SANGFOR
深信服科技

深信服企业级 WLAN

产品白皮书

深信服科技有限公司

2015 年 6 月

版权声明

免责条款

信息反馈

如果您有任何宝贵意见，请反馈：

地址：深圳市南山区学苑大道 1001 号南山智园 A1 栋 6 楼 邮编：518055

电话：0755-8662 7913

传真：0755-8662 7913

您也可以访问深信服科技网站：www.sangfor.com.cn 获得最新技术和产品信息

目录

一、 概述

随着移动互联网的发展，移动终端的爆炸式增长，无线终端和无线应用的快速普及，极大的推动了无线网络的发展。在这个移动互联的时代，无线已经成为终端接入的主导力量。BYOD、移动办公已成大势所趋，企业 WLAN 的应用需求正在进一步加大。

在需求的激增下，带来了 WLAN 的机会，同样也存在着挑战，特别在企业 WLAN，安全、用户体验等因素往往是主要关注的问题。

1.1 最安全

无线网络的发展与普及正在改变企业网的架构，从 802.11a 到如今的 802.11ac，传输速率及调制方式均有大幅的提升 ,但企业网对网络安全及业务管控的要求均是现有无线技术所欠缺的。

相对于有线网络来说，无线网络只是依靠电波来传送与接收，入侵者可以通过高灵敏的接收设备来进行破坏与入侵。传统无线采用 PSK 认证方式存在严重的安全缺陷，各种破解手段众多 ,对于企业而言 ,可能造成内部资源信息的泄露。同时 ,一旦接入企业无线局域网，黑客通过简单的方法即可获得此网中站点的 MAC 地址，然后利用这些 MAC 伪装地址进行更进一步的欺骗攻击。

针对企业 WLAN 中存在的安全问题，很多企业采用更高安全等级的认证方式，比如 802.1x 和证书等。但是 ,安全是一把“双刃剑”,安全加强的同时 ,便捷性往往会大打折扣。接入无线这个简单的过程变得像注册个人资料时一样复杂。这不免引来终端用户的怨言 ,他们更希望能有一种简单的方式方便的接入。依靠 IT 部门在每台移动设备上手动配置网络接入设置、证书和企业应用程序，这是不现实的。

深信服的安全无线理念，即为用户提供安全接入的同时，简化配置，让安全变得高效。企业在无线接入部署的过程中 ,我们保证用户端到管理端的接入认证和数据传输的一体化安全，杜绝各式安全隐患，以免由于网络泄密造成不必要的经济损失。与此同时，多项优化措施，简化用户和管理员繁琐的配置，为用户提供便捷可靠的移动工作体验。

1.2 会营销

很多企业建设 Wi-Fi 的初衷是灵活的解决有线端的接入问题，实际上，随着人们花在智能终端的时间越来越长，企业也可以让 Wi-Fi 由网络服务转化成业务运营，让无线投资产生商业价值。

我们处在一个移动互联网的时代，所有的流量入口都是兵家必争之地，从桌面、操作系统、搜索引擎，到即时通讯工具、浏览器、智能手机，再到电视盒子、电商平台等等，归根到底都是在争夺流量。移动互联网时代，流量是血液，没了血就要死。如果商超、酒店等公共区域的无线网络能利用免费 Wi-Fi 为入口来换取广告资源、用户信息、行为数据等，无疑是如虎添翼。

深信服企业级无线解决方案在提供 Wi-Fi 服务的基础之上 ,通过内置 Wi-Fi 广告运营系统，为企业营销提供一个新的平台，如：促销信息推送、商场信息查询、活动互动等，为企业不同的业务建立高效的移动平台营销，提高创收能力，带来商业附加值。

二、 安全

2.1 接入认证

企业为无线用户提供网络接入服务，实现用户访问网络资源（例如 Internet）的需求。网络服务没有使用任何接入认证，任何人都可以直接接入，安全系数太低；不同场景安全要求不一致，企业 Wi-Fi 接入需要满足不同场景的灵活认证方式。

深信服无线控制器拥有多重接入认证方式：

MAC 地址白名单：

MAC 地址白名单是对终端 MAC 地址进行过滤，在 MAC 地址白名单之外的终端无法接入 WLAN。

开放系统认证：

开放系统认证：开放系统认证是缺省使用的认证机制，也是最简单的认证算法，即不认证。如果认证类型设置为开放系统认证，则所有请求认证的客户端都会通过认证。

WPA/WPA2-PSK：

WPA/WPA2-PSK（预共享密钥认证）：PSK 认证需要实现在无线客户端和设备端配置相同的预共享密钥，如果密钥相同， PSK 接入认证成功；如果密钥不同，PSK 接入认证失败。

WAC 支持多重认证方式结合：

- 开放式
- WPA-PSK,WPA2-PSK（个人）
- 开放式+Portal 认证
- WPA-PSK/WPA2-PSK+Portal 认证
- WPA(企业)
- WPA2（企业）
- WPA/WPA2（企业）

2.1.1 多种认证方式

2.1.1.1 802.1x 认证

WLAN 具有移动性、开放性的特点，因此需要对用户的端口接入进行认证控制，以保护无线频谱资源的利用和网络安全。IEEE802.1x 是用于无线局域网的一种增强网络安全解

决方案，提供无线客户端与 RADIUS 服务器之间的认证。

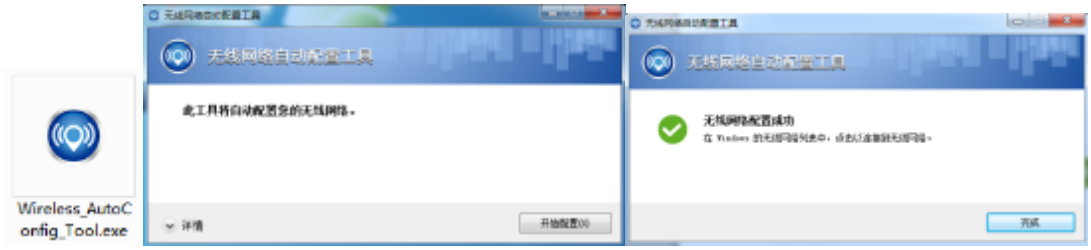
无线网络自动配置

部署 802.1x 认证的企业无线网络，对网络管理员的挑战在于，如何在不同平台，不同类型的计算机或移动终端，都能快速的接入企业无线网络，同时不降低安全性。

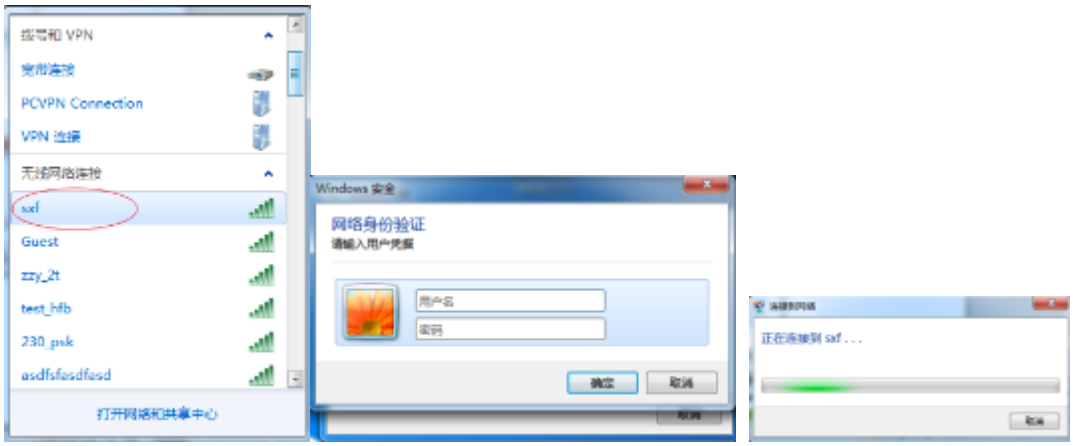
深信服科技提供 802.1x 一键配置工具 ,用户只需通过 web 界面下载网络自动配置工具，无需依赖 IT 人员的协助，一键即能完成 802.1x 的自动配置，简单便捷的加入到企业安全架构中。

1、连接开放式无线“sxf_auto_config_tools“进入 web 界面下载网络自动配置工具；

2、点击 web 页面上的下载配置工具并运行，点击开始配置，系统会自动配置好无线网络；



3、连接无线网络“sxf”，弹出网络身份验证的窗口，输入用户名和密码即可；



4、查看已连接的 sxf 的属性，WPA2 企业认证加密，类型为 PEAP，后续打开打开电脑即会自动连上无线并自动完成认证，无需重新配置。

2.1.1.2　CA 证书认证

CA 数字证书就是互联网通讯中标志通讯各方身份信息的一系列数据，提供了一种在 Internet 上验证您身份的方式，其作用类似于司机的驾驶执照或日常生活中的身份证。它是由一个由权威机构-----CA 机构，又称为证书授权（Certificate Authority）中心发行的，人们可以在网上用它来识别对方的身份。数字证书是一个经证书授权中心数字签名的包含公开密钥拥有者信息以及公开密钥的文件。最简单的证书包含一个公开密钥、名称以及证书授权中心的数字签名。

WAC 的证书管理功能可以分为以下几点：1、导入的设备证书；2、导入的 CA 证书；

设备证书和 CA 证书

设备证书用于用户接入认证的证书认证（EAP-TLS）。EAP-Transport Level Security

(EAP-TLS) 是在基于证书的安全环境中使用的 EAP 类型。如果您将智能卡用于远程访问身份验证 ,则必须使用 EAP-TLS 身份验证方法。EAP-TLS 的消息交换可以提供远程 VPN 客户端和验证程序之间的相互身份验证、加密方法的协商和加密密钥的确定。EAP-TLS 提供了最强大的身份验证和密钥确定方法。

内置 CA 证书颁发中心

CA 证书认证具有唯一性、不可抵赖性、在数据传输过程进行加密 ,拥有超高的安全性。

深信服 WAC 内置 CA 证书颁发中心，无需另外部署一台证书服务器，简化证书认证结构，实现安全的“实名制”，IT 人员可以发布唯一凭据，包括证书信息及用户和设备数据，保证设备的唯一性。同时，企业或者事业单位还可自建 CA 中心，不必购买单独的 CA 认证体系，为企业减少了投入成本。

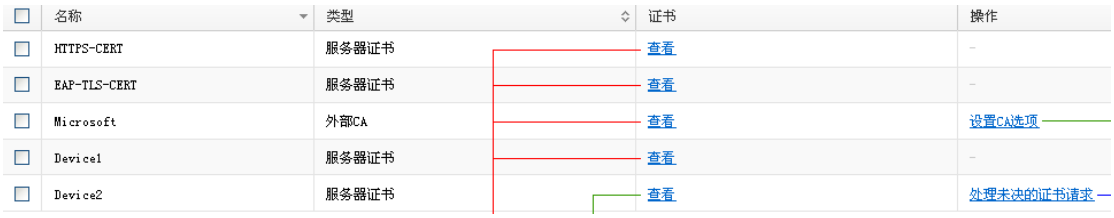
CA 证书的自动更新

WAC 支持两种显示的自动更新，包括 CRL（证书吊销列表）自动更新和 OCSP；

证书具有一个指定的寿命 ,但 CA 可通过称为证书吊销的过程来缩短这一寿命。CA 发布一个证书吊销列表 (CRL)，列出被认为不能再使用的证书的序列号。CRL 指定的寿命通常比证书指定的寿命短得多。CA 也可以在 CRL 中加入证书被吊销的理由。它还可以加入被认为这种状态改变所适用的起始日期。

OCSP(Online Certificate Status Protocol，在线证书状态协议)是维护服务器和其它网络资源安全性的两种普遍模式之一。OCSP 克服了证书注销列表（CRL）的主要缺陷：必须经常在客户端下载以确保列表的更新。当用户试图访问一个服务器时，在线证书状态协议发送一个对于证书状态信息的请求。服务器回复一个“有效”、“过期”或“未知”的响应。协议规定了服务器和客户端应用程序的通讯语法。在线证书状态协议给了用户的到期的证书

一个宽限期，这样他们就可以在更新以前的一段时间内继续访问服务器。



2.1.1.3 Portal 认证

Portal 认证介绍

Portal 认证通常也称为 Web 认证，一般将 Portal 认证网站称为门户网站。未认证用户上网时，设备强制用户登录到特定站点，用户可以免费访问其中的服务。当用户需要使用互联网中的其它信息时，必须在门户网站进行认证，只有认证通过后才可以使用互联网资源。

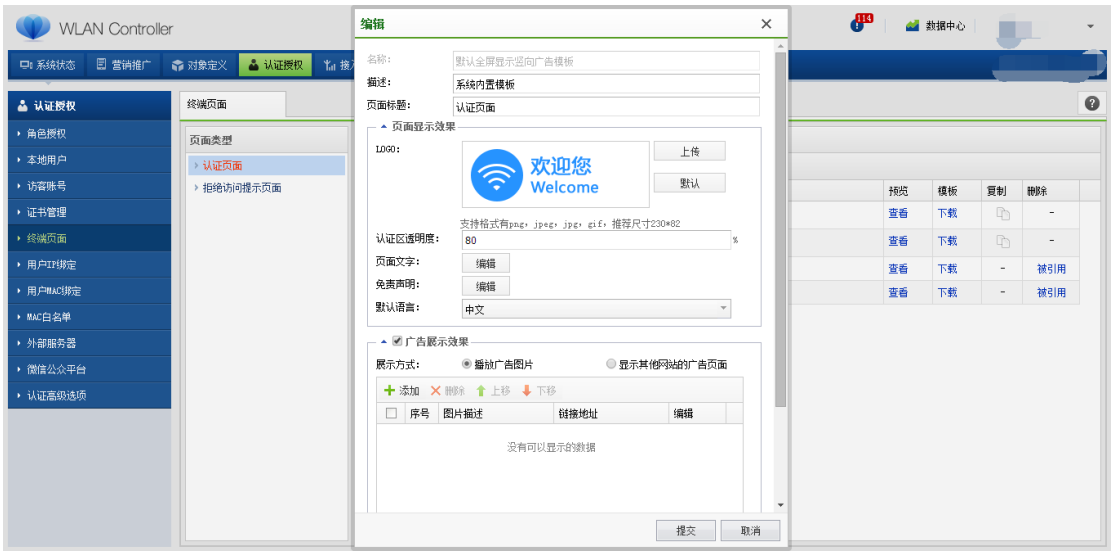
用户可以主动访问已知的 Portal 认证网站，输入用户名和密码进行认证，这种开始 Portal 认证的方式称作主动认证。反之，如果用户试图通过 HTTP 访问其他外网，将被强制访问 Portal 认证网站，从而开始 Portal 认证过程，这种方式称作强制认证。

Portal 认证实现

Portal 认证支持 WAC 本地认证（内置本地服务器，最多支持 65000 个本地账号），也支持第三方的认证服务器：RADIUS 服务器、LDAP 服务器、Windows Active Directory。

Portal 认证页面

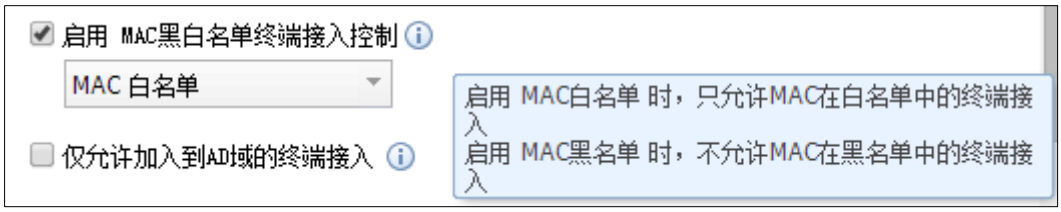
同时深信服无线支持 Portal 认证页面自定义，可方便灵活的根据自己的需求来制定 Portal 认证页面，包括但不限于页面标题、logo、背景颜色、文字描述、广告图片等信息。



支持 portal 页面预览功能，所见即所得，方便自定义个性化 portal 认证页面。

2.1.1.4 MAC 地址认证

MAC 地址认证是一种基于用户无线终端 MAC 地址的网络访问权限进行控制的认证方法，它不需要用户安装任何客户端软件，也不需要用户手动输入用户名或者密码。设备在首次检测到用户的 MAC 地址以后，即启动对该用户的认证操作。



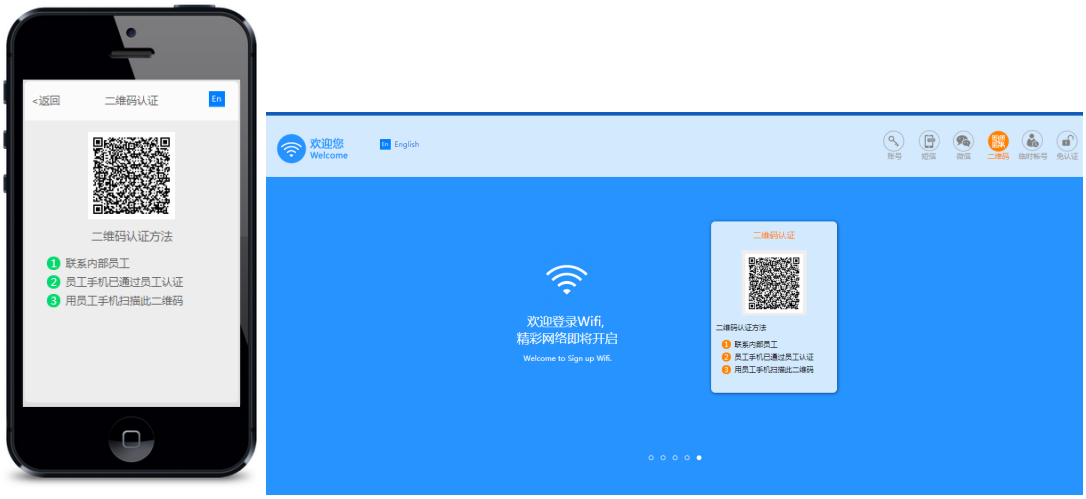
2.1.1.5 二维码审核认证

访客连接无线网络后打开浏览器，访问任意网站时，系统将页面重定向到认证页面，认证页面中会显示一个二维码，具备审批权限的内部接待人员，使用终端扫描访客的认证界面上的二维码，访客即可上网。

需要说明的是，内部接待人员的终端必须已连接到无线网络中，且能正常访问互联网。

此方式通常用于企业的访客无线网络认证，可以确保只有经过二维码审核的访客用户才具备访问无线网络的权限。认证选项中，可以设置访客的上网时长和流量配额。

简便快捷的二维码认证管理系统，有效解决了原有开放访客认证系统被蹭网的安全威胁，同时结合审计系统可以有效进行内容审计。

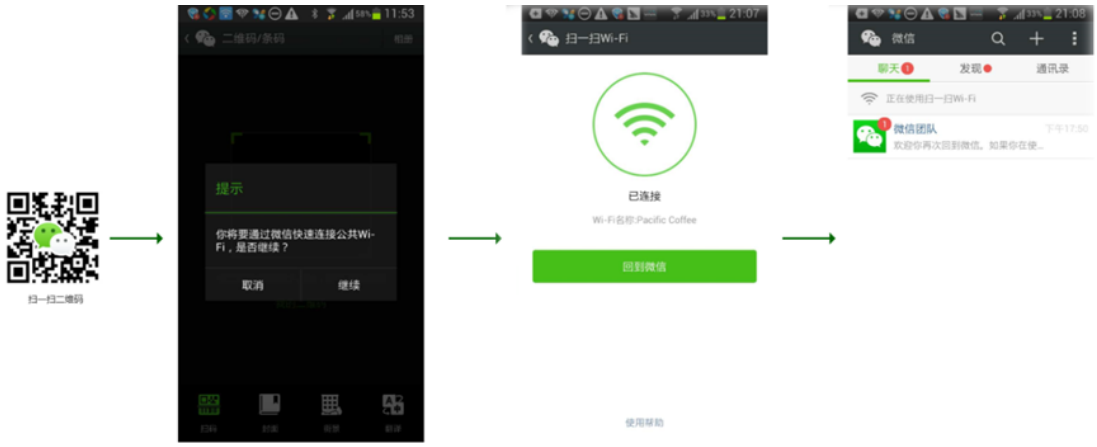


2.1.1.6 微信连 Wi-Fi

微信连 Wi-Fi 是解决传统商务 Wi-Fi 连接授权认证的一个方案，代替传统 web 认证需要用户输入用户名、密码等信息的过程，并在微信界面给予有安全性认证的 Wi-Fi 服务提供商一个信息展示广告位的入口，以充实其商业化价值。

WAC 内置微信连 Wi-Fi 功能，无需通过云平台/外挂服务器即可实现微信连 Wi-Fi。

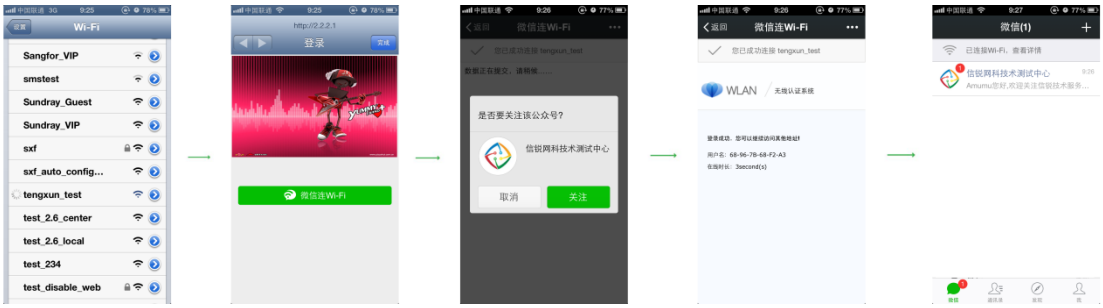
微信连 WI-FI 功能为用户连接无线网络时提供了很大的方便，提高了用户的体验性。腾讯微信连 WI-FI 功能，对于安卓手机，无需手动关联 SSID，只需用手机扫描二维码即可自动连上 SSID，自动验证后即可上网，认证过程如下图所示。



但是对于苹果 iPhone 来说，当 iPhone 扫描二维码时会提示需先关联 SSID，用户手动关联 SSID 后，自动验证后即可上网，认证过程如下图所示。。

微信连 Wi-Fi 一键关注

我司将微信连 Wi-Fi 与微信认证的优势特点进行结合互补，将微信认证一键上网与微信连 Wi-Fi 融合成深信服独有的微信连 Wi-Fi 一键上网，提升用户体验性，并增强营销功能。



深信服的微信连 Wi-Fi 一键上网将具有便捷、安全、营销能力强的优势：

1、 便捷

无需部署二维码，解决微信认证需要部署二维码的痛点，微信连 Wi-Fi 一键上网只需终端连上无线网络，点击 portal 页面的“一键关注上网”即可，

2、 安全

只有通过腾讯认证的厂商提供微信连 Wi-Fi 功能才具有“正在使用扫一扫 Wi-Fi”的标识，对于非法钓鱼 Wi-Fi 以及其他 Wi-Fi，均不会显示该标识，可以有效的预防钓鱼 Wi-Fi，保证无线网络的安全性。

除此之外，采用微信连 Wi-Fi，如果是用 QQ、邮箱注册的微信号，在认证过程中，腾讯微信会检测是否绑定了手机号码（要求绑定手机号码），若用户未绑定手机号码，系统会提示用户需要绑定手机号码，否则认证不通过（这也是公安部对腾讯的要求），当用户认证上网后，我们会记录用户的微信 openID、手机 MAC 地址、IP 地址、接入时间、访问时间等，满足审计要求。

3、 营销能力强

融合了微信认证一键关注上网的特点 ,微信连 Wi-Fi 一键上网强制要求用户关注微信公众号才能上网，有效帮助商家进行微信吸粉，并且可以获取到用户微信号 openID，实现在线广告推送、终端出现、首次接入、主动推送等微信认证的营销推送功能。

2.1.1.7 微信认证

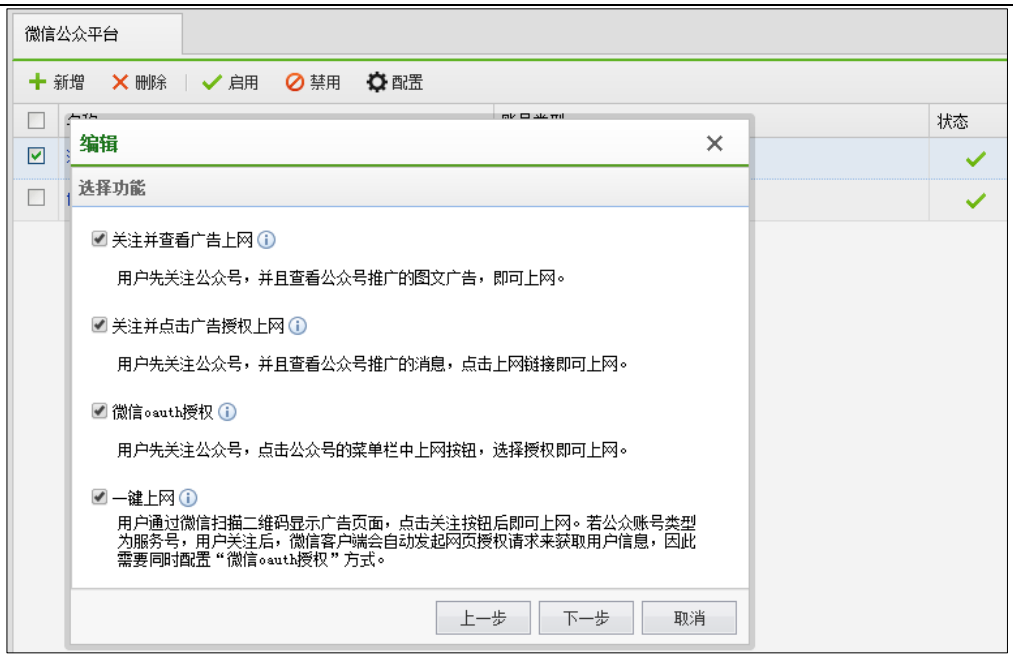
WAC 内置微信认证模块，无需通过云平台即可实现微信认证。

顾客连接 Wi-Fi 过后，无线控制器放通微信流量，让顾客可以登录微信，顾客通过关注微信公众号进行上网。

如果使用笔记本电脑等不方便使用微信的终端。登陆界面会显示一个二维码，这种情况先用手机完成微信认证，然后手机去扫一扫，完成笔记本电脑的授权。

微信认证方式不但简单快捷，而且有效的增加了企业的粉丝数量，为后期的微信营销提供基础。

WAC 支持多种微信认证方式，比如一键关注、关注并点击授权上网、关注并查看广告上网、微信 oauth 授权。



1. 一键关注

一键关注即扫描 WAC 生成的公众号二维码，跳转到关注页面，点击一键关注上网并关注公众号即可上网。

此种认证方式，无需进行任何代码开发，无需额外部署微信服务器，即能很好的满足微信吸粉的作用，且认证过程方便快捷。

2. 关注并点击授权上网

顾客关注微信公众号后，第三方服务器平台主动推送一条文本消息给用户，用户查看并点击上网链接即可上网。

顾客第二次来时，点击公众号菜单栏里我要上网，返回一条文本消息给用户，用户查看并点击上网链接即可上网。可配合广告推送服务，当用户点击上网链接后跳转到广告页面，即可上网。

此种认证方式，需要进行微信公众号的代码开发（控制器会自动生成代码，植入到微信公众号即可），可以获取到用户的微信昵称和 openID 等信息。

此种认证方式相比于一键关注，可以提供更丰富的微信增值营销功能，比如在线时长推送、终端出现推送、离线主动推送等。

3. 关注并查看广告上网

顾客关注微信公众号后，第三方服务器平台主动推送一条图文广告给用户，用户查看并等待图片加载完成后即可上网。

顾客第二次来时，点击公众号菜单栏里我要上网，返回一条图文广告给用户，用户查看并等待图片加载完成后即可上网。

此种认证方式同“关注并点击授权上网”，需要进行微信公众号的代码开发（控制器会自动生成代码，植入到微信公众号即可），可以获取到用户的微信昵称和 openID 等信息。

此种认证方式相比于一键关注，可以提供更丰富的微信增值营销功能，比如在线时长推送、终端出现推送、离线主动推送等。

4. 微信 oauth 授权

微信 oauth 授权分有感知 oauth 授权和无感知 oauth 授权两种方式。

有感知 oauth 授权

顾客关注微信公众号，进入微信公众号点击网页授权，系统会弹出一个授权界面，点击“允许”后即可上网（点击取消则无法上网）。

无感知 oauth 授权

顾客关注微信公众号，进入微信公众号点击网页授权，即可访问无线网络。

有感知授权和无感知授权的区别

有感知授权点击菜单栏会弹出授权界面，能获取到微信用户 openID、昵称等信息；无感知授权点击菜单栏不会弹出授权界面，只能获取到微信用户 openID，不能获取比如昵称等信息。

2.1.1.8 短信认证

短信认证是一种具有增值意义的、方便的、快捷的认证方式，可以帮助商家收集用户的手机号码，进行短信营销。

WAC 内置短信认证模块，终端连接 Wi-Fi 后，在短信认证界面里输入自己的手机号码，点击获取验证码，验证码会通过手机短信的形式发送到用户手机上，用户查看后并输入收到的短信验证码，点击登录即可上网。

深信服的短信认证相比于其他厂商的短信认证，具有一次认证，永久有效的特点，即只需首次接入时获取验证码，后续上网直接点击登录即可接入互联网，对于部署无线的客户来说，减少了短信支出费用；对于用户来说，提高了上网体验。

2.1.1.9 微信认证+短信认证

微信认证+短信认证相比单独微信认证增加了短信认证，用户关注微信公众账号后，点击菜单栏申请上网后，还需要输入手机号码来获取验证码。

场景适用于需要同时收集用户的微信账号以及手机号进行营销的客户。

2.1.1.10 临时访客认证

此方式通常用于企业、酒店的访客无线网络认证，可以在访客登记后，接待人员创建一个临时帐号，并设置帐号的有效期。访客使用此帐号完成无线网络认证。

以酒店的部署场景为例，顾客连接无线网络的过程如下：

1、顾客在酒店前台登记入住。

2、酒店的前台工作人员，在访客管理系统中，为此顾客添加一个临时帐号，以手机号或者身份证号码作为帐号的用户名，密码为手机号码或身份证号码的后 6 位。帐号的有效时间设置为顾客的离店时间。

3、顾客连接到酒店的无线网络，例如无线网络名称为：Example-Guest。

4、打开浏览器，访问任意网站，系统将把浏览器重定向到认证页面。

5、在认证页面中，输入此临时帐号及密码，完成无线网络认证。

6、顾客离开酒店后，帐号自动失效。

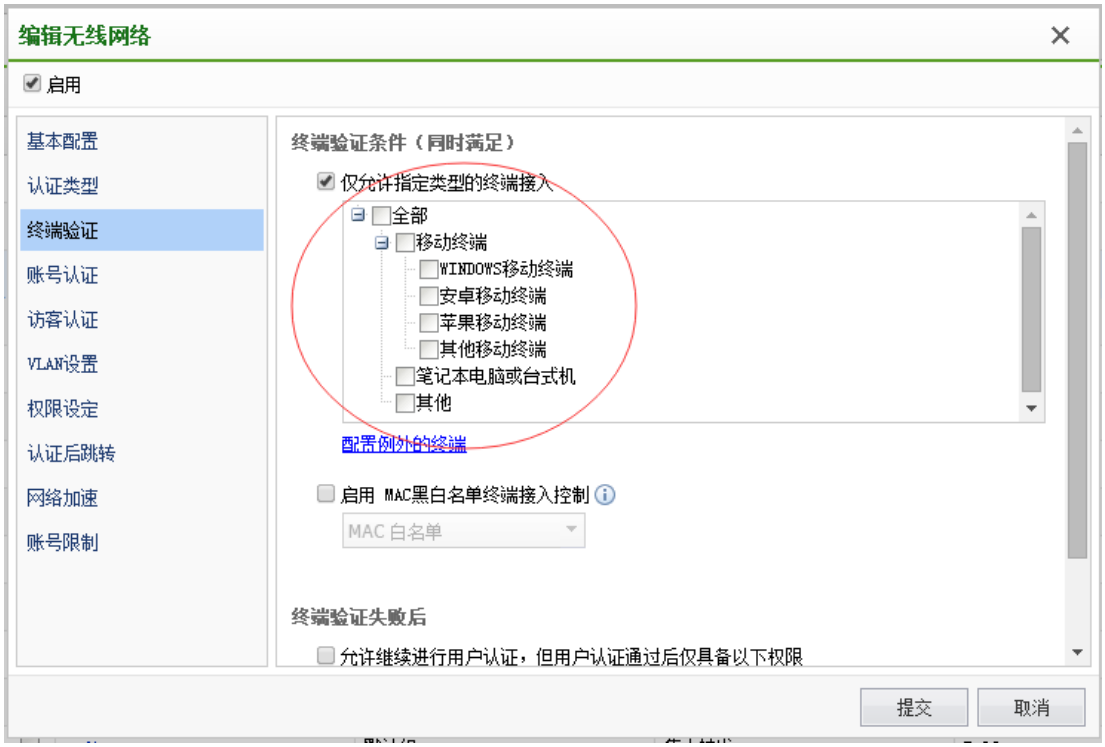
此外，临时访客支持以二维码的形式打印出来，贴在前台或酒店房间显眼位置，用户只需通过二维码扫描工具（同微信扫一扫，QQ 扫一扫）直接扫描二维码，无需手动输入上网账号和密码即可连入无线网。

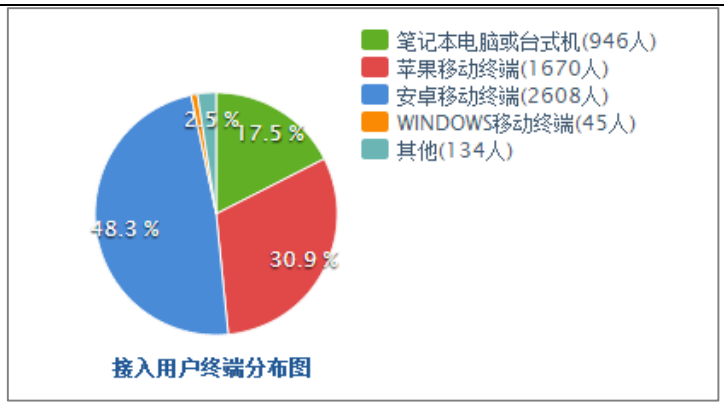
2.1.1.11 用户免认证登录

为了简化客户接入无线网络的步骤，节省客户时间，以及保护客户个人隐私，可以使用免用户认证方式登陆。用户在关联无线网络后，点击登录按钮，即可开始上网。

2.1.2 终端识别与准入

智能终端识别，能够对市面上主流终端进行精准识别，比如安卓、苹果、Windows 等智能移动终端以及笔记本和台式机，根据识别的终端类型进行接入权限控制，以及 ACL 控制。





2.1.3 第三方认证

通过 WAC 内置的本地认证服务器，可以实现 802.1x、CA、Portal 等认证，但有时候需要给不同用户、不同部门授予不同的授权，需要规划和建立组织的用户分组结构，或者需要关联已有的认证信息库，此时就需要支持第三方认证。

WAC 支持关联外置认证数据库 ,兼容的第三方的认证服务器有 :RADIUS 服务器、LDAP 服务器、Windows Active Directory。

一般组织均有自己的行政结构 ,WAC 可以完全按照组织的行政结构建立树形用户分组，实现父组、子组等多层嵌套的要求。在完成用户组的创建后，即可创建用户，并将用户分配到指定的用户组中，以实现网络访问权限的授予。用户创建的过程简单方便，除手工输入帐户方式外，WAC 能够根据 OU 或 Group 读取 AD 域控服务器上用户组织结构，实时的 AD 查询功能方便管理员管理运维。

实时 AD 查询，又叫做组织架构的同步，用于管理认证通过的无线终端。

WLAN 配置的认证服务器是 LDAP 服务器时，WAC 会和配置好的 LDAP 服务器同步服务器上面的组织结构，包括用户的组信息。

例：

无线终端接入到 WLAN 以后，可以通过同步的组织信息，以树形结构来管理在线的用户。

2.2　精细化的角色授权

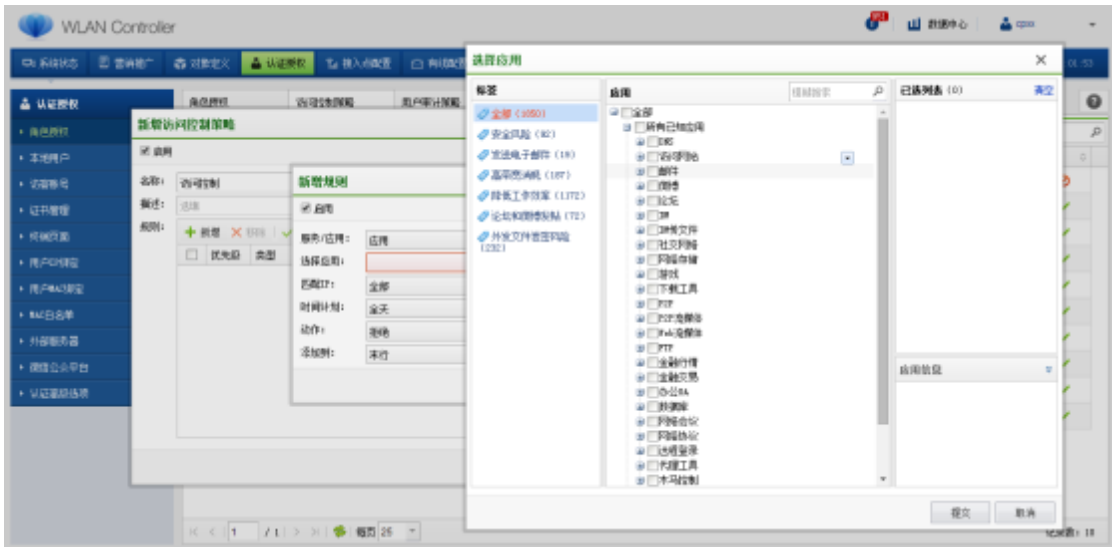
用户接入认证和加密可以实现用户的安全接入，而无线终端通过了用户接入认证以后，需要给用户分配正确的角色来实现授权管理 ,精细的管控每一个上网用户的网络访问权限和使用规范。

2.2.1 访问控制

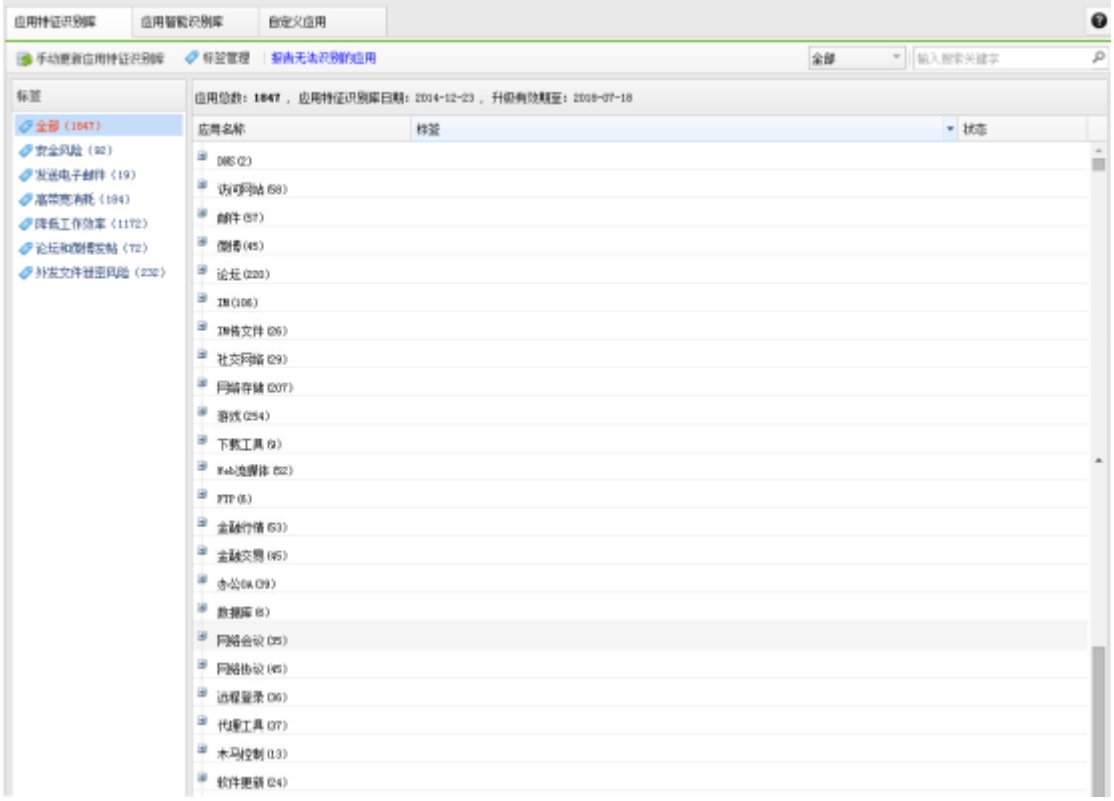
2.2.1.1　基于应用的访问控制

无线控制器内置国内最大的应用识别库，能够对主流网络应用进行识别，能精确识别包括办公应用、金融股票、IM、网络游戏、P2P、移动终端应用等 1800 余种应用。

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。



应用识别库一览：



2.2.1.2　基于服务的访问控制

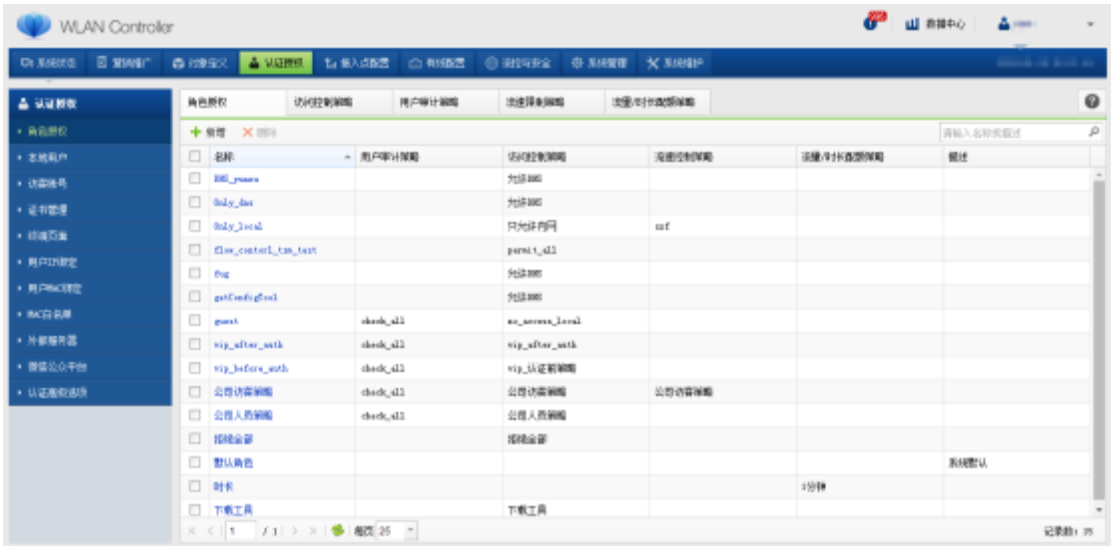
WAC 支持基于服务、协议、端口的访问控制，全面管控用户上网行为。即使控制器作为本地转发模式部署在网络中，访问控制策略也生效。

2.1.4.2 URL 网页过滤

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。

2.2.2 身份授权

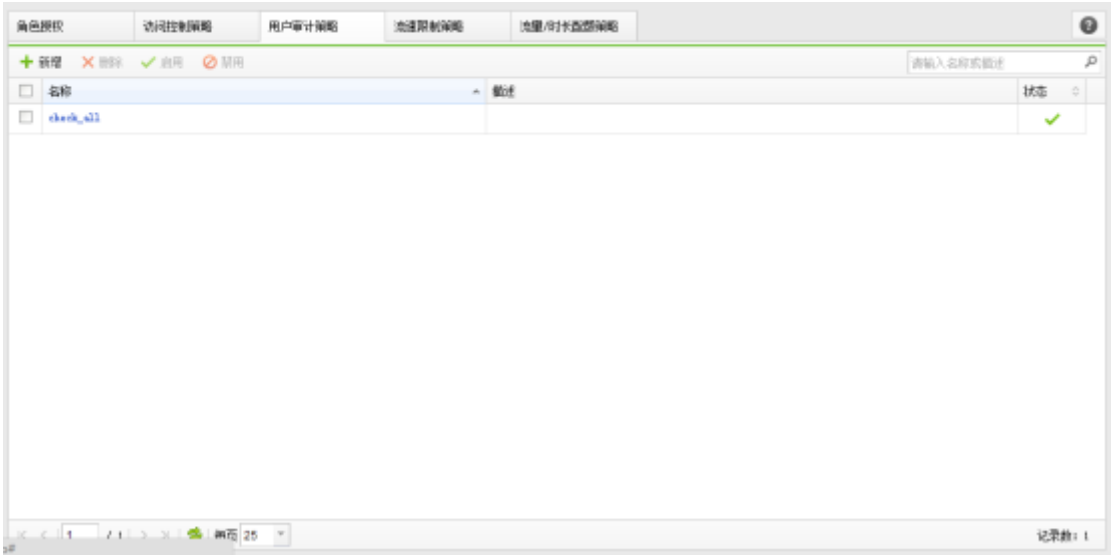
WAC 通过角色分配来达到用户权限控制，在接入 WLAN 以后，通过认证的无线客户端可以分配到一个角色，角色包含了访问控制策略、用户审计策略、流速限制策略、以及流量与时长配额策略。



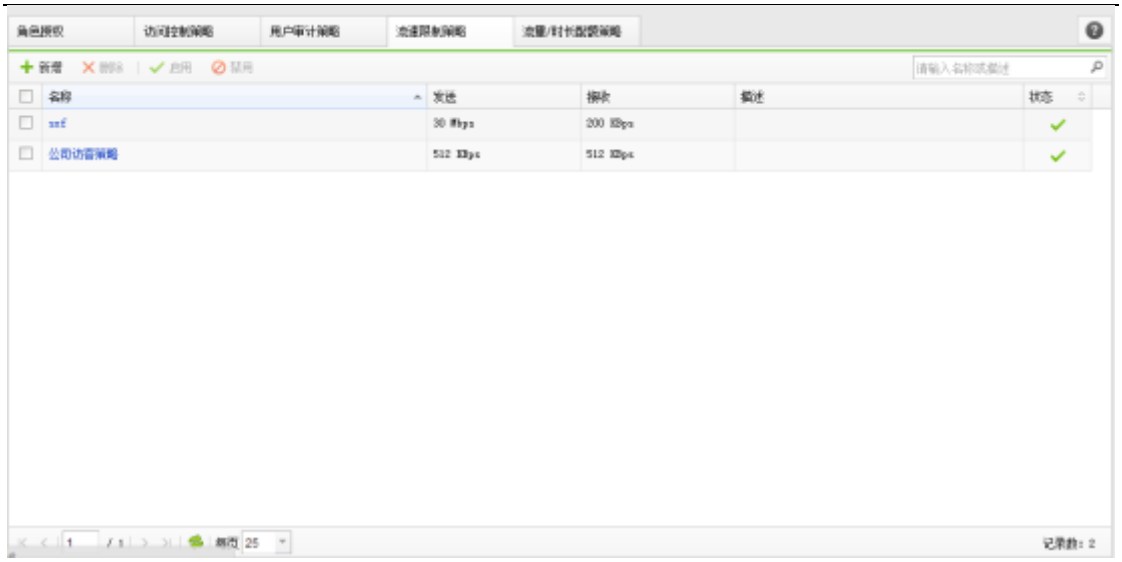
WAC 以角色的方式分配给每个用户，每个用户在不同的认证阶段拥有不同的角色。不同的角色就需要拥有不同的访问控制策略。

角色授权一览

访问控制策略一览



用户审计策略一览



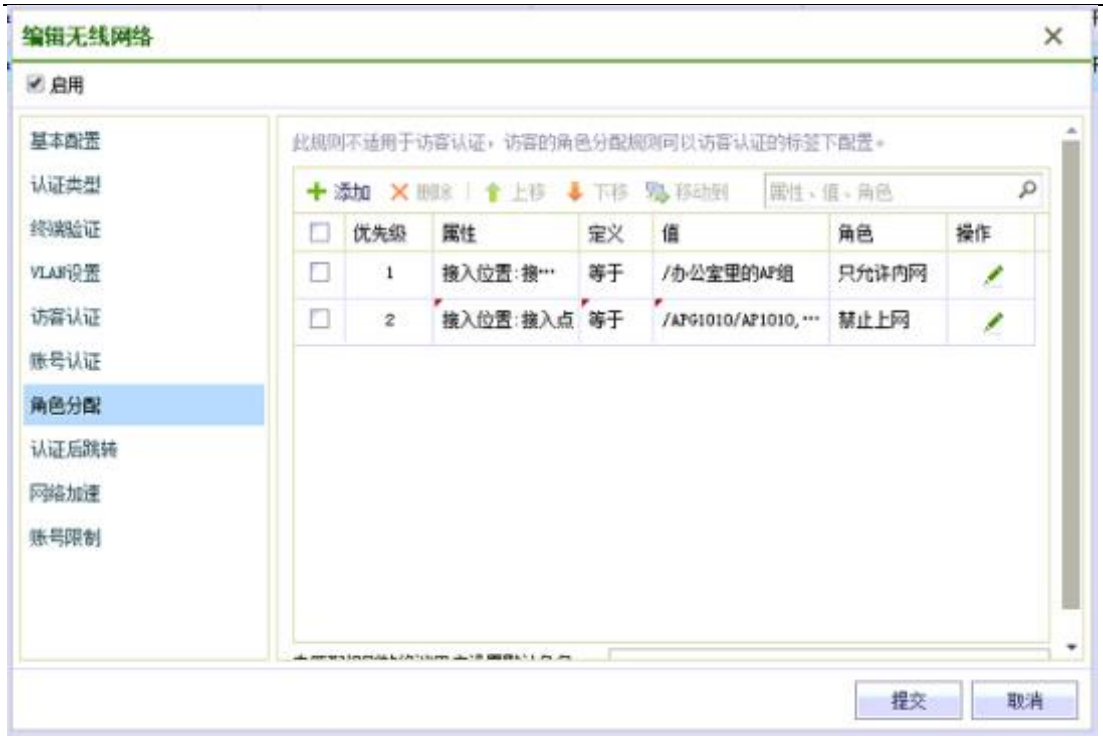
流速限制策略一览

1、 根据用户身份分配角色

在一个无线网络中，不同身份的用户，不能跨越界限访问其他团队的网络。WAC 提供根据用户身份分配不同权限的功能。可以用来区分用户身份的有：用户名、用户组、AD 域分组、RADIUS 属性、证书内容等。

2、 根据接入位置分配角色

对于公司来说，员工不在办公室内，就不应能访问办公内网。这是保障公司机密不泄露的基本前提条件。WAC 可以根据用户的接入位置，给用户分配不同权限的角色。



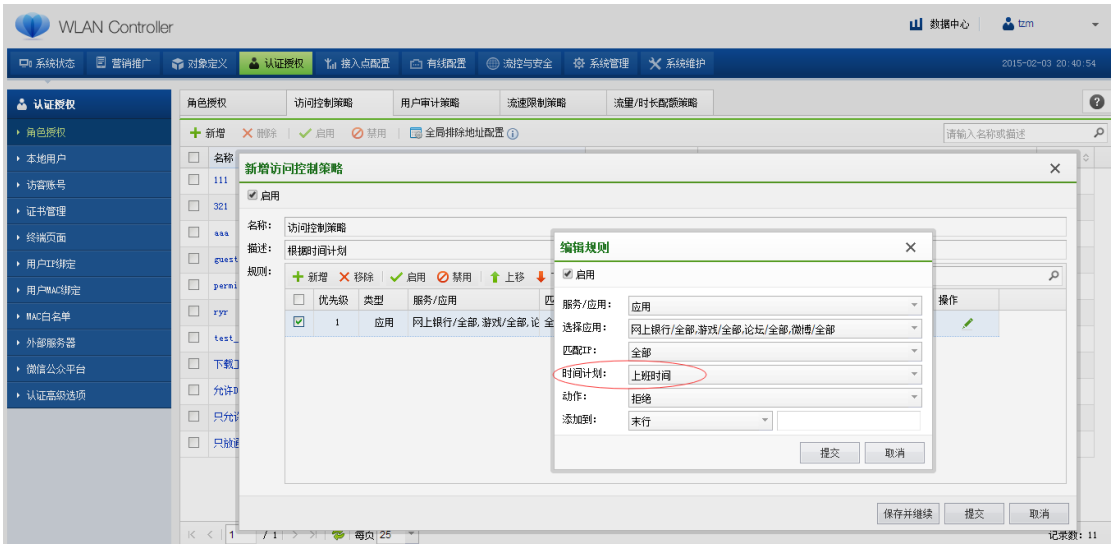
3、 根据终端类型分配角色

WAC 设备支持根据终端类型分配角色。我们可以为移动终端分配能访问外网的角色，同时为台式机和笔记本分配只能上内网的角色。这样我们就能避免公司员工利用工作资源上网，同时有满足必要的上网需求。

组建的访客网络时，往往只希望手机、平板移动终端接入，而不希望用户使用笔记本接入。这时可以使用终端验证功能，支持的客户终端类型包括：安卓移动终端，苹果移动终端，Window 移动终端，笔记本或台式机。

4、 根据控制时间段分配角色

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。



5、 根据用户属性控制用户接入

一栋建筑里，不同的团队总会有各自专属的无线网络，并且不希望团队之外的成员使用这个网络。例如研发人员不能去接入销售部门的无线网络，市场人员也不能接入研发的无线网络。无线网络控制器可以根据用户的属性，限制禁止团队的用户接入。

支持的用户属性包括：

- 用户名

- ❑ 用户分组
- ❑ AD 域分组
- ❑ Radius 属性
- ❑ 证书内容

2.2.3 流量和时长配额策略

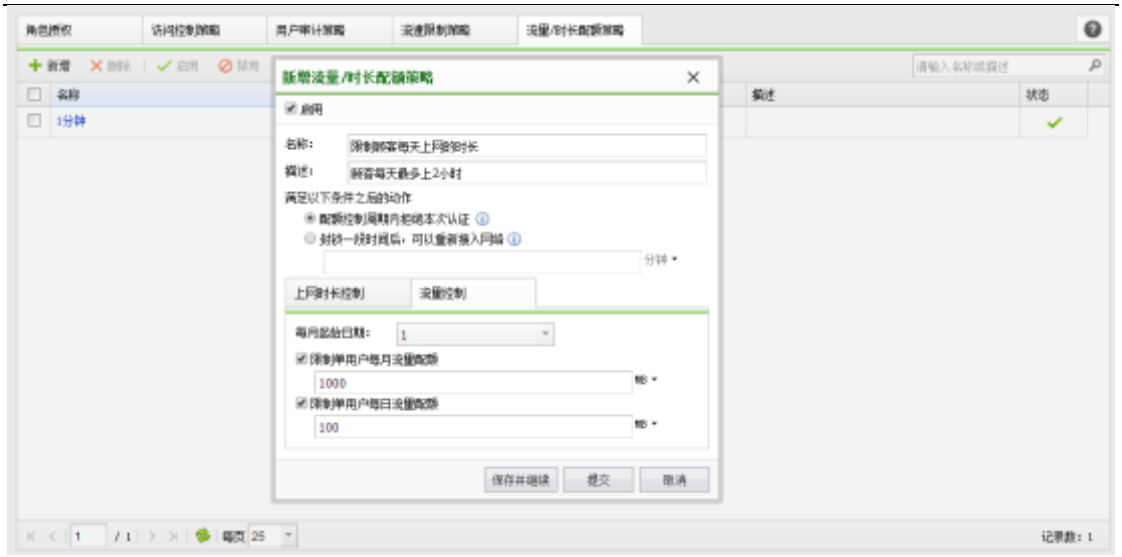
为了保护在线用户的上网体验，避免附近用户的蹭网行为，无线控制器可对用户上网流量或上网时长进行策略控制。

时长控制

可以自定义统计控制时间计划，在该时间段内限制上网时长（精细到分钟），比如按天计算，每天只允许上 2 个小时。

流量配额

设置每月起始日期，限制单用户每月流量配额和每日流量配额。



当达到阈值后

支持两种动作：

1、 拒绝接入，加入黑名单，控制时间段内提示用户认证失败

2、 封锁一段时间后时长、流量重新计算

2.3 上网行为审计

上网行为审计 ,支持对无线用户和有线用户的网络行为和内容进行审计 ,包括但不限于：HTTP 外发内容、访问网站/下载、邮件、FTP、Telnet、网络应用行为、网络应用使用流量与时长，审计记录的内容保存在设备的数据中心。

深信服 WAC 上网行为审计内容满足公安部令第 82 号，具体内容如下。

HTTP 外发内容

Web BBS 发帖；外发的 Webmail 邮件；通过网页上传的附件（包括 webmail 附件）；通过网页上传的文本；微博（可包含微博附件（图片、视频、音乐））

访问网站/下载

通过内置的千万级 URL 预分类库，可选择需要审计的 URL 类型，审计内容包括：网页地址和标题；网页内容；下载文件的文件名（不支持 URL 类型过滤，即对所有 URL 类型产生的下载文件进行进行审计）

邮件

SMTP 发送的邮件和 POP3/IMAP 接收的邮件正文内容和附件

FTP

通过 FTP 上传的文件（文件名及内容）；通过 FTP 下载的文件（仅文件名）

Telnet

通过 Telnet 执行的命令

网络应用

使用已识别的网络应用产生的用户行为；未知的网络应用（记录地址及端口），

网络应用使用流量与时长

统计用户使用网络应用的流量以及时长

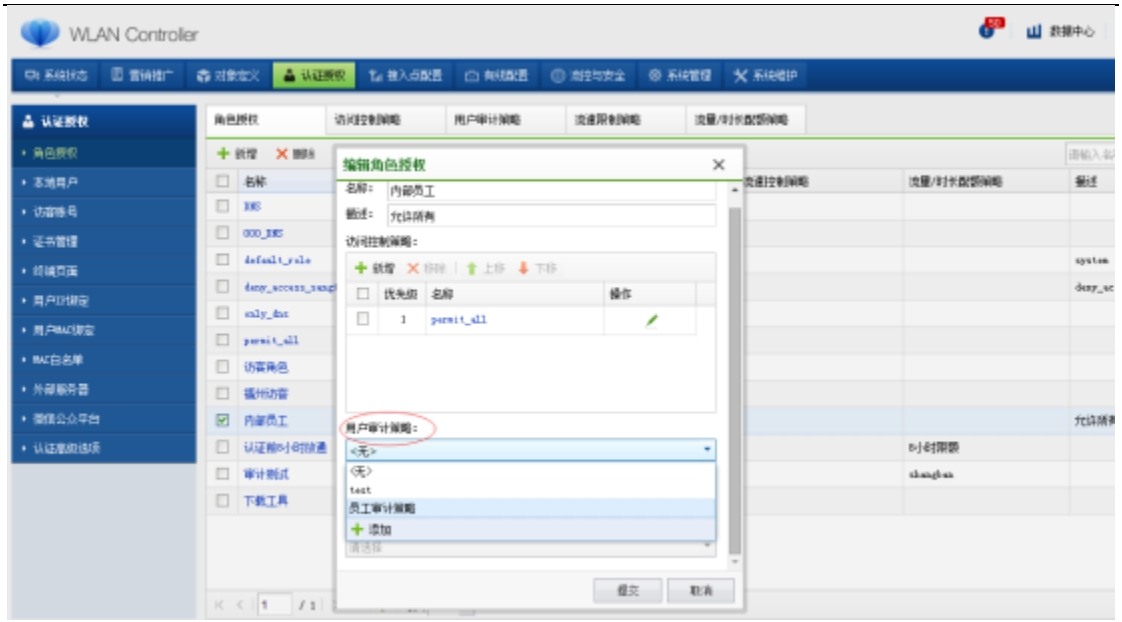
注意：

上网行为审计只审计用户访问网络的流量，包括有线用户和无线用户；但不审计用户间的流量，即不审计内网流量。

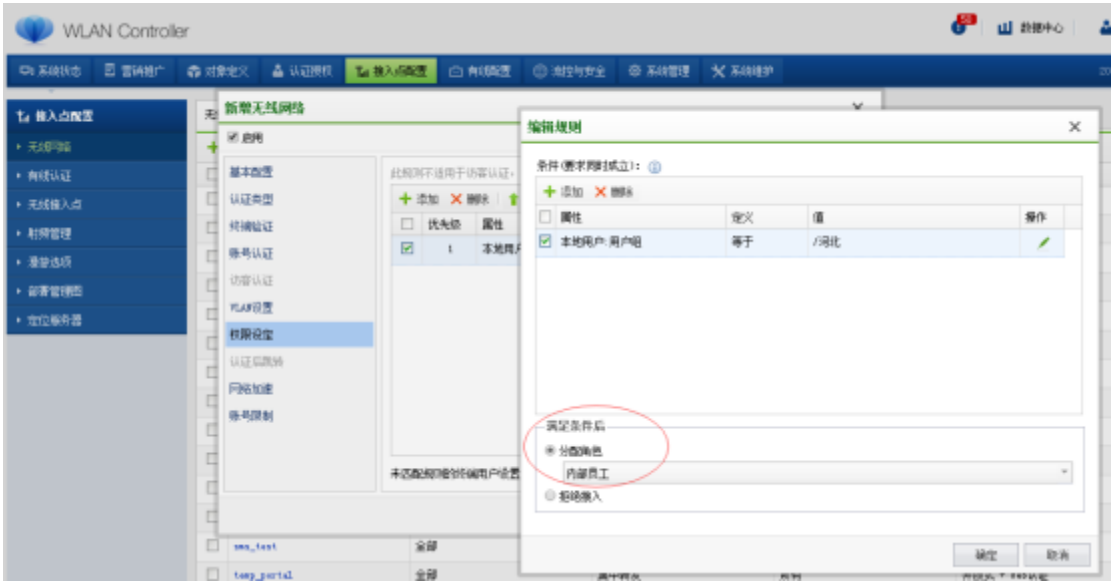
配置指南

1、在角色授权->用户审计策略，配置相应的审计策略，即需要审计的内容；

2、建立角色权限，在角色授权中用户审计策略引用建立好的用户审计策略；



3、在无线网络->新增->权限设定里将角色授权分配下去。



2.4　攻击防御

2.4.1 无线射频防护

2.4.1.1　射频防护

钓鱼接入点及随身 WI-FI 检测

网络中未经授权或者有恶意的 AP，它可以是私自接入到网络中的 AP、未配置的 AP、攻击者操作的 AP。这些 AP 上面部署了和无线控制上面有相同或是相似 SSID 的无线网络，终端用户接入这些 SSID 的无线网络之后，账号等一些隐私信息可能会被窃取。

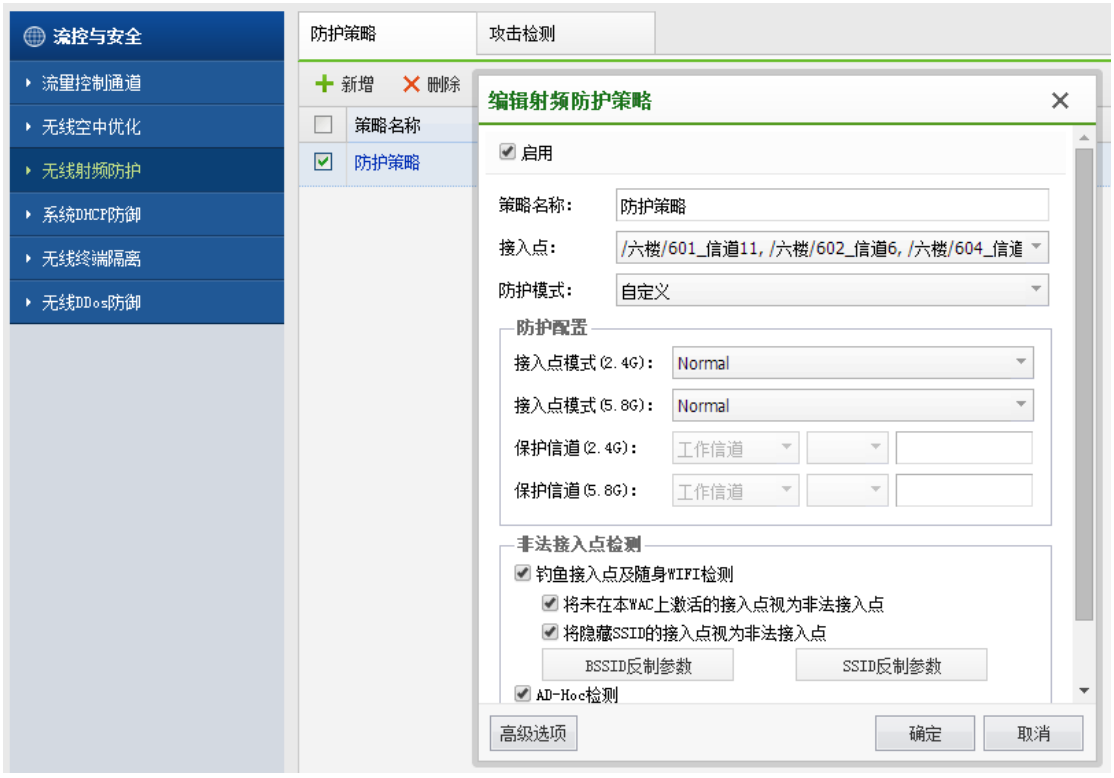
AD-Hoc 检测

把无线客户端的工作模式设置为 Ad-hoc 模式，Ad-hoc 终端可以不需要任何设备支持而直接进行通讯。

邻居 AP 干扰检测

和钓鱼 AP 类似。区别在于这一类 AP 通常不是恶意的，只是检测到的信号强度超过一定阀值（阀值可配置）。

WAC 拥有 WIDS/WIPS 功能，通过 WIPS，可以对非法接入点进行检测以及反制，可以对具备某些特性，如特定 SSID（与原网络相同或相似）、非法 AP 的 MAC（物理地址）或者非无线控制器所管理的 AP 发射出的无线信号，进行时时扫描、检测，对检测到的钓鱼 Wi-Fi 后可对其进行反制，广播相关报文给用户终端，让其不接入到非法接入点。



2.4.1.2　攻击检测

泛洪攻击（Flooding 攻击）检测

无线控制器在短时间内接收大量同种类型的报文，将导致系统资源被大量占用，可能无法处理无线用户的数据报文。启用泛洪攻击检测可以识别此类攻击，并自动将发起攻击的终端 MAC 地址添加到黑名单，一段时间内禁止接入无线网络。

欺骗攻击检测

欺骗攻击是指攻击者假冒其他设备/终端的名义发送报文。

例如：假冒无线接入点的身份，向无线客户端发送解除认证的报文，导致无线终端断开无线连接。启用欺骗攻击检测可以识别此类攻击，将发起攻击的终端 MAC 地址添加到黑名单，一段时间内禁止接入无线网络。

BSSID 冲突检测

BSSID 冲突检测是指检测到环境中 BSSID 地址冲突，可能会造成无线终端接入到有冲突的 BSSID 的 AP，会造成网络掉线，丢包等不可预知的情况。

2.4.2 防 DoS 攻击

DoS 攻击是一种基于网络的、阻止用户正常访问网络服务的攻击。DoS 攻击采用发起大量网络连接，使服务器或运行在服务器上的程序崩溃、耗尽服务器资源或以其它方式阻止客户访问网络服务，从而使网络服务无法正常运作甚至关闭。

我们提供的解决方案：

1. 限制每个终端的并发连接数（可配置）：一个终端（以 mac 为单位）统计当前该终端 session 总数，超过配置数则视为超限，不允许新建连接，不加入动态黑名单即不踢出去。

2. 终端 SYN 攻击检测：检测每秒发起的 SYN 包个数，超过配置的数目即认为发生攻击，拒绝所有数据包，并加入动态黑名单。

3. 小包攻击，可定义小包大小，如果在短时间雷小包个数超过配置数目则视为攻击（不区分五元组），拒绝所有数据包，并加入动态黑名单。统计小包个数时，如果终端发出了若干大包能够抵消相同数量的小包数，有若干发往终端的数据包（不区分大小）也能抵消相同数量的小包。

4. 用户可设置白名单功能，白名单中最多可以配置 256 个 MAC 地址，处于白名单中的 MAC 地址不受此功能控制。

2.4.3 动态黑名单

动态黑名单是用户隔离功能之一。当发现某个终端对系统网络发起恶意攻击，可以把它添加到黑名单中，从而实现隔离。

2.5 安全扩展

2.5.1 自动 VLAN 划分

支持基于用户/用户组、接入 AP /AP 组、终端类型/终端 MAC、RADIUS Class 属性值/Group ID、AD 属性值、证书属性值自动进行 VLAN 划分，终端接入时自动分配到相应的

VLAN 池中。

2.5.2 数据加密

保护无线链路数据的私密性，是所有无线网络均需要面对的挑战。与有线网络不同，只要持有适当的接收设备，任何人均可以被动监听帧且加以分析。

为了避免数据沦落到“不对的”人手中，必须对数据进行加密，防止数据被攻击者取得。WLAN 提供了一系列的加密协议，只允许拥有密钥的授权用户访问数据，同时确保数据在传输过程中未遭篡改。

数据加密方式

WAC 支持两种数据加密方式：

1、临时密钥完整性协议(TKIP)；

2、计数器模式密码块链消息完整码协议（CCMP）。

2.5.3 账户与终端 mac 绑定

为防止非法用户窃取合法账户后，使用未经认证的终端接入无线网络，无线控制器可以将账户与终端 MAC 地址绑定。如果非法用户使用终端与绑定列表中的不一致，无线控制器可以拒绝该用户登录。如果非法用户尝试用黑客手段仿造终端 MAC 地址，无线控制器还可以根据终端类型判断是否是合法的终端。

客户只需要经过如下步骤，就可获得账户与终端 MAC 绑定：

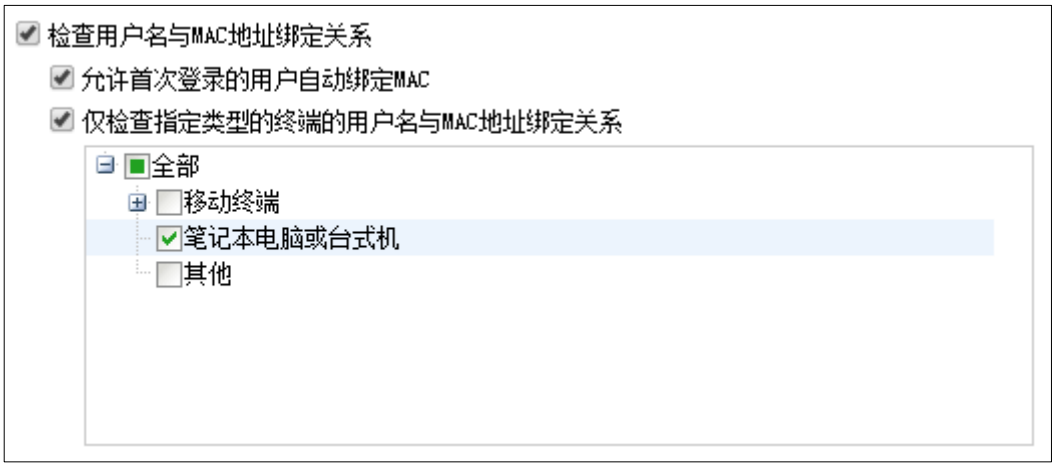
1、 在客户自己的手机上关联无线网络，并输入账户名和密码登录，例如账户名 test、密码 passwd，然后点登陆。此时页面会提示客户还无法通过认证。

2、到无线网络控制器的用户 MAC 绑定页面，审批账户 test 的绑定信息。

3、客户再次在手机上以账户 test 身份登陆，登陆成功。并且此后这个账户只能在客户的手机上登陆无线网络，无法在其他地方登陆。

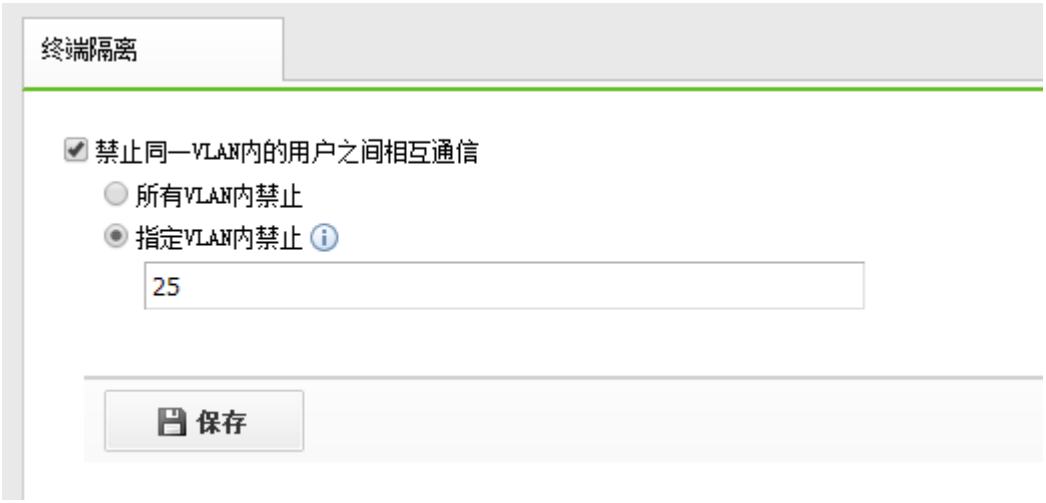
用户与终端自动绑定

可实现用户首次登录时，系统自动完成账号与终端 MAC 绑定，无需管理员参与，实现“人-机”唯一对应。同时，针对用户拥有多种终端的情况，可实现用户与多终端绑定关系，防止越权访问，加强安全性。



2.5.4 VLAN 内终端隔离

在无线网络部署时，启用此 VLAN 内用户隔离功能选项，禁止同一 VLAN 内的用户之间相互通信，可以减少同一个 VLAN 内无线终端间的广播报文，提高了无线网络性能，同时提高了安全性。还有避免某些感染了病毒的终端传播病毒的风险，最大限度地确保办公安全，提高办公效率，保障用户无线体验。

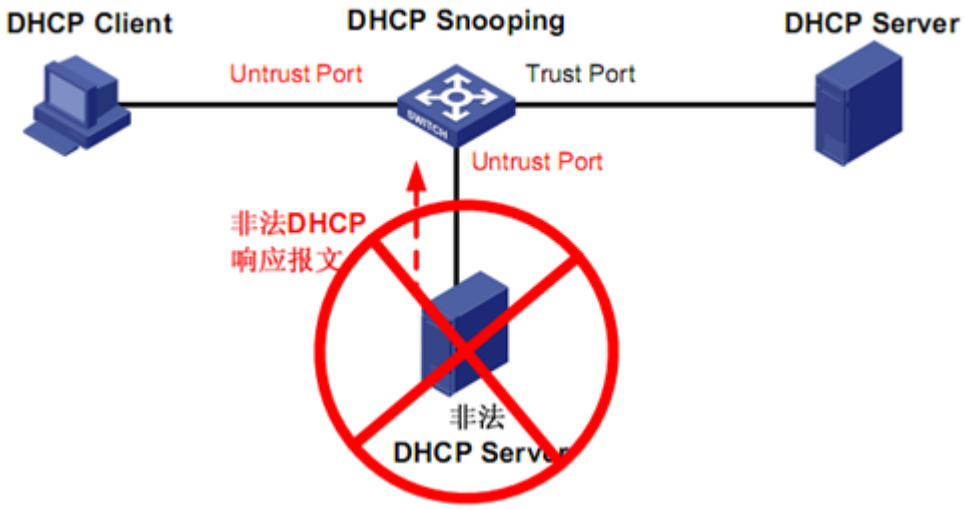


2.5.5 DHCP 防御

深信服无线控制器拥有 DHCP 防御功能，包括 DHCP Snooping、禁止客户端使用静态 IP 地址两种。

DHCP Snooping

启用“受信任的 DHCP 服务器”选项，并配置合法的 DHCP 服务器 IP 地址，无线控制器及接入点将只转发来自受信任 DHCP 服务器的 DHCP 报文，来自其它 IP 地址的 DHCP 服务报文将被丢弃，从而保证 DHCP 服务能正常运行，不受干扰。



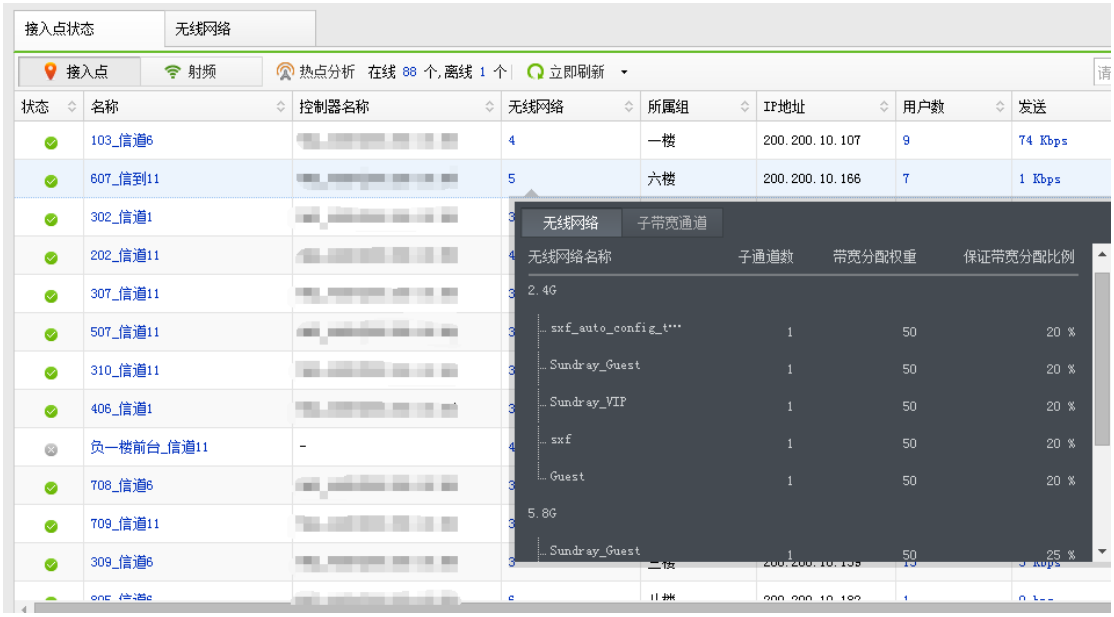
禁止客户端使用静态 IP 地址

在绝大部分的无线网络部署中，无线客户端都使用 DHCP 方式获取 IP 地址、网关、DNS 等。因此，为了避免手动配置静态 IP 地址可能带来的 IP 冲突问题，深信服科技提供了禁止配置静态 IP 地址的功能。

深信服科技支持根据 VLAN 来设定静止客户端使用静态 IP 的功能，可以在所有 VLAN 中禁止或指定 VLAN 中禁止。启用此功能的额外好处是，可以阻止无线客户端进行 ARP 欺骗攻击。

2.5.6 虚拟 AP

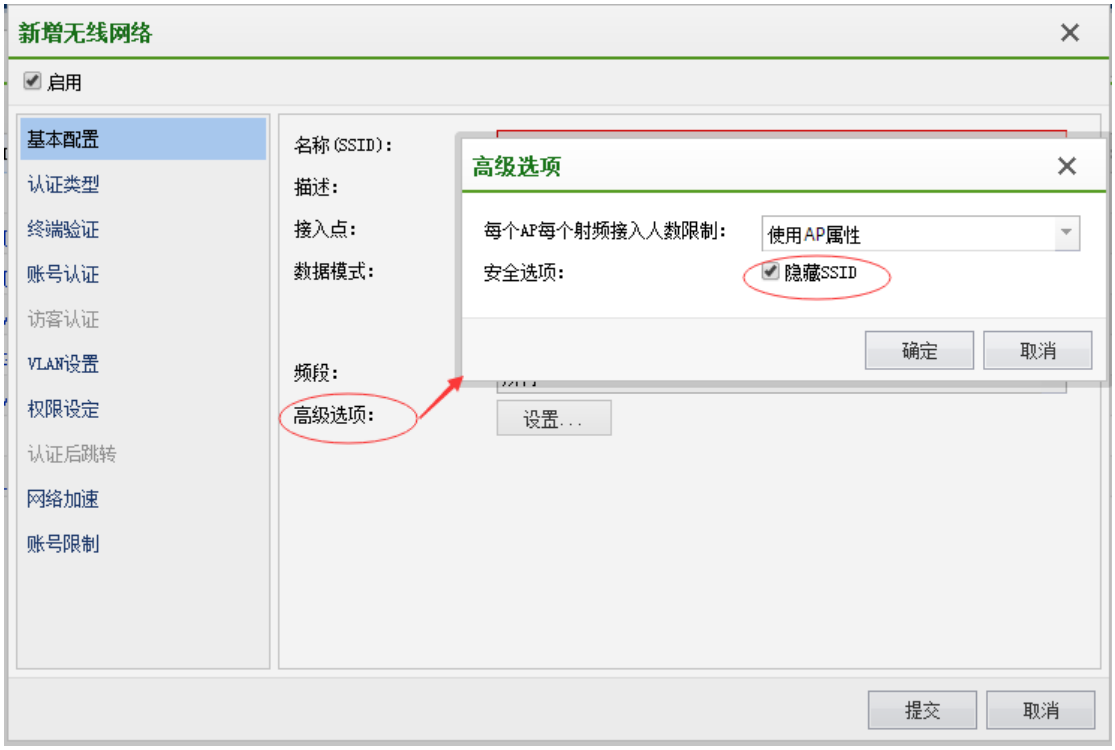
虚拟 AP（Virtual AP）又名多 SSID，即一个 AP 可以同时发射多个 SSID，深信服无线控制器最多支持 32 个 WLAN，具体数量由 AP 决定（单频 AP 可以同时发射 16 个 SSID，双频 AP 可以同时发射 32 个 SSID），不同 SSID 间是完全独立的，且是互相隔离的，通过虚拟 AP 满足不同人员接入不同的无线网络。



2.5.7 隐藏 SSID

在无线网络中，AP 会定期广播 SSID 信息，向外通告无线网络的存在，无线用户使用无线网卡搜索可以发现无线网络。为避免无线网络被非法用户通过 SSID 搜索到，并建立非

法连接，可以禁用 AP 广播 SSID，隐藏无线 SSID，当开启了隐藏 SSID 功能后，无线终端必须手动配置该 SSID 标识才能接入 AP。



三、 增值营销

随着现代城市生活步伐的加快和移动终端的快速普及，人们对无线的需求已经成为一种习惯，无线网络越来越多的影响着人们的生活方式。

当下，上网刷微信、朋友圈、看视频、玩游戏等已成为人们主要的娱乐方式，绿色实用的免费 Wi-Fi 更加受到人们的追捧。为了迎合了大众需求，为人们创建了一个安全稳定的上网环境，众多商场、酒店、餐馆、咖啡馆等陆续为顾客建立免费 Wi-Fi。如今，很多商家花费大量的资金建设的无线网络，回报能力且低的可怜，正是因为他们采购的是传统的无线网络设备，缺乏 O2O 增值营销、广告投放等功能。

深信服科技为商家提供稳定、快速的无线网络的同时提供丰富、多样式的营销增值功能，包括微信营销、短信营销、网页广告营销等等，且可以在顾客接入认证前、认证后、在线时、离店后进行广告投放，真正实现 Wi-Fi 的增值营销。

3.1 用户行为精准营销

用户行为精准营销，即关键字营销。关键字营销是目前业界只有深信服唯一一家拥有的精准 O2O 营销功能，这种基于关键字的网络营销模式由搜索引擎公司首创，是目前最为流行和有效的网络营销模式。

深信服关键字营销通过匹配用户在百度、谷歌等搜索引擎或淘宝、京东等手机 App 内搜索的内容进行精准匹配，根据预设置的关键字组进行广告推送，推送形式支持网页内嵌 banner 广告、微信、短信三种方式向上网用户推送精准营销广告。

无线控制器不管是部署在集中转发模式下还是本地转发模式下，都可以实现关键字营销推送。

3.1.1 精准营销之网页内嵌浮窗

匹配用户搜索的关键字，并按照设置的推广规则，在浏览器的最下方进行广告展示，即当用户搜索关键字时，深信服无线会匹配用户搜索的关键字，并推送相应的 banner 广告(最佳分辨率为 400*60)，实现精准营销，如下图所示。

3.1.2 精准营销之微信

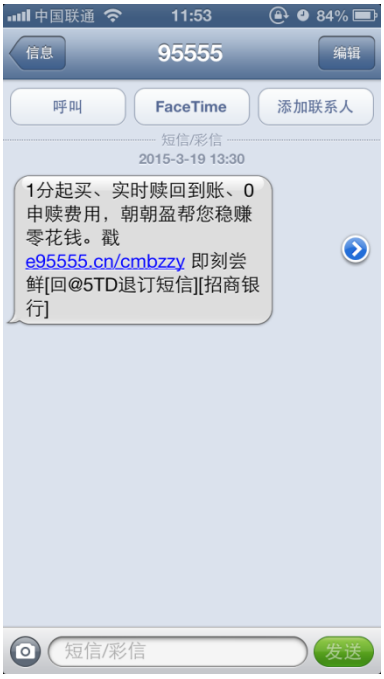
用户关注微信后，当用户在网页搜索引擎或 App 中搜索关键字时，可以通过微信的方式向用户推送广告，实现微信关键字营销。

例如：某用户使用微信认证的方式关注了银行的微信公众号并正在享受免费、高速的 Wi-Fi 网络，银行预先设置了“股票”的关键字组（包含股票、基金、股市等关键字），当用户搜索“股票“时，他立即收到了银行微信发来的理财信息。

3.1.3 精准营销之短信

用户使用手机短信认证方式接入网络后，当用户在网页搜索引擎或 App 中搜索关键字时，可以通过短信的方式向用户推送广告，实现短信关键字营销。

例如：某用户使用短信认证的方式接入了银行的免费 Wi-Fi 网络，银行预先设置了“小米”的关键字组，当用户搜索“小米“时，给他推送银行理财产品的相关信息。



3.1.4 用户搜索行为分析

搜索作为互联网重要服务之一，每天有上亿的网民使用，并由此产生大量的搜索记录。那么，企业如何查看并了解到用户的搜索行为习惯呢？

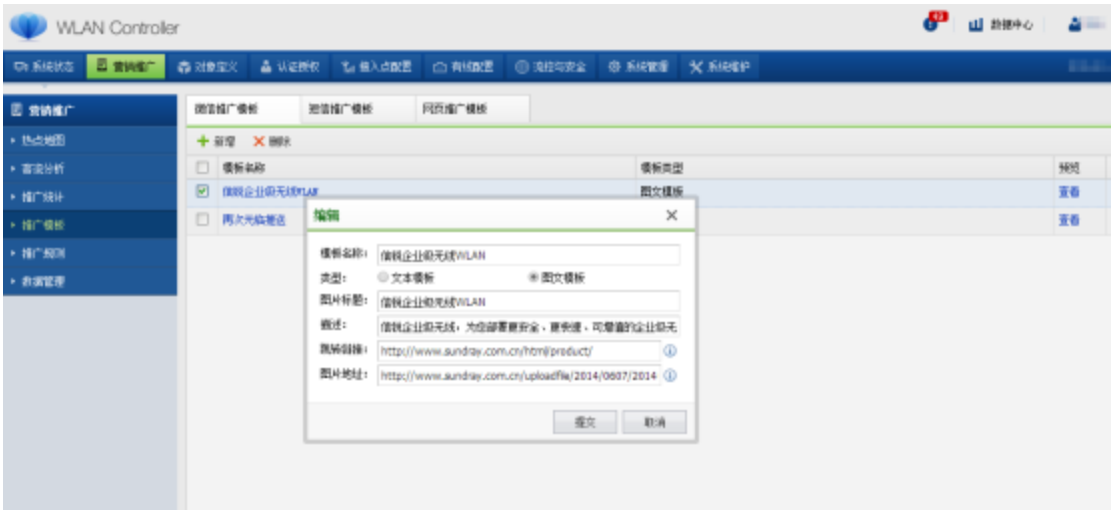
深信服科技提供了专业的基于用户搜索日志的用户行为分析，可以查看到哪些关键字/词被广大用户搜索。搜索分析可以统计到上网用户在百度、谷歌、淘宝、搜索大全所搜的关键字，分析时下流行元素，商家可以根据最热门的关键字信息进行商品广告的推送。

3.2 微信营销

通过微信认证的上网方式，实现微信营销，可以根据顾客首次接入、在线时长、终端出现、接入 AP 位置、出现次数等条件进行营销广告推送。

3.2.1 微信推广模板

微信推广模板支持图文模板和文本模板两种形式，图文模板可以自定义图片标题，描述，图片跳转链接。



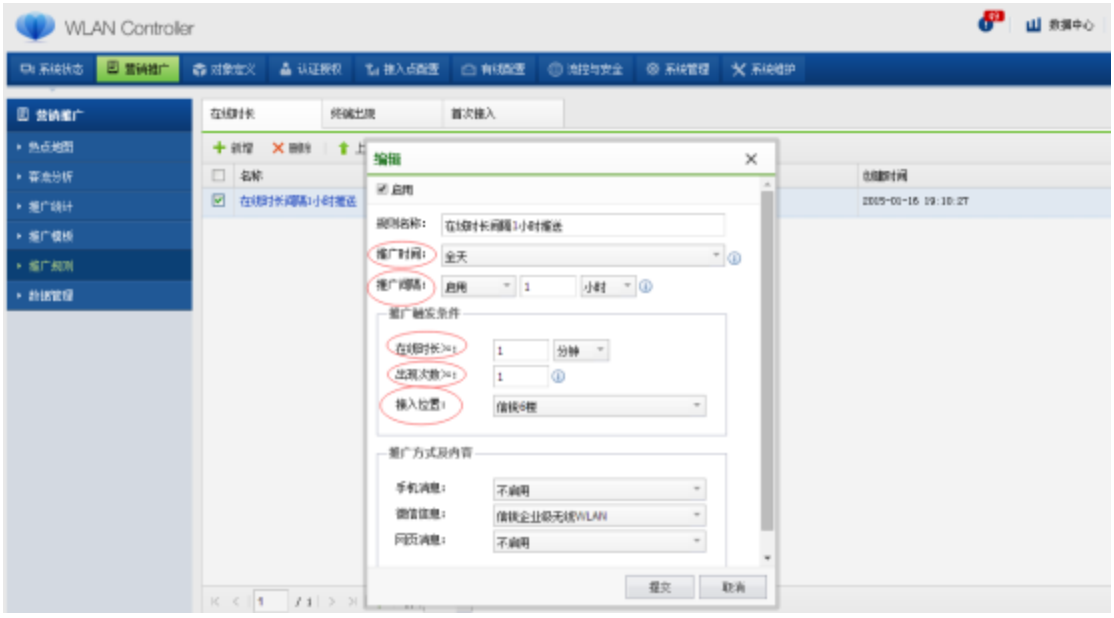
图文模板预览：

3.2.2 推广规则

1、 在线时长推送

微信推广的在线时长推送可以匹配推广时间、推广间隔、在线时长、出现次数、接入位置多个条件进行推送，灵活实现各种广告推送。

比如根据顾客接入位置，实现位置变更的广告推送；根据推广时间，实现定时或者不同时间段推送不同的广告信息。



2、 终端出现推送

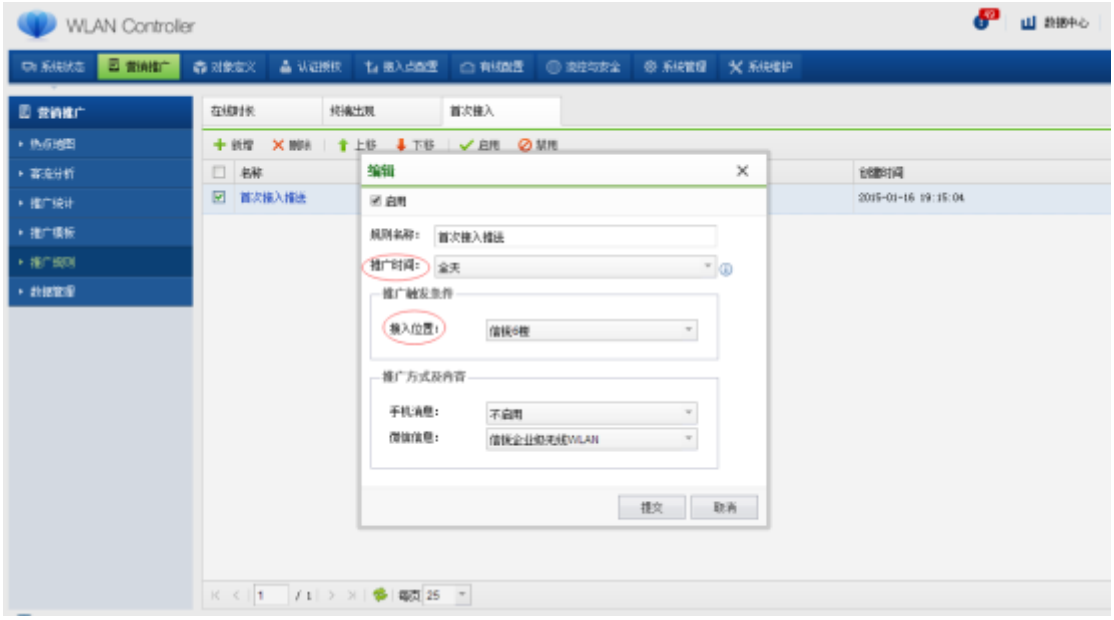
微信终端出现推送，可以简单理解为二次到店问候，即当顾客第二或多次出现的时候，顾客会收到商场的问候广告(只要顾客的移动终端打开了 Wi-Fi 功能 ,即使它没有连上 Wi-Fi ,

也会收到），可以给离开时长达到一定时间的顾客进行二次到店问候；也可以根据顾客的出现次数，当顾客出现次数达到一定时，才进行终端出现推送，或者推送三次、多次到店问候信息。

3、 首次接入推送

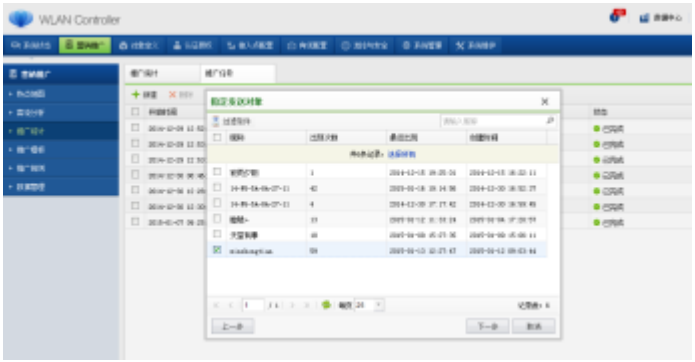
深信服首次接入推送可以实现顾客首次到店的温馨问候，不同于微信公众号本身的关注即发现新消息（只能文本消息），深信服的首次接入推送可以推送图文消息。

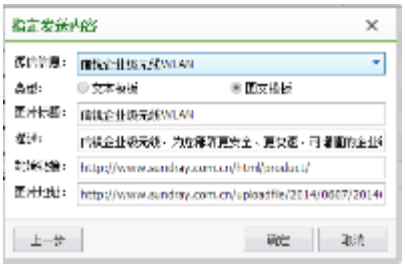
首次接入推送可以根据顾客的接入时间和接入位置进行广告推送。



4、 离店主动推送

除了以上丰富的在线微信广告推送外 ,我们还支持离店主动推送 ,即微信主动营销功能。微信离店主动推送是根据 WAC 获取到的顾客微信号的 openID 等信息进行的，在设备的推广任务里进行广告投放，可以给出现过一定次数、离开一定时长的顾客进行广告投放，即使顾客不再 Wi-Fi 覆盖范围内（在家、在逛街）

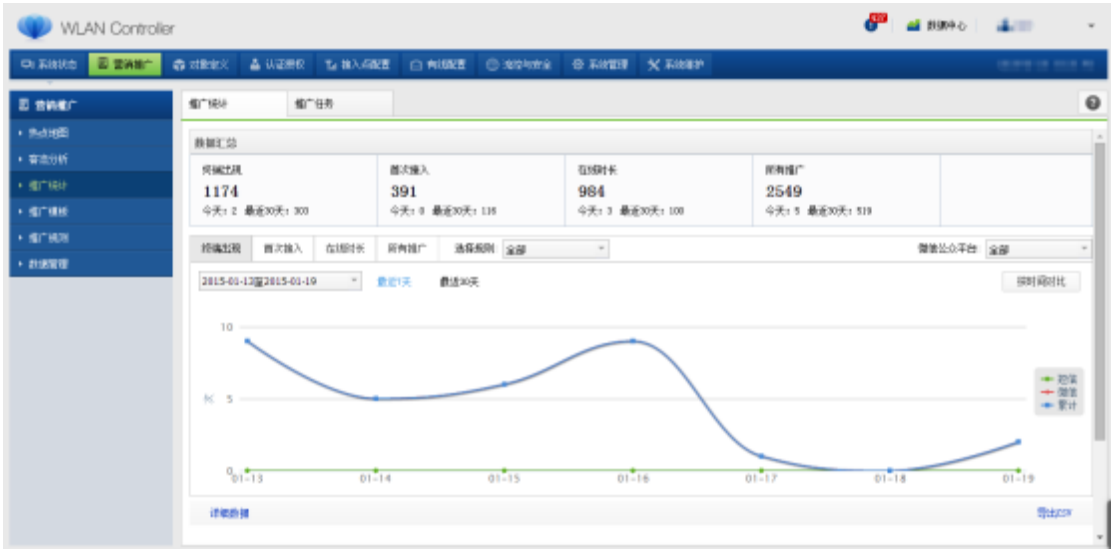




3.2.3 推广统计

微信推送可根据不同 AP、不同 SSID、首次接入、二次接入、接入位置、在线时长等方面进行广告推送，系统会统计广告推送的次数并提供趋势图,直观显示推送效果。

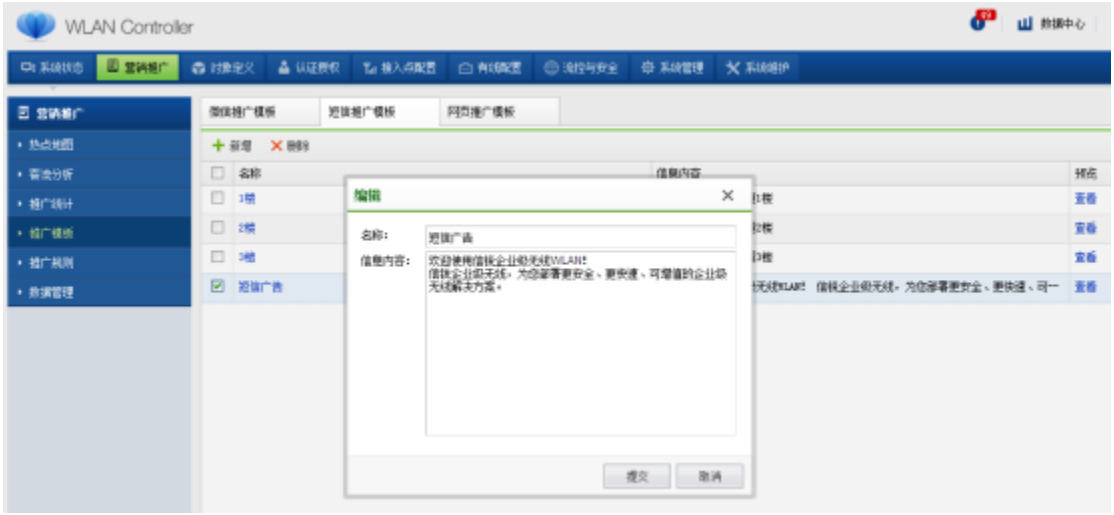
可根据最近 24 小时、最近 30 天和总计推送次数查看状态；可查看推送次数趋势图；能够根据终端在线时长、终端出现、终端首次接入三种类型的推送规则分类查看每种类型下每条规则最近 24 小时，最近 30 天和总计的数据，能查看新增微信号码日期明细，能显示最近 24 小时和最近 30 天的报表，且能查看趋势图；能显示已完成群发任务的次数，能够查看历史群发任务近 10 条的详情。



3.2.4 效果展示

3.3 短信营销

短信营销同微信营销，只是推广模板与形式不一样，推广规则是一模一样的。



3.4 网页广告营销

网页广告分网页内嵌和全屏网页两种形式。

网页内嵌广告

网页内嵌广告，即当用户在浏览网页或使用 APP（需要含有 http 流量）时收到内嵌 banner 广告的推送，如下图所示。

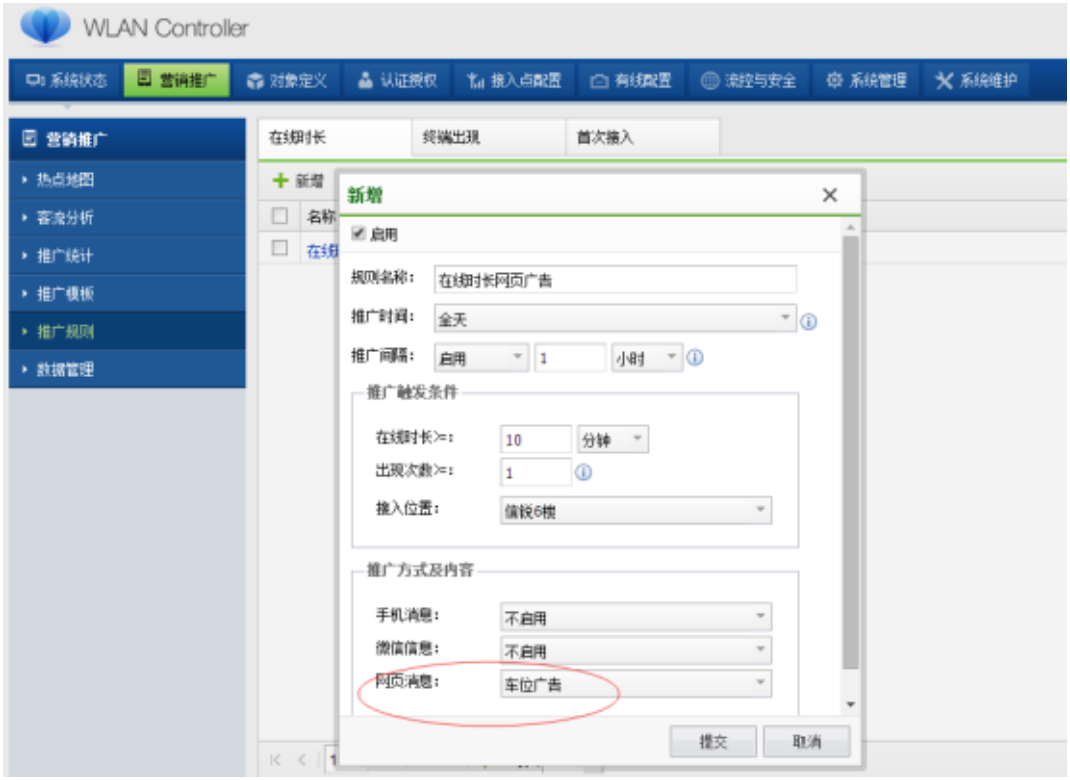
微信内广告浮窗

浏览器内广告浮窗

全屏网页广告

推广规则

只支持在线时长推送



3.5　广告投放

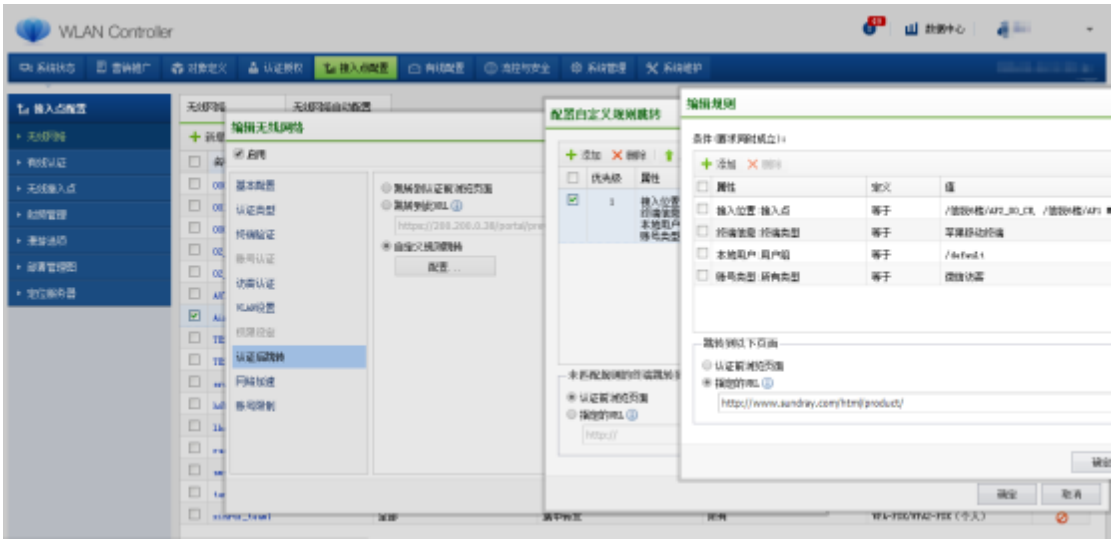
1、认证前广告投放

在用户接入 Wi-Fi 时首先观看到的认证页面，其上方支持 5 张广告轮播，用户在认证时可以观看广告，当用户点击图片时可以跳转到相应的 URL 网站。

认证前广告投放可以根据区域、位置、时间段进行投放，不同的区域、位置、时间段推送不同的广告 ,比如在商场的家电区域推送家电促销的广告 ,服装区域推送服装促销的广告。

2、认证后广告投放

当用户完成短信认证或其他认证后，系统就自动跳转到一个网页上，此跳转网页可以是用户认证前浏览的页面，也可以是特定的页面上，并且可以根据接入位置、终端类型等条件设置不同的跳转页面，让营销更精准。



3、在线时广告投放

在线时长广告可以通过微信、短信、网页三种形式向顾客进行投放。

根据客户接入位置推送广告：

可以根据用户所在的接入位置，推送不同的广告。例如在商场里，一楼推送金银饰品广告，二楼推送服饰广告；三楼推送电子产品广告。

根据访客来访周期推送广告：

对于频繁光临的老客户，推送更加优惠的广告；对于不常来的访客，推送近期活动广告；对于新到店的客户，推送新产品广告。

4、离店后广告投放

离店后广告可以通过微信、短信两种形式向顾客进行投放（详细见“3.1-推广规则-离店主动推送”）

1、 若顾客使用的是微信认证，需获取到顾客的 openID，才可以进行主动投放（关于获取哪些方式可以获取到顾客微信的 openID 请查看本文的“微信认证”）；

2、 若顾客使用的是短信认证，则可以通过短信的形式进行广告投放

5、再次来店广告投放

再次来店广告可以通过微信、短信两种形式向顾客进行投放。

再次来店微信广告投放

当顾客第二或多次出现的时候，顾客会收到商场的问候广告（只要顾客的移动终端打开了 Wi-Fi 功能，即使它没有连上 Wi-Fi，也会收到），可以给离开时长达到一定时间的顾客进行二次到店问候。

再次来店短信广告投放

短信广告投放和微信类似，短信广告投放不需要顾客的移动终端打开 Wi-Fi 功能，当顾客再次来店时，即会收到商场推送的短信消息。

3.6 客流分析

3.6.1 客流分析

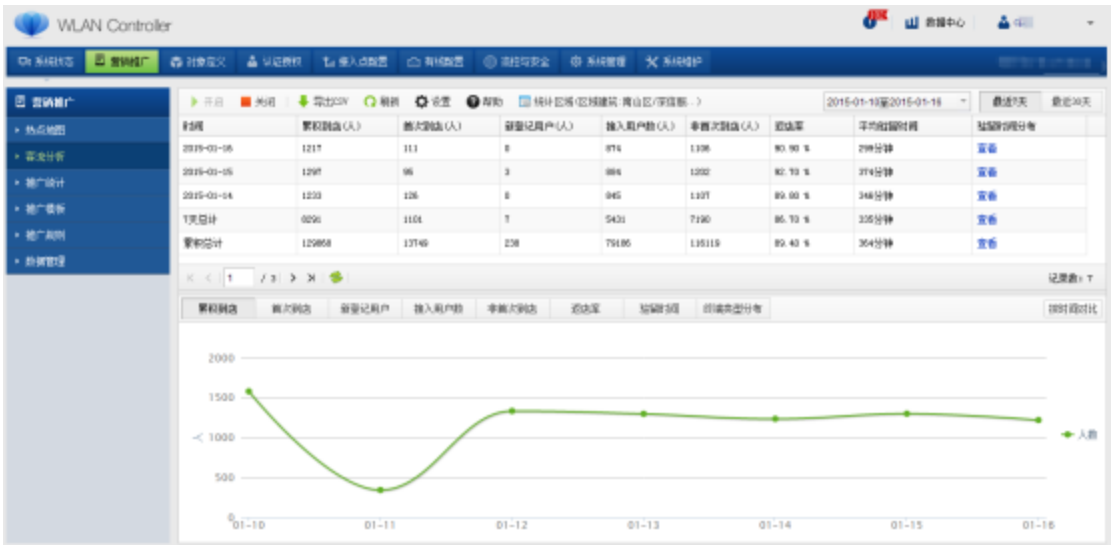
WAC 支持以单个 AP 组、楼层、建筑物、所有级别的报表数据统计查看。

客流量分析与统计列：到店客户、新到店客户、新注册用户、非首次到店、接入用户数、返店率、平均驻留时间、驻留时间分布。

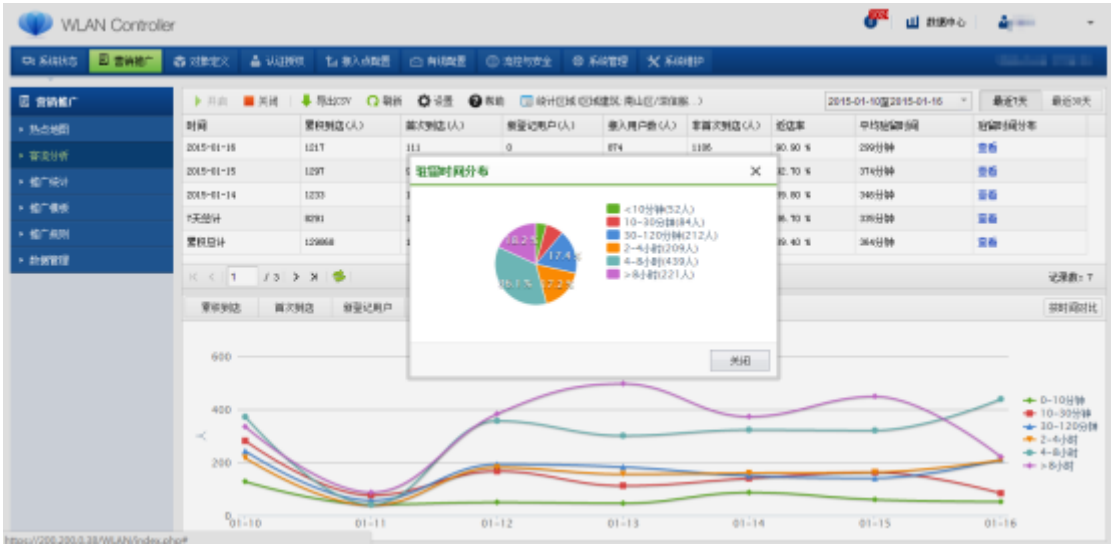
同时客流量分析支持原始数据导出支持定时上传到 ftp 服务器，每天导出一份。客流量分析的图例包括最近 30 天、最近 90 天的趋势，以及终端类型的分布饼图；驻留时间分布图包括小于 10 分钟、10-30 分钟、30-120 分钟，2-4 个小时，4-8 小时,8 小时以上。

为了更准确地区域新老客户，要求至少采集时间超过 24 小时，才开始统计新老用户的数据。

1、 客流分析



2、 驻留时间分布统计



3、 终端类型统计

3.6.2 客流分析数据导出

客流分析数据支持手动导出和自动导出到 ftp 服务器。

3.6.3 原始数据开放

深信服可对用户开放客流分析的原始数据 ,提供无线接入点所有扫描到的终端的相关信

息，为用户进行第三方应用或其他作用。

3.7　热点地图

3.6.1 热点地图

深信服无线控制器的热点地图上，可以直接将接入点、控制器标注在地图上。当发生异常情况时，故障点对应的图标颜色会变。管理员能在第一时间发现，并作出应对措施，例如调整无线网络分布关联 AP 情况，或增大周边 AP 功率等。

3.6.2 人流密度

对于大型商场、连锁店、商业城来说，了解店面周边或楼层的顾客分布情况，对于投放广告、发放宣传页、统计商业活动效果、分析客户行为趋势有积极的意义。

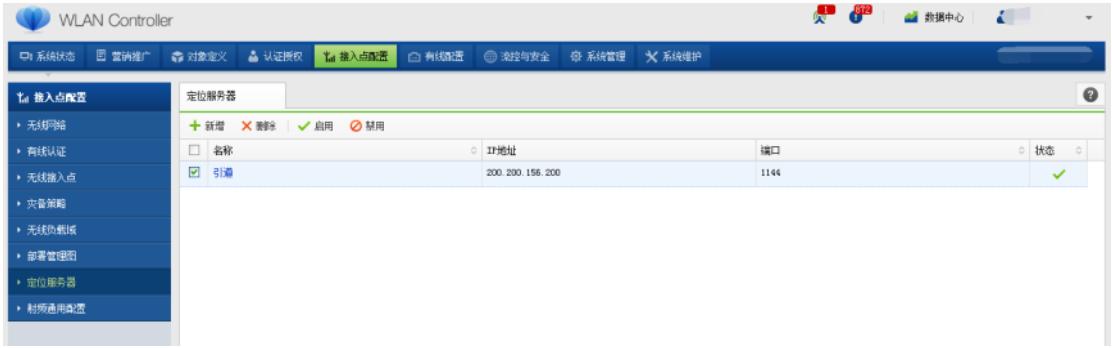
用户只需上传地图，并根据实际地理位置新建建筑、添加楼层，并设定好比例尺，深信服无线控制器即会自动统计人流密度情况。几个小时后，用户就能看到商铺周边的人流密度分布。人员越多的区域，颜色越红；反之，颜色越蓝。

客流密度分析必须配置比例尺，必须导入蓝图。客流密度分析功能可对区域、楼层节点进行客流密度分析，允许对最近 24 小时、最近一周、最近一月、最近一季、自定义时间段做客流密度分析并生成热图，同时支持导出客流密度分析图。

3.8　无线定位

为支持客户的大数据分析系统，深信服无线控制器开放无线定位接口，可通过第三方服务定位系统进行无线定位，比如广东引道地图、北京智慧图、上海猫酷等专业定位服务商。

结合定位系统，可以实现室内定位、室内导航、进店率分析、智能停车等。



3.9　开放访客信息

深信服无线控制器可以直接将自身收集的访客信息上传到客户的服务器，用以支持客户的大数据分析，商业效益分析等行为。


WLAN Controller
系统状态
营销推广
对象定义
认证授权
接入点配置
有线配置
流控与安全
系统管理
系统维护
系统维护
序列号
系统更新
日志查看
备份恢复
故障排除
调试选项
重启及注销
命令行控制台
导出系统记录
接入点授权更新
备份配置
访客数据库管理
备份服务器
启用
服务器目录：
ftp://200.200.0.33
登录类型：
匿名
用户名：
密码：
服务器编码：
GBK
测试有效性
保存
恢复本页默认参数

四、 网络加速与优化

随着网络技术的快速发展，基于网络的应用越来越多、越来越复杂。种类繁多的应用正在吞噬着越来越多的网络资源。网络作为一种新的传媒载体，也正在遭受媒体的冲击。尤其是网络视频、个人媒体、传统电视等媒体向互联网的渗入使得网络中的流量急剧上升，这使得企业的网络运营和管理成本大幅度增长。

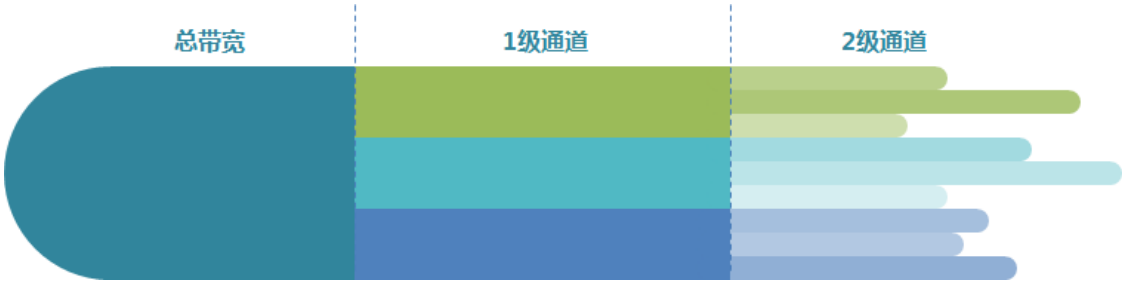
深信服科技拥有丰富的网络加速和优化技术 ,使得无线用户和有线用户都能享受流畅的办公环境，最大化利用带宽资源。

4.1 流量控制

传统的流量控制，仅仅只能对用户进行简单、统一的上下行限速，并不能很好的解决企业带宽足够却上网依据很慢的问题。深信服 WAC 的流量控制通道技术的出现便有效的解决这个问题。

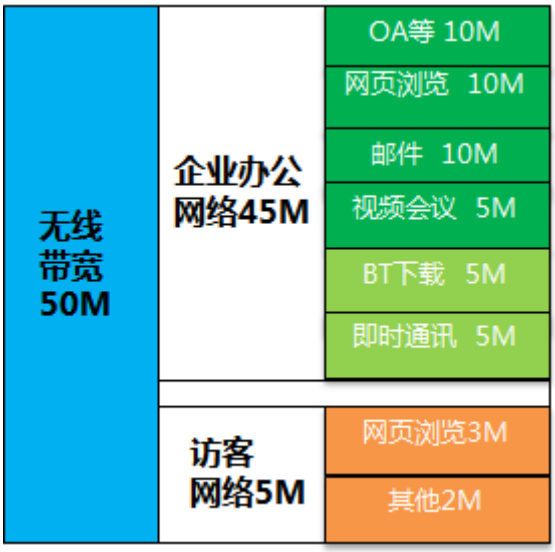
流量通道技术

WAC 支持根据不同的应用、用户、用户组、区域位置来划分限制或者保证流量通道，可以根据百分比或数值设置通道带宽大小，并支持设置各通道的优先级，并且支持 3 级父子通道，匹配组织架构，实现带宽精细划分。



1、基于应用

WAC 软件平台可以根据用户实际跑的业务，分配带宽比例。用以保障重要的业务能享受到相对高质量的网络，不重要的业务少占用网络。深信服可以根据应用进行流量管理，结合强大的应用识别库，保证某些重要应用，比如邮件、OA 等应用，优先保障其网络带宽。同时，可以避免大流量的网络应用干扰重要业务应用，比如下载。



2、基于区域位置

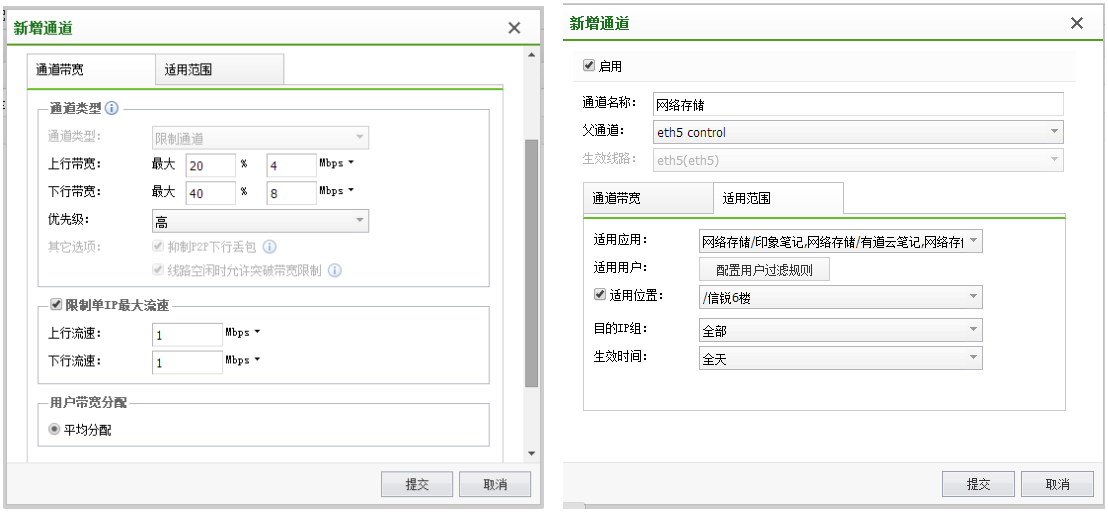
在一个企业或者商场内，为了最大化合理利用带宽资源，不同的区域由于业务需求、用户数量不一样，所需要的带宽也不一样，利用基于区域位置（AP/AP 组）的流量划分，可以灵活的按照实际需求进行带宽分配。

3、基于时间段

同理，不同的时间段由于业务需求、用户数量不一样，所需要的带宽也不一样，利用基于时间段的流量划分，不同的时间段分配不同的流量限速策略，灵活的按照实际情况进行带宽分配。

4、用户带宽平均分配

支持流量通道内智能平均分配用户带宽，根据在线用户数量平均分配带宽资源。比如：该流量通道总流量为 8M ,此时适用用户当中有 2 个人在线 ,则每一个用户享受 4M 的带宽，当 4 个人在线时，则每一个用户享受 2M 的带宽。



4.2　无线空口的资源管控

无线空口资源合理分配

WAC 支持基于应用、SSID 的空口资源分配，并支持 802.11e/WMM 优先级设置，全面保障无线空口资源的合理利用。

1、基于应用的无线空口的资源管道化精细管理，保证无线带宽资源合理分配，保障重要应用的优先传输；

2、支持用户间平均分配带宽，终端公平调度（时间公平算法），避免低速终端长时间暂用无线空口资源而造成的整体网络性能低下的问题；

3、支持基于 SSID 的智能带宽动态分配，保障重要 SSID 的流量的优先级；

4、IEEE 802.11e 为基于 802.11 协议的 WLAN 体系添加了 QoS 特性，WAC 支持基于 IEEE802.11e 标准的语音视频应用优先处理能力。

丰富的拥塞管理技术

拥塞管理的中心内容就是当拥塞发生时如何制定一个资源的调度策略，决定报文转发的处理次序。WAC 软件平台的 QoS 提供丰富的调度策略，会根据不断数据流的类型而选择不同的优先级发送，从而避免了关键数据流的阻塞和重传。

4.3 智能射频

在 2.4GHz 频段中，最多只能容下三个互不重叠的信道，一般选择 1，6，11。相同信道会造成同频干扰，重叠的不同信道之间会造成邻频干扰。随着 WLAN 的热潮，越来越多的场所搭建无线网络，空气中充斥着无线信号，容易产生信道干扰，深信服无线的智能射频可以很好的解决信号干扰问题。

智能射频功率调整

当部署的 AP 功率太大会干扰到周围的其他无线设备，同时浪费电能和增加辐射；当 AP 功率太小则会造成距离较远的终端接收困难、信号差，造成丢包，当丢包到达一定阈值，

也即确定了 AP 的覆盖范围。即太小的功率减小了 AP 的覆盖范围；

开启智能射频后，WAC 对周围无线射频环境进行实时监控，如果环境出现变化，系统就会对 AP 的发射功率进行适当的调整。

同时，支持自动调整和立即调整功能：

自动调整：设置自动调整时间段，在此段时间，收集 AP 上报的调整信息，每隔一段时间（默认 10 分钟）进行调整。

立即调整：触发各 AP 立即上报调整信息，从而马上做出调整，从而改善射频环境。一般用于调整时段外，有立即调整需求的场景：如 AP 上下线。

智能信道优化

智能信道优化即智能信道调整， WAC 支持动态智能的信道优化功能，能定时或自动调整 AP 的工作信道，让相邻的 AP 信道错开，避免信道冲突。

4.4 智能负载均衡

优先接 5.8G 频段

优先接 5.8 频段 ,使支持 2.4G/5G 双频的移动终端优先接入 5GHz 频段 ,平衡 2.4G/5G 网络利用率，提高终端用户的上网体验，实现价值最大化。

接入点间负载均衡

负载均衡，即终端请求接入某个 AP 时，WAC 根据该 AP 与邻居 AP 的负载情况，决定是否允许新的客户端接入，终端可自动连接其他空闲 AP，达到负载分担的效果。

根据 AP 当前的负载情况及其他条件（如：接入人数、信号强度等）控制终端的接入，达到 AP 间负载均衡，提高网络吞吐量和服务质量。

另外，根据不同场景设置不同的负载均衡参数，以实现漫游、无线体验的最佳效果。

动态负载引导（防终端粘滞）

终端在不同区域间移动时，为了让终端接收到信号最佳的无线接入点，获得良好的上网体验，深信服无线防终端粘滞功能，可以根据实际情况，设置切换阈值，漫游效果更好。

当接入点识别出终端的信号强度小于设定的信号强度阈值 ,并且该终端的无线流量小于流量阈值时，接入点将主动让终端漫游。

4.5 快速漫游

二层漫游

AP 与 AC 直连组网，AP 和 AC 连接在同一个 VLAN 内，终端在不同的 AP 间切换时，始终在一个 VLAN 子网内，且业务 VLAN 是跟用户 VLAN 授权信息一致的，保证业务不中断。

深信服 WAC 拥有优秀的二层漫游效果，能实现在整个无线网络的无感知快速漫游。

三层漫游

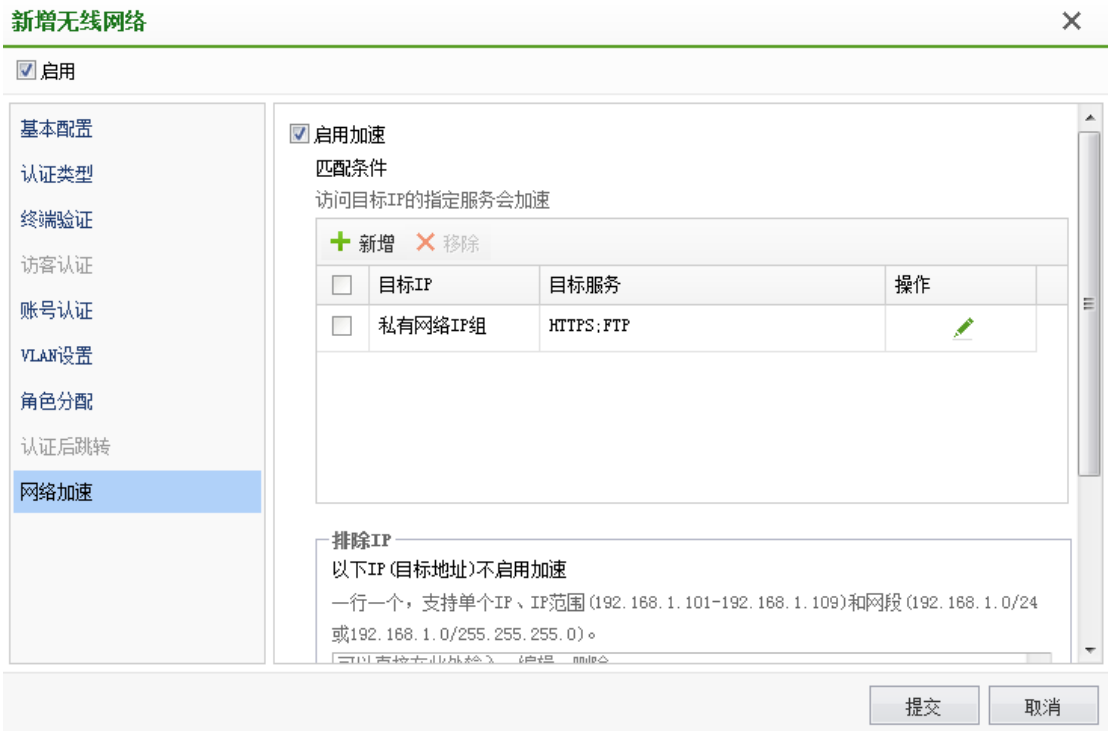
当网络规模达到一定时，为了网络安全性、易管理维护性，需要将整个无线网络划分为多个 VLAN，因此部分 AP 在不同的 VLAN 内，IP 网段也不相同。此时，如果用户在无线网络的覆盖区域内从某一个 VLAN 漫游到另外一个 VLAN 时，需要重新获取 IP 地址，这样就会导致业务中断，严重影响用户体验。

在此背景下，三层漫游（跨 VLAN 漫游）应运而生，它使用户在不同 VLAN 间漫游时，依旧保持用户的 VLAN 为初始 VLAN，从而保证用户在不同 VLAN 间漫游而业务不中断。

4.6 应用层加速

深信服 WAC 独有的应用层加速专利技术（也称为单边加速），是通过改善传统 TCP 协议传输机制，达到传输效率提升数倍的效果。使用该功能时，客户端无需安装任何插件，对用户侧完全透明，不存在兼容性问题。

应由层加速，解决了无线网络由于干扰导致的无线传输速率低、丢包等网络质量问题。在存在无线干扰的网络环境下，相比于其他厂家，无线网络速度提升 1.5-4 倍。



4.7 无线优化

4.6.1 ARP 转单播优化

通常，ARP 广播报文会发往同一个二层相连的所有主机或终端，在无线网络环境中，这种“垃圾”报文会占用有限的无线空口资源，当广播包过多时，由于其传输速率较慢，长时间占用无线空口，导致其他终端无法正常发送数据，从而影响整个网络性能。

通过 ARP 广播转单播功能，当无线接入点收到 ARP 广播包后，会解析出该广播包中的目标 IP，再查找 IP-MAC 对应关系，如果查找到 MAC 是某个无线终端，将直接把广播报文中的广播地址 FF-FF-FF-FF-FF-FF 替换成查找的 MAC 地址，从而将广播转换成单播，直接发往该终端。这样可以减少广播，提升无线传输质量。

4.6.2 禁止 DHCP 请求发往无线终端

DHCP 请求的报文为广播报文，因此接入点在接收到 DHCP 请求的广播报文时，将会把此报文转发到有线网络，以及所有的无线客户端。

在典型的部署环境中，DHCP 服务器只部署在有线网络中。通过禁止 DHCP 请求发往无线终端的机制，DHCP 请求的广播报文将只转发到有线网络中，而不会转发到其它无线网络，这减少了无线网络的流量，提高了无线网络的性能。

4.6.3 智能广播加速

广播默认是以 1Mbps 的速率来发送的，开启提高广播速度后，在无线网络中，广播报文由于没有确认机制，因此为了提高广播报文传输的可靠性，协议上默认使用 1Mbps 的最低链路层速率来发送。

但此方式带来了一个显著的缺陷，由于无线网络为广播介质，在广播报文较多的情况下会严重降低无线网络的总体吞吐率。

启用此选项后，系统将持续评估当前的无线网络环境，自动选择一个更优，且不显著降低广播报文可靠性的速率来发送广播报文。这提高了无线网络的总体吞吐率，改善了性能。

4.6.4 高密场景优化

在一些会议室，访客展厅部署无线时，经常回遇到在一个有限的空间内，有分布密集的终端上网体验，那么用户一旦多的话，体验效果就会下降，然而在这有限的空间里部署多台 AP 的话，往往解决不了用户多的问题，反而会带来更多的干扰漫游问题。

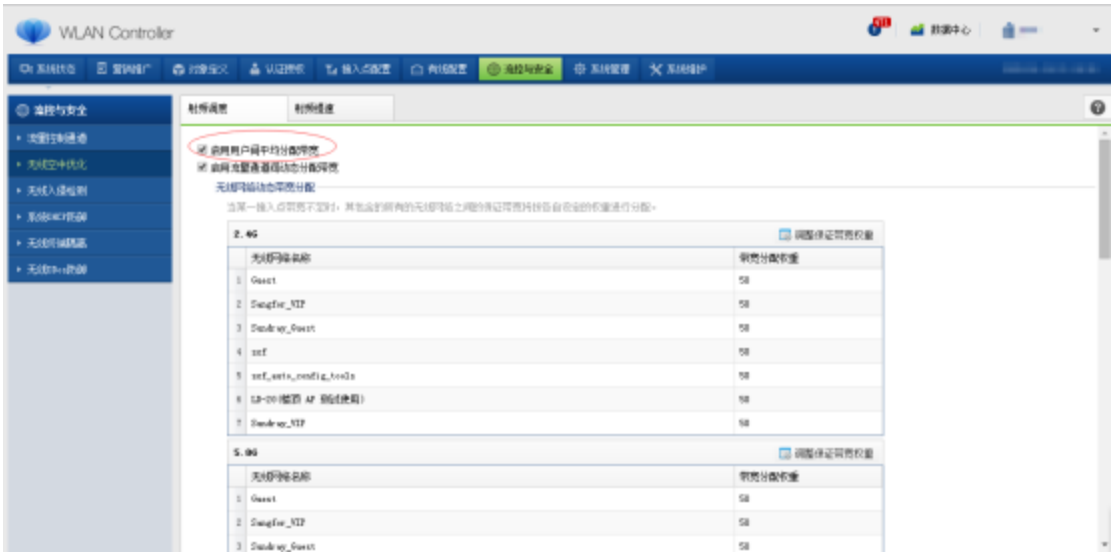
针对上述场景，对局部空间，终端分布密集场景进行网络优化，新增高密优化功能，在启用该选项后，AP 将不会响应终端广播的 probe request（探测请求），降低由于低速率发送 probe response（探测帧响应）消耗的性能空间，进行无线网络性能优化，从而提升高密度场景用户的无线上网体验。

4.6.5 防终端拖滞

由于所有终端抢到的空口机会差不多相等，高速率终端每次快速发完自己的数据后都要等待低速终端慢腾腾的发完它的数据，所以，高速率终端的性能基本上与低速率终端的性能是一样的，显然，整体的性能也被大幅拉了下来。所以，用户终端的连接速率过低时，会严重影响连接速率高的用户的上网速度，导致所有的接入用户上网体验差。

通过防终端拖滞（时间公平算法，也叫用户间平均分配带宽），有效的解决了某些终端接入速率过低导致整个网络性能下降的问题，让每个终端占用相等的无线信道时间，有效提

高无线网络总吞吐率。



4.6.6 电子书包场景优化

普教电子书包越来越流行，电子书包成为移动数字教学的重要载体，那么普教教室无线覆盖又是重中之重，然而，在无线电子书包的覆盖建设中，客户面临当接入的电子书包终端稍微多点时（现在一个教室学生至少 30 个以上），就会出现延迟大甚至卡顿的现象，学生上课利用电子书包学习的体验效果并不理想。

多播优化很好的解决电子书包场景由于接入终端并发数量多的问题，进行多播报文发送速率优化，多播通道带宽权重的设置，从而大幅度提高电子书包场景用户的上网速度，提升电子书包终端的体验效果。

4.6.7 禁止低速终端接入

在无线网络中，虽然连接速率低、信号弱的无线终端也可以接入到网络中，但是所能够获取的网络性能和服务质量要比信号强度较强的无线客户端差很多。如果弱信号的无线客户端在接入到无线网络的同时还在传输数据，就会占用较多的信道资源，最终必然对其他的终端造成的影响，并影响整个 AP 的性能。

禁止低速率终端接入功能，直接拒绝连接速率为 1/2/5.5Mbps 的无线终端接入到无线网络中，减少对其他终端的影响，从而提升整个无线网络的使用效果。

正常的室内无线覆盖，终端接收的信号强度可以保证，连接速率基本上不会低于 11Mbps，所以对正确部署的室内覆盖并不会有影响；若室内由于某角落信号差造成终端连接速率过低，也应该禁止其接入，这样可以保证整个无线网络的效果。

另外，室内部署的无线往往存在信号外泄的问题，在室外较远距离仍能搜索到无线，外面的人仍能采用微信认证、短信认证等方式的无线网络使用网络资源，禁止低速率终端接入后，在一定程度上可以防止外人蹭网。

五、 管理维护

5.1 有线无线一体化

深信服 WAC 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。

有线侧接入认证

有线用户支持 WEB 认证、临时访客认证、免用户认证的接入认证方式；支持基于 IP 地址的认证；其中 WEB 认证可以利用本地认证服务器实现本地认证，也可以关联外置第三方认证服务器（如 LDAP、RADIUS、AD），实现第三方认证。

有线侧精细化的角色授权

同本文“2.2 章节“无线侧的角色授权，支持基于用户、用户组、终端类型、时间段、外部服务器属性等的访问权限分配；

有线侧流量管理

同本文“4.1 章节“无线侧的流量管理，支持基于应用、用户、用户组、时间段等的流量管理；

有线侧上网行为审计

同本文“2.3 章节“无线侧的上网行为审计，支持基于应用、用户、用户组、时间段等的流量管理；

5.2 数据中心

对上网用户的网络行为和内容进行审计，审计的结果保存于数据中心。

我们支持内置数据中心和外置数据中心两种保留方式。其中内置的数据中心可以配置日志保留天数、磁盘预警百分比。

除了将审计的结果保存于数据中心之外，我们还提供多种类型的报表，这些报表可以更好的帮助客户分析网络状态，为客户提供更方便、快捷的的管理维护方法，以及更深层次的挖掘上网用户价值，助无线增值一臂之力。

日志查询功能

查看审计记录到的用户上网行为、上网流量、上网时长、访问指定网站的时长、ACL

拒绝日志，其中上网行为包括访问的网站、收发的邮件、论坛与微博、FTP 外发文件、HTTP 外发信息等内容；上网流量、上网时长可查看具体应用在指定时间内的访问流量、时长情况。

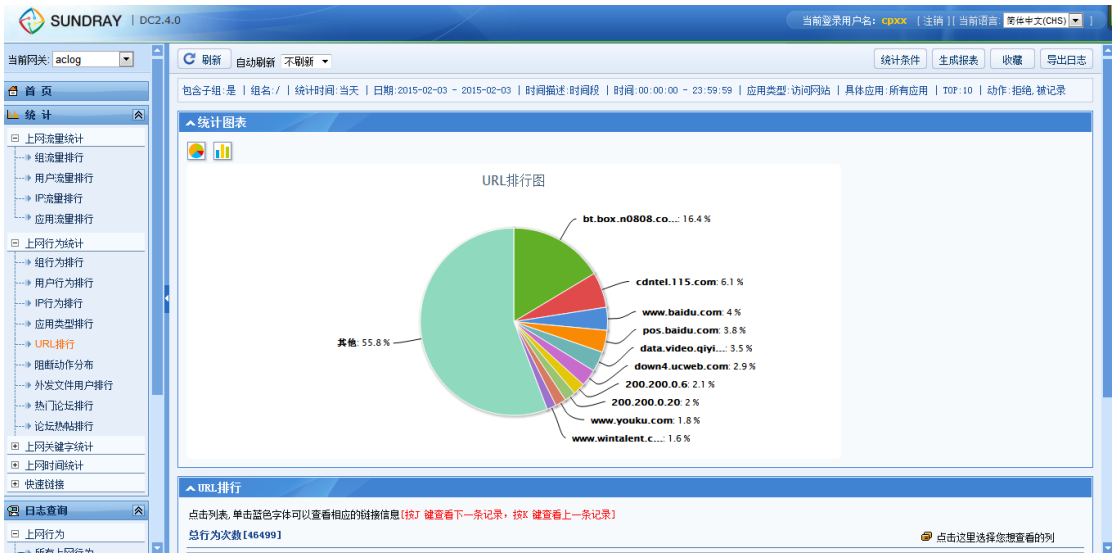
统计报表

1、 上网流量统计。按照组/用户/IP/应用的流量的上网流量统计及排行

2、 上网行为统计。组/用户/IP 行为/应用类型/URL 排行/阻断动作分布/外发文件用户/热门论坛排行/论坛热帖排行/手机验证活跃用户的上网行为统计及排行

3、 上网关键字统计。根据搜索关键字/搜索关键字用户/论坛微博关键字用户的关键字统计及排行

4、 上网时间统计。用户/IP/应用/具体站点用户的时间统计及排行



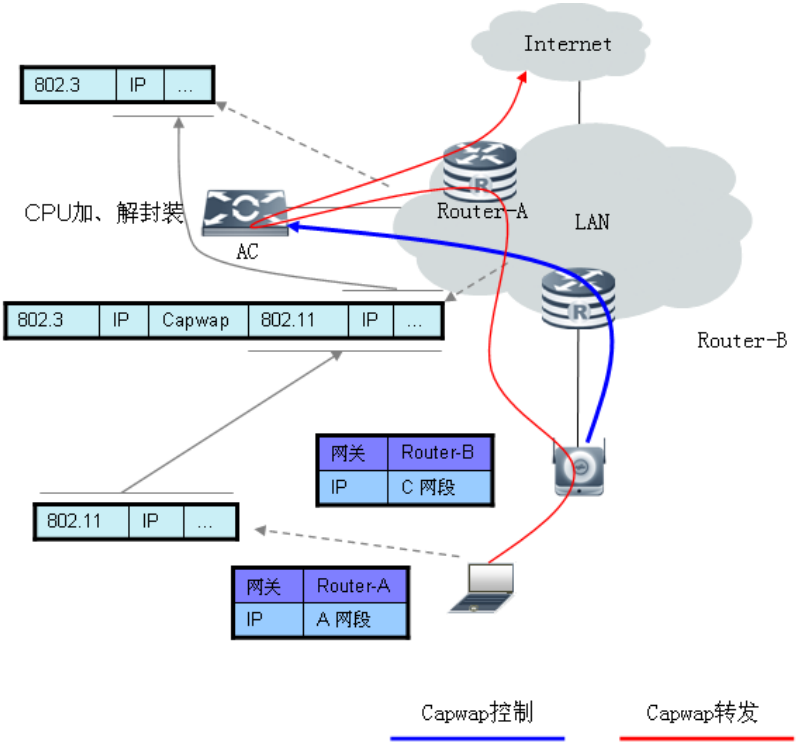
趋势报表

1、 流量趋势。根据组/用户/IP/应用/流量通道的流量统计趋势

2、 行为趋势（访问的应用被记录、被拒绝的次数）。根据组/用户/IP/应用行为的统计趋势报表

5.3 网络部署

5.3.1 集中转发



集中转发技术工作原理

集中转发模型处理方式如下：

1）用户的管理帧，如 802.11 管理、控制报文和 802.1x 协议报文等，直接通过认证模块传递给 WAC 集中处理，以实现用户的认证、授权等。

2）用户的数据帧，包括 802.11 数据和来自有线的 802.3 数据报文，在 AP 本地进行隧道封装处理，并由 AP 转发给 WAC，WAC 侧进行隧道解封装，然后按照用户 vlan 及其他授权信息发送至上层网络，实现数据的集中处理。

集中转发技术优势

深信服集中转发技术，无线终端的数据采用私有隧道协议封装，增加了用户业务的安全性。集中转发技术减少了接入（AP）侧配置的复杂度，便于 AP 大规模集中部署。同时由于用户数据流统一从 WAC 侧发送至交换网络，透明穿透 AP 与 WAC 间的网络结构，便于用户策略的集中管理以及流量统计。

集中转发的特点

集中转发组网，AP 和 AC 之间单独建立一条隧道传输数据业务，所有的数据业务都通过 AC 转发出去，所以 AC 的负荷比较大。

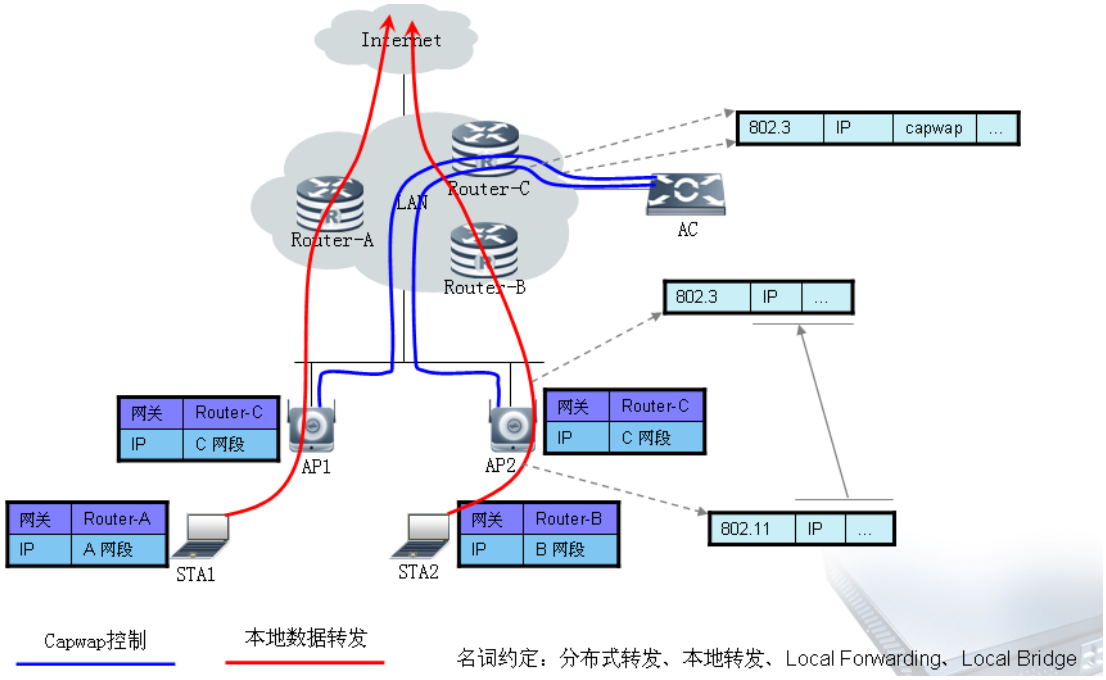
集中转发所有的数据包都要走隧道，所以对链路的带宽要求较高，并且对 AC 接口的带宽要求也较高。由于集中转发的数据包要封装到隧道里再转发走，所以对 AC 的 CPU 消耗比本地转发更大。

由于对带宽要求较高，所以集中转发的 AC 可管理的 AP 数量也会受到一定限制。这样对于规模较大的网络或者有备份要求的项目，会增加成本。

此外，当隧道转发出现不通或者丢包现象时，查找网络故障难度比本地转发高。

集中转发的优点是对于现网改动较小。

5.3.2 本地转发



WAC 采用集中转发部署时，要求用户的所有流量（包括上网流量）均通过 WAC 进行处理，对 WAC 性能要求比较高，同时也对 WAC 和 AP 之间的网络带宽造成压力。尤其是在 802.11ac 技术逐渐成熟，无线接入点的处理能力越来越强的背景下，单一的集中式转发往往不能满足无线数据高速处理的要求。

为了适应无线网络高带宽化的发展趋势，深信服 WAC+瘦 AP 架构在支持集中转发的同时也支持本地转发技术，以 WAC+瘦 AP 架构为基础，实现无线数据在 AP 本地的转发，突破了传统集中式转发的性能瓶颈。

本地转发的特点

利用瘦 AP 本地转发方式进行大规模组网，可以完全代替目前主要采用的集中转发方式，在本地转发方式下，网管、安全 、认证、漫游、QOS、负载均衡、流控、二层隔离等功能还是由 AC 统一控制，再由 AP 具体实施；只是业务数据不通过隧道传送到 AC，再经由 AC 解封后统一转发，而是由 AP 本地转发。

此组网方式的优势主要体现在，将业务数据转发任务分散到 AP，降低 AC 压力，轻松应对带宽挑战，彻底解决 AC 瓶颈问题，提高网络整体吞吐率，顺利迎接 11n 时代。

本地转发和集中转发对比

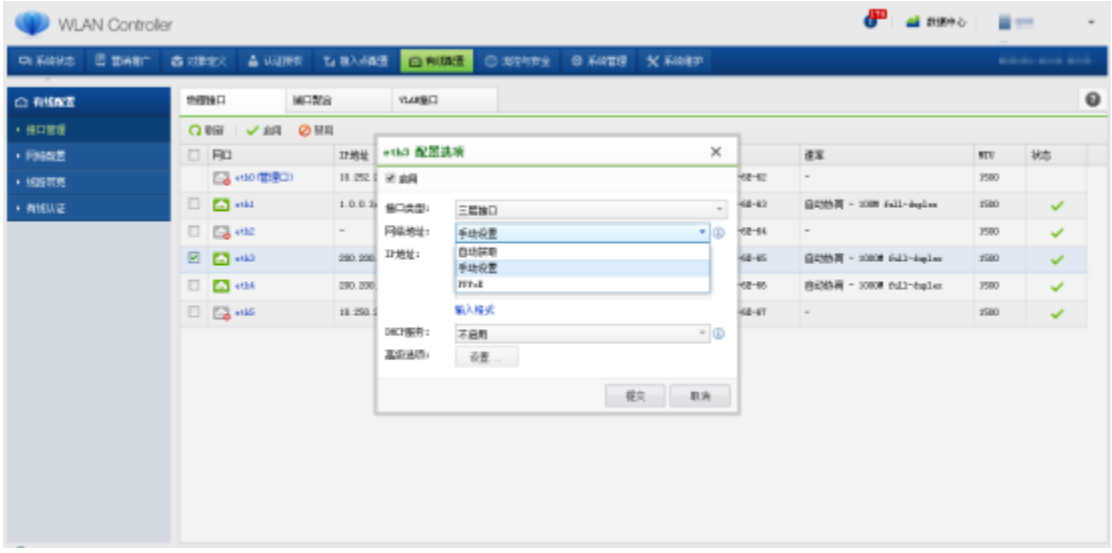
	本地转发	集中转发

AC 位置	一般旁挂核心交换机上	一般做二层数据转发
AC 性能压力	低	高
AP 性能压力	低	略高
业务隔离、热点区分	需要把无线用户和有线用户统一考虑从接入层开始的转发路径规划，一般跟 AC 对 AP 的管理路径是分离的。	无线用户从 AP 到 AC 的转发路径跟 AC 对 AP 的管理路径一致
无线加解密	AP 完成，充分利用 AP 的加解密引擎提高网络整体吞吐率。	AP 或 AC 完成，可以支持功能较弱的 AP，另一方面对 AC 的加解密能力要求提高，性能压力较大

5.3.3 网关模式

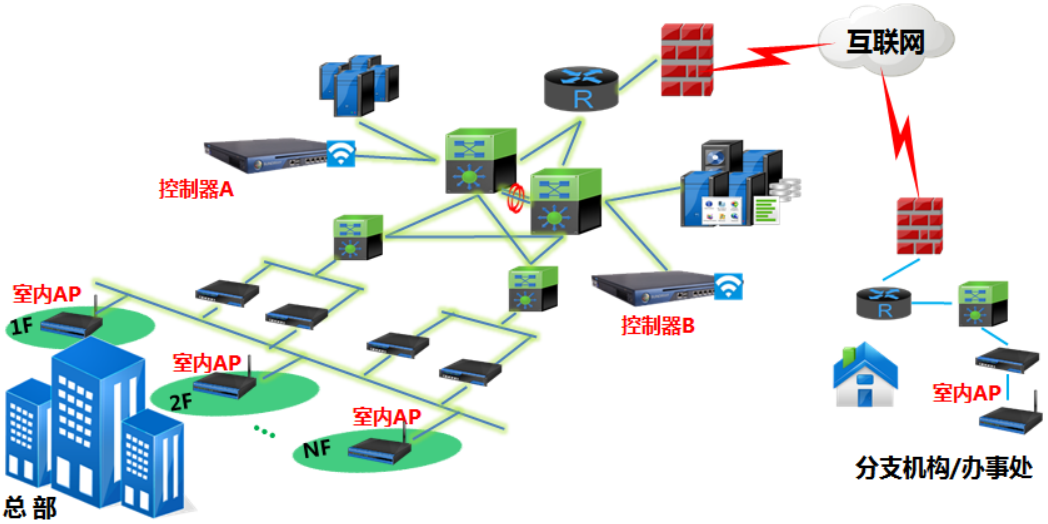
在网络规模较小的环境下，控制器 WAC 工作在集中转发模式下，可以充当网络出口的功能，WAC 具备 NAT 功能，支持 PPPoE 拨号、静态 IP、DHCP 自动获取三种主流上网接入方式，中国电信/移动/联通的光纤或普通网线接入的网络，并支持多出口线路以及带宽叠加。

例如：一个企业部署了一台 WAC-6200，拉了 4 条 ADSL 拨号宽带，配合策略路由，根据源 IP 和目的 IP 来控制流量往哪个出口出去。比如，利用源 IP 进行控制，让部门 A 走线路 1，部门 B 走线路 2；利用目的 IP 进行控制，用户访问联通服务器时走联通的线路，访问电信服务器时走电信的线路。

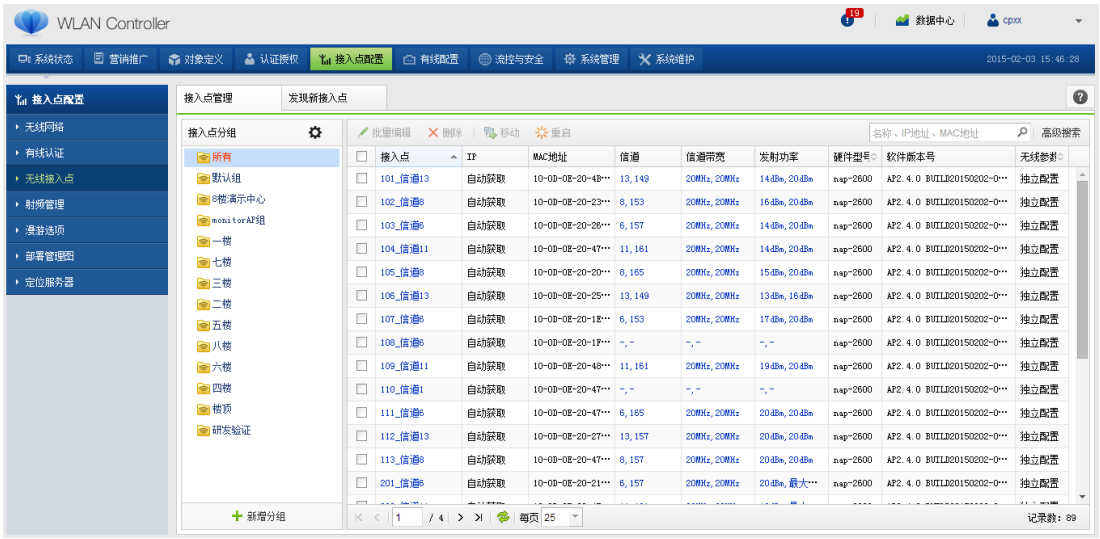


5.4 管理与运维

5.4.1 集中管理



无需部署桌面网管软件，即可实现对整个网络的 AP 设备进行集中管理。WAC 提供友好的中文 Web 管理界面，对所有 AP 进行统一集中管控，由 AC 下发配置到所有 AP，统一固件升级、信道功率自动调节等，实现真正的 AP 端零配置。



5.4.2 智能工勘

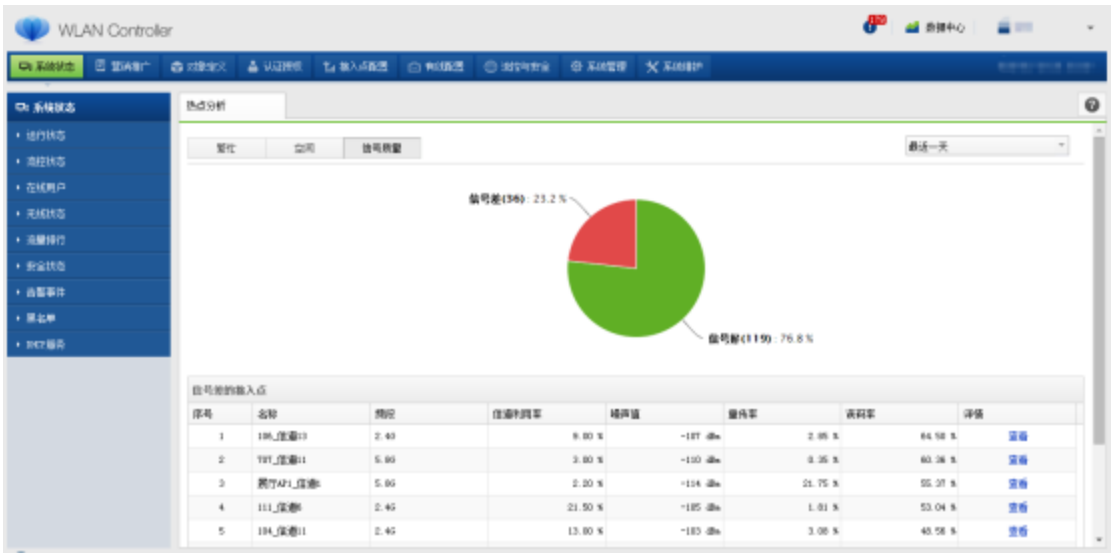
内置工勘软件，用户可以根据实际建筑结构，导入建筑图，标注建筑结构的参数，然后可以自动生成 AP 布点图，方便工勘管理。

5.4.3 图形化界面

图形化热点分析

热点分析就是对这些无线热点进行统计分析得到报告。WAC 可对管理的 AP 直观的查看实时状态：繁忙、空闲、信号质量等。

1. 列出当前最繁忙的无线热点，显示其实时状态。
2. 列出当前最空闲的无线热点，显示其实时状态。
3. 信号质量的好坏直接影响用户体验，通过热点分析可以找出信号质量差的无线接入点。如某个无线接入点信号质量差，从列表中可以得知哪个原因引起的。如果误码率过高，导致有效吞吐量上不去，可以检查该 AP 的功率设置是否过大或过小；如果信道利用率过高，可以尝试开启信道自动调整功能解决，或者手动设置到其他信道；如果噪声值过高，可以检查该 AP 周围是否有其他无线设备影响导致，如蓝牙发射器，微波炉，无绳电话等。

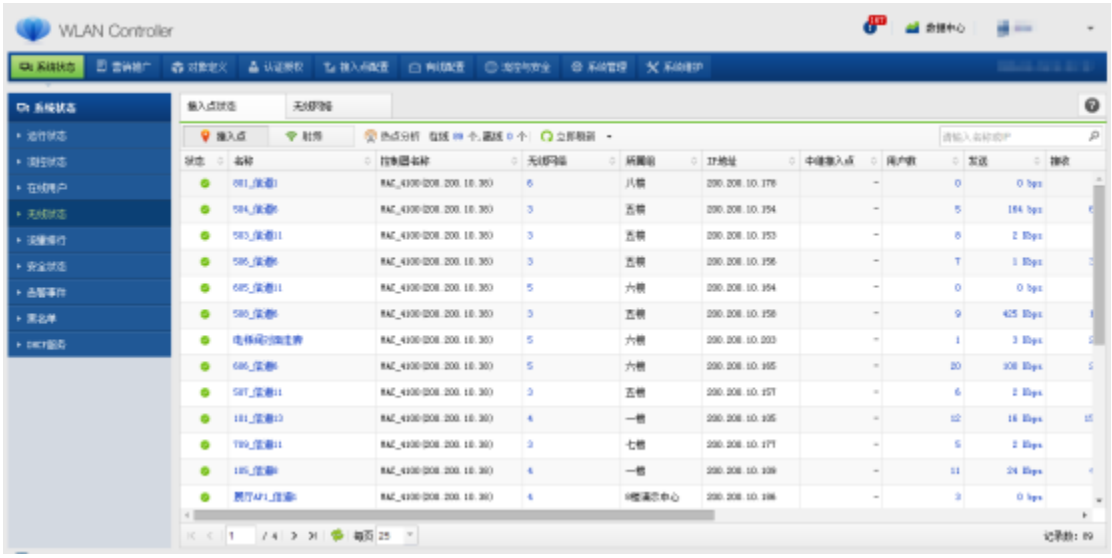


图形化状态显示

通过 web 界面，管理员可清晰直观的查看基于接入点状态、无线网络状态、在线用户的状态、设备运行状态：

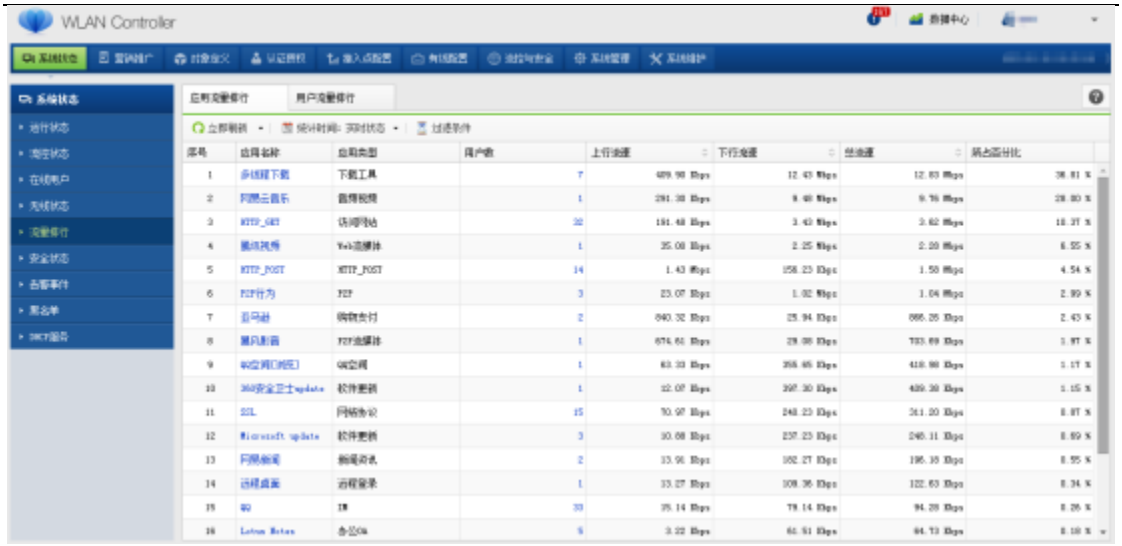
1、 运行状态

2、 接入点状态

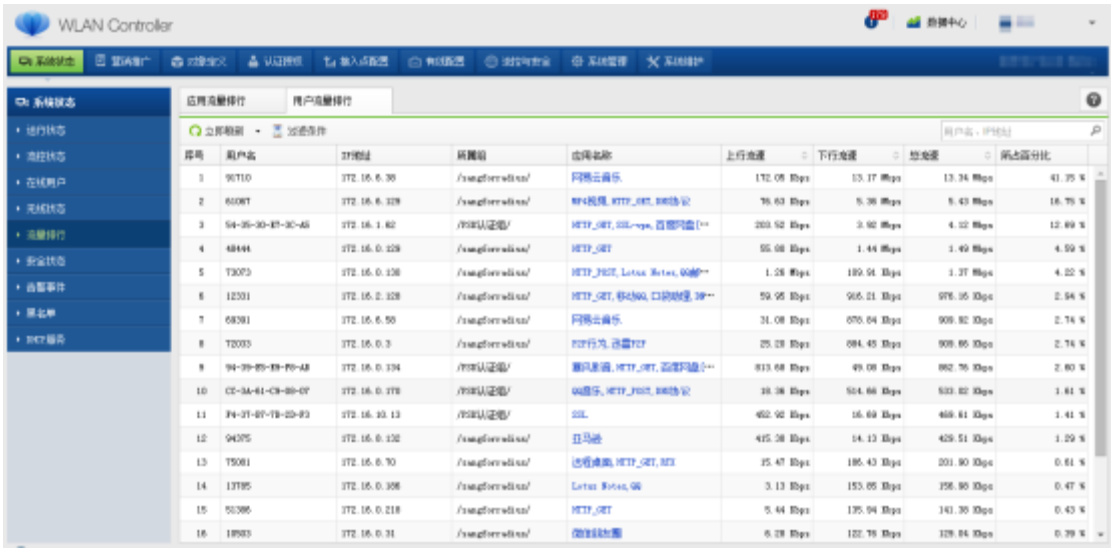


3、 流量排行

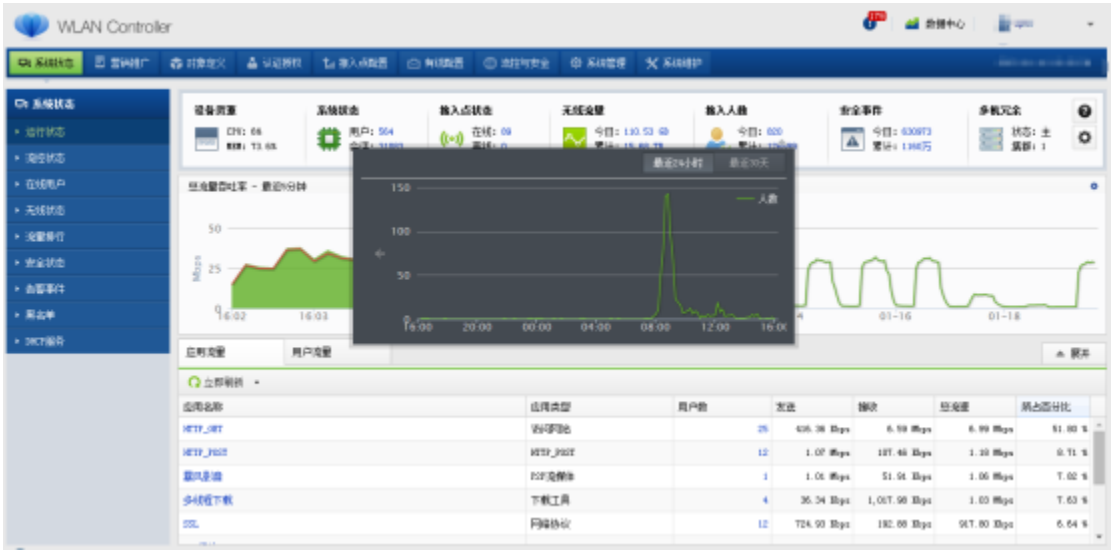
应用流量排行

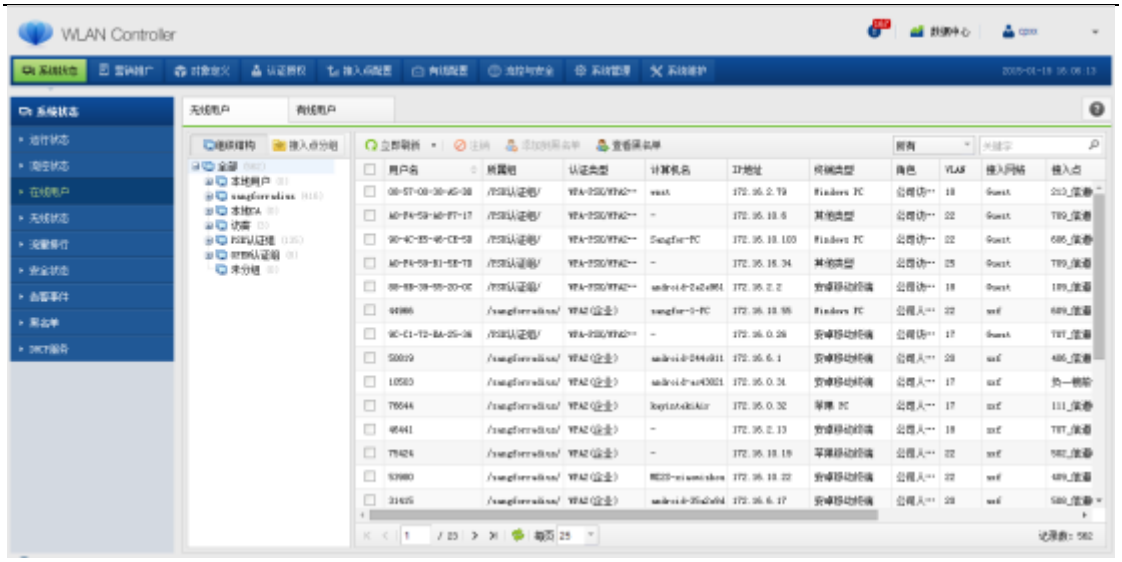


用户流量排行



4、 在线用户





5.4.4 日志查看

为了便于网络管理员更好的管理维护网络，深信服 WAC 支持全面、详细的日志记录，包括接入点日志、系统日志、管理日志、安全日志、用户认证日志

接入点日志

查看接入点日志产生的日志，协助发现及排除故障。

系统日志

查看系统运行过程中产生的日志，协助发现及排除故障。

管理日志

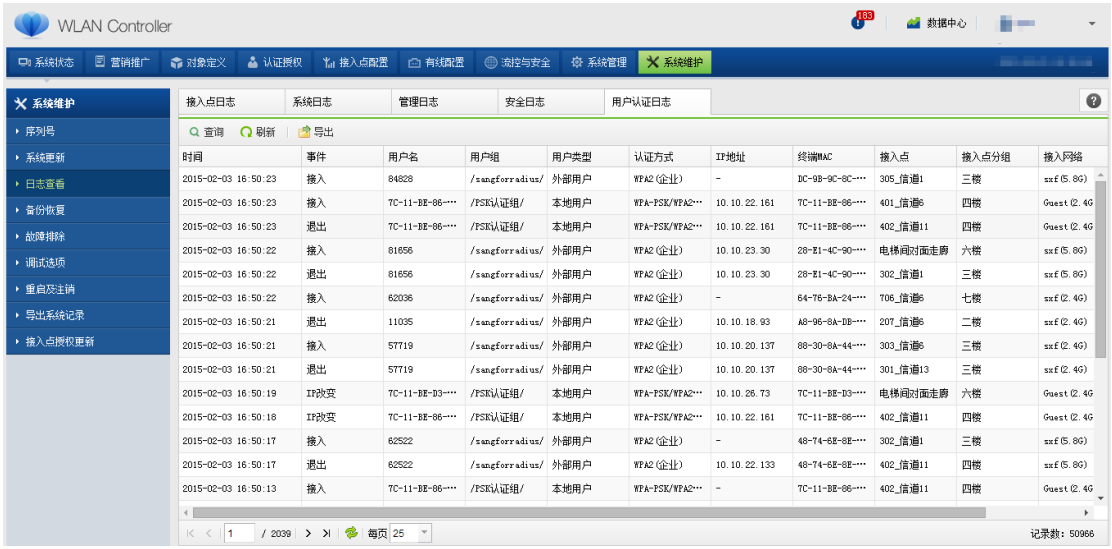
管理日志中，记录了管理员登录、注销、修改配置的日志。

安全日志

记录所有的检测到的无线网络安全事件，并记录检测到的结果。

用户认证日志

用户认证日志中，记录了所有客户端的认证日志，比如查询某一个用户的每次上线、下线具体时间以及位置。



5.4.5 SNMP

SNMP（简单网络管理协议）为不同种类的设备、不同厂家生产的设备、不同型号的设备，定义一个统一的接口和协议，使得管理员可以使用统一的软件来对这些需要管理的网络设备进行管理。

管理员通过网络可以管理位于不同物理空间的设备，从而大大提高网络管理的效率，简化网络管理员的工作。通过标准网管软件，管理员可以向所管理的网络设备获取数据信息【读】、执行设置操作【写】以及设备状态改变告警【Trap】。

SNMP 目前有 v1、v2 和 v3 三个版本，我们的无线控制器均支持 SNMP v1、v2 和 v3，以及支持 SNMP Trap。

5.5 高可用性

5.5.1 AC 双机备份

双机热备采用标准的 VRRP 协议。VRRP（虚拟路由器冗余协议）是一种选择协议，它可以把一个虚拟路由器的责任动态分配到局域网上的 VRRP 路由器中的一台。控制虚拟路由器 IP 地址的 VRRP 路由器称为主路由器，它负责转发数据包到这些虚拟 IP 地址。一旦主路由器不可用，这种选择过程就提供了动态的故障转移机制，这就允许虚拟路由器的 IP 地址可以作为终端主机的默认第一跳路由器。使用 VRRP 的好处是有更高的默认路径的可用性而无需在每个终端主机上配置动态路由或路由发现协议。

双机备份使用介绍

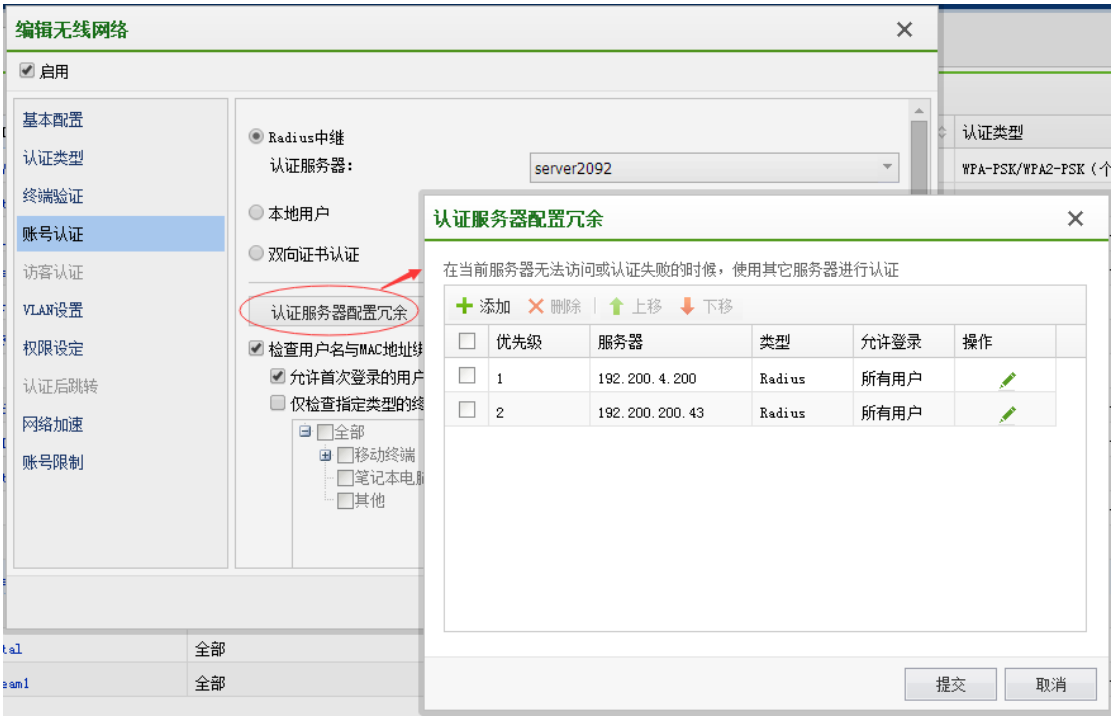
深信服双机备份功能实现在 WAC 上，两台 WAC 一台为主机，一台为备机。当主机运行正常时，备机处于待命状态。主机上的必要配置（例如 WLAN 配置，用户信息等）同步到备机上面。一旦主机出现运行故障，则 AP 自动切换到备机上运行，保证用户业务不中断；当主机恢复后，AP 切换回主机。

5.5.2 DHCP 服务器备份

在 DHCP 服务器双机热备的组网中，两台 AC 同时启用 DHCP Server 功能，并建立热备关系，两台 DHCP 服务器互为备份，实时同步用户已申请的正在使用的 IP 地址信息。当一台 DHCP 服务器宕机后，另一台 DHCP 服务器继续提供服务，不会影响用户的 IP 地址获取、续约等服务，为用户提供可靠的接入服务。

5.5.3 认证服务器备份

在使用 Radius 中继模式下，可配置多个 Radius 服务器，实现认证服务器的冗余备份，当一台 Radius 服务器宕机后，另一台 Radius 服务器继续提供服务，为用户提供可靠的接入服务。



5.5.4 灾难备份

5.5.4.1 无线控制器灾难备份

技术介绍

无线控制器冗机之后，仍然能保证用户正常上网以及新用户的认证接入，提高网络的稳定性和可靠性。

当 AP 与无线控制器因外界因素（如 AC 冗机、控制器与核心交换机网线断开）造成的通信连接断开后，通过 AP 灾备实现 WI-FI 续航，保证用户能够正常上网以及新用户的认证接入，新接入的用户会划分到指定的应急 VLAN 以及分配相应的应急角色，当网络恢复正常时，这些用户会从灾备角色中剔除。

适用范围

适用于无线控制器采用旁路部署在核心交换机的集中转发或本地转发，对所有的认证方式，包括 WPA/WPA2 企业、Portal、微信认证、短信认证、二维码审核、PSK、OPEN 等认证方式均适用。

灾备模式

在 AP 与控制器断开通信的情况下，通过灾难备份仍然能保证新用户正常接入，灾难备份的实现分两种模式：1、在原 SSID 的基础上实现灾备模式，对于终端用户来说是透明的；2、新建采用 OPEN 或 PSK 的应急 SSID。

值得注意的是：若无线网络采用的是 WPA/WPA2 企业（802.1x、CA 证书认证），则只能采用新建 OPEN 或 PSK 的应急 SSID 来实现灾难备份。

局域网部署模式

远程集中部署模式

5.5.4.2　认证服务器灾难备份

当无线接入点在无法连接用户认证服务器（包括内置和外置认证服务器）、短信服务器或微信服务器时，进入灾备模式后，仍然能保证新用户正常接入无线网络。

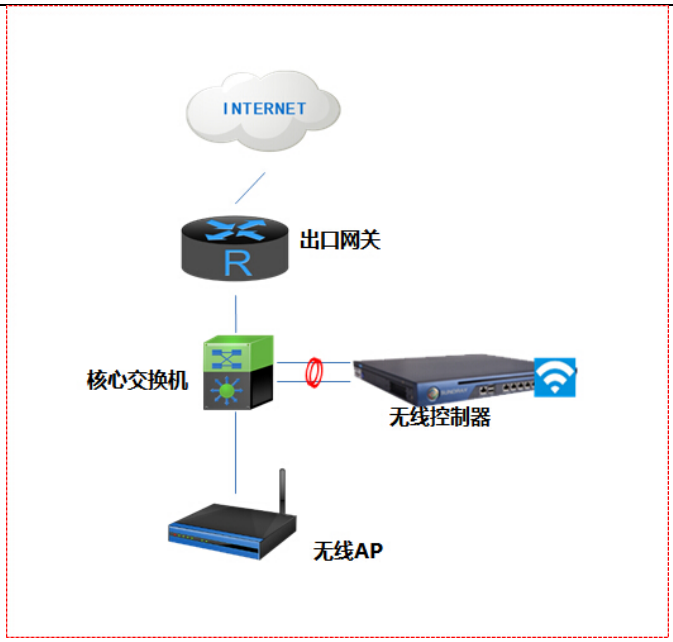
实例：

某 SSID 采用 Portal 认证方式，采用外置第三方 Radius 认证服务器，当所有的认证服务器均不可用时，此 SSID 进入灾备模式，新用户接入认证的时候，在 WEB 页面上输入账号、密码，点击“登录”按钮即可上网（后台并无与认证服务器进行效验）。

5.5.5 端口聚合

一般网络部署时，无线控制器作为本地转发时往往只会连一条网线接在核心交换机上，假如某一天这条网线出问题了（网线松了或者有人错拔了），此时无线控制器相当于脱离了原网络，造成整个网络出现问题。那么，该怎么预防这类问题，提高网络稳定性呢？

端口聚合也叫做链路捆绑，是将多个以太网接口聚合在一起，形成一个逻辑上的聚合接口，以实现流量在聚合接口的各个成员接口间负载分担，并实现链路冗余。



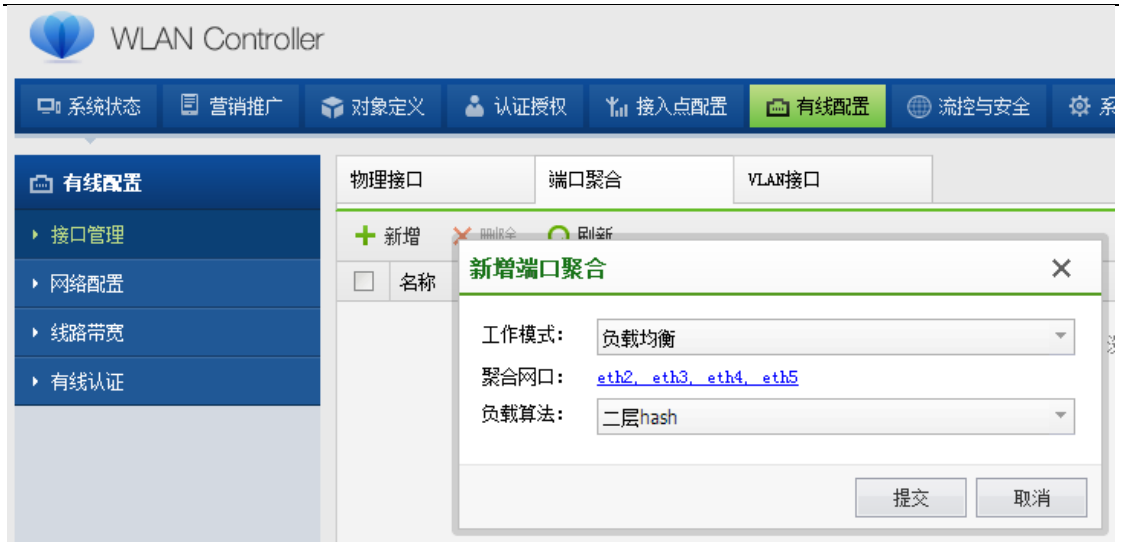
端口聚合支持两种工作模式：

1、 主备冗余

只支持选择 2 个网口组成聚合接口。此模式下，默认使用主网口进行数据通信，在主网口故障时，将切换至备用网口。

2、 负载均衡

支持选择最多 8 个端口组成聚合接口。实现在各成员端口间的流量负载分担，同时保障链路的可靠性，只要不是组内所有端口都故障，两台设备之间仍然可以继续通信。



5.6　节能环保

5.6.1 射频定时关闭

一般企业、商超、政府、金融等场景在晚上凌晨以后，都是没有人使用无线网络的，在这种情况下，启用自动关闭射频信号功能，一方面节能省电，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。

深信服 WAC 的射频关闭控制策略，可以定时自动关闭和开启无线网络的射频信号，另外，还支持设置基于 SSID 的例外无线网络，即对某些射频进行定时自动关闭，特殊 SSID 不关闭。

六、 深信服无线 AP 产品功能

6.1 AP 零配置

结合深信服 AC 无线统一集中管理平台，安装前无需对设备进行任何配置，AP 部署完成后由无线控制器统一下发配置，极大的减少实施和维护的工作量及成本。后期维护中，通过 AC 内置的图形化热点分析界面，可有效查找到问题点，轻松完成维护工作。

6.2 AP 的工作模式

AP 的工作模式有三种 ,分别是 Monitor、Hybrid、Normal ,默认工作模式为 Hybrid。

1.Normal（标准）

AP 仅传输 WLAN 用户的数据，不进行任何监测；

2.Monitor（监控）

在这种模式下，AP 需要扫描 WLAN 中的设备，此时 AP 仅做监测 AP，不做接入 AP。当 AP 工作在 Monitor 模式时，该 AP 提供的所有 WLAN 服务都将关闭。Monitor 模式的 AP，监听所有 802.11 帧；

3.Hybrid（混合）

这种模式下， AP 可以在监测无线环境的同时可以提供无线服务；

6.3 WDS 无线中继网桥

无线网桥和无线中继的区别

无线网桥，是利用无线传输方式实现在两个或多个网络之间搭起通信的桥梁。

无线中继，是无线 AP 在网络连接中起到中继的作用，能实现信号的中继和放大，从而延伸无线网络的覆盖范围。

无线中继网桥功能介绍

深信服 AP 支持的无线中继网桥功能，是无线中继和无线网桥的结合体，无线中继 AP 的以太网口可以再接有线交换机，实现延伸无线网络的覆盖范围的同时扩展局域网。

注意：目前 AP-240-S 和 AP-240-P 不支持无线中继网桥功能。

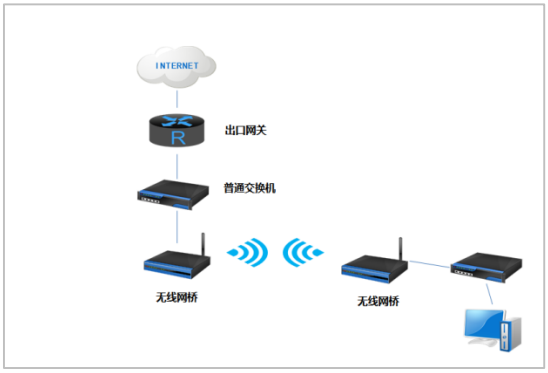


图 1：无线网桥

图 2：无线中继

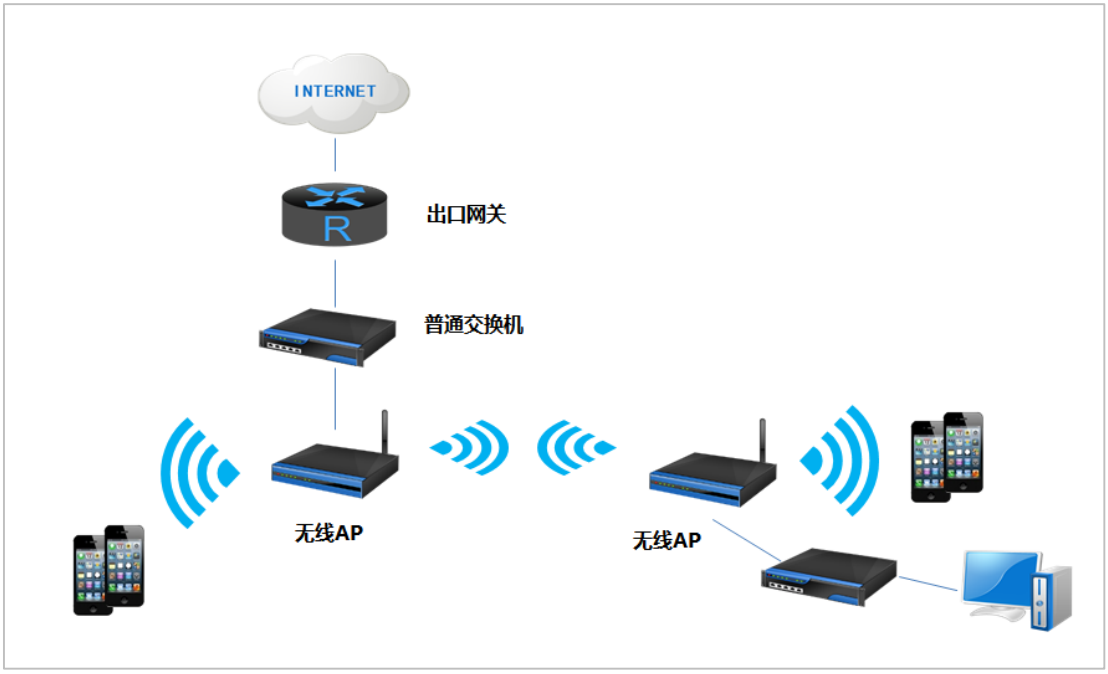


图 3：无线中继网桥

6.4　灵活的数据转发方式

AC+瘦 AP 架构可实现数据集中转发和本地转发，当数据转发为本地转发时，用户业务数据由 AP 承载。

以 AC+瘦 AP 架构为基础，实现无线数据在 AP 本地的转发，突破了传统集中式转发的性能瓶颈。可将无线网络的管理流和业务流分开，减少由于集中转发带来的负载压力，有效的节约有线带宽。

本地转发概述

深信服本地转发技术，控制流和数据流采用了不同的处理方式，用户和 AP 的管理由 WAC 处理，而用户的数据转发则直接由 AP 处理。本地转发技术有效的缓解了 AC+瘦 AP

组网方式下 AC 和数据隧道的压力，并减小了数据的传输延迟。同时，相对与传统胖 AP 架构，以 AC+瘦 AP 架构为基础的本地转发模型，保持了 AC+瘦 AP 架构在安全、管理等方面的优势。

本地转发数据处理方式

1）用户的管理帧，如 802.11 管理、控制报文和 802.1x 协议报文等，直接通过认证模块传递给 AC 集中处理，以实现用户的认证、授权等。

2）用户的数据帧，包括 802.11 数据和来自有线的 802.3 数据报文，在 AP 本地进行解析、封装等处理，并直接由 AP 进行转发，实现数据的高速处理。同时，用户流量信息将通过用户认证管理模块通报给 AC，以实现流量统计，计费以及负载均衡等应用。

6.5 射频优化与智能负载均衡

对于一些无线用户密集的区域， AP 产品结合 AC 无线控制器可智能、实时的根据用户数和频段的使用情况调整分配到不同的接入点，平衡负载压力，极大的提高无线网络的容量和连接可用性。

配合 WAC 可自动进行射频调整，有效避开自干扰，也可以自动进行信道调整，各 AP 工作在不同信道，有效避开信道间的干扰。

6.6 全面的安全策略

全面支持 IEEE802.11i 加密方式（WPA-PSK/WPA2-PSK、WPA/WPA2 企业级），并支持 802.1x、WEB 认证等多种用户认证的方式，无线网络用户可以根据需要方便选择。

配合深信服 WAC 提供诸如防 DoS 攻击，WIDS，无线安全等多种安全机制，同时能将攻击源定位并加入黑名单进行冻结，有效的防范 WLAN 内的安全威胁。

6.7 一体化管理

深信服全系列产品均通过 AC 平台进行一体化的管理，具备良好的扩展性，能满足客户对无线网络管理不断发展的需求。同时，基于 WEB 的管理界面，给无线业务管理员提供简单，友好，易用的管理平台，真正实现无线智能一体化管理。

七、 关于深信服科技

7.1 关于深信服

深信服公司成立于 2000 年 12 月，是中国规模最大的前沿网络厂商。多年来在网络安全&优化、无线与虚拟化领域持续发展，致力于提供创新的 IT 基础设施虚拟化与云建设解决方案。目前，深信服在全球共设有 55 个直属分支机构，其中包括香港、新加坡、马来西亚、印尼、泰国、英国和美国等七个海外办事处和分公司，员工规模超过 2000 名。

随着企业规模的扩大发展，深信服也获得了多方认可。先后获得了“CMMI5 国际认证”、“第一批国家高新技术企业”、“国家规划布局内重点软件企业”“亚太地区德勤高科技高成长 500 强”等殊荣。同时，深信服还是 IPSec VPN 和 SSL VPN 两项国家标准的主要承建单位、并受邀参与制定《第二代防火墙标准》。在行业合作上，深信服是互联网应急中心应急服务支撑单位、国家信息安全漏洞共享平台 CNVD 成员单位、中国国家信息安全漏洞库 CNNVD 技术支撑单位和公共漏洞和暴露组织 CVE 认证合作单位。

目前，全球有超过 30,000 家用户正在使用深信服的产品。其中，在中国入选世界 500 强的企业有 80%的企业都是深信服的用户。同时，凭借优秀的产品表现，深信服多款产品入围了包括国家税务总局、国家电网、建设银行、工商银行、中国移动和中国电信在内的各行业集采，各款产品均得到了广泛应用。

时刻走在行业前沿，深信服始终保持着创新能力

多年来，深信服持续将年收入的 20%投入到研发，并在深圳、北京和硅谷设立了研发中心，研发人员比例达到了 40%。在对创新发展的持续投入下，深信服一直保持着每 1-2 年推出一款新产品、每季度更新 1 个新版本的研发速度。截至 2014 年，深信服共申请超过 256 项国

内发明专利以及 10 项美国专利。此外，深信服是推出了全球第一台 IPSec VPN 和 SSL VPN 二合一 VPN，中国第一台上网行为管理和第一台下一代防火墙的厂商。

将产品和服务做到最好，深信服快速响应市场需求

深信服研发人员每月都会进行例行的客户拜访以收集产品需求，每年都能收到超过 1000 条有效需求，并在研发工作中将其迅速转化为产品新版本。同时，深信服在深圳、长沙、吉隆坡三地设有超过 100 坐席的 CTI 中心，提供 7*24 小时的电话咨询和远程调试服务。在全国范围内，深信服在 49 个城市设立了备品备件库，配有原厂工程师第一时间提供技术支持。

进入的每一个细分市场，深信服都会努力成为 No.1

深信服的硬件 VPN、SSL VPN 两款产品连续 7 年保持着市场占有率第一；上网行为管理产品连续 9 年市场占有率排名第一；广域网优化产品保持在市场第一位；应用交付产品市场排名第二、也是排名第一的国产品牌。目前，深信服 SSL VPN、上网行为管理、下一代防火墙、广域网优化、应用交付 5 款产品均入围了 Gartner 魔力象限，获得国际认可。

无线产品团队超过 250 人，研发团队超过 150 人，于 2015 年正式通过了软件能力成熟度模型集成 CMMI 五级，产品研发过程始终遵循国际最高的 CMMI5 标准，拥有专业先进的测试设备、测试环境，产品生产过程严格把控， 产品质量控制体系达到国际领先水平。研发无线产品多年，在无线硬件射频、软件控制、漫游、负载均衡、无线增值等各个领域有着多年深厚的技术积累。

截止 2015 年 5 月，已为超过 5000 家企业提供无线解决方案，向超过 1000 万用户提供安全、高速的无线服务。

因为更专注，所以更专业。Sangfor 投入 100%的工作精力和热情，致力于为企业、教育、政府、医疗、酒店、金融、商超、连锁等行业用户提供量身打造的最安全、会营销的应用层企业级无线网络。