深信服企业、政府非法 wifi 热点管控方案

应用背景

随着企业和政务信息化建设的发展，网络在给企业、政府办公工作带来巨大便利的同时，也带来了潜在的安全隐患。企业、政府部门的内部网络中有很多涉及机密的资料，一旦通过网络泄露出去，形成安全事件，造成的损失将无法估量。

问题分析

企业、政府内网管理严密，出于对信息安全的考虑，内网中往往禁止布设无线网络。

➢ 私接 Wi-Fi 给内网带来巨大隐患

部分办公人员为了一己之便，私接无线 Wi-Fi 共享设备，让自己的手机、平板电脑也能够访问互联网络。私接了无线 Wi-Fi 共享设备，相当于将内部网络公开暴露在外，无线网络的开放性为不法分子利用黑客渗透技术入侵到内网中提供便利，一旦被不法分子入侵，后果不堪设想：破坏网络致使网络瘫痪、盗取或删除资料、种植木马长期隐藏等等。

➢ 新兴廉价 Wi-Fi 工具降低私接 Wi-Fi 难度和成本

市面上推出的 360Wi-Fi、小米 Wi-Fi 和小度 Wi-Fi 等随身 Wi-Fi 工具，凭借其价格便宜而且方便使用的优势，迅速普及到用户手中，同时也催化了网络中私接无线 Wi-Fi 共享设备的安全隐患。

➢ 蹭网卡的流行使违规违纪行为难以发现和追溯

当前火爆的蹭网卡，通过软件破解技术直接破解其他合法设备的无线网卡密码，以其他人的身份接入网络，这种方式以其隐僻、难追溯等特点一度成为内网安全的巨大黑洞。

深信服非法 WiFi 热点管控方案

深信服提供非法无线热点管控方案：

发现私接 Wi-Fi 热点

当办公人员私接随身 Wi-Fi 或路由器等工具将内部网络共享给其他 PC、笔记本或移动终端时，深信服

提示并封堵非法终端

在发现到私接移动终端同时，将立即封堵该办公人员的上网权限并弹出告警页面，提示该用户私接网络共享工具为违规行为，从而促使用户停止使用共享工具，减少安全事故发生几率。

提供白名单信任列表

对合法用户，直接加入信任列表，不做检测和封堵。保证合法用户的用户体验。避免对合法用户封堵造成合法用户的投诉。

方案价值

提高内网安全性

通过深信服非法 wifi 热点管控方案，有效并迅速发现企业、政府内网中的私接 Wi-Fi 工具行为，通过其告警功能，使管理员能够及时响应事件禁止该行为，减少内网的私接 Wi-Fi 工具行为，防止内部网络被公开暴露，规避了内网受攻击、机密遭窃取等安全隐患，提高网络安全性。

上网查资料打不开网页等等。深信服非法 wifi 管控方案直接封堵私接终端，保障带宽不被移动终端侵蚀，从而保障核心业务正常运行和提高用户体验，同时还能保障员工注意力不被移动终端分散，提高员工办公效率。

案例分享

上海海关　南京海关

上海海关和南京海关通过部署深信服“内网私接 Wi-Fi 热点管控方案”，有效的杜绝了在办公网中私接非法 Wi-Fi 设备的行为，消除了办公网的安全隐患，为海关打造了一个健康、安全的办公网。

“深信服内网私接 Wi-Fi 热点管控方案”既可以像上海海关那样以路由模式部署在网络出口，开启 DHCP 和 NAT 功能，也可以像南京海关那样以透明网桥模式部署在内网汇聚层，最大限度减小对现网的改动。