Security Review: SSL VPNs

—Frederick M. Avolio

Executive Summary

Today's enterprises use the Internet to meet a variety of communication needs among employees, business partners, suppliers, customers, and potential customers. These users communicate across public and private networks, possibly from remote offices, homes, and Internet kiosks. Enterprises who care about communications security, secure their communications with VPN — virtual private network — technology.

This white paper compares the two common foundations for VPN implementation, IPSEC and SSL, assessing the pluses and minuses of each type of VPN in general — for site-to-site connectivity and remote access — and in some specific uses. It then focuses on security and deployment considerations, and recommends scenarios in which SSL VPNs are more secure, easier to deploy, and better suited than IPSEC VPNs.

The paper shows them to have the same level of maturity, acceptance, and use in the world. Both are viable for VPN deployment. Security policies, business needs, and user sophistication will dictate which to use. SSL VPNs are usually a better choice for remote access. They are usually easier to deploy and provide more options for access, while providing tighter access control. IPSEC VPNs are best suited for site-to-site VPNs.

Security Review of IPSEC and SSL VPNs

In November 2002, the author wrote a column[1] asking the question, "Do We Really Need VPNs?" and started by stating, "The year 2001 will be remembered as the year of the VPN," but then went on to point out that he said the same things about 1998 and 1999. While not ubiquitous, VPN usage did rise due to the rise in remote access requirements pulled along by the increase in high-speed Internet access available to teleworkers and work-extenders, and by the maturing of the base technologies that provide VPNs.

This white paper compares the two common foundations for VPN implementation, IPSEC and SSL, assessing the pluses and minuses of each type of VPN in general — for site-to-site connectivity and remote access — and in some specific uses. It then focuses on security and deployment considerations, and recommends scenarios in which SSL VPNs are more secure, easier to deploy, and better suited than IPSEC VPNs.

Technical Overview[2]

A VPN combines two networking concepts: virtual networking and private networking.[3]

> **Virtual networks** allow geographically distributed users and network hosts to interact and be administered as a single "group." They also allow splitting up a physical network into logically separate virtual networks.
>
> **Private networks** incorporate data protection with guaranteed confidentiality among hosts on a virtual network, allowing trust relationships to be established and enforced on the network. With confidentiality, or privacy, VPNs can traverse untrusted networks, as well as share a physical network with untrusted parties.

VPNs have been commercially available since the mid-1990s. They are commonly used for two main purposes today: Low-cost, ubiquitous, secure remote access and secure site-to-site interconnection. Today's VPNs are based on two different technologies: IPSEC and SSL.

IPSEC and IPSEC VPNs

"IPSEC" is the name of an evolving family of protocols[4] that came out of the Internet Engineering Task Force's[5] IP Security Protocol Working Group. IP security features were to be added to IPv6. When it became clear that the Internet could not wait for IPv6, the IPSEC effort was born to add security features to IPv4.

IPSEC provides packet-level data confidentiality through encryption (via ESP, the Encapsulating Security Protocol). It also provides packet-by-packet host-level authentication and integrity checking (also via ESP or AH, the Authentication Header protocol). The host receiving an IPSEC authenticated packet can be certain of the packet's source. Both the encryption and authentication/integrity check use secret and public key cryptography. So, IPSEC also provides a session management protocol to manage the setting up of secure connections, authentication schemes used, keys to use for encryption, key life time, and other policy-related things. Though we sometimes just think of IPSEC in terms of gateway-to-gateway or user-to-gateway VPNs, it was created to work between any pair of networked computing devices (PCs, servers, routers, and others). IPSEC encrypts any type of IP traffic. It is a Layer 3 protocol.[6]

In addition to these protocols, IPSEC VPNs should provide access control, and most do. Since IPSEC operates at the network layer, IPSEC VPNs usually

[1] http://www.avolio.com/columns/14.html

[2] Some of this discussion gleaned from the course "VPN Day: Fundamentals," produced in collaboration by Core Competence, Avolio Consulting, and OpusOne.

[3] There are also services ISPs call VPNs that incorporate methods for asserting service quality and maintaining Quality of Service (QoS).

[4] Defined in RFC2401-2409, RFC2451, and http://www.ietf.org/html.charters/ipsec-charter.html

[5] The IETF: "The Internet Engineering Task Force is a large open international community of network designers, operators, vendors, and researchers concerned with the evolution of the Internet architecture and the smooth operation of the Internet. It is open to any interested individual." From http://www.ietf.org/overview.html.

[6] In the ISO OSI model, Layer 1 is the Physical layer (e.g., Ethernet), 2 is Data Link (e.g., PPP, FR), 3 is Network (e.g., IP, IPX), 4 is transport (e.g., TCP, UDP), 5 is Session (e.g., SSL, TLS), 6 is Presentation (e.g., ASN.1, XDR), and 7 is Application (FTP, TELNET, etc.)

control network access by a packet filter; the VPN permits or denies passage through the VPN appliance based on the source, destination, port, and packet type of each packet.

SSL and SSL VPNs

Netscape Communications originated and published SSL, the Secure Sockets Layer protocol, to facilitate web-based e-commerce. SSL provides digital certificate–based client and server authentication, integrity checking, and confidentiality. SSL is not only an official Internet standard, it is also a de facto standard, as it is available on every web browser in common use, and in "Open Source" form.[1]

SSL was originally created to secure web traffic, but it is increasingly used to secure non-web application protocols (such as SMTP, LDAP, POP, IMAP, and TELNET). SSL provides transport-level confidentiality through secret key cryptography, and key management and authentication through public key cryptography. For this discussion, we are not just looking at SSL-encrypted HTTP traffic between web server and client (browser). SSL VPNs can carry any TCP traffic, and some can handle UDP as well.

Because SSL is a transport-layer service, an SSL VPN has the advantage of being able to apply this access control at transport- and application-layers, providing greater granularity of control.[2]

Security Strengths

There are differences in IPSEC and SSL related to the process level — IPSEC processes run at the operating system level and SSL is a user level process — but few directly relate to security.[3] Those that do will be addressed later. First, we will discuss security strengths in both SSL and IPSEC.

Maturity and Acceptance

Both SSL and IPSEC benefit from being established technologies, though SSL is more mature (and more stable). Netscape released SSL v2 in 1994. IPSEC's original RFC 1825[4] is dated 1995. It had "problems," and was replaced by RFC 2401[5] in 1998. IPSEC products in one form or another (the standards are still growing and evolving) have been around since 1995.

Both have been equally accepted and adopted. Without exaggeration, SSL is available and used in virtually every web server and client in existence. In addition, SSL[6] has been adopted by other services needing security, such as e-mail (SMTP) and directory services (LDAP). Many security-related devices that require a secure and authenticated connection use web-based administration over SSL. Also, SSL use for VPNs is popular, and its popularity is growing, for reasons discussed below.

IPSEC is built into some routers, switches, operating systems, Internet firewalls, and IPSEC VPN appliances. It has been accepted by the Internet standards body to be the protocol suite to secure all IP traffic.

SSL solutions are highly interoperable. It is rare to experience problems between an SSL client and server. IPSEC, even though it is made up of a set of Internet standards, continues to suffer from interoperability problems, even among some products that conform to the standards.[7] Again, a difference like this is not an issue of security as much as one of usability and availability.

Cryptography

Cryptography underpins all VPN security. Cryptographic methods are used for confidentiality, authentication,

[1] See www.openssl.org.

[2] For a discussion of benefits of granularity, see Avolio, Frederick, "Application Gateways and Stateful Inspection," http://www.avolio.com/papers/apgw+spf.html.

[3] Those that do are mentioned in Perlman and Kaufman, "Analysis of the IPSEC Key Exchange Standard," from The Proceedings of WET ICE 2001, http://sec.femto.org/wetice-2001/papers/radia-paper.pdf.

[4] ftp://ftp.rfc-editor.org/in-notes/rfc1825.txt

[5] ftp://ftp.rfc-editor.org/in-notes/rfc2401.txt

[6] Or Transport Layer Security, TLS, which was derived from SSL v3.0.

[7] Although, multiple products from a single vendor usually interoperate.

and integrity assurance. Both IPSEC and SSL provide confidentiality through secret key cryptography, authentication through digital certificates, and integrity assurance through cryptographically strong Integrity Check Values[1].

IPSEC is well known for having strong cryptography through the use of well-tested cipher suites.[2] IPSEC also allows strong enforcement of crypto-related security policies (such as permitted encryption algorithms, key sizes, and many other parameters).

Netscape released SSL v3 in late 1995 and it uses cipher software developed by cryptographic experts using cipher suites open for examination, testing, and certification. These are often the same cipher suites used in IPSEC implementations.

Web store fronts may allow SSL connections using weak cryptography, for example to accommodate browsers with small key sizes. This is not an SSL weakness, but a security decision made by the merchant to allow more potential customers to connect. With an SSL VPN, the server would be set up to enforce the enterprise security policy, which would include minimum key length and acceptable crypto algorithms, just as with an IPSEC VPN.

Both SSL VPNs and IPSEC VPNs could be vulnerable to a "man-in-the-middle attack." Any system using public-key cryptography can be vulnerable to such an attack. All it takes is a "man in the middle" who can pretend to be Bob to Alice, and Alice to Bob. This is especially easy if they do not know each other.[3]

For VPN use, it is important that one or both sides of the conversation — the server or both the client and server — use digital certificates. With digital certificates, each has a way of verifying the credentials of the other. Each can check out the certificate of the other to ensure that a trusted third party, their Certification Authority, signed it.

SSL gets some points for flexibility of security, particularly around digital certificates. IPSEC requires digital certificates at both ends of the connection or none. SSL allows the client the option of digital certificates. Practically speaking, this means that server authentication — the ability for the end-user to know that they're talking to the right server — is always present with SSL.

So, for basic security — and particular implementations not withstanding — IPSEC and SSL are on an equal footing. In practice, asymmetric support of digital certificates gives SSL an edge in flexibility of security.

Deployment Scenarios and Considerations

We will now look at VPN scenarios and deployment considerations, comparing IPSEC and SSL VPNs.

Remote Access

Both SSL and IPSEC VPNs can be used to support remote access users. Users may be connecting from home, hotels, or alternative work sites (for example, an employee working at another company as a contractor). They might be using company-provided computer equipment, a computer the employee owns, or a computer in an Internet café or kiosk.

IPSEC

One thing to consider about IPSEC: its designers did not create it with remote access in mind. It was designed for a world in which PCs have static addresses, and those addresses do not change as the packets pass through Internet gateways. That is not the world we live in. Most

[1] If the reader wants to learn more about cryptography, look at the Bruce Schneier book, referenced at the end of this paper.

[2] A cipher suite is a set of software programs or subroutines to implement cryptography, including cryptographic algorithms for encrypting and decrypting (e.g., IDEA, AES, RC4, RSA, Diffie-Hellman), signature and hash algorithms (e.g. MD5, SHA1), as well as supporting software such as pseudo-random number generators.

[3] Schneier, pp 48-49.

remote users will not have a static IP address, even if connecting from the same place all the time (home, for example). IPSEC is easiest and best suited for a host with known or enterprise-supplied IP addresses. (This is also important for access control, as we shall discuss.)

An IPSEC VPN for remote access requires a client device — a PC, for example — installed with IPSEC software. This is often a special IPSEC client program. Some operating systems may have IPSEC "built in."

The remote PC usually will need add-on client software with a security policy matching the IPSEC policy of the enterprise. This is one of IPSEC's strengths: the ability to make the client-side system very secure. This is also a weakness, making it practically impossible to access the enterprise using kiosks. Using home computers also becomes burdensome, as VPN client software must be added to the home computer, with all the related support and other expenses.

If the remote user is behind a firewall — a home firewall, or a firewall at another site, a customer site for example — IPSEC packets must be allowed to tunnel out through the firewall. In this case, however, it may be difficult to get IPSEC to work, depending on the client software used. The firewall almost certainly implements network address translation (NAT) so that the IP address of the client system and the source address of the packets that arrive from it at the VPN server are different.

From a security standpoint, IPSEC provides top-notch security. It allows tight control over permitted and denied protocols, how often to reissue the keys being used to encrypt all of the packets, the minimum key size, and so on. The downside is it may be impossible to get it to work for remote use. It depends on the particular implementation.

SSL

Using an SSL VPN for clientless remote access from a kiosk or Internet café — in other words, from someone else's computer — the web browser could provide access back to the enterprise network. In this case, the security policy might prescribe that the user could only access limited services. The user, from an unknown location, would use the basic SSL capabilities built in to every web browser, worldwide. Or the access policy could be exactly the same, but the authentication for access might be more stringent, for example requiring a challenge/response or other two-factor authentication. Or, after this strong user authentication, the web server could download a java applet — a specialized and very lightweight client that is available at any PC in the world. This would be the case for a home computer (not enterprise-owned) as well.

Another method of supporting remote access with an SSL VPN is with an add-on client. The client application makes the SSL connections back to the server, authenticates the user, and authenticates the VPN server's certificate. The application can then set up an SSL connection. The server may dictate policy, or the client and server can negotiate. The client software works in conjunction with access control and authentication mechanisms through the SSL VPN server. (The paper discusses both in more detail below.)

Finally, there is no concern about NAT or other addressing issues. Decisions are not made at the packet level. SSL VPNs base security decisions not on the IP address, but rather on the authenticated and established connection.

Authentication

For IPSEC, authentication really means host authentication. For remote access, we are more concerned with user authentication. Some IPSEC

clients allow non-IP address-based authentication using pre-shared secrets, raw public keys, or X.509 certificates. The IETF is developing IPSEC extensions to allow legacy authentication, security tokens, and other one-time password mechanisms. Some IPSEC clients use proprietary additions to do this today.

An SSL VPN can use any of the previously mentioned authentication methods. In a browser-only scenario, personal certificates are possible, and most organizations would use two-factor authentication (such as challenge/response systems) for entry from a less trusted environment.

Access Control

Encrypting a connection and authenticating the user and gateway make the communication channel secure and trusted. Authenticating the user enables the customization of a security policy for that user: where the user can go and what the user can do. VPNs allow access control based on authentication information.

IPSEC

As previously mentioned, many IPSEC VPN servers implement IP packet filtering. Based on the IP source address on the decrypted packets, the filter decides which destination addresses are permitted, for which protocols to which ports. To implement anything more than allowing access to all internal hostnames if the address came from an IPSEC connection requires a lot of address management. So, for example, remotely-connecting software developers would be assigned addresses from one pool, which would allow them — via the packet filter — to get to servers and desktops on the engineering network. Because it is making decisions at the packet-level, the VPN must check every packet against the filter.

Access can be tied to the authenticated user and the policy established between the client and the server. So, for example, if a user connection to the VPN server is from an "in office" wireless access point, the "permitted" list might be longer than if the same user were coming from the Internet.

One down side from a security standpoint is that because IPSEC is a Layer 3 protocol, it is possible for someone else with network access to the client PC to use the IPSEC tunnel to gain access to the protected network. All IP-layer traffic could traverse the connection, even from other systems on the LAN or from an attacking program on the PC itself. If properly configured, the IPSEC VPN would still filter the traffic but everything the legitimate user of the PC could access, an attacker could also access. This is because the connection and the access control are both at the network layer. Once authenticated, the IPSEC VPN server accepts all packets over that connection as from the authenticated user.

SSL

SSL VPN servers can also use packet filtering. But, they can and should also provide firewall functionality at the application level, allowing greater granularity in filtering. Because SSL is connection-based, after the authentication at connection set-up time and the connection is established, the firewall need only check that the packets are part of the established connection. If policy permits, the traffic can be SSL encrypted all the way from the client machine to the back-end server.

It is not practical for someone to launch an attack such as the one described above with IPSEC. The SSL VPN secures the connection at the transport layer. Rather than trusting all IP packets from the client PC, an SSL VPN trusts all packets that are part of the established transaction. An attacker would have to hijack the established TCP transaction in order to use it. This is not possible because SSL operates at the transaction layer and protects the data through encryption, strong authentication, and integrity checks. In the above IPSEC example, an attacker has to have access to

the client computer. With an SSL VPN, the attacker would have to have access to the client process. Further, with IPSEC, the attacker would have to turn the client machine into a router (and, indeed it may already be routing). An attack against the SSL VPN client requires the client computer acting as a proxy server (forwarder), which is harder to do.

SSL VPNs, as with IPSEC, can use different access rules based on where the user is connecting from and what level of access is requested. So, for example, if the user is connected via a web browser with weak cryptography, the policy might allow the user to send e-mail, but nothing else. If the user connects from a web browser with better crypto, the policy might permit sending and receiving. And if it is a remote connection from an approved SSL VPN client, the user might be allowed to "do calendaring" as well as activate a "remote desktop."

Site-to-site

IPSEC is the clear winner here. Implementers of site-to-site VPNs — for example, a VPN connecting remote offices with headquarters — usually want the potential to allow all IP packets, and to propagate packet streams with private addresses from the remote office to headquarters and back. An IPSEC VPN, in tunnel mode, will carry any type of packet from one network to the other over a public network such as the Internet. This allows the greatest flexibility while maintaining high security. Introducing firewall functionality after the IPSEC terminates allows for access control as granular as the firewall allows.

Client Desktop Integration

A special concern with remote PCs is the ability for client software to make security decisions based on the security state of the PC as reported by security-related software, such as antivirus and PC firewalls. Also, VPN client software should protect against covert packet channels, making sure that packets from the untrusted network cannot go through the PC onto the trusted network over the VPN connection. This is usually done in VPN software through "split tunnel" control.

Both SSL and IPSEC VPNs can protect the network in these ways, but not all products do.

Conclusions and Recommendations

For remote access, SSL VPNs are more flexible and easier to deploy while offering as much security as IPSEC VPNs. The user with a PC-installed SSL VPN client can remotely access all policy-permitted and business-required IP applications. With a web-only interface, SSL VPN access to any internal application that can be "webified" is possible, including e-mail, calendar, and file services (for document retrieval). Finally, for a broader range of application access without a client, an SSL VPN can provide web access to Java applets, providing a very lightweight VPN client. SSL VPNs support strong user-level authentication as well as very granular application-level access control through application proxies. They are the best solution for those wanting high security combined with flexibility and very granular access control.

IPSEC VPNs are the best solution for office-to-office secure LANs, especially with trusted and secured applications. Applications cannot make decisions based on running in that secure tunnel, since the IPSEC is "outside" the application and session layers, while SSL is able to communicate to the applications permitting them to take part in making security decisions.

SSL VPNs and IPSEC VPNs have the same level of maturity, acceptance, and use in the world. Though they have different levels of complexity in design and implementation, they both are viable for VPN deployment. Which to use will depend on an enterprise's security policy, business requirements, and the sophistication of its users. Security always strikes a balance with usability. The most secure system may also be an unusable system. Having a choice of technologies allows an enterprise to meet business requirements without sacrificing security.

For Further Reading

Rescorla, Eric, SSL and TLS: *Designing and Building Secure Systems*, Addison-Wesley, 2000, ISBN 0-201-61598-3.

Schneier, Bruce, *Applied Cryptography: Protocol, Algorithms, and Source Code in C, 2nd ed.*, John Wiley & Sons, 1996, ISBN 0-471-11709-9.

Yuan, Ruixi and Strayer, W. Timothy, *Virtual Private Networks: Technologies and Solutions*, Addison-Wesley, 2001, ISBN 0-201-70209-6

Frederick M. Avolio is President of Avolio Consulting, Inc. (http://www.avolio.com), specializing in computer and network security, and dedicated to improving the state of corporate and Internet security through education and testing.

Fred is a respected Internet security expert and has been involved in Internet computing and communication since 1979, working with Internet security systems for over 15 years. He led the team that created the first commercial Internet firewall offering, and helped create the commercial security products division of Trusted Information Systems, enabling a successful public offering and subsequent acquisition by Network Associates.

He is a frequent speaker, teacher, and writer on security related topics. He writes the "Just the Basics" column for INFORMATION SECURITY MAGAZINE. Areas of expertise include firewalls, intrusion detection, cryptography, security management, and electronic mail systems.