构建安全无线架构

构建安全无线架构

在本专题中，通过无线网络的转移、如何分割 WlAN 信息流、VPN 的作用、接入点的布置等内容，你可以学到如何构建安全的无线架构，理解 Wi-Fi 产品的功能，以及把如何传统的有线网络设备和配置应用到无线局域网中。

无线网络转移

WEP 已经破解了，WPA 是解决这个问题的方法，而且你的 CSO 建议将其升级为 WPA2。不错的建议，但是这并非一朝一夕的事。你如何转移你遗留设备的安装基础？TechTarget 中国的特约专家为转移工作提出了一个可行的策略，允许具有不同安全特性的新旧设备和平共存。

- 从这里到那里：WPA2 的转移

如何分割 WLAN 信息流

在企业网络中，虚拟局域网一直用于创建逻辑工作组、独立的物理地址和局域网拓扑结构。TechTarget 中国的特约专家在本文中讲述了如何使用这些在有线设备和无线设备中发现的虚拟局域网的相同性能，来标记和分隔 Wi-Fi 信息流，支持公司的安全和信息流管理策略。

- 使用 VLAN 分隔 WLAN 信息流（一）
- 使用 VLAN 分隔 WLAN 信息流（二）

VPN 的作用

早期的无线局域网经常再次使用远程访问虚拟专用网 （VPN）客户，克服 WEP 和相关的安全装置的局限性。但是，鉴于 Wi-Fi 安全性已经得到了提高，VPN 在企业无线网中是否仍然起到很大作用？在无线网中使用 VPN 的实际作用和局限性是什么呢？本节技巧讨论了如何充分利用 VPN，以及如何消除无线局域网漫游和 VPN 信道之间的冲突。

- VPN 在企业无线网中的作用

接入点布置

许多安装人员会犯这样的错误：认为 802.11 无线局域网仅仅和以太网相同，将接入点安置在特定位置，以促进外界访问企业网络。但是，从安全的角度而言，无线局域网应当和因特网形同看待——由信任用户和不受信任用户组成。但是本节技巧中，提供了网络拓扑结构和布置建议，可以获得更为安全的 AP 配置。

- 接入点(AP)布置的细节
- 是否有可能识别假冒的无线接入点？

从这里到那里：WPA2 的转移

WEP 已经破解了，WPA 是解决这个问题的方法，而且你的 CSO 建议将其升级为 WPA2。不错的建议，但是这并非一朝一夕的事。你如何转移你遗留设备的安装基础？TechTarget 中国的特约专家为转移工作提出了一个可行的策略，允许具有不同安全特性的新旧设备和平共存。

升级设备

WPA 版本 2(WPA2)是 Wi-Fi 联盟认证项目，专为那些执行 IEEE 802.11i 安全强化的产品而开发的。自 2004 年 9 月以来，就产生了 WPA2 认证的产品。今天，大多数企业和许多新住宅性 Wi-Fi 产品都支持 WPA2，并且从 2006 年 3 月起，WPA2 是强制使用的。

为了确定你的设备是否兼容 WPA2，可以查询 Wi-Fi 联盟认证产品列表。如果你的设备比较陈旧，而且不是 WPA (版本 1)认证的产品，那么让这个设备退休——如果不能立即更换，也要尽快更换。核查厂商的技术支持网站中的接入点固件或者插件驱动程序，进而对其它设备进行升级。你需要的硬件应该是使用不超过两年的；WPA2 需要执行高级加密标准（AES）的芯片集。如果你正在购买新的接入点，确保它们是经过 WPA2 认证的。

升级软件

WPA2 有两个流行版本：WPA2-个人版和 WPA2-企业版。WPA2-企业版需要一个 802.1X-capable RADIUS 服务器。没有 RADIUS 的小型办公室或家庭办公室可以使用带有 20+随机字符密码的 WPA2-个人版，或者使用诸如 McAfee Wireless Security 或者 Witopia SecureMyWiFi 的主机 RADIUS 服务。

大多数企业更喜欢用其内部的 RADIUS 服务器，比如 Cisco ACS、FreeRADIUS、Funk Odyssey、Interlink RAD、Meetinghouse AEGIS、Microsoft IAS、或者 Open.com

Radiato，来运行 WPA2-企业版。WPA 和 WPA2-企业版的差异几乎不会影响到 RADIUS 服务器，这样，如果你已经运行 WPA，WPA2 的升级可能不需要其它额外的 RADIUS。

运行这两种版本的 WPA2，你也需要客户端软件。这可能涉及到操作系统的补丁、802.1X 申请、和/或者新的无线网卡驱动程序。比如，虽然 Windows XP SP2 已经支持 WPA，但是使用 WPA2 要求安装 XP WPA2 补丁。对于其它操作系统，你需要 WPA2-capable 客户端软件，这些可以从无线经销商（e.g., Cisco）或者第三方（比如，Funk、Meetinghouse、wpa_supplicant、Devicescape）那里获得。WPA2 客户端和驱动程序可能永远不会支持内嵌有 Wi-Fi 的非典型设备（比如，VoWi-Fi phones、bar code scanners）和老化的适配器，这样的适配器根本无法支持 AES。

兼容

当你升级为 WPA2 时，就要开始逐步淘汰老化、安全性不佳的设备。实际上，你可能需要继续支持 WPA 和/或 WEP 一段时间。换句话说，你需要制定一个计划，以确保你现在的任何设备与 WPA2 能够共兼容。

策略之一就是作为一个新的覆盖网络来部署 WPA2。这意味着与旧的接入点并行安装新的接入点，用不同的安全策略和名称（扩展服务集标识符、a.k.a.服务集标识符（SSID）），创建两个独立的无线局域网。虽然这种方法比较昂贵，但是如果无论如何你已经准备好一个“升降机”式的升级——比如，当用下一代交换式无线局域网置换遗留下来的无线局域网时——这种方法便可以发挥作用。

另一个策略是在现有的接入点上升级固件，以及/或者置换接入点，逐步升级你的无线局域网基础设施，以支持 WPA2。所幸的是，WPA2 认证的产品必须支持 WPA，以反向地兼容同类竞争产品。大多数商业级接入点可以配置为既支持旧的安全策略，同时也支持新的安全策略。随着时间的推移，停止使用或者升级原有客户端，你就可以消除旧的安全策略。

这种多策略的无线局域网至少可以用两种方法实现：

如果你的接入点支持多个服务集标识符，那么为 WPA2 确定一个新的服务集标识符，保护旧的服务集标识符和相关的安全策略。比如，当 T-Mobile 将 WPA 添加到其热点上时，它就创建了一个新的服务集标识符。对于那些运行 T-Mobile 的连接管理器的客户端，只要与“tmobile1x”联合，现在就可以使用 WPA-企业版；而非 WPA 客户端仍然可以与旧的“tmobile”联合。在这种情况下，相同的物理接入点可以呈现为多个虚拟接入点，避免对较旧的客户端产生任何影响。

如果你的接入点支持 WPA2 的混合模式，你可以扩展现有的服务集标识符，进而支持多个安全策略。有了这个 Wi-Fi 联盟的 WPA2 选项，接入点就可以通过某个服务集标识符发送信标，告知几个密码（比如，TKIP [WPA]、CCMP [WPA2]）。客户可以从接入点列表中选择一个密码，这个客户当然必须能够理解接入点的信标。请注意，由于 TKIP 可以对局域网广播/多点发送加密，因此，旧的 WEP 客户可能不能在混合模式下工作。

一些接入点提供了其它经销商专用的选项，比如 Cisco 的 WPA 转移模式。如果你的无线局域网是同源的，并且你的客户设备组合不能由其它设备支持，考虑使用经销商专有的选项。

不论你怎么实现，WPA2 与较弱的安全措施相兼容应该是临时的一步。在过渡期间，你可能需要将 WPA2 和非 WPA2 分隔开来——比如，对来源于旧服务集标识符和新服务集标识符的信息流分别应用不同的虚拟局域网标签，然后，维护以这些标签为基础的不同信息流策略。为什么呢？因为攻击者喜欢挂的较低的果实；比较旧的接入点、服务集标识符和密码选项更容易吸引他们的注意力。

配置客户端

小型办公室或者家庭办公室的无线局域网发展为 WPA2-个人版时，客户端的配置几乎不需要费多少力气。只要你已经升级了客户端软件，从配置菜单中选择“WPA2-PSK”，输入一组密码，那么你就可以继续进行配置了。如果你正在 Windows XP 中使用 WPA2-capable 网卡，那么不要将 WPA2-PSK 视为一个配置选项，因为你尚未安装 XP WPA2 补丁。如果你已经安装了补丁，但是没有选择这个选型，你就漏掉了 WPA2 网卡驱动器。另外，

不要被采用 AES 支持 WPA 的产品所迷惑——这并不是 WPA2。要使用 WPA2-个人版，网卡和接入点都必须选择 WPA2-PSK 和 AES。

无线局域网发展为 WPA2-企业版时，尤其是大型的无线局域网，升级客户端是一项艰巨的任务。除了升级客户端软件，你必须选用一个 802.1X 认证方法、发行（或者重新使用）客户证书、并且将 RADIUS 服务器连接到一个用户帐户数据库中。好消息是，如果你已经配置了 WPA-企业版，那么你的工作就已经含盖了这一方面，就无需再进行这项工作。否则，请阅读我们的相关技巧“选择合适的 802.1X 版本”，并继续对你的 WPA2-企业版进行升级。

（作者：Lisa Phifer 译者：李娜娜 来源：TechTarget 中国）

使用 VLAN 分隔 WLAN 信息流（一）

在企业网络中，虚拟局域网一直用于创建逻辑工作组、独立的物理地址和局域网拓扑结构。TechTarget 中国的特约专家在本文中讲述了如何使用这些在有线设备和无线设备中发现的虚拟局域网的相同性能，来标记和分隔 Wi-Fi 信息流，支持公司的安全和信息流管理策略。

走虚拟化路线

在以太网的局域网中，连接到相同无力交换器的工作站是“广播域”中的一部分。每个工作站发送的广播数据包是由该域中的其它相隔工作站分别接收。但是争论和费用随着域的规模增加；最后，局域网由于冲突而堵塞并停顿下来。

通过将物理局域网分割成几个较小的逻辑广播域、或者虚拟局域网，就可以阻止局域网的堵塞和停顿。虽然虚拟局域网中的工作站可以共享相同的物理媒介，但是，信息流可以分割成独立的广播域。工作站可以参与特定局域网接收该虚拟局域网中所有其它站点发送的信息包，而不是其它虚拟局域网中的站点发送的信息包。

以太网交换器可以将组端口配置到编好号的虚拟局域网中。比如。当信息包到达端口#9（虚拟局域网 #1)时，交换器可以迫使这些信息包穿过所有其它属于局域网#1 的端口，而且只通过这些端口。这种简单的、静态的方法就是人们熟知的基于端口的虚拟局域网。

或者，这个交换器可以监测到达的信息包是否内嵌有“标记”，迫使信息包通过已确定虚拟局域网的所有端口。IEEE 802.1Q 讲述了如何在每个信息包的包头添加虚拟局域网的标识符（1-4096）和优先次序（1-7）。标记可以使 802.1Q-资格的设备在信息包的整个传播路径中执行虚拟局域网的分割。这些设备有 Layer 2 交换器和 Layer 3 交换器、路由器和防火墙。

比如，边缘交换器 A 可以通过端口#9 接收信息包，申请标签#1，然后促使这个信息包到达虚拟局域网中的所有端口，通过虚拟局域网的主干达到核心交换器 B。在促使信息包到达虚拟局域网#1 中的所有边缘交换器之前，交换器 B 会对其标签进行检查，然后通过其主路径传到上游路由器。这个路由器使用信息包的入口界面、虚拟局域网标签、以及源/目标 IP/端口，进而使用访问控制列表（ACL）。访问控制列表可以允许/拒绝进一步转发。

虚拟局域网允许你创建独立于物理地址的局域网工作组。参与某个特定虚拟局域网的工作站可以跨不同楼层、建筑物、甚至城市分布。可以添加或者删除工作组成员，配置集中管理的设备可以改变访问控制列表（ACL）。除了减少广播的费用，虚拟局域网标签可以用于赋予某个工作组的信息流高于其它工作组的优先权，并且允许成员听取信息流并获取网络资源，只有工作组成员可以获取这些资源，其他人不可以。

（作者：Lisa Phifer　译者：李娜娜 来源：TechTarget 中国）

使用 VLAN 分隔 WLAN 信息流（二）

将虚拟局域网扩展为无线局域网

现在我们已经了解科虚拟局域网在有线以太局域网中是如何工作的，我们再探讨一些我们为什么要将其扩展为无线 802.11 局域网，以及如何扩展。

从区分无线信息流的优先次序和控制这些信息流的流向中，许多公司可以受益不少。通过无线网，使用 802.11e 的服务质量(QoS)，可以区分 802.11 数据包的优先次序。此外，尽管我们不能控制对无线网的访问，但是使用 802.1X 端口访问控制，我们可以允许/拒绝无线接入点。虚拟局域网标签可以促使这些无线安全性和性能措施适合你的有线网络。

比如，所有的无线接入点可以分组为一个单一的虚拟局域网，指定一个任何以太网工作组都不能使用的标识符。边缘交换器可以将无线虚拟局域网的标签应用到从任何接入点接收到的信息包中。上游交换器可以将所有的无线虚拟局域网信息流通过信道传入因特网访问路由器中，并且网络层访问控制列表可以阻止无线虚拟局域网到达您公司网络内部的其它目的地。

这样隔离到达无线网信息流的方式，适合于仅使用 802.11 来提供客户因特网访问的网络。无线信息流也可以指派给较低的优先权，这样交换器和路由器会首先服务其它信息流。无线虚拟局域网也可以用于将接入点和工作站分组到一个 IP 子网中，与地址无关。那样的话，当无线工作站在接入点之间漫游时，它们可以更新相同的 IP，防止 TCP 会话和 VPN 信道的中断。

最终，这种单一虚拟局域网的方法会面临与物理局域网相同的问题：随着无线网络规模的增加，虚拟局域网会发生堵塞情况。此外，随着无线网络变得更加多样化，将单一虚拟局域网分别分割成不同的工作组（几个虚拟局域网），这对解决问题有所帮助。

无线虚拟局域网标记

所幸的是，802.1Q 标记也为我们提供了将无线信息流分到多个虚拟局域网时所需要的基础，这是以定义好的标准为基础的。

当来自无线接入点的信息流集中通过 802.1Q-capable 无线交换器或者网关时，这个设备在转发这些信息流之前，可以标记信息包。比如，无线网关可以位于接入点和受保护网络、认证工作站之间，然后按照职能将其送达到目的地。职能可以定义访问控制列表和虚拟局域网标签，进而可以应用于允许通过网关的任何信息包。“客户”职能的工作站可以接收虚拟局域网标签#1，而“员工”职能的工作站可以接收虚拟局域网标签#2，诸如此类等等。

另外，在将这些信息包送到分布式网络（比如，因特网）之前，802.1Q-capable 接入点可以标记到达 802.11 的信息包。换句话说，这个接入点扮演着边缘交换器的角色，在将其从虚拟局域网主干发送到任何上游交换器、网关或者路由器之前，首先标记这些信息包。接入点是以无线局域网入口的标签（比如，无线电接口、或者服务集标识符）为基础，而不是以准入交换器端口的标签为基础。比如，所有连接到 SSID“客户”端的工作站都可以接收虚拟局域网标签#1，而所有连接到 SSID“员工”端的工作站都可以接收虚拟局域网标签#2。

以上任何一种方法都可以按照需要将无线信息流分离到许多虚拟局域网中，以实现网络的目标。比如，虚拟局域网可用于从数据中区分无线语音，并赋予无线语音在无线网（带有 802.1e）和以太网（带有 802.1P）中传播的优先权。虚拟局域网也可以用于把管理信息流从终端用户信息流中分离开来，进而减少管理威胁带来的风险。最后，无限局域网可以使用 RADIUS 来绘制信息流的虚拟局域网标记——详细情况，请查看我们的另一条技巧：无线局域网认可中 802.1X 和虚拟局域网的结合。

虚拟局域网的最佳做法

不论有多少个前提条件，虚拟局域网可以帮助在有线网络和无线网络中划分信息流。然而，必须仔细配置虚拟局域网，以防发生制约到正确操作或者威胁到安全性的错误。比如，无线安全专家认证(CWSP)学习指南中有如下建议：

- 应当对在接入点和交换器之间的主要信道中传送的信息流进行过滤，仅允许属于正在工作的无线虚拟局域网的信息包通过。
- 为了避免动态虚拟局域网的重新配置，接入点不应该使用通用 VLAN 注册协议（GVRP）。
- 广播和多点传送到接入点的信息流都应当进行过滤，比如，通过使用 Internet 组管理协议（IGMP），进行窥探。
- 访问控制列表应该可将无线安全融入到有限基础设施中。
- 访问控制列表应当可以阻止终端用户访问接入点的默认局域网。

（作者：Lisa Phifer　译者：李娜娜 来源：TechTarget 中国）

VPN 在企业无线网中的作用

早期的无线局域网经常再次使用远程访问虚拟专用网 （VPN）客户，克服 WEP 和相关的安全装置的局限性。但是，鉴于 Wi-Fi 安全性已经得到了提高，VPN 在企业无线网中是否仍然起到很大作用？在无线网中使用 VPN 的实际作用和局限性是什么呢？本节技巧讨论了如何充分利用 VPN，以及如何消除无线局域网漫游和 VPN 信道之间的冲突。

VPN 如何起作用

VPN 信道一直都用于在诸如因特网之类的不受信任网络中提供数据的机密性和完整性。今天，许多公司使用信道来确保从远程工作者到公司网络边缘的 VPN 网关过程中信息流的安全。这个网关可以认证用户身份并控制可以达到哪个目的地。

今天，VPN 也正在强化终点安全的执行。在准许访问网络之前，会默认检查远程设备。比如，可能仅允许公共 PC 的工作者检查电子邮件，而允许公司笔记本电脑的工作者访问敏感的服务器。笔记本电脑丢失补丁或者感染了特洛伊木马，可以直接求助检疫的服务器，进行修补。

无线网用户可受惠于这些相同的安全措施。

- 诸如有线等效保密（WEP）或者无线相容性保护访问（WPA）的版本 1 或者版本 2，VPN 信道可以隐藏通过无线电波发送的信息流。WEP/WPA 不仅仅保护空中的连接，而 VPN 信道可以向任何干扰网络扩展。虽然这可能“在校内”并不重要，但是在使用住宅区无线局域网或者热点无线局域网时，这一点是很关键的。
- 像 WEP-企业、VPN 网关都可以验证无线网用户，采用密码、双因素令牌、智能卡、或者证书。但是 802.1X 对局域网提供了要么全有要么全无的访问，而 Layer 3 VPN 和 Layer4 VPN 则可以限制可到达的目的地和应用程序。对拥有广泛不同的用户社区的大型无线局域网来说，更为精细的策略在是非常重要的。

- 依赖这种产品，WPA-企业和 VPN 都可以强化终端的安全性。然而，VPN 使用一个代理器平台，跨越不同的网络、本地或者远程的网络，可以更容易地实施一系列持久连续的规则。
- 最后，这两种技术都需要客户端配置、用户身份管理、以及（某些情况下）软件安装。VPN 产品比 802.1X 产生的时间长一些，因此，许多 VPN 产品拥有更详尽的中央政策管理和更广泛的客户端操作系统/平台的支持。

VPN 如何阻止

有许多 VPN 信道标准，包括点对点信道协议（PPTP）、因特网协议安全（IPS）和安全套接层协议（SSL）。VPN 产品和安全特性有很大的不同，并且直接影响到它们是否能满足你的无线需求。

比如，虽然 PPTP 是最易攻破的共同 VPN 协议，但是，它也易于使用。PPTP 客户端内嵌在许多操作系统中：包括 Pocket PC 和 Mac OS，此外，基本不需要进行配置。在频谱的另一个终端，IPS 提供了坚固的安全性，并由复杂的配置所支持，由 VPN 客户机安装。在 SSL VPN 层之间——要比 PPTP 更安全，配置起来要比配置 IPS 更容易。

这种多样性使得很难相互比较 VPN，比 WPA 要简单得多。但是，关于 VPN 是如何阻止无线网，我们仍然可以做出全面的观察和评价。

- ?WEP 和 WPA 可以保护所有的链路层数据，包括局域网广播和组播。局域网使得更多的信息流暴漏出来，这样在信道开启之前，很难防止信息“泄露”。这尤其符合用于受信任（校内）的无线局域网和不受信任（热点）的无线局域网中的设备，这些局域网需要不同的 VPN 策略。
- 虽然 VPN 与远程安全措施相吻合，但是往往对网络拓扑结构比较挑剔。比如，WPA-企业可以为无线工作站分配虚拟局域网标签，支持当地和独立子网中的局域网访问控制。VPN 通常使用虚拟的 IP 来达到这一目的，这就可以命令路由，并过滤网络中的变化。

- 尽管当无线工作站漫游时，WPA-企业会带来延时，但是当工作站在 IP 子网间漫游，VPN 信道通常会破坏。虽然将所有无线用户集中在一个子网，就可以避免这一点的发生，但是这在非常大的无线局域网是不可能的。
- 因特网安全协议（IPS）中的 VPN 需要特定的客户端软件，在一些客户或者设备无法正常运行客户端的无线局域网中是不切实际的（比如，无线扫描器、智能电话、VoWi-Fi 步话机）然而，WPA-企业安装中需要特殊的 802.1X 请求，会面临类似的问题。

克服困难

大多数企业会采用 VPN 和 WPA2 的结合来结束对无线劳动力的保护。随着无线网的基础设施日趋成熟，许多人会将校内网升级成为 WPA2-Enterprise。虚拟专用网（VPN）会坚持保护无线热点的移动工作者和无线局域网首页的电话工作者。很少有公司可以控制远程网络，此外，安全状况也有所不同。用 VPN 托管所有校外无线网可能是在这些环境中执行公司制定的策略的唯一方法。

那么，在使用无线局域网的时候，你该如何面对 VPN 的挑战？

- 将终端安全软件与你的虚拟专用网客户端相结合，终端安全软件可以进行核查以确保只要无线链路处于连接状态，VPN 就在运行，并且如果 VPN 信道下降，就中断无线连接。配置个人防火墙以阻止非 VPN 信息流通过无线网进入或者离开。
- 对于单一接入点无线局域网首页和因特网咖啡馆的用户而言，由于漫游导致的 VPN 中断可能并不是一个大问题。当在不同地点移动时，仍然需要保持连接的工作者就可能需要一个移动的 VPN。可以从 NetMotio、Columbitech,、Ecutel 和 AppGate 购买到移动式无线专用网产品，当客户需要在网络之间移动时，这些移动式无线专用网产品可以提供持续的信道和会话。当某个设备暂时移出范围时，一些产片甚至可以排队等待接收的信息。虽然所支持的技术不同，但是移动式专用网通常都需要客户端软件。

- 当使用无线专用网来确保校内网工作者的安全是，应该使用无线网关或者交换器，它们可以提供“流动性”或者“子网漫游”。虽然这些特性使专有的，但是，当在子网间漫游时，通常会让 VPN 客户端保持相同的虚拟 IP。然而，当工作站离开无线网的覆盖范围时（比如，内部电梯、建筑物之间），仍然会发生应用层中断。

最后，为了支持那些不能运行 VPN 客户端软件的客户和其它设备，应该使用一个安全套接层协议 VPN 或者受控的入口。虽然受控的入口不需要对数据加密，但是，可以用于控制并追踪网络的使用情况。安全套接层协议 VPN 使用网络浏览器作为客户端平台，对数据进行加密，同时，它甚至可能适用于客户端设备。

（作者：Lisa Phifer　译者：李娜娜 来源：TechTarget 中国）

接入点(AP)布置的细节

许多安装人员会犯这样的错误：认为 802.11 无线局域网仅仅和以太网相同，将接入点安置在特定位置，以促进外界访问企业网络。但是，从安全的角度而言，无线局域网应当和因特网形同看待——由信任用户和不受信任用户组成。TechTarget 中国的特约专家在本文中提供了网络拓扑结构和布置建议，可以获得更为安全的 AP 配置。

布置事项

接入点带有出厂默认的全向天线，其覆盖范围大概是一个圆形，并且受到像围墙一样的射频障碍的影响。因此，在中央区域布置接入点是很普遍的，或者把办公室分割成几个信号区，每个区都布置一个接入点。

这种方法虽然非常直观，但是可能无法使成本、性能和安全性最优。理想的覆盖范围很少是圆形的。为了填补这个造成的差距，你需要停止购买更多的接入点，满足实际需要便可；同时停止“泄露”大量的信号。网站模型和/或定向天线可以帮助你避免这个问题。

建模工具把建筑材料性质、接入点性能和站点调查措施结合在一起，设法弄清楚用户的位置、密度和吞吐量要求，进而预测接入点应该配置在什么位置，并验证结果。虽然前期的计划需要花费很多时间和精力，但是最后会有回报的，尤其对于那些大型的无线局域网。比如，可以考虑应用 AirMagnet Surveyor、AirTight SpectraGuard Planner、Network Chemistry RFprotect Survey、以及 Trapeze RingMaster。

用定向天线替换接入点的“上等橡胶”全方位天线，可以更好地关注辐射信号的来源，提高内部覆盖面，并减少外部的信号泄露。

物理定位、以及诸如传播功率调节之类的相关步骤，可以使入侵者很难与接入点保持连接。但是你绝不应该指望只物理定位就可以阻止攻击者。

物理或逻辑局域网的分割

接下来，防止无线局域网信息流与“其它”局域网信息流混合。连接到你以太网无线局域网的工作站组成一个可信任的工作组。他们交换传播/多点传送信号，依赖共享资源：比如 Layer 2 网络集线器或交换器、DHCP 服务器、DNS 服务器和 Layer 3 交换器或路由器。在局域网上安置不受信任的设备，你就会把每个设备置于风险之中。不良代理人会导致广播风暴、破坏 ARP 高速缓冲存储器、毁坏 IP 地址协议等等。对你的接入点进行物理或者逻辑分割就可以减轻这一风险。

举例来说，将所有的接入点连接到一个新的以太网交换器上，而不是把它们连接到附近有线设备使用的现有以太网上。或者你可以将“瘦”接入点连接到一个新的无线交换器上（比如，Aruba、Cisco、Trapeze），该交换器主要负责管理和监测这些接入点。将所有接入点集中到一个物理局域网上，这很容易理解，但是这并不成比例。

较大的无线局域网使用虚拟局域网（VLAN），可以创建逻辑工作组。虚拟局域网使用用于控制信息流的标识符来标记数据包或者端口。比如，虽然可以将接入点连接到现有的以太网交换器端口上，但是也需要在新的虚拟局域网上分配这些端口。你可能会希望有至少两个新的虚拟局域网——一个用于接入点管理，另一个共无线用户使用。若要了解用虚拟局域网分割无线信息流的更多情况，请阅读我们的相关技巧“运用虚拟局域网划分无线局域网信息流”。

需要注意的是，分割局域网既会影响到安全，也会影响到性能。比如，服务质量措施可以应用到物理局域网或者虚拟局域网中，这样的员工的信息流优先权在客户之上。

创建网络屏障

有时候，无线局域网会遇到网络层设备，这里它可能会发送到公共因特网或者其它内部子网中。就是在这里，许多员工安装的接入点遭到破坏。将不受信任的设备连接到受信任的子网中，这就创建了一个不安全的“后门”。在信任子网的“前门”执行安全措施——防火墙、VPN 信道、网络病毒——将工作站连接到错误布置的接入点就可以规避这些安全措施。

出于这个原因，无线接入点应该总是与受信任的子网分离，使用网络层策略执行设备可以分离接入点和子网，这些种类的设备包括：

- 路由器
- 防火墙
- VPN 网关
- 无线网关和 Layer 3 交换器
- 网络访问控制器

比如，你的接入点可以直接连接到访问路由器中，配置为将无线信息流发送到因特网上，而不是发送到公司网络。或者你的接入点可以连接到 VPN 网关，该网关可以验证 VPN 客户机并阻止所有其它信息流。或者你的接入点可以配置在防火墙的隔离区（DMZ）内，允许无线访问一些受隔离区保护的服务器，但却阻止通过防火墙进入信任的网络。

在创建网络屏障时，考虑该设备必须运行的功能。为了执行安全策略，你可能需要访问控制点（基于 MAC、虚拟局域网、IP、端口或者应用层信息检查）、工作站或者用户认证、VPN 信道（子网漫游范围以内或者外部）、对话核算、病毒扫描、内容过滤、入侵检测/防御、以及带宽限制。虽然一般用途的防火墙可以完成大部分这些工作，但是无线网关或者 Layer 3 交换器可以填补这个角色，并且提供像接入点发现、供应和 RF 管理之类的 802.11 特定功能。不同的屏障可能适合不同的用户——比如，基于网络的访问控制器适用于客户，VPN 网关适用于员工。

最后，不论你选择哪个设备，都要制定输入和输出策略，以满足商业需要，并拒绝其它一切请求。比如，SNMP 请求、路由信息、或者隔离区更新都应当来源于你的无线局域

网，这可能是毫无理由的。虽然精细的策略可能需要更多的精力来维持，但是它也可以减少无线传播攻击危及核心网络安全所带来的风险。

（作者：Lisa Phifer　译者：李娜娜 来源：TechTarget 中国）

是否有可能识别假冒的无线接入点？

问：当接入无线局域网的无线热点，你如何判断正在连接的是假冒的还是真正的接入点？

答：如果你使用不安全的网络，很简单，你无法判断。在这种情况下，你拥有的唯一识别网络身份的证据就是 SSID（服务设置标志号），或者是网络传播的“名称”。不过，任何人都可以设置无线网络，命名他们想要的任何 SSID，因此，在这种情况下，并不存在真正的的身份识别证据。当使用不安全网络时，我强烈推荐将主机的防火墙设置为拦截所有接入连接。同时，你应该采用 VPN，对你的计算机与远程系统之间的所有通讯进行加密。

如果要寻找更有力的身份识别证据，你就需要转换到安全的无线选择。当共用密匙得以确认，WPA（Wi-Fi 网络安全存取）就可以提供一个网络连接。在 WPA 情况下，成功的接入尝试至少表明你连接到一个由知道这个共享密匙的人建立的网络。不过，如果你接入的是公共的无线热点，通常没有这种的验证。所以，你应该假设该网络是不安全的。为了确保你使用安全的无线网络，建议你采用我在前面提到的安全措施。

（作者：Mike Chapple　译者：Shirley　来源：TechTarget 中国）