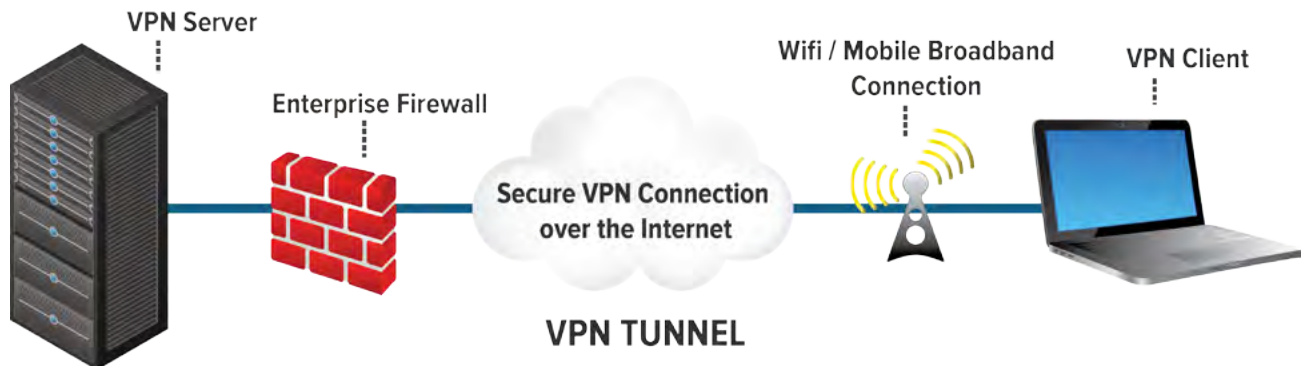# COMPARING MOBILE VPN TECHNOLOGIES

Executive Summary

Traditional approaches for encrypting data in transit such as IPSec and SSL are intended for wired networks with high-speed, highly reliable connections. In a mobile wireless WAN environment, where data transmission speeds are slower and connections are less reliable, traditional VPN performance suffers, frequently resulting in application failure, data loss, and reduced productivity. NetMotion Wireless offers a best-in-class mobile VPN built from the ground up for mobile, wireless environments.

VPN technologies validate the identity of and encrypt the data sent between two or more systems on the Internet.

Characteristics of an Ideal Mobile VPN

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, add-on Virtual Private Network (VPN) technologies were developed to validate the identity of and encrypt the data sent between two or more systems on the Internet.

Conceptually, a VPN is simply a way for two computers or networks to exchange data under the following terms:

- Each computer must be able to verify the identity of the other.

- The data that is exchanged must be kept confidential and unchanged in transit.

- The exchange must be reliable – computers exchanging data must detect when sent data is not received so that it can be sent again.

Mobile VPNs must also take the following into account:

- Mobile workers often move from the office to a customer site, changing their IP addresses and even the networks used to connect to the Internet. If the VPN doesn't accommodate these changes, a user must re-establish the connection each time the IP address changes.

- Mobile workers often need to suspend or hibernate their devices to preserve battery life. The mobile VPN should automatically resume without user intervention, otherwise applications that require the VPN to function are likely to fail. Users will lose data and must manually restart both the tunnel and any applications that use it.

- 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. Mobile VPNs must shelter those applications from the reality of mobile network performance or the application itself will become unstable, leading to data and/or productivity loss.

In essence, a mobile VPN bridges the gap between what users and applications expect (and get) from a wired network, and the realities of mobile computing. While resetting user expectations and rewriting applications for the mobile environment is possible, it's more cost-effective to deploy a single solution that takes mobility into account.

This paper discusses the strengths and weaknesses of several different approaches to meeting the connectivity needs of the mobile worker:

- IPSec client VPNs
- SSL client (browser-based) VPNs
- MobIKE (IKEv2) and MobileIP
- Purpose-built Mobile VPNs

IPSec VPNs

Internet Protocol Security (IPSec) is the most widely adopted solution for securing data in transit between two systems. It provides the following:

- Authentication so that the transmitting and receiving parties can trust each other
- A mechanism to negotiate the security algorithms and keys required to establish point-to-point security
- Integrity checking to ensure the data is not changed en route
- Encryption of data (privacy)
- Protection against certain types of security attacks, such as replay attacks
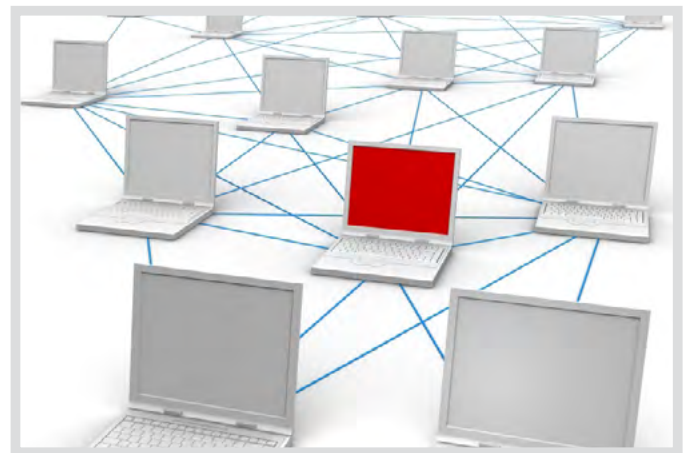
IPSec was originally developed to link private networks together over the wired internet.

IPSec was originally developed to link private networks together over the wired Internet. With the success of IPSec as a point-to-point protocol for securing data in transit between two wired networks, software clients were developed to connect single computers in the field to the corporate network. IPSec supports port/address-level access controls for traffic within the tunnel, multiple encryption algorithms, and it enjoys broad support across platforms and vendors.

IPSec is not, however, well suited for use in mobile and wireless environments because it requires that the IP addresses of the endpoints remain unchanged. IPSec disconnects the tunnel and requires users to reauthenticate when they encounter a coverage gap, move from one network to another, or suspend/resume their laptops. It also does nothing to address the unique performance requirements of mobile networking.

SSL VPNs

Browser-based SSL VPN solutions are designed to secure application streams between remote users and an SSL VPN gateway. In contrast to IPSec VPNs, which connect remote devices to trusted networks, SSL VPNs

connect remote users to specific applications and network resources inside of trusted networks via a Web portal configured to proxy the traffic. They secure Web-based traffic and are well suited for communicating to resources in a trusted network from non-corporate devices (such as kiosks, Internet cafés, or home computers) using a standard Web browser.

SSL VPNs require a client for anything but the most rudimentary connectivity. Before granting access, NAC security checks (frequently performed by ActiveX or Java applets) ensure that the remote device is running the proper security software (checking for the latest antivirus definition files, for example). Often, following necessary remediation steps is time-consuming and even impossible over an unreliable or slow wireless network.

Like IPSec VPNs, SSL VPN solutions do not meet all of the requirements for mobile and wireless use. They do not handle roaming between networks, crossing coverage gaps, or intermittent connectivity: applications crash or data is lost.

Other Enabling Technologies

IKEv2

An update to IPSec's IKE protocol is the IKEv2 Mobility and Multi-homing protocol (MOBIKE). IKEv2 supports a mobile device with multiple IP addresses, or addresses that change over time.

Since it's basically a key exchange protocol, IKEv2 does nothing to shield the applications on mobile devices from crashing when the device is unreachable (for example, out of range, or in hibernate mode). IKEv2 also can't do anything to enhance the performance of those applications over the network.

Mobile IP VPNs

Mobile IP solves the problems created when mobile devices change addresses as they roam, by hiding IP address changes from client applications. It has no native security functions and relies on another technology, such as IPSec, to keep data confidential and authenticate the identity of the systems participating in the VPN. Pairing Mobile IP with IPSec for basic security adds to the protocol overhead by requiring the following:

- IPSec encapsulation for protecting the end-point data

- Mobile IP encapsulation to hide the address changes

- A second layer of IPSec encapsulation for Home Agent and other security associations

This protocol overhead degrades throughput and adds configuration complexity. Like IKEv2, Mobile IP is not optimized for wireless networks, nor does it offer application persistence through wireless coverage gaps and the suspend/resume cycles typical of the mobile worker.

Password Caching and Automatic Reconnect

One of the problems that IKEv2 and Mobile IP leave unsolved is how to bring the tunnel back up after an interruption.

One approach is to simply cache the credentials used to create the tunnel and immediately re-submit them if the tunnel goes down. This approach is simple, effective, and easily understood by most users. Where it falls short, even when combined with technologies such as IKEv2 and Mobile IP, is that applications trying to use the tunnel when it is down will crash, taking valuable data with them, not to mention the time it takes to recover.

NetMotion Mobility: A Purpose-Built Mobile VPN Solution

NetMotion Mobility® is a standards-based mobile VPN that provides secure, continuous remote access to network resources and applications from mobile devices over any wired or wireless IP-based network.

Unlike traditional IPSec and SSL VPNs, which do not perform well in mobile and wireless environments, and point solutions that only solve part of the problem, Mobility was built from the ground up to address the unique challenges associated with mobile computing. These include wireless security, coverage gaps, and slow and unreliable networks.

The Mobility Mobile VPN enforces security from endpoint to endpoint, regardless of the combination of networks used. It is designed with an understanding of network types, providing a seamless solution for users transitioning from home networks to hotspots and to mixed-vendor environments, be they WWANs or WLANs. Although optimized for wireless networks, it also supports any type of network that uses the IP network protocol, including Ethernet, DSL, and dial-up.

Persistence

Mobility shields applications from changes in the network environment by intercepting network calls from the application and proxying those calls through a dedicated server on the core network. The Mobility server provides highly available and stable TCP connections that shield remote host applications from coverage gaps, address changes, and network changes. Mobility also offers enhanced application-based policy management and a secure end-to-end VPN for any application running on the mobile device.

Roaming

Mobility maintains a secure, stable VPN connection as devices roam from one network to another. The tunnel remains available and application sessions persist in many common scenarios, such as:

- Suspending operation on the mobile device and later resuming it

- Moving to a different location on the network

- Connecting a mobile device over slow, bandwidth-challenged, or high-latency networks

- Encountering interference from microwaves, stairwells, elevator shafts — anything that interferes with radio signals

- Changing network interfaces (for example, from a WLAN to a WWAN card)

- Moving across gaps in coverage

Performance Optimization

Mobility is designed to provide optimum performance over intermittent and low-bandwidth network links. Its architecture includes enhancements that allow network traffic over IP to more effectively deal with connectivity loss from a mobile device, whether due to coverage outages or external factors, such as power management or user intervention. It makes the most efficient use of the given bandwidth using advanced features that reduce the "chattiness" of transport protocols:

- Selective acknowledgments

- Data and acknowledgment bundling

- Message coalescing

- Reduced and synchronized retransmissions

- Fragmentation optimizations

- Data compression

- Error-reduction algorithms

- Web acceleration

Working in concert, these features provide for the efficient movement of data. In addition, Mobility is configured to automatically switch to the fastest-bandwidth network connection when multiple connections are active.

Extensive Platform Support

Mobility has extensive platform support, working on the majority of widely-used mobile operating systems. Mobility fully supports Windows operating systems, including Windows XP, 7 and 8, and Windows Pro Tablets, as well as all Android devices with Android 4.0 and above. Mobility also offers an OpenVPN solution to provide basic connectivity for Mac, Linux, and iOS devices.

VPN Feature Comparison

Security	Mobility	IP Sec	SSL
Standards-based encryption	Yes	Yes	Yes
FIPS-140-2 validated encryption libraries	Yes	Limited	Limited
Standards-based authentication	Yes	Yes	Yes
Integration with existing authentication schema	Yes	Yes	Yes
Support for CJIS-compliant smart cards and certificates	Yes	Yes	Limited
User-transparent multi-factor (user and device) authentication	Yes	No	No
Enforced reauthentication without disrupting applications	Yes	No	No
Network Access Control	Yes	Limited	Yes
Quarantine by device or user	Yes	Yes	Yes
Device-to-DMZ security	Yes	Yes	Yes
Common Criteria EAL4+	Yes	Yes	Yes
NSA Suite B	Yes	Yes	Yes
Productivity			
Application session persistence	Yes	No	Very Limited
Seamless roaming (slow handoffs — out-of-range conditions or suspend and resume operations)	Yes	No	No
Data compression	Yes	Limited	Limited
Link optimizations	Yes	No	No
QoS and traffic-shaping support	Yes	Limited	Limited
Web image acceleration	Yes	No	No
Real-time application optimizations	Yes	No	No
Transparency (ease of use)	Yes	No	Web only
Multi-platform support	Microsoft OS Only	Yes	Yes
Management			
Full support for laptops and Windows Mobile devices	Yes	Depends on vendor	Limited on Windows Mobile
Mobile-specific management information	Yes	No	No
Application Specific Policy management	Yes	No	Limited
Analytics on device / application / network use	Yes	No	No
NAT-friendly	Yes	Depends on vendor	Yes

Conclusion

While IPSec- and SSL-based client VPN technologies have their place, neither is suitable for the mobile computing environment because they fail to address the needs for application performance, usability, and productivity. Organizations investing in mobile computing as a way to improve field worker productivity should deploy a purpose-built mobile VPN solution to secure their remote data communications.

The dominant mobile VPN is Mobility —the flagship solution from NetMotion Wireless that is built from the ground up for mobile and wireless environments. Mobility is a mobile VPN designed to deal with wireless security, coverage gaps, roaming, and performance.

For More Information

Visit www.NetMotionWireless.com or contact sales@netmotionwireless.com.

NetMotion® WIRELESS

netmotionwireless.com

United States
Seattle, Washington
Telephone: (206) 691-5500
Toll Free: (866) 262-7626
sales@netmotionwireless.com

Europe
Germany and France
centraleasterneurope@netmotionwireless.com

United Kingdom
northerneurope@netmotionwireless.com