

Thinking About

Integrating Mobile Access into your VPN Environment

Introduction

If you haven't already done so, you're likely to soon face the task of integrating a variety of access services and devices onto your Virtual Private Network (VPN). Most large organizations can't afford to ignore the productivity benefits of letting workers retain access to resources when they leave their desks. After all, mobile networks and broadband last-mile networks now reach far enough and deliver enough bandwidth to support LAN applications from nearly anywhere. If employees aren't forced off-line when away from their traditional wired work spaces, they can continue to participate in meetings and support supervisors and colleagues. This translates into bottom-line benefits.

Enterprise Integration Challenges

Expanding the VPN to include multiple access networks and device types bodes well for boosting revenues and productivity. But the IT department will face some integration challenges. For example, IT will likely aim to keep access simple for end-users, which could make it difficult to also ensure that the disparate services conform to a unified security policy.

IT departments are also tasked with meeting mobile user expectations for continuous coverage and adequate bandwidth, coordinating billing from several access service suppliers and tracking and managing many disparate remote devices.

Often, a global software client or Web-based portal that allows access to the VPN service via multiple access methods can help with ease of use. Depending on your philosophy, you might choose to deploy and manage the software client platform internally or in conjunction with a managed services provider or services aggregator. A service partner can often help unify and manage the billing, settlement and security issues, as well.

Let's look closer at some of the specific issues that arise when bringing new access methods onto your VPN.

Coverage and Capacity

By definition, mobile users can wind up in unpredictable locations, making it particularly challenging to assure that they always have network coverage and adequate bandwidth. For example, for truly mobile users, mobile WAN services – also called cellular or 3G services – offer the broadest coverage. However, today, the highest-speed mobile WAN services are generally available in the fewest locations.

How Workers Connect to the Network

	Remote Workers	Mobile Workers
DSL	70.4%	61.6%
Cable Modem	70.4%	57.6%
Dial-Up	63.2%	55.2%
Wi-Fi Hot Spot	32%	46.4%
Cellular Data Service	27.2%	36%
Other	9.6%	7.2%

Source: Eleventh Annual Network World 500 Research study, May 2005 (Multiple responses allowed / N=500)

The VPN is embracing many diverse access methods, posing new management and security challenges for IT.

Classify Users with Needs Assessment

A useful exercise in selecting packages of access services for users is to classify the remote-user population into categories based on a needs assessment. You'll want to determine how often an employee travels and where, as well as what each employee actually does when traveling.



For users who basically use mobile access to keep up with messaging, for example, a minimum-minutes mobile WAN service plan might be adequate. But if the worker is basically conducting business while on the road in lieu of a stationary office, you'll want to recreate a LAN-like atmosphere to the degree possible. This might entail a mix of home broadband and several mobile wireless service types. And international users will require services and devices that work globally, whereas domestic users will not.

Once you have users classified into groups, you can consider purchasing a suite of appropriate access services and device(s) for each group.

What to Ask Mobile Operators

Mobile WAN services will likely be part of the mix for at least some of your user population.

- **Balancing Speed and Availability** – There are many generations of mobile WAN networks in various stages of deployment. As a result, different services with varying associated speeds are available from area-to-area, and they work with different communications devices.

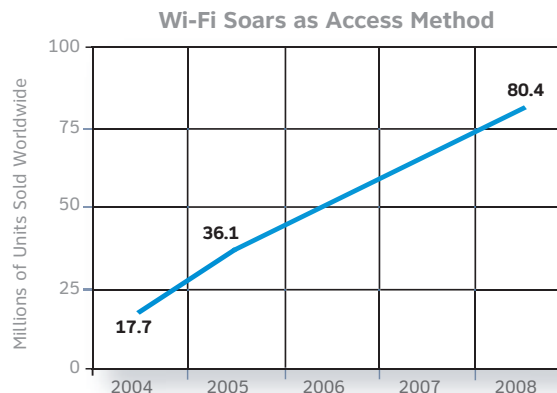
Be sure to match the appropriate device with the appropriate service. If you select a newer, high-speed service, ask the service provider whether it will “fall back” to the next-fastest service in non-coverage areas. Ask, too, whether the fall-back service will be accessible using the same device. Find out what the fall-back speed is, and whether it will meet the application needs of that user group.

Check as to whether roaming agreements are in place with a given provider or whether the service provider plays the role of aggregator to offer a larger coverage area. Often by merging the network footprints of multiple operators, users can get the collective effect of a seemingly much larger network.

If a user group will need both hot-spot (LAN-speed) and mobile WAN services, it might be financially beneficial to group them under a single billing plan, if available. Wi-Fi hot spots are available in increasing numbers of places, including airports, hotels, convention centers, coffee shops, restaurants and even airplanes, and many of the same providers offer a mix of Wi-Fi and mobile WAN services.

- **Internetwork Roaming** – You may wish to investigate a provider's plans for supporting Wi-Fi-to-cellular service handoffs. Dual-mode devices are emerging that support both 802.11 and mobile WAN connections, satisfying users' itch to carry a single device for both voice and data. This is one factor driving mobile operators to transparently enable a switchover from one network to the other as more bandwidth becomes available or as the available network type simply changes.

Real-time applications will also drive Wi-Fi-to-cellular roaming, because such sessions cannot tolerate a break in connectivity when users cross a network boundary. This type of transparent interconnectivity will also eventually be required for the successful implementation of presence-management applications and single-phone number support. It also will offer the potential for your business to save significantly on cellular phone bills when users are on-site.



Source: Infonetics Research, Inc.

Shipments of Wi-Fi equipment grew 51% from 2003 to 2004 and are projected to grow another 123% by 2008.

On-Premises Wi-Fi Architecture

Many organizations also are installing wireless LANs in-house, either for specific niche applications or to enable general employee mobility. Wi-Fi, or 802.11 technology, has come a long way since it first became standardized in 1997. Any wireless operation can be tricky, but here are a few tips to keep in mind.

- **Conduct a Site Survey** – An installation of a decent size requires a wireless LAN site survey. This exercise helps you determine where to install your access points (APs), the infrastructure radios that bridge your mobile users to your wired network. The site survey helps ensure that you place APs so that 802.11 users can always find a signal and access resources. Recent tools help automate this process. Generally, though, some amount of walking around with a scanner is required to unearth mysterious causes of interference and signal blockages.

The site survey should account for whether you plan to use the Wi-Fi network to support voice over IP (VoIP) alongside data. VoIP will require much broader coverage, finer tuning, and likely more channels for quality of service (QoS). Follow-up site surveys expose environmental changes and help you maintain performance.

- **Which 802.11 Technology(ies) to Use?** – At this juncture, you must decide what mix of 802.11 networks you plan to use: 802.11b, 802.11g, 802.11a and, possibly, the emerging 802.11n for 100-Mbps speeds and up. The 802.11n standard is not expected to be final until 2007.

The range, network speed, and interference issues vary with these network types. Adding 802.11a to the mix can be beneficial in dense populations and where voice is supported. 802.11a uses a different frequency than 802.11g/b, avoiding interference, and also supports many more channels than the other networks. A radio can only transmit on one channel at a time. The more channels you have, the more radios (and users) you can support in a tight geographic area. The downside to 802.11a is that most of the installed client base today is based on 802.11b/g.

Mobile Operators Checklist	
Questions to Ask	
<input checked="" type="checkbox"/>	<i>What's the coverage area?</i>
<input checked="" type="checkbox"/>	<i>Is a fall-back available?</i>
<input checked="" type="checkbox"/>	<i>What's the fall-back speed?</i>
<input checked="" type="checkbox"/>	<i>Is the fall-back accessible from the same device?</i>
<input checked="" type="checkbox"/>	<i>Are there roaming agreements?</i>
<input checked="" type="checkbox"/>	<i>What are the billing options?</i>
<input checked="" type="checkbox"/>	<i>What happens in Wi-Fi to cellular service handoffs?</i>
<input checked="" type="checkbox"/>	<i>Other?</i>

Security Threats and Mitigators

The security threats associated with enabling mobile access to your VPN can be roughly categorized into a few main areas. Among them are intrusions from infected mobile endpoints, the theft of data or authentication information from the airwaves in wireless networks, and unauthorized entry into the network from a “rogue” wireless device.

To a certain degree, your strategy for securing endpoints connecting to a network-based VPN (one that uses an infrastructure separate from the public Internet) will differ slightly than securing endpoints connecting to a CPE-, or Internet-based, VPN. Network-based VPN users include those, for example, who are accessing agency resources from remote or branch offices via an MPLS, frame relay or ATM service.

It is a recommended best practice for endpoints with direct contact with the Internet to run a personal firewall to prevent hackers from gaining control of the endpoint device and, consequently, potentially piggybacking onto a VPN connection from there. In addition, data encryption (such as AES, IPSec or SSL, which requires no special client software) is important for protecting the privacy of data en route over a public Internet connection. Usually, only the organizations with the tightest security needs are likely to use encryption over a network-based VPN service, because it already provides the privacy of virtual circuits through a semi-private network.

Intrusion Detection and Prevention (IDS/IPS)

This security category involves protecting the network against denial-of-service (DoS) attacks and other problems caused by malicious signatures and infections. Users might pick these up when they disconnect from your VPN, link to the public Internet when at home or on the road, then reconnect to the VPN using the same device.

IDS/IPS has quickly become recognized as a “must” area for supporting users who go off- and on-net. It involves scanning endpoint devices when they connect to the VPN for compliance with antivirus, software patch and operating system version policies. If a device is not in compliance or an infection is discovered, access can simply be blocked, or the connection can be redirected to a server that brings the software up to date.

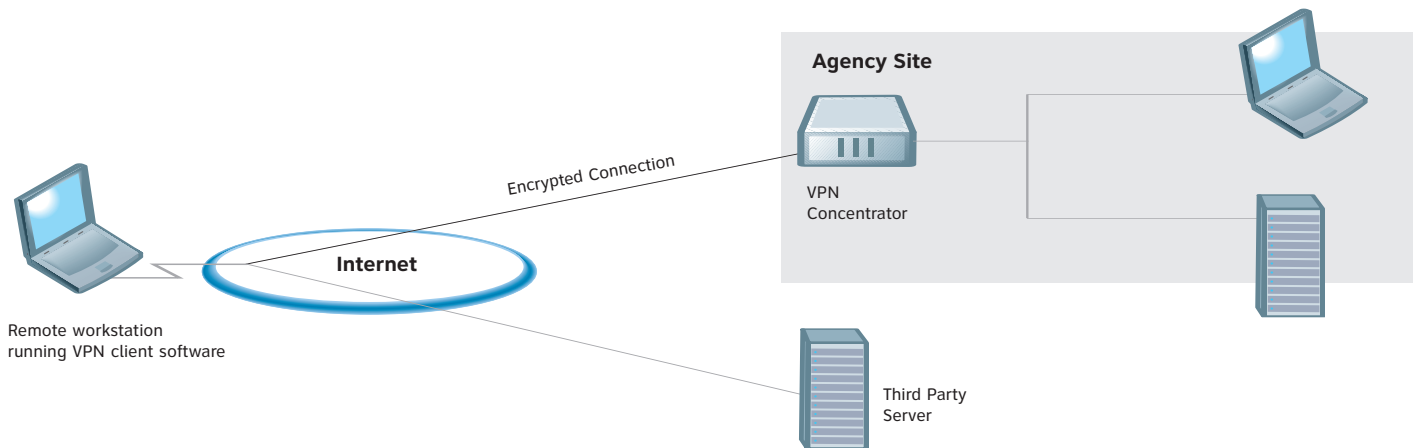
There are several ways to implement IDS/IPS. Industry initiatives have teamed router and antivirus leaders, for example, to enable this automated capability in the WAN access router. In addition, IDS/IPS services are available from some suppliers of the global remote-access client software mentioned that unify access method selection. Some VPN service providers also offer such a service.

On the premises-based wireless LAN, you'll also want to implement some degree of scanning for rogue Wi-Fi devices that might be attached to your network to detect and prevent access by unauthorized users. Scanning and device shutdown according to policy is available from some wireless LAN systems vendors, as well as wireless LAN location specialists. This is becoming a must, given that wireless LAN network interface cards are bundled in nearly every laptop shipped and that Wi-Fi access points can be purchased at any electronics store. It is difficult to keep rogue devices out without continually taking a peek at what's connected.

Data Theft: Break-in or Sniffing/Eavesdropping

A related issue has to do with home users who may wish to use a home computer and a DSL, ISDN or dial-up connection for both VPN access and public Internet access. A recommended best practice is to

Split Tunneling



disallow a capability called “split tunneling,” by which the user can use the same VPN access connection to reach the corporate intranet and to directly access the public Internet. It is recommended that users be required to access the Internet via the corporate VPN connection or using an entirely separate account with the VPN disabled so as not to expose the VPN to intruders and infections.

In Wi-Fi networks, consider setting specific policy for hot-spot usage, where, in some cases, user credentials are “in the clear” over the air before a user has been authenticated to the network. For example, if users already use VPN client software on their laptops, policy could require that they continue to use the software’s encryption capabilities when connecting at a hot spot. A policy could also require that Wi-Fi’s peer-to-peer mode be disabled on certain devices carrying sensitive information or that certain users’ hard drives be encrypted.

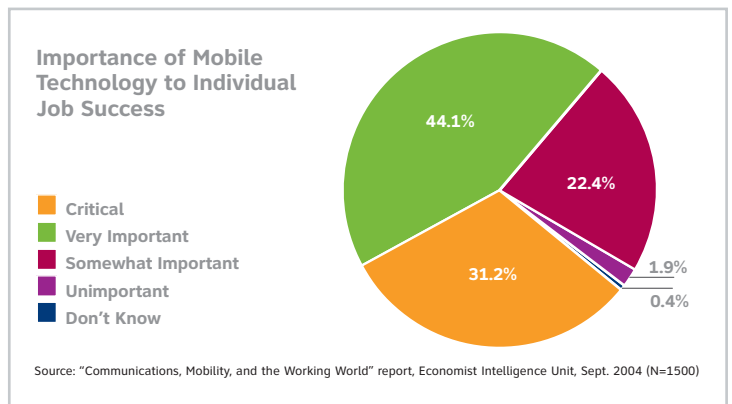
In the case of mobile WAN data networks, depending on your degree of security needs, consider a direct link from your mobile operator’s point of presence (PoP) to your VPN service, thereby bypassing the public Internet, if such a setup is available. Also, ask what, if any, data encryption is bundled in with the service. If none is inherent to the service, you may wish to run VPN encryption software with your mobile WAN connections.

For on-premises Wi-Fi networks, there is a whole set of best practices centered around the IEEE 802.11i authentication and encryption standards. It is also considered prudent to regularly audit your Wi-Fi LAN – including checking AP configurations and monitoring over-the-air packets – to ensure that the various security mechanisms and policies that you think you have configured are, indeed, the ones being enforced.

Virtual LANs (VLANs) can be used to restrict access of guests, contractors, and others to certain resources. Similarly, the wireless VoIP network can be configured to access just one device – the IP PBX – so that intruders cannot gain access to sensitive servers via VoIP devices.

Management Issues

Merging traffic from disparate access networks onto your VPN poses a number of management challenges. These can involve devices, users, software, airwaves and security policies.



Three-fourths of executive computer users said mobile access was either critical or very important to their job success.

Managing Multiple Operating Systems

Many handheld devices in use run mobile operating systems, such as Symbian OS™ and BlackBerry®, with which IT departments are unfamiliar. IT departments are accustomed to standardizing on a common client platform; now, a mix of laptops, handhelds, smartphones and PDAs is growing difficult to support.

You can get the devices down to a more manageable number by performing the user-classification exercise described to evaluate user needs. You can then elect to standardize on an OS for each device-type category.

In the meantime, there are multivendor management software products available for mobile environments, some of which include security management, if you prefer to keep this function in-house. Some remote-access management and security services are also available.

Wi-Fi Architectures and Scalability

Until a few years ago, all Wi-Fi networks consisted of a single, “intelligent” access point wired to a traditional Ethernet switch, with which mobile clients associated.

These are still available; however, now there are other configurations, including a number of centralized-management options. These facilitate scalability as deployments grow, rather than having you configure and manage hundreds or thousands of APs one at a time.

Some make use of so-called “thin APs” and controllers, whereby much of the intelligence once in the AP is now in a centralized device. Also, some of these controllers now contain automated tools for actually managing the RF air space for interference, location tracking and security infractions.

Finally, mesh architectures are available to alleviate the expense and burden of running cabling from AP to switch. Mesh APs automatically form a wireless backbone when they are powered up. APs autodiscover one another and route traffic across the air amongst themselves based on best-path conditions at the moment.

Managing Costs

Many of the automated and centralized tools, aggregated service packages, and global client/portal options mentioned also help IT departments rein in the costs associated with running a mobile work force.

From a service-cost perspective, you can save at least 30% on services by having a structured, centralized procurement plan rather than having individual departments across the organization buy their own services, according to Mobile Competency, a Providence, R.I., consulting firm focused on enterprise mobile networking issues. Pricing plans tend to allow pools of minutes to be spread across users, rather than individuals and departments wasting minutes or running over their allotment and having to pay steep per-minute mobile WAN charges.

Often, too, it might require multiple services and carriers to attain the coverage required. Aggregators come in handy here; without one, it could be difficult to negotiate a volume pricing plan and to validate disparate bills arriving from various providers, which is a costly and time-consuming endeavor.

Risks of Not Addressing Management Issues

Finally, using centralized management architectures, multivendor management software or services, automated management tools,

endpoint security systems and IDSs/IPSSs helps save on both operational expenses and alleviates the costs of network degradation and downtime. Without such assistance, it is difficult to supply network coverage and remain updated with a software patch or prevent a virus from bringing a network to its knees, even for a short period. These issues have both productivity and revenue repercussions.

The hard costs associated with network degradation and downtime average \$77 million annually, depending on industry, according to Infonetics Research’s January 2005 report, “The Costs of Enterprise Downtime: North American Vertical Markets.” They soar to \$222 million in the financial sector. The softer costs of lost productivity and damaged reputation associated with network downtime are more difficult to calculate.

Conclusion

Expectations are high for mobility in the workplace, because employees who have LAN-like capabilities when on the road or working at home can continue to problem-solve and support colleagues from nearly anywhere.

Wireless connections are routinely embedded in laptops and handhelds upon shipment and the availability of 802.11 APs in retail stores mean wireless is in the enterprise – whether or not it is formally sanctioned. As long as you have to manage and secure wireless, you might as well benefit from it, too.

However, supporting mobile access connections brings with it a degree of responsibility and VPN integration challenges. Most of them concern remaining consistent with meeting user expectations for application performance and network availability, continuing to successfully manage and secure data – whether it resides in the network or on individual user devices – and preventing the disruptions that can be caused by infections picked up by mobile devices from the public Internet.

Wireless LANs bring a unique set of new enterprise challenges, which fortunately are growing well documented with best practices. In addition, automated wireless management, monitoring and security tools, and global client software for unifying user access from a common platform are all becoming available to ease the IT department burden. Using these same tools while taking advantage of purchasing power and aggregated connectivity and billing services can help get a handle on managing the costs of running a mobile workforce.

For more information contact an AT&T Representative or visit www.att.com.

