A Bluesocket® *Bluepaper*

Wireless Gateways: Going beyond VPNs for WLAN security and management solutions

Roaming, Policy Management, and Flexibility in Configuration and Deployment meets WLAN users' needs while avoiding unnecessary load on WAN -oriented VPN resources

Traditional Enterprise VPNs

Virtual Private Networks (VPNs) introduce privacy into public networks. VPNs enable corporate use of the Internet instead of leased or dial-up modem lines. Besides being deployed by enterprises, VPNs are increasingly being offered as managed services by network operators—an area that is especially likely to grow over the next few years.

VPNs can broadly be categorized into three basic types:

1) Remote Access VPNs: These connect telecommuters, business travelers and off-site employees to a company's corporate network providing secure transparent access to business applications.
2) Site-to-site VPNs: These provide branch-to-branch connectivity between distant corporate and regional offices that would typically require traditional networking solutions.
3) Extranet VPNs: These provide external business partners, customers, suppliers and others with network access (like in 1 and 2 above) allowing use of specific applications.

Based on this assessment, and a review of various market reports on VPNs, the fact emerges that most enterprise VPNs are basically being used to deploy secure WAN connectivity solutions. Most enterprise routers being shipped today offer some VPN capabilities. While in some cases, VPNs are replacing existing WAN services, a majority of their success is in newer deployments. Yankee Group, in its report on "Wide-Area Connectivity: WAN and VPN Demand-Side Trends and Analysis", Feb 2002, says, "Vendors of managed WAN and VPN services report that, rather than replacing legacy WAN systems, VPNs are being adopted as complementary adjuncts that connect smaller, newer offices or locations where WAN services cannot be obtained more cost-effectively. The report goes on to show the two technologies (WANs and VPNs) to be complementary.

The Rapid Emergence of Wireless LANs

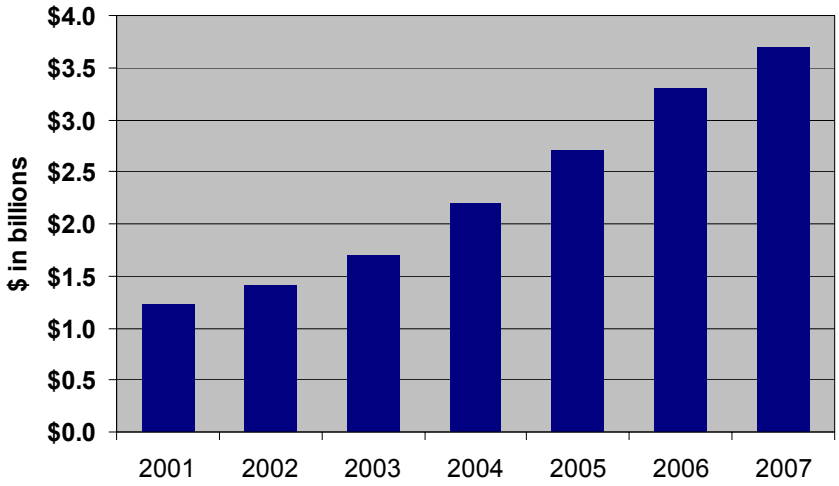
While VPNs have proliferated in the Wide Area (WAN) market, Wireless LANs have rapidly emerged as a cost-effective and efficient networking solution for Local Area (LAN) Networks. WLANs include smaller, peer-to-peer configurations, or larger, multiple LANs that provide the building blocks for high performance, infrastructure networks offering distributed data connectivity with roaming across access points and subnets. WLANs augment rather than replace, wired (Ethernet) networks, providing the final range of connectivity between the core network and the mobile user.

The benefits of WLANs are significant: Mobility leading to increased productivity, simplicity, flexibility, and most important of all in today's tough economic climate—reduced cost of ownership. Common vertical markets for WLANs include Universities, Healthcare, Government, Consulting, Manufacturing, Hospitality, and Public Access (Hotspots). For each of these segments, mobility adds a dimension leading to several direct and indirect advantages for WLAN users and managers.

However, IS/IT Managers deploying WLANs may quickly discover -- as numerous market reports make clear -- that the security feature included in 802.11 standard-based equipment, known as Wired Equivalent Privacy (WEP), is not strong enough to assure users' privacy or repel unauthorized users. In addition to WEP being vulnerable, most Wi-Fi access points do not offer any means to authenticate users before they are granted network access other than MAC addresses which can easily be spoofed. Emerging technologies such as 802.1x and the recently announced Wi-Fi Protected Access

(WPA) security initiative from the Wi-Fi Alliance (formerly known as WECA) have helped mitigate some of the security issues with WEP, but still do not provide for a comprehensive WLAN security architecture, including access control, encryption, and policy-based management. Many VPN vendors and analysts alike recommend VPN solutions to address WLAN security and management issues. Networking vendors are recommending that their VPN switches be used in conjunction with their VPN client software for WLAN environments. Meanwhile, security solutions are being announced for other mobile devices such as PDAs—essentially they are lightweight clients from vendors such as Certicom, Funk, and V-One.

Figure 1. Worldwide spending on WLANs through 2007. Source: Gartner.



So, Are VPNs the Panacea for WLAN users?

On the surface, securing WLAN services may seem like a very similar problem to that of securing remote connections using VPN technology. So why not use a VPN solution, especially if you're already using VPNs to support remote users? While VPNs may solve some problems associated with WLAN security, they are not a panacea for WLAN environments.

Implementing a VPN for securing and managing WLANs presents several challenges. A VPN approach involves deploying VPN Switches or Routers, treating wireless LAN users as remote access users. If you want to use a single VPN switch/gateway to secure all WLAN traffic, all that traffic will need to funnel through the corporate network before reaching the switch, unnecessarily increasing traffic over the corporate (WAN) network. You also need to ensure that all users have appropriately configured VPN clients, very often requiring a software installation on every device, including visitors, guests, or consultants at the premises. Although most Windows operating systems support some variant of a VPN client, not all devices support Windows-based OS'. Many of these non-standard operating systems are incapable of running VPN clients, and are not supported in these VPN-based network implementations.

In a VPN deployment for a WLAN, there is no solution for VPN access while users roam between subnets and require that their applications not be interrupted. Besides this transparent roaming for mobility, WLAN users have other requirements that VPNs don't address. A simple, open solution is sometimes required for temporary visitors or guests without requiring installation of a proprietary client. And there are additional challenges in implementing VPNs for today's WLAN users and emerging mobile devices (such as Symbols' handheld scanners) that work with 802.11 WLANs. Lastly, the security that VPNs provide, typically using IPSec encryption, may not even be needed by some wireless users.

Enter the "Wireless LAN Gateway"

The Bluesocket family of Wireless Gateways (WGs) provides the security, mobility and management functions needed, in a flexible, cost-effective manner, because they are

specifically designed to support the evolving uses of local wireless LAN access. Bluesocket has a simple, single component solution for your wireless LAN needs that brings all the benefits of WLANs without the expense and hassle associated with deploying a VPN.

Whether or not you already have a VPN-based network deployment, Bluesocket's Wireless Gateways are specifically designed for your wireless LAN users and their applications. For enterprises using VPNs, Bluesocket can keep WLAN traffic from interfering with the corporate VPN network – and avoiding unnecessary VPN server and client expenses. Here is a summary of the key differentiators between a VPN switch and a WLAN Gateway:

Figure 2. Differences between a VPN switch and WLAN Gateway using key WLAN parameters

WLAN Application Description	**VPN Switch**	**WLAN Gateway**
Design Philosophy	General purpose security solution	High Performance, best-of-breed solution designed for Wireless LANs
Typical Deployment Scenario	Remote Access; Site-to-site WANs	LAN oriented solution; supports high bandwidth “islands” of users
Mobility	No	Yes; across access points and subnets
Client support	Proprietary VPN client recommended	Proprietary client not required; but can work with several clients
Device Support	Limited number of 802.11 devices—closed solution	Wide range of mobile devices—open solution
Support for Guests, Visitors; Public WLANs	No (with some exceptions)	Yes (e.g., Browser-based log-in using SSL, Transparent Windows log-in)
Traffic Type	Encrypted traffic	Choice of Encrypted and Un-encrypted traffic
Investment Protection/ Future WLAN developments	WLANs are a niche segment for VPN vendors; emerging protocols and features may or may not be supported in future	Focus on WLANs ensures support for emerging technologies and protocols (802.1x, WPA, 802.11i, AP detection and management, 802.11e, 802.11f)
Ease of configuration and management	Complex multi-function deployment of security solution	Simple, elegant solution focused on WLAN security and management

A VPN by itself is not a complete security solution, although most provide end-to-end encryption and double as firewalls. In terms of protocols and technologies, VPNs generally use the Layer 3 IPSec protocol or other Tunneling Protocols (PPTP, L2TP). Typically, a VPN needs to be complemented by other security technologies leading to increased deployment complexity. Some of these technologies include tunneling, encryption, authentication, access control, key management, routing (optional), firewall and intrusion detection.

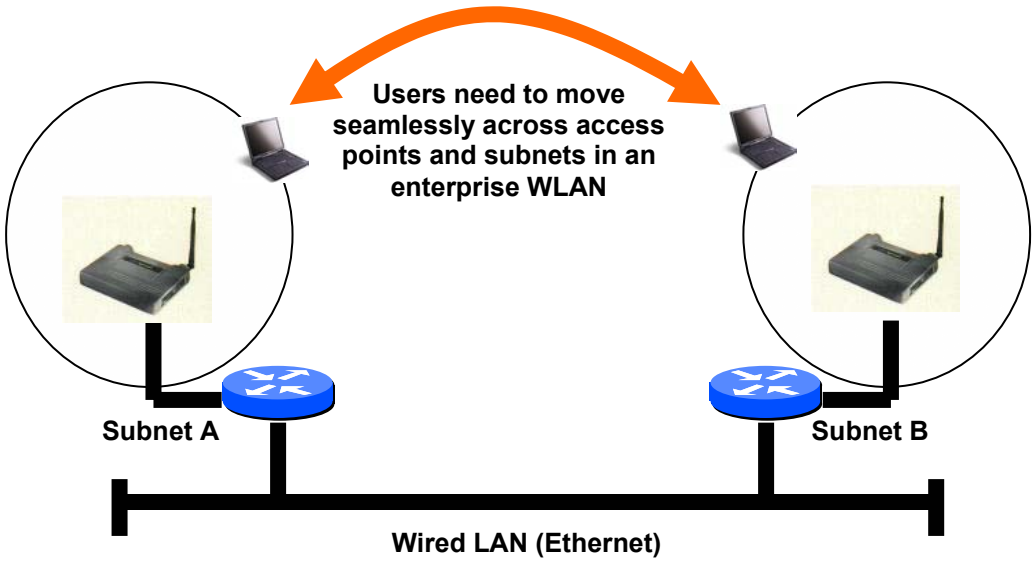
With such a multi-function approach, these VPN products (*aka* VPN appliances) are complex to install and offer varying degrees of performance — much to the dissatisfaction of many network administrators. In addition, to support such technologies in various phases of standardization, many VPN vendors require proprietary VPN client software to reside on each and every network device — increasing the support challenges faced by network managers. Specifically, as it relates to mobility — laptops, tablets, and PDAs — most VPN solutions requiring proprietary clients support

a limited number of mobile devices, making them more of a closed technology, rather than open-ended, standards agnostic security solutions.

While VPNs can provide the necessary security through encryption, tunneling, and firewall capabilities, they don't necessarily address WLANs' additional needs such as roaming, management and flexibility. This isn't a criticism; VPNs weren't designed for use by WLAN users. This is an important fact that needs to be taken into consideration in your WLAN planning. VPNs can play a real and important role in wired network access, for remote access and for site-to-site internetworking. Several users of WLANs have deployed VPN switches for the traditional VPN/wired networks over the wide area—but for WLANs they have decided to go with a Wireless Gateway instead of using the same VPN/Firewall switches.

Like a traditional VPN, Bluesocket's Wireless Gateways can create and maintain a secure IPsec tunnel. And, like the best-of-breed firewalls, Bluesocket's Wireless Gateways also do stateful packet inspection and filtering. Bluesocket also does things that VPNs traditionally don't do -- in particular Bluesocket's innovative patent-pending support for seamless subnet roaming plus flexible support for mobile devices and clients that offers an open, standards-based security solution that can be easily deployed and maintained.

Figure 3. Mobility is a key driver for Wireless LANs. Source: Bluesocket



Chris Kozup of the META Group writes in his paper, "Wireless LAN Security Update":

Deploying LAN based VPNs is not a simple or inexpensive proposition. Many users currently have existing VPN gateways deployed for remote access connectivity. While users may initially be able to leverage these existing products, scalability will quickly become a gating factor. Current VPN devices are capable of terminating anywhere from 40Mbps to 100 Mbps of IPSec traffic (running 3DES with SHA-1 hashing with predominantly small packets)—an amount sufficient for remote access users connected via dial-up or DSL/Cable modems.

VPN Gateways will be less scalable when terminating 802.11b, and more so 802.11a traffic as each user requires 1Mbps – 10 Mbps. With 802.11b networks and basic corporate applications (e.g. email, HTTP), users should plan on a ratio of 200 - 300 users to a single VPN gateway capable of 100mbps throughput. This ratio will decrease to approximately 100 users per 100mbps gateway as the application bandwidth requirements increases or access points migrate to 802.11a. Concerns associated with the VPN approach include the cost of additional gateways ($10k - $50k), lack of ubiquitous client support, limited roaming (due to fixed termination devices), and the loss of management control (due to tunneled traffic).

****

Here's a more detailed analysis of what Bluesocket sees as the limits of traditional remote-access-oriented VPNs when companies try to apply them to WLANs: why VPNs can't solve them, and how Bluesocket's Wireless Gateways are a significant step in the right direction for the rapidly emerging WLAN market:

1. WLAN users may want to roam across subnets; VPNs have limited roaming capability

One of the major benefits for wireless LAN networking is user mobility and the associated flexibility. So it's important to ensure that users can move seamlessly between access points without having to log in again and restart their applications, even where the access points are on different sub-nets.

A VPN can provide a secure wireless LAN connection -- but only through one subnet per session. If a user roams beyond the current Access Point's range, to an Access Point that's on a different subnet, a VPN will need to re-authenticate the user (because they need to be assigned a new IP address) and start a new session.

Using Bluesocket's unique patent-pending Secure Mobility™ feature, Bluesocket's Wireless Gateways allow users' devices to seamlessly roam across Access Points on the same or different subnets -- without any interruption in the session, not having the need to re-authenticate themselves on the network. Bluesocket's Secure Mobility can even preserve a secure IPsec tunnel during roaming across subnets, including among multiple vendors' APs.

2. Proprietary VPN clients are not the only ideal solution for WLAN environments

Many VPNs recommend users deploy proprietary client-side VPN software and/or hardware installed on their computer. This may not be a problem for employees and some regular visitors, but may be for others, interfering with their ability to work productively.

For business partners, consultants and other visitors, requiring installation of a VPN client can be quite a nuisance. Your company has to have appropriate software available for the range of visitors' devices, and visitors need be willing to install new software on their equipment (which may be incompatible with their own corporate networks). Providing VPN capabilities to non-employees also means needing to be able to configure for "visitor" status which cannot access undesignated corporate resources.

This may not be too much of a burden in the traditional VPN environment of a small branch office, but in a wireless network with large numbers of users this can be a major administrative headache. For brief and unscheduled visits, getting VPN clients installed and authorized may not even be feasible.

In comparison, Bluesocket's Wireless Gateways can be used with any computer or mobile device irrespective of operating system, using VPN features that are either included or are readily available. No special hardware or software needs to be provisioned and installed; access — authentication and authorization— is based on the user, not the machine. For business partners, visitors, consultants, etc.—where it is not feasible to install proprietary clients, Bluesocket Gateways offer a flexible mobility solution that is secure. Bluesocket's role-based access control can allow these users to use pre-defined accounts or "roles" such as a "guest" if all they want is access beyond the corporate LAN to the Internet.

3. High bandwidth WLAN traffic could easily swamp VPN switches, including with traffic that doesn't need tunneling/encryption security

VPNs intended for remote/wide-area use are expensive. A typical VPN server capable of handling up to 100 Mbps of encrypted traffic is currently a high-end device and thus an expensive product -- anywhere from $10,000 to $50,000. And in many cases, that does not include the per-device cost of client software.

A single 802.11b Wi-Fi access point -- and companies and campuses can easily have several dozens, even hundreds -- can generate 11Mbps of traffic, and up to 54Mbps for 802.11a traffic. It wouldn't take many active WLAN users to saturate a VPN server, in turn impacting service for remote and local users alike. Quite possibly much of this traffic is web-browsing or other activities that don't require the security of a VPN. And as your WLAN users increase in number, and bandwidth consumption increases, the aggregate traffic in your wireless environment will very quickly increase beyond the limits of your external facing security solution.

With a VPN deployment, irrespective of the type of client being used, encryption is not a choice— although you can certainly choose the type of encryption you deploy. With a Wireless Gateway, you decide on whether you need to run encryption based on the sensitivity of the data, the role of the WLAN user, and also the bandwidth allowed for that user. In contrast with VPNs, Bluesocket's Wireless Gateways are affordable, with a single Bluesocket WG capable of supporting multiple wireless access points. Each WG can accommodate tens, even hundreds of concurrent users (depending on total bandwidth consumption) and virtually unlimited total number of users. Since no special client software is required, the cost is highly controlled, and visitors and other transient users can be accommodated at no additional end-user cost.

Bluesocket's base Wireless Gateway, the WG-1000, supports up to 100Mbps — with all traffic coming from WLAN users on one or multiple Access Points. To support greater bandwidths and more WLAN users, simply add more Wireless Gateways (which can also be used to provide transparent back-up for each other using Bluesocket's exclusive Hot Failover feature). Or upgrade to Bluesocket's next-generation WG-2000, which offers hardware-based encryption acceleration delivering encrypted-data performance up to 150 Mbps; and up to 300 Mbps for unencrypted traffic.

VPN switches/servers are designed to be installed in an organization's central network facility. Unfortunately, all the access points need to be connected directly to this central point for the solution to work. On a large site such as an educational institution, high-tech campus, hospital or a government facility, this can be very difficult to achieve. Depending on the nature of your business, the number of WLAN users can easily spike periodically -- or continue to grow steadily and sharply. Adding more VPN capacity in a timely fashion won't be easy, and it may not be possible to add capacity only in cost-increments that match your user and bandwidth needs.

4. Wireless gateways can reduce user, device management overhead

Setting up and administering VPNs is relatively more complex, and adding new users such as guests, especially for limited privileges, may not be easy or quick to do. Using a VPN for WLAN security and management may require significant modifications to your current network architecture.

Technology consultant Joel Snyder reports in "A flooded field for IPSec-based VPNs is good for users" (Network World, October 1, 2001), "As VPNs move out of pilot mode into implementation, configuration and management of dozens or even hundreds of VPN devices becomes a major issue." In addition, a VPN solution imposes the same high level of security on all users whether or not their applications warrant it. For guests and other visitors, who may simply need access to the Internet, using a VPN can impose an otherwise-unnecessary burden.

In comparison, Bluesocket's Wireless Gateways are easy to manage. Administration is simple, using an intuitive web-based GUI — Bluesocket's systems integrators report that the average time for a basic setup of a WG-1000 is under one hour. Adding and changing users and roles can be done quickly and easily, using Bluesocket's web-based GUI -- and generic visitors can be given a group "guest" password, for negligible visitor administration and zero user configuration. Set-up information for multi-unit installations can be done automatically as any unit can be selected as master and all other units act as slaves, inheriting the user-defined policies on the master unit.

Bluesocket's Wireless Gateways can also share data and integrate with your other existing legacy administrative databases. User information can reside in local or enterprise databases for ease of management. For centralized authentication, Bluesocket supports RADIUS (Remote Authentication Dial-In User Service), LDAP (Lightweight Directory Access Protocol), NT 4 Domain and Windows 2000 Active Directory. A feature unique to Bluesocket is the ability to support transparent authentication using Windows domains or 802.1x, an IEEE standard for port-based authentication. 802.1x uses EAP (Extensible Authentication Protocol) and its many variants to provide user authentication for WLANs. This provides the convenience of a single sign-on for Windows domain, the Wireless Gateway and the Wireless Network.

Conclusion

Traditional VPNs are the solution of choice for remote Internet access to the corporate network and for site-to-site access, but aren't necessarily the most appropriate solution for wireless LAN access.

Bluesocket Wireless Gateways have been designed specifically for the job of securing and managing wireless networks. These gateways employ much of the best-of-breed functionality from security technologies like VPNs and firewalls, and introduce specific capabilities and efficiencies for Wireless LANs-- through a unique architecture, patent-pending technologies and a steadfast commitment to remaining agnostic in order to support the widest range of wireless standards for protocols, services and devices.

Bluesocket's Wireless Gateways give you easy-to-manage, cost-effective control of your wireless LAN environment, and preserve your VPN resources for the remote and site-to-site connectivity applications they're needed for.