室外无线安全的最佳实践

本文将介绍部署室外无线局域网的安全最佳实践。

挑战

很多地方政府都在设法通过部署无线局域网（WLAN）来改造他们的政府流程。WLAN 为改进业务运营、促进交流和向政府职员、民众提供更好服务带来了创新的方法。另外，室外 WLAN 可以将现有的、面向有线网络的服务和应用拓展到城市当前的物理基础设施之外。

越来越多的关键任务型业务应用和服务开始被部署到与公共互联网存在大量连接的开放网络之上。如果不采取适当的保护和安全措施，互联网连接可能会危及那些能够帮助政府机构提高效率的生产率改进成果。

当关键任务型信息通过公共和专用网络基础设施传输时，必须执行必要的安全控制和风险消除策 略，以确保信息得到妥善的保护和安全等级策略符合政府法规的要求。一个精心设计的、安全的 WLAN 可以帮助机构放心地将网络拓展到移动办公人员、执法警官 和民众，从而提高生产率、加强安全性和开辟新的收入渠道。

解决方案

尽管将网络拓展到建筑物边界之外的想法可能会引起对安全问题的担忧，但是足以让 IT 管理人员感到放心的是：通过采取适当的措施，室外无线网络可以像室内有线、无线局域网一样安全。

采用标准的企业安全手段

在室外无线网络行执行的公共安全和市政应用实际上是城市内部网络的延伸。因此，对于那些通过 室外无线网络访问城市网络的人员，也应当采用与政府网络相同严格的安全措施。这些措施不仅可以保护政府网络的安全，还可以让远程办公人员在现场办公室、家 中或者外出途中连接政府网络。思科的安全手段建立在思科自防御网络和 SAFE 蓝图架构的基础之上。它们可以提供集成、安全的有线、无线、数据中心和互联网 访客接入。一个支持安全功能的基础设施可以从网络的核心拓展到终端系统。网络中的每个设备—从移动设备到台式机，从 LAN 到 WAN—都在一个保护网络 环境的、完全分布式的防御系统中扮演着一定的角色。自防御网络可以发现威胁；根据严重等级采取适当的措施；隔离发生故障的服务器、台式机和移动设备；以及 针对攻击重新设置网络资源。终端安全设备包括思科网络准入控制（NAC）、思科安全代理和思科信任代理。这些技术可以为 PC 和服务器提供行为保护，防止受 到过去没有见到过的新型攻击的影响，以及提供关于主机安全状况的信息—主机安全策略需要在允许网络访问之前对其进行验证。

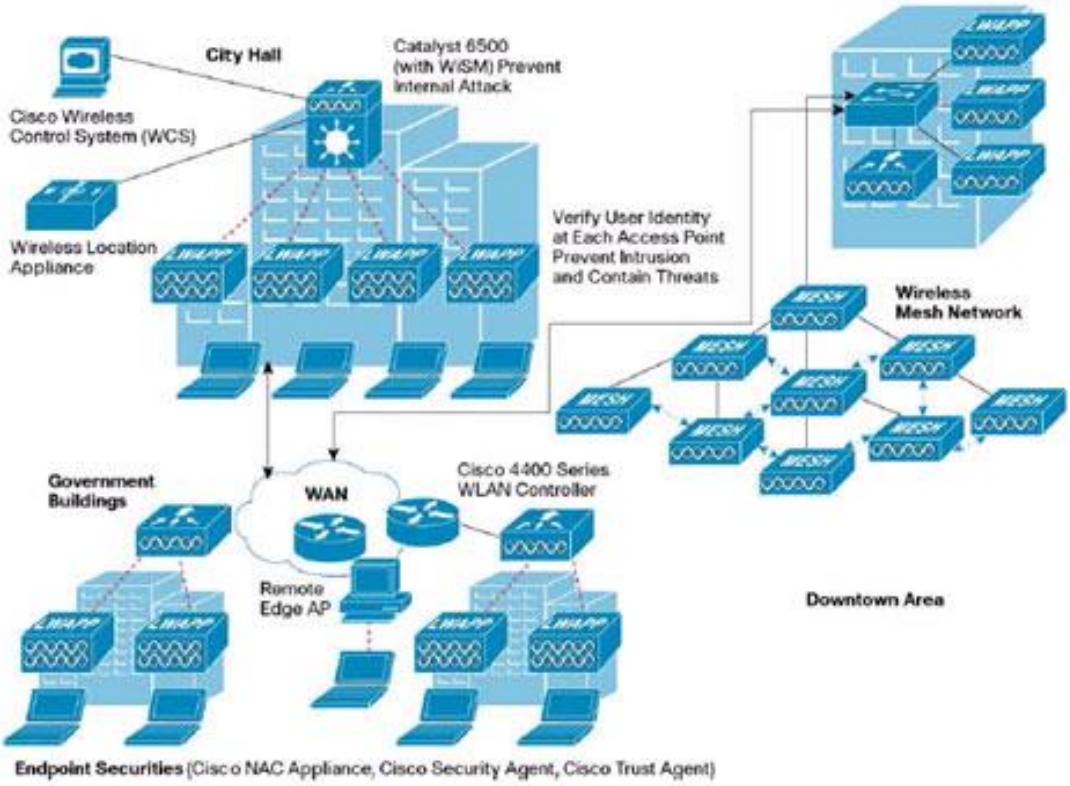
思科安全解决方案采取了灵活、可定制的部署方式，可以利用客户对多种平台（例如专用安全设备 和基于路由器、交换机的安全）和技术（例如防火墙、威胁防御、身份验证、授权和计帐[AAA]，URL 过滤，802.1x）的已有投资。如图 1 所示，思科 自防御网络的组件可以在三个区域协同保护网络：

- **威**胁防御，其中包括：

- 保护边缘—利用防火墙和入侵防御系统（IPS）加固网络边缘，防止受到入侵和攻击的影响；
- 保护内部—在重要节点采取安全措施，防止网络遭受新出现的内部攻击的影响
- 保护终端—主动地防止主机遭到感染和破坏

- 信任关系和身份识别，这意味着您始终知道谁在使用网络，并可以控制他们所能访问的内容
- 加密通信，包括加密的内部、外部语音和数据通信。

图 1 思科统一无线网络架构



利用现有的无线局域网安全标准和最佳实践

对 WLAN 的保护建立在拓展思科自防御网络战略的基础上。室外无线网络应当采用与室内 WLAN 一样的无线安全最佳实践，确保对网络上的用户进行适当的身份验证和保护数据的隐私性。下面几节将概要介绍保护无线局域网的最佳实践。如需查看对所 有这些领域的详细讨论，请参阅白皮书《保护企业无线局域网和防止无线威胁的五个步骤》。

加密通信

思科自防御网络的第一个核心原则是加密通信。在有线和无线环境中，这涉及到加密数据和对网络 用户进行身份验证。加密和身份验证并不一定要配合使用，但是对于大部分企业网络而言，我们建议同时使用这两种手段。室外无线网络的一个特殊例外是公用应 用，本文稍后将对其进行更加详细的讨论。例外，无线介质的某些特性使得它需要采取其他一些安全技术来保护网络。这些额外的安全技术包括：

- 修改缺省 SSID—通过修改制造商的缺省服务集标识符（SSID），可以防止不速之客进入无线网络。但是，公共接入 SSID（访客接入 SSID）可以公开给普通民众使用。

- 建立单独的 WLAN（SSID/VLAN）—可以被用于分隔不同的用户群组，以提高安全策略的等级。
- 使用严格的加密—如果移动设备可以提供支持，那么符合行业标准的 Wi-Fi 受保护接入（WPA）或者 WPA2 将是首选加密方式。Cisco Aironet?和思科兼容客户端（即经过思科兼容扩展计划验证，可以与思科产品互操作）都支持 WPA 和 WPA2。
- 在客户端和网络之间部署双向身份验证—IEEE 802.1X（WPA 或者 WPA2 所采用的身份验证方法）可以对客户端提供强大的身份验证。一个 IP 安全（IPSec）或者 SSL VPN 也将提供强大的双向身份验证。
- 利用 VPN 或者有线等效隐私（WEP）和 MAC 地址控制列表来保护不支持 WPA 或者 WPA2 的专用设备—VPN 可以为网络和设备的安全提供最佳的保护，因而我们强烈建议客户使用 VPN。如果移动设备只支持 WEP，那么最好使用定期密钥 轮换和额外的 MAC 地址控制加强安全管理，而不是敞开网络。
- 部署一个不在本地存储安全信息的轻型接入点架构—思科统一无线网络是一种轻型接入点架 构。这意味着敏感的安全信息不会存储在本地接入点，而是集中存放在思科无线局域网控制器。因为控制器可以部署在锁闭的网络配线间内部，所以失窃的可能性很 低。任何失窃的无线网格接入点都不会提供任何可能危及网络的安全信息。
- 确保管理端口得到安全保护—利用 SNMPv3、SSH 或者 SSL 来保护无线网络的管理接 口。一个像思科统一无线网络这样的轻型架构非常适用于室外无线网络，因为所有配置改动都可以通过安全部署在室内的思科无线控制系统（WCS）集中管理。不 能通过无线方式对 Cisco 1500 系列接入点的配置进行任何改动。思科 WCS 还可以降低长期运营开支（OpEx），因为所有升级任务都是集中完成，消除了对每个接入点进行现场升级 的需要。
- 掩藏或者保障接入点设备，防止被篡改—尽管放置在露天环境中，但是大部分无线网格接入点实际上比企业内部的接入点更难接触，因为它们通常安装在很高的位置，例如楼宇屋顶或者电线杆等。
- 修改缺省的网桥共享密码—这将确保在网格接入点上禁用桥接功能。

威胁控制和隔离

思科自防御网络计划的第二个核心原则是威胁控制和隔离。思科统一无线网络采用了独特的设计， 可以主动地监控和防范无线网络安全类型的威胁。思科统一无线网络接入点可以同时充当无线信号显示器和数据转发设备，让接入点可以在不中断服务的情况下，发 送关于无线网域的实时信息，包括对思科无线局域网控制器的潜在安全威胁。它能迅速地发现安全威胁，并通过思科 WCS 提交给网络管理人员，以便进行准确的分 析和采取纠正措施。

策略和遵从性管理

室外无线网络的部署为网络带来了一种无组织的状态。因为终端设备位于城市网络之外，监控成为 了确保系统、网络策略不被违反，危险威胁（例如病毒、蠕虫和间谍软件）不会进入政府网络的关键。策略和遵从性管理是思科自防御网络战略的最后一个核心原 则。主动监控和隔离对于保持网络的完整性非常重要。如果不进行监控，IT 管理人员就无法知道他们制定的安全策略是否得到了有效的执行。终端可见度和控制有 助于确保所有试图进入一个网络的有线和无线设备都遵从企业的安全策略。受到感染或者存在隐患的终端需要被自动发现、隔离和清除。

网络准入控制（NAC）是指一系列基于思科系统公司?所领导的行业计划的技术和解决方案。 NAC 利用网络基础设施来对所有试图访问网络计算资源的设备实施安全策略管制，从而防止新出现的安全威胁（例如病毒、蠕虫和间谍软件）所造成的破坏。使用 NAC 的客户可以只向符合规定的、值得信赖的终端设备提供访问权限，以及限制不符合规定的设备的权限。思科 NAC 设备（Cisco Clean Access）和思科 NAC 框架都可以为无线局域网提供安全威胁防护。这些解决方案可以在 WLAN 客户端试图访问网络时，通过隔离不符合规定的 WLAN 客 户端和为确保兼容性提供纠正服务，确保设备遵从安全策略。这两个解决方案都可以与思科统一无线网络进行互操作。图 2 显示了思科统一无线网络的 NAC 设备架 构。图 3 显示了 NAC 框架架构。

图 2 思科统一无线网络的思科 NAC 设备架构

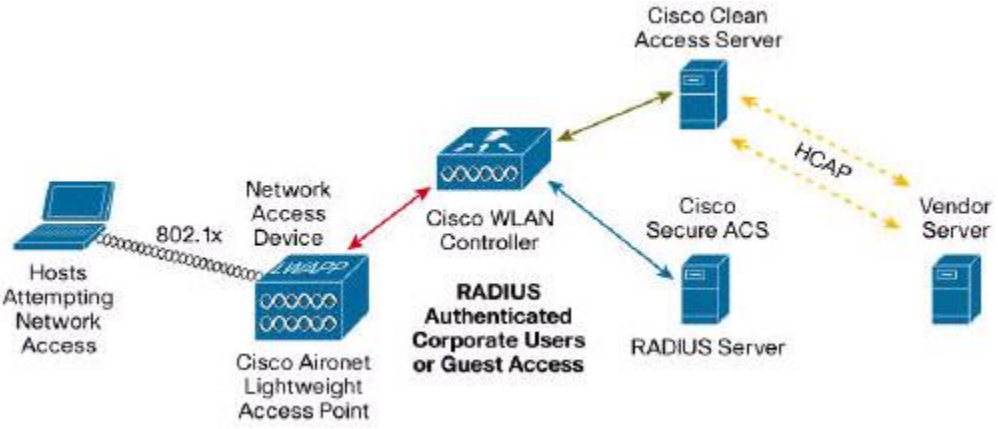
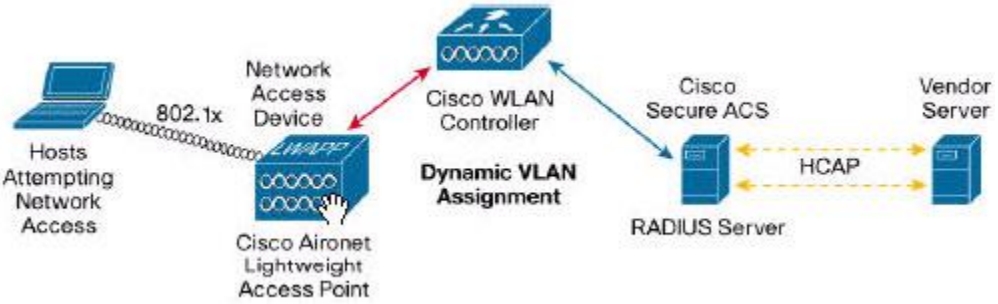


图 3 思科统一无线网络的思科 NAC 框架架构



保护网格回路

无线网格接入点添加了另外一个必须考虑的安全区域：接入点之间的无线连接。如果这条连接不够安全，网络将会面临威胁。

Cisco Aironet 1500 系列轻型室外网格接入点可以通过在网格接入点连接上提供最高等级的加密，消除这种顾虑。高级加密标准（AES）被用于对网格连接上的所有通信进行 加密。这与 IEEE 802.11i 安全标准中使用的加密方式相同，而且这种方法从来没有被破解过。另外，每个网格接入点的网桥共享密钥，且每对网格接入点都采用了唯一的密 钥。

在多用途网络上确保市政当局和公共安全通信的安全性

大部分城市计划都包含一个能够同时支持多个用户和应用类型的无线网格网络。例如，警察、楼宇 检查员和民众可以同时使用这个网络。为了在支持这些用户、应用的同时，确保网络的安全性，思科统一无线网络可以支持身份联网，即根据无线客户端的身份¯而不是物理位置¯分配和执行 WLAN 策略。利用身份联网，WLAN 系统只需要对无线设备进行一次身份验证。在设备四处漫游时，环境信息将始终伴随着它 们，从而确保了移动性。当 WLAN 与某个特定的虚拟 LAN（VLAN）相关联时，用户只能访问该 VLAN 上的网络资源。例如，楼宇检查员可以利用 SSID“cityhall”访问无线网格网络，该 SSID 只提供了对于特定的城市数据库和电子邮件系统的访问权限。警务人员可以利用 SSID“police”访问无线网络，该 SSID 则提供了对于犯罪记录和 DMV 数据库的访问权限。这些 SSID 都可以支持严格的 802.11i 或者 WPA 加密。

市政工程人员可以在执行存货和现场服务跟踪任务中采用支持无线通信的条形码扫描仪。这种设备 通常不支持当今严格的 802.11i 或者 WPA 安全，而是只支持不太安全的 WEP 加密。它们也可以被划分到一个支持 WEP，将流量发送到 VLAN 的

特定 SSID。该 SSID 将只允许他们访问一些与其有关的数据库或者应用。另外，通过频繁更改加密密钥和 MAC 地址控制列表，可以有效地消除潜在的安全风险。

最后，很多城市都对向居民、企业和旅游者提供 Wi-Fi 服务很感兴趣。无线访客网络可以在提 供 Wi-Fi 服务的同时，避免对每个用户进行授权。访客网络采用一个划分到某个特定 SSID 的开放安全方法，将流量路由到某个只能访问公共互联网的 VLAN。在这种情况下，SSID 通常会被公布，以便让访客可以自行找到。用户登录可以通过一个具有吸引力的门户网页完成，这样网络的使用将经过审核，而 且在访客使用服务之前必须同意所有条款。

使用专门的公共安全措施

公共安全应用的敏感性使其需要更高级别的安全性。在紧急情况下，思科统一无线网络能够防止网络被非紧急用户所占用。通过制止非紧急人员对所有 SSID 的访问，可以限制非紧急应用。通过这种方式，在发生危机时，网络的所有信道和带宽都可以专门供公共安全人员所使用。

另外一种永久性的方法是通过为公共安全人员分配一个单独的无线频段，将公共安全通信与市政当 局或者公共用户通信分离开。为了满足在使用 2.4GHz/5.8GHz 无需注册频率时对于加强隐私保护的要求，以及最大限度地减少干扰，FCC 已经授权将 4.9GHz 频段中的一大部分提供给公共安全机构使用。FCC 规定该频段只能供公共安全机构用于保护生命、健康和财产的安全。据估计，该频段的主要应用将 是对突发事件现场的管理，因为在这种场合下需要移动数据和其他紧急应用。

作为一个需要注册的频段，这个频段可以在加强隐私保护和降低干扰方面提供优势¯无需注册的 802.11 频段则无法保障这两点。因为 4.9GHz 产品使用了一个需要注册的频段，未经授权的终端用户连接网络的能力将大为降低。与 Wi-Fi 解决方案不同，4.9GHz 产品不会在零售商店或者 Web 上向普通用户销售。

对于 4.9GHz 频段，最激动人心的一点是管理该频段的法规与工作在 5GHz 频段的无线局域网产品的法规相同。因为只需要对现有的 5GHz 802.11 产品进行微小的改动，所以成本将得以降低，上市时间也将大为缩短，从而有助于充分利用紧缩的预算。

总结

总体而言，思科自防御网络战略可以消除因为无线信号传播和安全威胁所导致的室外无线安全顾 虑。第一步是利用三个基本原则部署有线基础设施，这三个原则分别是：加密通信、威胁防御和策略遵从。思科统一无线网络通过提供专门针对无线介质的、采用了 三个基本原则的安全措施，拓展了思科自防御网络战略的范围。通过为有线和无线网络采用思科自防御网络战略，可以让室外无线网络像让政府职员从远程现场办公 室或者家中办公一样安全。对于高度敏感的公共安全应用，可以通过采用需要注册的 4.9GHz 频段再添加一道防线。该频段可以将公共安全人员的通信与市政机 构或者公共用户的通信区别开来。