WHITEPAPER
IPSEC VPN VS. SSL VPN

AccessAnywhere

Introduction

Whether a result of tele-working initiatives, contingencies for events such as 9/11, SARS, and the East Coast Blackout, or just addressing the need to balance longer work days with family commitments, companies are being driven to provide expanded access to corporate IT resources from outside the internal network. However, addressing this requirement can be problematic.

One problem is that the modern enterprise network is a dynamic environment. Corporations have an ever-changing variety of applications to address the needs of its diverse community of users. In addition to the many web-enabled resources, heterogeneous data centers continue to exist with legacy (AS/400, mainframe and other character-based) and client/server applications, as well as significant file server resources.

The second issue is that it's no longer just company employees that require access to this heterogeneous environment. Contractors, business partners, and even customers may be included in the population of possible remote users.

Lastly, in addition to the broad user population, access points are not longer controllable by IT. Employees may want to connect from an airport kiosk or a relative's computer while on vacation, contractors may be working off site using their own equipment, and customers may be accessing from a wi-fi hotspot.

Until recently VPNs based on the IPSec protocol have been seen as the logical choice for providing secure network connectivity to remote users/networks because they leverage the Internet and thereby offer a less-expensive alternative to dedicated point to point networks and dial-up infrastructures. However, extending an IPSec VPN to this large and complex realm of remote partners, suppliers, customers and employees, while still ensuring network protection, has been one of the great hurdles to a successful remote-access deployment.

As a result, enterprises are turning towards SSL-based VPNs to satisfy the demands of today's heterogeneous enterprise networks and sophisticated end-user requirements, while ultimately delivering a lower total cost of ownership (TCO), especially when compared to IPSec VPNs.

IPSec VPNs: For Site-to-Site Connectivity

Traditional VPN's rely on IPSec (Internet Protocol Security) to tunnel between the two endpoints. IPSec works on the Network Layer of the OSI Model- securing all data that travels between the two endpoints without an association to any specific application. When connected on an IPSec VPN the client computer is "virtually" a full member of the network, able to see and potentially access the entire network. This virtual connection is the great strength of the IPSec design center: *to protect private data transmissions between trusted networks when sent over an untrusted network like the Internet*.
The problem, however, is that in the past there was a clear segregation between trusted networks and untrusted networks. Trusted networks were intra-networks and employees. Today, such distinction is difficult.

- Is your co-location or disaster recovery facility trusted?
- Is your outsourcing vendors' network trusted?
- Is your employees' home network trusted?
- Are consultants trusted users?
- Are telecommuting employees trusted?

The point is that, protecting the connection between trusted site-to-site networks is the sole task appropriate for deployment of an IPsec VPN.

IPSec VPNs: Costly to scale and maintain

Because IPSec VPNs operate at the network level and effectively provide the remote computer with full network visibility, as if it were a located on the corporate LAN, policy enforcement and security controls cannot be easily applied. As such, many companies are hesitant to deploy IPSec VPNs to anything but a corporate owned asset, and therefore to anyone but employees. Furthermore, remote access from a corporate asset almost always means a laptop computer, which despite the reductions in hardware costs, still results in at least an $800 per remote employee greater capital expense over a desktop computer.

The majority of IPSec VPN solutions require that the remote node/network have special IPSec software installed on the client computer. This introduces a significant financial burden to maintain licenses for client software and for distributing IPSec clients to remote

machines and configuring them for access, which is challenging, especially when the Information Technology (IT) department does not have easy access to remote computers.

Clearly, very few companies would even dream of providing a laptop computer and remote access to every single one of their employees. As a result, on average only select few (10 - 20%) of any given companies employees typically get VPN remote access.

Even for those fortunate few that do get remote access, connectivity with an IPSec implementation is not always simple, nor guaranteed. Network address translation (NAT) and remote firewalls can have a dramatic, disabling effect on IPSec VPNs. Often times these configurations exist in environments where making changes to the network configuration is beyond the users control, i.e. in airport kiosks, or at customer locations. This often results in frustration, time consuming help desk calls, downgrading to a dial-up connection, or all of the above.

SSL: Ubiquitous Secure Access

Secure Sockets Layer (SSL) for remote access is based on a simple concept: use the encryption and authentication capabilities built into every Web browser to provide secure remote access to corporate applications.

An important note, however, is that SSL isn't a new technology. A public key encryption system that was invented by Netscape, SSL is now an IETF standard under the moniker of Transport Layer Security (TLS). Poked and prodded by security experts around the world, banks, governments, and major retailers entrust billions of dollars in transactions to it.

SSL: Initially for Extranets

Several years ago companies recognized the potential of SSL-based browser access and have begun deploying web-enabled services through virtual Extranets. The problem, however, is that, although many products are now SSL-enabled, deployment becomes a one-off endeavor, and results in independent silos of remote access. For example, it would not be uncommon to see all the following SSL-based access points in a single company:

- An *Outlook Web Access* or *iNotes* server for mail access
- A *Citrix/Nfuse* server for windows client/server windows applications
- A *WRQ Reflection for the Web* server for AS/400 access
- A custom *J2EE* application for employee timesheets
- An *SAP Portal* for customer inquiries.

Each of these access points is a separate infrastructure, often replicated from what is used internally and each provides a potential attack point for hackers. The fact that management is distributed only serves to make the security risks even greater. And yet, with this entire infrastructure, and all the management/support resources required to maintain and operate it, users still don't have access to everything they need.

By combining SSL-enabled Web browsers with an SSL-enabled security appliance to terminate connections and provide policy enforcement and access control, so-called SSL VPNs can provide access to files, web-based, legacy client/server, and terminal applications. Most importantly, access can be from anywhere; home PCs, hotel business centers, Internet cafes, or a business partner's network; all without any special software.

IPSec VPN	SSL VPN
• Ties user to a single machine and requires deployment and configuration of software for every user you want to give remote access	• Ubiquity of Web browser access enables nearly universal access • Requires no software to be installed or configured
• Firewalls and network address translation often interfere with access	• All traffic is sent over a single port, 443, which is already open or available through web proxies.
• Provides full network access without application authentication or authorization	• Allows granular access control to applications

AccessAnywhere Whitepaper

SSL VPNs: Remote Access all Employees

By going beyond the original purpose of SSL (securing communications with web servers), today's leading SSL VPNs combine the benefits of SSL with policy-based proxies to deliver on the promise of cost effectively making **"application access as ubiquitous as voicemail access"**

Typically delivered as a single application-layer security appliance SSL VPNs address all application-access scenarios:

- Secure access to web-based applications, content, portals, and files
- Secure access for desktop client/server applications
- Secure clientless, access to remote legacy applications

Addressing all three of these application-access scenarios means companies can deliver any IT resource to all remote end-users, and establish enforceable policy-based access, based on classifications: telecommuter, road warriors/traveling employees, partners, vendors, etc. As a result, although more users have access, internal security will be significantly enhanced.

The key is that while IPSec is network-layer centric, SSL is application-layer centric and can provide the granular access control such that all users, both in and out of the physical office, and all connected foreign networks need explicit permission to access any resource within the intranet. They provide tunnels to specific applications rather than to the entire corporate LAN. So, users on SSL VPN connections can only access the applications that they are configured to access rather than the whole network.

The AccessAnywhere SSL VPN: A Comprehensive Remote Access Solution

In addition to addressing the core SSL VPN application-access scenarios through AnywhereWeb, AnywhereClient, AnywhereApplication, the AccessAnywhere appliances provide elements typically required in a production remote access deployment. These include:

- a robust, stateful packet filtering firewall
- pre-integrated two-factor authentication services
- highly redundant system components
- lights-out management capability
- proactive system monitoring

AnywhereWeb™

AnywhereWeb is the service component that provides ubiquitous access to web-based intranet/extranet applications and web-based, e-mail services such as Microsoft Outlook Web Access, Lotus iNotes. It also contains two sub-components, File Access and Mail Access, which provide access to network file shares (i.e. NFS, FTP, SMB and Netware), and standards based e-mail servers.

The core *AnywhereWeb* service delivers web based applications via a sophisticated URL rewriting, reverse HTTP proxy. The URL rewriter translates all of the URLs (for all HTML, JavaScript, and XML) to ensure that all intranet/extranet content is always retrieved from the AccessAnywhere appliance. The URL rewriter uses a powerful rules based XML engine to determine rewriting behavior. The default ruleset will permit most intranet and extranet content to be successfully rewritten and accessed remotely; additional rules can be written to support virtually any content or application. Using URL rewriting enables granular access control without having to specifically create mappings for resources as is done with traditional reverse proxies.

AnywhereWeb File Access delivers a lightweight Java applet to the client browser to support access to network file servers. Users can browse, upload, download, delete, compress, mail and search for files on remote file servers. All traffic to the AnywhereWeb File Access applet is transmitted over the SSL session, and can connect to remote file systems via SMB (Windows NT/2000/XP, Linux/Samba), FTP, or NFS. Configurable MIME-types allows automatic launching of the file into a local application.

AnywhereWeb Mail Access delivers either a standard HTTP application or a lightweight Java applet to the client browser to support access to non-web, standards-based, e-mail servers. Users can connect to e-mail servers using IMAP and SMTP. AnywhereWeb Mail Access consists of an appliance component and an optional Java client component.

AnywhereClient™

AnywhereClient enables a secure connection between an arbitrary client application on a system that is running a Java-enabled browser and a network resource behind a corporate firewall (i.e., E-Mail servers, Database servers, Telnet Hosts, Legacy Hosts (3270/5250), Terminal Servers, Remote Desktops, etc.). Since all traffic encrypted and sent through an SSL datastream over port 443, the remote client can even be behind a firewall and/or HTTP proxy. AnywhereClient is a

lightweight rules-based Java applet that is downloaded to the client browser and configured to listen and accept requests on administrator determined ports. Once a request has been accepted, AnywhereClient will route the traffic to the AccessAnywhere appliance where the connection is terminated and access control rules are enforced. Having passed all ACL's the request is passed onto the LAN in native format. Since the confidential nature of the information being passed over a client-server connection can vary greatly, and all encryption comes with a price, AnywhereClient can be configured to use specific encryption algorithms and key sizes on a rule by rule basis. As this implies, each connection results in different keys, providing significantly better security over single session key implementations. As an additional security feature, AnywhereClient can request acknowledgment and acceptance from the user anytime a new connection attempt is made, furthermore, this acceptance can be protected by a password.

AnywhereApplication™

AnywhereApplication provides a unique, non-intrusive, and modular way to provide client-less access to all corporate applications, including those that run on Microsoft Windows, UNIX, Linux, S/390 or AS/400 servers. There is no need to deploy client software, or modify networks, applications or the servers on which they run. AnywhereApplication provides seamless access all applications through a single, unified and familiar web-based interface. AnywhereApplication is a Java applet, which runs in the main AccessAnywhere browser window and communicates with the appliance through an AnywhereClient connection. By leveraging the dynamic nature of the Adaptive Internet Protocol, even applications with complex bandwidth interface elements (i.e. X11) can be delivered over slow WAN links. Additionally, client/server applications that do not perform well over anything but a LAN connection can be successfully deployed with the thin-client nature of AnywhereApplication. The administrator controls granting of application 'availability', with access ultimately being controlled by the back-end application server by whatever method is uses. AnywhereApplication will facilitate 'single-sign-on' to most back-end application servers, making moving through heterogeneous applications seamless for remote users.

AnywhereID™

AnywhereID consolidates key security features into the AccessAnywhere appliance with the singular goal to build a flexible and agile access procedure that can accommodate mobile workers while still safeguarding corporate assets. Enhanced client security elements for two-factor authentication is integrated into the platform for fast and reliable deployment. With AnywhereID users will identify themselves against an integrated RSA ACE/Server using username/password and SecurID tokens. RSA SecurID authenticators function like an ATM card for your network, requiring users to identify themselves with two unique factors - something they know and something they have - before they are granted access. By deploying AnywhereID to users, administrators can take advantage of strong, two-factor authentication, one-time passwords, and the true mobility that users demand.

SSL VPNs: Achieving a Balance between, Security, Ease of Use and TCO

While IPSec VPNs will continue to be deployed, their predominance and legacy will be as site-to-site VPNs. The less appropriate role of providing users with remote access to applications and data is quickly becoming the sole domain of SSL-based solutions.

SSL VPNs overcome the limitations of discrete Web-only SSL technologies to offer end-users the ability to access all information and applications, universally from any browser without sacrificing. IT administration and support is a fraction of that for an IPSec VPN because there isn't any complicated software client to deploy or manage and infrastructure costs are dramatically reduced versus deploying point SSL-based access technologies.

These factors, along with the ease of use, and speed of deployment, drive the total cost of ownership of secure remote access to the point that, like voicemail, it can be made available to the entire company.

IPSec VPN vs. SSL VPN: Feature Matrix

Features	IPSec VPN	AccessAnywhere SSL VPN
Confidential Communications	Yes - RC4, 3DES, etc ciphers	**Yes - RC4, 3DES, etc ciphers**
Authentication	Proprietary	**Flexible - LDAP, Radius, Active Directory, Token, PKI**
Authorization	Network Level (Hosts/Protocols)	**Application Level (URL, File Share, Host, Port, etc)**
Resource Access Options	Entire Network	**Web, Client/server, File shares, Mainframes, Terminal Services, Terminal emulation**
User Device Support	Limited - Corporate PC	**Corporate PC, Kiosk, Home PC, PDA, etc**
End Point Security	Limited	**Host Integrity Checker, Cache Clean-up, Virtual Desktop, Malware Protection**
Hardened Appliance	Yes	**Yes**
Site-to-Site VPN	Yes	**Yes**
Network Firewall	Yes	**Yes**
Audit, Analysis, Reports	Limited	**Extensive**
High Availability	Yes	**Yes**
Scalability	Subset of employees	**Entire employee population**
User Experience	Complex - special hardware, software, certificates	**Simple - Internet browser**
Product Line breadth	Small to Large	**Small to Large**
Relative Cost of Ownership	High	**Low**

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