Global Information Assurance Certification Paper

Considerations for Implementing an SSL VPN

GIAC GLSC Practical Assignment v1.0

Roger Crayton

Submitted March 16, 2004

Abstract

SSL VPNs have reached the point of being a practical technology worthy of consideration for the enterprise. They seem to be a PC administrator's dream – there is no software to install or manage on the client. This paper discusses the considerations for choosing an SSL VPN over a traditional IPsec implementation. Also discussed are considerations for securely implementing the SSL VPN.

Selection Criteria

Over the past two years, the SSL VPN has gone from being a niche product to a serious contender for the primary means of client-based VPN access. Research by The Tolly Group is a typical indicator of the growth of SSL VPNs. According to Karl Flinders, "The research, co-sponsored by indirect-selling SSL security appliance vendor Netilla, found that 75 percent of network managers believe enterprises will choose SSL VPNs when workers access the network externally, and expect the transformation to occur within two years." [1]

Remote access, commonly in the form of an IPsec VPN, is an important part of the enterprise architecture. At my company, every notebook that is deployed is expected to have remote access capabilities. For our Sales Force in particular, remote access is a requirement for important tools such as email, product catalogs, sales reports and other applications.

IPsec VPNs are one of the more demanding technologies to support. Our Help Desk spends a significant amount of time troubleshooting VPN problems. The ubiquitous availability of broadband connections in hotels has made this problem even worse. Our users expect the IPsec VPN to work on any hotel connection. This is often not the case. Many hotel firewalls do not support the ports and protocols required for an IPsec VPN to function. As security is tightened to prevent the spread of worms, these restrictions will become more widespread. It is time to explore other alternatives.

Management of remote computers and their connectivity is a high-profile security problem. According to Cisco, quoted in an article by Ryan Naraine, "Many organizations were successful at stopping recent worm attacks at their Internet boundaries, yet still fell victim to the exploits when mobile or guest users connected their infected PCs directly to internal local area networks." [2] Any VPN implementation must take security into consideration.

Discussion

Like any bandwagon, it is prudent to understand the technology prior to making the leap on-board. Simply stated, the client IPsec VPN operates at the network layer and looks like a network adapter to the applications and the user. One can do anything over an IPsec VPN that can be done over the LAN at the office, and it can be done in such a way that it feels just like being on the LAN. All

applications are accessible as long as they use TCP/IP. The IPsec VPN requires ESP protocol and TCP/UDP port 500 for IKE (Internet Key Exchange) to be passed. The IPsec VPN requires software on the client to operate.

On the back end in the Data Center, a VPN appliance is typically the device used to receive the connections. Authentication can be managed by the appliance itself or by external means. At my company, we use a RADIUS server to provide authentication.

In contrast, the SSL VPN requires no special software on the client. The connection is established using a browser. If the applications are browser-based, nothing else is required. If they are not, then Java or ActiveX plug-ins are required. As the SSL VPN market matures, more canned plug-ins are being offered. Dana Henrickson provides an excellent summary of the applications covered by SSL VPNs in the table on page 4 of the article "Are SSL VPNs Secure and Flexible Enough?" [3] The table is reproduced below and on the following page:

		SSL VPN			**IPsec VPN**
Remote Access	**Examples**	**Browser**	**Browser + Applet (or webified)**	**Installed Code**	**Proxy**
Web mail	Microsoft® OWA, IBM® IWA	X			X
Web Applications	Any custom or packaged	X			X
Web Term Services	Citrix®, Microsoft TSAC™	X			X
Web File Access	CIFS (SMB)	X			X
Web File Transfer	Microsoft Internet Explorer™	X			X
Native email	Outlook, Lotus, Eudora		X		X
Native File Access	NFS			X	X
Client-server	Siebel, SAP, PeopleSoft	Some		X	X

		SSL VPN			IPsec VPN
Remote Access	**Examples**	**Browser**	**Browser + Applet (or webified)**	**Installed Code**	**Proxy**
Legacy Host Apps	IBM 3270, 5250; VT100/320	X	X		X
Terminal Access	Telnet	X	X		X
File Access	NFS			X	X
File Transfer	FTP			X	X
Instant Messaging	Yahoo Messenger			X	X
Collaboration (UDP)	IBM Lotus Sametime®			X	X
Full TCP & UDP Support	All Applications & Data Stores			X	X

The table encompasses the applications that most companies are likely to encounter. Perusing the table, one can see that there are ways to run all of these applications over an SSL VPN. Of course, these applications can all be run transparently using the IPsec VPN. This illustrates the trade-off – the SSL VPN, while requiring no software on the client, requires more tuning and maintenance on the back end than does the IPsec VPN. Of course, the SSL VPN's tuning and maintenance is generally centralized on the appliance, making it manageable. Deploying maintenance upgrades to remote clients – of IPsec VPN software or anything else – can be supremely frustrating.

So, the SSL VPN is capable, but is it secure and manageable enough? The lack of client software, the feature that makes it so appealing, also makes it a security risk. With the IPsec VPN's requirement of client software, one can limit the computers that have access to the VPN by making sure that only those machines have the VPN software installed and configured.

In contrast, the clientless environment of the SSL VPN makes it possible to access the VPN from any computer – home PCs, PCs in hotel business centers, Internet cafes, etcetera. This is a wonderful convenience for the users, but access from uncontrolled machines poses a significant security risk.

Authentication into SSL VPNs can take many forms. The authentication methods supported by the NetScreen SA 3000 offer an example. According to the product specification sheet, RADIUS, LDAP, Windows NT Domain, Active Directory and Unix NIS provide user ID and password authentication. Stronger two-factor authentication is available in the form of ActivCard ActivPack™, RSA SecurID®,

and Secure Computing SafeWord™ PremierAccess ®. X509 client-side digital certificates are also supported. [4]

With this kind of open access, what are the options available for controlling access? SSL VPN manufacturers recognize the requirement for controls and are taking steps to implement them. According to Dana Henrickson, "forced user re-authentication, session time-outs, the automatic erasure of downloaded files, and the disablement of certain browser features like autocomplete, history and temporary files will become standard SSL VPN capabilities." [3]

Open access also increases vulnerability to attacks from viruses and worms. It is hard enough to keep these at bay with company-owned equipment in the hands of remote users. Here too, the manufacturers recognize the need and are building functionality into the products to address it. The NetScreen-SA 3000 can sense the presence of anti-virus and personal firewall software. If these items are not present on the PC, access to the VPN is denied. The product specification sheet discusses this and other features of the product. [4]

Since the SSL VPN operates at the application layer, not the network layer, authorization is granted by application, so a much more granular level of control is achieved than with an IPsec VPN. While this makes more work for the administrator managing authorization, it is inherently more secure since users are explicitly being granted access to what they need if the SSL VPN is being properly managed with a default-deny methodology. In a typical company, the profile for most users is probably pretty simple – access to email and maybe a network share or two. Additional applications can be configured for the small number of users who require them.

In addition to remote access for the Sales Force and other traditional remote users, the SSL VPN is a good fit for other types of remote access. It is a good solution for granting access to vendors for support. Access can be easily limited to the servers and applications supported by a particular vendor. Setup is trivial since no software is required on the PC. Another good use is establishing extranets for applications like employee benefits self-service or supplier reverse auctions.

The SSL VPN could be a useful addition to a wireless LAN. One could place the wireless LAN behind a firewall and limit access to just the SSL VPN allowing ports 80 and 443 only. The only way to access corporate applications would be through the SSL VPN. This in conjunction with standard wireless security precautions would make for a reasonably secure wireless network.

In implementing an SSL VPN, authentication methods, authorization and training need to be considered.

Authentication. Choose an authentication method that matches the sensitivity of the data and the level of access that will be authorized. Even for basic email and

file share access to non-sensitive data, I think a case can be made for two-factor authentication. Since no client software is required, it is easy to access the SSL VPN from any computer, broadening the exposure to unauthorized access. Take advantage of the features your appliance offers for validating the PC's environment, like checking for current anti-virus and personal firewall software. Apply re-authentication and cache cleaning settings to prevent unauthorized access from public computers should users forget to clean up after themselves. Audit your users often to be sure only current, active employees have access to the VPN.

Authorization. Study your users carefully and understand the applications they need to access remotely. Most users have simple needs. Provide authorization for just the applications needed and no more. If a user asks for an exception, request that their manager provide justification. Audit the use of applications regularly, particularly the exceptions, to be sure these exceptions are still required.

Training. The SSL VPN is simple to use, but it definitely has a different look and feel than the IPsec VPN does. The IPsec VPN behaves just like a standard network connection, the SSL VPN is not as transparent. It requires modified behavior on the part of the user, like accessing files through a browser window instead of Windows Explorer. To be successful, the users will need some form of training. Since many of them are remote, a CBT or some good clear documentation might be appropriate in place of a face-to-face session. Any training should stress security. The users should be asked to sign a security policy that outlines acceptable use and user responsibility.

Train the support staff to be ready to handle any problems the users may encounter. The administrators should be especially well-trained in the features of the product to be able to maximize security.

Conclusion

As a result of my research and testing, I believe the SSL VPN warrants strong consideration as an enterprise remote access solution. Flexibility, ease of deployment and the ability to use it from networks that restrict the use of IPsec VPNs are all advantages. Properly deployed, an SSL VPN can provide improved access for remote users while reducing the load on the support staff.

References

[1] Flinders, Karl. "Secure Future for SSL VPNs." 02 Oct. 2003. URL: http://www.vnunet.com/News/1138593 (10 Mar. 2004).

[2] Naraine, Ryan. "Cisco Declares War on Network Worms." 18 Nov. 2003. URL: http://news.earthweb.com/ent-news/article.php/3110421 (10 Mar. 2004).

[3] Henrickson, Dana. "Are SSL VPNs Secure and Flexible Enough?" Mar. 2003. URL: http://www.breakawaymg.com/readingroom/bmg_sslvpn1.pdf (10 Mar. 2004)

[4] NetScreen Technologies Inc. "NetScreen-SA 3000 Series – Neoteris Secure Access Appliances."
URL: http://www.neoteris.com/products/SA3000_specs.pdf (10 Mar. 2004)