GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials (Security 401)"
at http://www.giac.org/registration/gsec

Are SSL VPNs Ready for the Mainstream?

Michael D. Jackson
GIAC Security Essentials Certification (GSEC)
Version 1.4b Option 1
June 2, 2004

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Abstract:

The growing demand for external access into a company's internal network and internal resources is driving the rapid deployment of remote access via virtual private networks (VPNs). This paper looks at one of the newest remote access technologies, the Secure Sockets Layer (SSL) VPN. SSL VPNs are generally held to be a user-friendly, cost-effective, secure remote access method. This paper discusses the relative strengths and weaknesses of SSL VPNs and examines whether or not SSL VPNs are ready for mainstream use.

What is a VPN?

A virtual private network (VPN) is defined as "a private data network that makes use of the public telecommunication infrastructure, maintaining privacy through the use of a tunneling protocol and security procedures," by the Virtual Private Network Consortium, VPNC, an organization created to promote VPN technologies.[1] To be considered a VPN, all traffic on the tunnel must be encrypted and authenticated by both of the end points making up the tunnel. In addition, there cannot be any way that an outside party can change the security properties of any part of the VPN. VPNs were originally developed to reduce the costs of connecting branch offices to the main office of a business. Thus, VPNs were initially created to address the high costs of leased lines and dedicated connections between offices. Later, VPNs were adapted to allow individual remote users access to a company's internal network across the public Internet.

What is an SSL VPN?

The Secure Sockets Layer (SSL) VPN was developed to simplify access to internal company network resources for remote end users. An SSL VPN is a VPN based on the Secure Sockets Layer protocol developed by Netscape Communications during the 1990s. Netscape Communications developed this protocol to transmit private documents via the Internet by initiating a connection from a client to a server using data encryption and other options such as server authentication, message integrity, and client authentication [2]. SSL is now a standard built into every major web browser and web server. In addition to being used in web browsers, SSL has been adapted to secure other protocols (e.g., POP3, IMAP, and SMTP).

The Strengths of SSL VPNs:

There are several benefits to using an SSL VPN for remote access into a company’s internal network. As an overview, SSL VPNs do not require a special client for basic access. They can enable the external user to tunnel remote

[1] VPN Consortium "VPN Technologies: Definitions and Requirements"

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

applications through their web browser-based VPN connection. In addition, SSL VPNs are not hindered by firewalls or other devices running network address translation (NAT). Further, SSL VPNs have a lower Total Cost of Ownership then other VPNs, and they have a number of strong security features that will be described in detail below.

The first and foremost benefit of an SSL VPN is that it does not require a specialized client. Instead, the SSL VPN merely requires a web browser that has SSL support. At the present time, virtually all web browsers come standard with SSL included. Additionally, because web browsers are available for almost any operating system and hardware platform, a user is not restricted to accessing the VPN from a PC with Windows only. That opens up VPN access to users on Macintosh computers, most UNIX servers and work stations, PDA's and even some cell phones. The versatility of this remote access technology gives the external remote user the freedom to connect from anywhere where there is Internet access. The user can be in a coffee shop, an Internet kiosk, at home, or even in a customer's office, and they can VPN back into their office and access a variety of resources. The user simply opens up their web browser, enters in the web page address of the SSL VPN, and authenticates to it. They then gain immediate access to their company's web-enabled resources such as web-based email, and applications with web interfaces.

SSL VPN vendors are aware that many of the company internal resources that are important to users are not web-enabled. To address this problem, SSL VPN vendors have expanded the functionality of SSL VPNs such that they are now capable of providing access to many non-web-enabled resources. As an example, a common feature of SSL VPNs is the enabling of Windows and UNIX file shares to operate through the web browser. Users can have the option of browsing for a server or clicking on predefined links to view the available company internal network shares. The SSL VPN administrator can grant the user full access to shares or restrict the user to only select functions such as viewing certain shares or only being able to upload or download files.

Vendors have also created some client-server applications that run directly in the web browser and increase the web browser’s functionality. Two common applications are telnet and SSH [3]. The user simply selects the telnet or SSH application from the SSL VPN web page, and after a short download, the user's web browser functions just like a standard telnet or SSH client. The browser tunnels all of the telnet or SSH traffic through the SSL connection back to the main office allowing the user to perform their functions just like they were in their office.

For other applications, remote users might need to run in a client-server scenario. SSL Vendors have come up with a variety of methods to relay the user's connection through the web browser using a variety of proxy technologies. This paper will not go into the specifics of the methods that each vendor uses. In

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

general terms, it is done by the SSL VPN downloading to the user's web browser a special Java or ActiveX application. This application configures the user's computer to forward traffic from applications on the user's computer through the web browser's SSL connection back to servers on the company's internal network [3;4;5]. In this configuration, the user can run virtually any client-server application they need. Once the user starts the application, they are transparently tunneled through the Java or ActiveX application into the company internal network. Programs like Windows remote desktop client, telnet and SSH binaries, and even Microsoft Outlook function just like the user was back in the office.

Some SSL VPNs vendor's have enabled a feature that gives a user full remote access into the company's internal network. The user's computer is given an IP address and becomes a node on the company network. To use the full remote access feature, an ActiveX control is downloaded to the end user's computer and runs in conjunction with the web browser. The ActiveX control starts up a tunnel through the web browser that routes all traffic from the end user's computer to the SSL VPN. On the Netscreen-SA SSL VPN, by Juniper Networks, this ActiveX control is called "Network Connect" [3]. This option allows the user to use real time applications such as Voice over IP, streaming, and other applications that require dynamic ports to function or use UDP packets between the client computer and the company internal network.

Another benefit of SSL VPNs is that they allow a user to initiate a VPN connection from locations where other types of VPN would not typically work. SSL VPNs are not blocked by devices running NAT, such as firewalls, like other VPNs such as IPSEC based VPNs. SSL VPNs function at layer four, the transport layer of the OSI network model, and IPSEC VPNs function at layer 3, the Network layer [6]. When a device such as a firewall runs NAT, it breaks the tunnels formed by non-SSL VPNs operating at the lower layer, but does not directly interfere with the higher layer SSL traffic. Firewalls can also break VPNs in a way other than NAT. A lot of firewalls are set to prevent inbound and outbound traffic from the company's internal networks on specific ports with blocking access control lists (ACLs.) These blocking ACLs frequently cause VPNs to fail. SSL VPNs will typically get around this problem because they operate on TCP port 443, a port not normally blocked [7].

From a Total Cost of Ownership standpoint, the SSL VPN comes in far lower than other VPNs. As mentioned before, no special client has to be purchased for the remote user side of the connection; all that is needed is a web browser, keeping initial costs lower. Companies no longer have to purchase and maintain laptops for all remote users. Additionally, support costs are lowered considerably because end users and support staff do not have to deal with as many configuration problems and as many software conflicts [8].

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Security Benefits:

In addition to having a lot of functionality, SSL VPNs have quite a few security features. The common security features include multiple forms of user authentication and authorization, tight access control into company resources, detailed logging, client security verification, and cleanup of temporary files on the client's remote computer during the session and when the user is done. All of these options combine to make a user's connection from remote locations almost as secure as being on the company LAN.

For authentication and authorization of the user there are several different methods available. Some of the most common methods are usernames and passwords stored locally on the SSL VPN device, RADIUS, two factor authentication with RSA Secure tokens, and client-side digital certificates [3; 4; 5]. Additionally, the option to tie the SSL VPN into an LDAP and Active Directory server can ensure users are authenticated and authorized to only access resources specified in their stored profile. This means users will not get access to any resources through the SSL VPN to which they should not have access.

There are quite a few options available for additional access control and security directly enabled on SSL VPNs. Users can be restricted to only being able to access the SSL VPN from specific remote IP addresses; if they try to come from elsewhere they will be refused connection or not be able to log in. The user's profile can also be set to only work with a specific web browser. The user can be set to only view specific websites, specific links on websites, specific files, or even specific ports, locking the user into only the web resources that they need. The administrator can then go one step further and mask the real addresses of those internal web sites and web page links to keep all internal company network information confidential.

When it comes to security for the client-server applications that can be proxied through the downloaded Java or ActiveX applications, there are a plethora of options available. Remote users can be given access to run any application they want or they can be restricted to running only select applications through the tunnel. The restriction of applications can be achieved by any or all of the following options: specifying the names of the application executables; specifying that the application have an MD5 checksum match between that of the application that it is trying to run and a stored value on the SSL VPN; specifying incoming ports to which the application can talk; and specifying internal company hostname or company IPs to which it can talk.

In addition to the blocking features that the SSL VPNs employ, there are some more advanced security options available. Some SSL VPNs have additional security helper applications that can be downloaded to a user's computer to perform specific tasks. One example, the "Host Checker" included in the Netscreen-SA SSL VPN examines the user's computer at the beginning of a

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

connection to make sure the current computer abides by the company's security policies and requirements [3]. The application can be customized to check that the user's computer is actively running a personal firewall and/or an anti-virus program. A similar application from Whale Communications can check to make sure the latest virus definitions are being used, and it can check the registry for specific settings [4]. The security checking does not stop with just those options, options also exist for some devices to check for open ports, and applications running on the end user's computer. If those requirements are not met at the time the user connects and periodically throughout the connection, then the user is not allowed to complete the connection or they are given only limited access to the company internal resources. This option is ideal for users that have access to a lot of resources, but who frequently make use of public terminal Internet kiosks or unsecured computers to connect. With the host checker option enabled, if this user chooses to connect from an Internet kiosk they could potentially receive access from only a subset of their normal resources. As soon as they go back to a computer that is running the required software and that computer passes the full check out with the host checking application, the user gets full access to their normal resources for that session.

A second type of security helper application that some SSL VPNs employ is a tool designed to clean-up after a user, and prevent any future users of the computer from gaining information about the company's data or network. While the user is connected to the SSL VPN the application tries to watch what the user downloads and then remove those files when the user is done. The clean-up application looks for cookies, cache files, and temp files [3; 4].

One final security feature that SSL VPNs tout are their ability to log, in detail, actions taken by the user while they are connected to the VPN. SSL VPNs have options that allow logging of most actions a user takes across the VPN tunnel. If a user clicks on a link to request an internal web page or clicks on corporate web mail to read email, or starts up a client-server application that connects through the VPN it can be logged. In addition to all valid traffic being logged, invalid activity is also logged [3; 5].

The Negatives of SSL VPNs:

Even though SSL VPNs have a lot of good points they are not necessarily the right VPN solution for all scenarios -- they do have their share of problems. SSL VPNs are not designed for an environment where the VPN connection needs to be always on and shared by multiple users; it requires a web browser to function. There are potential problems with the downloadable helper applications -- some are convenience problems and some are security related -- these will be described below. There are also some security problems with running non-web-enabled applications; by using them, users may inadvertently introduce worms and viruses through the proxy applications to the company's internal network. The non-web-enabled applications may also leak information about the

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

company's network out to the Internet.

The first problem arises from the fact that the SSL VPN requires a web browser on an individual's computer to act as the client end of the service to function. This makes SSL VPN connections only suitable for a single user to connect instead of like other VPN implementations, such as IPSEC, where the client can be a single computer or a hardware device that tunnels multiple users' traffic back to the office VPN server [9].

A second problem could arise when a user tries to use the advanced features of SSL VPNs, those that require the helper applications. Users may encounter problems when they try to use any of the helper applications. There are a several reasons for this. First, the web browser on that particular computer may not be allowed to run Java or ActiveX because it has security settings that may be set too high. With the browser set to the high security settings, the user may be prevented from downloading and running any Java or ActiveX, not just the SSL VPN applications. Computers at Internet cafes or kiosks may be set this way. Another way that the helper applications could be prevented from running is by the user using pop-up blockers in their web browser or an external pop-up blocker program. Pop-up blockers are intended to keep nuisances, such as pop-up advertisements, from coming up and running on the user's computer, but they are not smart enough to determine a good pop-up application from an unwanted one automatically. The pop-up blocker may see pop-ups coming from the SSL VPN as nuisances and block the helper applications from performing their security and proxy functions. Two other things could stop the helper applications from functioning: not having Java or ActiveX available or installed on the user's computer. Java, from Sun Microsystems, may not be installed or may be disabled on the computer that the remote user is trying to use. Like Java, if the downloadable helper application requires ActiveX, the web browser has to be Internet Explorer and have ActiveX enabled or it will not work [10]. One final reason the helper applications for some SSL VPNs may not work is because the user may not have the correct access level on their computer to let downloaded applications perform any necessary temporary changes that are needed. Without these temporary changes to the computer the tunneling of their client-server applications over the port 443 SSL connection back to the office may not function [11]. Windows XP and Linux are two operating systems that may have this issue. Both operating systems have different levels of access for users, and both put the standard user account at a level that does not allow the kind of changes on the local computer that are needed for the helper applications to run.

Even if a user does have the right access level on the local computer and does have the ability to run Java and or ActiveX, they could still encounter problems with a helper applications downloaded from the SSL VPN. Some of the helper applications make subtle changes to the user's computer when they run, and they must undo those changes when they are done running or the user disconnects from the VPN connection. Should the helper application fail to

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

reverse the changes that it made to the computer for any reason, the user's computer could be left in an unusable state and may have to be fixed by hand [5].

Security Concerns:

Going beyond helper application runtime and cleanup problems, there are some security concerns that still need to be addressed. The first is that the host checking application may only check the remote computer once when the user logs into the SSL VPN. If the host checking application does not run continuously while the user is logged in, the user could potentially breach the company's security requirements and policies without censor [12]. The remote computer could then introduce viruses or worms to the company's internal network. In addition to the virus and worm threat, the user's computer, if not sufficiently monitored, could also become a conduit for a backdoor into the network while the user remains connected to the SSL VPN. In sum, the host checking application needs to run continuously on the end user's computer to fully protect the company's internal network. The host checking application should even go as far as to automatically disconnect the user in the event that they stop conforming to the security policy and requirements. This security concern may be correctable by adjusting the host checking applications parameters to continuously check the remote user's computer for compliance, and in the event of non-compliance, the host checking application can force the user's SSL VPN connection to disconnect immediately.

A second security concern that exists with the current generation of SSL VPNs is that the cache cleaning application could fail to run. There are a couple of reasons for this. First, if a user's computer crashes before the cache cleaning application runs, critical files may be leaked out because they were never cleaned up. This problem may not ever be completely resolvable because the user and the company may not have control of the remote computer after a failure. Another reason that the cache cleaning application might not work is because it may not know how to handle the operating system and the web browser that the user is using. Each operating system and web browser will have their own set of criteria that need to be met in order for this function to work. Additionally, the cache cleaning application may not know all of the places on the local computer that the user has downloaded files to, and the application could miss some critical data, such as authentication information, when it is cleaning up. The only way to ensure that data does not get left behind is to prohibit the use of the advanced options of SSL VPNs on computers in which the company does not maintain control. In other words, Internet kiosk computers should be avoided if advanced features of the SSL VPN are required. If the user has to use a public Internet terminal, a recommendation would be to have users stick to basic web-only applications and not allow them to download any files [10].

A third security concern also arises from the fact that users can use SSL VPNs

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

from virtually anywhere. Is a computer at an Internet café or kiosk really secure? Could that computer be rigged to record all activity that occurs on it? Could there be a keystroke logger or any other hidden application installed that can keep or steal company data? The SSL VPN downloadable applications may not be able to detect any spy ware programs, thus lending the company and remote user a false sense of security [13].

A fourth security concern is that SSL VPNs encrypt data going to and from the outside port on the SSL VPN to the remote user, but they do not necessarily encrypt data coming from the internal company servers to the inside port of the SSL VPN device. Chances are that while the data is traversing the company LAN from the internal server to the inside port on the SSL VPN, it is vulnerable to being intercepted and read unless it has been encrypted by some other means. Users must not assume that just because the data is on the internal LAN, behind the SSL VPN, that it is safe. A company's own employees located on the LAN may take advantage of that unencrypted traffic and have access to sensitive or unauthorized data that may not have been available if it was not going through the SSL VPN.

Yet another security issue with SSL VPNs is the question of what constitutes an appropriate amount of logging and what level of detail is sufficient for the logging? Is the log accurately recording all actions users are taking through the SSL VPN connection? Are security violations being recorded? In addition to recording the activity is there a method to alert network administrators should an access violation be logged? These are all questions that may not be answered without some sort of built-in tool analyzing each action taken by users.

One last security concern of SSL VPNs involves security not from the SSL VPN perspective, but from the perspective of the network that the remote user is on. Is an SSL VPN connection something that should be allowed to pass through firewalls? Because most firewalls do not block port 443, the port on which the SSL VPN operates, users could violate security policies and procedures that are in place to stop VPNs from going out of a secured private network. A user could initiate a connection back to his or her home office from inside a network and potentially be a conduit for remote traffic into the private network s/he is on. The user could also transmit data to a remote location without the knowledge or consent of the network administrators of the network s/he is on.

Conclusion:

The SSL based VPN is a young, rapidly evolving technology. While SSL VPNs are not perfect, they offer features previously not available with other VPNs. In the short period of time they have been available, the technology has gone from a tool that just allows for secure web browsing of a company's internal web pages to a tool that can give a user located anywhere in the world selective, relatively secure access to virtually any of a company's internal resources. This

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

access gives the potential for employees to perform job functions from anywhere in the world, using almost any Internet accessible device. This could lead to increased employee productivity and success of organizations that make use of this technology.

In addition to providing remote access from anywhere, SSL VPNs offer a wide variety of security options including authentication, selective access to internal resources, verification of applications, remote host security checking, and clean-up to protect the user and the company. While these features offer reasonable security, it must be kept in mind that these features do not always function properly on a remote user's computer. In the case of reduced functionality of these features, the company could be left wide open to viruses or hackers, or company data could leak to the outside world. Users must be diligent, cautious, and aware of the potential security risks when they make use of SSL VPNs.

The benefits are numerous and will likely attract many businesses; that said, to effectively use the SSL VPN technology users and administrators must weigh the convenience and security features afforded by SSL VPNs and take appropriate action to protect their company's resources while using this service.

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

References:

1. VPN Consortium. "VPN Technologies: Definitions and Requirements." January 2003. URL: http://www.vpnc.org/vpn-technologies.pdf (25 May 2004)
2. Netscape Communications Corporation. "Secure Sockets Layer." URL: http://wp.netscape.com/security/techbriefs/ssl.html (25 May 2004)
3. Juniper Networks. “Netscreen-SA 5000 Series.” URL: http://www.juniper.net/products/ssl/dsheet/ds_sa5000.pdf (20 April 2004)
4. Whale Communications. “The e-Gap Remote Access Appliance SSL Access Platform.” http://www.whalecommunications.com/site/download.asp?fileID=s_1358 (27 May 2004)
5. Permeo. “Permeo SSL Remote Access FAQ.” URL: http://www.permeo.com/ssl_faq.htm (21 April 2004)
6. Corrent Corporation Knowledge Base. URL: http://www.corrent.com/KnowBase/Kinds_Of_Security.htm (20 April 2004)
7. Warden, Waheed. "SSL VPN in Detail." 01 Dec 2003. NetworkNewz. URL: http://www.webpronews.com/it/networksystems/wpn-21-20031201SSLVPNinDetail.html (21 April 2004)
8. Breakaway Marketing Group. "Ownership Economics" SSL VPN Central. 2003 URL: http://www.sslvpn.breakawaymg.com/ownership_economics.php (7 April 2004)
9. Avolio, Fredrick M. “Security Review: SSL VPNs.” URL: http://www.avolio.com/papers/SSLVPN_SecWP.pdf (21 April 2004)
10. Snyder, Joel. “The Myth of no Finger prints.” Network World Fusion. 12 Jan 2004. URL: http://www.nwfusion.com/reviews/2004/0112revmyth.html (20 April 2004)
11. Fratto, Mike. “The SSL Alternative.” Network Computing. 13 Nov 2003. http://www.networkcomputing.com/showitem.jhtml?articleID=16000510&pgno=2 (15 Mar 2004)
12. Fratto, Mike. “E-Gap Remote Access Appliance Compliance Police.” Network Computing. 4 Mar 2004. URL: http://www.nwc.com/shared/article/printArticlePage.jhtml?articleID=18100142&pgno=1 (5 April 2004)
13. Associated Press. “Kinko's spy case highlights risks of public Internet terminals.” KioskCom. 23 July 2003 URL: http://www.kioskcom.com/articles_detail.php?ident=1828 (21 April 2004)

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.