

Options Expand for Data Transmission Security

BY J. SHARPE SMITH, EDITOR

As the automation of sales and service personnel has grown, secure communications from wireless handheld computers to company back offices has become more and more of an issue. There is more than one answer to keeping your company's information and transactions secure while you are on the road, including: encryption protocols, virtual private networks and private networks. Additionally, a new service where the private network can be outsourced to a third party has expanded those options.



it just doesn't work because it makes the system slower than a dial-up."

According to a White Paper by the Wi-Fi® Alliance, weaknesses have been identified in WEP. Even with WEP enabled, an intruder could easily gain unauthorized access to the wireless network via the WLAN. As a result, enterprises found it necessary to supplement WEP with third-party security solutions such as VPN, IEEE 802.1X authentication services servers, or add-on proprietary technologies.

The first and simplest level of security is the Wired Equivalent Privacy (WEP) encryption protocol, built into wireless enabled portable computers. The security mechanism for wireless local area networks (WLANs) uses the Institute of Electrical and Electronics Engineers' 802.11 specification. It is very easy for an unauthorized 802.11 wireless computer coming within range of another 802.11 device to join the network unless its WEP encryption is enabled. WEP is secure enough for most homes and businesses, but can be hacked, according to HomeNetHelp.com, a home networking and Internet sharing site.

Along with being less secure, WEP will also slow down the wireless network from 20 percent to 50 percent reduction depending on the products in use. "The speed issue is often the result of an access point without enough processing power," says HomeNetHelp.com. "A full strength 802.11b signal will get you about 3.5-4.5 Mbps without WEP enabled. With WEP enabled, expect 2.5-3.5 Mbps."

Whatever the means of encryption is, it is going to take up a lot of bandwidth," says Shelly Greco, spokesperson, IDC Global. "So when they are using their applications, which can be bandwidth hogs themselves,

To address this situation, the Wi-Fi® Alliance introduced two new interoperable Wi-Fi security specifications for both enterprise and home networks.

In 2003, the Wi-Fi Alliance introduced Wi-Fi Protected Access (WPA™). It was designed to be a strong, standards-based interoperable Wi-Fi security specification that would provide enhanced data protection and ensure that only authorized users may access the users' networks. WPA uses Temporal Key Integrity Protocol (TKIP) for data encryption.

A year later, the second generation of WPA security was introduced by the Wi-Fi Alliance, known as Wi-Fi Protected Access 2 (WPA2™). Like WPA, WPA2 provides enterprise and home Wi-Fi users with a high level of assurance that their data will remain protected and that only authorized users can access their wireless networks. WPA2 is based on the final IEEE 802.11i amendment to the 802.11 standard ratified in June 2004. WPA2 uses the Advanced Encryption Standard (AES) for data encryption and is eligible for FIPS (Federal Information Processing Standards) 140-2 compliance. You can find out more about deploying WPA and WPA2 at the Wi-Fi Alliance's web site: www.wi-fi.org.

Virtual Private Networks

As the Internet has become more accessible and bandwidth capacities have grown, according to an Adtran White Paper, "Understanding Virtual Private Networks." companies began to offload their Intranets to the web and create what are now known as Extranets to link internal and external users. But no matter how cost-effective the Internet is, there is one fundamental problem to this approach – security.

VPNs gain their security through the use of tunneling technology, which encrypts and encapsulates network protocols within the Internet protocol. The user can route and bridge, enable filters, and deploy cost-control features the same way as with other traditional wide area networks. The Internet-based VPN transmission is transparent not only to the users, but to network management operations, as well.

"Using the Internet, companies can connect their branch offices, project teams, business partners and e-customers to the main corporate network. Mobile workers and telecommuters can get secure connectivity by connecting with a local Internet Service Provider. With a VPN, corporations see immediate cost-reduction opportunities in their long distance charges, leased line fees, equipment inventories (like large banks of modems), and network support requirements, Adtran continues. For more information, visit www.adtran.com.

Private Networks

Private Networks may be the most secure of all the options, because they provide the business mobile worker with a secure, direct connection to the corporate network without exposure to the Internet. PNs are fast, requiring less encryption, but owning and operating your own PN requires leasing phone lines and other equipment, which makes it expensive.

IDCGlobal has designed Secure IP in Motion™, which is designed to provide all the pluses of a private network, speed and security, without many of the expenses of owning and operating a PN. Once the signal has gone from the computer to the cell site, it

traverses the same secure network used by the telephone carriers. Without the VPN Overhead and Internet Overhead, the private network uses less encryption, which translates into faster speeds, the company says.

Another plus of private networks is simplicity. "With a VPN, there are so many elements that could be problematic. If the system goes down, you have to ask whether it is the DSL or cable line or the box that supports it. Is it the VPN? Is it the security that my company provides? With Secure IP in Motion, you have the wireless data card and you have our network. That's all. We are the single point of failure and the single point of contact in the network architecture," says IDCGlobal's Greco.

According to Greco, outsourcing the private network may not be that much more expensive than owning and operating a VPN. Not only is there the cost of the hardware and software of a VPN, but there is the expense of the day-to-day support and upkeep, none of which are incurred when the management of the PN is outsourced.

"IDCGlobal — through our carrier network interfaces, owned and operated data centers, and proprietary switching fabric — has designed a network to provide Quality of Service across multi-vendor networks and "last mile" technologies," says Greco. "Our customers can deploy and prioritize voice, data, multimedia and Internet over the same physical connection." For more information, visit www.idcglobal.com.

Conclusion

Of course, there are other methods of keeping your data safe, such as firewalls that monitor network access requests. Software is available to combat viruses, spam, web bots and spyware, as well other harmful content. Undoubtedly new defenses will be invented in the future to combat the perennial problem of maintaining security. The choices of WEP, VPN or PN have now been expanded by IDCGlobal, which provides users the opportunity to outsource the management of their private networks with a network that it manages and monitors, end-to-end, around the clock. □