RYSAVY
RESEARCH

SECURE WIRELESS NETWORKING USING SSL VPNS

Prepared by Peter Rysavy
http://www.rysavy.com
1-541-386-7475

TABLE OF CONTENTS

Executive Summary

Companies are embracing wireless technologies to increase productivity, provide more flexible work arrangements for their employees, and work more closely with their business partners. Wireless technologies include both local area and wide area systems. However, the multiplicity of networking options as well as computing platforms creates significant security issues, including:

- Different native security options for wireless local area networks (WLANs) than cellular networks.
- An evolving security framework for WLANs and interoperability issues between vendors.
- Outdated WLAN equipment that is insecure.
- The danger of rogue access points.
- Internet traversal for many wireless remote-access solutions.
- Employees using both managed devices and unmanaged devices, such as home computers and public terminals.

The security architecture that addresses all these issues is an SSL virtual private network (VPN), particularly as implemented by Aventail. The company's Smart SSL VPNs provide a means of protecting every node, whether internal or external to the enterprise, leading to the concept of an inverted security model that does not depend on a hardened perimeter. By taking advantage of installed browsers and the associated SSL security layer, companies can not only provide access through computers that have no VPN client software installed, but can also provide additional communications flexibility for systems with dynamically installed software. Aventail® Smart SSL VPNs also provide highly granular access, limiting users to specific application resources.

To go beyond the realm of traditional SSL VPNs, Aventail has also developed the following capabilities to enhance security and to minimize deployment and management costs:

1. **Aventail® Smart Tunneling™.** A full IP network tunnel created over SSL allows any application to function, even demanding ones like those using voice over Internet protocol (VoIP).

2. **Aventail® End Point Control™.** Aventail's Policy Zones accommodate a wide range of remote access scenarios and include items such as inspection of user computers to protect against malicious local software and clearing of caches at the end of sessions.

3. **Integration with Existing Security Infrastructure.** Aventail® Unified Policy™ provides for integration with existing security infrastructure systems such as Remote Authentication Dial-In User Service (RADIUS), Lightweight Directory Access Protocol (LDAP), Active Directory, digital certificates, and two-factor authentication.

Prevalence of Wireless Networks

Many companies are embracing wireless networking technologies to enhance the productivity of their workers, to improve customer service, and even to provide Internet access to visitors. Business travelers are taking advantage of wireless hotspots in public locations such as airports and restaurants, as well as enjoying the convenience of Wi-Fi in their hotel rooms and homes. They are also using cellular networks for communications from almost anywhere.

Although most wireless-data usage has been with Wi-Fi (based on the IEEE 802.11 family of standards), companies are increasingly using cellular-data services, which now offer a near-broadband experience over wide geographic areas. Cellular-data usage includes smartphones, PDAs and laptops with PC Card modems, and laptops using phones as modems by means of a cable or Bluetooth connection. Cellular-data networks encompass multiple technologies, the most prevalent of which today include Enhanced Data Rates for GSM Evolution (EDGE), Wideband CDMA (WCDMA), and the CDMA2000 group of technologies. Despite the alphabet soup of names, they all have a common capability—the ability to support IP-based packet communications from almost anywhere.

Emerging technologies such as WiMAX promise even higher performance over the wide area. Whereas cellular-data networks offer rates approaching 1 Mbps, WiMAX vendors are hoping to provide higher throughput rates.

Many professionals use a combination of Wi-Fi and cellular data networks. Wireless networking not only increases productivity, but it also enhances personal lifestyles—employees can telecommute not just from home but from practically anywhere.

The multiplicity of connectivity options, however, raises significant security challenges for your organization, which needs to secure these connections while accommodating a wide variety of mobile computing platforms, providing a simplified user experience, and limiting access to specific resources, all within a system that can be managed easily.

Security Challenges of Wireless Connectivity

The number one concern expressed by IT managers regarding wireless networking is security. This is justifiable, because radio signals are inherently subject to eavesdropping due to their extended propagation.

Fortunately, there are many effective approaches for securing both Wi-Fi and cellular-data connections. To understand the benefits and limitations of the various approaches, we need to first consider the security issues in greater detail.

Wi-Fi Issues

Initial implementations of Wi-Fi security, called Wired Equivalency Protocol (WEP), were completely inadequate, allowing any determined attacker to easily monitor connections or access the network. A new Wi-Fi security standard, IEEE 802.11i, addresses the security problems of WEP. This standard has come in two iterations: Wi-Fi Protected Access (WPA), which addresses all the deficiencies of WEP, and WPA2, which bolsters encryption by using the Advanced Encryption Standard (AES). IEEE 802.11i is based on IEEE 802.1X, a port-based security architecture where authentication is handled by using Extensible Authentication Protocol (EAP) methods in conjunction with authentication systems such as RADIUS. Most new equipment supports WPA or WPA2, both of which are considered reasonably secure.

A number of issues exist, however, for organizations using IEEE 802.11i for Wi-Fi security. First, IEEE 802.11i does not accommodate older deployed equipment; second, it applies only to access equipment in the organization's control; and third, the complexity of IEEE 802.11i-based security solutions is already raising interoperability concerns among different vendors' equipment.

To fill the Wi-Fi security gap, many Wi-Fi vendors have implemented security enhancements in their equipment. Many of these enhancements have required customers to buy cards and access points from the same vendor. This vendor dependence also applies to new WLAN architectures that employ centralized controllers to coordinate and manage access points. These controllers often include security functions, such as detecting rogue access points and providing VPN tunnel end points. However, any security benefits from these architectures apply only to the directly connected WLAN nodes and do not extend to other connections, such as Ethernet, or to WLAN connections in public places or employee homes.

Cellular-Data Issues

With cellular-data connections, the security issues are somewhat different than for Wi-Fi. For example, whereas Wi-Fi attackers can use normal Wi-Fi hardware for their attacks, cellular-network attackers require specialized equipment to receive and decode the radio signal. The cost of such specialized equipment by itself, however, is not a sufficient deterrent. As a result, some—but not all—cellular networks encrypt the radio link. The general trend of cellular networks is for 3G technologies, with the most current generation of these technologies designed to offer strong encryption based on algorithms such as Kasumi and AES. Even after these next-generation networks are widely available, though, they are still likely to rely on previous-generation technology for coverage in less densely populated areas, where encryption is not always provided. And even if your home operator encrypts the link, you may roam onto a partner network that does not. The bottom line is that you cannot depend on the protection of the radio link.

Cellular-data connections share a common issue with Wi-Fi hotspots. Both primarily offer connectivity to the Internet, and even when they encrypt the radio signal, the IP traffic over the Internet portion remains unprotected. As an option, some cellular operators offer more secure back-end connectivity options to connect from the operator's core network to the customer network, including dedicated frame relay circuits or IPSec-based, network-to-network VPN connections. However, these arrangements incur additional costs, both through initial networking setup fees and then through recurring monthly fees.

Multiplicity of Connections and Platforms

Although it is possible for you to implement specific security solutions for Wi-Fi and for cellular-data connections, each solution will be unique, and managing both is probably not practical.

Another concern is that employees may use a variety of computing devices, including portable computers, smartphones, PDAs, home computers, and public systems. IT will have control over some, but not all, of these devices. Unmanaged devices, including home systems and public workstations may leave the network open to security risks.

Recommended Security Architecture

There is a clear need for a security solution that embraces the world of mobile and wireless computing—with an approach that addresses all forms of connectivity, including Wi-Fi on premises, Wi-Fi off premises, cellular data, public kiosks, home access, and whatever else may become available.

But before you can specify an effective security architecture, there are other important security features that you will probably need, including the ability to:

ß Support both managed and unmanaged nodes as well as accommodate a wide range of device types, including desktops, portable computers, PDAs, and smartphones.

ß Provide granular control to resources, rather than just providing access to a network.

ß Have control over the end-point node to check for proper software configuration such as virus protection, to scan the system for dangerous code, and to clear caches.

ß Allow conformance with government regulations that protect items such as financial and medical information.

The security architecture that meets all of these needs is an SSL-based VPN. SSL VPNs take advantage of the browsers and the SSL security layer that are available for nearly all computing platforms, including notebook platforms, PDAs, and smartphones. Figure 1 shows an SSL appliance securing all forms of wireless access and shows how IP traffic is redirected into an SSL tunnel.

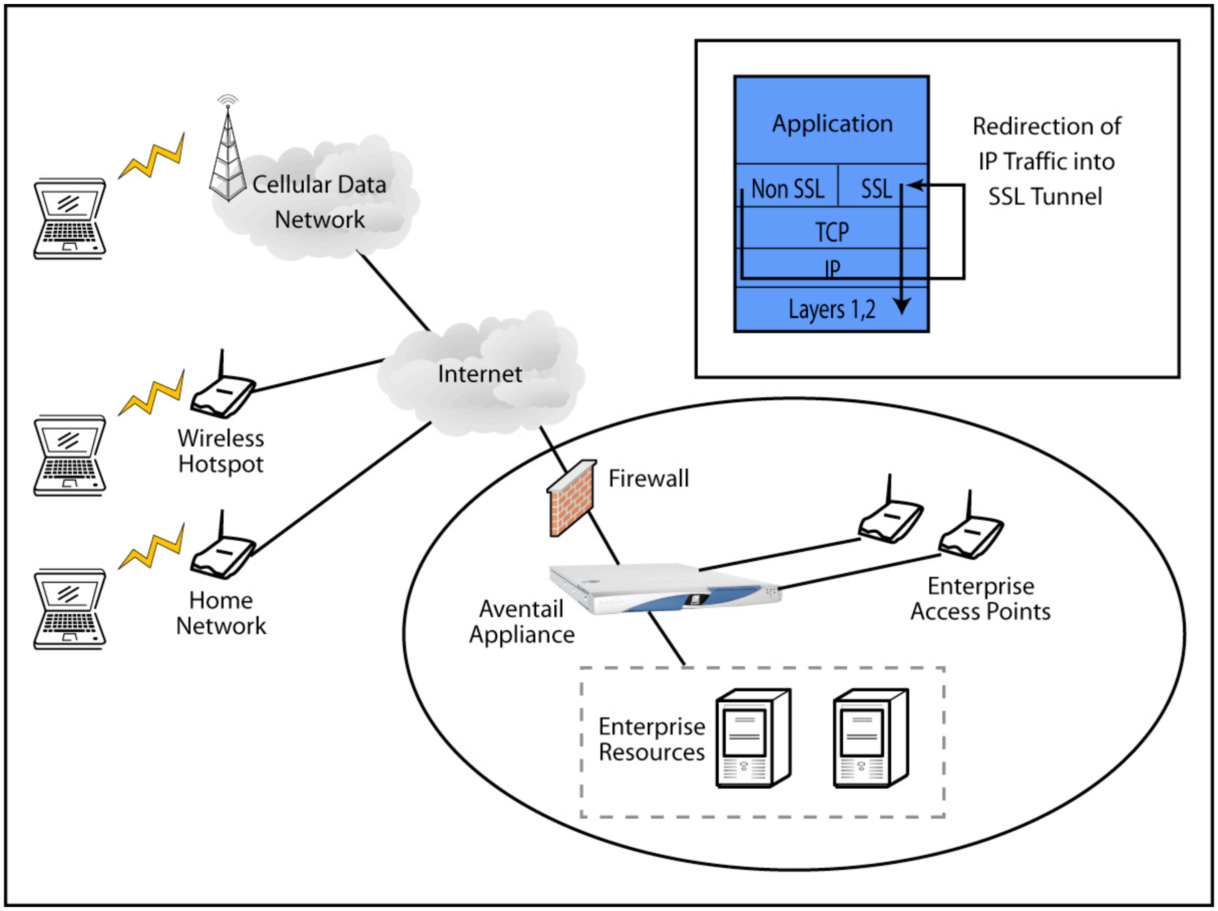

Figure 1: *An SSL VPN can secure both external remote access and internal access.*

Inverted Security Model

Traditional security architectures are based on the concept of a perimeter, where firewalls mediate between nontrusted external networks and trusted internal networks. However, this model breaks down when a significant portion of your employees reside on public networks. The perimeter model also falls short when your network needs to allow select access by contractors, business partners, and customers.

The inverted security model assumes that you trust no node, whether internal or external. It shifts the emphasis to granular identity and access management. SSL VPNs enable this model by providing strong control of end points, strong user authentication, access to predefined resources, data integrity, nonrepudiation, and detailed auditing. By restricting access at the application layer, SSL VPNs shift security management from the network domain to the user domain.

SSL VPNs Compared with Other Approaches

Forrester Research[1] sees SSL VPNs as becoming the dominant remote access solution: "By breathing new life into secure mobility and remote access, SSL VPNs will experience significant growth as both vendors and service providers mature their offerings. This growth will continue and Forrester expects SSL VPNs will enjoy dominant market share by 2008." Meanwhile, wireless connections are becoming the favored form of remote access.

The reasons for using SSL VPNs are clear. SSL VPNs provide trusted and proven data confidentiality, multiple user authentication methods, control over accessed applications, the greatest flexibility in platform types, and the ability to secure any connection, whether external or internal, thus fully protecting against the security risks of wireless networking.

IPSec-based VPNs will continue to be used but have a better fit for network-to-network connections. As for other wireless security approaches, there are a variety of secure application-specific solutions, such as the RIM Blackberry. These are highly optimized for specific applications such as push e-mail and calendar synchronization, with some support for synchronization of other mobile data. They are not, however, general-purpose networking solutions like SSL VPNs. In some cases, your SSL VPN can obviate other mobile platform security solutions, whereas in other cases, you might want to use both approaches. Table 1 summarizes the aspects of different security approaches.

Table 1: Summary of Pros and Cons of Different Security Approaches

Type of Security Solution	Pros	Cons
IEEE 802.11i Security Standard	Comprehensive security framework for Wi-Fi security.	Available only in corporate settings. Does not address other wireless connections such as cellular. Does not support outdated hardware. Vendor interoperability issues.
Cellular Data Security Mechanisms	Primarily designed to protect operator from fraudulent use. Many networks, but not all, encrypt the radio link.	Only a partial security solution, and only if operator offers data encryption. Normal configuration has data passing the Internet in the clear. Does not address other wireless connections such as Wi-Fi.
IPSec VPN	Mature and available from multiple vendors.	Requires client code. Not necessarily available for all mobile platforms. Optimal for network access, not application-level access.
Wireless-specific VPN	Efficient for wireless networking.	Specific to wireless networking and not necessarily applicable as a comprehensive enterprise security framework.
Application Specific Solutions (e.g., Wireless E-Mail)	Efficient for wireless networking. Limits access to specific resources.	Requires client code. Limited to small application base such as e-mail, calendar synchronization, and contact databases. Not a general-purpose, remote-access solution.

[1] Forrester Research, SSL Is The Future Of Remote Access VPNs, June 2004

Type of Security Solution	Pros	Cons
SSL VPN	Efficient for wireless networking. Enhanced features such as persistent sessions can address wireless challenges. Secures all forms of connections, whether WLAN, cellular, or other. Provides the greatest degree of control over access to resources. Greatest client flexibility between browser, browser with agent code, and full client version.	Not yet as widely adopted as IPSec VPNs. Market still evolving.

Capabilities of the Aventail SSL VPN

Aventail is a market leader in SSL VPNs. Aventail SSL VPNs support a full range of access options, giving users secure anywhere access to applications from nontrusted, semitrusted, and trusted Internet-enabled devices—everything from public workstations to corporate-managed computers. By offering broad access methods, support for multiple platforms, and granular policy management with advanced data protection and remediation, Aventail enables companies to extend secure access to more applications and resources while using more networking methods, such as wireless networking, at a low total cost of ownership.

Aventail's proven SSL VPN adds a layer of security and control that complements wireless architectures. An Aventail SSL VPN appliance can provide a secure gateway between your wireless or other remote access network and your internal network. It provides strong SSL-based encryption, user-level access control, and stringent user authentication, including RSA SecurID tokens and digital certificates.

Aventail SSL VPNs work over any IP network, including Wi-Fi and cellular-data networks. Because the Aventail appliance creates an encrypted and authenticated SSL connection at the application layer of the network protocol, it secures your network, independent of the wireless connection at the link layer and even if all embedded Wi-Fi security features are disabled at access points. This is a likely scenario when the session is initiated from an employee's home or a public hotspot.

Aventail SSL VPNs provide granular access control to administrators, while providing a transparent access experience to authorized users. Sheltering your internal network domain name system (DNS) and network topology from wireless users reduces the risk of unauthorized access or attacks on your network resources. With granular access control, you can limit access based on parameters like source (IP address or host name) and port, destination, user identity and/or group affiliation, time and range, day and/or date, application and/or service, authentication method and/or encryption algorithm, and URL-level access. This additional protection of your wired network is precisely what you need to confidently provide remote access to the corporate network.

For more complete protection, Aventail has partnered with several vulnerability-assessment vendors to proactively verify your network and application security, helping protect your sensitive information assets even further.

Additional features and technology built into Aventail Smart SSL VPNs include Aventail® Smart Access™, Smart Tunneling, End Point Control, and integration with existing security management infrastructure.

Aventail Smart Access

Aventail Smart Access automatically determines and deploys the right remote access method, so your users don't have to think about how they access any of the corporate resources that they need. Aventail offers options that handle every access possibility, giving you granular access control, split-tunneling capability, and the NAT and firewall traversal necessary for truly secure everywhere access. In addition, by using Aventail Smart Tunneling technology, Aventail Smart SSL VPNs provide users with extended application reach, including support for UDP, TCP, and IP protocols, as well as back-connect applications such as those using VoIP.

Flexible access methods include the following:

ß Aventail® WorkPlace: Aventail offers users secure, clientless access to internal Web applications, file shares, and client/server applications from any Web browser through Aventail's personalized, policy-driven secure access portal. Behind the scenes, Aventail Smart Access automatically chooses and deploys the most appropriate access method in a manner that is transparent to the end user. For example, when a user needs to access thin-client applications such as Citrix or client/server applications such as Microsoft Exchange, SAP, and Lotus Notes, Smart Access automatically deploys the Aventail® OnDemand™ client to whatever device is being used, eliminating the need for a manual download or additional actions for the user.

ß Aventail® Connect™: Aventail Connect is a Web-delivered Microsoft Windows client that provides authorized users with secure access to any resource on the corporate LAN. Although it does require an initial download, Aventail Connect is not a traditional VPN client. It provides the same "in-office" experience as Aventail WorkPlace with an even higher level of transparency and simplicity for users, so they gain unlimited mobility and complete integration with the Windows desktop.

Aventail Smart Access works hand-in-hand with Aventail Unified Policy, allowing all access methods and resources to be managed in one centralized management location. Another feature of Aventail Smart Access is persistent sessions. These sessions allow the user to move from one access method to another without losing the network connection, which is particularly useful in mobile and wireless environments.

Smart Tunneling

Aventail Smart Tunneling technology allows full IP network tunnels to operate over SSL, advancing SSL VPN capability to new levels and outperforming virtually all other SSL VPNs. Most importantly, Smart Tunneling makes any application function—an improvement over the limitations of previous SSL VPNs.

Aventail Smart Tunneling allows controlled access directly to an application, with access rules set by policy management that determine the opening of the tunnel. In other models, tunnels are always open, but with Aventail Smart Tunneling, the tunnel is closed until it is dynamically opened to a specific application based on access rules and the security of the end device.

Aventail's technology interrogates the end device to capture vital information about the IP address and routing information used by that access network; it then detects and resolves any potential conflicts and assigns IP addresses accordingly. Aventail Smart Tunneling then transparently routes IP packets with no interference or address conflict.

Aventail Smart Tunneling is not a PPP tunnel like some other SSL VPN solutions. PPP tunnels still have network reach limitations as well as IP addressing challenges. With alternate approaches such as IPSec, policy and security controls are difficult to set and do not provide strong authentication provisioning.

Unlike IPSec or other solutions, Aventail Smart Tunneling technology provides the SSL benefits of firewall and NAT traversal as well as granular policy management.

The Aventail OnDemand client and the Aventail Connect client, described in the prior section, are also available in combination with Smart Tunneling.

End Point Control

Vulnerabilities in Windows and the insecurity of wireless networks increase the potential for breaching a wireless network, unless its networking and sharing settings are properly configured. Public kiosks connected over WLANs are particularly susceptible.

With Aventail End Point Control (EPC), you gain the strongest SSL VPN policy enforcement available today. By using EPC, you can enforce policy based on the level of trust that you have for the user's environment—whether it's wired or wireless—as well as for the user. By using Aventail's technology to manage access by environment and using the technology of Aventail partners to make those environments safer, you can truly deliver secure anywhere access over any network.

With Aventail EPC, you'll be able to set highly granular access control policy that goes beyond "on" and "off" access, so users can get varying degrees of access depending on their environment. With Policy Zones, you can create up to 10 zones that accommodate myriad remote access scenarios. Aventail's partners enforce policies for firewalls, intrusion detection, virus protection, and other client-side security issues, while Aventail encrypts and authorizes access to all corporate resources with access control policies based on the user's identity and the security of the user's environment.

Integration with Existing Security Management Infrastructure

Aventail Unified Policy offers centralized administration with one rule set for all resources and access methods. Aventail Smart SSL VPNs integrate easily with your existing information security infrastructure, including authentication and authorization systems including RADIUS, LDAP, Active Directory, digital certificates, and two-factor authentication such as RSA SecurID or other tokens. Essentially, by taking advantage of the directory and security components that your remote access users probably are already using, you save on end-user training and support, lower your administration and management costs, and reduce IT headaches.

By deploying an Aventail Smart SSL VPN today, you can immediately make your wireless connections more secure while gaining vendor independence. Aventail SSL VPN solutions work across all wireless networks by using a single, integrated infrastructure that secures remote access over your wireless connections as well as all the other networks that your employees, business partners, and customers will encounter. With Aventail, you will gain a clientless, enterprise-ready solution with proven security and easy anywhere access to more applications from more places—including risky environments like Wi-Fi hotspots.

Conclusion

Although Wi-Fi technologies have significantly improved their security capabilities, many of the features and abilities are available only in newer equipment for IT-managed infrastructure. Meanwhile, cellular-data networks rely on a completely separate security architecture that emphasizes protection of the radio link and does not provide end-to-end encryption.

By using an SSL VPN, you can secure all forms of wireless communication, both externally and internally. Moreover, this approach accommodates a wide range of user equipment. With Aventail SSL VPNs, you obtain significant additional benefits, including use of almost any networking application through Smart Tunneling, a high degree of control over user equipment with End Point Control, and effective management and integration with existing security management infrastructure through Aventail Unified Policy.

Not only does the Aventail SSL VPN make a great deal of sense for securing wireless connectivity, but it also lays the foundation for the extended enterprise based on an inverted security model where the security architecture controls user access centrally, providing granular access to resources. The resulting flexible network supports both workers and business partners, allowing organizations to reach their full potential in efficiency and competitiveness.

About Aventail

Aventail is the leading SSL VPN product company and the authority on secure application access technology. Aventail delivered the first SSL VPN solution in 1997. And today, Aventail meets the secure communication needs of more than one million end users globally. Aventail's family of SSL VPN appliances increases productivity for end users and IT professionals, while maximizing security and lowering costs. Aventail appliances lead the industry in End Point Control, policy management, and transparent, easy-to-use access options to the broadest range of applications. Aventail is the SSL VPN of choice among leading enterprises and service providers worldwide, such as AT&T, DuPont, IBM Global Services, MCI, Office Depot, Sanyo, and TNT. For more information, go to www.aventail.com.