



Mobile VPN Secure Connectivity on the Move



Enabling secure remote connections to the office, Virtual Private Networks (VPNs) have allowed millions to work from anywhere, as long they stay in one place. Now, mobile personnel on the go—in public safety, industry, and government—are connecting to the office, even at highway speeds. Police officers receive confidential suspect information en route to the scene. A bridge inspector downloads restricted blueprints and shares sensitive photos taken minutes ago. Utility workers monitor critical flow data while traveling between sites. Mobile VPN technology makes this possible.



Benefits of Mobile VPN

- *Mobile connectivity – even at highway speeds*
- *Data connections encrypted for security and data integrity*
- *Session persistence through coverage gaps*
- *Data traffic shaped for maximum efficiency*

Introduction

Demand for mobile connectivity has been building for years. As office workers slowly disconnect from Ethernet jacks and landlines and work from home or a coffee shop, people in jobs that have always been mobile look to receive increasing amounts of data in a “virtual office” that travels with them. They expect that data will get to them securely as it does at the office, and that familiar applications will continue to run, even when in a moving vehicle.

But this isn't easy. Wireless networks are radio networks, and radio is a broadcast medium. How do you ensure that all parties in the conversation are legitimate, that no one else is listening, and that data transmissions aren't being tampered with—even when data travels on third-party infrastructure and public airwaves?

Many network applications were not made for mobility. How do you run software designed for fixed-line networks in an environment where your connection can change many times an hour?

The answer is Mobile VPN.

Benefits

The main benefit of Mobile VPN is that users can remain connected while on the move. Provided they are within the coverage area of at least one network, mobile personnel can send and receive data without having to wait or go back to the station or office. In real-world terms, this means that a police officer can submit an incident report while still on patrol and protecting the public, repair personnel can receive a new route map, and a social worker can update client information while still in the field, instead of being in the one place where they are needed least—headquarters.

Perhaps just as important is data traveling securely. Encryption standards used on a Mobile VPN are the same as those used for secure, fixed-point connections. End-to-end security means that sensitive data can be sent to mobile personnel without fear of third-party eavesdropping. Authentication prevents impersonation of both

headquarters staff and field personnel, as well as unauthorized data feeds. Even sophisticated criminals with scanners and data equipment will not be listening in or joining the conversation.

Encryption can also provide data integrity, ensuring that data hasn't been tampered with during its transmission—which has important legal implications, particularly in law enforcement where chain-of-custody concerns loom large.

For customers using narrowband wireless networks, some mobile VPN implementations can offer the ability to use bandwidth more efficiently. This can bring visible improvement in networked application performance, on top of enhanced security.

Challenges

Originally, VPNs—like IP networking itself—were designed for communication between machines using wired, static connections. Their designers assumed that a connection would always be available to the VPN, and that connection information would not change. In fact, their assumptions went further: in the design of most VPN software, the connection information must not change—if it does, the VPN thinks its connection has been compromised. This made perfect sense: after all, a new network meant a new location—most likely one with a hacker who is trying to cut in. So the VPN would disconnect the session. Clearly, this is not acceptable behavior for mobile connections, where someone can roam from one network site to another or even from one network to a completely different network.

Many VPNs also assume that the network is always available. Even a short interruption will cause them to drop the session and reset, requiring that you stop and log back on. This was a problem even in the days of hard-wired connections, but for someone needing a secure link while on the highway, it is unacceptable. A disconnection not only requires you to stop what you are doing and log back on, interrupting your work, but it also disconnects applications being used, requiring their own restarts. The result is that even a 5-10 second interruption in connectivity requires a 3-5 minute interruption

Mobile VPN Requirements

- *Maintain a secure connection while client is moving*
- *Make the network appear fixed and constant, regardless of changes*
- *Handle coverage gaps gracefully*
- *Provide security on par with wireline VPNs*
- *Use standards-based encryption: AES or 3DES*
- *Use standards-based authentication*

in work flow—a negative multiplier effect. Imagine if this happened several times in an hour! While it would be nice if all VPNs and application software could handle interruptions gracefully, the fact is that for many, the opposite is true: an interruption is a catastrophic event requiring manual clean-up. Since you can't rewrite all the software, your VPN should be designed to prevent the problem from occurring in the first place.

Mobile VPN Requirements

While potentially obvious, the most basic requirement for a mobile VPN is that it be designed for a mobile environment. That means it must maintain a secure connection even as its client moves from network to network, changing IP addresses and encountering occasional coverage gaps. Ideally, the mobile VPN should completely insulate fragile network applications from the bumpy realities of network roaming. Regardless of network changes and coverage gaps, the network should appear to the end user to be fixed and unchanging.

A proper mobile VPN should not just handle network changes, but also respond gracefully to network outages. If the client device briefly loses its connection, applications shouldn't be aware of this. Data should be queued up, and sent/received when the connection becomes available, without requiring a reset of the application.

Security provided by a mobile VPN should be on par with what's available for a fixed VPN. Connections must be authenticated and encrypted with standard well-known algorithms. In some cases, users require that encryption meet government standards.

Standards-based Components of Mobile VPN

IPSec (Internet Protocol Security)

You may have used a secure connection on the Web; for example, when banking online. That connection was encrypted by your web browser, and decrypted by the bank's web server. Support for secure communications had to be built into both browser and server, which required significant developer resources. Most developers lack the time and skill to integrate security into their applications, so it's no surprise that the vast majority of network applications are either completely unsecured, or worse, secured inadequately.

The aim of IPSec, introduced in 1998, is to build encryption into the Internet Protocol. An application uses an IPSec connection the same way it uses an IP connection; in fact, the application can't distinguish between the two. Switching to an IPSec

Multi-Net Mobility™

Part of Motorola's MOTOA4™ portfolio, Multi-Net Mobility software was designed to address the needs of mobile workers for connectivity, mobility, and security.

Multi-Net Mobility allows seamless roaming between wireless networks, transparently handling network changes and coverage gaps. It responds intelligently to network congestion and signal fade by adaptively optimizing TCP traffic or switching networks before connectivity is lost.

Multi-Net Mobility provides strong security protection, with support for AES, DES, and 3DES encryption, as well as standards-based authentication. The software has received U.S. government FIPS 140-2 certification.

For more on Multi-Net Mobility, see www.motorola.com/multinetmobility or contact your Motorola representative.

MOTOA4™

connection makes all the applications running on the network secure, without any upgrades to the software or changes in its configuration.

In VPNs (fixed or mobile), IPSec ensures that original outgoing IP packets are completely encrypted, put into new IP packets, and sent across the network to the receiver, where the process is reversed. Anyone intercepting these packets along the route would see very little in terms of usable information: just routing information, indecipherable characters (the encrypted data), and some basic information about those characters. In contrast to our online-banking example, the eavesdropper will not even be able to tell which application is using the network. Video, tactical data, database queries—all IPSec packets look the same. This feature is valuable for two reasons: not only wouldn't eavesdroppers know that, say, streaming video is being sent to headquarters from a squad car, they also won't know that a video server is available on the network. This is important, particularly if the video server software has known, exploitable vulnerabilities.

Two other features provided by IPSec:

- Reliable, standards-based authentication, to ensure that both sides are who they say they are
- A mechanism for negotiating which encryption and authentication the two sides will use

Encryption Algorithms

IPSec supports several encryption methods. Amongst the most widely used are DES, 3DES, and AES.

A modern mobile VPN system must provide at least 3DES encryption. The best systems will support AES encryption, which has the benefit of better performance.

First published by IBM in 1975 and adopted as the U.S. Government's **Data Encryption Standard** in 1977, **DES** encrypts data using a binary key 56 bits long. A message encrypted with DES can have any one of 2^{56} , or 72,057,594,037,927,936 possible keys. This may seem like a lot of keys to try, making DES very secure—and for many years, it was. But consider

this: a modern desktop computer can perform more than two billion operations per second.

By the late 1990s, it was clear that DES was no longer secure, but it was still the most implemented, best-known encryption algorithm available. The simplest solution was to take some DES-encrypted data, and encrypt it again, with a different key. Not satisfied with this, the new standard required encoding the data three times; hence **3DES** or triple-DES. This encryption method is considered highly secure, and is in wide use today.

The main problem with 3DES is that encrypting and decrypting data three times is slow and resource-

intensive. This gave rise to a new **Advanced Encryption Standard (AES)** in 2002. AES uses a new algorithm and is fast and easy to implement. Its keys can be up to 256 bits long. (2^{256} is a 78-digit number. A trillion computers, each a trillion times more powerful than our desktop, would require trillions of trillions of years to go through all the keys.)

Avoid proprietary, non-standard encryption methods: unlike published algorithms, they haven't been subject to much scrutiny—at least, not by people with honorable motives.

Mobile IP

Mobile IP gives you the ability to show a static, non-changing IP address to the Internet, even as you move around. But it does more: it also lets applications on your mobile device believe they have a static IP address. (As mentioned earlier, that is how most network applications are designed to work: the server and the client assuming that their network is fixed and constant.)

The mechanism is straightforward: your computer or other mobile device is first registered with a Home Agent—a server with a fixed network connection that will receive all IP traffic addressed to your device. As you roam to different networks, you keep your Home Agent updated with your new address (called the care-of address), allowing you to keep receiving your data. Software installed on your mobile device handles this, hiding all the roaming and updates from your applications.

Putting it all together: the Mobile VPN

It is the combination of Mobile IP and IPSec that is the basic framework of a Mobile VPN:

- Mobile IP ensures that data will always reach you.
- IPSec allows you to transmit—even broadcast—highly sensitive data, knowing that only authorized personnel will receive it.

But that is only the beginning. A well-designed Mobile VPN system such as Motorola's Multi-Net Mobility™ takes advantage of its unique knowledge of both outgoing data and available networks. For example:

- Your Mobile VPN software should handle temporary connection losses by keeping applications open and holding data traffic until the connection is restored.

- Not all data is suitable for every network, nor does all data have the same priority. Your Mobile VPN should allow you to configure data and network selection criteria. For example, you should be able to block video from low-bandwidth links.
- As it has visibility to network bandwidth and all traveling data, a high quality Mobile VPN client should compress and repackage this data so that each TCP/IP packet carries as much data as possible. The VPN software should also optimize TCP by lowering the number of overhead packets traveling on the network. This reduces overhead and can dramatically increase throughput, particularly on low-bandwidth networks.
- Just as it must use standards-based encryption, your Mobile VPN must also support standards-based authentication of both users and devices.
- The Home Agent server for Mobile IP is the heart of the entire system. It must be reliable, which means using robust hardware, a stable operating system, and supporting redundancy.

Conclusion

With more and more personnel accessing data on the move, wireless connectivity and the right Mobile VPN will be more essential than ever. That's why it's important to partner with a proven provider that knows wireless technology inside and out. For nearly 80 years, Motorola has been recognized as the leading provider of wireless communications systems, networks, devices and services. To learn more and see in action how Motorola's MOTOA4™ mission critical products can help government and public safety agencies receive the immediate benefit of wireless connectivity and Mobile VPNs, please call your Motorola representative or visit us at www.motorola.com/multinetmobility.



MOTOROLA

Motorola, Inc. 1301 E. Algonquin Road, Schaumburg, Illinois 60196 U.S.A. www.motorola.com/multinetmobility 1-800-367-2346

MOTOROLA and the Stylized M Logo are registered in the U.S. Patent and Trademark Office.
All other product or service names are the property of their registered owners. © Motorola, Inc. 2008 (0805)
RO-99-2157