Title:
Mobility And Security Part 1: SSL Based VPN's

Word Count:
510

Summary:
What does SSL and VPN mean?

SSL (Secure Sockets Layer) is a protocol developed by Netscape to secure data transmission between a client and a server. It was soon adopted by the likes of Microsoft Internet Explorer and other leading web browsers, providing a secure means to transact data in an encrypted format over the web, most commonly seen with e-commerce sites taking credit card payments for purchases.

A VPN (Virtual Private Network) is a private communications netwo...

Keywords:

Article Body:
What does SSL and VPN mean?

SSL (Secure Sockets Layer) is a protocol developed by Netscape to secure data transmission between a client and a server. It was soon adopted by the likes of Microsoft Internet Explorer and other leading web browsers, providing a secure means to transact data in an encrypted format over the web, most commonly seen with e-commerce sites taking credit card payments for purchases.

A VPN (Virtual Private Network) is a private communications network usually used within a company or by several companies that have a need to share information over a public network. VPN traffic is carried over the Internet using standard (often insecure) protocols.

What is the fuss with SSL VPN's?

SSL VPN technology has been around for several years, but only in the past year has the market literally exploded with low cost purpose built devices. The likes of Juniper, Nortel and now even Cisco have developed these low cost SSL based VPN solutions for various business types including SMEs.

SSL VPNs work at the application layer. Unlike IPSEC VPNs they are far less

complicated to setup, support and maintain. As they work with most modern web browsers no software is required to be configured and they are not restricted to a particular computer. Also, as almost all corporate networks globally, including those with stringent firewall policies, permit web traffic including the SSL port, SSL VPNs being utilized by mobile workers are almost guaranteed to work in every environment. This is one of the downfalls of the more common IPSEC VPN technology which struggles over NAT environments. One other benefit with SSL VPNs is it gives the administrator per-user access control to a strictly specified list of applications.

Summary of Benefits:

1. Low Total cost of ownership

2. End point Security in differing environments (e.g. if no Antivirus on mobile machine, only permit extranet access)

3. Clientless (web browser SSL VPN access for shared folders, applications & extranet resources)

4. On demand client for full network layer access

5. Helps secure thin client access in the public domain (Citrix, terminal services published on the web)

6. Per-user or per-group application list control

What should I do next?

1. Understand your company’s goals and what you are trying to achieve from your VPN solution

2. Consider what applications and services you intend to provide over your VPN solutions and understand the VPN options available to you.

3. Understand the security and service requirements of your VPN Solution and determine which VPN products provide these

4. Consider if you should be implementing additional security safeguards to further protect your VPN solution

SSL based VPN solutions are now very affordable and they ensure mobile workers can access crucial company information from almost any device anywhere in the

world. They ease simplicity and availability when implemented in a well planned and thought out manner and they help to achieve a trouble free environment for remotely accessing crucial data.

SSI's mobile and security specialists are available to provide mobile and security solutions for companies of all sizes covering consultancy, planning, deployment, support and user training.