



**SANGFOR**  
深信服科技

XXX 项目  
有线无线统一上网行为管理  
解决方案

深信服科技股份有限公司  
2014 年 11 月

# 目录

第一章 项目背景.....	1
第二章 项目需求分析.....	1
第三章 推荐解决方案.....	2
3.1 推荐方案拓扑.....	2
3.2 部署说明.....	2
3.3 推荐解决方案说明.....	3
第四章 Sangfor AC 其他优势功能介绍.....	6

# 第一章 项目背景

XXXXX

## 第二章 项目需求分析

为了满足 XXXX 的要求，XXX 公司需要实现有线网络和无线网络的统一上网行为管理，具体需求如下：

1. 有线网络和无线网络统一管理界面，方便学习和运维
2. 行为管理设备内置无线控制器功能，能够直接管理 AP，节省无线控制器的采购成本
3. 办公区员工无线上网需求
4. 员工互联网上网行为做审计，审计记录需要保留 30 天

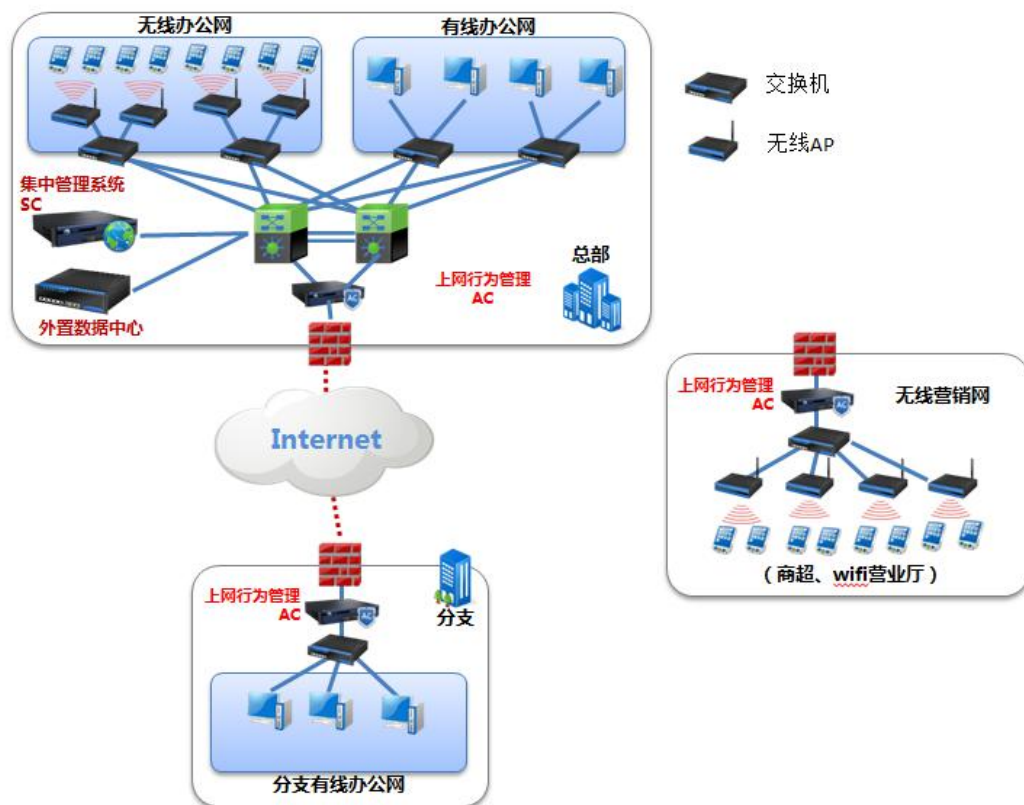
。 。 。 。 。

。 。 。 。 。

。 。 。 。 。

## 第三章 推荐解决方案

### 3.1 推荐方案拓扑



图一 有线无线统一上网行为管理推荐拓扑

### 3.2 部署说明

整体网络分成总部办公网络，营销网络，和分支网络三大块：

1. 总部同时部署有线网络和无线网络，有线网络和无线网络在同一台行为管理设备上进行管理，界面统一，两套网络间模块内部联动（如：用户内部同步）。
2. 总部网和营销网的上网行为管理设备直接管理 AP，无需额外部署无线控制器设备。
3. 有线网络和无线网络用户统一维护，内部员工、访客、不同职权部门权限灵活划分。可针对位置、应用、终端、用户、SSID 五种维度做权限控制。
4. 总部网、分支网、营销网通过各自出口的行为管理设备做 IPsec 组网，保证不同地域间内网能够互联，同时保证数据在互联网上传输的安全性。

5. 总部部署 SC 集中控制平台，对全网的行为管理设备做统一管控，全网行为管理设备可以统一升级、统一更新、统一配置并下发，SC 可以对全网 AP 做统一的配置管理。

6. 总部部署外置数据中心，同步全网行为管理设备的日志，进行统一汇总、统一查询、统一呈现。

### 3.3 推荐解决方案说明

本方案能够实现全网全终端统一管控、管理无漏洞：

#### 3.3.1 集成无线控制器功能，直接管理 AP，即插即用

深信服有线无线统一上网行为管理解决方案内置无线控制器功能，节省购买无线控制器的成本。本方案将有线网络管理和无线网络管理合二为一，模块内部联动，用户统一维护。有线用户和无线用户统一管理，与组合方案（上网行为管理+无线控制器）相比，无需做用户同步，节省开发接口和实施对接的时间成本和经济成本。无线 AP 直接接入网络即可使用，无需配置。做到即插即用，简化实施。

#### 3.3.2 统一的管理界面

本方案同时管理有线和无线网络，统一管理界面，降低学习成本和运维成本。同时，还能够管理移动终端和 PC，让管理更加全面无漏洞，真正做到全网全终端的网络管理。



图二 统一管理界面



图三 移动终端管理

### 3.3.3 移动应用进行有效的识别和精细管控

本方案依托国内最大的深信服应用特征识别库。该特征库包含 4500 多条规则,2000 种以上的应用,以及 600 种以上的移动应用,能够识别市面上大部分常用应用,识别更加全面。同时,本方案能够对移动应用进行细分控制,如针对微信这一种移动 APP,我们会细分为:微信传文件、微信聊天、微信朋友圈、微信游戏这几个动作,并可以进行分别管控,让控制更加细致灵活,满足各种场景的细分需求。

不仅如此,深信服上网行为管理系统还结合 URL 识别、文件类型识别、深度内容检测、代理识别、ssl 内容识别、智能识别等技术形成一套强大的应用识别技术架构,无论网页访问行为、文件传输行为、邮件行为、应用行为等 AC 都能帮助组织形成一个全方位应用识别体系,保证识别完整准确,为上网行为管理的封堵、流控、审计提供坚实的基础。



图四 深信服应用特征识别库

### 3.3.4 非法无线热点及时发现和精准控制

通过移动 APP 识别技术、系统检测技术、HTTP 协议分析技术等多种识别技术组合方案，能够秒级发现非法 Wi-Fi 热点，将内网管理风险降到最低。支持白名单功能，能够把信任的用户或 IP 添加到信任列表，保障合法热点的正常使用，业务不中断。针对非法热点，能够选择是否封堵，满足不同程度的控制需求；发现非法热点之后，支持发送邮件给管理员进行告警，以便管理员尽早掌握网络状态，及时处理网络事件。

### 3.3.5 五维一体的识别与权限控制

深信服有线无线统一上网行为管理方案能够基于位置、应用、终端、用户、SSID 五个维度进行权限划分，满足各种场景需求：比如会议室和办公区需要区分上网权限；比如不允许非工作相关的 PC 应用、网站、移动 APP 在内网使用；比如不允许 android 系统的移动终端接入内网；比如对不同分组的用户使用不同的上网权限；比如对于接入访客 SSID 的客户只允许访问互联网，不允许访问内网等。通过多种维度权限划分，达到最低权限的管理原则，保证内网的安全可控。

## 第四章 Sangfor AC 其他优势功能介绍

### 4.1 上网行为管控更有效：上网应用识别更有效、管控更精细

1. 应用识别种类更多（2000 多种应用，600 多种移动应用）、时效性更强（2 周更新及时淘汰）、准确度更高（迅雷、PPStream、风行等全流量识别）
2. 应用控制更精细，区分动作（如社交网站的浏览、发帖回帖、上传）、区分方向（如网盘的上传，下载）
3. 应用行为标签化管理，策略部署更简单、无遗漏

### 4.2 上网行为管控更有效：流量管理更精准、控制保障两不误

1. 精确控制 P2P 上下行流量，带宽利用率提高 30%
2. 流量管理策略更灵活，呈现更直观（能够针对 URL 类型、文件类型做流控，通道流量实时可视化以及细粒度的可视化报表）
3. 动态流控，突破限制上限，不浪费带宽

### 4.3 上网行为管控更有效：外发数据识别更精确，真正防泄密

1. 多种外发途径的有效管控（网盘上传附件控制、论坛上传附件控制、邮件外发附件审计与控制、IM 外发文件控制等）
2. SSL 加密内容识别与控制（邮件客户端收发加密邮件、加密论坛审计等）