

FEBRUARY 2006

Technology Backgrounder

on SSL VPNs: The Secure Access Landscape

By Steven Taylor

Produced By:  Webtorials

Sponsored By:  Juniper®
NETWORKS

The widespread availability of broadband Internet access connections, high-speed mobile networks, wireless LAN hot spot services, and smart handheld devices has driven many workers out of their traditional offices to home offices and into the field to solve business problems. Global research firm IDC expects the number of mobile and remote workers to grow to more than 150 million worldwide by 2006.

The “extended enterprise” of remote and mobile workers, partners, and consultants delivers compelling productivity benefits. But it has left organizations without a single definable enterprise network border, making it particularly challenging for corporate IT departments to support user connectivity needs and meet the requirements for tighter security. Increased security procedures are being dictated by the growing number of Internet viruses and legislative mandates for greater access control. Administrators must provide remote employee and partner access to a multitude of different user groups while keeping the network and applications secure.

Providing secure access to corporate resources has grown into a critical requirement for the enterprise, often making the difference between those companies that are successful and those that are not. Whether users are working in a remote office or their hotel room, they need easy access to corporate resources to accomplish their jobs and maintain their productivity. In addition, corporate business partners and customers increasingly need real-time access to corporate resources and applications.

In the early 1990s, there were limited options to extend the availability of the enterprise’s network beyond the boundaries of the corporate central site, comprised mainly of extremely costly and inflexible private networks and leased lines. Frame relay and ATM provided some degree of cost relief, but both services were deployed primarily as a less expensive form of leased lines rather than providing any-to-any connectivity. As the Internet grew, however, it spawned the concept of virtual private networks, or VPNs,

as an alternative. Most of these solutions leveraged the free/public long-haul IP transport service and the proven IPSec protocol to provide a flexible, cost-effective solution for secure remote access. IPSec VPNs effectively addressed the requirements for fixed, site-to-site network connectivity; however, for mobile users, they have had significant drawbacks and high support costs. For business partners or customers, they were impossible to deploy as they require software to be installed and configured on each endpoint device and provided only full network-layer access, exposing all of the enterprises resources. Alternatively, many enterprises chose to deploy an Extranet for their partners and customers, a solution that was very expensive and complex to deploy and maintain.

Today users can access many different network services from various types of client devices. A number of these access networks and client devices, such as the Internet and public kiosks, are outside the enterprise’s management purview and should be considered “untrusted.” This situation can make it difficult to ensure that all user connections comply with a cohesive corporate security policy. It is in this environment that SSL VPNs were introduced, providing to remote/mobile users, business partners and customers an easy, secure access to only selected corporate resources they need from a single platform.

As a result, the SSL VPN market has grown into an estimated \$200 million market in 2005 and is projected to grow into a close to \$400 million market in 2006, and more than \$600 million by 2008, according to Infonetics. Meta Group has estimated that by 2006 SSL-based solutions will be the dominant method for remote access, with 80% of users utilizing SSL. According to Gartner, by 2008, SSL VPNs will be the primary remote access method for more than two-thirds of business teleworking employees, more than three-quarters of contractors and for more than 90 percent of casual employee access.

This paper examines the criteria to be considered when evaluating an SSL VPN solution.

What Is An SSL VPN?

The term SSL VPN is used to refer to a new and fast-growing product category comprising a variety of technologies. To broadly define what products and technologies are within this category, you can begin with the term “VPN” itself. VPN, or Virtual Private Network, refers to the practice of using a public network like the Internet to transmit private data. Up until 2001, most in IT did not add a descriptor to VPN because almost all VPNs available at that time used some type of network-layer transport. The early standard in the VPN space was the IP Security Protocol (IPSec), although some vendors used other methods, including Layer 2 Tunneling Protocol (L2TP), and Point-to-Point Tunneling Protocol (PPTP).

SSL VPNs use a different methodology to transport private data across the public Internet. Instead of relying upon the end user to have a configured client on a company laptop, SSL VPNs use SSL/HTTPS, which is available without additional software deployment on all standard Web browsers, as a secure transport mechanism. Using an SSL VPN, the connection between the mobile user and the internal resource happens via a Web connection at the application layer, as opposed to IPSec VPNs’ open “tunnel” at the network layer. The use of SSL is ideal for the mobile user because:

- SSL VPNs do not require a client download onto the device being used to access corporate resources.
- SSL VPNs do not need to be configured by the end user.
- SSL is available wherever there is a standard Web browser, so users don’t need a company laptop.

SSL is familiar to most users, even those without a technical background. It is already installed on any Internet-enabled device that uses a standard Web browser, and no configuration is necessary. SSL operates at the application layer, independent of any operating system,

so changes to the OS do not require an update in the SSL implementation. And because SSL VPNs operate at the application layer, it is possible to offer extremely granular access controls to applications, making it ideal for mobile workers and those users coming from an unmanaged or untrusted end-point.

SSL VPN technology has evolved to include a variety of different types of access via dynamically downloaded agents. These advances enable the delivery of client/server applications, as well as network-layer connections, which are enabled via SSL. Dynamic delivery facilitates the use of agent-based access methods, without the cost or hassle of installing, configuring, and maintaining individual client software. Additionally, SSL VPNs can solve Network Address Translation (NAT) and firewall traversal issues that are associated with legacy IPSec VPNs.

Another advancement in SSL VPNs is the provisioning of additional endpoint security. Unlike IPSec VPNs, where a level of endpoint security can be assumed, SSL VPNs were designed to provide granular access from any endpoint. A means of ensuring that each endpoint is in compliance with a minimum corporate security policy is mandatory. This can be done via dynamic endpoint security checks, which should be done both before a session is initiated, and periodically throughout the session.

IPSec VPN or SSL VPN?

Many users are struggling to decide which technology should be deployed and where. Where do IPSec VPNs and SSL VPNs fit into your network security policies, and which problems can each technology best address? What does it really take to deploy and administer an IPSec and SSL VPN?

This confusion is not mitigated by the fact that most debates over IPSec and SSL have largely focused on the technical details of the protocols and not on what should be the most significant deciding factor between these methods – the usage scenarios themselves. The fact is

that IPSec and SSL are not mutually exclusive technologies. They can – and in fact, often are – deployed in the same enterprise. The deciding factor between them lies not in what each protocol can do, but in what each deployment is designed to accomplish. When you consider the cost/benefit of each type of deployment, as well as what problems each technology was designed to address, the deployment choices become clearer.

Administrators that need to achieve site-to-site connectivity will be well served by IPSec VPN offerings. They were created to meet the challenge of how to provide employees around the world with secure “always on” connectivity that will enable them to access the corporate resources they need to achieve optimal productivity. For years, IPSec VPNs have been delivering the resilient, reliable connectivity that is imperative for ongoing communications between coworkers at different offices. IPSec VPNs provide users at geographically distributed locations an experience akin to that which they would receive if they were logging in at the corporate headquarters, allowing them easy access to all network resources that they would be able to access if they actually were on the LAN. In addition, the level of management resources required for deployment and maintenance is fairly limited in the site-to-site use case: the number of sites is limited; the device, which usually serves also as a firewall, is managed; and the session is fixed.

Administrators that need to allow mobile employees, contractors, offshore employees, business partners or customers access to certain corporate resources will be well served by SSL VPNs. SSL VPNs are designed to address the needs of diverse audiences that need secure access to administrator-specified corporate resources from anywhere and to change both the access methods and the resources allowed as the users’ circumstances change. SSL VPNs can also be configured to check endpoint security compliance and to either provision resources accordingly or to provide the end user with the means to remediate. This combination of granular access

and endpoint defense functionality mitigates the risks that access to corporate resources from an unprotected endpoint, untrusted network, or unauthorized user can introduce. As a result, SSL VPNs offer users the convenience of being able to access corporate resources using any Web-enabled device from anywhere.

Provision by Purpose: Application-Layer or Network-Layer Access?

Today it is expected that an SSL VPN solution can combine three SSL-based access methods within a single appliance: clientless Web-based access, thin-client application proxy, and thin-client full network connectivity combined with powerful access provisioning and management tools. The three options specifically map to key enterprise requirements. These can be provisioned from a single appliance to serve various user constituencies and business needs.

In order to meet all the access needs of an enterprise, SSL VPNs need to have best-in-class solutions for all access methods. Two typical examples are application-layer and network-layer access:

- Web-based (clientless) access requires best-in-class rewriting that is based on knowledge and expertise of many custom applications. Therefore the more customers a vendor has the more it is likely to support these applications. By rewriting each and every packet, SSL VPNs don’t reveal the name of the servers at the backend and protect them from any attack that is based on knowing their hostname. Being able to do it on the fly, including the replacement of all hostnames and socket calls for complex content (e.g. JavaScript, XML, Flash, and PDF), cannot be done by all SSL VPN vendors.
- For network-based access, enterprises want to have the strengths of IPSec and SSL VPNs in a

single solution. Some vendors would try to explain that this means supporting legacy IPsec VPNs and SSL VPNs from the same appliance. But in reality a solution like that can combine the disadvantages of both: the administrator has to pick one of these solutions for each user resulting in either the need to install and maintain the IPsec clients on the endpoints or the loss of performance for applications like voice over IP (VoIP) running over SSL. By contrast, another solution is an SSL VPN that can provide a dual-mode network-layer access capability that dynamically detects the best method of connection between IPsec and SSL transport to ensure the highest level of connectivity supported by the network environment. This enables the high performance required for accessing latency and jitter-sensitive applications like VoIP, while providing the ubiquity and reliability that SSL VPNs are known for with none of the IPsec VPN management overhead. SSL is used for the authentication so there is no need for installing a client and if IPsec cannot be used for the transport (e.g. because of NAT or firewall traversal issues) then the session falls dynamically into SSL.

Once the business need has been identified, provisioning access should be easy with the SSL VPN application. Administrators typically only need to create user groups (i.e., partners, contractors, temporary employees, telecommuters, wireless LAN users) that correspond to the business need of their users. They can then usually associate the access method and security controls that apply to each. When the security, resource, and TCO concerns outlined above are assessed, it is very often the case that even large user groups can be mapped to a few major constituencies. Most importantly, the SSL VPN solution should be able to allow for dynamic provisioning of the connectivity type based on the need, meaning that any of the three access

methods can be applied for a given user or user group based on where the user is located, the type of network and device being used, the endpoint security posture, and the resources to which access is required. Without the flexibility to address all of these parameters, access provisioning that is cost-effective and commensurate with security best practices is not possible. (See chart on next page.)

Security

Ensuring the best security for a remote employee and partner access solution is the most critical element. Various factors need to be considered.

Transport Protocol: SSL vs. IPsec

Comparisons between IPsec and SSL often lead to a "Which protocol is more secure?" debate. In reality, these debates have little relevance to the choice between SSL and IPsec. These protocols achieve similar goals; they provide for secure key exchange and provide strong data protection during transport. Despite significant differences in the protocols, IPsec and SSL are actually quite similar in terms of transport security at a high level. Both technologies effectively secure network traffic, and each has associated trade-offs, which make them appropriate for different applications. Though the protocol implementations differ greatly, the two systems share many similarities, including strong encryption and authentication, and protocol session keys that are specified in a conceptually similar manner. Each protocol offers support for leading encryption, data integrity, and authentication technologies such as Triple DES, 128 bit RC4, AES, MD5, and SHA-1.

Hardened Appliance

SSL VPNs are usually deployed in the DMZ facing the public network. Therefore it is imperative to make sure they are purposely built and have the appropriate security posture.

The advantage of using SSL hardened appliances is that they are usually built on a purpose-built operating system. In other words, the appliance is not designed to run any

SSL VPNs: The Secure Access Landscape

other services. There are no backdoors to exploit or hack. There is no interface, or interactive shell, or protocol to run on the machine.

Some vendors have taken security a step further by putting their solutions through rigorous third-party securi-

ty audits that can provide customers the assurance that the appliance is secure to be placed at the DMZ. In addition, in some verticals and theaters, SSL VPNs are expected to have certifications such as Common Criteria and ICOSA Labs.

Access Methods Overview			
	Web-based Clientless Access	Thin-client Application Proxy	Full Network Access
Application support	Web-based applications (e.g. Intranet, Microsoft Outlook Web Access, Lotus iNotes)	Client/Server applications (e.g. Microsoft Outlook, Lotus Notes) or any application running over a known TCP port	Any application you can access from the LAN including server-initiated applications and VoIP
Endpoint requirements	Anytime, anywhere (requires only a browser)	ActiveX enabled or Java	ActiveX enabled or Java
Granularity of access controls and auditing	High – at the application layer: up to the file and URL level	Medium	Medium
Key questions to ask	<ul style="list-style-type: none"> • Which content can be rewritten? (e.g., JavaScript, Flash, XML, PDF, ...) • How granular is the logging? • How comprehensive and granular are the authorization policies? • How many customers use the product? 	<ul style="list-style-type: none"> • What type of thin-client is provisioned? Windows-based only or also Java-based? • How is the application checked for authenticity? (e.g., MD5 checksum) 	<ul style="list-style-type: none"> • Which platforms are supported? (e.g., Windows, Mac, Linux) • What transport protocol is used to ensure high performance as well as high availability?
Use cases examples	<ul style="list-style-type: none"> • Access to remote employees who need web-based applications • Access to specific files/URLs for partners and customers • Access to specific files/URLs for users from a kiosk or from an unmanaged device. 	<ul style="list-style-type: none"> • Employee access to a native email application (e.g., Outlook) • Employee access to a terminal services environment 	<ul style="list-style-type: none"> • Access for power users and admins • Access to VoIP applications • Access from the corporate wireless LAN

Endpoint Security

Endpoint defense is important to ensure that the end device connecting the user to your internal servers and to your network is secure. When workers are temporarily remote, for example, workers might be on- and off-net using the same client device. When off-net without the proper safeguards, client devices are exposed to Internet-bred viruses, worms, and other security issues, which could leave the corporate network vulnerable to corruption and denial of service (DoS) when users reconnect. The same risks exist when users connect to the corporate network using devices not managed by the enterprise, such as kiosks, which can contain malicious applications that put the corporate network at risk if not blocked at the corporate site.

Because users in different situations pose varying levels of risk to the organization, some enterprises are seeking to support different levels of user access depending on who the user is, what kind of client device is in use, the type of access network used, time of day, the security posture of the endpoint, and possibly other variables. Some of the current SSL VPN products have evolved to support these levels of access.

SSL VPNs should be expected to provide the following endpoint security features:

- Host integrity checking: scanning for viruses and other infections using APIs to partner-company antivirus systems before granting client access
- Checking for compliance with current versions of antivirus, personal firewall, and OS software (e.g., checking whether the antivirus signature is up-to-date)
- Protecting from malware applications (e.g., key-stroke loggers)
- Denying access, quarantining, and/or providing remedial action (e.g., updating the antivirus sig-

nature without help-desk involvement) if compliance test fails

All of these conditions should be evaluated before the session starts (and even before the end user sees the sign-in page) as well as during the session. The results of the endpoint security evaluation should be integrated into the existing Authentication, Authorization, and Auditing (AAA) framework to provide limited or no access in some cases as well helping the end user to remediate the endpoint.

Integration with AAA Infrastructure

In order for SSL VPNs to enable secure extranets and intranets, they need to provide access to highly diverse user communities. Given the varied user base and the resulting array of access privileges, SSL VPNs should be capable of enforcing advanced access management policy decisions at the time of each request. In addition, with growing user communities that need access, SSL VPNs should enable seamless access across application environments in order to reduce user helpdesk/support costs and increase user productivity.

Another consideration is the integration with your existing AAA infrastructure. Most enterprises already have a policy server and/or directory, and a key requirement is to integrate with it in a seamless manner while providing features like single-sign-on (SSO) and password management. Being able to integrate with existing policy servers and protocols such as RADIUS, LDAP, Active Directory, SiteMinder, RSA, and others, is a key differentiator among SSL VPN vendors. In addition, advanced access management capabilities can enable dynamic authentication and role mapping, as well as very flexible and expressive resource-based authorization (e.g., mapping users to a specific role and granting them access to specific resources based on an LDAP attribute). These capabilities can enable adherence to corporate security policies in an extremely cost-effective way.

Auditing

Being able to track user behavior is becoming more and more important. For instance, in some cases, federal mandates for compliance reporting, such as Sarbanes-Oxley and the Health Insurance Portability and Accountability Act (HIPAA), require more diligent tracking and logging of network access. Remote and mobile connectivity practices must comply with these new rules.

Working at the application layer, SSL VPNs are expected to log not only configuration changes and user logins but also to track specific files and URLs that end users access. They also serve as a means for troubleshooting access problems at the endpoint.

Some vertical markets and organizations also require a different level of administrator delegation for different administrators.

In addition to access and security considerations, you should also consider system requirements such as scalability, performance, and high availability. As remote access becomes a more important factor for the enterprise, the cost of downtime increases with more users suddenly becoming unproductive. High-availability features such as backup power supply and redundant hard disk with data mirroring become a necessity.

Conclusion

SSL VPNs have revolutionized the remote employee and partner access market. Authorized users, whether they are remote employees, business partners, or customers, are now able to gain secure remote access to network resources from any standard Web browser and Internet connection, including PCs, laptops, and mobile devices. They are no longer constrained to use specific devices or work from designated locations. And, unlike traditional IPsec VPNs, end users don't need a client to achieve remote access, which enables greater mobility and productivity.



Steven Taylor

consultant and broadband packet evangelist, is President of Distributed Networking Associates and Publisher of Webtorials. An independent consultant, planner, author, and teacher since 1984, Mr. Taylor is frequently quoted in the trade press and is one of the industry's most published authors and lecturers on high bandwidth networking techniques. He has served as a Contributing Editor for Data Communications magazine, publishes articles in both Business Communications Review and Network World, and co-authors two newsletters - Convergence and Wide Area Networking - distributed by Network World Fusion.

WEBTORIALS TECHNOLOGY BACKGROUNDER

Produced By
Webtorials,
a venture of
Distributed Networking
Associates, Inc.
Greensboro, N.C.
www.webtorials.com

Design/Layout Artist

Debi Vozikis
dvozikis@rcn.com

Copyright © 2006
Distributed Networking
Associates, Inc.

For Editorial and Sponsorship Information

Contact Steven Taylor,
taylor@webtorials.com

Professional Opinions Disclaimer

All information presented and opinions expressed in this Webtorials Technology Backgrounder represent the current opinions of the author(s) based on professional judgment and best available information at the time of the presentation. Consequently, the information is subject to change, and no liability for advice presented is assumed. Ultimate responsibility for choice of appropriate solutions remains with the reader.