DCYKOS RFPROTECT 模块

DCYKOS RFProtect™ 模块是可选的软件模块，安装在 DCYK 移动控制器中。RFProtect 可以保护网络基础设施免受无线安全威胁，并提供了针对射频 (RF) 干扰的关键层监控能力，分析对无线 LAN (WLAN) 性能的影响。

RFProtect 提供了业界独有的集成无线安全性以及频谱分析系统，适用于企业 WLAN。DCYK 的 WLAN 基础结构使得接入点 (AP) 在为 WLAN 客户端提供服务的同时，可以监控无线中的干扰源和恶意设备。DCYK AP 还可以转为专用的无线监视器，专门用于检测未经授权的 AP 和设备并进行隔离。

此外，**神州云科** AP 可以配置为频谱分析器，用于远程扫描 2.4GHz 和 5 GHz 频段，确定 RF 干扰，区分来源并提供实时分析。通过 RFProtect，进行频谱分析无需专用的硬件或客户端软件，因而无需使用专门的 RF 传感器网络和安全设备。

通过与 RFProtect 联合使用，DCYK 的 AirWave 提供了事件历史记录、事件关联、频谱可见性、位置跟踪和安全报告功能，用于满足法规遵从要求，例如支付卡行业 (PCI) 的规定。

频谱分析

WLAN 中的 RF 干扰无可避免也无从预测。临近的 Wi-Fi 网络或非 Wi-Fi 源都可能造成干扰，例如 2.4 GHz 无绳电话、微波炉、模拟摄像机、游戏机和无线遥测系统。RF 干扰的性质和严重性根据设备的类型和位置不同而不同，可能会对客户端接入以及 WLAN 的性能造成影响。

神州云科 AP 利用集成了高分辨率频谱分析功能的 Wi-Fi 芯片组，实现了始终在线的同步频谱分析、客户端服务和无线安全监视。通过同步扫描 RF 频谱中的干扰和入侵检测保护功能，无需使用专门的硬件和安装有客户端软件的手持分析器，从而降低了成本和复杂性。因此，DCYK 解决方案的成本仅为其他产品的一半，并减少了 IT 员工手动采集 RF 干扰事件所需的时间。

基础控制器操作系统中包含的 DCYK 自适应射频管理 (ARM) 功能使得 DCYK AP 可以避免干扰。DCYKOS RFProtect 模块包含频谱分析功能，可以确定干扰源并将其归类到多达 13 个类别中，从而提升了 ARM 的功能， 然后，通过 12 个图表向管理员提供干扰分析，包括 FFT 和频谱图。

无线入侵防护

对于拒绝服务 (DoS) 和中间人攻击而言，无线网络是很有吸引力的目标。带有 RFProtect 的 DCYK 移动控制器可以维护签名，用于识别和阻止无线攻击，以免中断服务。DCYK 接入点可基于位置签名和客户端分类，删除非法请求并生成警报，用于向管理员通知攻击。

DCYK AP 监视无线以检测其他无线站点冒充有效 AP 的情况。RFProtect 跟踪网络中每个无线客户端的独特签名。如果新引入的站点宣称自身是特定客户端，但缺少正确的签名，这就检测到了站点模拟或中间人攻击。检测到中间人或无效/仿冒 AP 时，将实施防御机制以隔离未授权的设备，防止机密数据损化或丢失。

分类并禁用恶意接入点

对于保护公司环境免受未经授权的无线接入而言，分类是第一步。采取适当的措施以快速阻止入侵，对于保护敏感信息和网络资源至关重要。必须对 AP 和站点进行准确分类以确定这是有效、恶意还是临近的 AP，并且必须实施自动响应以防止可能出现的入侵尝试。

使用 RFProtect，**神州云科** AP 支持 TotalWatch™ - 这是一种扫描 RF 频谱所有信道的功能，包括 2.4 GHz、5 GHz 和 4.9 GHz 公共安全频段。TotalWatch 还能在频段中进行 5 MHz 的细粒度信道扫描用于检测恶意设备，并能动态扫描停留时间以重点关注有流量的信道。TotalWatch 提供了一组先进的功能，用于检测未经授权的无线设备， 并有一组可自定义的规则，用于重点区分确实对网络造成了威胁的设备。

检测到分类为恶意的设备可以使用无线和有线手段进行隔离。无线设备阻止提供了有效的方法，可以隔离无线恶意设备而不会影响临近设备。此阻止方法相比通过重复取消授权请求进行恶意设备隔离要更为高效。网络管理员将收到恶意设备通知，并可通过使用AirWave来确定恶意设备的物理位置。
RFProtect 可以阻止无线流量通过恶意 AP 转发到有线基础设施，这样就阻止了无线网络入侵威胁到有线网络。

策略定义和实施

RFProtect 可以配置并动态实施网络策略。无线策略的例子包括有效站点防护、AP 错误配置保护、临时网络检测和保护、未经授权的网络接口卡 (NIC) 检测以及无线桥接检测。RFProtect 提供有策略配置向导，简化了组织创建无线安全策略的过程。

RFPROTECT 功能频谱分析器

- 同步的 RF 频谱分析、客户端服务和安全扫描
- 集成到 神州云科 AP 中
- 可像控制器上的 AP 一样扩展（最多为 M3 上的 1024 个 RAP 监视器）
- 扫描 2.4 GHz 和 5 GHz 频段
- 将干扰分为最多 13 个类别，包括：
  - 蓝牙设备
  - 无绳电话、网络和基站设备
  - 固定频率视频和音频设备
  - 微波
- 通过 12 个频谱分析图表提供直观指示，包括：
  - FFT 占空因数
  - 实时 FFT
  - 扫谱图
- 与 DCYK AirWave 集成，可以显示和汇总显示干扰分类，位置及 RF 信息

模拟检测和防护*

- 热点攻击检测
- MAC 地址欺诈

TOTALWATCH 无线监视

- 基于规则的自动分类
- 通过阻止设备阻止无线接入
- 通过 AirWave 进行位置跟踪
- AP 模拟
- 中间人攻击
- 序号异常检测

客户端入侵防护*

- 蜜罐 AP 防护
- 有效站点防护

拒绝服务攻击检测*

- 自动免疫攻击、节能攻击、管理帧泛洪、取消验证攻击、验证泛洪、探测请求泛洪
- 虚假 AP 泛洪
- 空探测响应
- EAP 握手泛洪

探测和网络发现*

- 检测 NetStumbler 和广播探测网络入侵检测

*

- 无线桥接
- ASLEAP 攻击

神州云科 Yunke China
北京市海淀区上地九街9号数码科技广场
吴寄遥: +86.13693208636I wujyj@digitalchina.com
汪要娣: +86.18721819116I wangydw@digitalchina.com