SSL VPN vs. IPSEC VPN: A Study and Comparison
By: David Van, CTO & Cofounder, Xceedium, Inc.

To put it simply, SSL and IPSEC are both encryption protocols that protect IP-based data streams over any TCP network. In my opinion, one can argue that one encryption protocol may be stronger or weaker than another from a technical point of view; however, it is not scientific and practical to argue which one is better in terms of the applications of these encryption protocols. There is no right or wrong in choosing which protocol to use when it comes to choosing which type of VPN companies should use as both have their own unique features and advantages.

Historically, IPSEC VPN technology was intended as a means to protect data communication between private networks over the Internet years ago. Later on, it was extended to protect data communication between mobile users accessing a company's internal network in favor of the legacy direct dial-in methods. Over the years, as mobility has become a trend, increasing usage of IPSEC VPN in securing mobile users' access has become a burden and a high cost to companies. The burden is having to maintain the client VPN software that each mobile user must have pre-installed to connect to a private network. This has a direct impact on operational cost to support mobile users. Also as broadband proliferates, telecommuting users were added to the mix - connecting insecure employees' home networks to the company's network. Before long, as outsourcing and business collaboration practices were adopted, un-trusted networks were connecting to companies' private network in a rush. IPSEC VPN is a powerful full-spectrum access security solution that was once very effective in securing intra-office connectivity. However, over time, it has evolved into a one-size-fits-all solution for all remote access. Consequently, as we know today, IPSEC VPN has become a potential security vulnerability for companies - not because the protocol is weak but because of how it is being used.

SSL was designed specifically to secure the HTTP protocol. By encrypting the data streams transmitted via this protocol, SSL provides a secure "wrapper" to protect IP packets between a browser and the web server, with both sides being setup to support SSL. There are a few key philosophical differences in the design of the IPSEC and SSL protocols. First, IPSEC is network-layer centric while SSL is application-layer centric. Second, IPSEC requires specific client software while SSL uses any SSL-enabled browser as the client. Lastly, SSL is natively mobility centric while IPSEC is not. Case in point, the SSH protocol, while also an application-layer-centric encryption solution, has the potential to evolve into a new SSH VPN but it is not. The key success of SSL is its mobility.

In recent years, SSL VPN was derived as a more fitting solution for securing application-based access because of the protocol's philosophy. In action, one can easily recognize that SSL VPN can quickly address most of the IPSEC VPN related vulnerabilities. The intrinsic application-centric methodology allows granular control of user access, thereby creating a per-user policy-based access to be established and enforced. The perceived clientlessness, although a browser is truly the client, increases user convenience while decreasing maintenance burden and cost to the company. Lastly, combining the restrictive access and clientless convenience, SSL VPN can effectively secure all data streams between the user and network while IPSEC VPN remains as a proven solution to protect data streams from network to network. As such, it is appropriate to consider
SSL VPN as an augmenting solution, rather than a competing one, to IPSEC VPN, at least for now.

At the current pace, SSL VPN is catching on like wild fire. Questions pertaining to the faith of IPSEC VPN is natural but pointless. IPSEC VPN is a proven solution and will forever remain one, unless the computing world as we know it today drastically changes. Companies should ask "how can the two technologies co-exist?" rather than "Which one is better?"

Fundamentally, IPSEC VPN was designed to protect private data streams between trusted networks from all un-trusted networks. SSL VPN was derived to protect data streams between associated sources, and all sources are un-trusted regardless of whether they are users or a network. This is the key concept to grasp in order to properly optimize both VPN solutions. Once upon a time, there was a clear segregation of trusted sources and un-trusted sources. Trusted sources were intra networks and employees. Today, such distinction is difficult. For network-to-network connectivity, are your partners’ networks trusted? Is the off-shore or domestic outsourced vendors’ network trusted? Are the shared co-located and DR facilities trusted? Is the telecommuting employees' home network trusted? For user-to-network connectivity, are consultants or outsourced agents trusted users? Are business partners’ employees trusted? Diving deeper into the organizational layers, are disgruntled employees trusted? Are telecommuting employees trusted? And if trust means access privilege, then should all trusted employees have equal access clearance? In other words, should business users and technical users have the same level of access to the resources in the IT infrastructure? Should a junior IT employee have the same level of access for administering critical systems as a senior IT employee or manager? The point is, intra-network should be the sole trusted infrastructure that can be protected at the highest level by IPSEC VPN. Inside it, SSL VPN 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. Technically speaking: IPSEC VPN protects network-to-network data communications between intra networks across the Internet while SSL VPN protects intranet data communications from classified users, extranets, and Internet.

The Upcoming Trends

As SSL VPN helps companies consolidate and secure remote access for all types of users, the next logical trend is to favor an available solution that can effectively integrate various forms of access so that all ingress points can be managed centrally, within the SSL VPN infrastructure and outside of the firewall and IPSEC VPN management. Achieving such a goal means companies can establish an enforceable policy-based access for all end-users based on classifications: telecommuter, traveling employees, partners, etc. Internal security will be significantly enhanced and auditable.

One final point is that the need to create SSL VPN was actually driven by the concerns of information disclosure due to the lack of access manageability, theft, or actions of an uninformed mobile user. All of which IPSEC VPN was unable to address effectively. However, in light of recent global turmoil such as 9/11, SARS, and the East Coast Blackout of 2003, mobility interests are on a steep rise. Different than before, mobility applies to the IT infrastructure as well, rather than just remote users. SSL VPN, as new
as it may be, is already transforming the IT landscape. Instead of providing just inbound access, such as remote users accessing applications in the companies' network, SSL VPN must fill the need for outbound access, such as IT staff supporting remote IT infrastructures that are staged far away in anticipation of future disasters. As such, a comprehensive SSL VPN solution must be able to support both end-user access as well as remote IT administration; furthermore, it must also support advanced remote access methods required by technical users, such as all out-of-band and power control capabilities. Essentially, what is need is a powerful SSL VPN solution that can provide any IT personnel, from anywhere, the ability to access any device of a remote and diversified IT infrastructure. This solution is the Xio Universal Access Gateway.

About Xceedium's Universal SSL VPN Gateway Solution

Xceedium, as one of the earliest adopters of the SSL VPN concept, rolled out the eXtensible In-band Out-of-Band Universal Access Gateway (Xio UAG) appliance in 2001. The significance of Xceedium's offering is not only that it is the first SSL VPN appliance on the market and already has more than two years of refinements, but it is still the only solution that encompasses remote access for IT management and business end-users alike at the present time.

Xceedium recognized early on that SSL VPN can significantly augment IPSEC VPN to improve mobility and to enhance internal security for remote access. In late 2000, Xceedium also predicted that as SSL VPN becomes main stream in managing mobile business users accessing applications, the evolutionary trend will demand for securing remote administrative access. As such, Xceedium engineered a secure remote access solution based on SSL VPN that is still years ahead of its time. In 2002, as all SSL VPN solutions emerged to only fulfill end-user access requirements, such as remote application and file access, Xceedium's complete SSL VPN framework extended accessibility to include remote power control of any device, administrative access to serial console ports of network devices and UNIX servers, as well as network-enabled KVM console on Intel servers. At present time, Xceedium's solution is a 2nd generation SSL VPN product and the only solution that can satisfy both end-users and technical engineers. In 2004, Xceedium's SSL VPN will be extended to include remote monitoring, trending, and asset tracking. Additionally, Xceedium will offer the first network-to-network SSL VPN solution that will further augment traditional IPSEC VPN by securing the application-level data communications across all TCP networks.

Xceedium has established key strategic partnerships with companies such as Ingram Micro in China and Canon Business Solutions in Japan. Xceedium was founded and is headquartered in New York City, and has operations in Los Angeles, United Kingdom, Japan, Shanghai, Peking, and Taiwan, plus over 40 support centers globally. Its SSL VPN framework solution has been deployed in virtually all industries worldwide.