

## 企业办公无线解决方案

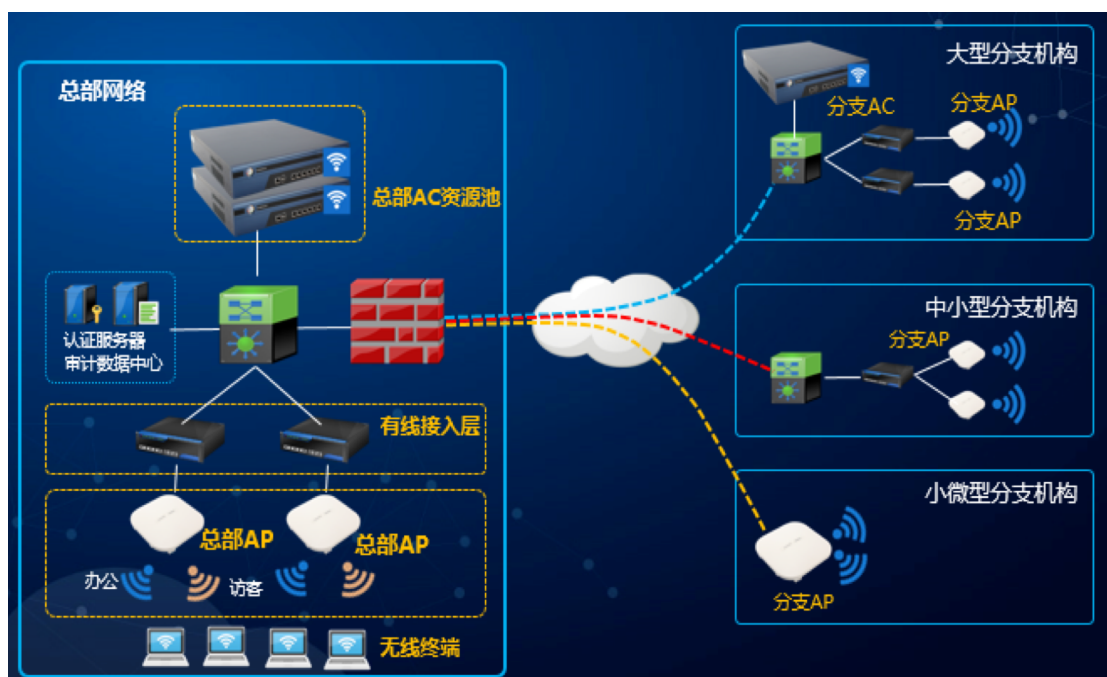
### 行业背景

大型企业在无线网络建设期间要充分考虑访客（领导、客户、合作伙伴）接入网络的需求。首先从安全性考虑，访客网络必须要和办公网络分开，访客网络单独提供给访客使用。从用户体验角度考虑，访客接入网络的验证方式一定要做到简单易行，繁琐的验证方式会降低访客对企业的整体印象。同时对于访客网络，企业还需要建立完善的网络安全管理机制，避免由于访客的网络不良访问给企业带来的法律风险。对于企业员工移动办公上网，更需要做到可管控，上网行为做到可追溯，企业有效的带宽资源得到合理的分配和保证，才能使企业的业务系统正常且稳定高效地运行，同时保证企业信息安全，避免机密信息泄露。

### 用户需求

- 1、接入不安全：缺乏安全可靠的认证机制，企业无线网络接入不安全
- 2、上网权限混乱：缺乏有效的控制策略，员工上网权限不分明
- 3、数据信息安全：缺乏有效的数据加密机制，企业数据被黑客窃取篡改
- 4、无线信号差：AP性能不佳，上网总掉线，点位规划不合理，信号盲区多
- 5、漫游效果差：不能实现二三层漫游，移动办公时，业务中断

### 解决方案：



结合用户无线网络需求情况,结合信锐产品自身技术特点,为了满足用户构建一个高速、稳定、安全、可靠、易于管理的无线接入网络的需求,本设计方案按照 AP+AC 的结构化无线网络解决方案进行设计。具体设计为在总部设置总部 AC,在大型分支机构设置分支 AC 与分支 AP,中型分支机构设计二级,三级交换机,分支 AP。微型分支机构直接设置分支 AP。总部 AC 可以对大型分支机构的 AC 进行管理,当网点控制器采用集中管理的模式进入到中心端控制器时,会自动下载中心端的公共配置,比如 IP 组、MAC 地址库、时间计划、角色授权、认证页面等。总部 AC 也可以直接管理中小型分支机构的分支 AP,实现统一管理。

## 方案设计:

### 安全无线整体解决方案:

接入前&接入时进行身份认证、信锐安全无线网卡、账号绑定(硬件码+手机号),非法热点检测及防御、网络攻击防护、射频定时关闭及安全加固。

接入后&上网时进行访问权限控制。

上网后进行上网行为记录。

### 上网用户身份实名认证:

无线办公网采用 802.1X/Portal/WAPI 认证,外置 AAA 和 RADIUS+AD 用于存储用户账号密码。

每个账号对应一个员工,包括姓名、部门、性别以及身份证、手机号等个人信息,保证每个上网的账号都是可寻的,便于安全管理。

用户输入账号密码上网验证时均采用加密传输,防止黑客空中拦截,窃取账号密码等数据。

### 上网账号自动绑定终端:

自动将账号与终端的硬件特征码进行绑定,防止账号被他人使用或者被盗用。

每台设备的硬件特征码是唯一的,无法通过软件修改。即使通过软件修改了仍然可以识别原始的。

每个账号最多可以绑定 5 台终端,超过 1 台时需要管理员审核。

### 上网账号二次绑定手机号码:

账号首次登陆时需要绑定手机号并输入短信验证码,当用户账号在新终端登陆时(换终端/被他用/被盗),不仅需要输入密码,还需要输入短信验证码,解决员工账号认证的安全

## 问题

绑定手机号码的用户，可以自助重置密码和修改密码，无需通过 IT 管理员。

### 用户密码管理及自助修改：

无需通过管理员即可修改密码，提高效率及减轻管理员工作压力。

通过口袋助理、钉钉、企业号等手机 MOA 类 APP 软件进行无线密码修改。

若账号绑定了手机号码，可通过手机验证码自助修改。

### 上网终端合法效验：

采用信锐安全无线网卡接入无线网络，终端与 AP 热点的双向验证，提高安全性。

可以将无线网络设置为只有安装了信锐安全无线网卡的终端才能接入无线网络。

支持设置安全无线网卡只能连指定 SSID 无线网络，无法连接非授权 SSID。

信锐网卡与 AP 数据传输时自动进行数据加密，保证无线的空口安全。

### 无线热点扫描及非法热点抑制：

背景：黑客在附近搭建一个一模一样或者类似的 WIFI 名称，诱使用户连到虚假钓鱼 WIFI 上，黑客利用分析软件从用户上网产生的数据包中分析提取用户隐私信息。

我们通过 WIPS 无线入侵防御系统实时检测周围无线信号，当检测出来的信号 BSSID、且 AP 源 MAC 地址不在授权列表中时，我们向对应的 AP 和终端发送解除关联帧，让终端无法连上钓鱼 WIFI。7×24 小时不间断监测网络。

### 上网行为严格控制：

强大的管理：通过应用识别技术，可以根据应用类型或者具体某一种应用进行封堵，包括视频、论坛、游戏、金融、下载等 2400 多种网络应用。

通过应用识别技术，可以根据应用类型或者具体某一种应用进行封堵，比如上班时间不允许炒股，不允许 P2P 下载，不允许外发敏感文件等；支持主流移动平台，可识别 IM、社交、Mail、新闻、炒股等应用。

无线控制器内置千万级别的 URL 分类库，能够对 URL 进行识别，包含新闻、购物、金融、教育等 18 个种类的 URL 地址；准确识别目前主流网站，识别率高达 99.9%，有效实现网页过滤。例如禁止登陆非法网站

通过基于时间段的访问控制策略，实现不同的时间段不同的访问权限，比如上班时间，禁止访问网上银行、游戏、论坛贴吧等与工作无关的应用，下班时间则不受限制。

办公区域内，不同办公部门总会有各自专属的无线网络，并且不希望部门之外的成员使

用这个网络。无线网络控制器可以根据用户的属性，限制禁止非本部门的用户接入。

#### **典型无线网络攻击防护：**

对典型的危险攻击行为进行检测，当超过设定的阈值后自动将攻击者加入到黑名单中，并冻结一定时间，即时发现网络攻击并进行防御。

检测的攻击包括：DDOS 防御、ARP 扫描、IP 扫描、端口扫描防御，禁止客户端私设 IP 以及 ARP、网关欺骗防御、DHCP 请求泛洪防御。

#### **无线射频定时关闭开启：**

通过射频关闭控制策略，可以指定某 SSID 网络，定时自动关闭和开启无线网络的射频信号，晚上下班后自动关闭无线射频信号。

一方面可以节能减排、节省电费支出；另一方面又能防止非法用户利用深夜时间入侵无线网络，做一些非法的操作。

#### **有线无线一体化管理：**

信锐 NAC 的有线无线一体化，支持对有线用户的接入认证、访问控制、流量管理、上网行为审计等，

并提供统一中文 Web 管理界面，一站式服务，极大的降低网络建设成本。

#### **网络分权分级管理：**

分配不同的管理员分别管理各自权限区域的无线 AP，可以精细到对某 AP 分组有管理权限，该管理员可以在该 AP 分组上建立无线网络，能够激活、删除接入点，能够对 AP 的配置进行编辑修改。

可指定管理员针对每个页面的编辑或可查看权限，控制粒度到控制器上的各个页面，对某个页面没有读权限则登录时不显示。

#### **移动 APP 随时随地运维管理：**

支持跨互联网运维管理

登陆 APP 进行维护管理：不同管理员，不同权限

查看网络运行情况：在线用户、在线 AP 数量、实时流量

无线网络管理维护：开启关闭 SSID、终端绑定审批、二维码上网审核

故障、审批实时通知：AP 离线警告、服务器离线警告、网络攻击告警

### **方案优势：**

1、最丰富的无线安全机制，提供从安全接入到安全上网等端到端的安全策略

- 2、合理管控工作人员上网行为，提升工作效率、防止带宽浪费，有线无线双重管控
- 3、为会议室，报告厅等人员密集区域接入网络提高保证，解决有线网口不足的问题；
- 4、为企业员工的移动办公提供支撑，内部员工可通过无线网络随时安全接入内部网络，实现办公；
- 5、内部员工账号及个人信息绑定，便于安全管理；
- 6、内部员工可通过自己的办公设备在企业大楼内快速移动办公，网络接入更快速，上网行为管理系统对员工上网行为进行审计与管控
- 7、来访客户接入企业网络，可根据不同需求，分配不同的上网权限，保证了接入的安全性同时提升群众上网的体验
- 8、丰富的认证机制，满足组织对无线网络安全、快速接入
- 9、投资成本低，通过部署信锐无线控制器替换原有网络的出口路由、行为管理以及无线控制器

## 成功案例：

作为下一代企业级无线的引领者，信锐技术一直秉承“无线连接一切”的愿景，在智慧医疗的无线网络建设中继续承担推动和发展使命，一起推动智慧医疗的发展，目前已经有近百家三甲医院用户选择我们的方案。

部分客户：红牛中国区总部、吉利控股集团春晓基地、石家庄君乐宝乳业有限公司、无限极（中国）有限公司、祈福集团、优速物流、浙江省建设集团、广元天然气、比亚迪厂区、宝燕集团、汤臣倍健等。