Mobile VPNs: Enabling On-the-Go Workforces

Lisa Phifer

Secure, transparent and persistent access to corporate applications is the name of the game with these new MVPNs.

After years of anticipation, and fueled by high-speed wireless broadband, the business use of mobile handheld devices is finally taking off. PDA and smartphone shipments are expected to more than double in 2006, according to ABI Research, while Gartner predicts that two out of three workers will use mobile enterprise applications by 2007. However, delivering secure remote access to mobile workforces is not that easy.

Conventional remote access VPNs based on IPSec, SSL and L2TP enable secure access from stationary laptops, but often disappoint mobile users who require on-the-go access from handheld devices. A recent study by Action Engine found that many mobile users are frustrated by slow application response. Three out of four simply abandon mobile application sessions after just two connect attempts. Between productivity losses and help desk calls, this dissatisfaction is generating renewed interest in mobile VPNs.

Overcoming Barriers

Mobile VPNs were created years ago to secure communication over painfully spotty and slow radio networks. 3G and Wi-Fi networks are now much faster, but today's mobile users still encounter many of the same old problems, from coverage gaps and handoff delays to roaming disruption and broken sessions. Today's mobile VPNs add capabilities that are designed to solve these problems, while using authenticated, encrypted tunnels much like conventional remote access VPNs.

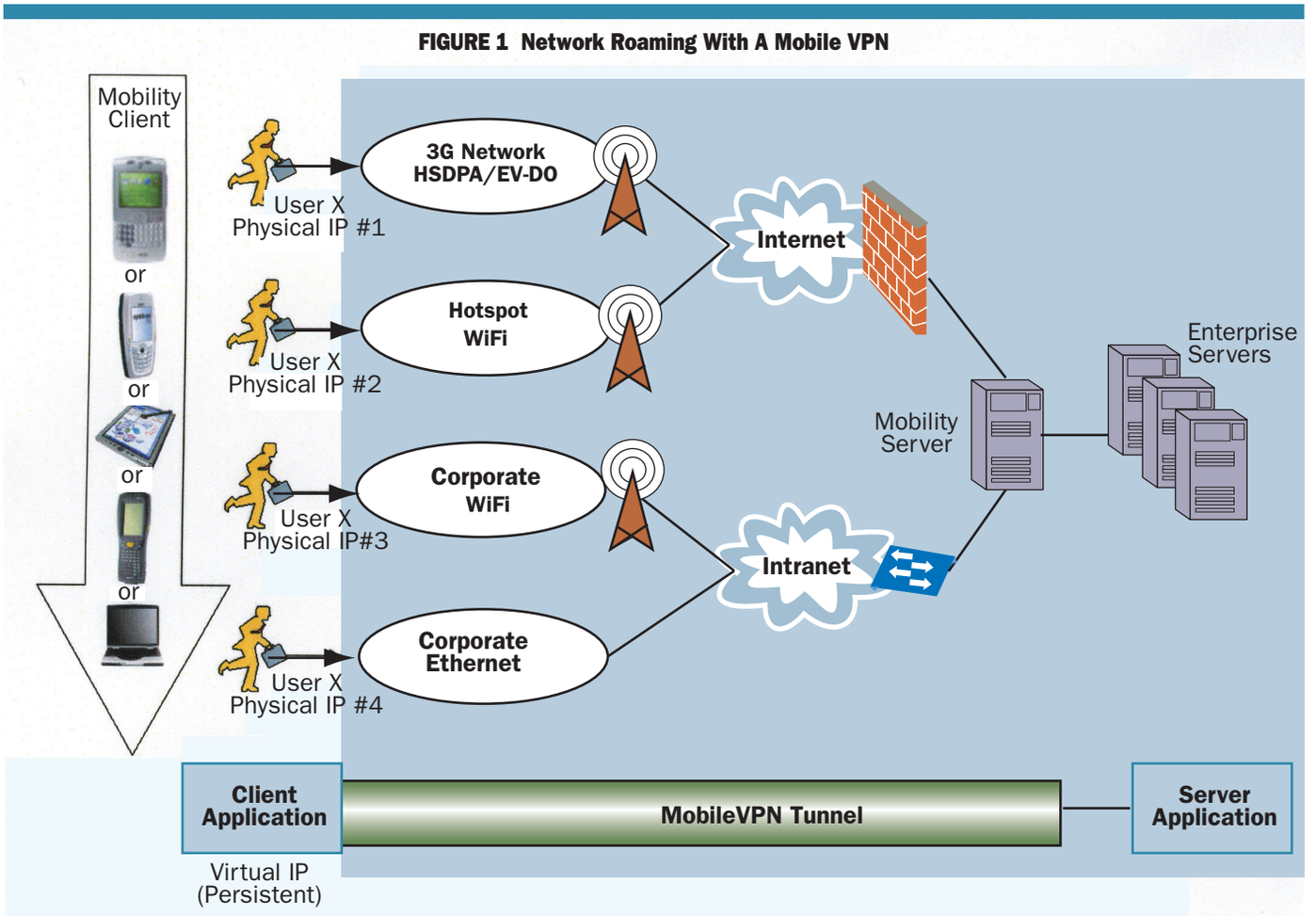
"A mobile VPN is specifically designed to provide a very efficient work environment for people who are on the move as a component of their job function, and who need access throughout the day," explained John Knopf, senior project manager at NetMotion Wireless. "We see a big distinction between mobile and remote. IPSec and SSL work wonderfully for remote users, but a truly mobile user requires a different solution."

Here are the capabilities that differentiate mobile VPNs from their conventional counterparts:

- **Network independence**: Mobile VPNs operate over just about any kind of public or private, wired or wireless network, including dial-up, residential broadband connections (e.g., DSL, cable), Ethernet LANs, Wi-Fi hotspots, wireless WANs (e.g., GPRS, CDPD, TDMA, UMTS HSDPA, CDMA2000 EV-DO), satellite networks (e.g., Wireless Matrix's Norcom, Inmarsat), and/or non-IP radio networks (e.g., the open standards DataTAC and Mobitex).
- **Network transparency**: Mobile VPN users spend little or no time dealing with the specifics of these disparate networks—"the connection" is simply up or down, and the mobile VPN always delivers the same degree of security, application interface, and user experience.
- **Network persistence**: Conventional VPN users lose their connection and IP address every time they roam into a different network. To avoid this pain, the virtual (or home) IP address of each mobile VPN client remains the same when the physical (or "in care of") IP address changes. By communicating through this persistent IP address, clients can avoid network connection reset and re-authentication (Figure 1).
- **Transparent suspend/resume**: When endpoint devices go to "sleep" to conserve battery life, the mobile VPN server maintains enough information about the devices and clients so that they can "awaken" and resume network communication without disrupting the VPN tunnel or associated state.
- **Application persistence**: When mobile VPN devices pass through coverage gaps that last minutes or hours, the mobile VPN server queues undeliverable application messages, resending

Lisa Phifer is vice president of Core Competence, Inc. (www.corecom.com), a network security consulting firm specializing in emerging technologies, including wireless communication and virtual private networking. She can be reached at lisa@corecom.com.

FIGURE 1 Network Roaming With A Mobile VPN



them when the device later regains coverage. Some applications still may time out when using a mobile VPN, but many can survive frequent or lengthy disruptions—even the swapping of adapters in devices with a single card slot.

■ **Wireless optimization**: Some mobile VPNs optimize TCP/IP's notoriously chatty performance by adjusting to each link's characteristics. For example, NetMotion can avoid unnecessary-but-costly fragmentation and retransmission over wireless links; IBM's WebSphere Everyplace Connection Manager (WECM) can compress data sent over GPRS by up to 67 percent.

■ **Policy-based roaming among multiple networks**: Mobile VPNs manage the use of multiple links with roaming policies. For example, ipUnplugged policies can use signal strength thresholds to trigger wireless roaming; Columbitech uses speed, pricing and preferences to select and log the device into the best available network. The ability to manage multiple links is critical, as most laptops now ship with Ethernet and Wi-Fi, most smart phones with 3G and Bluetooth, and Gartner estimates that half of large enterprises will be using at least five wireless technologies by 2007.

■ **Network-aware rules**: Like conventional VPNs, mobile VPNs enforce security policies. But mobile VPN rules also can incorporate network characteristics—for example, disabling encryption when connected to a trusted Ethernet, blocking file transfer over a low-bandwidth or high-tariff WAN, or automating Wi-Fi hotspot login before VPN tunnel establishment.

According to Asa Holmstrom, president of Columbitech AB, persistence is the primary reason that customers choose a mobile VPN. "Persistence keeps frustration down because the user does not have to reconnect or log in again," he said. "As soon as coverage is resumed, he can continue right where he left off."

"We think of mobile VPN as an always-on service," said Gregory Singh, CEO of ipUnplugged AB. "For example, with applications like VOIP, if you are moving between different networks, that's when we see real demand for fast seamless roaming. Who wants to lose a VOIP call because they have to log into the network again? That's just not going to work for real-time applications."

NetMotion's Knopf argues that mobile VPNs must actually improve application performance. "We have many customers who tried to support their mobile deployments with IPSec or SSL, but found their performance degraded significantly—up to 40 percent with IPSec," said Knopf. "With [a

The value of the Mobile IP standards is hotly debated by vendors who use their own proprietary transport-layer protocols to improve performance

mobile VPN], you should at least have no degradation. We have seen 2–5 times improvement over low-speed wireless or dialup. Even over EV-DO and HSDPA, we can do quite a bit to improve throughput performance."

Nuts And Bolts

To succeed, mobile VPNs must improve mobile user experience while delivering many of the same security capabilities offered by conventional IPSec and SSL VPNs.

These security systems implement a variety of authentication and encryption algorithms. Among mobile VPNs, AES support and FIPS 140-2 certification is growing but not yet universal. Most can interface with RADIUS, LDAP and Active Directory servers to reuse corporate network logons and enable single sign-on. Several also support client-side certificates, tokens, biometrics (e.g., Columbitech) or their own PKI (e.g., Nokia).

Mobile VPNs also may play a role in mobile device security policy enforcement. For example, Columbitech, IBM, ipUnplugged and NetMotion can quarantine a user account or device when a handheld is lost or stolen. IBM and ipUnplugged can check mobile devices for required applications at connect time—for example, to mandate use of firewall or anti-virus software.

When it comes to mobility, the value of standard protocol compliance is hotly debated. Ecutel, IBM, ipUnplugged and Nokia mobile VPN clients and servers all buckle a standard mobile IP implementation onto a standard IPSec implementation, making it possible to integrate them with compatible third-party IPSec clients and gateways.

In contrast, Columbitech, NetMotion, Padcom and Radio-IP use proprietary, transport layer protocols to improve wireless performance. They perform essentially the same functions as Mobile IP and IPSec—tunneling, encryption, and authentication—but they implement these functions using non-standard protocols.

Enterprise RFPs that mandate standard protocols overlook the potential merits of proprietary alternatives. In its January 2006 market study, The 451 Group concluded, "The advantage of using standards [instead of] proprietary protocols from a pure technology perspective is unclear."

From a capex standpoint, however, standards can help to leverage existing investments in IPSec remote access. For example, Nokia's mobile VPN client can be used with Nokia, Check Point or Cisco IPSec gateways. The ipUnplugged Roaming Client is compatible with Lucent, Cisco, Juniper and Check Point IPSec. While running IPSec under a proprietary transport-layer mobility protocol may be technically possible, doing so would add complexity without gaining value (why encrypt a second time with IPSec?).

Like IPSec VPNs, mobile VPNs require installed client software. But mobile VPN vendors have learned from the market success of SSL VPNs, and most provide a Web portal from which mobile users can download a near-zero-config mobile VPN client, and activate a default VPN connection. Centrally-defined policies (and future updates) are then pushed to the mobile devices. Nokia and Columbitech can even auto-generate and install client certificates, used to strongly-authenticate all future connections.

Default VPN policies are usually coarse—for example, granting a pre-defined Windows Group access to the entire network attached to the mobile VPN server. This lets you get a simple VPN up and running quickly. However, most companies will want to apply new policies at the group, user, or even device level. Filter granularity ranges from subnet/port (in mobile IP-VPNs) to application content (in some transport-layer VPNs). For example, NetMotion policies can permit or deny traffic based on hotspot SSID and application command—but controlling mobile access with this granularity requires purchase of an advanced Policy Management Module.

Streamlining client installation and policy configuration is only part of the battle. Mobile VPN clients also must run efficiently on a wide variety of portable and handheld devices, each of which can pose its own unique hardware, OS and interface challenges. Most mobile VPNs support Windows32 and Windows CE, but there are a dozen versions of WinCE and hundreds of hardware platforms that run WinCE. For example, readily-

TABLE 1 Mobile VPN Client/Operating System Support

Mobile VPN Clients	Win32	WinCE[1]	Palm OS	Symbian
Columbitech Wireless VPN www.columbitech.com	✓	✓	—	—
Ecutel Viatores Iproam www.ecutel.com	✓	✓	—	—
Ericsson Mobile Corporate Access[2] www.ericsson.com	✓	✓	—	—
IBM WECM Mobility Client www.ibm.com	✓	✓	✓	✓
ipUnplugged Roaming Client www.ipunplugged.com	✓	✓	—	—
NetMotion Wireless Mobility XE www.netmotionwireless.com	✓	✓	—	—
Netseal MPN www.netseal.com	✓	✓	—	—
Nokia Mobile VPN www.nokia.com	—	—	—	✓
Padcom TotalRoam[3] www.padcomusa.com	✓	—	—	—
Radio IP MTG www.radio-ip.com	✓	✓	—	—
Symbol AirBEAM Safe[2] www.symbol.com	✓	✓	—	—

1 Includes Windows Mobile, Smartphone, and/or Pocket PC
2 Columbitech OEM Partner
3 Merged with NetMotion Wireless in June 2006

available Windows Mobile 5 PDA mobile VPN clients do not run on Windows Mobile 5 smartphones (now supported by NetMotion and Columbitech). As shown in Table 1, Palm and Symbian clients are harder to find. In fact, IBM is the only vendor that now supports devices in all four major mobile platform categories.

Workforces with specialized mobile devices (e.g., barcode scanners, point-of-sale terminals) may be satisfied through custom client development. For example, 15 wireless device manufacturers have used Columbitech's SDK to port its WVPN to at least 150 different devices running DOS, Wind River System's VxWorks and other embedded operating systems, according to the company. Mobile VPNs insulate applications from network differences, but those who want their applications to see and control network connections can do so by using an SDK.

Most MVPNs support Windows32 and Windows CE— but there are a dozen versions of WinCE and hundreds of hardware platforms that run WinCE

Platform is also an important consideration on the back end. Ecutel, ipUnplugged and Nokia sell mobile VPN server appliances; others are sold only as software. According to ipUnplugged's Singh, many customers prefer to install mobile VPN software on their own off-the-shelf servers. "We do pre-package solutions for those who want them, but we're moving to being a pure software vendor so that our resellers and customers can choose which platform they want."

Most mobile VPN servers can be run on Windows 2000/2003 and/or Linux, except for IBM, which requires AIX or Solaris. Server capacity, reliability, and scalability are critical. Several mobile VPN product architectures split the back end, letting you distribute data functions across several servers while centralizing certain control functions (e.g., provisioning, policy storage, activity logging). Companies with large workforces or high-speed LANs should look for a mobile VPN that supports server pools, load balancing and failover.

Vendors supply metrics to assist with capacity planning, but sizing can be tough when mobile user traffic is highly variable. To better understand your own needs, conduct a mobile VPN field trial with a representative mix of devices, networks and mobile applications.

Learn By Example

One way to more fully understand the potential of mobile VPNs is to examine how other companies have used them to meet their own business needs. Mobile VPN adoption is minimal in comparison to conventional remote access VPNs. But thousands of companies have successfully deployed mobile VPNs—in many cases, after a conventional VPN failed to satisfy mobile workforce needs.

Mobile VPNs are frequently used to improve the usability and performance of field service automation applications. For example, more than 1,200 Carlsberg Brewery delivery trucks use GPRS to communicate delivery receipts, order changes and provide other status information to back-office systems. Drivers use Columbitech WVPN to remain logged into Carlsberg's SAP enterprise resource planning (ERP) system as they roam through and between GPRS coverage areas. Wireless optimizations permit larger volumes of data to be sent over GPRS, and switching seamlessly to WiFi enables high-speed access whenever a truck pulls into a Carlsberg depot. The company used Columbitech's SDK to integrate WVPN into Carlsberg's Smart Route application, making the mobile VPN invisible to drivers.

Jacksonville Electric Authority (JEA), a Florida utility, used NetMotion Mobility XE to provide more than 400 field workers with secure mobile access to dispatch data, CRM tools and electrical service delivery applications. When JEA tried to use IPSec, they found that workers were spending 20 to 30 minutes logging into the network and connecting to applications. Repeating this over and over again while roaming throughout an 840-square-mile service region proved frustrating and wasteful. JEA wanted to deploy a mobile VPN to improve workers' productivity and their ability to respond quickly to problems. JEA chose NetMotion because it satisfied their application and high availability needs, keeping workers connected securely and reliably while roaming between wireless WAN and LAN links.

When York, which manufactures HVAC systems, wanted to increase the number of service calls handled by each field technician, this equipment supplier used a mobile VPN to speed synchronization between wireless handhelds and a Siebel (now Oracle) work dispatch application. Synchronization requires about 20 minutes—ideally, this is completed as the technician drives from one job to the next. However, before upgrading to its current mobile VPN, if the wireless connection were to break for any reason, synchronization had to be restarted from scratch. By using NetMotion, York technicians can now pass through coverage gaps lasting a half hour to an hour, resuming synchronization right where it left

Session persistence cannot make lengthy outages invisible to real-time applications

off, improving productivity. Instead of changing the application to fit the network, York made the network more transparent to the application.

Any workforce that requires secure connectivity over a geographically-distributed area—from public safety workers to professional services firms—can benefit from a mobile VPN. For example, Cap Gemini, a global technology consulting firm, uses the ipUnplugged Roaming Client to provide its consultants with secure connections wherever they happen to be working—whether via broadband at home, wireless on the road or Wi-Fi at the office. Cap Gemini adopted ipUnplugged not only to make network roaming more invisible to users, but to apply a single consistent security solution to internal and external networks. Moreover, the same solution can be applied to Pocket PCs and laptops, giving the IT department one wireless security infrastructure and policy database to manage.

In fact, many companies use mobile VPNs to secure in-house networks, smoothing over both the coverage gaps that break IPSec VPNs and the support issues with handheld device clients. For example, the retail industry is Columbitech's largest market. "They want the same security environment in all stores, and the same security for all devices—wireless printers, scales, point-of-sale devices," said Holmstrom. "Some of those systems run Windows CE, but many are proprietary and it has been challenging to create VPN clients for all of them." Columbitech's focus on this vertical market is evident in its partnership with Symbol, which resells WVPN in its AirBEAM Safe product line.

The health care industry was among the first to embrace wireless, thus representing another mobile VPN sweet spot. For example, Saint Luke's Episcopal Hospital in Houston makes extensive use of wireless handhelds and laptops, letting staff maintain patient charts, dispense prescriptions and manage patient care more effectively. According to NetMotion's Knopf, a single application like bed management can justify a hospital's investment in mobile wireless by filling empty beds faster and increasing revenue. But blanketing a large hospital campus with Wi-Fi is impractical—even impossible. Saint Luke's deployed NetMotion Mobility XE to maintain Citrix Metaframe sessions as doctors and nurses move between buildings, enter elevators and pass through areas where Wi-Fi signal is absent. A conventional VPN would not provide adequate security in this environment, but a mobile VPN's persistence enables it to deliver secure communication far more reliably.

Conclusion

These examples illustrate how companies have applied Mobile VPNs to insulate users and applications from coverage gaps, support suspended devices, optimize the use of limited bandwidth and streamline network roaming—solving the most basic problems that impede mobile communication over conventional VPNs. Mobile VPNs support a broad mix of IP-based applications, but session persistence cannot make lengthy outages invisible to real-time applications like streaming media or in-progress VOIP calls. If mobile VPNs sound like a fit for your workforce, conduct a field trial to set realistic expectations about the benefits and limitations of any mobile VPN solution□

Companies Mentioned In This Article

ABI Research (www.abiresearch.com)
Action Engine Corp. (www.actionengine.com)
Carlsberg Brewery (www.carlsberg.com)
Cap Gemini Group (www.capgemini.com)
Check Point (www.checkpoint.com)
Cisco Systems (www.cisco.com)
Citrix Systems (www.citrix.com)
Columbitech (www.columbiech.com)
Ecutel Systems (www.ecutel.com)
Gartner (www.gartner.com)
IBM (www.ibm.com)
Inmarsat (www.inmarsat.com)
ipUnplugged (www.ipunplugged.com)
Jacksonville Electric Authority (www.jea.com)
Juniper Networks (www.juniper.net)
Lucent Technologies (www.lucent.com)
NetMotion Wireless (www.netmotionwireless.com)
Nokia (www.nokia.com)
Oracle (www.oracle.com)
Padcom (www.padcomusa.com)
Palm, Inc. (www.palm.com)
Radio-IP Software (www.radio-ip.com)
St. Luke's Episcopal Hospital (www.sleh.com)
Symbian (www.symbian.com)
Symbol Technologies (www.symbol.com)
The 451 Group (www.the451group.com)
Wind River Systems (www.windriver.com)
Wireless Matrix (www.wirelessmatrixcorp.com)
York (www.york.com)