SSL VPN In Detail

networknewz.com/networknewz-10-20031201SSLVPNinDetail.html

By **Waheed Warden, MCIM**
Expert Author
Article Date: 2003-12-01

2.1 Benefits
As with any security technology, SSL VPN will have to demonstrate tangible business benefit before it will even be considered. The current benefits of SSL VPN were briefly outlined in section 1.2.2, but are discussed in greater detailed below.

- Cost saving - Because SSL VPNs can be clientless, the cost of deploying clients is saved. For a typical VPN deployment of just 100 users, Netilla estimate the cost of client support for SSL VPN is just $125 per user, rather than 313 for a Cisco IPSec client. This is based on 2 hours support per year for an IPSec based client user and just 30 minutes for a clientless user. These figures may be questionable, but some costs savings will always be apparent.

- Platform independent - Access can be granted from many types of machine (Linux, Windows 2K/XP, Apple Mac, Palm OS, Symbian, Pocket PC). Although VPN client platforms are available for most common operating systems, very few vendors produce these clients in parallel (E.g. The Apple Mac and Linux clients always appear six months behind the Windows ones).

- Client type mobility - Although IPSec clients can grant access across most mediums (Leased line, DSL, Dial, GPRS) they only offer access from the corporate desktop on which the client is installed. SSL VPNs can be configured to allow access from corporate build laptops, home desktops, customer or supplier desktops or any machine in an Internet caf. This extra choice allows a much wider audience (I.e. non laptop users) to boost productivity and work whilst at home or travelling.

- Client IP mobility - Although widespread deployment is yet to take hold, mobile IP network deployment is growing steadily. A side effect of a mobile IP network is that the client source address can change as a client moves between cells and networks. This has the effect of breaking an IPSec VPN connection, but because SSL VPNs are not bound to the source IP address, connections can be maintained as clients move.

- No NAT issues - Traditionally Hide Network Address Translation (Hide NAT) has caused issues with IPSec VPNs. Vendors have generally overcome these issues by developing vendor specific NAT traversal mechanisms based on payload encapsulation in UDP packets. Although these mechanisms normally function well, they break and interoperability between vendors deployments. SSL VPNs do not suffer such issues because they are not tied to the IP layer.

- Granular access control - Although IPSec VPNs also offer highly granular access control (by machine and service), SSL VPNs can offer a greater granularity, even as far as URL. SSL VPNs also lend themselves to more granular access control because each resource accessed must be explicitly defined. This differs from IPSec VPN because entire corporate networks can be defined with a single statement.

- Restrictive firewall rules - As a consultant working from customer sites, access back to your corporate resources is normally very restrictive. This is because those organisations with a reasonable security infrastructure will employ a firewall rule set which limits outbound access to only those services key to business profitability. Your IPSec VPN connection is unlikely to count as a core business function. Once key advantage of SSL based VPNs is that they tend to communicate on the port used for Secure HTTP (TCP port 443), which is one of the few ports allowed outbound access form any machine in the corporate network in most environments. Even in situations where proxy cache servers are deployed, because HTTPS traffic is encrypted, they will normally pass this traffic un-inspected.

2.2 How do they work?

As stated above in figure 2, SSL VPNs make use of the existing SSL functionality already present in most IP Stacks. Because SSL fits into the stack between layers 4 and 5, each application must explicitly define its use. Based on this fact, SSL VPNs fall into 3 distinct categories:

- Application layer proxies
- Protocol redirectors
- Remote control enhancers

Most commercial SSL VPN products will use a combination of the above techniques, although some insist that only one of these techniques offers a complete solution. Each of the techniques is covered in detail below.

2.2.1 Application layer proxies

Application layer proxies are the simplest form of SSL VPNs because they rely on the SSL functionality used by existing applications. Because of this, application layer proxies have the least application support. Generally, they only support

- Email
- Web based traffic

However, to provide additional functionality over and above this they do tend to web enable' greater functionality, such as file transfer. Even with this, functionality tends to be limited.

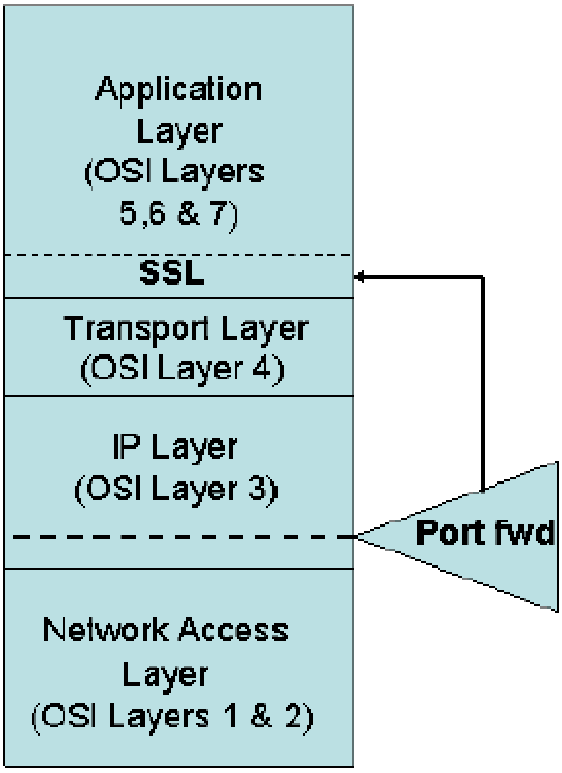
They work by using the SSL setup in existing applications, for example, you would web browse to the gateway which then proxies web traffic internally (using a simple method to display links to internal systems). To use email, your administrators would configure the SSL functionality in your email client and proxy all email traffic via the gateway.

One of the advantages of application layer proxies are that they are truly clientless. They operate with nearly all operating systems and web browsers.

2.2.2 Protocol redirectors

Protocol redirectors have more flexible than application layer proxies, but they are not truly clientless in their operation. Protocol redirectors work by downloading a mini client from the gateway, which installs locally and redirects traffic. The redirection is illustrated in figure 3 below.

Figure 3


Application Layer (OSI Layers 5,6 & 7)
SSL
Transport Layer (OSI Layer 4)
IP Layer (OSI Layer 3)
Port fwd
Network Access Layer (OSI Layers 1 & 2)

For example, if a connection is made from an application, which does not use the SSL layer, the connection is captured at the base of the IP layer and then encapsulated within an SSL tunnel. Once the traffic reaches the SSL gateway, it is decrypted and then proxied to the original destination. This would appear to be an ideal mechanism, because all normal applications work with minimal intervention for the user. The reality though is slightly different.

The only realistic way the shim can capture the traffic on the way through the IP stack is to redirect traffic based on name resolution to a local resource. For example, I may try to connect to mail.trinitysecuirty.com, which normally connects to 9.180.214.10. Once the port redirector is enabled, the name mail.trinitysecurity.com will be forced to connect to localhost (127.0.0.1) through the use of a host file. This means the mini client must have the ability to write changes to the hosts file, which in a hardened corporate desktop may not always be possible. Also, in most implementations some administrative permission is required on the local desktop to install the mini client, which is rarely possible using a machine in an Internet Caf.

The main advantage of the protocol redirection system is that it can support any application that works on fixed TCP or UDP ports and in some implementations, applications with dynamic port applications can be supported (such as MS Outlook).

2.2.3 Remote control enhancers

Remote control enhancers are the most flexible form of SSL based VPN, but they also have the highest overhead. They work by enhancing a remote control protocol like Windows Terminal Services or Citrix Metaframe and adding SSL VPN functionality and Web Browser support. This means any application can be added to the SSL VPN by adding the application to the remote control desktop. As a stand-alone application, this has serious limitations, because applications that reside on the local desktop cannot be used directly. This is why most remote control enhancers are partnered with other SSL VPN technologies.
On the positive side though, they can offer features like the ability to read and update a documents held centrally without ever having to download the entire document. When travelling and using VPN over low speed connections, or when connection quality is poor this could be very advantages (because connections are restarted without loosing any work).

2.2.4 Technical considerations

Other technical considerations include

- Performance - Any system for enterprise deployment must be able to scale to meet the demands of the large volume of users it is required to service. Most SSL VPNs are shipped as appliances, and with models which scale to 1000 concurrent users available, performance should be adequate.

- High Availability - Once again, for enterprise deployment, high availability and failover is key. Most vendors (especially the ones with more mature products) are able to perform some form of internal HA / failover mechanisms.

- Network performance - As many vendors push the mobility aspect of SSL VPNs, you would expect that performance over a low speed link (GSM data or GPRS) to be good. Looking into this slightly deeper, it can be seen that SSL VPNs can offer some performance advantages over IPSec VPNs. Ignoring the setup operations, which can be considered "one time" for a relatively short lived connection, the overhead of IPSec on a packet is between 50 and 57 octets (including the new IP header, the ESP header and the trailers), representing a 10% increase on an average packet (500 byte). In contrast to this, SSL VPNs add only 5 octets of data to each packet, just a 1% increase on the average packet. Of course, setup operations cannot be ignored totally, but these are roughly similar in size for IPSec and SSL connections. Also, because SSL VPNs work at a much higher layer, they suffer much less from the packet fragmentation issues normally associated with IPSec VPNs. Finally, SSL has built in compression mechanisms.

Click here to read part 1 of this article.

Click here to read part 3 of this article.

About the Author:

Waheed Warden, MCIM, Channel Marketing Manager, Trinity Security Services
Waheed.Warden@trinitysecurity.com
http://www.trinitysecurity.com
M +44 (0) 7879 647 497
T +44 (0) 870 350 1284
F +44 (0) 845 280 2712

We don't compromise on your security
