FortiGate 无线组网指南

上一篇我们介绍了 FortiGate 开箱配置的一些列方法和过程，我们可以通过 PC 和 iPhone，使用 FortiExplorer 进行 FortiGate 的开箱配置，此外，我们还介绍了传统的 Console 配置模式。

在本篇中，我们将介绍如何使用 FortiGate 进行组网。相信大家在很多介绍中已经了解到 FortiGate 一大优势就是将无线控制器 AC 集成到了防火墙中，那么如何使用呢？当您购买了 FortiGate 及 FortiAP 无线接入点设备之后，该如何快速搭建起一套无线网络，并通过 FortiGate 进行妥善管理呢？

目录

拓扑环境介绍

下面图 1 就是我们这次演示的拓扑环境

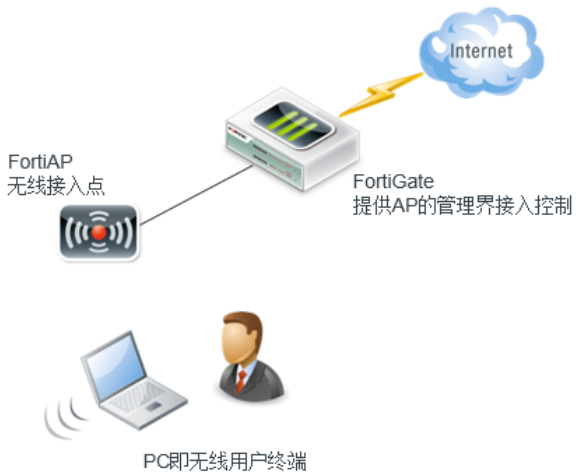

图 1：FortiGate 无线网络演示拓扑

如上图所示，我们使用了一台 FortiGate（90D-PoE）来作为组网核心，以及 FortiAP 无线接入点，还有笔记本作为无线接入终端，通过无线网络访问互联网。

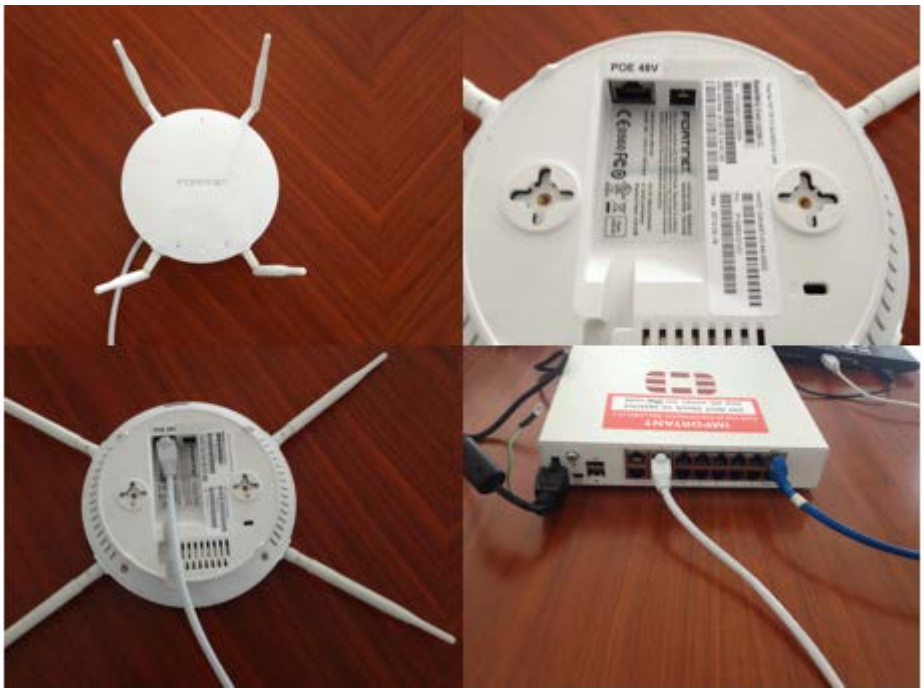

图 2：FortiAP-223B 外观与 FortiGate-90D-PoE 互联

如图 2 所示，左上角的 AP 为 FortiAP-223B，右下角为通过网线连接到 FortiGate-90D-POE 的 poe 端口通过以太网直接供电。

这款 AP 产品外置 4 根天线，2 根提供 5GHz，2 根提供 2.4GHZ，可布置于大会议室和走廊等空间开阔面积大，或需要定向提供信号的区域。还有内置天线的版本 FortiAP-221B，这里就不赘述了。

图 2 右上角的图，可以看到 AP 背面有两个接口，一个是 RJ45 以太网接口，还标示出了 POE 48V，说明这个设备是可以通过 POE 供电的，只需将网线连接到远端的 POE 交换机或其他 poe 供电设备，就可以直接使用了。图 2 右上角的图还有一个小的接口，是电源插口，当没有 POE 供电设备的情况下，就需要在 AP 边上放置一个电源来供电了。当然，由于我们使用的 FortiGate-90D-poe 本身提供 4 个 PoE 接口，因此我们省去了 POE 交换机等 poe 供电设备和电源，简化了网络拓扑。

图 2 左下角和右下角就是 AP 与 FortiGate 互联的情况。

无线管理与配置

我们先过一下配置的思路：

- FortiAP 连接 internal 接口之后自动获得 ip 地址：192.168.1.xxx/24
- 在 FortiGate 中创建 SSID
- FortiGate 自动发现 FortiAP，将 FortiAP 添加到 FortiGate
- 将 SSID 和 FortiAP 关联
- 创建防火墙策略

下面我们就来一起看看在 FortiGate 中该如何配置。

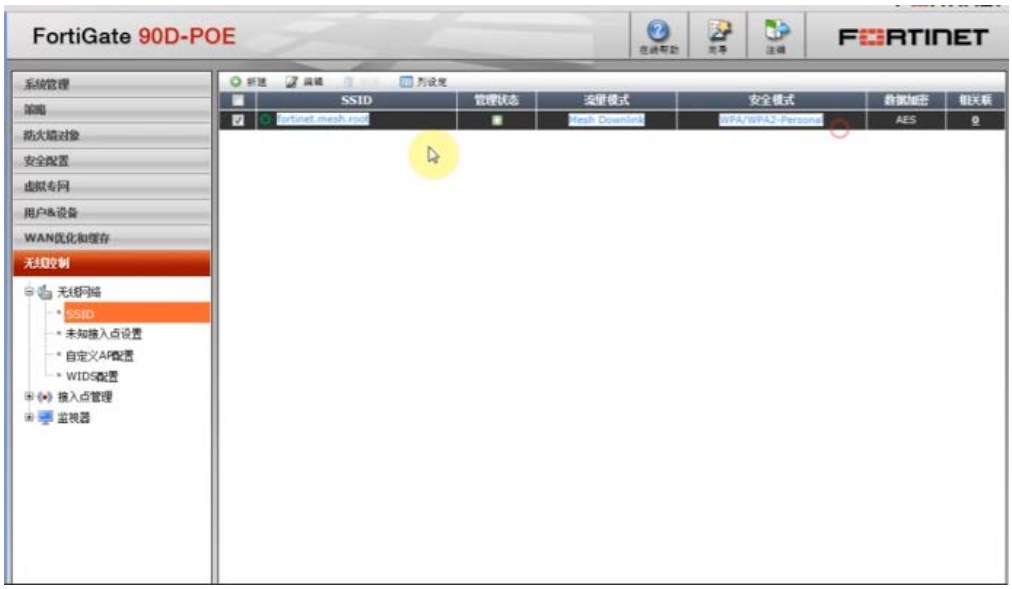

图 3：无线控制界面

在上一篇《产品安装及快速配置》中我们已经讲过该如何进行初始配置，以及语言调整等等，我们这里就不再讲了。在系统主界面中点击无线控制，选择 SSID，我们可以看到已经默认存在一个 SSID 了，但是这个是用于多个 AP 之间做 mesh 的，也就是多个 ap 之间做桥接互联用的。我们现在需要新建一个 SSID。

图 4：新建 SSID 配置界面

我们新建无线的接口为 fortinet-ap，类型为 WiFi SSID，流量模式为通过隧道模式连接，再创建一个 IP 地址和掩码（192.168.2.1/24），同时开启一些访问协议。然后启用 DHCP，可以让 AP 自动为连接上的设备分配 IP 地址。

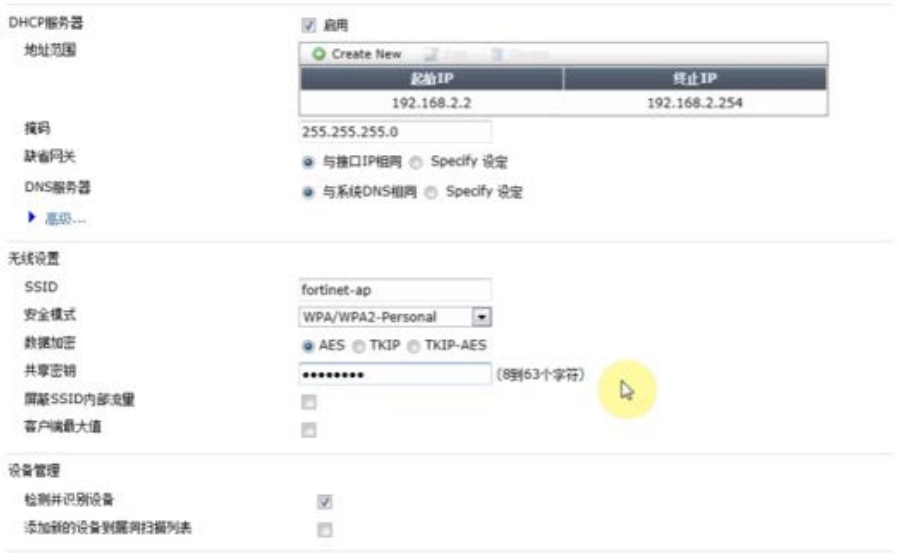

图 5：新建 SSID 配置界面

无线 SSID 我们也设为了 fortinet-ap，安全模式选择默认的 WPA/WPA2-personal，加密方式默认为 AES，再输入密钥，这样一个 SSID 的配置就完成了，点击最下方的确定。

图 6：新 SSID 创建成功

如图 6 所示，我们之前配置的名为 fortinet-ap 的 SSID 已经出现在 SSID 的列表中了。接下来我们需要点击接入点管理，来看看 FortiGate 设备发现了那些 FortiAP。

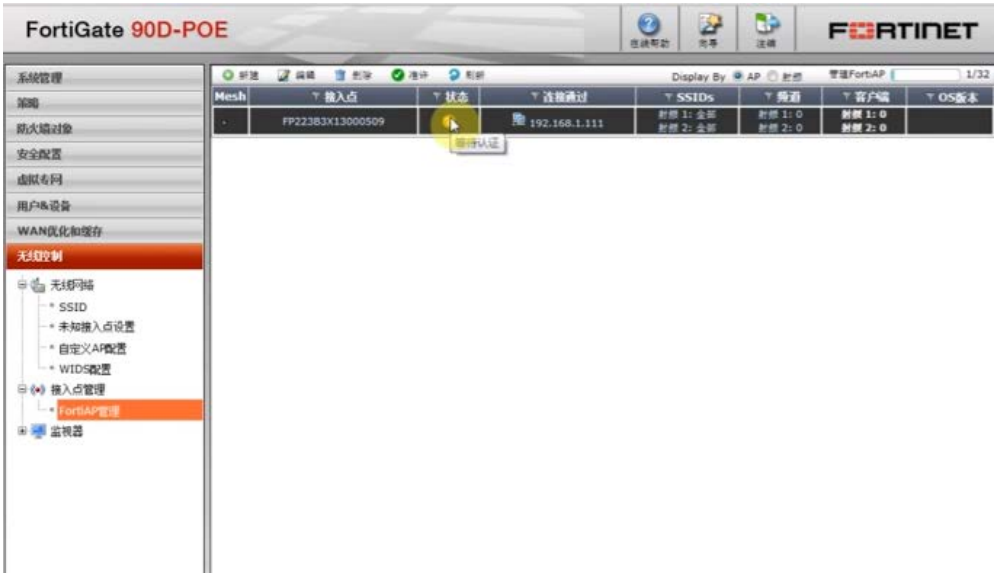

图 7：发现 FortiAP

我们在接入点管理中的 FortiAP 管理中看到，FortiGate 已经发现了我们接入的这台 FortiAP-223B，但是设备状态为黄色的问号，我们将鼠标移到该图标上，发现状态为等待认证，可以看出，虽然该 AP 是直连到设备上的，但是我们仍然在只是识别出，并没有直接让其接入，也就是说这时这台 AP 还不能上外网和广播无线信号，这是为了更安全的考虑，管理员需要手动允许该 AP 加入，我们才能使用这个 AP。

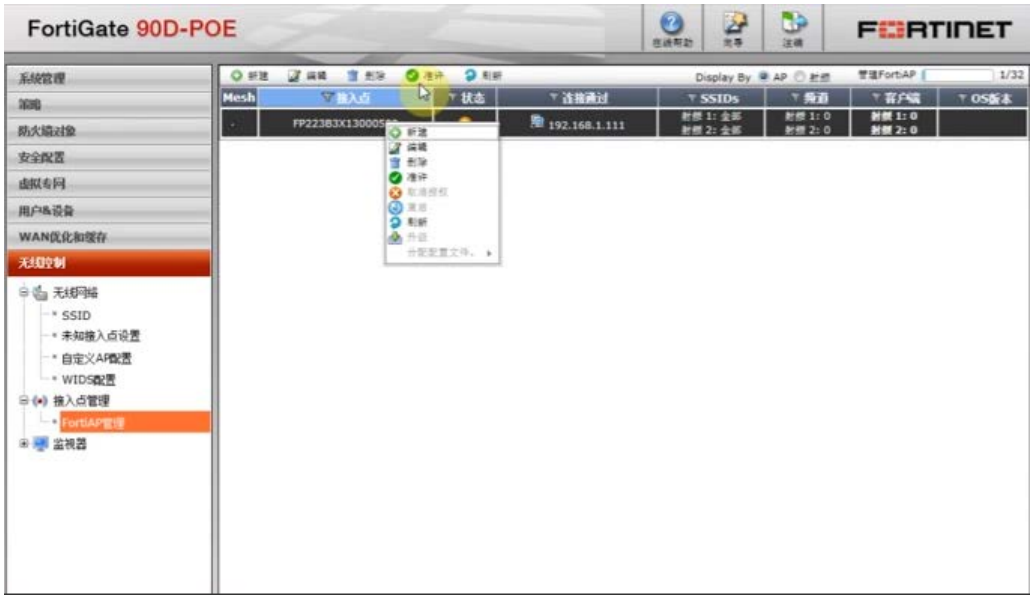

图 8：允许 FortiAP 接入

如图 8 所示，我们可以右击 AP 的序列号，来选择准许，或者在菜单栏中选择准许。

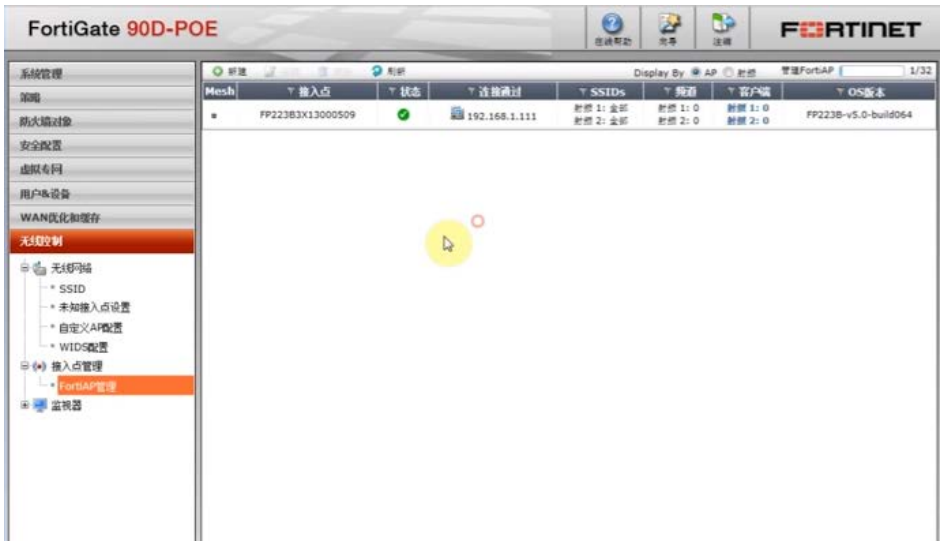

图 9：成功注册界面

如图 9，FortiAP-223B 已经成功注册到 FortiGate 上了，通过 192.168.1.111 的 IP 连接到 FortiGate。包括设备版本，频道，SSID 信息等都能看到。

图 10：AP 管理界面与升级信息

在列表中，我们右击该 AP，选择编辑，就来到了接入点管理界面，可以看到更多细节的信息，其中可以直接在界面中对 AP 进行版本升级，从本地导入升级文件，如图 10 所示。

图 11：SSID 自动继承

启用无线射频的时候，SSID 会默认选择自动继承所有 SSID，也就是说，默认情况下，创建一个 SSID，准许了某一个 FortiAP，该 AP 会自动广播这个 SSID。

防火墙策略配置

在无线管理页面允许了 FortiAP 接入，并且创建好了 SSID 之后，我们就需要创建防火墙策略了。

图 12：无线接口信息

如图 12，在系统管理-网络-接口中我们可以看到，多了一个 fortinet-ap 这样一个接口(SSID 名称为 fortinet-ap)，类型为 WiFi，与我们之前配置的一样。

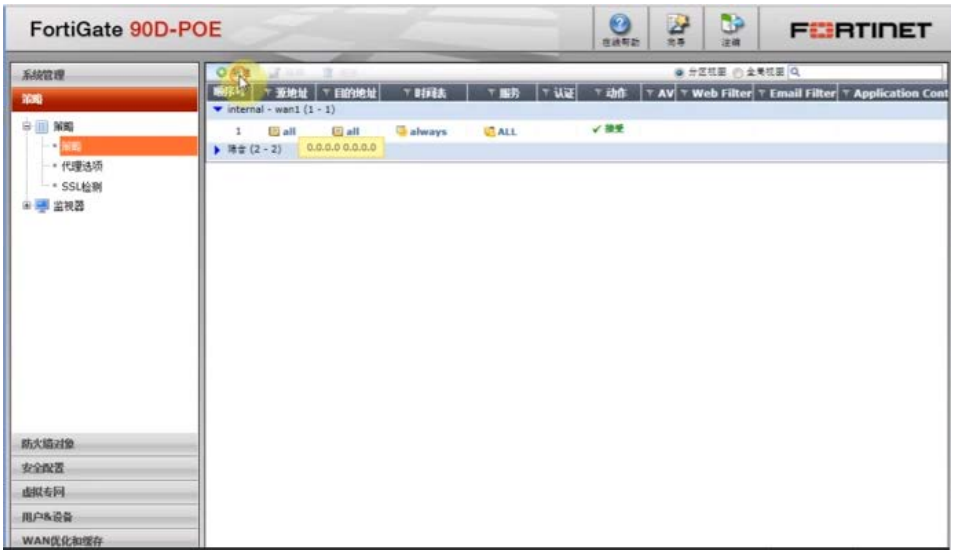

图 13：新建策略

在图 13 中，策略-策略-策略中，我们新建一条策略。

图 14：新建策略示意

图 14 中我们可以看到，策略类型选择防火墙，子类型选择地址，流入接口就是我们 AP 的 fortinet-ap 接口，源地址为 all，流出接口为 wan1，目的地址为 all，时间表选择 always，服务也是 all，动作为允许，这里我们要启用 NAT，进行地址转换。其余的安全配置我们暂不启用。直接点击确定。这样我们针对 ap 这个接口的策略就做完了。

完成了上述步骤，我们的 pc 和手机等设备就可以通过该 AP 访问 internet 了。

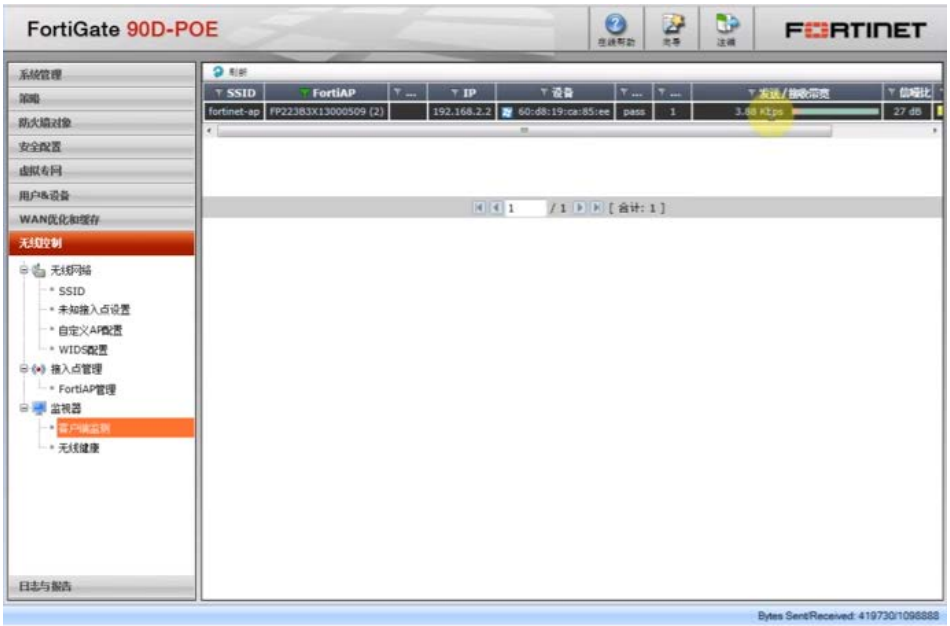

图 15：设备识别

如图 15，在无线控制-监视器-客户端监测，可以看到已经识别出了我们连接的设备，通过哪个 SSID，哪台 AP，IP 地址是多少，设备 MAC 地址和系统，占用带宽，信号强度等等。

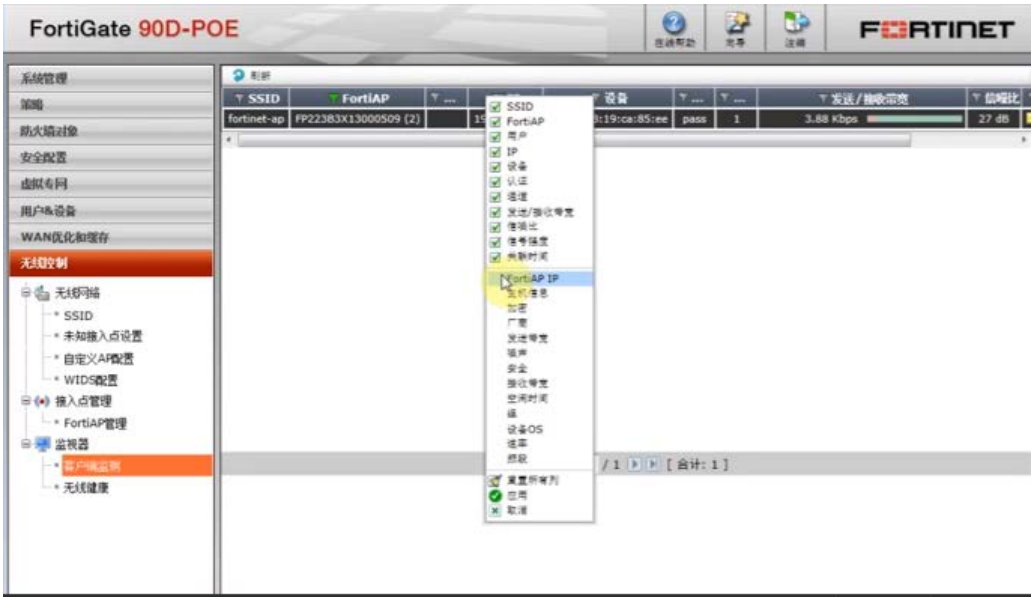

图 16：菜单添加与移除

如图 16，我们可以看到有多种不同等的菜单选项，可以选择添加和移除菜单项，来控制自己想在菜单栏中看到的内容。

图 17：无线健康状态

我们可以看到 24 小时之内 AP 重启的次数，接入用户的数量，每 AP 客户数量排名，无线接口排名等等。

除此之外，我们还可以对非法 AP 进行检测，也就是无线控制-无线网络-未知接入点设置的功能

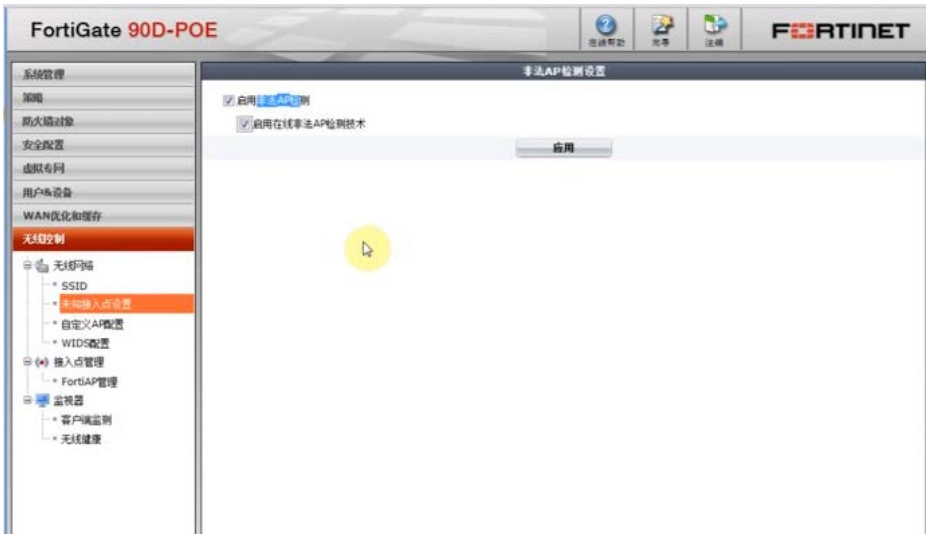

图 18：非法 AP 检测

在未知接入点设置中我们可以启用非法 AP 检测，启用在线非法 AP 检测技术。点击应用之后，这个功能就启用了，在无线控制-监视器中就会增加一个未知接入点检测的项。

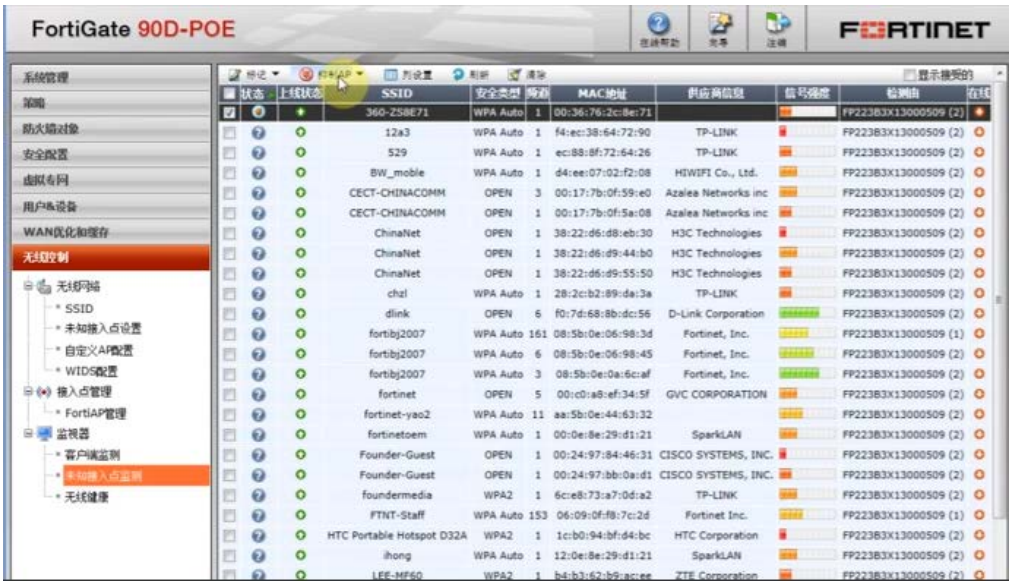

图 19：标记与抑制非法 AP

如图 19 所示，在未知接入点监测中，我们看到了很多识别出的无线接入点。我们认为其中某个是非法 AP，可以右击标记为非法 AP，然后状态就会如图所示产生变更，在图 19 中我们第一个高亮出的 AP 就是被标记为非法 AP 的，可以点击菜单栏中的抑制 AP，连接在 FortiGate 上的 AP 就会发出抑制信号，禁止选定的 SSID 向外广播信号。这个功能通常是为了禁止员工在内网私接 AP，以防私接 AP 对内网正常的无线网络造成影响，而且也可以防止用户接入到伪造 SSID 的 AP，从而造成数据泄露的情况。

到此为止，我们介绍完了通过 FortiGate 和 FortiAP 快速打造无线网络。接下来我们还会介绍通过 FortiGate 进行上网行为管理和 VPN 搭建等等众多功能。