

# Secure Wireless Made Easy – Selecting A Next-Generation Solution for Pervasive WLAN Implementations

*Sponsor: SonicWALL*

*Author: Mark Bouchard*

**AimPoint Group**  
*keeping IT on target*

## Introduction

To date, most organizations are having mixed results with their wireless local area network (WLAN) implementations. Although they enjoy the flexibility and increased productivity that WLANs provide, many businesses remain concerned about security, the cost and complexity of deployment and ongoing management, performance constraints, and the ability to adequately support a modern portfolio of bandwidth-hungry, latency-sensitive applications. In fact, concerns about security in particular are why some organizations have yet to invest in WLAN technology at all.

This paper examines the characteristics of a next-generation solution that helps alleviate the prevailing issues and challenges associated with today's WLAN implementations. The emergence of products that conform to related criteria holds the key to enabling enterprises to utilize WLANs more widely and to having them more fully realize the important benefits that wireless technology has to offer.

## The Wireless Conundrum

There is little doubt at this point that WLAN implementations have the potential to yield a number of significant benefits. The flexibility to continue working from locations where doing so would otherwise be impractical or impossible helps boost the productivity of employees, not to mention on-site partners, contractors, and guests. A richer and more fruitful user experience can drive increased sales and improve customer satisfaction and retention – think retail and professional settings, such as coffee shops, department stores, and the waiting rooms for doctors and lawyers. IT costs can even be reduced, particularly in situations where deploying wired infrastructure would be problematic. And that's just a handful of some of the more obvious examples.

Not surprisingly, the result is that most enterprises have deployed WLANs, *at least to some extent*. The qualification in this case stems from the fact that although IT and business managers alike are interested in more fully taking advantage of the flexibility and other gains WLANs can provide, associated solutions are, unfortunately, not without their challenges. Indeed, common complaints and criticisms include the following:

- Initial deployment is not always straightforward. Access point layout, accounting for AC power distribution, and the configuration of a multitude of remote devices are just a few of the areas that can cause headaches, even for seasoned IT departments.
- Ongoing administration typically involves numerous inefficiencies and complexities. Some of these are simply inherent to distributed technology solutions, while others are due to the policy and control “overlap” that occurs between the different devices that comprise the boundary between an organization's wireless and wired environments.
- Ensuring that the wireless implementation is sufficiently secure – whatever that means – is not straightforward. Security remains a major concern and, very often, is also a point of contention. On one hand, business managers typically fall into one of two diametrically opposed camps: either they are worried that wireless is hopelessly insecure, or they can't understand why IT can't “just do it.” On the other hand, security savvy practitioners realize (a) that WLANs can be adequately secured, but (b) that doing so entails considerably more than simply turning on native authentication and encryption capabilities.

Of course, at the same time there are a number of business and technology trends that are also having an impact. Ongoing and even pending changes are introducing additional considerations that can cause a degree of “analysis paralysis” and/or conflicts of interest when it comes to deciding whether and when to expand the organization’s use of WLAN technology. For instance, some representative scenarios that often arise include the following:

- Business management wants to expand the scope of wireless services to include many more users and applications. However, IT is concerned that the additional load will significantly degrade performance on the wireless network, negatively impacting user satisfaction and productivity. They are also afraid that managing all the associated security policies will become quite onerous and that the resulting complexity will substantially increase the frequency of configuration errors that introduce vulnerabilities.
- To further cut costs, the organization is interested in extending its VoIP solution over the WLAN. Once again, though, there are very legitimate concerns about performance. Is the wireless infrastructure capable of servicing this type of latency sensitive traffic in a way that guarantees adequate voice quality?
- The business wants to forge ahead with 802.11n WLAN technology which should alleviate mounting performance limitations by delivering significantly higher throughput rates (up to 300 Mbps). In this case, however, IT is concerned about compatibility issues, the practical need to support a mix of client types, and the indeterminate but very real performance hit that will occur when 802.11n and 802.11b/g/a technologies are used at the same time.

There are just about as many examples of these issues, differences, and arguments as there are individual companies. The key point to take away, in any case, is that although WLANs have a lot to offer, organizations are generally not using them to the fullest extent due to one or more challenges that the associated solutions continue to present.

## Overcoming Obstacles and Objections

The good news is that the obstacles and objections being raised by most companies are by no means insurmountable. IT organizations can overcome many of the challenges that complicate wireless networking simply by selecting and implementing the right solution for the job. In this regard, when evaluating products emphasis needs to be placed on the ability to address key requirements in the areas of performance, security, life-cycle management, and overall cost and complexity.

### Meeting the Need for Speed

The desire to service larger numbers of users in conjunction with growing utilization of high bandwidth and latency sensitive applications, such as those involving voice and video content, means that support for 802.11n is absolutely essential. Merely having greater throughput, though, is not enough. An ideal solution should be able to preserve this throughput by including capabilities to control if and how different types of clients get access, or to otherwise minimize the performance penalty associated with n/b/g/a co-existence.

Some basic options would be to restrict access to just 802.11n clients or, with dual band/dual radio access points, to confine 802.11n clients to the 5Ghz band, leaving the 2.4 Ghz for use by 802.11b/g endpoints. Other, more innovative capabilities should be sought out as well. Ideally there shouldn’t be any need for a tradeoff, but if there is, then organizations should have sufficient flexibility to strike their own balance between maintaining high levels of performance and supporting a high degree of client compatibility.

In addition to up-front bandwidth preservation capabilities, administrators should also have granular control over how available bandwidth is actually utilized. In other words, an ideal wireless solution should include the ability to allow, deny, and limit use of the wireless network based not only on user, time, and date, but also on the types of applications being used. This way, by throttling non-essential traffic, IT organizations can effectively reserve wireless bandwidth for more important services and ones that are sensitive to latency or latency variation (i.e., jitter).

### **Achieving Air-tight WLANs is Possible – With the Right Tools**

When WLAN technology first came out, security was a pretty big deal. Widely publicized vulnerabilities with the WEP algorithm legitimized concerns about protecting sensitive content as it traversed an inherently accessible medium (i.e., the airwaves). A plethora of articles and dramatic news clips covering wardriving, warchalking, and the challenges posed by rogue access points added further fuel to the fire. As a result, businesses elected either to stay away from WLAN technology altogether, or to deploy WLANs but only with supplemental security tools such as an overlay IPSec VPN, or to invest in non-standard solutions featuring alternative protection mechanisms.

Ratification of the 802.11i standard and introduction of the strong security associated with WPA2 subsequently silenced the critics and, all of the sudden, WLANs were deemed “enterprise ready.” The all-too-common mistake that has occurred ever since, however, is for less-well-informed individuals – pretty much anyone who is not a security practitioner – to attribute greater protective capabilities to WPA2 than it really conveys.

What everyone needs to realize is that WPA2 only addresses authentication (i.e., how users gain access to the network in the first place) and encryption (i.e., how wireless traffic is kept private). Providing comprehensive security for wireless environments actually entails quite a bit more than this base-level functionality, including:

- **Wireless-specific security capabilities** – Also known as wireless intrusion detection/prevention (WIDS/WIPS), these include functionality to prevent rogue access points and clients, to detect and eliminate hacker access points (e.g., evil twins and honeypots), and to help counteract wireless DoS attacks.
- **Countermeasures to thoroughly cleanse and control “allowed” wireless traffic** – These pick up where WPA2 leaves off, providing multiple layers of much-needed protection based on what the traffic actually contains.
  - **Pre-treatment** – This involves network access control (NAC) –oriented functionality, whereby access to the wireless network can be made conditional to the presence and status of the security software and settings on accessing endpoints.
  - **Threat detection/prevention** – This entails “scrubbing” traffic streams for both known and unknown threats/malware using an overlapping – though hopefully unified – array of countermeasures, such as IDS/IPS, antivirus, and anti-spyware technologies.
  - **Application-level identification and control** – It has been well-documented in recent years that network-level security mechanisms are insufficient. To truly be effective, today’s security solutions also require a full range of protective measures that operate at the application/data level, such as the ability to control usage of individual applications, to identify and prevent data leakage, and to prevent the transfer of specific files and documents.

In general, the goal for IT organizations should be to enable a level of security for wireless networks that is at least on par with that which is commonly being implemented today for wired networks. This is certainly a tall order, but not an impossible one. By embedding an extensive array of security capabilities comparable to the ones identified above, next-generation wireless solutions are poised to offer enterprises a very attractive alternative to the current approach – one that typically relies on stitching together a not-so-small collection of standalone tools and products.

### **Much Depends on Management**

The perennial problem for distributed technology solutions is maintenance and management. This is especially true for solutions that are feature/function rich. Accordingly, when evaluating WLAN products enterprises should place particular emphasis on capabilities that simplify not only initial deployment of associated components but their ongoing administration as well. In this regard, having the ability to centrally manage elements of the solution is just a starting point. Other helpful capabilities to look for include:

- Support for POE (power-over-Ethernet), so that access points can be optimally deployed without the challenge, complexity, and cost of extending existing electrical infrastructure to new, sometimes hard-to-reach locations
- The ability to auto-discover new access points *and* then auto-provision them with a centrally defined and maintained configuration
- The ability to centrally obtain, evaluate, and push out firmware updates, including time-sensitive patches
- Robust monitoring and reporting to facilitate troubleshooting, “tuning” of policy and configuration settings, and other life-cycle administration functions

As will be discussed further in the following section, having a single, unified security policy to administer would also be beneficial.

### **The Keys to Minimizing Cost and Complexity**

Overlaying the various technical criteria is the fundamental need to minimize cost and complexity. This is especially true in tough economic times, but also as organizations increasingly suffer from the phenomenon known as infrastructure sprawl. For most enterprises it seems that new “stuff” – applications, servers, and networking and security systems – is always being added to the computing environment, while very little ever gets retired. In any event, a couple of the keys to meeting this objective have already been mentioned. Support for POE eliminates the cost of extending electrical infrastructure. And maintaining backward compatibility for earlier generations of wireless clients ensures maximum utilization rates without having to refresh client systems

Another interesting and *potentially* very beneficial approach to pursue, however, is one that consolidates some of the essential components of a complete WLAN solution. For instance, to enhance the security of their wireless environments, many organizations have chosen to supplement the capabilities native to their WLAN solution – often just WPA2, and possibly WIDS/WIPS – with one or more security products that reside “behind” the Wireless Access Switch/Controller (WAC) that serves as the consolidation point for a given collection of access points. This is usually done with a handful of dedicated firewall, VPN, and IPS gateways, or, more efficiently, with a multi-function unified threat management (UTM) device.

Either way, the best-case scenario still incurs the cost and complexity of purchasing, installing, managing, and maintaining at least two separate devices (i.e., a WAC and a UTM). IT organizations can avoid these penalties however by taking advantage of a next-generation wireless solution that combines the traditional capabilities of a WAC with a full set of UTM countermeasures *in a single physical device*. Such a solution also conveys the benefit of enhancing security even further.

With a unified policy model, it is no longer necessary to re-create object definitions in two management interfaces. Neither is it necessary to manually replicate policies from one device to the next to ensure they remain consistent. The result is increased operational efficiency as well as a decreased likelihood of allowing something to slip through the cracks. Furthermore, intra-WLAN traffic can now be “fully secured.” Traffic from threats that are attempting to propagate, VoIP solutions, and other services that operate in a direct, peer-to-peer fashion get the benefit of a full complement of threat filtering and application identification and control capabilities, as opposed to just a handful of difficult-to-manage access control lists (ACLs) and possibly some basic firewalling – which represents a best case scenario, since many WACs don’t support even this minimal amount of security functionality.

As good as using a consolidated approach sounds, it is important to realize that representative solutions will still fall short if emphasis is placed solely on having a comprehensive set of security capabilities. Indeed, the overall benefits will be eroded unless the solution also incorporates functionality that is at least on par with that exhibited by an average WAC product. Furthermore, the combined device needs to have an architecture that delivers sufficient performance to simultaneously execute all of the advertised security, wireless, management, and other networking functions it supports at line rate and without introducing an unacceptable amount of latency. The primary characteristic to look for in this regard is a purpose-built design, typically featuring a custom operating system and – at least for models with higher throughput ratings – some advanced hardware/ components (e.g., network processors, multi-core processors, and/or accelerator cards).

## Unlocking the Full Potential of WLANs with a Next-Generation Solution

Many organizations have held back on implementing WLANs, at least on a widespread basis, due to the fact that the benefits to be gained are often outweighed by lingering challenges associated with legacy technology, products, and implementation techniques. However, emerging next-generation solutions that conform to the performance and management criteria and which eliminate the need for separate, standalone security devices – as summarized in the table below – are poised to tip the scales. Indeed, such solutions pave the way for businesses of all types and sizes to cost effectively implement highly secure WLANs for the broadest set of potentially beneficial use cases, including within retail stores/branches, manufacturing facilities, warehouses, professional offices, and the enterprise computing environment at-large.

## Characteristics and Criteria that Define a Next-Generation WLAN Solution

### PERFORMANCE

- Support for 802.11n (with throughput rates up to 300 Mbps)
- Throughput preservation mechanisms
- Highly granular bandwidth control

### SECURITY

- Support for WPA2
- Wireless IDS/IPS
- NAC-like functionality (e.g., for antivirus/antispysware enforcement)
- Extensive threat/malware filtering
- Application-level identification and control

### MANAGEMENT

- Centralized, life-cycle administration of access points
- Simplified access point deployment (e.g., auto-discover/auto-provision)
- Support for power-over-Ethernet
- Robust monitoring and reporting

### COST AND COMPLEXITY REDUCTION

- Effective consolidation of security and wireless access controller functionality
- Unified policy model
- Inherent, comprehensive security coverage for intra-WLAN traffic

### About the Author

Mark Bouchard, CISSP, is the founder of AimPoint Group, an IT research and advisory services company specializing in information security, compliance management, application delivery, and infrastructure optimization strategies. A former META Group analyst, Mark has assessed and projected the business and technology trends pertaining to a wide range of information security and networking topics for more than 12 years. During this time, he has assisted hundreds of organizations worldwide with strategic and tactical initiatives alike, from the development of multi-year strategies and high-level architectures to the justification, selection, and deployment of their security and networking solutions. A veteran of the U.S. Navy, Mark is passionate about helping enterprises address their IT challenges.