安全无线防御系统

产品白皮书

目录

一. 概述

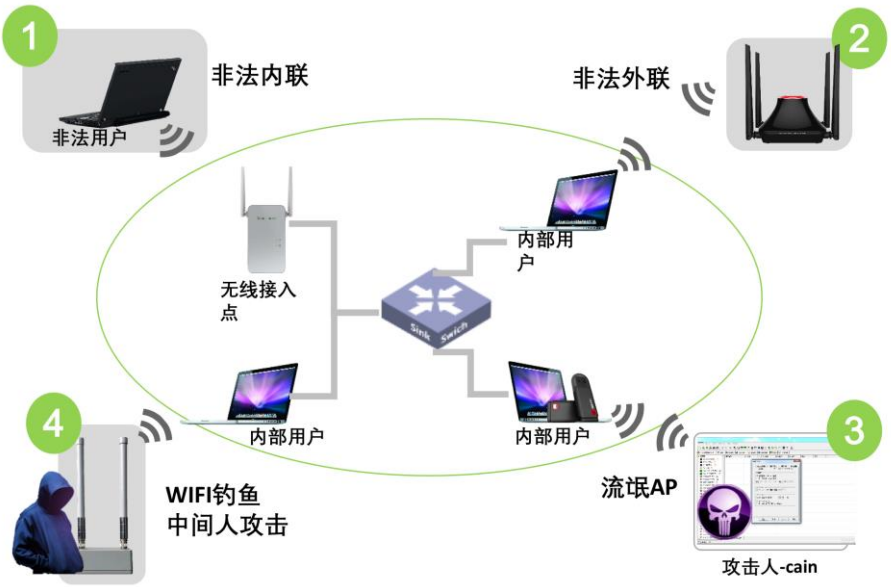
移动化，已经支撑起企业运行的方方面面，关键业务从有线网络转移到无线网络，不但赢得了时间、还数倍提升了运转效率。然而，在 WLAN 正逐渐成为 IT 系统主要基础架构的同时，WLAN 的安全风险却正与日俱增，人们对 WLAN 网络安全担忧加剧，目前在欧美等国家，已出台 WLAN 安全相关法规和技术管理办法，一些重要场合正考虑或已开始部署 WLAN 的安全防护产品，或定期进行 WLAN 安全检查。在我国，WLAN 对应的相关安全防护法律、法规也正在和相关技术和产品也已经开始起步。

如何有效面对已建设完成、或正在兴建的大量 WLAN 网络进行安全防护，是每一个安全厂商和 WLAN 设备供应商，都必须要面对的问题。针对这种现状，绿盟科技推出了业界领先的无线入侵防御系统(WIPS)，通过智能化无线安全引擎，为 WLAN 系统提供可靠、持续的环境监测，对非法无线攻击行为实施有效检测，对危害性高、具备流行趋势的无线安全事件进行智能化反制，最终实现 WLAN 系统的全面安全保障。

二. 发展史

2.1 无线对传统安全的挑战

有线网络安全设备主要部署在网络出口，防范来自互联网的安全威胁，由于网络位置及防护技术的限制， 在应对 WLAN 无线安全威胁时往往力不从心。而防火墙只能在有线网络层面阻止非法无线客户端，无法阻止无线客户端通过射频信号接入 AP，而一旦非法无线客户端接入 AP，相当于进入企业内网，信息泄露的大门已经打开。以下是最具攻击性，并且风险最高的无线安全事件：



传统安全方案，流氓 AP(例如员工私自接入有线网络的 AP)的接入，只能通过有线交换机的端口控制，但最新流行 USB 随身 wifi，让无法实现终端端口控制的场景的网络边缘安全被人为撕裂了一个更大的缺口，造成内网数据安全无法得到保障，对于无线扫描、无线欺骗、无线破解、无线 DoS 等攻击更是鞭长莫及，无法防护。

用户不了解射频开放空间中的无线网络状况，谁在使用无线网络？有没有非法无线客户端接入？是否存在无线网络攻击？传统有线安全手段是无法解决的。

2.2 为什么需要无线安全

Gartner 数据显示，在众多网络安全威胁中，WLAN 面临最高的安全风险等级，安全形势已迫在眉睫。

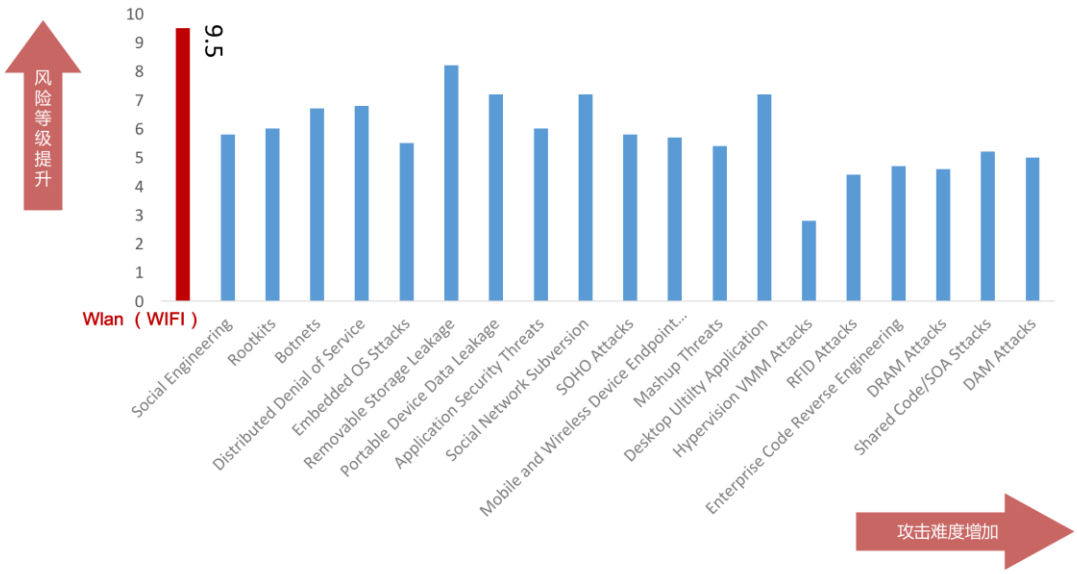


图1. 传统安全面临的挑战

- 流氓 AP
- Ad Hoc 连接
- 无线 DOS 攻击
- 无线破解
- 无线中间人攻击
- 无线钓鱼
- 无线扫描与探测
- Windows 共享 wifi 无线风险... ...

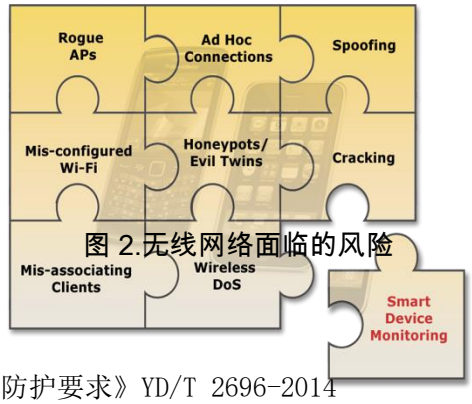


图 2.无线网络面临的风险

合规性要求：

1、中国法规：

- 《公众无线局域网网络安全防护要求》YD/T 2696-2014
- 《公众无线局域网网络安全防护检测要求》YD/T 2697-2014
- 《铁路站(场)局域网无线安全接入暂行技术要求》TJ/XX001-2014

2、美国法规：

- DISA(美国数据交换标准协会)要求美国国防部网络，无论是否部署了 WLAN 设备，必须部署 WIDS/WIPS 设备，7×24 小时不间断监测网络。
- PCI DSS（支付卡行业与数据安全标准）要求每季度对所有支付卡场所进行一次无线扫描，无论该场所是否部署了无线设备。

2.3 无线安全常见误区

用户	误区	真相
未部署 Wi-Fi 办公环境	与我们没有关系：“我们没有部署 Wi-Fi 网络，因此不会面对 Wi-Fi 安全问题”	Wi-Fi 使数据泄露无处不在： ● 流氓 AP：各种随身 Wi-Fi ● 员工私自架设的 AP、软 AP ● 针对员工的无线钓鱼 ● 员工非法无线外连 … ...
已部署 Wi-Fi 办公环境	我们的 Wi-Fi 足够安全：“我们部署了加密、FW、IDS、AV，因此我们的 Wi-Fi 网络已经处于保护之中”	Wi-Fi 边界缺少防护： ● Wi-Fi 共享软件 ● 流氓 AP、钓鱼 AP ● 用户连接外部 AP ● Ad Hoc/Wi-Fi Direct ● 无线 DoS 攻击 … …
员工移动设备	我安装了× × ×卫士 “我的手机安装了×××安全软件，无线安全有保证”	无法甄别真/伪 Wi-Fi： ● 无线钓鱼攻击 ● 无线中间人攻击 ● 无线窃听/嗅探 ● 丢失的智能终端 ● 恶意软件 … ...

2.4 WLAN 安全关键问题

- 防火墙、UTM 等有线安全设备是否能防护 WLAN 网络，阻止 WLAN 网络攻击？
- 对于没有部署 WLAN 的网络，如何确定真的没有人使用无线？
- 对于部署了 WLAN 的网络，管理员能否清晰的了解无线网络状态和面临的威胁（Who、When、Where、How）？
- 当员工大量使用无线智能终端时，如何确定企业数据没有泄露的风险？
- 如果企业不允许上外网，如何确定员工没有通过隔壁的 WLAN 网络或无线热点连接外网？

针对不断上升的 WLAN 风险，安全和无线厂商也在不断推出相应的解决方案，先后推出物理层干扰、链路层防护、网络层加密、应用层发现等无线安全解决方法，在多种安全方案中，无线入侵防御（wIPS）逐渐成为被认可的主流 WLAN 安全解决方案。

三. 体系架构

3.1 系统构成

无线入侵防御系统主要由两部分组成：无线入侵防御、无线安全引擎

无线入侵防御：针对无线扫描、无线欺骗、无线 DoS、无线破解等无线网络威胁，提供实时、精确、可靠、有效、持续的无线安全监测和防御能力。

无线安全引擎：是无线安全产品海量信息处理中心。完成无线安全事件的存储、分析、审计和处理功能。

3.2 软件结构

绿盟科技无线入侵防御系统涵盖：无线入侵检测、无线攻击防御、及无线安全态势评估，本着安全、高效原则将各层功能模块化设计，整个过程数据信息由系统统一监控、配置和调整。

3.3 管理结构

无线入侵防御系统提供灵活丰富的管理，支持分布式的瘦架构 wIPS 探针部署和强大的安全管理、分析中心，系统由 Web 进行统一管理、集中信息采集和发送、功能配置；而无线安全引擎则高效分析无线安全事件，并将其分类、统计、挖掘，将无线安全态势展示给用户。

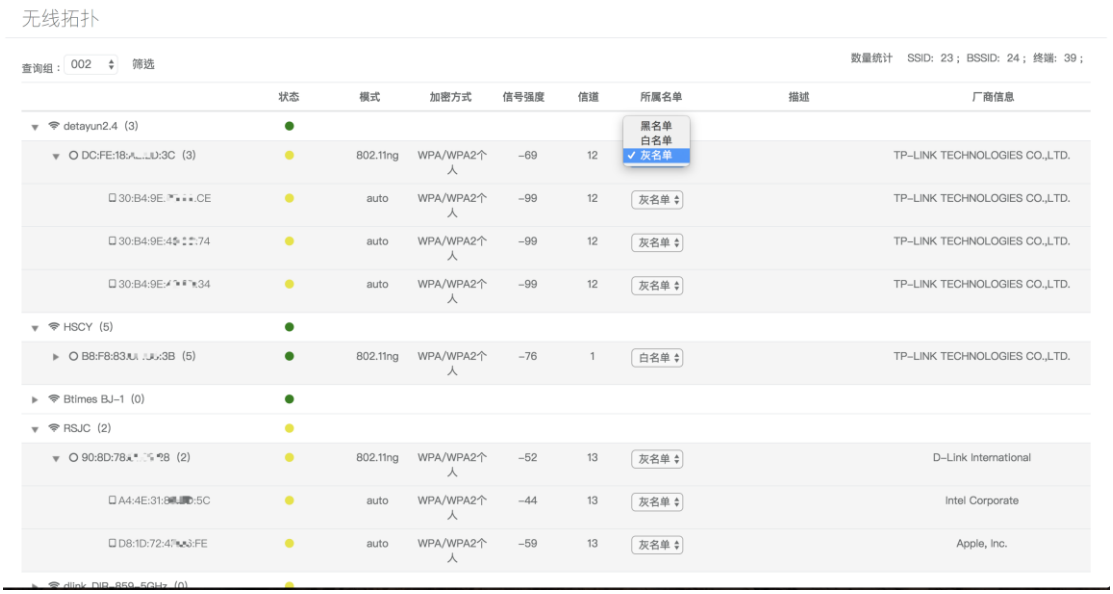
四. 关键技术

无线入侵防御系统采用了创新技术，将有线安全和无线安全有效的融合，为用户提供更可靠的无线安全保障。

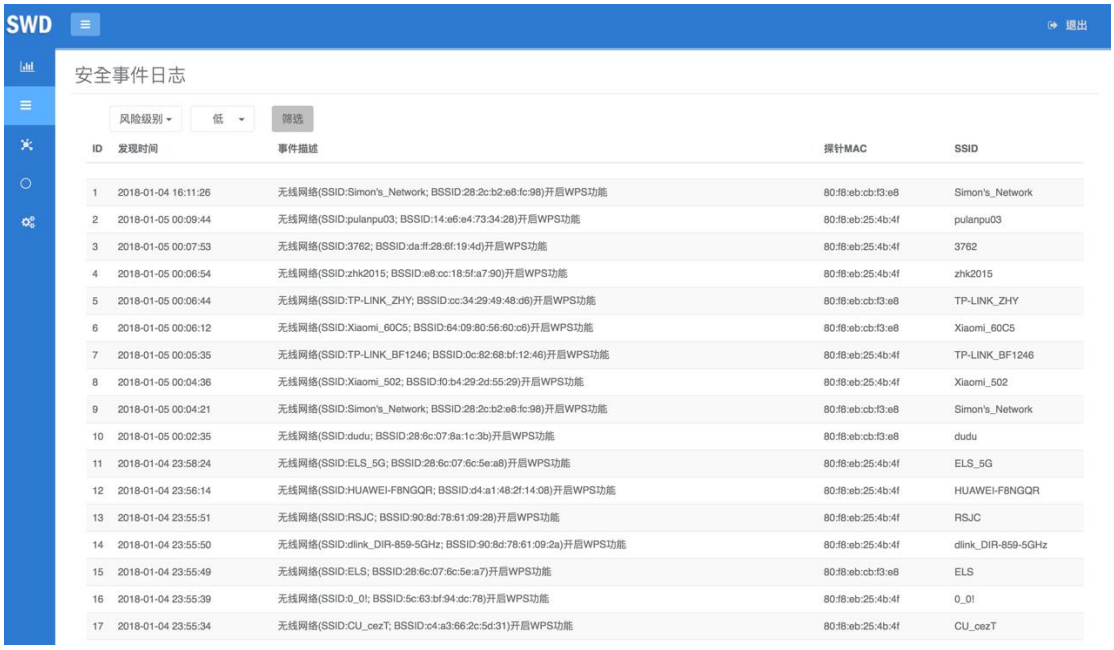
4.1 自动学习无线拓扑

对于传统有线网络而言，网络管理员在规划网络时，将具体的网络设备、用户终端与指定的物理端口进行对应，就可方便的进行管理。而对于无线网络而言，由于终端的“无线”、“便携”特性，使得网络管理员很难将无线用户对应到具体的物理位置，即使是了解无线网络运行的状态，也是一项棘手的任务。

绿盟科技无线入侵防御系统可自动学习无线网络，并将其网络状态、无线设备属性、无线拓扑等内容展示给用户，为用户提供直观的无线分析、管理方法。系统通过侦听模式，尽可能学习更多无线设备，并对无线设备的属性进行详细统计，如下图所示：



通过持续监测无线环境，无线入侵防御系统就能实现对拓扑信息进行分类统计，将运行状态展现给用户，帮助用户进行智能分析，及时发现存在的安全隐患。



4.2 高效的无线攻击检测

传统的有线网络攻击主要位于网络层之上，因此 IPS/IDS 等安全设备通常在网络层报文中深度查找攻击的特征，并将这些特征相互关联，从而定位对应的网络攻击。

在无线网络中，由于其链路层协议的脆弱性尤为突出，所以目前已知的攻击方式中，大多数都是针对无线链路层协议进行的，也有一部分攻击是针对无线网络架构本身的，因此，无线攻击的识别技术也需要根据攻击的特点而变化，这一点与传统有线网络攻击检测是有区别的。

绿盟科技无线入侵防御系统内置高效无线安全引擎，针对无线链路层攻击特征具备智能的识别能力，同时，面对无线网络架构的组合攻击，无线安全引擎通过一体化关联分析技术，以及高精度协议分析和自适应匹配算法实现攻击行为的有效识别，确保无线攻击被有效监测。

4.3 基于射频的精确反制

在无线网络环境，绿盟科技无线入侵防御系统采用自主研发的基于无线链路层的阻断技术，满足用户精准识别、可靠阻断的要求。

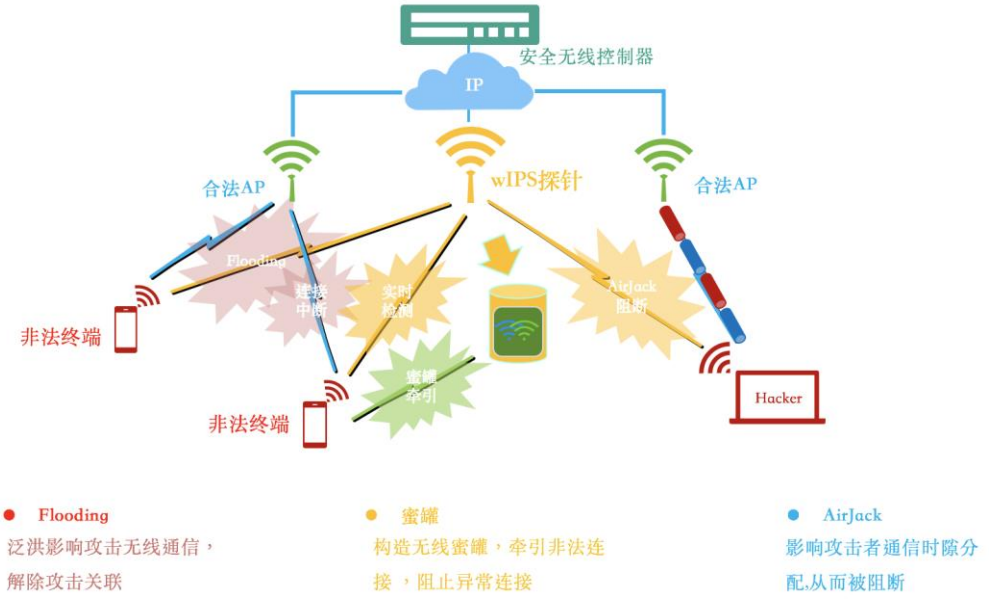


图2. 无线攻击精确防御

射频阻断通常有两种方式，一种是射频干扰，通过长时间、大功率发送所在频段的干扰信号，来干扰无线设备的接收。但信号干扰的干扰效果与干扰器信号场强成正比，反之，则达不到理想效果，而且干扰器在对攻击设备发起干扰的同时，也会对合法的无线设备通信造成干扰，甚至通信中断。

因此绿盟科技无线入侵防御系统采用了更先进攻击反制方式：采用无线报文干扰攻击设备，使其攻击行为受到压制甚至被阻断。因为采用与干扰器不同的工

作方式，精确阻断设备可以用更低的发射功率来抑制无线设备的发射，从而达到与干扰器相同的工作效果，例如，阻断同等面积区域内的无线设备，精确阻断设备的发射功率只需干扰器的一半或更低，某些情况下，甚至只有干扰器发射功率的十分之一。

另一方面，当无线入侵防御系统工作的区域内，没有出现攻击行为时，设备将处于监听状态，对外不发射任何射频信号，一旦攻击行为出现并被有效检测，设备即开始针对性的反制动作。此外，精确阻断不会对其他无线设备的工作造成任何的不良影响，甚至在同一无线 AP 下的非法终端被反制，也不会对合法接入的无线终端造成影响。并且策略支持用户自定义或自动策略下发。这种智能的攻击反制方式，是传统射频干扰器望尘莫及的。

目前，绿盟科技无线入侵防御系统的攻击反制手段包括：针对无线设备、针对无线关联关系实施防御策略；在技术手段上，采用了泛洪反制、AirJack 反制 、FakeAP 反制等；无线入侵防御系统能够自动、灵活、动态下发的反制策略，实现可靠的攻击反制效果。

五. 产品综述

5.1 无线安全防御体系

- 无线环境监测：有效发现无线环境内运行的无线设备及其相互间的关联关系；
- 无线入侵防御：有效检测无线扫描、欺骗、DoS、破解等 8 大类超过 100 种无线攻击行为，同时对攻击行为实施自动或手动的反制，有效防止内网信息通过无线网络向外泄露；
- 丰富的报表统计，提供实时无线网络拓扑、实时无线安全事件风险展示等丰富的统计信息，让无线安全态势一目了然。

5.2 丰富特性

- 兼容并防护所有类型无线设备和网络；
- 支持旁路接入；
- 智能而完善的无线安全策略；
- 支持自定义 WLAN 资产属性，并匹配无线安全策略；
- wIPS 可靠有效的链路层反制能力，让无线攻击设备无法接入合法无线网络；

- 智能黑名单，让攻击者无法二次入侵；

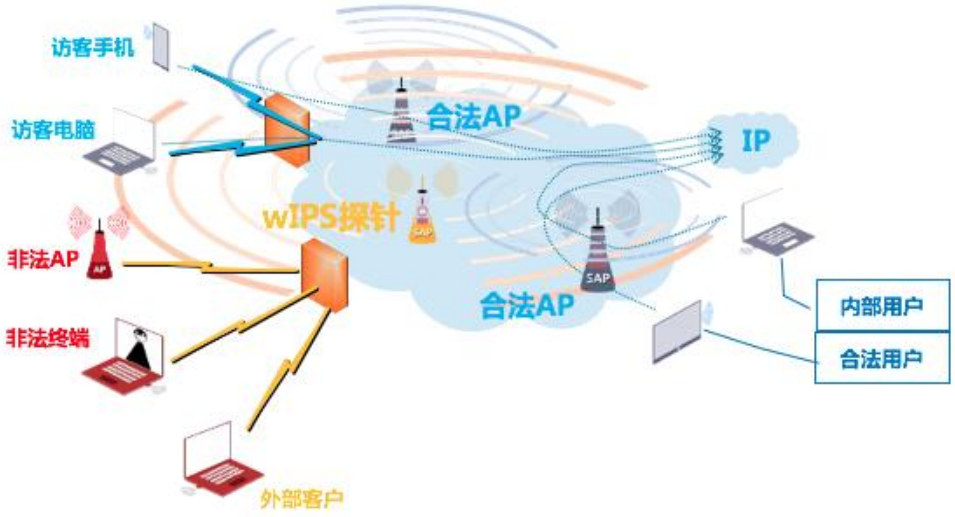


图3. wIPS 实时检测

5.3 产品覆盖方式

无线入侵防御系统支持 2.4GHz/5GHz 双频、室内外均可采用全向天线进行实时 wIPS 监测。其无线电覆盖的模型如下图，以 WIPS 为圆心，呈铁饼形状，因此应该将 WIPS 部署在需防护区域的中心位置，将会取得较好的效果。

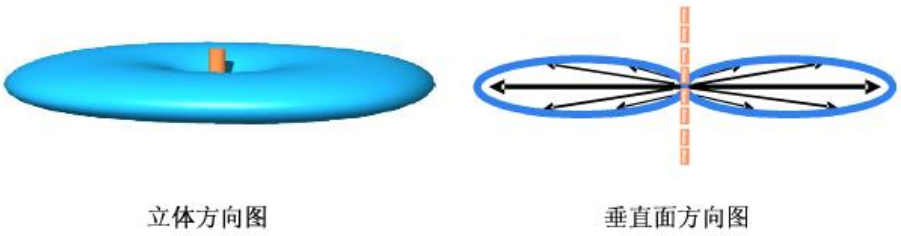


图4. WIPS 无线覆盖模型