Security for Wireless Networks

A comparison among SSL, IPSec and Mobile VPNs

WHITE PAPER

NetMotion Wireless
701 N 34th Street, Suite 250
Seattle, WA 98103
206.691.5555
www.netmotionwireless.com

Security for Wireless Networks

Executive Summary

More and more organizations are incorporating mobile access via wireless networks into their remote access strategies. These organizations are deploying mobile solutions to achieve specific business goals, improve productivity and reduce costs. When they add mobile access via wireless networks (WLAN or WWAN) to their remote access strategy, user authentication, data security and other security issues become significantly more complex and challenging than when dealing only with wired or tethered networks.

Enterprise Mobility	
Benefits	**Risks**
• Increase productivity	• Lack of enterprise control
• Improve efficiency	• Critical data loss / leakage
• Improve response time	• Compliance issues
Bottom line: *Threats affecting mobile enterprises are severe and difficult to manage, with potential companywide implications.*	

Benefits and Risks of Enterprise Mobility, Yankee Group, 2006

Clearly, the desired goal is to achieve the benefits of enterprise mobility, while minimizing the risks. Security is imperative, but the security must be implemented without substantial impact to productivity or usability, lest the mobility project not meet its objectives, or the users discard the project or disregard the security practices.

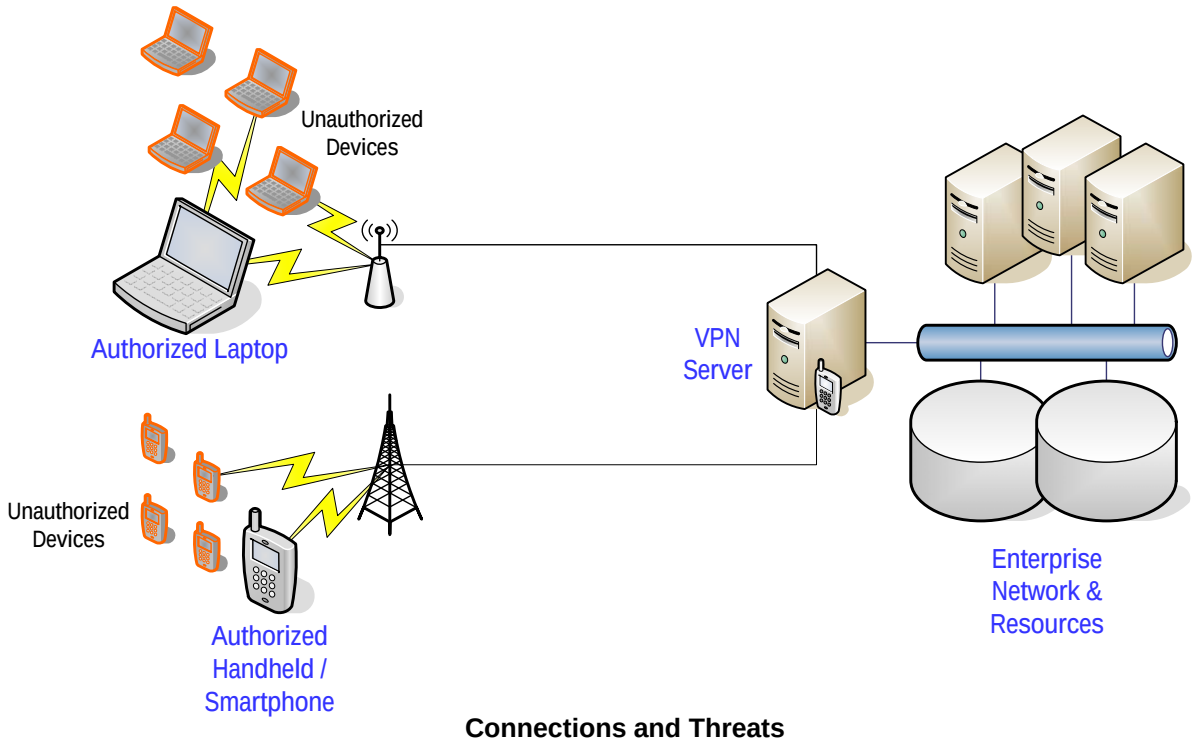
This paper will outline common threats and issues regarding wireless security in the context of typical uses of mobile devices over wireless networks. It will then explore secure remote access solutions and evaluate them in comparison with NetMotion Mobility XE. NetMotion Mobility XE is a mobile VPN that provides strong encryption and industry-leading security specifically for mobile workers using wireless networks. Unlike other solutions, Mobility XE does not require administrators to forgo usability or productivity in favor of security. It is a user-transparent solution that does not require user training or intervention and typically results in lower IT support costs. Mobility XE is optimized for WWAN, WLAN or any other IP-based network mobile workers use for remote access, including Ethernet LANs, home networks, dialup, and public and private hotspots.

Threats and Risks

There are many threats inherent in moving to wireless networks. Many of these threats can be categorized:

- **Authorization**
    - Who is attempting to connect, with what device?
    - Should a connection be allowed to the enterprise network?
    - What access permissions should be given?

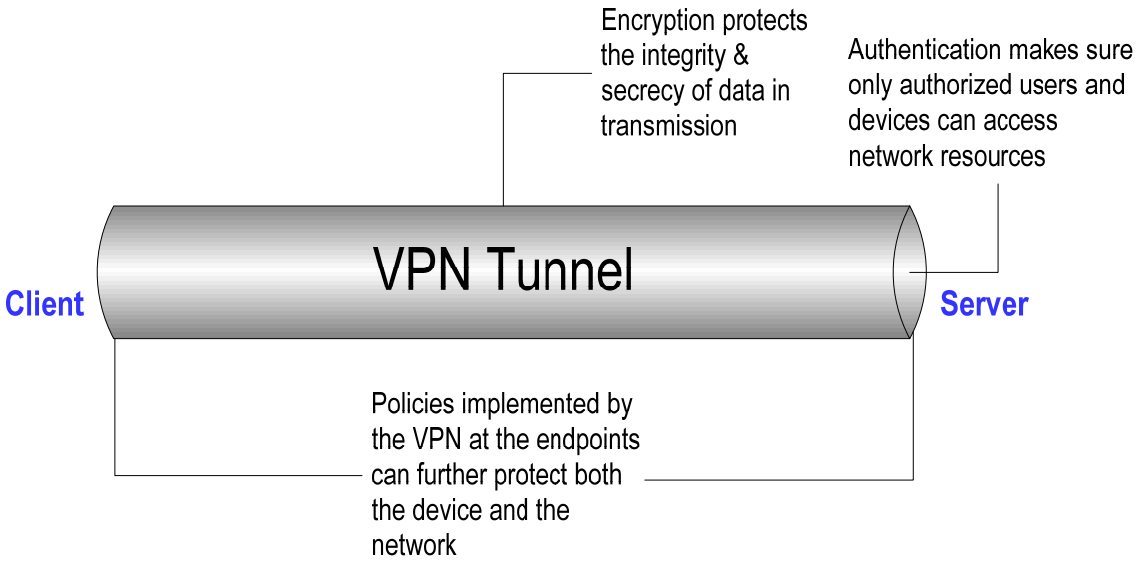
- **Data integrity & security**
  - Is the transmitted data being altered?
  - Is someone else able to eavesdrop on the data?
- **Network protection**
  - How can the network be protected against unauthorized use?
  - How can the network be protected against lost or stolen devices?
  - How can the network be protected against worms, viruses, etc.?
- **Device protection**
  - How can the remote device be protected against other (unauthorized) users and devices?



Connections and Threats

Against these threats are arrayed a number of techniques:

- **Authentication** helps provide a reasonable assurance that the user and device attempting to connect are, in fact, who they claim to be.
- **Encryption** can be used to assure that the data in transmission has not been altered, and that no one can eavesdrop on the transmission.
- **Policies** can be used to further protect both the network and the device, providing controlled access to each



VPN Techniques

Topics Covered

In analyzing the security implications of mobile access via wireless networks, this paper will consider:

- Access methods, including WWAN, Internet, WLAN and the use of multiple networks
- Traditional options for secure remote access, including IPSec and SSL VPNs
- NetMotion Wireless's Mobility XE, including authentication, encryption, security protocols, policy management, mobile & wireless optimizations, and management
- Device security & management
- Ongoing development

Access Methods & Networks

Wireless access methods currently include both wide area wireless (provided by cellular data carriers or privately owned), or wireless LANs, including both those installed and operated by an enterprise, and publicly accessible hotspots). New networks being installed are based on IP (Internet Protocol), and legacy private radio networks are gradually being replaced or augmented by 802.11 (Wi-Fi) and/ or carrier-based networks (e.g. HSDPA/UMTS, EV-DO, EDGE, 1xRTT).

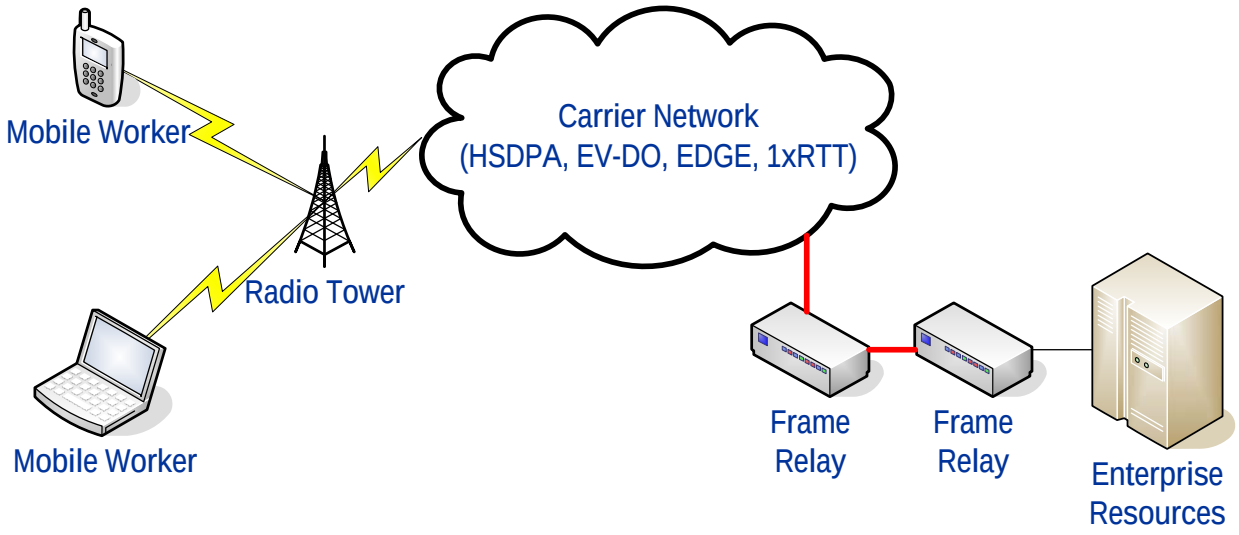
The wide and local area wireless networks cited above support TCP/IP communications, the standard protocol used for virtually all application traffic and for sending and receiving data via the Internet. Use of TCP/IP over wireless infrastructure greatly extends the reach of an enterprise by providing access to data and applications that were previously available only via internal network access or occasional dial-up by mobile field workers, telecommuters, and partners. However, as with many technology advances, remote access via wireless networks also creates substantial security risks for those who are unprepared.

WWAN

Wireless wide area networks such as EDGE, 1xRTT, EV-DO (including Rev A), and HSDPA provide an elegant solution for keeping mobile workers in contact with the enterprise. Data routing associated with such carrier-based networks typically is offered in two forms – dedicated or via the public Internet.

WWAN & Dedicated Network

In a dedicated configuration, the mobile user connects to a carrier network and is then routed via a dedicated frame relay (or sometimes ATM) network back to the enterprise:



Dedicated Network

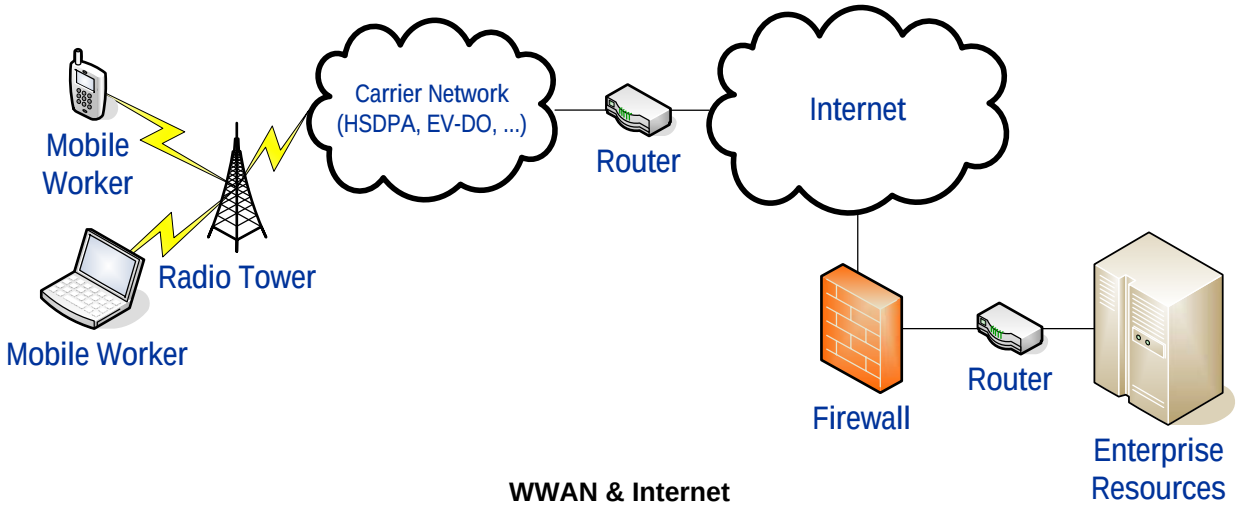
These networks provide an additional layer of security in that the data transmitted over the carrier network, from the mobile worker, is over a private link (frame relay) to the enterprise. The security used for the wireless link on WWANs depends on the access method and the telecommunications carrier. For example, in GSM and derivative networks, SIM (Subscriber Identity Mechanism) cards are used to supply key information during encryption.

However, while wireless WAN security systems encrypt the data over a wireless network, security becomes the responsibility of the individual user once the data leaves the carrier and travels the dedicated circuit. In addition, lost or stolen mobile devices (or mobile data PC cards and wireless phones serving as modems) also pose very real security threats. Without additional security measures in place such vulnerabilities can quickly put an enterprise at risk.

For example, the security used on GPRS/EDGE only uses a 64-bit key, and as of 1998, researchers at California Berkeley were able to break the security protocol (comp128) within a day [HSDPA/UMTS uses a 128-bit Kasumi algorithm; EvDO/1xRTT uses 128-bit AES].

WWAN & Internet

Internet-based routing typically is a more affordable solution than the dedicated network described above because it does not require a dedicated link from the carrier to the enterprise. In this model, the path from the mobile worker to the enterprise is via the carrier network and then to the enterprise using the public Internet.



WWAN & Internet

Again, data security over the wireless link depends on the access technology and the wireless carrier involved. In addition, unless an enterprise provides its own security solution, the risks associated with this model are severe because information traverses the public Internet on its way to and from an enterprise data center. The number of security threats that exist for communications across the public Internet are, of course, legion.

Placing a firewall at the perimeter of the enterprise network offers some protection because it helps to secure the type of traffic allowed in or out of the enterprise. But this approach is insufficient with regard to validating the integrity of the data and the identity of the mobile user or device – both essential aspects of mobile computing security.

WLAN

In the WLAN industry, the IEEE 802.11a/b/g standards have made it possible for hardware vendors to create interoperable systems. The success of these initiatives has resulted in a high WLAN adoption rate in the corporate environment, both inside and outside the trusted network.

But with this success has come an increased risk to corporate security. Security options included with older wireless access points have been repeatedly shown to be insufficient.

- **Wired Equivalent Privacy** (WEP) is easily compromised and its exploits are well documented.
- **Wi-Fi Protected Access** (WPA) improved some of the deficiencies of WEP, but even WPA is susceptible to brute force dictionary attacks (to retrieve pre-shared keys used in authenticating a device to the access point) and Message Integrity Check (MIC) Denial of Service attacks.

Newer standards are far more robust.

- **802.11i Counter-Mode/CBC-MAC Protocol** (CCMP) uses 128-bit keys and as of publication, has not been broken. WPA2 is the Wi-Fi Alliance's name for 802.11i certification testing.
- **802.1x** addresses many of the device to access point authentication issues. Of particular note is how it incorporates RADIUS servers, typically between authenticator and authentication server.

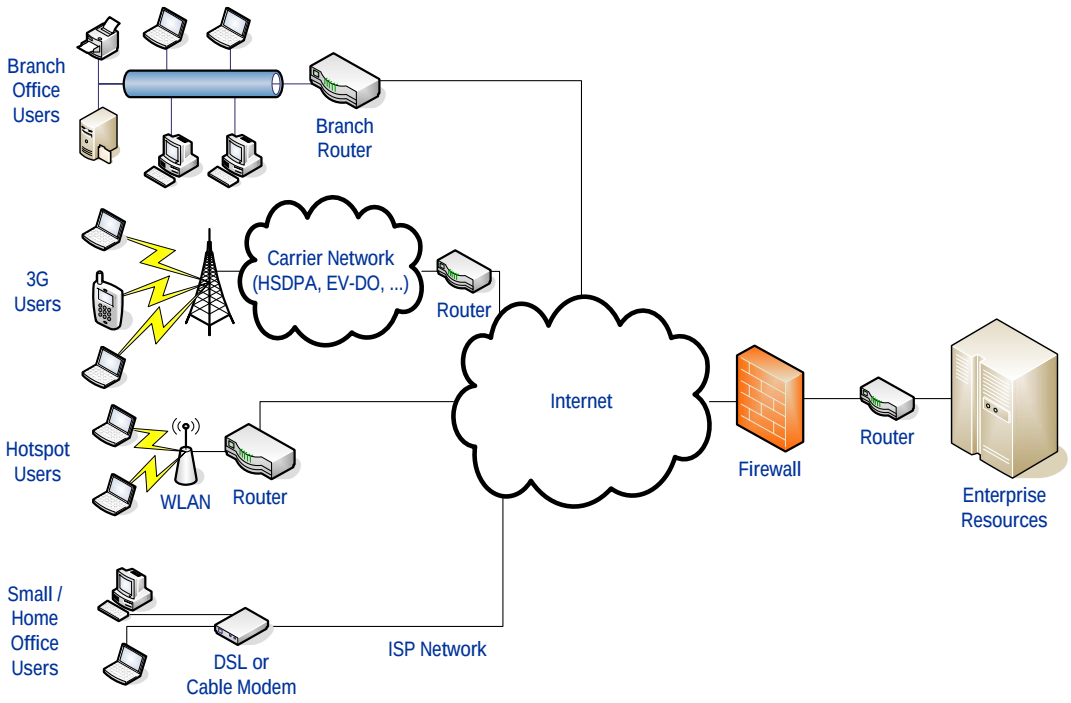
These improvements are needed and welcome, and NetMotion Wireless recommends that organizations implement them. However, many older access points may not support these new standards, and organizations may be forced to either replace their infrastructure, or configure their access points for the security protocol common to all devices.

WLAN Hotspots

Additional challenges ensue when mobile workers are using public hotspots: publicly accessible Wi-Fi hotspots which are connected to the enterprise. Repeated studies have shown that absent strong authentication and encryption, enterprise data is at risk when workers connect via the hotspots available in coffee shops and other public areas. Furthermore, incorrectly configured laptops and handhelds are at greater risk when connecting over hotspots, as they are effectively on a LAN with all other devices connected to that hotspot, or even directly connected to other devices!

Multiple Networks

Enterprise use of multiple networks is a reality. Different mobile workers have different use cases. A single mobile worker may access enterprise resources from home via a home Wi-Fi network connected via DSL or a cable modem, travel to an office and use an Ethernet LAN, visit a customer site and connect via a WWAN such as HSPDA or EV-DO, or connect via a public hotspot at a coffee shop. Two different mobile workers performing the same role for the same company may need to use different WWAN networks because of different coverage in the areas they cover. A campus or large building may have multiple subnets.



Multiple Networks

This complexity mandates that whatever security choices are made be applicable across all networks in use or readily foreseen. Further, the security strategy must allow for the special requirements of wireless networks — coverage gaps, slower speeds, and higher latency.

All too often, the convenience, productivity and efficiency gained by adopting mobile and wireless solutions are offset by increased costs related to security, management and deployment. While it is not possible for an organization to physically manage and secure all of the external networks used for remote access, it is possible to validate the authenticity of the user and device, to secure and encrypt data, and to protect the privacy of the user. Traditional options for secure remote access require significant tradeoffs between productivity and security, thus reducing the value of the mobile solution. In essence, the historical axiom has been, "The more secure the solution, the lower the productivity."

Traditional Options for Secure Remote Access

An organization's security requirements are substantially dictated by the wireless infrastructure it uses (or plans to use). When using wireless networks, security at the perimeter, in the DMZ, and on the trusted network is as important as the need to manage and control users and devices. A comprehensive security solution must protect mobile devices, authenticate users to the corporate network, and protect the integrity of the data, regardless of the wired or wireless networks used. This section reviews solutions commonly available today and their performance over wireless networks.

IPSec and Mobile IP VPNs

Internet Protocol Security (IPSec)

One of the weaknesses of the original Internet protocol (TCP/IP) is that it did not include a means for ensuring the authenticity and privacy of data as it is passed over a public network. Operating at layer 3 of the OSI model, IP datagrams are typically routed between two devices over unknown networks. Without a secure IP header, information in the datagram can be intercepted or altered. This became a growing concern when people started using the Internet to transfer sensitive data. Thus IP Security (IPSec) was developed. Its mission:

- Encryption of user data for privacy
- Authentication of the integrity of a message to ensure that it is not changed en route
- Protection against certain types of security attacks, such as replay attacks
- Establishment of a mechanism to negotiate the security algorithms and keys required to establish point-to-point security. IPSec uses the IKE (Internet Key Exchange) protocol for this.

IPSec on its own is not well-suited for wireless networks. IPSec "protects" the source IP address, which must remain static for the duration of the secure tunnel to validate the integrity of the sender. While this provides effective protection against spoofing, it also means that an IPSec VPN connection cannot survive wireless coverage gaps, loss of connectivity, or network transitions where the source address may change or be released. Resolving this weakness in IPSec is one of the missions of the Mobile IP working group.

A new development in IPSec is MOBIKE. MOBIKE is the IKEv2 Mobility and Multihoming protocol, an extension of the IKEv2 protocol. MOBIKE provides a method for a host with multiple IP addresses and/or where IP addresses may change over time (for example, due to mobility). While this is a positive development in that the VPN tunnel may be maintained and persisted during mobility, it does not address application session persistence.

All said, IPSec is ideal for fixed or site-to-site communications. However, earlier versions of IPSec create a user intensive login/logoff process when users hit coverage gaps, network transitions or suspend/resume cycles, and even the more recent MOBIKE implementations do not address application session issues. IPSec has poor wireless performance, and no application level control.

Mobile IP

Mobile IP is a modification to IP that allows a node to continue to send and receive datagrams regardless of where the node happens to be attached to the network. Mobile IP masks IP address changes, allowing transport layer connections to survive network transitions. It does this by pre-pending the IP header with a Mobile IP header (called IP in IP) that manages the source address. This overhead can be costly in bandwidth-sensitive networks and is further exacerbated when NAT traversal (NAT-T) is a requirement.

The security components of Mobile IP also address a security problem: redirection attacks. This is generally reasonable when one considers that redirection attacks are the only new vulnerability introduced by Mobile IP.

Mobile IP is sometimes used to augment IPSec for the purpose of hiding IP address changes while roaming, but when done so, several layers of encapsulation and tunneling are required. This can include an IPSec encapsulation for protecting the endpoint data, a mobile IP encapsulation to hide the address changes, and a second IPSec encapsulation for Home Agent, Foreign Agent security. This excessive use of encapsulation and tunneling and the associated overhead make this approach inappropriate for most wireless networks.

Redirection Attacks

A redirection attack occurs when a "malicious node" gives false information to a home agent in a Mobile IP network. The home agent is informed that the mobile node has a new care-of address. In reality, the new care-of address is controlled by the malicious node. After this false registration occurs, all IP datagrams addressed to the mobile node are redirected to the malicious node.

Mobile IP does not address other security risks associated with distributed networks. Any implementation of Mobile IP that is targeted at unsecured networks, such as a wireless network, should incorporate other security mechanisms.

SSL VPNs

SSL VPN solutions are designed to secure application streams between remote users and an SSL VPN gateway. In contrast with IPSec VPNs, which connect remote devices to trusted networks, SSL VPNs connect remote users (independent of device) to specific applications and network resources inside trusted networks. SSL VPNs are a security solution for web-based traffic. The SSL client is pre-built into many of the web browsers common to today's operating systems, including Windows, Macintosh, Linux, Palm, Symbian, and Windows Mobile. The SSL VPN solution is also well-suited for communicating to resources in a trusted network from non-corporate devices such as kiosks, Internet cafés, or an employee's own computer.

Though clearly convenient, these scenarios introduce a number of privacy- and security-related vulnerabilities. Connecting to the enterprise network from non-trusted devices leaves the user vulnerable to keyboard recording utilities. The user may also leave behind cookies and data that were cached during a browsing session. To address this vulnerability, most SSL VPN solutions use ActiveX or JAVA applet utilities to "clean up" after a user by deleting the local cache and cookies when a session ends. Enterprises also are susceptible to worms or Trojans that may have infected non-trusted equipment used during an SSL session. SSL VPN vendors are addressing these threats using cooperative enforcement with third-party client software such as antivirus or personal firewall software. Additional SSL VPN utilities (ActiveX or JAVA applets) are downloaded to ensure that the remote device is running the proper security software (checking for the latest antivirus definition files, for example) prior to allowing access.

SSL VPN solution providers have been very responsive to addressing these vulnerabilities as their reach has expanded. At the same time, the complexity of SSL VPN deployments has increased to satisfy the requirements of a secure computing environment. The method for addressing these vulnerabilities is elegant in that it is performed without much user intervention and within a browser environment. The trade-off is that the browser must be enabled to support the download of ActiveX controls and Java applets, both of which have a number of documented vulnerabilities.

Additionally, SSL VPN solutions have had a hard time maintaining application compatibility. As a result, the vendors have been forced to develop ActiveX, Java or other client-based software to help maintain application compatibility. Further, administrators may have to add additional configuration per application.

The allure of SSL VPNs has been their clientless nature, inherent simplicity and initial basis in accepted security standards. But with the need for ActiveX, Java or Win32 controls deployed to the client, and the need for configuration to maintain application compatibility – often on a per-application basis, SSL VPN solutions can quickly become neither clientless nor simple.

SSL VPN solutions fall down in additional areas for mobile and wireless use. They do not handle roaming between networks, coverage gaps or intermittent connectivity without data loss. Additionally, their design using the SSL protocol operating at layer 7 (typically using the chatty TCP protocol rather than the more efficient UDP protocol) results in lower performance, which can be crucial over wireless networks.

Some SSL VPN vendors now recognize these shortcomings, and are attempting to address them, and are claiming primitive roaming and session persistence support. Here are a few key questions to consider:

- Mobile workers often move from the office to a customer site. Will the VPN roam successfully from an internal address to an external address without any intervention by the user or loss of data?
- Mobile workers need to suspend/resume devices to make the most efficient use of their batteries. Will the VPN support application session persistence through a suspend/resume event?
- Coverage may be poor in areas frequented by mobile workers, such as elevators, and parking garages. Can the VPN ensure that there will be no data lost if there is a coverage gap?
- Does the VPN optimize traffic over slower, higher latency wireless networks?
- Will users run VoIP or other real-time applications? Both WWAN and WLAN networks have much higher error rates (ranging from 1% to 70% depending on time and location) than wired networks. SSL VPN's using TCP as their transport perform very poorly handling these applications over these networks.

Finally, one key security concern is policy enforcement. While IPSec can enforce policies at layer 3, SSL VPNs enforce policies at the application level (layer 7). However, experience has shown that different policies may be required for identical applications when they connect via different networks – thus a mix policies for layers 2 through 7 is optimal for mobile workers.

For more information on the relative merits of IPSec, SSL and Mobile VPNs, consult the Yankee Group's paper, *Optimize Enterprise Productivity Through Mobility: Choosing the Right VPN Solution*, available on the NetMotion Wireless website.

Mobility XE

NetMotion Wireless' Mobility XE is a mobile VPN. It is a standards-based, secure, virtual private network designed for wireless networking. Mobility XE is designed with an understanding of disparate network types. It provides a seamless solution for users transitioning from home networks to hotspots and to mixed vendor environments, be they WWANs or WLANs It offers single-sign-on authentication through Microsoft Active Directory, RADIUS, and RSA SecurID. It also uses standard Microsoft® Windows® login credentials so there are no additional steps to learn or passwords to remember.

Mobility XE encrypts all data transmitted between the client and server using 128-bit (or stronger) AES and offers the advantages of IPSec solutions without its configuration, client provisioning, and management burdens. Mobility is a layer 4 VPN optimized for both wide and local area wireless networks. The transport layer implementation allows Mobility XE to manage and protect the data flow from the application layer by acting as a proxy for the local application queries at the Mobility XE server. In addition, Mobility XE's location in the TCP/IP stack allows it to seamlessly roam from one network to another. No matter what network a client device moves to, the mobile worker is automatically authenticated and the encrypted tunnel is established.

<table>
<tr><th>OSI Layer</th><th>TCP/IP Internet Protocol</th><th>Security Model</th></tr>
<tr><td>Application
Layer 7</td><td></td><td rowspan="2">SSL</td></tr>
<tr><td>Presentation
Layer 6</td><td rowspan="2">Telnet, FTP, SMTP, etc</td><td></td></tr>
<tr><td>Session
Layer 5</td><td rowspan="2">Mobility XE</td></tr>
<tr><td>Transport
Layer 4</td><td>Transmission Control Protocol (TCP)
Unacknowledged Datagram Protocol (UDP)</td></tr>
<tr><td>Network
Layer 3</td><td>Internet Protocol</td><td>IPSec</td></tr>
<tr><td rowspan="2">Data Link
Layer 2</td><td>Network interface cards: Ethernet, Token-Ring, FDDI, ATM, etc.</td><td></td></tr>
<tr><td>NIC drivers: Network Independent Interface Specification (NDIS),
Open Datalink Interface (ODI)</td><td></td></tr>
<tr><td>Physical
Layer 1</td><td>Transmission media:
Wireless media, fiber optic, coax, twisted pair, etc.</td><td></td></tr>
</table>

Security Model Comparison

The Mobility XE client is a software component with a small footprint that is transparent to the end user and does not require user configuration. Its location at the transport layer, below Winsock, allows Mobility to offer a secure end-to-end VPN for any application available to the mobile user or device.

The Mobility XE client also helps secure the mobile device and provides local network firewall capabilities. When the Mobility XE client is active it listens only on the active interface, and the only data path to the device is through the Mobility XE tunnel, which is established between the Mobility XE client and server. With Mobility XE connected the device is hardened against local network attacks (port scans, man-in-the-middle attacks, etc.)—it adds another layer of security to the remote workstation.

NetMotion Mobility XE Security Architecture

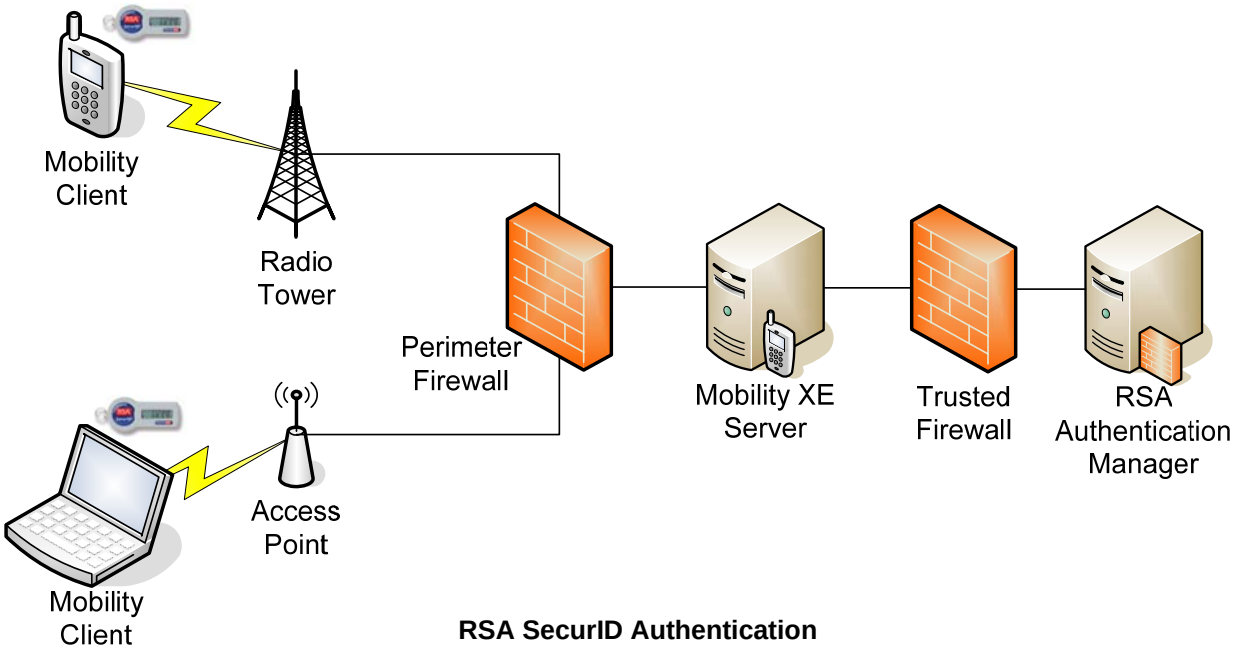
Authentication

Before Mobility XE begins transporting data between the network and NetMotion Mobility XE client, it must ensure that the end user has the required permissions. A user typically establishes his identity by logging in to the Mobility XE client using his Windows domain user name and password. Using the

Windows domain credentials allows for a single sign-on process and involves no extra work for the IT department. Single sign-on also gives users access to other domain resources, such as file system shares.

Once a user has been authenticated, Mobility XE establishes the communications path for transporting application data. NetMotion Mobility XE supports three protocols for user authentication:

- **NTLM (Windows users and groups, including Active Directory)**
  When a Mobility server is configured to use NTLM (version 2), users' credentials are authenticated against either the Windows domain that the Mobility server is a member of, or against local Windows users defined on the Mobility server itself. Users from other domains are allowed to connect if there is a trust between the domain the user is in and the Mobility server's domain.
- **RADIUS (Remote Authentication Dial-In User Service)**
  When using RADIUS, users' credentials are sent to specified RADIUS servers for authentication. Mobility XE supports three authentication protocols: RADIUS - LEAP, RADIUS - PEAP, and RADIUS - MD5.
- **RSA SecurID**
  Mobility supports native SecurID authentication. Mobility XE servers communicate directly with the RSA Authentication Manager using Authentication Agent software installed on the Mobility server machine. RSA SecurID two-factor authentication meets RSA certification criteria, including native authentication via the RSA Authentication Agent and support for new PIN Mode and Next Tokencode Mode. Key fobs, PINpads, USB tokens, smart card tokens and software tokens are supported, and the implementation has been certified as RSA SecurID Ready. For more information about Mobility XE and RSA authentication see Tech Notes 2214 *Enabling native RSA SecurID Connections for Mobility Clients*, and 2150 *Enabling RSA SecurID Connections for RADIUS.*



RSA SecurID Authentication

With Mobility XE, unlike WEP, passwords are user-specific. Only one password is required of a user within the Windows domain, and any policies applied to that user (limited login times, for example) will also apply to his or her Mobility network access and all resources in the domain. For more information on authentication in general, see Tech Note 2177, *Setting up Mobility Authentication*.

Integration with Active Directory

When the Mobility server is configured to use the NTLMv2 protocol for user authentication (the default), its security is integrated with the security features in Windows 2000 and Windows 2003, including the Active Directory service. For a Mobility client to connect to a Mobility server and use Mobility XE services, the person using the client must have a user account on the Mobility server or in the domain in which the server participates. He must also be a member of either the local NetMotion Users group or of a specified domain user group. The Mobility XE setup program creates the local NetMotion Users group during installation, and allows the administrator to specify a global domain user group that contains users who are allowed to connect to a Mobility server.

NetMotion Mobility Client and Server

On the mobile device running the Mobility client, data is processed at the session level. All application data destined for TCP and UDP sessions can be secured. (Connection-oriented applications generally use TCP for communications; others, like streaming media use UDP.) Address management allows all IP datagrams destined for mobile devices to be secured by the NetMotion Mobility server.

Encryption

Mobility uses FIPS 140-2 validated libraries for encryption: to encrypt and decrypt datagrams, and for key exchange. NetMotion Mobility offers the following types and levels of encryption, allowing administrators to weigh performance against security strength:

- **AES/Rijndael**. AES is the Advanced Encryption Standard for the United States. This algorithm is used to encrypt datagram traffic which will be sent across the network. The default setting is 128-bit key strength. Administrators may also choose 192-bit and 256-bit key strengths.
- **Elliptic Curve Diffie-Hellman** (ECDH). This algorithm is used for key exchange. The key sizes for ECDH are chosen based on the AES key size as recommended by NIST in FIPS PUB 186-2, "Digital Signature Standard."

AES Key Size	ECDH Key Size
128	256
192	384
256	521

Corresponding AES & ECDH Key Sizes

Security Protocols

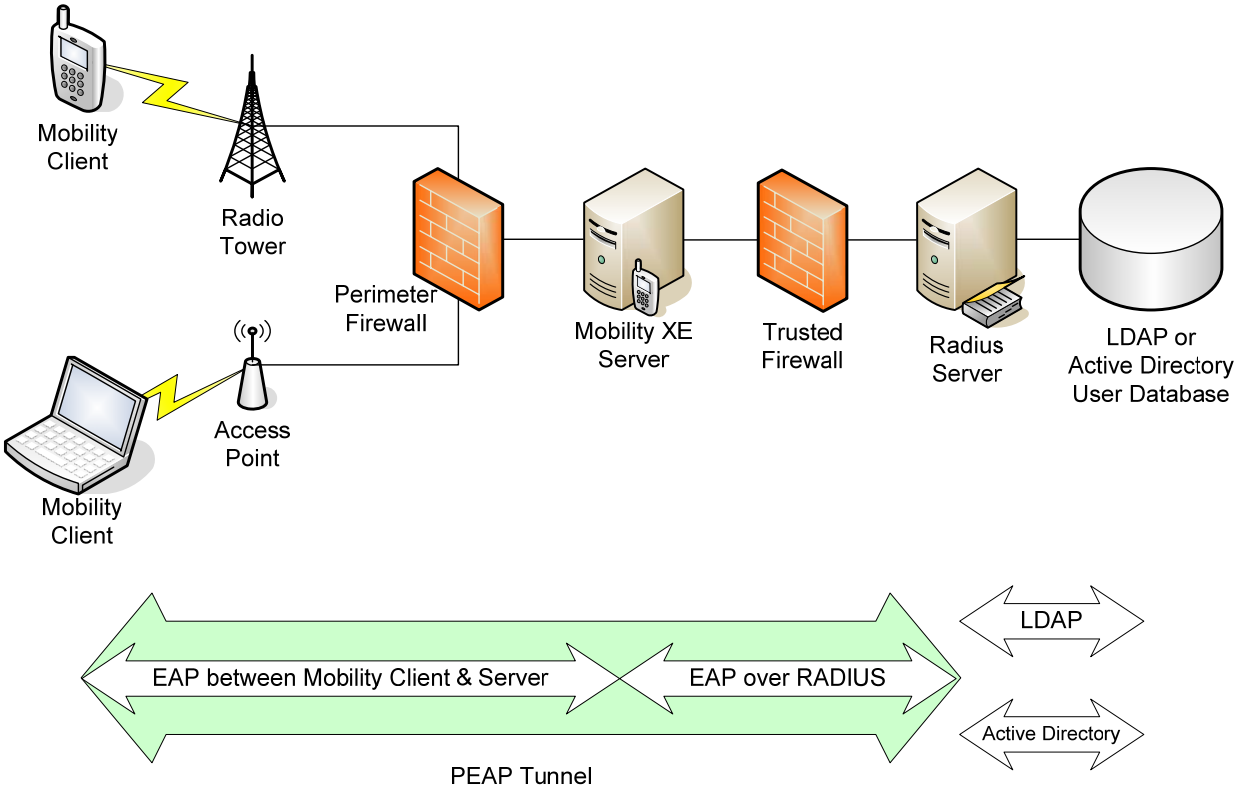
For secure connections, authentication and encryption processes are shared between the Mobility server and client. NetMotion Mobility XE synchronizes the processes by exchanging security protocol messages between the server and client. Here are several authentication examples, followed by additional notes regarding encryption.

NTLMv2 Authentication

The basic components of this exchange are as follows. NetMotion Mobility uses the NTLM version 2 challenge/response protocol to authenticate and validate the user. The client sends the user name and domain information as part of an NTLM "hash". The server challenges the client with a nonce. The client then uses the challenge, password, and other information to generate a hashed response. The connection is disallowed if this response does not match the value calculated by the server. If the values match, the user is successfully authenticated.

RADIUS Authentication via PEAP

PEAP is the Protected Extensible Authentication Protocol, jointly proposed by Cisco, Microsoft and RSA. It uses a server-side PKI certificate to create a secure TLS tunnel to protect user authentication. It is the outside wrapper – there is always another protocol inside it. As it is extensible, PEAP allows different inner authentication protocols. Mobility XE supports two PEAP sub-types EAP-MSCHAPv2, and EAP-GTC.



RADIUS, PEAPand EAP Methods

Under PEAP, the NetMotion Mobility Server acts as a pass through authenticator. The RADIUS server is the authenticator. The Mobility Client is the supplicant. They use certificates and public key methods to establish a secure tunnel in which authentication information can be delivered to the RADIUS server. Once the client is authenticated, the RADIUS server informs the Mobility Server of the result.

After Authentication

The Mobility server sends the Mobility client a data-security-level specification (turning encryption on or off). The server mandates the data security level—it is not negotiated—which prevents possible downgrade attacks.

A signed Diffie-Hellman key exchange occurs between the Mobility client and server that establishes the encryption keys for the session. When a Mobility client connects to a Mobility server, the fastest key computation method that they have in common is automatically negotiated.

For NTMLv2 and LEAP authentication, Mobility protects against man-in-the-middle attacks by signing the Diffie-Hellman parameters in the key exchange. The receiver authenticates the parameters by checking the signature.

Automatic re-keying enhances Mobility VPN security by periodically changing the keys used to encrypt data passing between the Mobility client and server. When re-keying is enabled, the server initiates a key

exchange with each client connection at random times within a configurable re-key interval. The exchange produces a new, unique session key for each client connection; it is unrelated to the previous key, so compromising one key does not compromise future communication based on the new key.

Policy Management

IPSec and SSL VPNs

IPSec VPNs implement policies at layer 3 (network layer). This allows control by IP address, for example. These policies are enforced at the IPSec concentrator, allowing or denying the user access to a given network.

SSL VPNs implement policies at layer 7. Enforced at the SSL VPN appliance or server, they allow or deny a user access to a given application or resource.

Mobility XE

Mobility Policy Management allows the administrator to centrally define rules and rule sets that can enforce policy from layer 2 to layer 7. For example, rules can be defined using interface name, speed, SSID, BSSID (all layer 2), transport (layer 4), session (layer 5), and application (layer 7).

In addition, the policy is deployed to each mobile device or user and enforced at the end point. There is no bandwidth cost in denying access and securing internal networks or resources.

User or device policy is defined on an interface or network basis. That is, an administrator can choose to enforce layer 2 through layer 7 security based on the networks available to the device or user. For example, an administrator may wish to prevent bandwidth-heavy applications from passing traffic while on a bandwidth-sensitive WWAN or if the connection speed of that network is below a certain (definable) threshold (i.e., less than 256kbps). This granular approach to policy management allows the administrator to centrally manage and control WWAN costs, bandwidth usage, and user experience while applying a solution that is consistent with the organization's security policies.

	IPSec VPN	SSL VPN	Mobility XE
Layer(s)	Layer 3	Layer 7	Layer 2 through 7
Created	At the concentrator	At the server appliance	At the server
Enforced	At the concentrator	At the server appliance	At the client
Paradigm	User by network	User by application	User by interface, network, application
Control access to	Networks	Applications & resources	Networks, applications & resources

VPN Comparison

	Mobility XE VPN	IPSec	SSL
Standards-based key exchange	Yes	Yes	Yes
Standards-based encryption	Yes	Yes	Yes
Integrates with existing authentication schema	Yes	Yes	Yes
Device-to-DMZ security	Yes	Yes	Yes
Wireless-friendly	Yes	No	Tolerant
Seamless roaming (fast handoffs)	Yes	No	Yes
Seamless roaming (slow handoffs -- out-of-range conditions or suspend and resume operations)	Yes	No	No
Application session persistence	Yes	No	No*
Data compression	Yes	Some	Some
Web image acceleration	Yes	No	No
Link optimizations	Yes	No	No
QoS and DSCP support	Yes	Some	Some
Compatible with Win32 applications without modification	Yes	Yes	No**
Transparency (ease of use)	Yes	No	Yes***
NAT-friendly	Yes	No****	Yes
Quarantine by device or user	Yes	Yes	Yes
Policy Management	Layer 2 through 7	Layer 3	Layer 7
Client required for Win32 applications	Yes	Yes	Yes
Support for secure, clientless connectivity	No	No	Yes
Multi-platform support	Windows-only	Yes	Yes

*Some SSL VPN vendors provide extremely limited session persistence based.

**Requires the installation and configuration of client software

***For web based traffic

****Many third-party IPSec solutions are now supporting the NAT-T RFC

Increased Productivity

Application Session Persistence and Wireless Optimizations

In addition to being a secure VPN, NetMotion Mobility actually increases mobile worker productivity by addressing their specific needs, via wireless optimizations and network and application session persistence.

- Wireless optimizations mean that data is transmitted as efficiently as possible: Mobility provides the ability to automatically switch to the fastest bandwidth network connection when multiple connections (Wi-Fi and GPRS, for example) are active. (For more on how Mobility provides optimum performance over intermittent and bandwidth-challenged network links, see our white paper, NetMotion Mobility Link Optimizations.)
- Network session persistence means that users don't have to repeat the login process when they move from one IP subnet to another, or when they go out of range of the network and return, or suspend & resume. NetMotion Mobility automatically re-authenticates the connection every time users roam, without user intervention.
- Application session persistence means that standard network applications remain connected to their peers, preventing the loss of valuable user time and data. For example, some major airline carriers offer high-speed, wireless access using the 802.11b protocol ("hotspots") in their terminals and waiting areas. Any customer with a mobile device equipped with a WLAN card can gain access to the Internet, corporate network, and e-mail. You open your laptop in the nearest cafe, log in to the corporate network, and start transferring data. But what happens when your flight is announced and you move to the gate at the other end of the terminal? The Mobility user suspends his laptop, moves to the new area, and then resumes the session. The user without NetMotion Mobility has to start from the beginning again: log in, get authenticated, re-open the application, and restart the transfer.

Quality of Service & DSCP

QoS (Quality of Service) & DSCP (Differentiated Services Code Point) support can be crucial to maintaining productivity as workers move from high-speed, high-bandwidth networks, to lower capacity, high latency networks. For example, while connected to the LAN via Ethernet, performance may be just fine for the mission-critical enterprise application, running alongside e-mail, web browsing, and other applications. But on a WWAN, administrators want to prioritize use of the narrower bandwidth, and make sure that a web browser and e-mail client do not use capacity needed by the enterprise application. Other VPNs may allow administrators to shut off non-essential applications.

Mobility XE allows administrators to specify Quality of Service parameters which are applied between the Mobility client and server, and additionally put DSCP settings which can be used as network traffic moves beyond the Mobility server. In particular, Mobility XE allows for different settings based on the network and its characteristics — there can be one set of QoS rules applied to a 1xRTT network, another to EV-DO, etc.

This allows an enterprise application to always have the appropriate share of network resources, but other, non-critical applications to use whatever bandwidth is available once the enterprise application has used what it needs or is assigned.

Deploying NetMotion Mobility Securely

For Mobility security to be effective, it must be deployed in a secure fashion in concert with other security mechanisms and practices. NetMotion Wireless makes recommendations regarding both server and client deployment.

Server Deployment

Regarding server deployment, we recommend that organizations follow both Microsoft and U.S. government recommendations regarding hardening Windows servers. See the resources listed at the end of the paper for specific recommendations. Beginning with version 7.2, Mobility XE server includes hardened server testing following the Windows Server Hardening Guide.

If a Mobility server is going to be accessed by users outside an internal WLAN (or LAN), NetMotion Wireless recommends that Mobility servers be deployed in a firewall DMZ, with port 5008 (or other port as chosen by the administrator) open in the external firewall. If authentication is to a RADIUS server or RSA server, these should be deployed inside the internal firewall.

Should organizations decide to deploy a Mobility server in locations other than a DMZ, specific suggestions for locations and settings can be found in Tech Note 2161 *Where to Deploy your Mobility Server*.

Extending the Firewall

The NetMotion Mobility server, located behind the corporate firewall, acts as a transport-level proxy. As a proxy for all network traffic, user transactions are forced through controlled software that protects the user's machine from attacks using malformed packets, buffer overflows, fragmentation errors, and port scanning. Because NetMotion Mobility is a transport-level proxy, it provides this protection for a wide range of applications.

Client Deployment

Depending on your requirements, Mobility can be used to strongly tighten security, particularly by client lockdown — forcing clients to use the Mobility VPN (preventing network access other than through the VPN tunnel to the Mobility server), by putting lost or stolen devices in quarantine, and by preventing access from new devices.

- **Client lockdown**. This ensures that *all* IP traffic is tunneled through the Mobility server. This forces implementation of the policy management rules. For example, an administrator could limit the IP addresses that can be accessed, and the applications that can use the network by a Mobility client while traffic is tunneled through to the server. If however, the Mobility client is bypassed, the client system could access otherwise forbidden IP addresses and unapproved applications could access the network. With lockdown in place, the security can be substantially enhanced, and is especially valuable when users access the network via public hotspots.
- **Quarantine — Lost or Stolen Devices**. A client in quarantine has no access to network resources. This is useful in case of lost or stolen devices – an administrator can put the device in this state, securing the network, data and applications.
- **Quarantine — Preventing Access from New Devices**. A common use of the Quarantine feature is to put all new client devices in quarantine until approved by the administrator. The new device can register, but is then immediately disconnected, allowing the administrator to then go back and validate any newly connected devices. This keeps unauthorized devices off the network, even if the user has valid credentials.

NetMotion Wireless recommends a strong password policy:

- Change passwords frequently

- Avoid short, common words
- Use a combination of letters, numbers and other characters

Other Security Components & Interoperability

A Mobile VPN is only part of a secure system. Security-conscious enterprises use additional solutions to further secure and protect their mobile devices. NetMotion Mobility has been tested with and complements these solutions:

- **Anti-virus:** Maintaining and requiring the latest anti-virus definition files is crucial. Mobility interoperates with common cooperative enforcement solutions (Network Access Control), which restrict network access to security-compliant devices.
- **Distributed firewall:** Personal or distributed firewalls (like anti-virus solutions) have become commonplace. Mobility is compatible with mobile device firewall solutions commonly used on both the Windows and Windows Mobile platforms.
- **Device authentication:** Requiring a user to authenticate to a device before authenticating to the network is becoming more and more common, especially with handheld devices that are often set down when the user performs other tasks (like handing over a package or working on a piece of equipment). Because these devices have a higher risk of being lost or stolen, many organizations are requiring that the data stored on them be encrypted and locked. These device authentication and encryption solutions can be paired with Mobility to provide a unique authentication solution.
- **Device security:** Encrypting the data stored locally on mobile devices, and preventing the leaking of data via USB drives and other removable media. If a device is compromised, some device security solutions include a poison pill that destroys the data on the device after a failed login threshold has been met or upon a command from the network administrator.
- **Mobility management:** Patch management, and software updates are features common to mobility management solutions. These mobility management tasks will occur within the secure tunnel provided by Mobility, and are even optimized by Mobility's link optimizations.

Ongoing Development

Security moves quickly. New security standards and technologies continue to be developed and adopted. NetMotion Wireless is actively engaged in the international community of industry trade groups and standards-making bodies that follow and shape security, mobility, and wireless technologies. We continue to incorporate and complement these standards and technologies as they are adopted in the marketplace. Please check our website, http://www.netmotionwireless.com for up to date information.

Resources

IEEE, "802.11 Standard," November 1997

IETF, RFC 2002, IP Mobility Support, October 1996

IETF, RFC 2474 Differentiated Services Field (DS field) in the IPv4 and IPv6 Header, December 1998

IETF, RFC 4621, Design of the IKEv2 Multihoming and Mobility Protocol, August, 2006

NetMotion Wireless Tech Notes, www.netmotionwireless.com

Paul Leach and Dan Perry, CIFS: A Common Internet File System, Microsoft, November 1996

Sandra Palumbo, Nathan Dyer and Eugene Signorini, *Optimize Enterprise Productivity Through Mobility: Choosing the Right VPN Solution*, December 2006. Available on www.netmotionwireless.com

Bruce Schneier, *Applied Cryptography: Protocols, Algorithms, and Source Code in C*, 2nd Edition, John Wiley & Sons, 1996

Security configuration guidance support, Article ID: 885409, updated 2007, support.microsoft.com

Step by Step Guide to Internet Protocol Security (IPSec), Microsoft, February 2000

Wagner, D. *GSM Cloning*. http://www.isaac.cs.berkeley.edu/isaac/gsm.html (1998); accessed 28 October, 2006.

Wi-Fi Security, February 19, 2001. (From the Wi-Fi Alliance.)

Windows Server 2003 Security Guide, updated 2006, www.microsoft.com

Wireless Application Protocol, John Wiley & Sons, 1999

Elizabeth D. Zwicky, Simon Cooper, and D. Brent Chapman, *Building Internet Firewalls*, O'Reilly & Associates, 2000