WHAT’S A MOBILE VPN?

Technology for Successful Mobile Deployments

The foundation of a successful mobile deployment is a Mobile VPN (virtual private network), software that provides mobile workers with secure, reliable, remote access to network resources and information from virtually anywhere. Only a Mobile VPN is designed to deal with the unique challenges associated with mobile computing such as wireless security, performance and roaming.

Traditional VPNs Not Built for the Mobile Environment

One of the weaknesses of the original Internet protocol (TCP/IP) is that it does not include a native means for ensuring the authenticity and privacy of data as it passes over a public network. To address this weakness, VPN technologies were developed that would validate the identity of and encrypt the data sent between two or more systems on the Internet.

These conventional VPN technologies, including PPTP, IPsec and SSL work great for users who connect from stationary devices (a home PC over residential broadband, a laptop over a hotel LAN, or even a PDA at a wi-fi hot spot), as they use the IP address to identify the device at the far end of the tunnel. But once that device is in motion, physical connectivity, point of network attachment, and IP address are all likely to change. A conventional VPN simply cannot adapt to these changes. The network tunnel is disrupted, causing application sessions to disconnect, time out, fail, or even the computing device itself to crash. This often forces the user to restart the communication from scratch, possibly having lost work or data transmission that was in process at the time of the disruption.

Add these drops up, factor in the time and productivity lost, and you start to see how challenging a mobile technology deployment can become without the right tools.

Unlike traditional VPNs, a mobile VPN is built to support devices that are in motion, where IP addresses, physical connectivity and points of network attachment often change.
Choosing a Mobile VPN

As with any software, there are multiple options on the market to choose from. When choosing a mobile VPN, the following key features should be considered:

- **True Application Persistence:** A mobile VPN should have the ability to sustain application sessions even through suspend-and-resume cycles and loss of connectivity. Mobile workers often need to suspend or hibernate their devices to preserve battery life.

  Many VPNs in this situation will lose application sessions, causing data loss and corruption, and forcing users to re-login and restart applications. True application persistence involves maintaining open application sessions during dropped connections, suspending the transmission of data – for days if necessary – until the user is able to re-connect, and then resuming transmission at the exact point the application was interrupted.

- **Standards-Based Security:** Keeping data transmission secure is of the utmost importance for a mobile worker. Especially since the tunnels are often built over public cellular and wi-fi connections. A good mobile VPN should support standards-based security, including two-factor authentication, device authentication, FIPS 140-2 AES encryption, NSA Suite B encryption and the ability for IT managers to quarantine remote devices or force re-authentication policies.

- **Centralized Management Console:** A true mobile VPN should provide a robust management console with the ability to generate views into connected devices. A good console allows IT managers to generate reports and see trends on user activity, application usage, and bandwidth consumption, among others. It should also provide the ability to create custom policies that fit the business environment, allowing organizations to manage and view their wireless deployment, just as they would their wired network.

- **Wireless Performance Optimization:** Mobile workers use cellular data networks characterized by lower throughput, higher packet loss, and higher latency when compared to wired networks. The applications they use are typically written for stable, high-speed, wired networks. A good mobile VPN should provide the ability to automatically reduce network consumption and improve throughput and application responsiveness, particularly over these cellular networks.

  Many VPNs typically degrade over wireless networks, often by as much as 50%. But a true mobile VPN uses link optimizations to reduce the number of retransmitted packets, excess control information and other network “chatter,” and dramatically improves throughput by compressing data and images. A good mobile VPN should also offer best-bandwidth routing technology to ensure the fastest and most efficient available network connection is used.

**Mobility Resources Online**

To learn more about mobile VPNs and best practices for mobile deployments, visit: