NETGEAR®
Connect with Innovation™

白皮书

确保无线网络安全的五个步骤

现今的公司逐渐依赖于无线网络的移动性和低成本。K-12学校和中小企业纷纷投资Wi-Fi以利用其带来的各种好处，包括灵活的网络连接、提高生产效率和降低成本费用。

随着无线局域网（WLAN）成为运营的标准，相关的技术正变得更安全、快速以及容易部署和管理。正确地部署，无线网络可以提供与有线网络相当或更高的安全性。通过基于多层保护的高级技术，政府和企业正在将机密和业务关键的应用运行在WLAN上。

确保无线网络安全

无线局域网包括无线客户端（如台式机、笔记本电脑、智能电话、掌上设备和销售站点）、无线接入点（AP）、集中无线管理和监测系统以及无线网络接入的有线局域网。为了建立一个无线网络，至少必须安装一个无线接入点。

尽管许多因素不仅影响到AP的信号强度，而且影响到每个接入点可以同时管理的客户端数量，但是大多数的无线接入点仍可以在150英尺或更远的范围内接收信号。对于客户端来说，某些因素可能会影响吞吐量，例如每个客户端使用的应用程序类型——大型文件传输、高清视频流、VPN和基于Wi-Fi的语音通讯。对于无线接入点的覆盖范围来说，像高密度墙体（例如砖）、家具、小间隔和其他障碍物等的物理因素会降低实际的覆盖范围。像校园等较大的区域，多个无线接入点共同工作来提供完整的无线覆盖。

尽管无线网络具有唯一的特性，但是WLAN的安全措施与那些在有线网络中使用的措施并没有明显的区别。关键是对于无线环境如何进行连接。无线网络连接可以配置为“非安全”或“安全”两种模式。一个非安全的网络或“开放”的网络意味着连接不需要认证。安全的网络意味着采取了一些用于连接的安全措施。

图 1. 分段的无线网络

确保网络安全可以保护公司免受意外的安全威胁和控制用户访问网络，同时也可以避免客户端的滥用，例如笔记本电脑和智能电话或者网络用户为了加速访问而设置的非安全的“流氓”接入点，无意中让无线网络易受到入侵者的攻击。

然而，基于五个简单步骤的安全规划可以确保无线网络保持安全。

步骤1：创建一个安全策略

对于任何一个公司，制定能覆盖有线和无线网络的安全策略是非常重要的。总体上，网络安全就好像网络最薄弱的环节——事实上，大多数安全漏洞都可以追溯到疏忽或整体安全策略在执行上的错误。例如，如果入侵者可以走到现场并轻易地插入以太网线缆来获得网络访问的权限，那么确保网络安全就变得毫无意义。

安全策略定义了对于特定公司来说什么是安全，规定了用户和网络管理员的正确行为以及对外部入侵者在物理和虚拟环境上的限制。安全策略包括对无线局域网功能、流量、以及访问的限制。制定的书面策略是很有用的，有可遵循的安全规定并且帮助改进社区内的安全环境。这样的策略成为一个实实在在的文档，可以不断地进行更新和被引用来支持当前的网络策略。

步骤 2：配置安全网络访问

配置安全访问对保护无线网络至关重要。在有线网络中，访问控制就像为已授权的用户提供以太网连接一样简单。然而，为了限制对无处不在的无线信号的访问，管理员可能会采取以下措施：

1. 建立密码保护：员工应该改变为接入点管理端口预设的管理密码。这将避免内部（在无线网络内的）或外部的恶意访问。例如，如果入侵者试图通过WEB接口或直接通过控制端口重新配置接入点，改变密码将会阻止恶意的入侵企图。

2. 物理上保证WLAN的安全：物理上保证接入点和控制网络的无线管理系统的安全是很重要的。不像网络交换机通常只放置在配线室里，接入点则是安装在桌子、墙、天花板等可视物体的上面。为了充分的物理安全所做的规划（例如，架构设计中的隐藏接入点、或确保监控摄像机的覆盖安装）将有助于保护网络避免受到物理上的入侵。

3. 确保WLAN的安全：通过实施无线认证，无线网络可以防止入侵。所有的无线接入点都具有内置的认证技术。认证的目的是控制谁可以访问WLAN。认证技术有很多种。每种认证技术具有不同的安全级别。

在无线安全的早期阶段，WEP（有线等效加密）是保证无线访问安全的标准。然而，WEP在设计上是有缺陷的，并且可以相对轻松地被破解。当有更好的替换技术并且幸运的是有许多更好的技术可以替换时，则应该避免使用WEP。WPA和WPA2（Wi-Fi保护访问）解决了WEP的脆弱性并且已经替代WEP成为更安全的技术。WPA2完全实现了IEEE 802.11i中定义的安全要素。不像WEP和WPA，WPA2使用AES（高级加密标准）算法来对数据进行加密，并且是当前无线认证中最安全和建议采用的方法。

WPA2支持两种认证模式。WPA2-PSK(预共享密钥)或WPA2个人模式是设计用于家庭或小型的网络，在这种网络中特定SSID的所有无线客户端共享一个共同的密匙。WPA2企业模式（EAP/RADIUS）允许使用WPA2和802.1x认证。在这种模式下，无线客户端通过具有单独的登录证书的RADIUS服务器来进行认证。这允许IT管理员创建不同的无线访问级别。对于业务来讲，这意味着可以更好地控制谁可以访问哪些信息，并最终实现更安全的无线网络。WPA2企业模式应该在任何企业的无线网络中使用。

步骤 3：控制无线的可见性

无线局域网都创建一个服务集标识（SSID）。SSID标识无线网络的名称并且广播出去指示无线网络的可用性。这便于附近的无线客户端发现无线网络，但也会使网络对一定范围的任何其它无线设备可见。

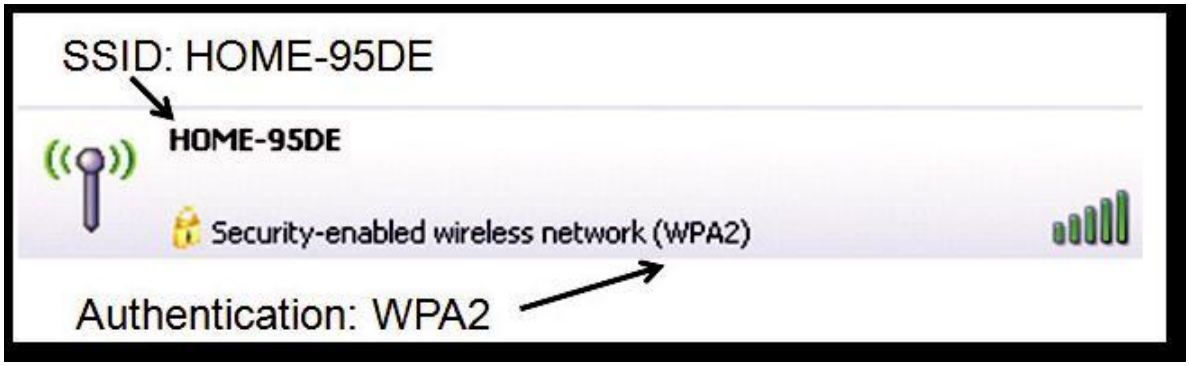

图2：无线网络示例

如果你想限制可见到无线网络的人员，则应该禁止SSID的广播来限制访问到那些可能正在寻找开放的无线网络的设备。同时，SSID标识应该改变，因为即使SSID不进行广播，专业的黑客知道常用的缺省SSIDs并可能利用这些缺省的SSID获得访问网络的权限。

为了根据位置实现访问限制，可以采取几个简单的步骤。首先，降低无线接入点的发射机功率会限制信号的覆盖范围——例如，限制只在管理区域内对学校的办公网络进行访问是可取的。限制无线信号的位置是非常困难的，然而这确实提供了最小化网络访问的可能。

步骤4：通过虚拟局域网保证网络的安全

保证信息安全的下一步是通过在网络上将“信任的”流量从“不信任的”流量区分出来以限制到特定工作组或团队的数据访问。WLAN的安全策略可以基于特定无线客户端的身份精确地执行访问限制，和到接入点的连接创建访问网络上不同工作组的不同类型。这种分段被称为“虚拟局域网”或“VLAN”，并可以映射到一个特定的SSID。这允许用户只访问特定的网络资源，并可用于为合约商、学生或项目临时联系人创建一个“访客” 网络。

VLAN可以进一步建立用来保证特定类型流量的安全，如条形码扫描或Wi-Fi电话通讯。VLAN确保如Wi-Fi语音等某些流量是安全的，并使这些流量不受像文件传输或流媒体音乐等消耗网络带宽的其它流量的影响。

步骤 5：当前安全维护和教育

没有网络可以单独地设置和运行。在已建立的安全策略的支持上，正如之前的讨论那样经常性地维护无线网络最高的安全级别是很重要的。在较大的环境中完成此项任务的关键是集中管理软件，它可以用来监控、检测和确定网络中的问题。集中管理软件可以导出或导入配置文件以降低配置错误导致WLAN安全漏洞的可能。集中管理软件也可以帮助检测、报告并拒绝由员工带入到网络中的非法AP的接入。

不是每个公司都认识到教育员工以保证网络安全是很重要的。研究显示大多数的安全事故实际上是由员工的错误造成的。许多公司没有意识到像改变笔记本电脑的设置这样简单的事情都可能危及网络的安全。经常遵循完美的网络安全原则可以帮助企业确保信息、人员和设施的安全。

总结

当今的无线网络正帮助机构和企业降低成本、增加效率并且提高机构改革和降低预算时的效率。如果他们遵循管理实践，无论小型还是大型的公司都可以从安全、稳定的网络连接中受益。

创建和维持一个安全的无线网络的关键是日常的管理。合适的工具将减少配置变动和固件升级中用户的错误和能够检测像非法AP和其他威胁在内的安全隐患。

NETGEAR提供为教育和小型企业设计使用的无线解决方案，该无线方案提供一个安全可靠的无线网络经验。无线解决方案包括为AP提供供电的PoE交换机、管理网络的无线管理系统、支持802.11a/b/g/n标准的各款AP、终端用户使用的无线适配器和终生保修的服务包。这种端到端的解决方案为公司提供无线网络快速轻松的配置、日常的管理及优化的安全性。