An Intro To SSL VPN

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

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

1.1 Introduction

In recent years, Virtual Private Networks have become the de facto standard for secure remote access. They enable teleworkers, day extenders and business partners access to corporate network resources across un-trusted networks. Typically, the untrusted network will be the Internet, but VPNs offer excellent flexibility and can also be used across more traditional network mediums such as frame relay or ATM networks. VPNs guarantee the confidentiality and integrity of corporate data through the use of strong encryption and authentication techniques.

VPNs have become popular because they offer excellent cost savings and performance improvements in comparison to more traditional remote access mediums. The ability to be able to connect securely across xDSL and cable modem connections, removes the ‘per minute' connection costs of dial and increases bandwidth by a factor of ten.

This bulletin will discuss the types of VPN available, benefits, and considerations necessary when deploying SSL VPNs. To aid this discussion, a description of SSL VPN operation is presented in section 2.2.

1.2 Types of VPN

VPNs are normally split into two distinct categories

- Site to site VPNs, between two or more offices or datacentres
- Client to site VPNs, between a desktop client and a central office or datacentre

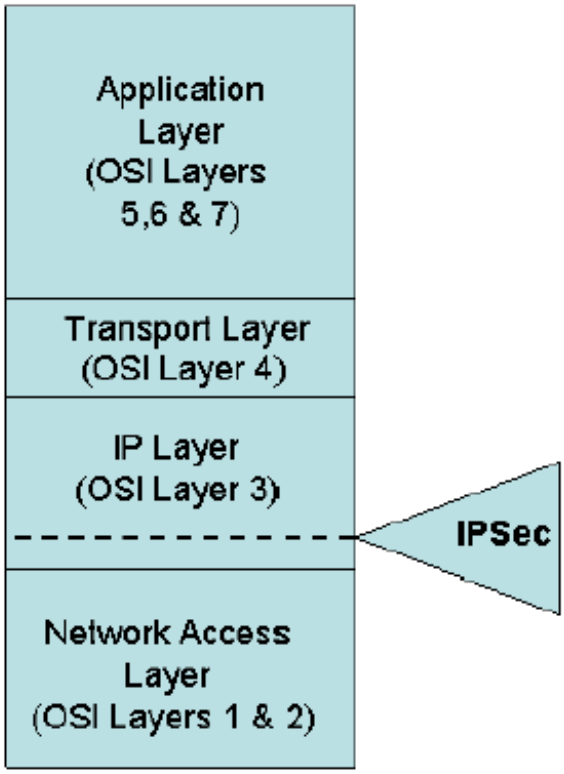
For the purpose of this paper, we are only considering client to site VPNs. As with any IP network related issue, using an IETF standards based solutions is normally considered key. This brings all the benefits of interoperability between different vendors and the peace of mind that the security of a solution has been securitised by the Internet community. Two such standard based solutions are introduced below:

1.2.1 IPSec

Most client to site VPNs are based around IPSec (short for IP Security), which is a suite of protocols developed by the IETF to support secure exchange of packets at the IP layer. Typically, an IPSec tunnel connection will be created from a Client software component to a VPN gateway (or firewall with VPN functionality). Following the initialisation of this tunnel, all packets destined for the remote corporate network will be routed down this tunnel. The tunnel provides the necessary security, by encrypting each packet (using one of a selection of algorithms) before forwarding it to the remote gateway. When packets reach the remote gateway, they are decrypted and then forwarded ‘in the clear' to the final destination.

IPSec was initially devised for site to site VPN connections, so to add the necessary functionality to IPSec to allow effective client to site connections and management, each vendor has added vendor specific features to it's IPSec implementation. Good examples of this include Check Point hybrid mode to allow strong user authentication without certificates and NAT traversal techniques from the majority of vendors.
As shown in figure 1, IPSec clients work by adding extra functionality at the bottom of the IP Layer. This functionality inspects traffic, and encapsulates and encrypts traffic as necessary.

Figure 1



1.2.2 Secure Sockets Layer (SSL)

The emerging trend in Secure Remote Access VPNs is to use Secure Sockets Layer (SSL). Secure Sockets layer is a protocol, which is already imbedded in most IP stacks and sits at the base of the application layer, as shown in figure 2. SSL has been traditionally and widely deployed for securing web based applications in the form of HTTPS (or secure HTTP). Even the most novice users are normally aware of the padlock symbol shown on secure web sites, even if they are unaware that this means the site is protected by SSL.

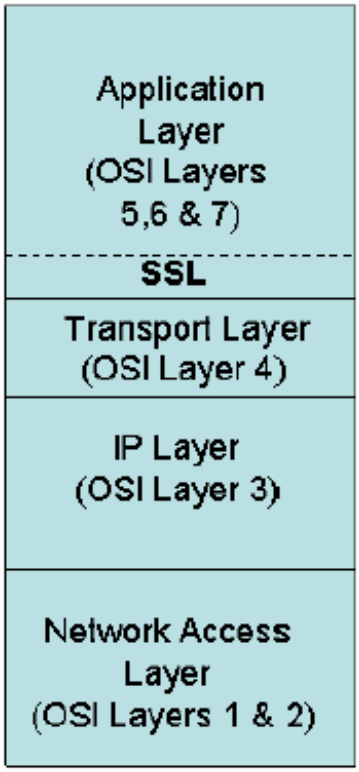
Figure 2

Some SSL VPNs claim to have clientless or near clientless operation. This means access to the VPN can be created from any machine with a Web browser, including machines in Internet café's and home machines.

The main drivers for SSL VPN are:

- Cost saving - Because SSL VPNs can be clientless, the cost of deploying clients is saved. For large organisations this can be a large outlay.
- Platform independent & mobile- Access can be granted from many types of machine (Linux, Windows, PDAs) and from many locations.

With these benefits, SSL VPNs also bring many complications and considerations. The details of these are considered in this document.



Click here to read part 2 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