跨越安全门槛让企业网络无线更“ 无忧 ” PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/142/2021_2022__E8_B7_A8_E8_B6_8A_E5_AE_89_E5_c101_142885.htm “ 对无线网络而言，安全性仍然是各类公司最关心的头号问题。只有加深对无线局域网安全的了解，并大力推广某些最佳实践经验，才能充分享受无线网络带来的各种便利。只有提高了安全性，使数据安全有了保障，使用者才会放心地使用。 ” Jupiter Research研究主管Julie Ask 前景之争 21世纪伊始，关于“ 无线 ”与“ 有线 ”局域网发展趋势的争论便已开始，迄今为止，这一辩论正有愈演愈烈之势。 积极的观点认为：无线局域网必将取代有线局域网。有关调查机构预计，随着无线局域网的普及，到2009年全球WLAN设备市场收入将增长120%，达到38亿美元规模。同时，分析师们也纷纷对消费级无线应用，最终将影响企业级应用发展的前景表示了乐观态度。原因很简单：当习惯使用移动办公的员工数量发展到相当的规模时，企业将被“ 一次性 ”地推向无线网络。 而不同的观点则坚持：从特性上来说，由于无线网络是通过无线电波在空中传输数据，所以在无线电波覆盖区域内的任何一个无线用户都能接收到这些数据，这显然为信息安全埋下巨大了隐患。因此，无线网络仅能作为有线网络的有效补充，特别是在企业网络的建设中，绝不可委以重任。 可见，随着无线局域网市场、应用整体规模的高速增长，们对于其安全性的担忧始终伴随左右。事实上，这甚至已成为妨碍无线局域网普及的最大障碍之一。 无线安全特性 无线局域网和有线局域网的实现形式迥异，这也就决定了它们有着不同的安全特性。 虽然

在面向Internet的接入时，有线网络于无线网络的安全性问题大体相同，但是，单就网络内部而言，有线局域网面临的潜在威胁要明显小于无线局域网，且技术也更加成熟。因此，前者安全性相对更高。而无线局域网则不然，它一方面要接受来自外部用户的挑战，另一方面，其网络内部还要防范“客人”随时不请自到。“无线局域网遇到的最大安全问题是恶意接入公司无线局域网的外部用户。第二个问题是内部假冒接入点，第三个问题则是加密。”Jupiter Research的研究助理Ina Sebastian说。 其中，假冒接入点的问题在无线网络中比较普遍。比如，在家里使用无线网络的员工可能希望获得与工作地点相同的自由度。他/她可能会购买便宜的接入点，然后在未经允许的情况下将接入点插入网络，这种接入点就称为假冒接入点，大部分假冒接入点都是由员工而不是恶意入侵者安装的。即使是企业批准的接入点，如果配置不当，也可能带来安全风险。 然而，查获假冒接入点并不难，可以使用相应的工具。如果网管人员每天对新的无线接入点实施扫描，就能及早找出假冒接入点。相比起来，实施安全无线局域网加密和验证的解决方案更为关键。 华硕网络设备：完善的加密和验证机制 验证的作用无非是为了最大限度防止非授权用户接入并使用无线网络，唯一的登录名和密码是验证的基础，但也可以利用其它工具提高验证的安全性和可靠性。最保险的验证是在用户与验证源之间执行每用户、每进程相互验证。 而加密则是为了保证数据不被非法读取，而且在接入点和无线设备之间传输的过程中不被修改；加密要求发送方和接收方都拥有密钥，才能对传输数据进行解码。多数安全加密都使用非常复杂的密钥或算法，而且密钥必须定期更

换才能有效保护数据。当然，随无线设备实际采用加密和验证解决方案的不同，必然提供不同级别的安全防护。 目前，华硕网络的无线设备（包括无线路由器、无线AP以及无线网卡）已全面支持WPA和WP2加密技术。并在其无线路由器产品中全部加入了RADIUS服务器认证及NAT/SPI防火墙功能。 支持WPA和WP2加密技术 我们知道，WEP（Wired Equivalent Protection，有线对等加密）是最早在无线网络中使用的加密技术，早期决大多数甚至现在不少无线设备都采用的是这一技术对数据进行加密处理。但由于该协议在制定时相当仓促，所以遗留了很多安全隐患，以至即使不同黑客也可以轻松攻破。所以WEP只能对无线网络提供十分有限的保护。 而华硕无线设备上采用的WPA和WPA2则是Wi-Fi Alliance专为企业、中小企业和小型办公室/家庭办公室无线局域网开发的标准安全认证方法，它能够通过相互验证对每个用户进行验证，是一种先进的加密方法。WPA提供企业级加密，作为第二代Wi-Fi安全特性的WPA2则支持政府级加密。 具有RADIUS服务器认证功能 相对来说，普通用户对于RADIUS会比较陌生。其实，这是个AAA协议，也就是通常所说的认证、授权和计费协议。它也是目前大多数ISP用来认证用户接入的协议。在无线安全方面，RADIUS典型的使用设备的MAC地址，有时候是用户名和密码组合来认证用户，给设备授权和对网络链接计费。由于其需要一台RADIUS服务器，因此一般应用于大单位。对于防止非法用户的接入，使用RADIUS认证非常有用。 提供NAT/SPI防火墙 NAT防火墙虽然和SPI防火墙同为防火墙，但它们的实现途径不尽相同。NAT防火墙是一种常用的网络安全工具，它建立专用网，网内的计算机可以主动

跟外网建立连接、收发数据，但来自外网的连接通常会被阻止。NAT防火墙隐藏了内网上的计算机，保护它们免受外网的入侵和未授权访问，提高了安全性。 SPI防火墙是在外网的数据包进入内网之前先对其进行检查的一种技术。它在默认情况下拒绝所有来自外网的请求，并且通过防火墙的发自内网请求的连接动态地维护所有通信的状态（连接），只有对内网请求回复的连接并符合安全要求的数据包才能通过防火墙进入内网。相比NAT防火墙， SPI防火墙的安全性更高。此外，华硕的无线路由器产品还全部包含了MAC存取控制、IP地址过滤、网域存取控制等多项技术，为用户提供了更完美的存取权限。支持目前流行的DoS检测，保证了防火墙的正常运转。这些华硕无线网络设备所特有的高安全特性和技术联合在一起，为无线局域网提供了全方位的安全保护，让企业用户能够随心所欲地遨游网络。 无线网络安全：明日之光 作为一种新兴的商业工具，无线网络是我们用肉眼所不能看到的。但是，当我们说到无线网络的安全保护时，却绝对不能因为看不到就想不到。因为，对那些希望部署无线网络的企业来讲，安全性毫无疑问是至关重要的。并且，有市场研究公司预计，WLAN还将进一步向教育和医疗等市场挺进。未来WLAN将用作课堂教学工具和用于改进教师和学生之间的沟通，医生也将配备支持WLAN的设备，方便医生在诊断时输入和检索数据。此外，金融和专业服务等垂直市场也将大量采用WLAN.而这些都要基于无线网络安全性的妥善解决才能实现。 就像Infonetics Research的无线局域网（LAN）首席分析师Richard Webb说的那样：“ 为改善安全功能，源厂商们已经作了大量的工作。另外，用户对无线网络的了

解也越来越深入。但是，各种威胁依然层出不穷，各厂商必须继续努力，才能消除人们对无线局域网不安全的误解。”幸运的是，现在无论是用户对安全知识的了解，还是华硕网络这样技术厂商提供的解决方案，都在不断进步当中，且日趋成熟。无线网络已经具有了比较全面的安全功能，及妥善保护，企业能够放心地享受无线网络带来的各种便利再不只是憧憬。