

FEATURE

THE RISE OF SSL VPNS

by Ian Kilpatrick, chairman Wick Hill Group

1300 words

Summary of feature

- * Recent growth of SSL VPNs
- * Aim of VPN technology - controlled, secure and managed access to any application, from any device and from any location.
- * Integrated authentication
- * Inclusion of client integrity
- * Fewer security issues with SSL
- * SSL VPNs ADVANTAGES
- * SSL VPN Disadvantages
- * Cost considerations and benefits
- * How do you choose a VPN?

FEATURE

The growth of Secure Sockets Layer virtual private networks (SSL VPNs) has accelerated in the last 12 months due to greater awareness among users of the commercial advantages, better marketing which focuses on benefits rather than technology, and improved security features.

The ultimate goal of SSL VPN technology is to allow controlled, secure and managed access to any application, from any device and from any location. Early implementations had some limitations such as user account information not being cleared down from the browser after user sessions, no support for dynamic port assignment, support only for web-enabled applications, and no strong authentication of the user or the access device.

All of these, and other concerns, have been addressed as SSL technology has matured. Recent enhancements, for example, include the integration of user authentication. Many SSL VPN vendors offer, or are planning to offer, integrated third party strong authentication products such as those from VASCO and RSA. Netilla, from AEP Networks, and FirePass, from F5, both natively embed VASCO user authentication with their SSL VPN offerings.



The addition of 'client integrity' is another significant step forward for SSL VPNs. Client integrity involves the scanning of the client access device to check for trojans, viruses, etc. and scanning to check if the device has the latest Microsoft security patches installed. This checking ensures that the device is 'safe' and traffic from the device can be passed to the server side. Aventail, through their integration with Check Point's Zonelabs personal firewall, and Array Networks are two SSL VPNs which have implemented this feature.

An SSL appliance would normally sit behind the firewall taking all traffic from Port 443. Some SSL appliances have built-in firewalls that specifically protect the SSL device and can therefore sit in front of the firewall. Putting an SSL appliance in front of the firewall, without its own protection, leaves it open to potential hackers. As no client-side software is required, user security issues relate primarily to authentication and access security.

As a result of the growth in popularity of SSL VPNs, many manufacturers are jumping on the bandwagon and releasing their own products. Early technology evangelists were Netilla from AEP Networks, Neoteris from Juniper, and Aventail. These were followed by many other vendors including Check Point, Whale Communications, NetScaler, Array Networks and Nokia, who all offer SSL solutions. To date, there are some 70 different vendors providing an SSL product, with many more in the pipeline.

Continued...

Benefits of SSL VPNs

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

Benefit: 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 a number of 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 VPN Disadvantages

1. Optional (as opposed to in-built) user authentication. 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: This can be true, but can be addressed by clustering, load-balancing multiple appliances, by utilising SSL accelerators such as Radware's CertainT 100 or by traffic prioritisation technologies such as Allot's NetEnforcer, or by using high performance SSL appliances such as those from Array Networks.

5. Some enterprises need broader application support than SSL provides

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

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 issue when deciding whether to use SSL or IPsec VPNs. Unlike most IPsec environments, you do not need paid-for client software. Additionally, set-up and management is typically much easier.

Choosing a VPN

There are a number of factors to consider when choosing an SSL VPN. What applications do you want to use it for and how many users are there. For small numbers of users connecting to a small number of applications, ease of use and management are key considerations. Suppliers such as Array Networks and NetASQ have low cost solutions designed for SMBs and distributed enterprises.

Other considerations include: Does it have an integrated firewall? The inclusion of this will give maximum flexibility of implementation and granularity. Does it include integrated strong authentication or does it provide scalability and interoperability with third party strong authentication products?

Can the SSL VPN provide client integrity, i.e. checking the client machine for security threats? Will it support legacy and web applications, and does it provide support for SSL tunnelling, which mimics IPsec. You also need to be sure that it will support any device (PC, lap-top, PDA, Internet Cafe device) to which the SSL owner does not have access rights. As with any VPN system, you will need comprehensive reporting that helps you keep track of VPN tunnels throughout your organisation.

Then there are vendor related issues to consider. You should check the vendor and distribution/reseller support infrastructure. Do you need next business day replacement and 24x7 telephone support? If your SSL VPNs (as is likely) are an essential part of your business operations, you want to be sure that you can replace any problematic systems very quickly and that help is always available to keep the VPNs functioning well. It would also be wise to check out the vendor's plans for enhancing the product's functionality and capability, to ensure that it will keep up to date with your changing needs.

Other considerations

Another consideration for the purists is the strength of the encryption technology. SSL uses single DES (56-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.

Continued...

Conclusion

Vendors of both IPsec and SSL VPN technologies have recognised the strengths of each other's solutions and introducing hybrid products. For instance, Check Point offers Connectra, an SSL product, as well as its long-established SecureRemote IPsec product. NetASQ has an integrated firewall/ IPsec VPN/SSL VPN appliance.

SSL technology is rapidly maturing to the point where there are few clear differences between SSL and IPsec technology. SSL is gaining the upper hand if you count the number of users, 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 feature, then theoretically SSL would be unnecessary. But by then SSL may have become the dominant technology.

A recent report from Forrester Research indicates that SSL will take over. It concluded that spending on SSL VPN technology will increase at a 53% compound annual growth rate and that by 2008 SSL VPNs will have overtaken traditional IPsec VPNs as the remote access security standard.

ENDS

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, www.wickhill.com

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 and is the moving force behind its dynamic growth. 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.

About Wick Hill www.wickhill.com

Established in 1976, VAD (value added distributor) Wick Hill specialises in secure infrastructure solutions. The company's portfolio covers security, performance, access, services and management. Wick Hill sources and delivers best-of-breed, easy-to-use solutions through its channel partners, providing customer support, implementation, training and technical services.

ENDS

April 07