Security for Wireless Networks
A Comparison Among SSL, IPSec and Mobile VPNs

WHITE PAPER
Executive Summary

Mainstream companies and organizations throughout the world are incorporating mobile access via wireless networks into their remote access strategies. These mobile solutions go beyond traditional remote access via wired networks, such as dialup and at-home Internet access. The goals include improved business productivity and reduced operating costs. But wireless access also increases the complexity and challenges of security issues, such as user authentication and data security, compared to simpler systems of the past.

<table>
<thead>
<tr>
<th>Benefits</th>
<th>Risks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Increase productivity</td>
<td>Lack of enterprise control</td>
</tr>
<tr>
<td>Improve efficiency</td>
<td>Critical data loss/leakage</td>
</tr>
<tr>
<td>Improve response time</td>
<td>Compliance issues</td>
</tr>
</tbody>
</table>

**Benefits and Risks of Enterprise Mobility**  
*Source: Yankee Group, 2006*

Security is an essential component of a mobile deployment, but must be carefully considered so the organization reduces its risks while also reaping the rewards. Mobile workers do not generally adopt technologies or adhere to security practices that impede their productivity or hinder them from doing their “real job.” Security must be implemented without substantially degrading worker productivity and overall usability, or the mobility project will likely fail to meet its business objectives.

This paper outlines common wireless security considerations for typical enterprise mobile device deployments. It then evaluates common VPN solutions used for secure remote access in comparison to NetMotion Mobility XE.

Mobility XE is a mobile VPN that combines tight security with industry-leading productivity features. It provides strong user authentication and FIPS 140-2 validated encryption, and unlike other solutions, does not require administrators to sacrifice mobile worker usability or productivity in favor of security. It is a transparent solution that typically results in lower IT support costs, and is designed specifically for mobile workers using wireless networks. Mobility XE is optimized for WWAN, WLAN, or any other IP-based network that mobile workers use for remote access including Ethernet LANs, home networks, dialup, and public and private hotspots.

**Topics Covered**

This paper analyzes the security implications of mobile remote access via wireless networks, and considers the following topics:

- Access methods, including WWAN, Internet, WLAN and the use of multiple networks
- Traditional options for secure remote access, including IPSec and SSL VPNs
- The Mobility XE mobile VPN, including authentication, encryption, security protocols, policy management, network access control, and productivity-enhancing features
- Measures for secure deployment
- Ongoing development
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 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 unauthorized users?
There are a number of techniques used to combat these threats:

- **Authentication** helps provide reasonable assurance that the user and device attempting to connect are, in fact, who they claim to be.
- **Encryption** assures that the data in transmission has not been altered, and that no one can eavesdrop on the transmission.
- **Network Access Control (NAC)** ensures that devices that connect to internal networks are configured correctly and have prescribed security measures that are installed, enabled, and up-to-date.
- **Policies** protect both the network and the device, providing controlled access to each.

### VPN Security Techniques

<table>
<thead>
<tr>
<th>Authentication</th>
<th>Encryption</th>
<th>Network Access Control (NAC)</th>
<th>Policies</th>
</tr>
</thead>
<tbody>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
</tbody>
</table>

**Access Methods & Networks**

The two most common wireless access methods are wireless WANs (WWANs) operated by public cellular data carriers or private owners, and wireless LANs (WLANs) operated by private companies or by publicly accessible hotspot providers. Most legacy private radio networks owned by state and local municipalities are gradually being replaced or augmented by the publicly available WWANs and WLANs.

**WWANs Using Public Backhaul (Internet)**

Wireless wide area networks operated by cellular data carriers use technologies such as 1xRTT, 1xEV-DO Rev. A, EDGE, UMTS, HSDPA, HSUPA and WiMax. These networks provide cost-effective solutions for keeping mobile workers in contact with the enterprise. By default, data traffic is routed through the public Internet.

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. Internet-based routing typically is a more affordable solution than a dedicated network (described in the next section) because it does not require a dedicated link from the carrier to the enterprise.
Data security over the wireless link depends on the access technology and the wireless carrier. 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, well-publicized.

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 are essential aspects of mobile computing security.

**WWANs Using Private, Dedicated Backhaul**

Some WWAN providers provide dedicated routing options with a private data connection — via a dedicated frame relay (or sometimes ATM) — from the carrier’s network to the enterprise’s private network.
WWANs with a dedicated backhaul connection to the corporate network provide an additional layer of security, but the security used 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 the encryption key.

Once the data leaves the carrier’s network and is on the dedicated circuit, security becomes the responsibility of the individual mobile worker. In addition, lost or stolen mobile devices (or mobile data PC cards and wireless phones serving as modems) also pose very real security threats. For example, the security used on an EDGE network only uses a 64-bit key. Researchers at California Berkeley have demonstrated the ability to break the security protocol (comp128) within a day. Without additional security measures in place, such vulnerabilities can quickly put an enterprise at risk.

**WLANs**

In the WLAN industry, the IEEE 802.11b/g/n 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 many 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.

- **Wi-Fi Protected Access 2 (WPA2)** has replaced WPA. It uses a new AES-based algorithm called CCMP that uses 128-bit keys. WPA2 is the Wi-Fi Alliance’s name for 802.11i certification testing and as of publication, is generally accepted as a reasonably secure algorithm.
- **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 in WLAN security are needed and welcome. 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 lowest-common-denominator security protocol.

**WLAN Hotspots**

Additional challenges ensue when mobile workers use public Wi-Fi hotspots. Repeated studies have shown that absent strong authentication and encryption, enterprise data is at risk when workers connect via public 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 local LAN with all other devices connected to that hotspot. It is even possible for other devices to connect directly to them.

**Multiple Networks**

Many organizations have to rely on a combination of networks and network technologies to get the coverage necessary for their mobile workers. And different mobile workers have different use cases. A mobile worker may access enterprise resources after-hours over 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 WLAN for visitors; connect while traveling or out in the field using a carrier’s WWAN; and 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 their service areas.
Multiple networks and networking technologies present individual security challenges. Each may or may not have link-layer security implemented, much less configured correctly or totally up-to-date. Therefore, it is especially important to have a single, reliable security framework in place that will secure communications both over the air and through the Internet, regardless of the network infrastructure being used.

Furthermore, the security solution must allow for the special requirements of wireless networks such as 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, further reducing the value of the mobile solution in achieving the original business objectives. In essence, the historical axiom has been, “The greater the security, the lower the productivity.”

**Secure Remote Access: Traditional Options**

The number and types of wireless networks an organization uses play a major role in guiding the requirements for the mobile security infrastructure. When using wireless networks, security at the perimeter, in the DMZ, and on the trusted network are 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 network infrastructure in use.

This section reviews solutions commonly available today and their ability to help satisfy both the security and productivity requirements for mobile, wireless deployments.
**Internet Protocol Security (IPSec) VPNs**

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. IP datagrams are typically routed between two devices at layer 3 of the OSI model. Without a secure IP header, information in the datagram can be intercepted or altered by any entity on the routing path between the two devices. This became a major concern when individuals and organizations started using the Internet to transfer sensitive data. IP Security (IPSec) was developed to help solve the problem. Its mission:

- Authentication so that the transmitting and receiving parties can “trust” each other.
- 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.
- 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 on its own is not well-suited for wireless networks because its security association requires that the source IP address remain unchanged. While this provides effective protection against spoofing, it also means that an IPSec VPN connection cannot survive coverage gaps or loss of connectivity for any appreciable duration. Nor can it withstand network transitions where the source address may change or be released. Resolving this problem with IPSec is one of the objectives of the Mobile IP working group.

IPSec and Mobile IP also suffer from NAT-traversal challenges. And while there are solutions that help to resolve many of these issues, the solutions also come with a cost: significant protocol overhead. This can appreciably degrade the performance of wireless networks, especially on carrier data networks with variable, moderate-speed bandwidth and higher latency and jitter.

A new development in IPSec is MOBIKE — the IKEv2 Mobility and Multihoming protocol. MOBIKE provides a method for a mobile device with multiple IP addresses and/or IP addresses that may change over time (for example, due to mobility). While MOBIKE is a positive development in that the IPSec VPN tunnel can be maintained and persist during IP address changes due to wireless network mobility, MOBIKE does not shield the underlying applications from the adverse affects of the IP address changes. And neither MOBIKE nor MobileIP are capable of shielding the applications from connection gaps lasting more than a handful of seconds.

While IPSec is an ideal protocol for fixed, site-to-site communications, many vendors’ IPSec solutions have an onerous logon/logoff process when users hit coverage gaps, network transitions or suspend/resume cycles. Even the more recent MOBIKE implementations, which don’t require reauthentication when an IP address changes, do not address the application session issues.

**Mobile IP VPNs**

Mobile IP is an IEEE standard that modifies IP, allowing 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 additional protocol overhead can be costly in bandwidth-sensitive networks and is further exacerbated when NAT traversal (NAT-T) is a requirement.

**Mobile IP with IPSec.** Mobile IP is sometimes used to augment IPSec for the purpose of hiding IP address changes while roaming. This requires several additional layers for encapsulation and tunneling, including IPSec encapsulation for protecting the endpoint data, mobile IP encapsulation to hide the address changes, and a second IPSec encapsulation for Home Agent, Foreign Agent security. Excessive use of encapsulation and tunneling and the associated overhead make this approach inappropriate for most wireless networks, because it appreciably degrades throughput and mobile-worker productivity.
Redirection Attacks. The security components of Mobile IP also address a security problem: redirection attacks. This is generally reasonable when one considers that these attacks are the only new vulnerability introduced by Mobile IP. 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 to IPSec VPNs that connect remote devices to trusted networks, SSL VPNs connect remote users (independent of device) to specific applications and network resources inside of trusted networks. SSL VPNs are targeted at securing web-based traffic. The SSL client is pre-built into most common web browsers on mainstream operating systems, including Windows, MacOS, Linux, Palm, Symbian and Windows Mobile. SSL VPNs are 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 from untrusted devices leaves the user vulnerable to keyboard recording utilities, and may also leave behind cookies and data that were cached during a browsing session. To address these vulnerabilities, most SSL VPN solutions use ActiveX or JAVA applet utilities to “clean up” after a session by deleting the local cache and cookies.

Enterprises are also susceptible to worms or Trojans that may have infected non-trusted equipment used during an SSL session. SSL VPN vendors are attempting to address these threats by implementing Network Access Control functionality, including cooperative enforcement with third-party client software such as antivirus or personal firewall software. Additional SSL VPN utilities (ActiveX or JAVA applets) ensure that the remote device is running the proper security software (checking for the latest antivirus definition files, for example) prior to allowing access. Often, the need to download the ActiveX or JAVA applets as well as the NAC enforcement and remediation software, and then run the scans and remediate the device become extremely time-consuming for the user. They can extend the amount of time required to establish an SSL VPN session to many minutes depending on the speed of the connection.

SSL VPN solution providers have been very responsive in addressing 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 allow applications to run. Administrators may have to add additional configurations for each new application.

The allure of SSL VPNs has been their clientless nature, inherent simplicity and 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.

Issues Specific to Mobile Environments. SSL VPN solutions fall down in several respects that are specifically related to mobile and wireless use. They do not handle roaming between networks, crossing
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 materially degrade performance of wireless networks.

Some SSL VPN vendors now recognize these shortcomings, are attempting to address them, and claim 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 in handling these applications over wireless 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 of 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 specifically for wireless networking in highly mobile environments. Designed with an understanding of disparate network types, Mobility XE provides 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 supports running over any type of network that uses the IP network protocol including Ethernet, DSL and dial-up.

Mobility XE offers single-sign-on authentication through Microsoft Active Directory, RADIUS and RSA SecurID. The use of standard Microsoft® Windows® login credentials means there are no additional steps to learn or passwords to remember. In addition, Mobility XE supports two-factor user authentication using RSA SecurID tokens, smart cards or X.509c3 user certificates, allowing organizations to implement strong user authentication required by many industry and federal security mandates. It encrypts all data transmitted between the client and server using 128-bit (or stronger) AES, which has been FIPS 140-2 validated.

MobilityXE is an OSI layer 4 VPN. The transport layer (layer 4) implementation allows Mobility XE to manage and protect the data flow between the application (layer 7) and the networks (layer 3) by remotely proxying the mobile devices’ application queries on the Mobility XE server. It offers the application compatibility advantages of IPSec solutions without their configuration, client provisioning and management burdens.
Security for Wireless Networks White Paper

From a networking perspective, Mobility XE’s location above the TCP/IP stack allows it to seamlessly roam from one network to another. No matter what network a client device moves to, the user, applications and VPN tunnel are automatically shielded from the changes. From the operating system perspective, it works at the transport layer, below Winsock. This allows Mobility to offer a secure end-to-end VPN for any application running on the mobile device.

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. The client adds a layer of security to the mobile device and provides local network firewall capabilities, although it does not entirely replace the need for a local firewall. 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 established between the Mobility client and server. When Mobility XE is connected, the device is hardened against man-in-the-middle attacks, port scans, and other local network attacks.

**Mobility XE Security Architecture**

**Authentication**

Before Mobility XE begins transmitting data between the network and Mobility client, it ensures that the end user has successfully authenticated and has the required permissions. A user typically logs in to the Mobility client using Windows domain credentials – typically user name and password, or a certificate on a smart card. Using Windows domain credentials allows for a single sign-on process to the device, domain and VPN that gives users access to domain resources such as file system shares. Once a user has been authenticated, Mobility XE establishes the VPN tunnel for securely transmitting application data.

Mobility XE also supports strong user authentication using several different methods, including smart cards, X.509v3 user certificates, or RSA SecurID. Two-factor authentication methods require (1) something the user has (a smart card, device, or token) and (2) something the user knows (a PIN or password). Strong user authentication is important for protecting mobile devices that can be easily lost or stolen. Strong user authentication is also a requirement for many industries and government organizations required to comply with federal security mandates and standards.
Authentication Protocols

NetMotion Mobility XE supports these 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 RADIUS - LEAP, RADIUS - PEAP, and RADIUS – EAP-TLS.

- **RSA SecurID**
  Mobility XE supports native SecurID authentication. Mobility 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. 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.

Mobility XE does not require the user to use different credentials than are required to log in to the Windows domain, or additional credentials from the logon process. And domain policies applied to that user (limited login times, for example) are applied to his or her access to network and domain resources. 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 authentication protocol (the default), its security is integrated with the security features in Windows, 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 Windows machine running the Mobility server or in the domain in which the server participates. Users must also be members 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 configure a global domain user group that determines which users are allowed to connect to a Mobility server.

Two-Factor Authentication

Organizations dealing with sensitive or privileged data often require authentication stronger than traditional user name + password credentials. In some cases, such as in law enforcement, there are statutory requirements. For example, the federal Criminal Justice Information System (CJIS) specifies stringent user authentication requirements for municipalities that connect to CJIS via wireless networks, the Internet or dial-up. All newly procured systems must meet the standards, and existing systems must comply by September 30, 2010. Other federal regulations call for similar advanced authentication measures.

Mobility XE supports the following strong, two-factor user authentication methods:

- **RSA SecurID** uses key fobs and PIN pads as well as USB tokens, smart card and software tokens. The various supported devices all require that the user enter a PIN in order to access the revolving complex number.

Mobility XE also supports two-factor authentication in a manner that allows organizations to meet federal standards at minimal cost. It uses the RADIUS-EAP protocol as the front-end to Microsoft’s Active Directory Authentication and Public-Key Infrastructure (PKI). Because the Microsoft PKI infrastructure is bundled with their server operating systems, and with several free or low-cost RADIUS server options available, this approach is a very low-cost and robust option. It is especially useful for public safety agencies that must comply with the CJIS requirements, but may not have allocated the budget to bring their systems into compliance.

Two-Factor Authentication via X.509v3 Certificates, Smart Cards, RADIUS and PKI

This RADIUS/PKI approach supports:

- **Smart cards.** Mobility XE supports PKI smart cards from vendors that meet Microsoft’s smart card mini-driver requirements, and from vendors that provide a Microsoft Cryptographic Service Provider (CSP). Of particular note, Mobility XE supports smart cards conforming to these
requirements: Homeland Security Presidential Directive 12 (HSPD-12); Federal Information Processing Standards Publication 201 (FIPS 201); Personal Identity Verification (PIV) of Federal Employees and Contractors; and NIST Special Publication 800-78-1, Cryptographic Algorithms and Key Sizes for Personal Identity Verification.

- **X.509v3 user certificates.** Certificates are supported when stored on the mobile device in a protected location only accessible to users who successfully complete desktop authentication and who provide the user certificate password. Non-Microsoft PKI solutions are supported if they are compatible with X.509v3 user certificates, standard Microsoft CAPI-enabled access to those certificates, and the RADIUS EAP-TLS or EAP-TLS inside PEAP authentication protocol.

- **Biometric systems.** Mobility XE supports biometric systems where those systems are used in place of a PIN or password to unlock access to X.509v3 certificates. Mobility XE also supports biometric-based user authentication on the Ubtek and Wave biometric systems, which are commonly installed on Lenovo, Itronix, and Dell portable computers.

**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 such as streaming media use UDP.)

**Encryption**

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

- **AES.** 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. Mobility XE’s 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.”

<table>
<thead>
<tr>
<th>AES key size</th>
<th>ECDH key size</th>
</tr>
</thead>
<tbody>
<tr>
<td>128</td>
<td>256</td>
</tr>
<tr>
<td>192</td>
<td>384</td>
</tr>
<tr>
<td>256</td>
<td>521</td>
</tr>
</tbody>
</table>

**Corresponding AES & ECDH Key Sizes**

**Authentication Process**

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, PEAP and EAP Methods**

Under PEAP, the 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 (ECDH) 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 two automatically negotiate the fastest key computation method that they have in common.
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 controlling access to resources by IP address. These policies are enforced at the IPSec concentrator, allowing or denying the user access to a given network or resource address.

SSL VPNs implement policies at layer 7. Enforced at the SSL VPN appliance or server, these 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), IP address and port (layer 3), transport (layer 4), session (layer 5), and application (layer 7). In addition, the policies are deployed to each mobile device or user and enforced on the mobile computing device. There is no bandwidth cost in denying access and securing internal networks or resources.

Policies are 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). In addition, policies can combine multiple layers for more granular control. For instance, a policy can block the functioning of a particular named application, except to a specified address and/or port. This granular approach to policy management allows the administrator to centrally manage and control WWAN costs, bandwidth usage, and user experience while applying a powerful solution that is consistent with the organization’s security policies.

<table>
<thead>
<tr>
<th>Layer(s)</th>
<th>IPSec VPN</th>
<th>SSL VPN</th>
<th>Mobility XE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Created</td>
<td>Layer 3</td>
<td>Layer 7</td>
<td>Layer 2 through Layer 7</td>
</tr>
<tr>
<td>Enforced</td>
<td>At the concentrator</td>
<td>At the server appliance</td>
<td>At the server</td>
</tr>
<tr>
<td>Paradigm</td>
<td>At the concentrator</td>
<td>At the server appliance</td>
<td>At the client</td>
</tr>
<tr>
<td>Controls access to</td>
<td>Networks</td>
<td>Applications &amp; resources</td>
<td>Networks, applications &amp; resources</td>
</tr>
</tbody>
</table>

**Policy Enforcement Comparison**
Mobile Network Access Control

Mobile devices in the hands of naive and unsuspecting users have emerged as one of the greatest threats to organizational security. These devices can harbor key loggers and other malware, planted via unpatched security holes. Network Access Control (NAC) inspects devices to ensure that they are configured and patched correctly, and that security software (such as anti-virus, anti-spyware and firewalls) is up-to-date and running. If mobile devices are not properly configured, Mobility’s NAC module warns users, prevents or restricts network access, and facilitates remediation.

Many IPSec and SSL VPNs provide NAC capabilities or can co-exist with them. But in a mobile deployment, buttoning down security via tight NAC enforcement can seriously hamper productivity. For example, requiring a mobile worker to download a series of operating system updates or an antivirus signature file in the middle of the work day, while at a customer call, can take many minutes (and consume unnecessary bandwidth) if the user only has access via a WWAN network.

Mobility XE has an integrated Mobile NAC module that gives administrators great control and flexibility over when and how to enforce remediation policies. It monitors the complete security posture of a device and can detect when key security-related components are missing, disabled or out-of-date including:

- Antivirus
- Antispyware
- Firewall
- Operating system version
- Windows™ Update status
- Registry keys
- Other applications

Mobile NAC works hand-in-hand with the Mobility XE Policy Management module to push out highly customized warnings and apply remediation policies. Based on severity and connection speed, administrators can specify simple alert messages or remediation instructions, limit application access, launch websites, initiate software downloads, quarantine the device or disconnect it. For instance:

- If anti-virus signatures are more than seven days old, send a warning message
- If more than 14 days old, send a more strident warning message if on a WWAN connection, and initiate immediate download of the signature file on a fast Wi-Fi connection
- If more than 21 days old, quarantine the device immediately
# VPN Comparison

<table>
<thead>
<tr>
<th>Security</th>
<th>Mobility XE Mobile VPN</th>
<th>IPSec</th>
<th>SSL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Standards-based encryption</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>FIPS-140-2 validated encryption libraries</td>
<td>Yes</td>
<td>Some</td>
<td>Some</td>
</tr>
<tr>
<td>Standards-based authentication</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Integrates with existing authentication schema</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Support for CJIS-compliant smart cards &amp; certificates</td>
<td>Yes</td>
<td>Yes</td>
<td>Some</td>
</tr>
<tr>
<td>Network Access Control</td>
<td>Yes</td>
<td>Some</td>
<td>Yes</td>
</tr>
<tr>
<td>Quarantine by device or user</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Device-to-DMZ security</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Productivity</th>
<th>Mobility XE Mobile VPN</th>
<th>IPSec</th>
<th>SSL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wireless-friendly</td>
<td>Yes</td>
<td>No</td>
<td>Tolerant</td>
</tr>
<tr>
<td>Seamless roaming (fast handoffs)</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Seamless roaming (slow handoffs – out-of-range conditions or suspend and resume operations)</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Application session persistence</td>
<td>Yes</td>
<td>No</td>
<td>Very limited</td>
</tr>
<tr>
<td>Data compression</td>
<td>Yes</td>
<td>Some</td>
<td>Some</td>
</tr>
<tr>
<td>Link optimizations</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>QoS (DSCP) and traffic-shaping support</td>
<td>Yes</td>
<td>Some</td>
<td>Some</td>
</tr>
<tr>
<td>Win32 compatible, without modification</td>
<td>Yes</td>
<td>Yes</td>
<td>Requires client</td>
</tr>
<tr>
<td>Real-time application support</td>
<td>Yes</td>
<td>Yes</td>
<td>Very limited</td>
</tr>
<tr>
<td>Transparency (ease of use)</td>
<td>Yes</td>
<td>No</td>
<td>Web only</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Management</th>
<th>Mobility XE Mobile VPN</th>
<th>IPSec</th>
<th>SSL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Clientless connectivity</td>
<td>No</td>
<td>No</td>
<td>Web only</td>
</tr>
<tr>
<td>Multi-platform support</td>
<td>Microsoft OS only</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Full support for laptops &amp; Windows Mobile devices</td>
<td>Yes</td>
<td>Depends on vendor</td>
<td>Limited on Windows Mobile</td>
</tr>
<tr>
<td>Mobile-specific management information</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Policy management</td>
<td>Layers 2 through 7</td>
<td>Layer 3</td>
<td>Layer 7</td>
</tr>
<tr>
<td>Analytics on device / application / network use</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>NAT-friendly</td>
<td>Yes</td>
<td>Depends on vendor</td>
<td>Yes</td>
</tr>
</tbody>
</table>
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 the white paper *Technical Overview for System Administrators* on the NetMotion Wireless web site.)

- **Network session persistence** means that users don't have to repeat the login process when they move from one IP subnet to another, when they go out of range of the network and return, or suspend-and-resume. Mobility XE 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 through 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. Suppose a user opens a laptop in the nearest cafe, logs in to the corporate network, and starts transferring data. What happens when the flight is announced, requiring a move to the gate at the other end of the terminal? The Mobility user suspends the laptop, moves to the new area, and then resumes the session. By contrast, the user without Mobility XE has to start from the beginning again: log in, get authenticated, re-open the application, and restart the transfer.

Quality of Service

Quality of Service (QoS) support can be crucial to maintaining productivity for workers using wireless networks that have lower bandwidth and higher latency. 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.

Mobility XE allows administrators to specify Quality of Service policies which apply traffic shaping to prioritize and allocate the bandwidth available to different applications. They can also apply differential services code point (DSCP) tagging which can be used to prioritize the routing of application traffic as it moves through wireless networks and beyond the Mobility XE server. And the QoS policies respond dynamically as applications come and go, putting lower priority applications in the background when mission critical applications access the network. When the mission critical application(s) no longer need the network, the bandwidth is restored to the other applications.
Secure Deployment

For Mobility security to be effective, it must be deployed in a secure fashion in concert with other security mechanisms and practices.

Server Deployment

NetMotion Wireless recommends 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.

If a Mobility server is going to be accessed by users on public WLANs or WWANs, Mobility servers should be deployed in a firewall DMZ or behind the corporate firewall. Port 5008 (or other port as chosen by the administrator) must be open in the protecting firewall(s) to allow access to the Mobility server.

Specific suggestions for server pool locations and settings can be found in Tech Note 2161 Where to Deploy Your Mobility Server.

Extending the Firewall

The Mobility server acts as a transport-level proxy. Application 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 Mobility XE is a transport-level proxy, it provides this protection for a wide range of applications.

Client Deployment

Depending on security requirements, Mobility XE can be used to strongly tighten security on mobile devices. Administrators can force clients to use the Mobility VPN (preventing network access other than through the VPN tunnel to the Mobility server), put lost or stolen devices in quarantine, and prevent access from new devices.

- **Client lockdown.** When the Mobility client is connected, all IP traffic is tunneled through the Mobility server. In addition, while traffic is tunneled through to the server, an administrator can use the Policy Management module to limit the IP addresses that can be accessed by a Mobility client and the applications that can use the network. Putting lockdown in place substantially enhances security. This 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, preventing access to the corporate network, data and applications.

- **Quarantine — preventing access by new devices.** A common use of the Quarantine feature is to put all new client devices in quarantine until manually approved by an administrator. The new device can register, but is then immediately disconnected and placed in quarantine, 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.

Password Policy

NetMotion Wireless recommends a strong password policy:

- Change passwords frequently
- Avoid short, common words. Passwords should be more than 8 characters long.
- 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 XE’s NAC module interoperates with products from leading anti-virus vendors to ensure that protection is enabled and up-to-date.

- **Distributed firewall.** Personal or distributed firewalls have become commonplace. Mobility XE is compatible with many mobile-device firewall solutions commonly used on both the Windows and Windows Mobile platforms. The NAC module can verify that the firewall is enabled before allowing a connection.

- **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 (such as 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.** Solutions are available that encrypt the data stored locally on mobile devices, and prevent leakage of data via USB drives and other removable media. If a device is compromised, some include a device-wipe option that destroys the data on the device after a failed login threshold has been reached or in response to a command from a network administrator.

- **Device management.** Patch management and software updates are features common to device management solutions. Device management tasks occur within the secure tunnel provided by Mobility XE, and are further optimized by Mobility’s link optimizations.

Ongoing Development

Security moves quickly. New security standards and technologies continue to be developed and adopted. 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](http://www.netmotionwireless.com) for up-to-date information.
Resources

IEEE 802.11 LAN/MAN Wireless LANS, IEEE, November 1997, standards.ieee.org


Cryptographic Algorithms and Key Sizes for Personal Identity Verification, NIST Special Publication 800-78-1, August 2007, csrc.nist.gov

NetMotion Wireless Tech Notes, www.netmotionwireless.com


Personal Identity Verification (PIV) of Federal Employees and Contractors, Federal Information Processing Standards Publication 201-1, March 2006, csrc.nist.gov

RFC 2002, IP Mobility Support, IETF, October 1996

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

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


Security Configuration Guidance Support, Microsoft, Article ID: 885409, updated 2007, support.microsoft.com

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

© 2009 NetMotion Wireless, Inc. All rights reserved. NetMotion and NetMotion Mobility are registered trademarks, and Mobility XE, Roamable IPSec, InterNetwork Roaming, Best-Bandwidth Routing and Analytics Module are trademarks of NetMotion Wireless, Inc. Microsoft, Microsoft Windows, Active Directory, ActiveSync, Internet Explorer, Windows Mobile, Windows Server, Windows XP, SQL Server, Windows XP Tablet PC Edition and Windows Vista are registered trademarks of Microsoft Corporation. All other trademarks, trade names or company names referenced herein are used for identification purposes only and are the property of their respective owners. NetMotion technology is protected by one or more of the following US Patents: 6,918,920; 6,428,324; 6,546,425; 6,826,405; 6,981,047; 7,136,645; 7,293,407; and Canadian Patent 2,303,987. Other US and foreign patents pending.