



# GOING MOBILE, STAYING SECURE

**BUSINESS RESILIENCE IS REINFORCED WHEN USERS CAN SECURELY CONNECT FROM WHEREVER THEY ARE**

**H**ow can enterprises remain productive and competitive in the face of changing—and often unpredictable—business conditions?

This question is on the minds of many IT managers today. One reason is that businesses worldwide witnessed unprecedented economic changes and disasters this past year. As a result, IT departments are building extra measures of business resilience into their computing, application, and network infrastructures.

Today, enterprises are discovering that in addition to mirrored data centers and network backup systems, mobility is becoming a key component of business resilience. Empowering users to remain productive wherever they are located keeps businesses agile and competitive as they decentralize their operations and scatter employees among headquarters, branch offices, and home offices, and while users spend increasing amounts of time away from the office on business travel.

“If users do not have access to all their productivity tools when they are away from their desks, this is a missed opportunity to push a business forward,” says Charlie Giancarlo, senior vice president of technology development at Cisco Systems. Cisco helps businesses address this challenge with the Cisco Mobile Office, a set of solutions that empowers IT departments to provide secure, high-speed connectivity to mobile users.

One example of mobility as it relates to business resilience is the impact that new security regulations in the airline industry have had on the traveling public. Business travelers now find themselves with significantly more “down” time in airports. If equipped with wireless LAN

client adapters and secure virtual private network (VPN) client software in their portable computers, these users have the ability to leverage emerging public wireless LAN services to remain productive. In addition, hotels and conference centers are also offering both wireless and wired Ethernet services for connecting mobile users to their corporate resources via the Internet.

“Similarly, if a natural disaster or weather conditions prevent employees from getting to a physical workplace, users who can connect securely from home can also keep the business moving without much interruption,” says Giancarlo.

## THE THREE FLAVORS OF MOBILITY

Users become mobile when they leave their wired LAN connections and roam elsewhere with their laptops and handheld data devices. From there, they might switch to a wireless LAN connection as they join a meeting down the hall or work from an airport. Or they might plug into another wired broadband connection from home or a hotel that offers wired Ethernet services.

Through the Cisco Mobile Office, Cisco offers the networking tools that enable IT managers to support these different types of connections. With these liberating capabilities, though, emerge fresh security challenges, particularly in the wireless sector. Successfully addressing security is critical to maintaining business resilience.

Here, we’ll examine how the Cisco Mobile Office enables both wireless and wired mobility for business customers while solving the security challenges associated with them.

**AT WORK: WIRELESS LANs**

The Cisco solution for mobility within the enterprise centers around the Cisco Aironet® wireless LAN system, which includes the Cisco Aironet 1200 Series dual-mode access points for both IEEE 802.11b (11 Mbps) and 802.11a (54 Mbps) networking, client adapter cards, and the Cisco Access Control Server for authentication.

Wireless LANs deliver the freedom to work virtually anywhere within a building or around a corporate campus without the limitation of wires or cables. People in a conference room can access information needed to make decisions, for example, rendering meetings more productive. Moreover, wireless networks can serve as a cabling replacement to overcome business limitations created by older buildings and temporary work areas.

Evidence of the potential impact of wireless LANs on user productivity was revealed by a study conducted last fall by NOP World – Technology, a research company that surveyed more than 300 U.S.-based organizations with 100 or more employees using wireless LANs. The study showed that wireless LAN technology allowed users to stay connected for an additional 1.75 hours each day, which increased their productivity as much as 22%.

**SECURITY AT WORK**

Despite the significant productivity-enhancing potential of wireless LANs, many enterprises have been hesitant to fully embrace them, largely because of security concerns. These worries were fueled by reports last year that the basic security algorithm in the IEEE 802.11b wireless LAN standard is easy to crack.

These vulnerabilities have since been overcome by the security enhancements in Cisco Aironet products. The Cisco Wireless Security Suite, which includes reinforced encryption and authentication, makes it possible for IT departments to untether users without sacrificing network security.

Sharp Healthcare, a regional healthcare delivery system based in San Diego, California, for example, uses Cisco Aironet wireless LANs to improve patient care by enabling bedside care-givers to access patient data records, order lab tests, and issue pharmaceutical prescriptions. Without the Cisco Aironet



enhanced security measures, Sharp would be hard-pressed to meet the stricter standards for patient confidentiality recently mandated by the Health Insurance Portability and Accountability Act (HIPAA), comments Mark Weisenberg, Sharp's director of network services.

"The HIPAA requirements have a direct bearing on wireless data transfer, and we needed absolute certainty that we were not going to put patient records in jeopardy with our wireless system," he says.

What are the security risks associated with wireless net-

works? In general, enterprises must protect themselves from unauthorized individuals gaining access to corporate servers or "stealing" data in transit. They also need to guard against denial-of-service attacks on corporate Web servers, which clog them up with bogus service requests and prevent user and customer access to data and services.

These vulnerabilities exist in wired networks, too, but wireless LANs open an additional exposure that must be addressed specifically, because radio signals can penetrate walls. If the proper security mechanisms are not in place, someone outside a building but within range of an access point could circumvent the firewall and hop onto the enterprise network.

Today, enterprises using wireless LANs have deployed four distinct forms of security: open access (no security), basic security, enhanced security, and specialized security. The primary reason some enterprise installations have no security is that, in accordance with IEEE 802.11b specifications, systems ship by default with basic encryption disabled, and companies are not turning it on. Even when these features—called Wired Equivalent Privacy (WEP)—are activated, though, the static nature of the WEP encryption key still leaves companies at risk. Static encryption keys rarely change, leaving hackers plenty of time to decode them.

The Cisco Wireless Security Suite enables both enhanced and specialized security to overcome static WEP vulnerabilities for enterprise-class protection. Within the enterprise, enhanced security is recommended, while specialized security in the form of a VPN based on the IP Security (IPSec) standard is appropriate for users on the road.

For enhanced security within the enterprise, Cisco

has expanded the industry-standard Extensible Authentication Protocol (EAP), which fits into the IEEE 802.1x-standard authentication framework, to create an authentication algorithm called EAP Cisco Wireless (also called "Cisco LEAP"), which enables per-user, per-session authentication. Cisco products also support dynamic encryption keys and a pre-standard version of Temporal Key Integrity Protocol (TKIP), which adds per-packet keying, fast rekeying, and message integrity checks to 802.11 security. Together, these capabilities make sessions nearly impossible to hack.

To guard against wireless-initiated denial-of-service attacks, EAP Cisco Wireless supports mutual authentication. "In addition to the user being authenticated, the access point to which the client is connecting must also be authenticated," explains Pejman Roshan, Cisco technical marketing engineer. "This prevents unauthorized access points from being set up inside buildings, from which someone could launch denial-of-service attacks onto a corporate Web server."

#### **ON THE ROAD: PUBLIC LAN SERVICES**

Users who spend a substantial amount of time on the road have an increasing array of connectivity options. As mentioned, the availability of wireless LAN services for high-bandwidth access to the Internet is proliferating in airports, convention centers, public hotel areas, restaurants, and coffee shops. Wired Ethernet connections are also becoming available in hotel rooms and other locations.

The property owners and service providers supplying these services to enterprise users can deploy them using infrastructure equipment made by Cisco. For example, hotels can run Cisco switches that support Cisco Long-Reach Ethernet technology to support multimegabit-speed connections in guest rooms wired with older Category 1/2/3 telephone wiring. Similarly, Cisco wireless access points can be installed in public venues to enable open-access wireless LAN connectivity to the Internet.

All traveling business users need to use these services are the appropriate client adapters in their portable computers to access these wired or wireless networks. As mentioned, VPN client software is also highly recommended for security.

What about handheld devices? Presenting content on small displays necessitates a transformation function to reformat the HTML and XML content residing in corporate Web servers that has been tuned to

desktop-sized displays. In addition to performing markup language translation (such as HTML to WML), it is important to deliver the right subset of data to the requesting device. The Cisco CTE 1400 Series Content Transformation Engine, for example, front-ends an organization's Web servers to transform content for display by a variety of mobile devices using default or customized rules.

#### **SECURITY ON THE ROAD**

When users connect to their corporate networks from the road, IPsec VPNs protect against hack-attacks on remote-access connections. IPsec VPNs have two components: client software that resides in the user's mobile computer and a security gateway at the corporate site, such as the Cisco VPN 3000 Concentrator. Encrypted tunnels run between the client and the gateway, which terminates the tunnels and decrypts data.

For public wireless LAN services, IPsec VPNs are especially encouraged. Access points in these loca-



tions generally run with their vendor-specific security mechanisms disabled to encourage open access to all potential users. Since the radio signal does not have any physical security associated with it, strong encryption in the wireless access network, supplied by the client VPN software, prevents hackers from stealing data out of the air.

#### **AT HOME: BROADBAND ACCESS**

The mobility component of business resilience includes corporate teleworking programs, which let employees work productively from home. According to a 2000 survey by Kinetic Workplace, U.S. companies with teleworking programs saved approximately \$12,000 a year per teleworker and also reduced real-

estate costs as much as 60%.

Workers at home require secure, high-speed connections to their corporate networks. Sometimes the access services available in the various employee locations differ, so a company might need to support a mix of ISDN, DSL, cable modem and other broadband connections.

Cisco has a variety of broadband access products for at-home workers. For example, the Cisco 806 Broadband Gateway Router connects to any type of high-speed access connection through an Ethernet WAN port. So while an organization may not be able to standardize on the type of broadband network service used by its teleworkers, it can standardize on a single equipment platform.

**SECURITY AT HOME**

IPSec VPNs again come into play for securing connections from the user's home site across the untrusted public Internet to the corporate VPN gateway. There are several equipment options for teleworker security; the choice often depends on the equipment available from the service provider.

The Cisco 827 Router, for example, has built-in security, including stateful-inspection firewall capabilities and VPN support with IPSec 3DES encryption. There are other security options as

well, including the Cisco PIX® 501 Firewall and the VPN 3002 Hardware Client. To ease the administration of corporate teleworking programs, central IT staff can use special software that distributes predefined security policies out to large numbers of Cisco 800 Series routers and security appliances.

**EMPOWERING THE ENTERPRISE WITH MOBILITY**

Because of the enhanced capabilities now available for securing connections across untrusted wireless networks and the public Internet, enterprises can embrace mobility as a key component of their business resilience strategies. This empowers companies to keep business processes going when users are away from a traditional office workspace with a wired connection to the corporate network. Employees who can get connected both within and outside of the corporate walls are employees who stay productive and, as a result, increase their companies' competitive power.

**FOR MORE INFORMATION**

[www.cisco.com/offer/mobileoffice](http://www.cisco.com/offer/mobileoffice)  
[www.cisco.com/offer/aironet-security](http://www.cisco.com/offer/aironet-security)  
[www.cisco.com/offer/security](http://www.cisco.com/offer/security)  
[www.cisco.com/offer/hotspots](http://www.cisco.com/offer/hotspots)

**SECURE ENTERPRISE MOBILITY SOLUTIONS FROM CISCO**

Mobility Application	Product	Description
At Work	<i>Cisco Aironet 1200 Series Access Point</i>	Dual-mode 802.11a/802.11b radio that provides wireless access to the corporate network
	<i>Cisco Aironet Client Adapter Card</i>	Wireless LAN interface card that secures connections using the Cisco Wireless Security Suite
	<i>Cisco Access Control Server</i>	A RADIUS authentication server that supports Cisco LEAP security protocols
On the Road	<i>Cisco IPSec VPN Client Software and VPN 3000 Concentrator</i>	Together, establish secure "tunnels" for remote access using DES or 3DES encryption algorithms
	<i>Cisco Aironet Client Adapter Card</i>	Wireless LAN interface card. When used with public network services, security is achieved using specialized IPSec VPN technology (see above).
	<i>Cisco CTE 1400 Series Content Transformation Engine</i>	Dynamically transforms Web content so that it is properly displayed on the small screens of handheld devices
At Home	<i>Cisco 800 Series Routers</i>	Connect users to broadband Internet services for access to corporate resources. Some support integrated stateful firewall and IPSec capabilities.
	<i>Cisco PIX 501 Firewall</i>	Security appliance that provides up to 10 Mbps of firewall throughput and 3 Mbps of 3DES throughput
	<i>Cisco VPN 3002 Hardware Client</i>	Provides secure connections to a VPN 3000 Concentrator at a central site using IPSec tunnels