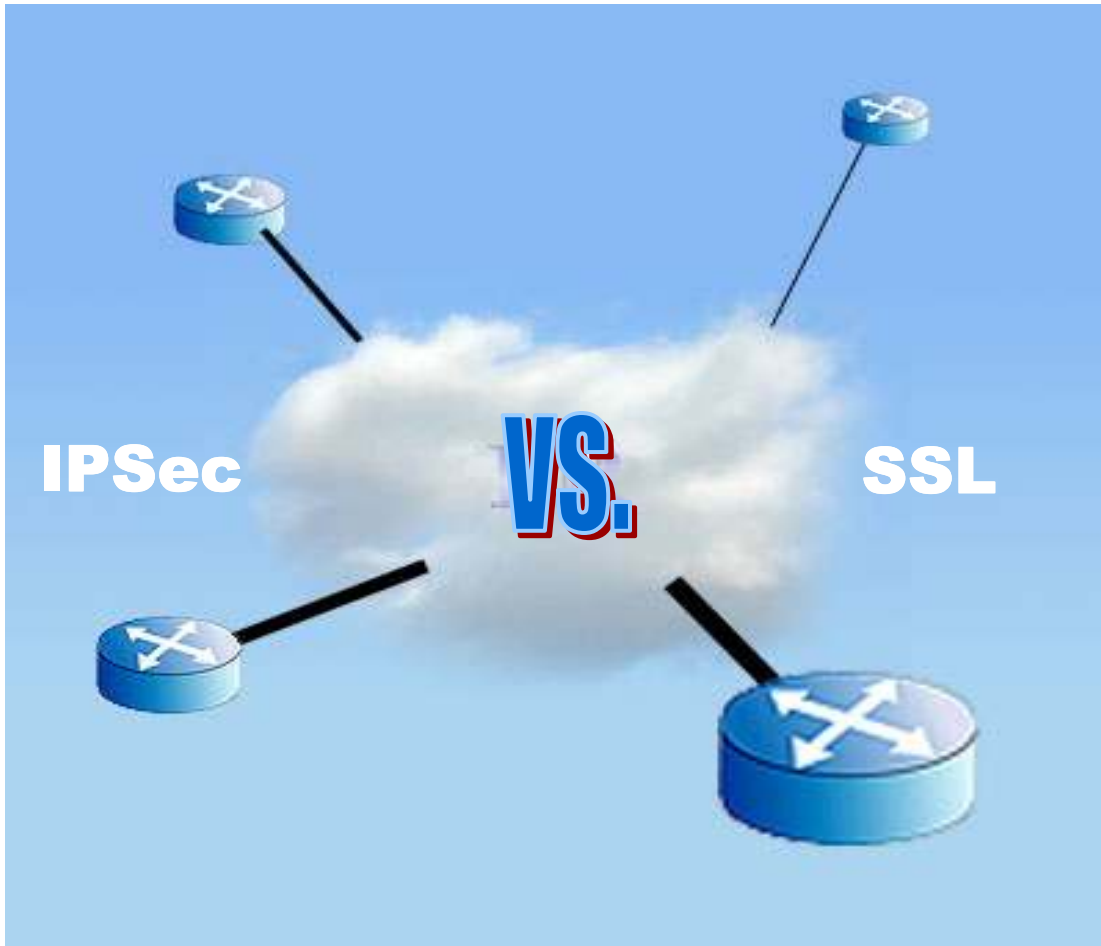


Virtual Private Networks: IPSec vs. SSL



Michael Daye Jr.
Instructor: Dr. Lunsford
ICTN 4040-001
April 16th 2007

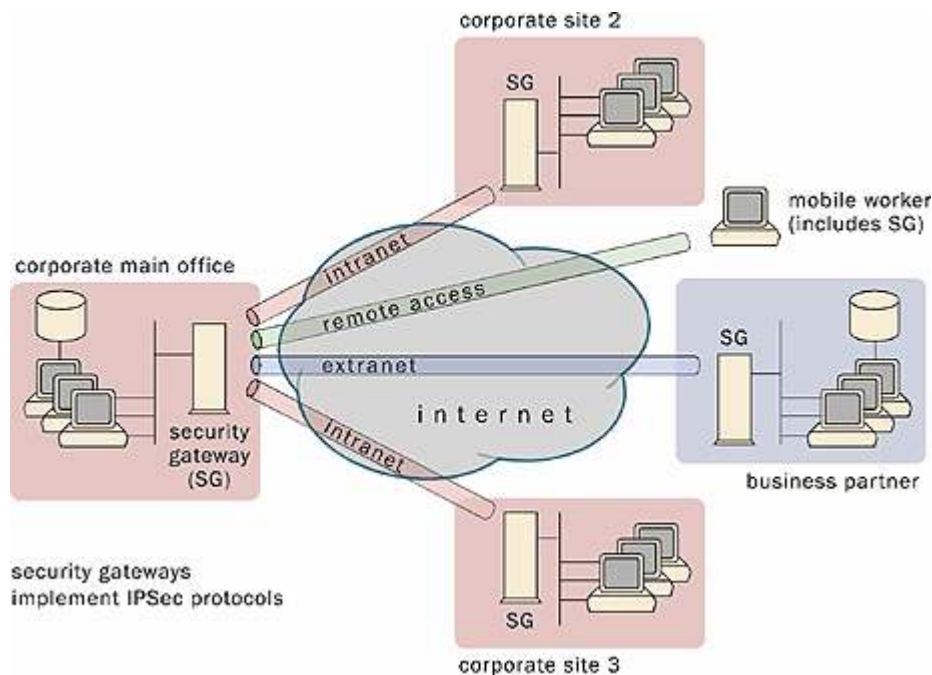
Virtual Private Networks: IPSec vs. SSL

In today's society organizations and companies are expanding globally from region to region. Employees working from home offices are also becoming very popular, which organizations benefit financially by utilizing less office space, and reducing total expenses incurred by having office workers on site. With this expansion, organizations develop a need to communicate with these offices over highly secure, confidential, reliable connections regardless of the location of the office.

VPNs or Virtual Private Networks are used by many organizations and companies to fulfill the need to communicate securely and confidentially over the internet with its employees and offices outside the corporate network. A VPN creates a private and secure connection, known as tunnels, throughout systems that use the data communication capability of an unsecured and public network—the Internet. VPNs use secure protocols to provide private communications over the Internet; they also connect the private corporate network to home-office employees, or to a remote business site through virtual connections routed through the Internet. Organizations which decide to use VPNs as their means of secure communication, would choose between the more commonly used IPSec and SSL secure protocols. Both protocols have their advantages and disadvantages; the deciding factors between the two depend on the infrastructure of the corporate network, its specific security requirements, costs, and reliability.

Many organizations choose IPSec VPNs through the internet because the cost for private WAN connections, leased lines, and long distance phone charges are extremely high. Organizations and companies save tremendously by choosing IPSec VPNs. It aids in productivity by increasing business-to-business communications, sales, and customer service management. IPSec provides the capability of allowing home-office employees and

telecommuters to connect to the organizations network resources securely and conveniently via remote access through the internet. The diagram below provides a visual of how an IPSec VPN connects corporate offices, businesses, and mobile workers to the organizations network over the internet.



IPSec was designed by IETF IP Protocol Security Working Group to maintain a secure exchange of packets at the IP layer. IPSec operates at layer 3 of the OSI model, which is the network layer. It provides security services at the IP layer by enabling a system to select required security protocols, determine the algorithms to use for the services, and put in place any cryptographic keys required to provide the requested services. The set of security services that IPSec can provide includes: an access control, connectionless integrity, data origin authentication, rejection of replayed packets, confidentiality, and limited traffic flow confidentiality. Before two devices can communicate on an IPSec VPN, they must first agree on the security parameters used during the communication, which is known as establishing a

Security Association (SA). The SA specifies the authentication and encryption algorithms to be used, the encryption keys to be used during the session, and how long the keys and the security association are maintained (IPSec VPNs). IPSec uses two protocols to provide traffic security; one is the Authentication Header (AH) protocol which provides connectionless integrity, data origin authentication, and also an anti-replay service which is optional. The other is the Encapsulating Security Payload (ESP) protocol which provides confidentiality, and limited traffic flow confidentiality (Kent 6-7). The (AH) protocol does not provide secrecy for the content of a network communication, but the (ESP) protocol does along with system authentication and data integrity verification. Either of these protocols can be used in IPv4 or IPv6 and can be used together. If they are used in conjunction with each other, they can provide a wider range of security services. IPSec works in two modes of operation known as transport and tunnel mode. In transport mode only the IP data is encrypted not the IP headers, which allows intermediate nodes to read the source and destination addresses. In tunnel mode, the entire IP packet is encrypted and is then placed as the content portion of another IP packet. Once this is done, these systems then transmit the decrypted packets to their true destinations. (Whitman and Mattord 378-379).

In order for a client (employee or telecommuter) to connect to their organizations IPSec VPN, they must have VPN client software installed on the computer virtually accessing the organizations network. Some popular IPSec VPNs are developed by Microsoft, Cisco, Nortel, and TheGreenBow. Organizations which choose IPSec may experience slow and ineffective service from support technicians, due to the fact that the technicians require access to multiple networks. Once they are connected to an IPSec Virtual Private Network, it locks their PC to a single organization's network which limits their support capabilities. Organizations utilizing

IPSec must also manage VPN accounts, login credentials, and security keys which also puts a burden on the organization to keep that information confidential, as well as protecting it from unauthorized usage. Organizations can minimize the cost and responsibility of credential management by issuing a single account to a third-party or support organization but this leads to other security vulnerabilities.

The L2TP (Layer 2 Tunneling Protocol) is often implemented with IPSec due to the fact that when used alone, it lacks confidentiality. Along with authentication and integrity, IPSec is used to secure L2TP packets by providing the confidentiality it lacks. L2TP represents a merging of the features of PPTP with Cisco's Layer 2 Forwarding Protocol (L2F), which was originally designed to address some of the weaknesses of the Point-to-Point Tunneling Protocol (PPTP). Both L2TP and PPTP operate at the data link layer, layer 2 of the OSI model. PPTP is the most widely deployed tunneling protocol, which is a commonly used protocol for establishing connections over a serial line or dial-up connection between two points (Ciampa 231-232). Some of the PPTP weaknesses are that this protocol is vulnerable to man-in-the-middle attacks related to data integrity and data origination. One of the most defiant weaknesses of the PPTP is that it only supports single-factor, password-based authentication. The Layer 2 Tunneling Protocol (L2TP) supports two types of mutual authentication, which makes it more secure than PPTP. The primary benefit of configuring L2TP with IPSec is that remote users can access a VPN over a public IP network without a gateway or a dedicated line, enabling remote access from virtually anyplace with POTS (Plain Old Telephone Service). An additional benefit is that the only client requirement for VPN access is the use of Windows 2000 with Microsoft Dial-Up Networking (DUN); no additional client software, such as Cisco VPN, is required (*Cisco Systems 28-1). When L2TP and IPSec are used together often referred to as

L2TP/IPSec, IPSec encapsulates the L2TP packets between the endpoints. The L2TP packet is transferred and hidden inside the IPSec packet, which ensures that information cannot be gathered from the encrypted packet about the internal private network. Implementing L2TP with IPSec also narrows down on the software requirements for the end client (home-office employee or telecommuter) to connect to the VPN. IPSec can benefit an organization tremendously, in numerous ways, but it is not the only secure protocol offered for use when Virtual Private Networks are implemented.

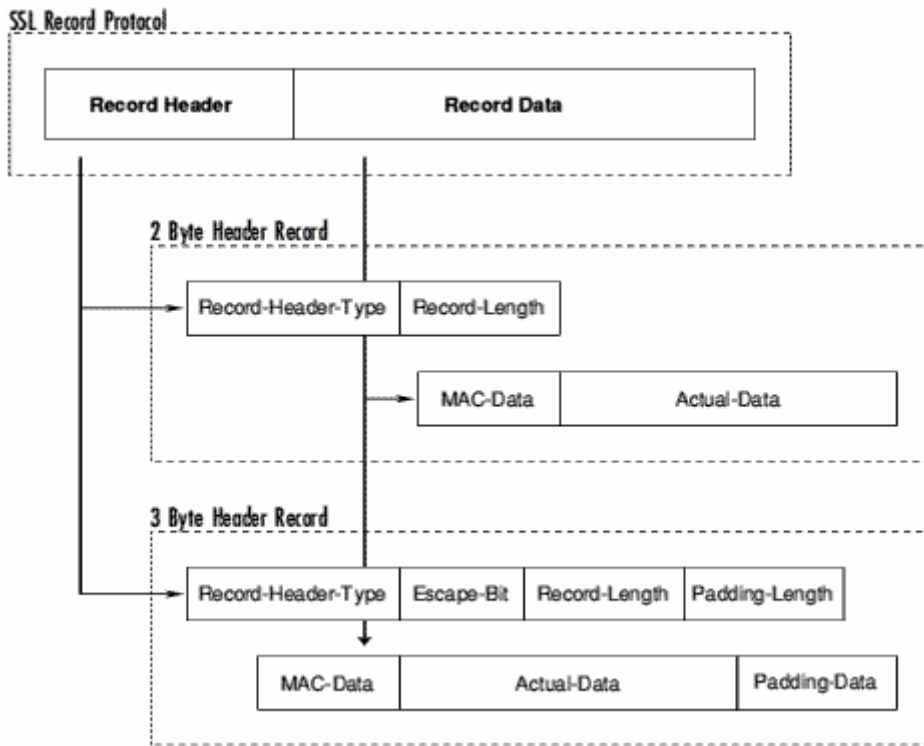
Some organizations choose to implement their VPN with the Secure Sockets Layer (SSL) protocol. SSL is also used to allow access to home-office workers and telecommuters who need to use their organizations resources from outside of the internal network. SSL VPNs do not require client software, like Cisco VPN, to be installed on the client machine before it can access the organizations network. According to VPN expert Ted Studwell, what SSL (VPN) devices allow you to do is to put a device behind the corporate firewall, and basically establish an SSL session from pretty much any browser. Basically, these devices will negotiate the session and determine what you'll have access to (Ringleben). Therefore, end users are not required to be at their PC to gain access to the organizations network; they can simply access the organizations network resources via any device which utilizes a web browser which supports SSL sessions.

Secure Sockets Layer (SSL) is a protocol developed by Netscape for securely transmitting documents over the Internet. Some of the major companies which make SSL VPNs are uRoam, Neoteris and Netilla. SSL uses a private key to encrypt data that is transferred over the SSL connection (Ciampa 210). Along with providing data encryption, SSL also provides integrity and server authentication. When SSL is properly configured, it also provides client authentication. SSL works by establishing a normal HTTP session between a client and a server;

once the client request access to a portion of the Web site, which requires secure communications, the server sends a message to the client indicating that a secure connection needs to be established. The client responds with its public key security parameters and the handshaking phase is complete once the server finds a public key match and responds by sending a digital certificate to the client in order to authenticate itself (Whitman & Herbert 376). Once this process is complete, it is up to the client to verify that the certificate is valid and then the SSL session is established between the server and the client. A digital certificate is a public key that has been digitally signed by a recognized authority attesting that the owner of the key is whom they say they are (Ciampa 290). Digital signatures are used to prove that the person sending the message with a public key is actually whom he or she claims to be, also proving that the message was not altered, and that it was actually sent (Whitman & Herbert 289). Data can be transmitted securely in any amount, as long as the SSL session remains active between the client and the server. To ensure that data is not altered during transmission, SSL uses cryptographic hashing. Hash values are computed by both the web server and the web browser using the same hash algorithm. If these two values match you can ensure that the data transmitted has not been altered.

SSL provides two layers of protocols within the TCP framework; the SSL Record Protocol which is responsible for the fragmentation, compression, encryption, and attachment of an SSL header to the cleartext prior to transmission, and Standard HTTP which provides the Internet communication services between client and host, without consideration for encryption of the data that is communicated over the connection (Whitman & Herbert 376). The SSL Record has two parts, the header and the data. The header of a SSL Record can be 2-bytes in length with a maximum record length of 32767 bytes, or the header can be 3-bytes in length with a

maximum record length of 16383 bytes (Hickman). This figure below demonstrates how a SSL Record Protocol is constructed.



The data portion of the SSL Record consists of a Message Authentication Code (MAC) which is the actual data, along with padding data if needed. The MAC is a hash or message digest of the secret write key of the sending party, the actual data, the padding data and a sequence number in that order. The sequence number is a 32 bit integer, which is incremented after each message is sent (Hickman). SSL provides secure and reliable connections between clients and servers, and organizations can benefit greatly from its features.

SSL is more friendly toward third party and vendor technicians than IPsec, due to the fact that numerous technicians are able to connect to an organization's network and they are not locked to a single organization's network. This can lead to even more security vulnerabilities, along with account and credential management problems. With SSL, it is also possible to assign login credentials to technicians requiring access, but this places a huge burden on an

organizations IT team to keep track of enabling and disabling third-party and vendor accounts, along with their own organizations accounts. When using IPsec, it requires client end software to connect to the VPN, but SSL does not. This doesn't mean that SSL is better to use, because SSL encryption and decryption process requires a huge amount of CPU processing power and affects the server tremendously. This drawback using SSL lead to the creation of SSL adapter cards designed to help off-load the server's CPU load and increase performance. W. Chou mentioned that today, content switches with SSL accelerators can encrypt and decrypt data at the network edge, eliminating the need for a Web server's CPU to perform any SSL-related calculations (*Chou).

According to Ted Studwell, IPsec offers more benefits toward network managers. He also states that, one of the major issues with the SSL (VPN) is that when you set up the SSL connection, it's pretty much open ended on the back end. With an IPsec VPN, you can limit what one user gets versus other users (Ringleben). This basically means that if the SSL VPN is used, an organizations network manager won't have much granularity for control. An advantage of SSL over IPsec is that the installation process is a lot easier. With IPsec, you can install client software and configure each PC that will access the network; with SSL, the only configuration needed is to setup the VPN device, and end users don't have to install any additional software and can be up and running in no time. Another advantage of IPsec is that it operates at the network layer and it secures all data between two endpoints including all applications such as, E-Mail, File Share, Web (HTTP), Client-Server, Databases, and Terminal Services. The SSL secure protocol operates at the application layer, limiting access to only the resources that are browser-accessible like Web (HTTP), E-mail, and File Share (OpenReach, Inc.). Studwell also mentioned that majority of the VPN Service Providers favor IPsec, because SSL has limited

functionality which works great in some cases but doesn't fix the problem for most corporate IT infrastructures (Ringleben). As far as costs, both IPsec and SSL VPNs require VPN-capable servers at the corporate site to establish remote user sessions. Since SSL VPNs don't require client software and can be deployed easier, the IPsec their total costs of ownership is usually less (OpenReach). The decision between these two protocols also may depend on which type of network the organization uses IPv4, IPv6, or both. If the network only uses IPv6 such as high-speed broadband internet, then the choice would be IPsec-based security. If the networks are using IPv4 or a combination of IPv6 and IPv4, it is best to use SSL-based security (*Zhang, Fenghai, Jianyong, Yang, and Chenwen). Here is a comparison chart of IPsec and SSL stating some of their strengths and weaknesses.

	SSL	IPSec
Applications	Web-enabled applications, file sharing and e-mail	All IP-based services
Encryption	Strong but variable—depends on browser	Strong and consistent—tied to specific implementation
Authentication	Variable—one- or two-way authentication using tokens and digital certificates	Strong—two-way authentication using tokens and digital certificates
Overall Security	Moderate—any device can be used creating holes	Strong—tied to specific devices and implementations
Users	Sales, Marketing, Executives, Customers, Partners	HR, Finance, IT Staff, Engineering, Operations
Accessibility	Casual access to broadly distributed user base	Formal access to well-defined and controlled user base
Cost	High-fixed/Low-variable (the box does all the work)	Moderate-fixed/High-variable (manage client software)
Complexity	Moderate	High
Ease of Use	Very High—uses familiar web browsers	Moderate—can be challenging for non-technical users
Scalability	High—easily deployed, requires tight application integration	Very High—-independent of applications

Organizations and companies may choose whichever VPN secure protocol they desire, but it is evident that IPSec has more to offer an organization seeking secure data communications with employees, telecommuters, and regional businesses than SSL. They both have their strengths and weaknesses, which are considered when a decision between the two is necessary. It is possible to use both IPSec and SSL, but the cost factor of using them together usually put organizations in favor of one over the other. IPSec is more useful to users which seek to use all applications and resources remotely as if they were physically connected to the organizations LAN. SSL is useful to users who need mobile access to applications like E-mail and file sharing, users who are not going to be physically at one PC location, and will be accessing the organizations network via PDA's, laptops, and cell phones. Both of these secure protocols can be very useful in their own way and provide organizations with the security they need. Many factors are to be considered when deciding which secure protocol to use and with the information provided, organizations can make that decision easier and with more confidence.

Works Cited

- *Chou, W. "Inside SSL: Accelerating Secure Transactions." IT Professional. Sep/Oct. 2002: 37-41.
- Ciampa, Mark. Security+ Guide to Network Security Fundamentals. 2nd Edition. Massachusetts: Thomson Course Technology, 2005.
- *Cisco Systems, Inc. Cisco Security Appliance Command Line Configuration Guide. Version 7.2. California: Cisco Systems, 2006.
- Hickman, Kipp. The SSL Protocol. Netscape Communications Corp. 29 Nov. 1994. 23 Mar. 2007. <<http://www.llnl.gov/atp/papers/HRM/references/ssl.html>>.
- IPSec VPNs: Conformance & Performance Testing. 12 Jan. 2003. White Papers Ixia. 11 Apr. 2007. <http://www.ixiacom.com/library/white_papers/display?skey=ipsec>.
- Kent, S. Security Architecture for the Security Protocol. Network Working Group. Nov. 1998. Javvin Network Managing & Security. 05 Apr. 2007 <<http://www.javvin.com/protocol/rfc2401.pdf>>.
- OpenReach, Inc. *IPSec vs. SSL: Why Choose?*. Jan. 2002. Open Reach. Security Tech Net. 20 Mar. 2007. <http://www.securitytechnet.com/resource/rsc-center/vendor-wp/openreach/IPSec_vs_SSL.pdf>.
- Ringleben, Kurt. SSL VPNs: Great for Basic Access but Not for Power Users. Search Networking. 20 Jun. 2002. 23 March 2007. <http://searchnetworking.techtarget.com/qna/0,289202,sid7_gci834329,00.html>.
- Whitman, Michael and Herbert Mattord. Principles of Information Security. 2nd Edition. Massachusetts: Thomson Course Technology, 2005.
- *Zhang, JG, Yu Fenghai, Sun Jianyong, Yang YY, and Liang Chenwen. "DICOM image secure communications with Internet protocols IPv6 and IPv4." IEEE Transactions on Information Technology in Biomedicine. Jan. 2007: 70-80.