IPSec vs. SSL: Why Choose?

Remote VPN Access from Anywhere

An OpenReach Backgrounder Comparing VPN Technologies

OpenReach, Inc.
660 Main Street
Woburn, MA 01801
888.783.0383
www.openreach.com

Overview

Virtual Private Networks (VPNs) allow enterprises to build secure, private communications over public network infrastructures. Several different technologies are used to create VPNs, including Internet Protocol Security (IPSec), Secure Sockets Layer (SSL), and Multi-protocol Label Switching (MPLS). This white paper focuses on the two technologies used to provide remote VPN access for mobile users—IPSec and SSL.

To date, the networking industry has been divided over which technology is the right choice for remote VPN access. This controversy has caused some enterprise customers to delay their adoption of VPN, to avoid making the wrong technology choice. However, when applied appropriately, both IPSec and SSL can be effectively used in an enterprise virtual network. Each technology employs standards-based encryption and authentication techniques that secure access to corporate data over the Internet. Enterprises do not need to choose between IPSec and SSL, rather they can utilize a combination of both methods to meet their security and business needs.

This white paper guides enterprises in selecting the appropriate technology—or a combination of both—for their remote access VPN by answering the following questions:

- *What is IPSec?*
- *What is SSL?*
- *What are the advantages and disadvantages of each?*
- *Which technology should I use to provide remote access for mobile users?*
- *What considerations should I be aware of when designing my remote access VPN?*

What Is IPSec?

IPSec—or Internet Protocol Security—is a suite of protocols that provides security for IP traffic at the network layer. It defines how to provide data integrity, authenticity and confidentiality across a public network like the Internet. It accomplishes these goals through tunneling, encryption and authentication, but allows enterprises to select the specific security policy appropriate for their business. Configuration choices include:

- **Tunneling.** Authentication Header (AH) or Encapsulating Security Payload (ESP)
- **Encryption.** 56-bit DES, 112- or 168-bit 3DES, 128-, 192- or 256-bit AES, or none
- **Authentication.** Username and password (such as RADIUS), username and token + pin (such as RSA SecurID), or X.509 digital certificates (such as Entrust or VeriSign)

But with flexibility also comes complexity. For two entities to communicate via an IPSec connection, both must agree to the same security policy, called a security association, which must be configured in the devices on both ends of the IPSec connection. A single IPSec tunnel secures all communications between the devices, regardless of traffic type (TCP, UDP, SNMP) or application (e-mail, client-server, database). Tunnels can be established from server-to-server and user-to-server. An IPSec server can secure traffic for many devices and is referred to as a *gateway*; an IPSec user (an individual device) is referred to as a *host*.

Because IPSec operates at the network layer, users gain access to all company resources as if they were physically in the office connected to the corporate LAN. Special-purpose software is available to create IPSec connections. This software is typically available for user workstations, PCs and mobile devices, as well as edge routers and firewalls. Some vendors offer special-purpose VPN appliances with the IPSec software integrated.

What Is SSL?

SSL—or Secure Sockets Layer—is a protocol used to secure web-based communications over the Internet at the application layer. It uses encryption and authentication to keep communications private between two devices, which are typically a web server and a user machine. Like IPSec, SSL also provides flexibility in allowing enterprises to define the level of security that best meets their needs. Configuration choices include:

- **Encryption.** 40-bit or 128-bit RC4 encryption
- **Authentication.** Username and password (such as RADIUS), username and token + pin (such as RSA SecurID), or X.509 digital certificates (such as Entrust or VeriSign)

With SSL, each application is secured one at a time, unlike IPSec, which operates independent of the application. To ensure security, each application server must support user access via a web browser and support the SSL protocol. All common browsers such as Internet Explorer and Netscape include SSL support by default, but not all applications do. This requires upgrading existing systems, which can be expensive and time-consuming.

To solve this, some enterprises purchase special-purpose SSL VPN gateways that are deployed at the edge of the corporate network and serve as a proxy (or go between) to LAN applications such as e-mail, file servers and other resources. We browsers connect to the SSL VPN gateway as they would to a web server. The browser thinks it is communicating directly with the application, and the application thinks it is communicating directly with the browser or client software. The SSL VPN gateway makes this transparent to each side of the connection.

To minimize cost, complexity, and maintenance, enterprises need a single VPN gateway that supports both IPSec and SSL forms of remote access. OpenReach is the first VPN provider to combine IPSec and SSL in a single VPN gateway under a unified management architecture.

What Are the Advantages and Disadvantages of Each?

IPSec and SSL are both effective ways to provide secure remote access to corporate resources over the Internet. The two technologies are similar yet different in their approach to VPNs, each having its advantages and disadvantages. The primary differences are:

- Accessibility and Ease-of-Use
- Security
- Management Complexity
- Scalability and Performance
- Cost of Ownership

Accessibility and Ease-of-Use

IPSec VPNs require special-purpose client software for remote user's workstations. Certain operating systems like Microsoft Windows™ include embedded support for the tunneling protocols PPTP and L2TP over IPSec, but not standards-based IPSec. Therefore, VPN providers have developed their own IPSec software clients for Windows-based systems to work with their IPSec gateways. These are usually designed as closed, proprietary systems that are not interoperable with other vendors' products. They also are not commonly available for other operating systems.

Because users can only access the VPN using that specific IPSec client, IPSec VPN access is tied to a specific machine (laptop, desktop) often for a specific user. This can provide stronger security but may limit accessibility and mobility. IPSec clients may also require manual configuration making them somewhat difficult to use for non-technical workers like sales personnel. OpenReach has completely automated VPN client configuration and installation, simplifying set-up for both the IT administrator and the end user.

IPSec's primary advantage is that it operates at the network layer, securing all data between two end points, including all applications. Remote users have access to corporate resources as if they were physically in the office connected to the corporate LAN. This makes IPSec ideal for telecommuters and workers in branch offices. IPSec users can access the following applications:

- E-mail
- File share
- Web (HTTP)
- Client-server
- Databases
- Terminal services

SSL VPNs use standard web browsers like Internet Explorer and Netscape as the remote user's interface. A key advantage is that web browsers are familiar to just about all users and are embedded in every type of user device from PCs to iMACs to PDAs and cell phones, as well as every client operating system from Windows to MAC OS to Linux and Solaris.

Given the universality of web browsers, SSL remote access is extremely mobile in nature. Users can access the corporate network from any browser, whether at a customer site, in an airport lounge, or at a conference. This makes SSL ideal for traveling executives and sales forces. Because there is no special-purpose client software to deploy, enterprises can also use SSL to provide fast and easy extranet access for customers and partners. OpenReach recommends the use of SSL access for casual extranet use, but for permanent or always-on extranet access, OpenReach recommends installing a VPN gateway to create a site-to-site IPSec connection.

SSL's primary disadvantage is that it operates at the application layer, limiting access to only those resources that are browser-accessible or for which the SSL VPN gateway has developed

special-purpose proxy capabilities. Applications accessible using SSL depends on the VPN solution, but common applications include:

- E-mail
- File share
- Web (HTTP)

Security

A major difference between IPSec and SSL is the security protection they provide. In many cases, security is used as the primary criteria for selecting which users and applications should use IPSec versus SSL. Both can play a role in an enterprise virtual network if applied appropriately.

Enterprises should consider two critical security components when comparing IPSec and SSL: encryption and authentication. *Encryption* is used to maintain the privacy of data as it moves across the Internet. *Authentication* guarantees the identity of each device and user, ensuring that people and systems are who they represent themselves to be.

ENCRYPTION

Both IPSec and SSL support the use of encryption but use different encryption algorithms. IPSec typically uses 56-bit DES or 112- or 168-bit Triple DES (3DES) encryption. SSL typically uses 40- or 128-bit RC4 encryption. Each of these cryptographic algorithms is similar in that they ensure data privacy over the Internet, but IPSec provides the stronger (3DES) encryption method.

One common concern among enterprises is how to ensure that remote users adhere to the corporate security policy for encryption strength. This is a standard feature in IPSec VPNs. IPSec accomplishes this because both devices must agree in advance on the security association in order to establish the tunnel between the end points. This is not always a feature of SSL VPNs, however. Some SSL implementations negotiate down to the lowest common denominator (40-bit encryption), and therefore enterprises cannot guarantee the use of strong encryption for their remote users. New, more advanced SSL VPN solutions, like OpenReach, provide the IT administrator with the ability to only allow browsers that support 128-bit encryption, overcoming this potential security weakness.

An important consideration for global enterprises is exportation of strong encryption algorithms like 3DES. Check with your VPN provider to ensure that they are approved by the U.S. government to export security technology. OpenReach is authorized to export strong encryption.

AUTHENTICATION

Like encryption, both IPSec and SSL support authentication to ensure validity of each end point. Yet unlike encryption, the authentication techniques can be the same for both access types. Supported authentication technologies are largely dependent on the VPN provider, but both IPSec and SSL can employ username and password (such as RADIUS), username and token + pin (such as RSA SecurID®), or X.509 digital certificates (such as Entrust® or VeriSign®). Digital certificate support can vary from using a certificate only on the server (VPN gateway) to both the client machine (user's PC) and the server.

Although both IPSec and SSL can use the same authentication technologies, SSL provides an inferior implementation of authentication than IPSec. This is largely due to the fact that IPSec requires a specific piece of client software be installed on a specific machine to access the network, whereas SSL users can potentially gain access from any device with a web browser. To overcome this security hole, enterprises can utilize two-factor authentication technologies like RSA SecurID, which combines something you know (password) with something you have (token). This approach guarantees the identity of the user, not the machine. Another option is using a

digital certificate on a smart card, but this requires access from machines that support smart card readers, which are still limited in deployment.

Enterprises that choose to use digital certificates should understand that the most secure implementation is when both server- and client-side certificates are used. This is true for both IPSec and SSL. However, with SSL, browsers are often configured to prompt the user whether or not they will accept the certificate being presented by the VPN gateway as authentic. This is not the case with IPSec software, since IPSec clients are proprietary to the VPN vendor and are configured to know which server-side certificates to accept.

A disadvantage to SSL is that authentication requires the end-user to verify that the certificate being presented by the server is correctly representing the server's identity. There is risk that an imposter will successfully fool the user into accepting a bogus certificate, thus creating a secure communications channel with a hacker and exposing the corporate network to what's known as a "man-in-the-middle" attack. Enterprises should consider this risk when selecting SSL.

The OpenReach Service provides a fully managed pubic key infrastructure (PKI) that automates creation, distribution, maintenance, and revocation of digital certificates for all users and VPN gateways. OpenReach IPSec access provides both client- and server-side certificates. OpenReach SSL access currently provides server-side certificates only, but will support client-side certificates in a future release. Today, OpenReach SSL access supports two-factor authentication using RSA SecurID, to ensure the identity of the remote user.

OTHER SECURITY ISSUES

A key advantage of SSL is its accessibility and device independence—users can access the corporate network from any browser on any workstation in any location connected to the Internet. But some view this ubiquity as a security threat in that users may be accessing the VPN from unknown machines. There is risk that corporate data cached in the computer's memory can be accessed by the next individual using that machine, or that stored cookies could provide information about the user's identity that could later be used to break into the corporate network.

Newer, more advanced implementations of SSL VPNs, including the OpenReach remote access solution, overcome these potential security holes through session management techniques. IT administrators can configure parameters, such as user inactivity time-out, to ensure the SSL session is dropped if the user walks away from the machine. OpenReach also removes cookies and cached content to "clean up" the workstation after the secure session is over.

Note that one security risk cannot be mitigated. Public machines like Internet kiosks are inherently insecure because they are operated by an unknown (un-trusted) third party and are placed in uncontrolled environments. For this reason, kiosks are subject to key stroke capture, a common technique of hackers. This risk is most prevalent in public locations such as airports and conferences. For this reason, enterprises may choose to limit the applications accessible over SSL to non-sensitive corporate data or may choose to lock down access from specific devices identifying themselves with a device-resident digital certificate.

Management Complexity

While IPSec is considered more secure than SSL, IPSec VPNs can be more complicated to deploy and manage. This is because IPSec requires special-purpose VPN client software, whereas SSL VPNs are browser-based. Another reason is that IPSec requires configuration of many networking parameters and security policies to create an end-to-end VPN tunnel.

Deploying an IPSec-based VPN involves several steps, the first of which is distribution of IPSec client software to all remote users. Although OpenReach has automated this critical step, few VPN solutions on the market today have followed suit. Most require IT administrators to burn CDs and mail them to users. Another common approach is to make the software downloadable from a

LAN-based server, although this will not work for telecommuters who may never be present in the office and thus can't access the LAN without first getting the VPN client software.

Once users have received the IPSec software, they must successfully install it on their PC. This step alone is often the greatest cause for help desk calls, because the installation may be complicated or not succeed due to incompatibility issues. This is especially true when the IPSec software is being installed on a PC that is not owned or controlled by the enterprise, as is typical when trying to connect customers, partners and suppliers to an extranet. Many IT administrators take installation into their own hands by installing the client image themselves, usually when PCs come in for repair or maintenance or when new laptops are issued. This approach not only is labor intensive, it also greatly slows down VPN deployment.

OpenReach automates IPSec client deployment by e-mailing users simple instructions for downloading the IPSec software and enrolling in the VPN. In addition, OpenReach provides a fully configured IPSec software client that automatically installs on a user's PC without requiring complicated set up.

SSL VPNs are often referred to as "client-less" because they work with existing software embedded in user operating systems, although they do require technology on the server side that can accept SSL sessions. This saves enterprises significant deployment cost and headache. IT administrators can enroll users in the VPN "on the fly" by simply enabling their username and password and providing them with the URL of the VPN gateway. In addition, SSL VPNs provide enterprises with additional savings through reduced help desk support costs. With SSL, users are typically connected trouble free.

IPSec can also be more complex than SSL because most IPSec VPN products require IT administrators to become experts in tunneling and encryption technology by requiring manual configuration of security associations. Making decisions on IPSec configuration parameters (like rekeying intervals and perfect forward secrecy) can be daunting to even the most security-savvy IT manager. Because IPSec manual configuration is so complex, many IT managers rush through by accepting the defaults, which significantly reduces the security of the network. Others make incorrect choices or configuration mistakes that open up security holes in the network perimeter.

OpenReach eliminates many of the management headaches common in traditional IPSec VPN products. To create a VPN connection, IT managers simply point-and-click between two location icons on the OpenReach Interlock Manager GUI. The OpenReach Network Operations Center (NOC) then configures all security association parameters to create the IPSec tunnel. OpenReach also replicates all policy changes throughout the network instantaneously, eliminating the operational burden found in other VPN solutions.

Scalability and Performance

SSL VPNs are scalable in that they can be quickly deployed to remote users regardless of machine or location, but IPSec is more scalable in terms of its transparency to the network. From the user and application perspectives, the secure network (once established) is indistinguishable from a trusted LAN. Existing network-accessible applications can be used through the VPN without modification. Changes to the applications are independent of changes in the VPN.

SSL VPNs require tight integration with the application, as it becomes the interface to the user. Additions or changes to the applications require commensurate changes to the web front end.

Additionally, not all applications are suitable for use through a web browser. For example, the stateless nature of HTTP makes session-oriented applications difficult to integrate and can provide poor performance. Conversely, e-mail and file-sharing applications are well suited to SSL access and offer users comparable performance levels to when they are in the office.

Cost of Ownership

SSL and IPSec VPNs are comparable in terms of capital outlay. Both require VPN-capable servers at the corporate site to terminate remote user sessions. But because SSL VPNs do not require client software and can be less of a deployment and management burden, their total cost of ownership is usually less. However, to date, enterprises that want to take advantage of both SSL and IPSec have needed to purchase and maintain separate systems, significantly increasing the overall cost of VPN. OpenReach is the first provider to combine IPSec and SSL in a single solution, providing a flexible and cost-effective remote access service for enterprises.

Which Technology Should I Use to Provide Remote Access for Mobile Users?

IPSec and SSL can both be used in an enterprise virtual network when applied appropriately. Each has its strengths and weaknesses that make the technology better suited to some remote access users and applications than others. Table 1 summarizes the differences between SSL- and IPSec-based VPNs.

	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

Table 1. SSL vs. IPSec VPNs

In general, IPSec is best suited to users that require access to all applications and resources as if they were physically connected to the corporate LAN. IPSec also supports stronger encryption strengths (3DES, AES) and guarantees the identity of the remote user because it requires the use of specially provisioned IPSec client software. While IPSec may take longer to deploy, as a system it is more scalable because it operates independent of the applications.

In general, SSL is best suited to users that need casual or mobile access to applications like e-mail and file sharing. It is also ideal for extranet applications because SSL-enabled browsers are prevalent and can be used to quickly and easily connect customers, partners and suppliers.

However, for permanent or always-on extranet connections between offices, IPSec VPN gateways are recommended.

Most users can benefit from both types of access under different circumstances. For example, enterprises may provide remote workers with IPSec client software when telecommuting, but permit SSL access when visiting a customer or attending a tradeshow. To effectively manage both types of access, it is critical to join IPSec and SSL in a unified management architecture. OpenReach allows enterprises to provision users with IPSec, SSL or both, and provides the application-level policy control to meet an organization's security and business needs.

What Considerations Should I Be Aware of When Designing My Remote Access VPN?

When designing a remote access VPN, enterprises should consider:

- Business need
- Security requirements
- Resources and expertise
- Time
- Budget

Enterprises must balance their business needs with their requirements for a secure network. Many enterprises quickly jump to select IPSec VPNs without considering whether IPSec is actually too much security (and overhead) for their needs. For example, the strong data encryption and user authentication technologies provided by SSL may be sufficient for the sales team and corporate executives that need to read e-mail or download presentations when they travel. On the other hand, IPSec may be required for engineers that telecommute and need access to client-server applications, finance and HR personnel who require access to sensitive corporate data, or for nurses and doctors that access patient records from a branch office clinic.

Enterprises also should take stock of available resources and in-house expertise, especially given the often complex and time-consuming process of deploying and management a remote access VPN. Depending on your vendor, both IPSec and SSL VPNs can be major projects. Service providers like OpenReach can significantly reduce the operational burden of a VPN by managing the entire VPN infrastructure, including VPN gateways, client software, public key infrastructure, monitoring and reporting.

Finally, the time it takes to deploy a remote access VPN is dependent on whether an enterprise requires IPSec, because of the need to provision special-purpose IPSec client software. Some enterprises may benefit from first deploying SSL for basic e-mail, file sharing and intranet access, to quickly meet users' needs for access while IPSec is rolled out. This can be a more expensive solution in the end if the enterprise is forced to purchase two distinct systems for IPSec and SSL.

OpenReach offers the benefit of a combined IPSec and SSL solution in a single VPN gateway under a unified management architecture. This provides enterprises the flexibility to use both technologies as needed, rather than making a technology selection up front when deploying a remote access solution.

Conclusions

IPSec and SSL are both effective, standards-based technologies to use when deploying remote access VPNs. Each technology has its advantages and disadvantages as well as strengths and weaknesses. Factors to consider include application and user accessibility, ease of use for non-technical workers, encryption and authentication security, deployment and management complexity, scalability and performance, and total cost of ownership.

Enterprises can benefit from using both IPSec and SSL in their virtual networks when applying each technology appropriately. The primary factors to consider are who the remote users are and what they need to access. This must be balanced with the sensitivity of their communications and the impact on the business should the data be compromised.

When deploying a remote access VPN, enterprises should determine the resources required to effectively deploy and maintain a virtual network, and if no in-house expertise exists, should consider using a service provider like OpenReach to manage their network.

About OpenReach, Inc.

With customers in 40 states and 28 countries, OpenReach provides network overlay services that augment or replace existing data networks (frame relay, ATM and leased line) to extend coverage, increase capacity, and reduce operational expense.

With ten patents pending in its Interlock Capability Suite, OpenReach's fluid networks shape effortlessly to the needs of changing businesses, unlike carrier services and standalone products that force companies to adapt their business to the constraints of their communication networks.

Learn more about OpenReach at http://www.openreach.com.

