THE CHANGING LANDSCAPE OF SECURE REMOTE ACCESS

AccessAnywhere

What the Experts Say

"Enterprises that want easier and more flexible ways to deploy secure remote access should consider SSL for new investments and as upgrades for legacy VPNs"

- John Girard, VP and Research Director, Gartner Inc.

Executive Summary

It's unanimous; the analysts agree that SSL has emerged as the remote-access VPN technology of choice. According to Mark Bouchard of analyst firm Meta Group: "We expect adoption of SSL VPNs to accelerate. By 2006, it will become the dominant approach for achieving secure remote access, with greater than 70 percent of all users employing it as the method of choice."

In addition, analyst firm Frost & Sullivan estimates that by 2008, SSL VPN sales will exceed USD $1 billion. In fact Forrester Research indicates that the typically conservative financial services sector is the most aggressive vertical deploying SSL VPNs, with 56% currently using the technology. Business services rounds out the verticals that have passed 50% penetration.

As the market continues to mature SSL VPNs will help solve specific business and regulatory issues. The research highlights healthcare, retail, and manufacturing are especially suited to the adoption of SSL VPNs because of their requirements for extranets and remote access to legacy applications [1]

Why is SSL VPN so widely accepted as the remote access technology of choice and if it's so clearly better than IPsec, why has there not been more universal adoption by businesses?

What is an SSL VPN

SSL is a commonly used protocol for managing the security of message transmission on the Internet. SSL works by using a public key to encrypt data that is transferred over the SSL connection. SSL is a higher-layer security protocol, sitting closer to the application. This close connection to application layers means that SSL can more easily provide the granular access control that remote access and extranet VPNs require.

An SSL VPN uses SSL and proxies to provide authorized and secure access for end-users to HTTP, client/server, and file sharing resources. Adding proxy technology to SSL offers companies greater security, because it prevents users from making a direct connection into a secured network. SSL VPNs deliver user-level authentication, ensuring that only authorized users have access to the specific resources as allowed by the company's security policy.

What the Experts Say

Highlights

SSL protects over $50 Billion in e-commerce transactions every year.

"The global SSL VPN market is expected to grow 291% between 2004 and 2007."

→ *Jeff Wilson, Infonetics*

"SSL remote access is 45 percent less expensive than IPSec solutions and 72 percent cheaper than dial up."

→ *Zeus Kerravala, Yankee Group*

"By year-end 2005/06, SSL based solutions will be the dominant method for remote access, with 80% of users utilizing SSL."

→ *David Thompson, Meta Group*

SSL - The Standard for Internet Security

The security standard for the Internet, SSL protects over $50B in e-commerce transactions a year, and is supported by all of the most widely used browsers, web servers, and open source software. Because it was developed for Internet use, it was designed with firewalls, gateways, network address translation (NAT), and public-key infrastructure (PKI) in mind.

By design, SSL VPNs make it simple for users to connect securely to appropriate resources. For example, by automatically navigating firewalls and NAT, SSL VPNs significantly reduce help desk costs. SSL VPNs also lower support and maintenance costs because they are clientless—meaning they avoid installation, updating, and configuration issues that plague traditional VPN's.

Some security administrators may view SSL VPNs as less secure than IPsec VPNs, since remote devices do not need to be under IT control with an SSL VPN. That works for site-to-site, when you can control both ends of the network. However, when you need to extend remote access to devices beyond your network and beyond your control, which technology delivers the strongest security?

SSL is Replacing IPSec for Remote Access VPN's

Traditional remote access focused on providing a simple network connection for mobile workers to gain access to the resources of a corporate LAN. But enterprises' requirements are growing. Enterprises want access to a wider set of applications for a more diverse set of users — at a reduced cost. SSL VPNs are the answer. They provide a lower-cost and more scalable option than dial-up for remote users to get access to corporate applications.

Enterprises have two choices for remote-access IP VPNs: Internet Protocol Security (IPsec) and Secure Sockets Layer (SSL). IPsec is today's most widely deployed technology, but the high costs of ownership and functionality limitations are quickly migrating users to SSL as the more logical choice.

IPsec works by establishing a "tunnel" over the Internet to connect users outside a corporate firewall or gateway to internal corporate resources. It requires compatible hardware or software, almost always from a single vendor, on both ends of the tunnel. With IPsec, the corporate IT department dictates the technology used on both ends of the tunnel. Few companies are willing or able to mandate the technology their business partners or customers use, and this limits the extranet capabilities of an IPsec VPN.

As for the remote access market, IPsec satisfies the basic requirements when there are a limited number of tunnels to create. However, when there are thousands of remote users at different locations, distributing and managing the required client software can be cumbersome and costly. These are just some of the many factors that make IPsec VPNs less than ideal for remote access and extranet implementations.

What the Experts Say

Highlights

36% of companies using IPSec VPNs say troublesome home-based workers are a significant deployment challenge.

→ *Gartner Inc.*

Superior Features of SSL VPNs:
- More Levels of Granularity
- Better End-Point Security
- Wide Choice of Device Types and Locations

→ *Robert Whitely, Forrester Research*

SSL VPNs reduce the cost and effort of setting up secure VPNs, which leads to significant cost savings.

→ *Michael Suby, Stratecast Partners.*

Although IPsec VPNs freed organizations from the high cost of dial-up, they introduced an expensive support requirement to organizations while still not solving the issue of employees needing to connect from behind customer or partner firewalls. The issues with IPsec VPNs are as follows:

- IPSec VPNs introduce administrative headaches and high support costs to an organization.
- IPsec VPNs are not firewall friendly. This prevents the use of VPN by employees who want to remotely connect to a private network from some other organization, where it is not possible to contact network administrators and request them to change firewall policies.
- IPsec traffic is considered “business-level” by many DSL and cable providers. This means that employees who have residential DSL and cable modem service will have their IPsec traffic blocked by that provider.
- IPsec VPNs aid in worm traversal by opening up a tunnel between one network and another. This is because the remote PC is assigned an IP address on the destination network.

According to Gartner, 36 percent of the companies using IPsecVPNs say trouble-shooting home-based workers is a significant deployment challenge; 28 percent also cite IPsec VPN-user training as a barrier.[2] By leveraging the familiar Web browser, present on nearly every desktop, laptop and PDA, companies may avoid installing, configuring and updating VPN software on remote devices. Browsers also tend to be easier for employees to understand, launch and use. To capitalize on the surging demand for Web-based remote access, the clientless feature is the key reason why SSL is replacing IPsec for remote access VPN’s.

According to Robert Whiteley of Forrester Research Inc., SSL VPNs provide three essential features that make it clearly superior to IPsec VPN [1]:

More levels of granularity.
Because it is at the application layer, SSL knows more about the remote user — his location, type of computer, and OS — than IPsec does.
This allows enterprises to comfortably extend remote access to new areas like Internet kiosks or partner sites, where granularity of user information assures that remote users have access to only the necessary resources.

Better endpoint security.
Closely tied to granularity, SSL VPNs leverage the additional application-level information to apply security policies to incoming users. This allows enterprises to apply more flexible security instead of the one-size-fits-all approach that IPSec requires. This comes in handy: A user may be identified as connecting from a trusted laptop, but what if that laptop’s Symantec antivirus app is out of date?

Resources like remediation portals redirect users to the Symantec Web site for updates before further passage to the network.

Wider choice of device types.
SSL VPNs are capable of running on a standard browser. As a result, a wide variety of client types, such as PDAs and cell phones, can securely connect remote users via standards-based browsers. Conversely, IPsec requires proprietary client software that might not be installable or is too resource-intensive for these devices. This is increasingly important for mobile environments where vendors are integrating Wi-Fi into virtually every device type — but without any security framework.

What the Experts Say

Highlights

In-house VPNs can require weeks or months to deploy, and they can involve complex network and/or application integration and generally require security-savvy administrators for configuration, maintenance and monitoring.

"IT departments have also discovered that designing, deploying and managing secure remote access solutions takes specialized knowledge and significant resources. Managed service providers alleviate this complexity by expertly delivering comprehensive solutions with around-the-clock support."

→ *Eric Paulak, Gartner Inc*

Why has there not been more adoption of SSL VPN Technology?

While the main issues with IPsec VPNs are the recurring annual operating costs, the main issue with SSL VPNs is the high acquisition costs in terms of product pricing, professional services, and software maintenance costs.

Most articles on SSL VPNs warn potential customers to be wary of the "add-on" costs for "custom connectors" for basic functionality like FTP, e-mail, file sharing, etc. These custom connectors can cost an additional $5,000 per connector and can significantly drive a $10,000 base SSL VPN package upward. A recent quote from one of the leading SSL VPN vendors for 50 concurrent tunnels totaled $30,000. Add to this a 20% annual maintenance agreement and any subsequent professional services for webification of applications where there is no custom connector, and the acquisition costs increase rapidly. SSL VPNs will eventually cause an organization to spend additional capital on application upgrades as they do not inherently support all applications or protocols.

Additionally, since there are setup issues involved to ensure that applications can be accessed correctly from both inside and outside of an organization's firewall, there is significant IT setup time required on both the application side and on the client PC side.

These in-house VPNs can require weeks or months to deploy, they can involve complex network and/or application integration and generally require security-savvy administrators for configuration, maintenance and monitoring. Because time-to-implement the cost of new infrastructure and hiring skilled people are top Internet Business System barriers [3], many companies are now looking to buy managed VPN services rather than build their own in-house VPNs.

The Business Case for Managed SSL VPN Services

According to Gartner, the managed security-services market is expanding rapidly, doubling from $4.1 billion in 2001 to nearly $9 billion by 2006. [4] Lisa Phifer from Core Competence highlights that managed services are gaining in popularity because they free up capital, reduce ongoing operational costs and decrease the need for in-house security expertise. By outsourcing to a managed-service provider, companies can increase internal focus on their own business goals by leveraging the provider's security infrastructure and expert staff to ensure the safety of business traffic over the Internet. [5]

What the Experts Say

Highlights

AccessAnywhere is much easier to deploy than in-house IPsec and SSL VPNs. By leveraging existing Web browsers and employee desktops, AccessAnywhere can also be less expensive to operate than client-based VPNs.

"Managed services are gaining popularity in the enterprise community as a cost-effective and secure method of addressing increasingly complex business communications"

→ *Zeus Kerravala, The Yankee Group*

"Managed remote-access cuts down one of the most-significant cost components - labor - involved in overseeing and administering a far-flung WAN. End-user administration is a major headache and significant cost. We found that companies spend on average $14 per remote user, per month - or a whopping $168 per year. For a company with 1,000 employees, that's a lot of change - and managed remote-access solutions can reduce that burden by up to 40%."

→ *Johna Till Johnson, "Handling the Remote office Revolution"* Network World *February 2004*

AccessAnywhere SSL-based Managed Service

AccessAnywhere, an SSL-based managed remote-access service, is unique because it capitalizes on all of these emerging trends. As a SSL- based managed service, AccessAnywhere is much easier to deploy than in-house IPsec and SSL VPNs. By leveraging existing Web browsers and employee desktops, AccessAnywhere can also be less expensive to operate than client-based VPNs.

AccessAnywhere provides secure tunneled and encrypted remote access to ANY application—including Web, legacy, client/server, file transfer, terminal servers, and mainframe. Users get secure, hassle free, and highly controlled access to a broad range of critical applications and resources including:

- E-mail programs such as Microsoft Exchange and Lotus Notes
- Customer relationship management (CRM) tools such as Siebel
- Business management software such as SAP
- Intranet resources, including custom applications
- Enterprise file servers

With AccessAnywhere remote users simply enter www.yourcompany.com in the address line of any standard web-browser. There is no remote VPN client software to load or configure or firewall rules to negotiate.

Once a remote user accesses the login screen they authenticate with one time random number passwords that authenticate access to email and authorized file and application resources. AccessAnywhere will automatically check the remote users PC to ensure that it complies with your company's security policies and requirements before presenting the login screen and enabling the remote connection.

Once connected, remote users communicate directly with your companies network and servers to access email, files and business applications from any location. No sensitive company data or proprietary information is ever transmitted across the AccessAnywhere network or servers ensuring that confidential data remains confidential and system performance is not degraded by the number of remote users or the level of service you purchase.

When the remote user terminates their connection, enhanced security software automatically removes any proprietary company information that may inadvertently have been left behind by the remote user on non-company owned PC's.

Because AccessAnywhere is a fully-managed service, policies and reports are accessed through a secure admin portal. AccessAnywhere requires no end-user configurations and no network infrastructure or firewall modifications. AccessAnywhere provides centralized administration with one policy setup for all access methods and resource.

End-user access to any given resource is restricted unless authorized, a vastly different approach from that of IPsec VPNs. AccessAnywhere provides a secure, proxied connection that reduces risk because users never have a direct network connection to the resources they are authorized to access. In addition, our proxies hide the internal domain name system (DNS) namespace, providing an extra level of protection for your network.

What the Experts Say

Solution Benefits

"AccessAnywhere offers enterprises secure, anytime access at a reduced cost and on a foundation they trust."

→ *Masha Khmartseva, The Radicati Group*

By 2006, the leading providers of remotely managed network infrastructure and telecommunications solutions will be systems integrators and outsourcers, not carriers (0.9 probability).

→ *Eric Goodness, "Identifying Solutions and Providers for Network Managed Services," Gartner IT/Expo 2003.*

A client organization can convert variable costs (when done in-house) to fixed costs (services), realize a tax advantage by deducting MSSP fee expenses from current year earnings versus depreciating internal assets, and experience cash flow improvements resulting from the transfer of software licenses (and possibly personnel) to the MSSP.

→ *Network World, February 2004*

AccessAnywhere for Secure Remote Access

AccessAnywhere is a convenient, cost-effective alternative for companies just getting started with secure remote access. Companies with existing VPNs can save money by using AccessAnywhere to offload end users – especially teleworkers and day extenders.

AccessAnywhere for Small and Medium Sized Business

For small to medium businesses, in-house SSL VPN set-up costs are currently higher than IPsec set-up costs because low-end IPsec security appliances are less expensive than the least expensive SSL VPN appliances. The two VPN alternatives do get closer together as the end-user population increases, but an SSL-based service like AccessAnywhere still requires less up-front investment and no outlay for capital equipment.

With its low set-up cost, AccessAnywhere can help a small business avoid up-front capital investment. Better yet, AccessAnywhere continues to cost less than either IPsec or SSL every month. Of course, an inexpensive remote-access solution is meaningless if it does not satisfy business requirements. AccessAnywhere can provide secure remote access to virtually ANY application meeting all end-user access requirements including those needs of tele-workers and occasional travelers.

AccessAnywhere: a straightforward solution for remote access and extranets

Whether an SSL VPN is the right choice for a company really depends on the enterprise's needs. Traditional IPsec VPN technology is designed for site-to-site VPNs and does the job quite well. SSL VPN technology, on the other hand, works much better for secure
remote access and extranet implementations—offering clientless access, simpler deployment, greater ability to gain access from anywhere, better security, and easier ongoing administration.
AccessAnywhere makes SSL-based remote access affordable - the cost per user is as little as $9.95 per month with no upfront capital investment- and completely portable - an employee, supplier or business partner can now access your companies data and information from a home PC, hotels, warehouses, customer sites or airport kiosks - wherever and whenever - business demands.

References

[1] SSL VPNs Poised for Significant growth, Robert Whiteley. December 31, 2004
[2] Virtual Private Networks: Research Conducted for Cisco Systems, Gartner, Fall 2001
[3] The Net Impact Study, Varian, et al., January 2002
[4] North American Security Services Market Forecast: 2001-2006, Gartner, Oct. 2002
[5] Cutting Remote-Access costs in the Enterprise, Citrix Online, 2004

AccessAnywhere

Corporate Headquarters
2425 Matheson Blvd East, 8th Floor
Mississauga, ON
L4W 5K4

Tel: (905)361-2853
Fax: (905)361-2781
http://www.accessanywhere.net