

FEATURE

SSL VERSUS IPSEC - CHOOSING YOUR VPN

by Ian Kilpatrick, director of business development, Wick Hill Group

Summary of feature

- * Now a choice between SSL and IPsec VPNs
- * Key differentiators between the two
- * IPsec - built-in authentication through certificates and the option of different encryption levels. Greater security and more flexible but more complex to manage and typically more costly.
- * SSL VPNs - no client software making so more cost-effective and easier to manage. Only one encryption option. Security can be enhanced by incorporating third party authentication.
- * SSL strengths and weaknesses
- * IPsec Strengths and weaknesses

Other factors in choosing right VPN

- Strength of encryption technology used by both types of VPN
 - The type of application
 - Sensitivity of the data
 - Type of user base
 - Location of user base
 - Size of user base
 - Cost factors
 - User access to browsers
 - Whether you have multiple sites
 - Whether it's a business to business or business/organisation to consumer situation
 - Whether IT has access to and control of user devices.
- * Which types of applications are suited to which VPN, with examples.
 - * Future developments

FEATURE

Initially, the only VPN (virtual private network) technology available for securing confidential data in transit between two points was the IPsec VPN standard. In 1999, however, a serious challenger emerged based on SSL (Secure Socket Layer), a capability standard in all browsers.

Companies now have a choice of which VPN to use. But which is best for their particular requirements? This article attempts to balance the arguments for and against each option, looking at them from both a technical and business viewpoint. It assumes the reader is familiar with the basic concepts of the two technologies.

Early implementations of SSL VPN technology had numerous technical limitations or issues to overcome e.g. translation of URLs embedded in Java, user account information not being cleared down from the browser after user sessions, point-to-point tunnelling, no support for dynamic port assignment, support only for web-enabled applications.

However, all of these, and other concerns, have been addressed in later releases. The ultimate goal of SSL VPN technology is to allow controlled and managed access to any application, from any device and from any location. IPsec VPN technology has been established much longer and has its own strengths and weaknesses.

The key differentiator at the moment between the two is that IPsec VPNs have built-in authentication through certificates and the option of different encryption levels. This delivers a higher degree of security but makes them more complex to manage, and typically more costly. SSL VPNs have no client software making them more cost-effective and easier to manage, but they have only one encryption option. Security can be enhanced by incorporating third party authentication.

SSL Strengths

1. No client software required for accessing web-enabled applications

Benefit: low-cost. Deployment, management and administration extremely simple and effective

2. SSL is a de-facto standard

Benefit: interoperability between different vendors and applications

3. Included as default in Microsoft and Netscape web browsers

Benefit: no client software costs

4. As commonly deployed, only servers require digital certificates to establish the encrypted session

Benefit: enormous reduction in the requirement to manage certificates

SSL Weaknesses

1. User authentication not built in. This is a major security weakness.

Answer: integration with 3rd party strong authentication products such as VASCO

2. Requires Java or ActiveX downloads to facilitate access to non-web enabled applications

Answer: download is transparent to user. Depending on implementation and network topology, this may cause a problem if the firewall (whether on the server side or on a personal firewall) is set to block Java or ActiveX controls.

3. SSL Tunnelling (basically mimics IPSec) is not supported on Linux or non-Windows OS.

Answer: True - SSL vendors offering SSL Tunnelling as an option utilise the virtual adapter technology within Windows OS to encapsulate traffic, which is not currently available in other operating systems.

4. SSL is processor-intensive leading to poor performance under high loads

Answer: True but can be addressed by clustering, load-balancing multiple appliances, by utilising SSL accelerators such as Radware's CertainT 100 or using traffic prioritisation products such as Allot's NetEnforcer or high performance accelerated SSLs such as those from Array Networks.

5. Some enterprises need broader application support than SSL provides

Answer: SSL vendors are addressing this by enhancing proxy support and supporting port redirection.

IPSec Strengths

1. No restrictions on applications run through a tunnel and no need to define the applications that are available.

Benefit: wider applicability

2. Included in IPv6 client

Benefit: reduced costs compared to current client-side requirement but requires widespread adoption of IPv6. This is some way off as IPv6 is still work in progress.

3. Stronger end-point security and built in authentication (via certificate)

Benefit: no requirement for 3rd party authentication

IPSec Weaknesses

1. Lack of standards between different IPSec vendors can create problems for the IT department tasked with setting up a VPN that involves integrating different vendors.

Answer: IPv6 will overcome this limitation

2. IPSec VPN does not always offer easy solutions to complex remote access situations involving network address translation (NAT) or firewall traversal.

Answer: True

3. Some residential broadband services have started blocking IPsec traffic from home users unless that customer pays more expensive business rates.

Answer: IPv6 may force service providers to remove this additional cost

4. IPSec VPNs generate higher demands on support desks than SSL VPNs.

Answer: accepted, but IPv6 should reduce this overhead.

5. High management overheads and costs in supporting certificates, software and users.

Answer: True, but should reduce if IPv6 is widely adopted. Even so, unlikely to match SSL in ease of implementation and management.

Other considerations

Another consideration for the purists is the strength of the encryption technology. SSL uses single DES (128-bit key), IPSec can use 3DES or the emerging AES standard. For the majority of applications and requirements, DES is adequate. However, for highly secure requirements such as military, 3DES/AES is probably mandated. Browser vendors would have to move to supporting 3DES or AES before SSL VPNs could match the encryption strength of IPSec.

In deciding which type of VPN to use, it comes down to the application, the sensitivity of the data, the type of audience, the location of the audience, the size of the audience and the cost. It's also quite possible to run both types of VPNs on the same network for different applications. This is quite a common scenario in larger organisations.

There are a number of factors to consider, such as whether users have access to browsers. If they don't, then SSL VPNs are not possible. How big is the potential user base? The number of people in your user base is an important factor. The larger the user base, the more you should be leaning towards SSL because it will be cheaper, easier to maintain and easier to manage.

The location of users is a further factor. If you have members of the public dialling in from many different locations, that mitigates towards SSL VPNs, partly because of the numbers and partly because with IPsec, the end users would require client software and would not be familiar with dealing with authentication certificates.

Typically, organisations have used IPsec for multiple sites. This is for a variety of reasons. Primarily it's because most SSL solutions don't support site-to-site, but also because, when there are a limited number of connected sites, IPsec benefits significantly exceed any complexity issues.

Additionally, with site-to-site, the ease of accessing multiple applications without pre-configuration is also important. IPsec is better for this. However there are now SSL solutions from suppliers such as Array Networks that can deliver site-to-site, so this benefit of IPsec may diminish over time.

An important issue is whether you are dealing with a business-to-business or a consumer situation. IPsec involves the management of authentication certificates, which consumers would normally not be familiar with. As a broad generalisation, consumer applications will tend towards SSL VPNs, whereas business applications could use either.

Is the IT department allowed access to and control of user devices? If you are using an IPsec VPN, then you have to be able to manage the client on the user's device. If you can't get that control, then you may want to use SSL VPNs. If NAT (Network Address Translation) is used at the server end, SSL again might be preferable as IPsec requires specific configuration if NAT is used, although IPv6 is meant to come up with a solution to this.

Cost is another very important consideration. Management of authentication certificates can be very time-consuming and is not necessary with SSL VPNs. This makes SSL VPNs much cheaper and this factor alone may be a key decider.

Some applications are obviously suited to one type of VPN or the other. With Internet banking, for example, management could be very costly and difficult if a large number of customers had to deal with the client software used by IPsec VPNs. A combination of SSL VPNs and strong authentication from companies such as VASCO or Cryptocard would provide a cost effective, easy-to-use and secure solution. However, if you were doing financial transfers in a corporate situation from point to point, you may well prefer the extra security of IPsec VPNs.

If you were a doctor out on call and wanted to refer back to medical records in the practice, IPsec may be the preferred option. This is because, even though the location is potentially anywhere, the nature of the data being accessed and transmitted over the Internet is highly sensitive and confidential, so it requires authentication. The number of users is likely to be small, making administration and management easier and the user's access mechanism (laptop) will be a known, controlled and accessible item.

If you are a warehouse-style retail shopping outlet, and you want your customers to have access to stock information, you might veer towards SSL VPNs because of the large numbers, the diverse locations and the costs of managing these. If you were a distributor making pricing information available to a limited number of business partners, you might go for IPsec because of the commercially sensitive nature of the information.

Conclusion

SSL technology is rapidly maturing to the point where there are few clear differences between the options. SSL is gaining the upper hand - but it remains to be seen what difference the introduction of the IPv6 standard, which includes IPsec, will make. All IPv6 end node implementations will include IPsec as an option, so IPsec advocates hope for a

resurgence of IPsec VPNs. If all applications used this IPsec feature, then theoretically SSL would be unnecessary.

Vendors are looking at delivering hybrid SSL/IPsec solutions which address both requirements - this could give users the best of both worlds.

However, the perceived wisdom is that, in the future, IPsec will probably be used principally for site-to-site communications, rather than individual client remote access. SSL VPNs will become the dominant and preferred solution for remote access to applications, whether web-enabled or not.

Suppliers of IPsec and SSL VPNs.

Array Networks

Array Networks makes high performance SSL VPNs. The company offers a suite of integrated products that address the issues relating to deploying applications and web content to a large number of mobile and globally dispersed users. Array's SPX Series is the world's highest performing SSL VPN secure access system. Array also has what is claimed to be the world's first SSL for site-to-site connectivity. www.arraynetworks.net

WatchGuard Technologies

WatchGuard is a market leader in security appliances and has supplied systems to tens of thousands of small-medium sized businesses around the world. The company's range of integrated security solutions includes both SSL and IPsec VPN options.

www.watchguard.com

Acknowledgements/Sources - Aventail, Burton Group Report on The Changing Face of SSL-based Remote Access, WatchGuard, Netilla, VASCO, Radware, Array Networks, NetASQ, Check Point.

Further reading options on IPsec

<http://search.barnesandnoble.com/booksearch/results.asp?WRD=ipsec>

IPsec Working Group <http://www.ietf.org/html.charters/ipsec-charter.html>

Bio - Ian Kilpatrick

Ian Kilpatrick is chairman of Wick Hill Group plc, specialists in secure infrastructure solutions for ebusiness. Kilpatrick has been involved with the Group for over 30 years. Wick Hill is an international organisation supplying most of the Time Top 1000 companies through a network of accredited resellers.

Kilpatrick has an in-depth experience of computing with a strong vision of the future in IT. He looks at computing from a business point-of-view and his approach reflects his philosophy that business benefits and ease-of-use are key factors in IT. He has had numerous articles published in the UK and overseas press, as well as being a regular speaker at IT exhibitions.

For further press information please contact Annabelle Brown on 0191 252 8548, email abpublicrelations@btinternet.com. For reader queries please contact Wick Hill on 01483 227600, email info@wickhill.co.uk, web www.wickhill.com