SSL VPN Deployment Considerations

archive.networknewz.com/networknewz-10-20031201SSLVPNDeploymentConsiderations.html

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

Now we have discussed some of the advantages to SSL VPNs and have an understanding of how they operate, it is important to look at some of the deployment considerations (or in some ways disadvantages) of SSL VPNs.

- **Client Security -** Because SSL VPN offers a much greater choice of client platform with ‘clientless' or ‘near clientless' operation, the security of any client connecting to the network must be heavily scrutinised. For example, in no way would any organisation consider a PC in an Internet café to be as trusted as a corporate issued laptop. Based on this assumption, vendors have developed several mechanisms to boost the trust associated with an un-trusted client connection. Some of these are outlined below:

- **Client integrity scanning -** When a client connects to the VPN a small java applet is downloaded to the client which searches for good or bad files, process or ports listening. For example, it can check for a running AV program with current definitions, the presence of a personal firewall with a standard rule set or the presence of any known Trojans. The disadvantage of this mechanism is it may place limitations on the types of clients that can connect, but more importantly, it is only a onetime snapshot of a system. Also with an understanding or the rule set, it seems feasible that these checks could be fooled.

- **Sandbox -** A sandbox is used to store any files downloaded from a corporate network over the SSL VPN. Once the VPN session is terminated, the contents of the sandbox are securely deleted. This avoids issues of email attachments and corporate data being accidentally left on un-trusted machines. Sandboxes can also be used to ensure Citrix Metaframe or other interactive session data is wiped from a machine at logoff.

- **Secure logoff and credential wiping -** This ensures that when users logoff the system, all logon credentials are wiped form the client machine. Of course, with an enterprise strength VPN solution, a strong authentication solution should also be used to protect credentials further.

- **Timeouts and re-authentication -** To avoid systems being left connected to the network by users, sessions can be terminated after periods of inactivity. Also, to ensure the correct user is still using the connection, periodic authentication during a session can be implemented on some systems.

- **Virus, malicious code and worm activity -** Because the client is nearly un-trusted, most SSL VPNs can also filter traffic at the application level (especially if an application level proxy is used, rather than a protocol redirector), blocking worms and viruses at the gateway.

- **Audit and Activity awareness -** Any security appliance, hardware or software system should include a good level of auditing. With SSL VPN this functionality is seen as key, because of the relatively simple systems needed to abuse an SSL VPN by a remote hacker (I.e. A web browser), should logon credentials become compromised. Further to this, some form of real time alerting of unusual actions (such as trying to copy an entire disk over the VPN) must be included. Some of this functionality is seen as less key by vendors and is still evolving.

- **Application support -** The major block to deployment of SSL VPNs is likely to be application support. As SSL works at the boundary of layers 4 and 5, each application must support its use. Vendors add additional support through the use of protocol redirectors, but these often require some user knowledge to operate. Based on this, the first step to take when designing an SSL VPN solution is to look at the access that will be required and assess how simple this will be to provide.

- **Internal Network Security Failings -** Using IPSec VPN, a large number of organisations allocate specific IP addresses to remote clients using the Radius Protocol. This gives the ability to filer and control traffic based on source IP, ensuring internal network security. Because all sessions from an SSL VPN are normally proxied from a single address, all clients sessions originate from this single IP. This means, a network administrator is unable to allocate privileges using source IP addressing. In reality, this level of control can be handled on the SSL VPN gateway, but if a network is already configured for source IP based security, the overhead of altering is can be very high.

Conclusions

SSL VPNs used for remote access, without doubt, have significant advantages over the IPSec alternatives. But alongside these advantages they also offer added complexity, which must be weighed up against the advantages. Before considering an SSL VPN deployment you should consider:

1. Can I accept or mitigate the security risks involved?

2. What will I gain from the added mobility and flexibility?

3. Which protocols do I need to support?

If all these questions can be answered, it may be time to start looking at which vendors can offer the best solution. One interesting point in relation to SSL VPN solutions is that most vendors (all but a few at the current time) consider SSL based VPNs to be separate from their IPSec counterparts in terms of hardware and software. If your network manager tends to follow rather than lead the trend, I suggest they will be looking for a solution which offers a complete VPN solution, offering both SSL and IPSec on a single system.

As nearly all vendors see SSL VPN as additional to IPSec VPN, rather than a replacement, we can conclude the SSL VPN is not "the new definition of secure remote access", but a complimentary solution to IPSec.

Finally, if you are not considering SSL VPN deployment, you should certainly consider the effect that SSL VPNs are already having on your network. Are contractors, consultants or employees bypassing your security controls by tunnelling their traffic out of your organisation over your SSL VPN? Is the use of SSL VPNs covered in your security policies and standards?

Click here to read part 1 of this article.

Click here to read part 2 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