AdMaster 精硕科技公司无线网络安全接入解决方案

Fortinet（中国）公司

2013 年 5 月

目录

一、概述

随着移动设备与应用的激增，以及 IEEE 802.11n 的广泛采用，如今 Wi-Fi 环境与形势变得复杂难控。对所有的无线用户与应用都采用相同的网络策略已经不能有效的保证无线网络的安全，配置与实施 WLAN 控制策略是迫切需要的。

移动设备的日益普及和削减成本之需要促进了无线 LAN（WLAN）的采用。分析师预测企业 WLAN 设备的开支将从 2011 年的 34 亿美元攀升到 2016 年的 79 亿美元，复合年均增长率达 18.4%。此外，各类公司、组织机构纷纷支持无线边缘设计，进一步的促进与边缘交换机和有线部署相关的成本削减。

IEEE 802.11n 无线标准是更多的企业采纳无线部署方案的催化剂， 由于 IEEE 802.11n 新标准覆盖范围更广，比传统无线标准性能增强五倍，远优于有线高速以太网 LAN。籍由此，WLAN 的采用更为普及，其在网络应用服务，如 WLAN 网络管理和安全中的需求更为显著。

二、用户现状分析

2.1 公司概况

AdMaster 精硕科技是中国领先的互联网广告全流程效果监测、分析评估、媒介优化咨询服务和技术解决方案提供商。AdMaster 成立于 2006 年，总部位于上海并在全国各地设有多个分支机构。

AdMaster 将多年对中国网络营销的理解和实践经验注入产品的研发和创新，通过技术驱动帮助广告主实现网络广告效果监测与调研的更深入结合、网络营销的平台化整合，以实现广告主的品牌传播与营销效果 ROI 的有效提升。

2010 年，AdMaster 成功实现高速发展，同时得到了广告主和媒体的高度认可。同年底，AdMaster 获得知名风险投资商金沙江创投(GSR Ventures)首轮融资，为今后公司的发展奠定了更加坚固的基础。2011 年又推出了更全方位的网络营销效果评估系统，为客户提供更有效、普遍的广告评估体系。

2.2 网络现状及需求分析

AdMaster 北京技术研发中心办公场所大约 1000 平方米，由原来的商住两用楼改造而成。互联网出口 xx 兆 xx 链路，千兆链路到桌面，部分墙壁和工位留有网线节点。整个网络由交换机、路由器组成，尚无专业安全设备进行防护，存在一定的网络安全隐患。

随着移动智能设备的广泛应用，平均每个员工拥有 3 个设备需要连接互联网（大多为企业需要），无线接入需求日益增加。目前由非企业级无线产品搭建的网络出现拥塞、连接不稳定等问题，降低了员工上网体验。同时，有线网络无法满足如会议室、培训室等环境的网络连接需求。随着互联网应用的增多，移动用户安全接入公司内网的需求也在增加，整个公司网络有必要进行升级改造，具体思路如下：

1、 内网用户和服务器采用高性能的 NAT 设备确保上网质量；

2、 将网络划分为不同的 VLAN，减少广播数据包；

3、 根据应用控制流量带宽；

4、 利用 IPSec VPN 与境外服务器安全通讯；

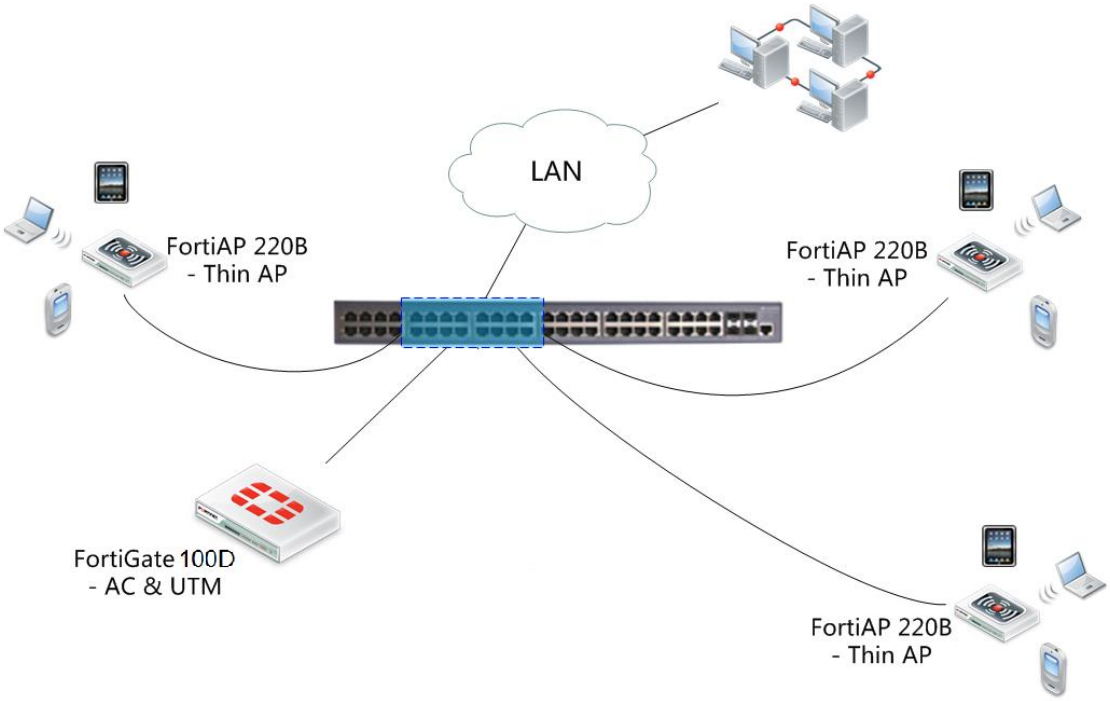
5、 员工从公司外使用 SSL VPN 安全访问内网资源；

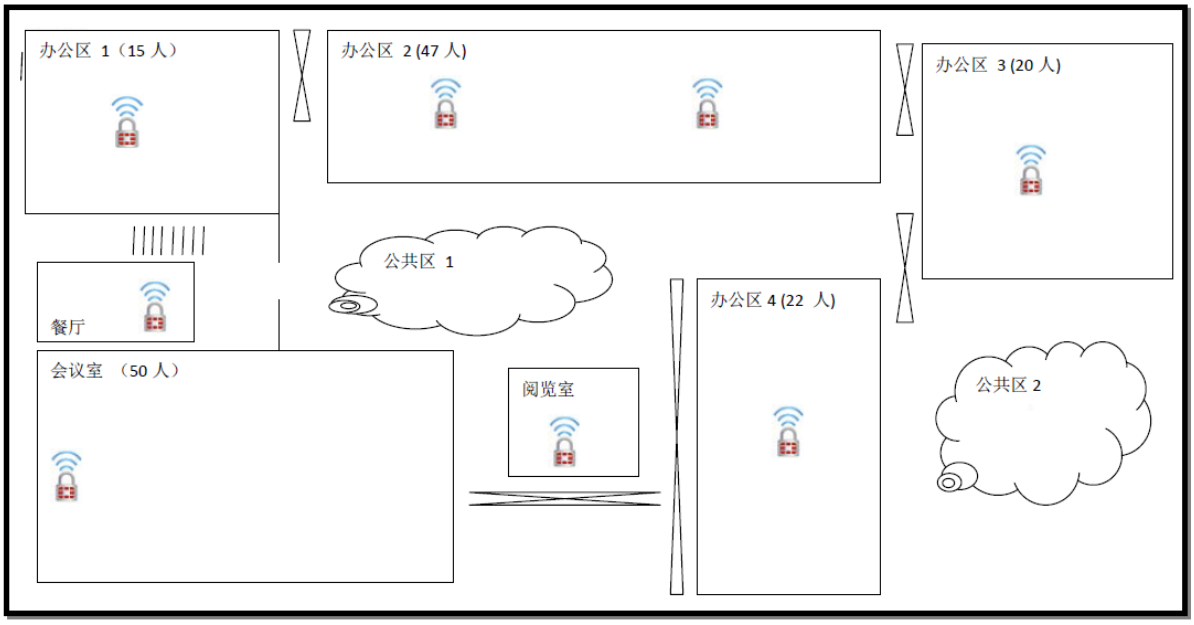
6、 用户上网认证单点登录，提高应用安全性和方便性；

7、 对访客及移动设备 BYOD 的管理。

三、无线安全组网

3.1 组网拓扑示意





根据上述示意图，在互联网出口部署 **1** 台 FortiGate-100D 无线控制安全网关，按照考察的实际办公空间环境，总共部署 **9** 台 FortiAP-220B 无线接入点设备。结合业务需要，FortiGate-100D 上将启用如下功能：

- 防火墙访问控制策略，对服务器做地址映射，发布到互联网；
- 设置 IPSec VPN 与远端服务器建立 VPN；
- 设置基于策略或策略路由分配不同的业务流量到相应的链路；
- 设置 SSL VPN，使公司网络外员工安全加密接入访问内网资源；
- 启用无线控制器（AC）功能，管理和控制部署的 9 台 AP 设备；
- 设置无线用户认证访问，配置适当的访问控制策略；
- 设置基于应用或服务的带宽控制，保障关键核心业务网络带宽资源；
- 配置来宾用户管理，安全审计所有经过公司网络的互联网访问。

详细的无线网络安全部署，请参考下面内容。

3.2 无线组网设备

Fortinet 的无线网络接入及安全方案由 AP（无线接入点）和 AC（无线接入控制器）两部分组成。

FortiAP 是可管理的瘦 AP(以下简称 AP)。FortiAP 配备最新的 IEEE 802.1n 的无线芯片以提供高性能的无线接入，在每个无线波段集成监控和多个虚拟 AP 功能。AP 产品与一系列丰富的 FortiGate 控制器（以下简称 AC）产品给用户提供了增强的无线空间。无线运行模式、通道设定、传输功率强弱等，都由 AC 集中控制，以更方便安装和管理。

每个 AP 都把流量引入到集成在 FortiGate 平台的 AC，该流量经过身份识别、UTM（统一威胁管理）引擎检查，仅授权的无线数据流量被转发。除从一个控制台控制网络访问、快速方便的更新策略和监控外，FortiGate 的深度检查引擎还能提供防火墙、VPN、防病毒、IPS 等网络层和应用层安全防御手段，建立在 Fortinet 多年的网络安全经验基础之上，为客户提供安全的无线网络接入。

FortiAP（AP）和 FortiGate（AC）的无线控制功能提供超强的安全解决方案：

- **身份验证：**强大的身份验证功能，支持 WPA2、802.1x 等。
- **安全防御：**为无线网络提供业绩顶级的 UTM 安全保护。
- **高性价比：**灵活的安装，多功能安全与无线接入的整合，实现较低的总体拥有成本。

本方案选择的 AC 型号为 FortiGate-100D，数量 **1** 台；AP 型号为 FortiAP-220B，数量 **9** 台。

FortiGate-100D

FortiAP-220B

可供选择的 FortiAP 型号如下：

技术参数 **硬件特征**	***FortiAP-210B***	***FortiAP-220B***	***FortiAP-222B***
部署方式(室内/室外)	室内	室内	室外
射频数量	1	2	2
频段基带(GHz)	2.400 - 2.4835 • 5.150 - 5.250 • 5.250 - 5.350 •5.470 - 5.725 • 5.725 - 5.850		
天线数量	内置 2 个	内置 4 个	外置 4 个
射频 1 的频段	2.4GHz b/g/n 或 5GHz a/n	2.4GHz b/g/n 或 5GHz a/n	5GHz a/n
射频 2 的频段		2.4GHz b/g/n	2.4GHz b/g/n
Tx 数据流	2×2MIMO，双流/300Mbps	2×2MIMO，双流/600Mbps	2×2MIMO，双流/600Mbps
以太网接口	1 个 10/100/100 接口	1 个 10/100/100 接口	1 个 10/100/100 接口

串口	1	1	0
PoE	802.3af(15.4w)	802.3af(15.4w)	802.3at(30w)或内置
支持 WME	是 (4 个优先级队列，语音、视频、数据和背景流)		
WMM 多媒体标准	获得 Wi-Fi Alliance's Wi-Fi Multimedia™ certification program 认证		
SID	7 个为接入用户，1 个监控	14 个为接入，2 个监控	14 个为接入，2 个监控
EAP	EAP-TLS EAP-TTLS/MSCHAPv2 EAPv0/EAP-MSCHAPv2 PEAPv1/EAP-GTC EAP-SIM EAP-AKA EAP-FAST		
最大传输功率	17dBm(50mW)	17dBm(50mW)	硬件支持27dBm(500mW)，受限于软件
物理安全	锁	锁	混凝土和打孔
MTBF	86013 小时	68006 小时	305420 小时
尺寸			
外形	高 2.7cm, 宽 16.3cm, 长 12.9cm	高 2.7cm, 宽 16.3cm, 长 12.9cm	高 7cm, 宽 19.7cm, 长 25.4cm
重量	320g	320g	2.3kg
安装位置	墙上或者桌面	墙上或者桌面	墙上，或打孔安装
环境			
电源	电源适配器输入 100-240V, 50/60Hz, 0.6A 输出 12V, DC,1.5A	电源适配器输入 100-240V, 50/60Hz, 0.6A 输出 12V, DC,1.5A	交流电供应的 POE 模块
湿度	10%到 90%非凝结	10%到 90%非凝结	0 到 100%
工作温度	0 到 50°C	0 到 50°C	20 到 60°C
存储温度	-25 到 70°C	-25 到 70°C	20 到 60°C
工作目标	专用的 AP 接入或监控	专用的 AP 接入，同时监控	室内，室外，工业环境，以及其他危害的地方
指令	低电压指令/RoHS		

FortiGate-100D 设备性能：

硬件性能			
防火墙吞吐量 (1518/512/64)	2500 / 1000 / 200 Mbps	IPS 吞吐量	950 Mbps
防火墙延迟	37 µs	反病毒吞吐量 (代理扫描 / 流扫描)	300 / 700 Mbps
并发会话数	2.5 Mil	虚拟域(默认 / 最大)	10 / 10
每秒新建会话数	22,000	最大 FortiAP 数量	32

防火墙策略 (系统/VDOM)	10,000	最大 FortiToken 数量	1,000
IPSec VPN 吞吐量	450 Mbps	客户端到网关 IPSec VPN 隧道数	5,000
SSL-VPN 吞吐量	300 Mbps	并发 SSL-VPN 用户数 (推荐最大)	200

四、无线安全部署

4.1 AP 与 AC 的连接

在内网交换机上划分一个 VLAN（例如：VLAN 160），专门用于 AP 和 AC 的连接。

AP 和 AC 各使用一个接口连接至 VLAN 160，IP 地址设置为同一地址段。例如：AC 的 Port19 接口地址设置为 10.160.1.230/24，并配置默认路由指向 10.160.1.254，使之能访问内部有线网络的其它部分。AP 的 Eth 接口地址分别设置为 10.160.1.1-10.160.1.200，并将 AC 地址指向 10.160.1.230。AP 的 IP 地址和 AC 地址既可以通过 console 手工设置，也可以通过在 AC 上配置 DHCP 服务动态获取（此时无需对 AP 进行任何配置）。

AP 自动连接到 AC 后，需要管理员手动进行授权，才能接入网络，防止非法 AP 接入的发生。

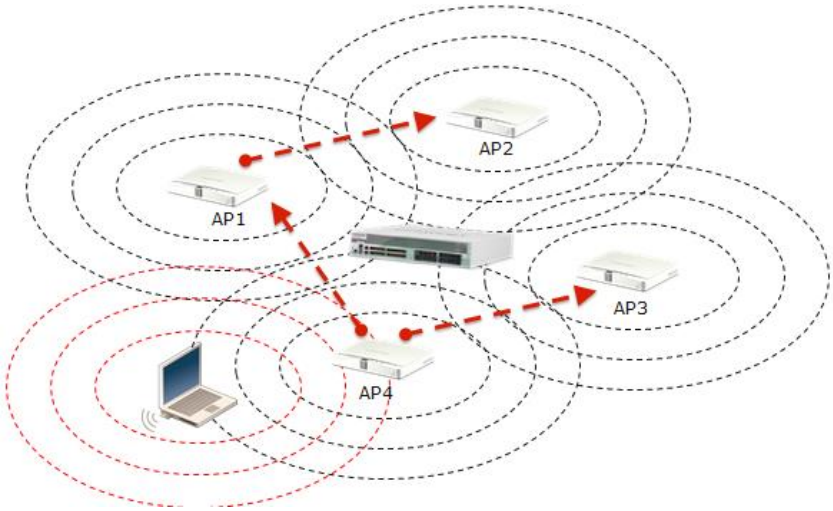
AP 和 AC 之间支持多种连接环境，包括直连、交换环境、路由环境，以及跨广域网的远程环境，AP 与 AC 可以工作在相同或不同 IP 网段，可以在同一局域网或广域网的不同地区，只要 IP 可达，即可正常工作。

AP 和 AC 之间使用标准的 CAPWAP 协议（无线接入点控制与配置协议），AP 仅作为一个无线信号接入点，不处理任何数据，透明地将无线设备（PC、PAD、

手机等）的流量通过 CAPWAP 隧道传输到 AC，由 AC 统一处理，并由 AC 负责进行网络层及应用层的安全过滤（包括防火墙访问控制、用户身份认证、入侵防御、病毒过滤、上网行为管理、内容过滤等）。

CAPWAP 协议的控制流量和数据流量均可以使用 DTLS 加密，保证通信内容不被窃取。

一台 AC 可以同时接入管理多台 AP，AC 可以把相同的 SSID 分发到所有 AP，使无线用户在不同 AP 的覆盖范围内无缝漫游。

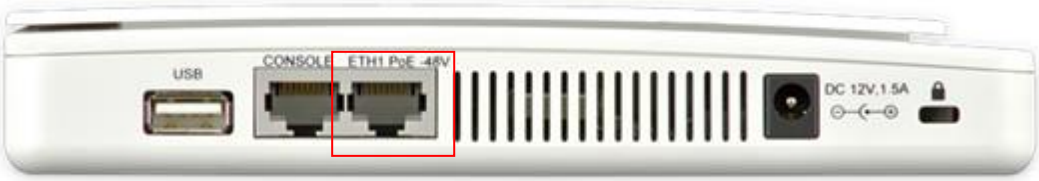


本次选择的 FortiGate-100D，配合 FortiOS v5.0 版本软件，可以同时接入管理 32 台 FortiAP。

4.2 AP 的部署和供电

为保证型号覆盖及传输质量，应该将 AP 按照不超过 20 米的间隔进行蜂窝状部署，并考虑各种墙体对信号的屏蔽作用。

FortiAP-220B 支持适配器和 PoE 两种方式供电，只要将其与支持 PoE 的交换机或网络设备相连，便可直接通过网线供电，不再需要连接外置电源。



4.3 无线用户与 AP 的连接

无线上网用户（PC、PAD、手机等）使用标准的 802.11 无线协议族连接到 AP，从而接入无线网络。

FortiAP 支持以下 WIFI 协议：

- IEEE 802.11a (5-GHz Band)
- IEEE 802.11b (2.4-GHz Band)
- IEEE 802.11g (2.4-GHz Band)
- IEEE 802.11n (5-GHz & 2.4-GHz Band)

FortiAP-220B 内置 4 个天线，支持两个 Radio 同时工作，例如一个 Radio 处理 5-GHz 802.11n，另一个 Radio 处理 2.4-GHz 802.11n。

Fortinet 的无线方案支持 ARRP（自动无线资源管理）功能，所有 AP 都会自动周期性地检查无线网络环境，选择最佳频道进行通信，减少网络干扰，获得最佳通信质量。

AP 可以使用 DHCP 为无线上网终端分配 IP 地址、掩码、网关、DNS 等网络设置，减少终端配置工作量。

4.4 无线通信的安全保护

4.4.1 通信加密

Fortinet 无线方案支持多种无线加密方式，包括：

- 开放模式（不加密，不建议使用）；
- WEP（64bit 或 128bit RC4 加密）；
- WPA（256bit TKIP 或 AES 加密）；
- WPA2（256bit TKIP 或 AES 加密，在 WPA 的基础上支持 802.11i 标准的安全要求）；

从安全角度考虑，建议使用 WPA2 和 AES 加密方式。

目前 FortiOS 4.3 已经将开放式和 WEP 方式加密放在命令行，图形界面中的加密方式仅保留 WPA-WPA2personal、WPA-WPA2-Enterprise、强制门户，如下图所示。

本项目建议用户使用 WPA-WPA2-Enterprise 或强制门户的认证方式，在 FortiGate-100D 无线控制器上配置本地用户，添加到本地用户组，在选择该用户组认证即可。采用强制门户，将会在用户接入无线网络时弹出认证页面，输入用户账号认证通过后才能接入无线网络。如果移动设备不支持

WPA-WPA2-Enterprise 认证窗口，建议使用该认证方式。

4.4.2 无线准入控制

为防止非法用户对无线网络的滥用以及可能产生的安全威胁，Fortinet 无线方案可以使用如下几种方式对无线用户的接入进行控制。

- 关闭 SSID 广播——其它无线用户无法扫描到 SSID，降低安全风险。
- 控制发射功率——减少不必要的覆盖，例如办公区域以外。

- MAC 地址过滤——建立 MAC 地址白名单，不在名单内的终端无法接入网络。
- 无线接入用户认证——支持强制 Web 认证页面、WEP 预共享密钥、WPA/WPA2 预共享密钥、802.1x、动态令牌等。用户认证数据库既可以在 FortiGate 本地建立，也可以使用第三方认证服务器，包括 Radius、LDAP、TACACS+、Windows AD 等。
- 访问控制用户认证——防火墙策略控制用户登录。

4.4.2.1 关闭 SSID 广播

为了确保公司内部上网的无线 SSID 的安全，不需对外公开，建议关闭 SSID 广播。来宾用户的 SSID 开启广播，以方便访客使用。

4.4.2.2 MAC 地址过滤

MAC 地址过滤可以建立黑名单也可以建立白名单。所谓黑名单就是缺省状态下全部允许，但是部分 MAC 不允许。

这里要注意的是，当某无线设备 MAC 地址被阻断时，表现出来的现象与无线 WPA 认证通不过的现象是一样的。

4.4.2.3 基于 Radius 认证

如果用户已有或未来将使用 Radius 认证，可参考下面的使用方法。

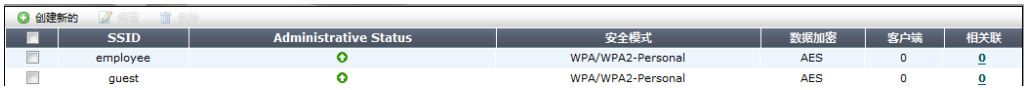
配置 Radius 认证有两种方法，一种是直接启用，但需要修改客户端无线的认证参数，另外一种方法是建立一个用户组，将 Radius 引入到用户组。第一种方法对现网改造来说不太方便，不建议采用

4.4.3 访问控制

Fortinet 无线方案能对无线用户接入网络后的访问权限进行控制，包括以下几种方式：

- 使用不同的 SSID 将用户分组。例如内部员工使用 employee SSID，来宾使用 guest SSID。这两个 SSID 使用不同的 IP 地址段，不能直接互访，必须经过 FortiGate 安全设备的过滤。本次部署的方案支持最多 14 个接入用的 SSID。

  还可以为不同的 AP 分配不同的属性（AP profile），实现不同的部署。例如：AP1 部署在会议室等公共区域，启用 employee 和 guest 两个 SSID；AP2 部署在办公区域，只启用 employee 一个 SSID。

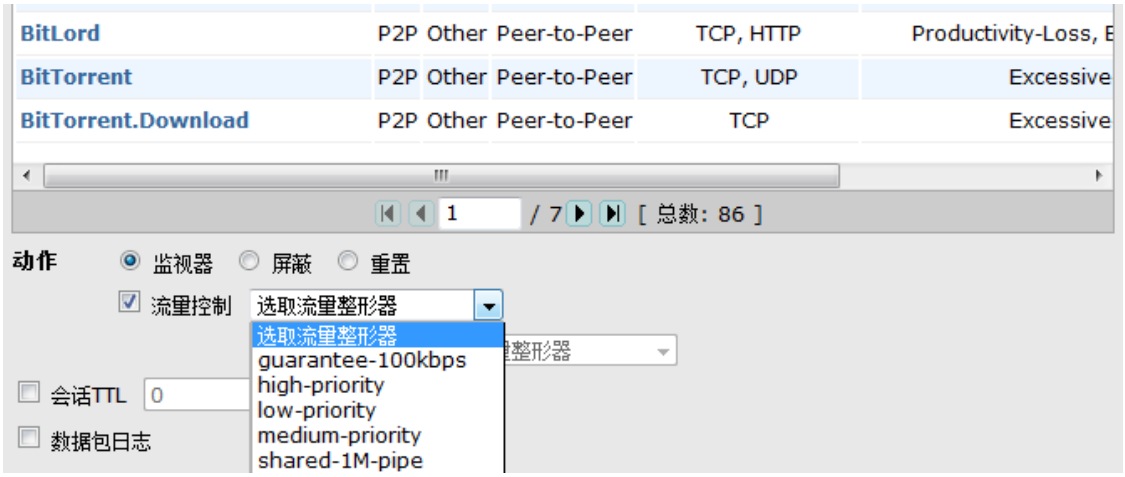


- 防火墙访问控制。各组用户通过不同 SSID 接入无线网络后，无论互访还是访问网络其它区域（如生产网、办公网等），都要经过防火墙策略的控制。FortiGate 可以对源/目的接口、源/目的 IP 地址、源/目的端口、

时间、用户等进行过滤，从而使每一个无线用户都仅能访问他可以访问的资源。

4.4.4 应用安全功能

Fortinet 无线安全方案无缝集成了 Fortinet 公司领先业界的 UTM（统一威胁管理）安全解决方案，除防火墙外，还可以直接使用 VPN、入侵防御、网关防病毒、Web 内容过滤、应用带宽控制、Email 过滤、数据泄漏防护等网络层及应用层安全功能，对无线用户的网络访问进行全面的安全防护，使整个无线网络达到一个很高的安全水平。

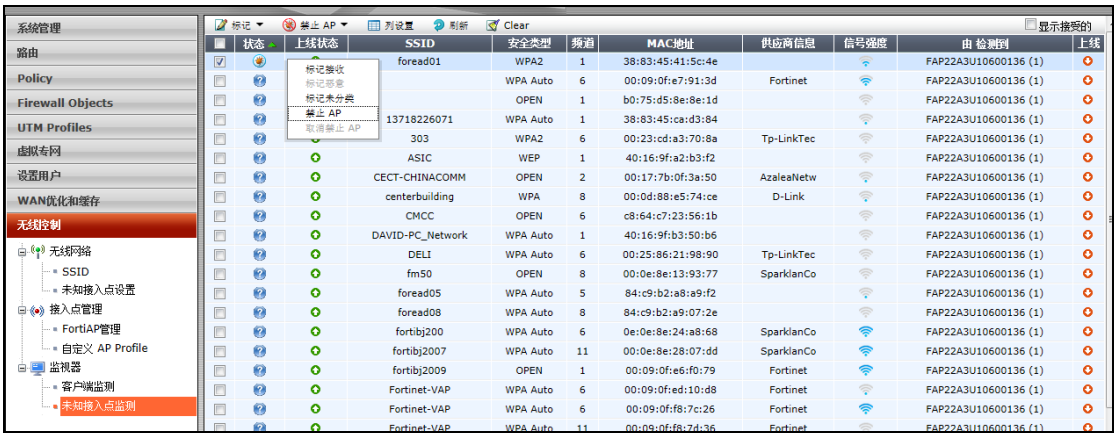


4.6 无线资源的管理

4.6.1 非法 AP 压制

FortiAP 可以对非法的 AP 进行无线压制，进行无线压制建议最好采用支持 2.4G 的 Radio，将其设置为“专属监测”，该频段不再作为无线终端连接的 Radio。

开启非法 AP 检测，此时，监控所有无线 AP，并且可以选择非法 AP 进行压制了。



4.6.2 基于 AP 的负载均衡

无线控制器将客户端信号切换到最不繁忙的 AP，客户端基于 AP 阈值（缺省：30）切换到另一个 AP。 AP 切换时，目标 AP 接收到的客户端信号强度应大于等于配置的 RSSI 阈值。

4.6.3 基于频段的负载均衡

无线 AP 可以主动引导支持 2.4/5GHz 的无线终端优先采用 5Hz 频段关联无线接入点。FortiOS 5.0GA 可以支持该功能，也就是说当即支持 2.4G 又支持 5G 的客户端接入无线网时，自动地根据实际情况将其引导到 5G。

4.6.4 无线频段管理

在 FortiGate 中可以实现对 Radio(频段)中的频道进行管理，以 2.4G 为例，可以选择 1、6、11 的频道。

如果担心该频道被其他 AP 使用，也就是说频道冲突，可以选择“无线资源提供”，这样它可以自动地回避被其它 AP 使用的频道。

建议内网用户使用 5G 频段，来宾用户使用 2.4G 频段。

五、无线方案优势

以 FortiGate 作为 AP 集中管理器，与 FortiAP 组合起来构成一个无线接入网络，具有 AP 的集中管理、集中认证、无线漫游；充分发挥 FortiGate 的防火墙、应用控制、带宽控制等安全功能，并且能够和企业的认证体系和网管体系结合在一起，为用户提供一个安全的、可靠的无线接入平台。其优势特点如下：

- **最高安全性**。

  提供防火墙、防攻击、IPsec VPN、SSL VPN、用户认证、BYOD、应用控制、带宽控制等功能。

- **无线控制无需额外许可**。

  FortiGate-100D 支持管理 32 台 FortiAP，完全满足用户现在和未来扩展的需要。

- **最高性价比**。

  FortiGate-100D 无线控制器为用户提供了全面的安全性和灵活性。

- **总体拥有成本和维护成本低**。

- **简化安全和无线管理**。

- **整体方案扩展性强**。