5.2 无线收发引擎部署

办公区

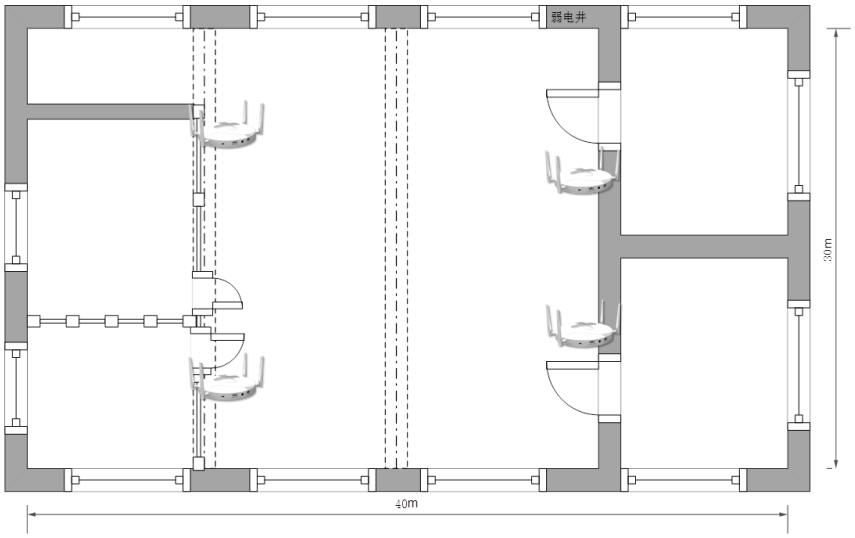
会议室

办事大厅

户外公共场所

6.5.3 网络部署

6.5.4 部署示例



七. 技术支持体系