

Astaro OrangePaper

Comfortable Remote-Access without Compromises

SSL-VPN in comparison with
traditional VPN technologies

Author: Udo Kerst

*Astaro Sr. Product
Manager*



Date: 2008-05-02

Content

Page

Introduction	2
“Traditional” VPN Technologies.....	2
Microsoft’s Original Solution: PPTP.....	3
Open Standard: IPSec	4
Combination Package L2TP.....	5
Remote Access as the Main Problem	6
From SSL to SSL VPN	7
Limitations of SSL	8
Back to the Software Client	9
Conclusion	11

Introduction

Online communication and processing of internet transactions — summarized under the term e-commerce — have become standard technologies for companies in the past ten years. However, many of the promised time and cost benefits could not be realized immediately. From the very beginning, the World Wide Web has been an insecure place where professional and semi-professional data thieves do mischief, discrediting it as a means of safely exchanging confidential information. Naturally, this has been a well-known fact for IT managers who consequently slowed down the adjustment of IT environments, which was necessary for economic reasons but caused negative side-effects.

At a very early stage, security experts reacted to these demands by trying to establish secure transmission routes based on the available technological infrastructure, inaccessible to outside attacks. This marked the beginning of Virtual Private Networks (VPN), allowing for the establishment of leased line communication shielding information exchanged between two internet users. When, for example, data is being sent from a company's central network to its affiliates, it is possible to even exchange confidential or secret information. In this scenario, encryption usually includes data packages of network layers two and three; examples of such commonly used protocols include PPTP (Point-to-Point Tunneling Protocol), L2TP (Layer 2 Tunneling Protocol) and IPSec (IP Security). combining both positive and negative aspects. Originally designed for secure remote web access to email accounts, the protocol instead uses encryption capabilities which are already part of the browser. This whitepaper discusses why there are SSL VPNs nonetheless, and why they are able to compete with other solutions in terms of security.

"Traditional" VPN Technologies

Virtual private networks are nothing more than dedicated connections between computers of various users belonging to the same network but located at different sites. Through VPNs, members of a given project team are able to exchange work results, or employees at a subsidiary can access central databases and applications. In order to ensure maximum confidentiality, data transmissions are encrypted. Before establishing VPN connections, users need

to authenticate themselves and exchange transmission details in between computers, including cryptographic algorithms and encryption keys in particular. It is mandatory to follow a fixed sequence of steps to initiate information exchange, which are determined by three different data transmission protocols designed in the nineties: PPTP, IPSec, and L2TP. Despite the different designs, the general concept is the same: all of the protocols use the Internet as a cost-effective communication platform, leveraging encrypted connections that can only be hacked with enormous effort, if at all.

Microsoft's Original Solution: PPTP

As far as the standards listed above are concerned, only two of them (IPSec, and L2TP) received official approval by the Internet Engineering Task Force (IETF) which published them in RFC 2401, and RFC 2661. PPTP, on the other hand, was kept to an informal status, even though the protocol, published in RFC 2637, profited from a much wider use than the rest. Implementation and usage of the protocol co-developed by Microsoft were straightforward, indeed, so that the Redmond company integrated the technology into its operating systems, starting with Windows 95 Release 2. However, this very version suffered from significant security weaknesses causing renowned security experts, such as crypto analyst Bruce Schneier, to send out public warnings against the use of PPTP at a very early stage. Still, Microsoft's protocol contained all of the basic functionality required to provide user authentication and encryption of reference data.

At first, the critics focused on cryptographic algorithm RC4 with supported key lengths of only 40 bit, a security level which, at the end of the nineties was already widely considered inadequate and virtually invited eavesdroppers to hack into VPN connections. This issue merely scratched the surface, however. The real problem in the design of PPTP could not be reconciled by more powerful key lengths such as 128 bit: PPTP derives keys from the user password's hash algorithm. Potential attackers didn't have to break the session key; they only needed to initiate a dictionary attack, as most of the users choose weak passwords.

In the course of advancing PPTP, Microsoft introduced a new authentication method, MS-CHAPv2, including, amongst other additions, a program routine to

regularly change passwords and thereby improving security. However, the Redmond-based company tried its best to achieve downward compatibility, allowing Windows 2000/XP users to use older methods and thereby reintroduced the very same security problems. The operating system's latest generation, Windows Vista, tries to remove this weakness by exclusively supporting MS-CHAPv2. However, as it will take time until IT environments have fully updated, the problem will persist for now. As a result, it can be concluded that secure PPTP implementations are achievable, but they rely on a number of outside criteria. Especially with regard to remote access via the internet, expert advice is to deploy different protocols.

Open Standard: IPSec

Apart from PPTP, the oldest VPN security protocol is IPSec. In its basic form, its design goes back to the year 1995, but in 1998 it was redesigned by a diverse team of developers, including Cisco Systems employees, members of the National Institute of Standards and Technology (NIST), and representatives of the National Security Agency (NSA) – the most influential secret service in the US. As defined in RFCs 2401 through 2412, the protocol is generally considered to be the most secure one of its kind, and, consequently, it has become the de facto standard for all virtual private networks.

Due to the integration of several security mechanisms and options, IPSec allows for gradual shielding of connections. In Transport Mode, only user data is encrypted, whereas in Tunnel Mode, IP packets, including header information, are fully scrambled. The first mode of operation is mainly used for direct connections between two computers within a company network, while the second mode secures data transmissions between two separate networks over the internet. In terms of cryptographic algorithms, IPSec uses at least Data Encryption Standard (DES) with 56 bit key lengths; alternatively, cryptographic standards like Triple DES, IDEA, Blowfish, and the Advanced Encryption Standard (AES), the successor of DES, with key lengths of up to 448 bit, can be deployed. When implemented according to standards, VPNs with IPSec encryption are difficult to hack into, which is why attackers refrain from the necessary costs.

On account of its attributes, IPSec is the best choice for stationary connections, for instance, when a company's central network and individual branches

are connected (“site- to-site”). Similar to PPTP, there are a couple of disadvantages, though. Ironically, IPsec’s powerfulness results in a restricted number of possible deployment scenarios. Less experienced administrators are likely to make mistakes in this complex environment, allowing network connections that should not be open for security reasons. Despite stable internet access, mobile workers are also prone to suffering from failed connections to the company network or be unable to run an important application when a necessary port is blocked by a firewall and exceptions are not included in VPN configurations. As a remote access solution, IPsec has its limitations, and less complex protocols are of better service.

Combination Package L2TP

In many ways, the Layer 2 Tunneling Protocol is a solution of compromise, combining typical PPTP characteristics like simple implementation and ease-of-use with high security standards which are typical of IPsec. Hence, there are many variations, ranging from L2TP/IPsec-Transport and L2TP-over-IPsec to L2TP/IPsec. Historically, the protocol’s design is derived from PPTP and Layer 2 Forwarding (L2F) which was developed by Cisco and Nortel (no official standardization). Technically, it is based on the Point-to-Point Protocol (PPP) which is used by telecom carriers and Internet Service Providers when establishing connections between two end points or peers, for example, when accessing the internet via modem or ISDN. Primarily designed to establish connections, it is a very robust protocol which will rarely ever decline communication between two peers – for example, in the event of users entering the wrong password.

By connecting two end points, PPP was originally developed to transport data packets of network protocols like IP, IPX, and NetBEUI. Operating on the Data Link Layer, the second layer of the Open System Interconnection reference model, the name L2TP alludes to its core functionality. Additionally, L2TP establishes a communication tunnel allowing for data packet exchange of Network Layer protocols like PPTP or IPsec. Visually speaking, it runs underneath the Network Layer, even though, by definition, it belongs to the Application Layer, the highest layer of the OSI reference model.

Broadly speaking, L2TP has two advantages. Firstly, it allows the establishment of several connections via a so-called Access Concentrator (LAC), which means

that a number of users are able to log in using the same network node. L2TP then either establishes direct connections to the target server or moves requests over to an Access Concentrator (LAC), coordinating the respective details. Secondly, L2TP works together with Network Address Translation (NAT), enabling uninterrupted replacements of data packets' address information. This allows for connections to the target system, even when done via routers or firewalls. This combination of functions propels L2TP for remote access solutions.

However, a major disadvantage of L2TP in original design has always been that it refrains from encrypting data packets, even though it supports diverse authentication systems (PAP, CHAP, MS-CHAPv2, EAP). This lack of encryption initiated Microsoft's quest for an alternative to PPTP at the end of the nineties. Consequently, the development team decided to add the necessary IPSec functionalities and mechanisms, the result being L2TP/IPSec – a variation of the protocol combining its original robust design and routing capabilities with added security. Since the introduction of Windows 2000, such a client has been a steady component of the operating system – one of the side-effects being that 90 percent of all computers are equipped with L2TP/IPSec now.

At first glance, this protocol seemed to be the solution for most of the problems associated with establishing and shielding VPN connections, but L2TP was far from being perfect: Similar to IPSec a rather complex implementation process was mandatory which proved to be especially true for the correct LAC and LNS configurations.

Remote Access as the Main Problem

All differences aside, the technologies discussed so far have one important thing in common: connections to the target computer or network are established by client software. This approach consumes memory and requires regular fine-tuning when, for instance, port access is restricted or changed due to upgrades of firewalls, routers/gateways, and operating systems. Without adjustments, employees will not be able to connect to the company network. Moreover, there is the problem of separate installations of Linux/UNIX and

MacOS X VPN clients. And some of the important Windows VPN client features need to be adapted to these platforms first.

Mainly companies with a large number of mobile workers and/or employees working from home ran into these problems when internal resources had to be accessed frequently. They were looking for a remote access solution which was deployable at each and every location, regardless of the operating system in use, while at the same consuming as little memory as possible. This resulted in clientless systems utilizing existing technology. SSL seemed to be the magic formula.

From SSL to SSL VPN

Secure Socket Layer (SSL) is one of the basic technologies on the internet. As revealed by the signature "https://" in the address line, almost every online surfer has used it when shopping at amazon or ebay or when performing home banking tasks, for example. SSL connects two applications – the user's browser and the web shop or home banking server – and encrypts all of the data packets exchanged. Leveraging digital signatures and certificates of highest security levels (class 3 certificates), the protocol enforces strong authentication between web server and browser. SSL utilizes trusted algorithms like RC4, DES, RSA, and AES, for encryption and integrity checking – usually with key lengths of 128 bit. Occasionally, there are still processes in place working with 40 and 56 bit keys, but these operations cannot be trusted and should be avoided. For the individual user, all of these processes are performed more or less hidden in the background – his role limited to accepting or declining potentially insecure certificates.

SSL is an integral part of every browser – no doubt the protocol's greatest benefit – and this is also true for its enhancement TLS (Transport Layer Security) as defined by RFC 2246 and 4346, which has been part of standard browser technology since 1994/95. For remote access to protected websites, data or applications, no additional client software is necessary, fulfilling the first and foremost precondition of easy and efficient remote access solutions. Configuration efforts are also kept within limits, as far as users and server administrators are concerned: in general, SSL always uses port 443, greatly simplifying firewall and gateway configuration. As long as users are authenti-

cated correctly, they should always be in the position of having network access. Last but not least, network configurations can be updated automatically in this way; changes to VPN configurations, to DNS and WINS servers do not have to be performed manually.

Limitations of SSL

So much for theory. In reality, there are a couple of obstacles. Three or four years ago, there was intense discussion whether SSL was actually able to build “real” VPNs, but this is not the greatest concern. The debate started when several companies clung to the idea of labeling SSL VPNs as full-scale alternatives to existing solutions based on IPSec. This argument clearly went too far, but the main counter-argument was not on target either, claiming that installation of such networks was not possible due to the fact that SSL operated on the Application Layer, and not the Network Layer. As a matter of fact, this is also true of PPTP and L2TP, even Microsoft critics admit.

Restrictions resulting from deployment scenarios and technology design are more important than academic discussions, though. Naturally, security aspects are at the very forefront again. True, SSL provides access to company networks from virtually every location, but this also includes potentially insecure environments, such as internet cafés, and WLAN hotspots. Here, neither user nor administrator have any control over the security of connections established which might be vulnerable to attacks. Additionally, access information might not be fully deleted, and companies acting wisely will exclude such deployments in their security policy or face running the risk of turning one of SSL’s biggest advantages into a weakness.

Another limitation has to do with the fact that clientless usage can only be utilized in regard to web-based and browser-based applications. Every other scenario requires rather complex enhancements, including “webifiers” which run on VPN gateways and translate programs into web applications. The downside of this is that the “translation process” results in reduced ease-of-use, slow and deficient performance, and increasing demand of processing power. Port Forwarding (i.e. an applet on the client directing application data via SSL connection to SSL gateways) could be an alternative. However, in order to do

this, users require administration rights on the client which have to be applied manually, and, if worse comes to worst, might result in compromised security. A third alternative is to deploy ActiveX controls (agents), with the browser transmitting all of the data to a given SSL gateway and creating a virtual interface for true network access (even though restricted to Windows computers running Internet Explorer software). However, hackers have a history of exploiting ActiveX controls to gain backdoor access, so the technology is deemed insecure, even if secure implementations are possible by all means.

Back to the Software Client

The technical limitations listed above have led an increasing number of companies to develop specialized SSL software clients with full network access which allow for flexible and convenient operations within a familiar environment. Ironically, this change of mind boosted installation efforts, as access had to be configured individually, quite contrary to the developers' original attempt of avoiding complexity by introducing SSL VPNs.

For this reason, many vendors followed a different approach. Astaro Corporation, for instance, has coined the term "One-Click VPN" for its Astaro Security Gateway V7 (ASG) Unified Threat Management appliance, combining a set of security technologies in a fully integrated solution. ASG combines firewall and intrusion prevention systems, filters viruses from mail traffic, blocks spam and phishing attacks, and encrypts email messages automatically.

Similar to this approach, remote access is handled accordingly when enabling connectivity to company networks, with the ASG leveraging the full scale of protocols outlined before. There are two software packages included in the gateway, Astaro Secure Client and Astaro SSL VPN Client, the latter being our primary interest.

This software is based on James Yonan's Open VPN Client which is available for free. Astaro SSL VPN Client utilizes the latest advancement of the TLS protocol (version 1.1) to initiate authentication and encryption of all internet applications. Apart from Windows, the client supports Linux, MacOS X, Solaris, plus several BSD variations, a multitude of connection options (DSL, UMTS, etc.),

and dynamic allocation of IP addresses. The software is unique in allowing hassle-free installation directly on the gateway. The administrator merely needs to configure VPN user accounts and assign appropriate access rights as usual. Users then simply need to log into a portal directly residing on the gateway, in order to receive individual download packages, including client software, keys, certificates, and configuration files respectively. This portal also provides installation help files and necessary updates.

After downloading the software, users find a ZIP data file on their computers which includes a setup wizard. By double-clicking the icon, the installation routine starts automatically. After successful installation, the task bar contains a new VPN client icon. By double-clicking again, a log-in screen opens up where users enter user ID and password – done. Using the solutions integrated in Windows would be even simpler, of course, but in heterogeneous networks this is not an option due to the security concerns discussed before (susceptible to outside attacks, complex installation). For existing ASG customers, Astaro's SSL client solution is offered at no additional cost.

Conclusion

Generally speaking, client-based SSL VPN solutions offer a valid alternative to conventional remote access software. Factors like platform-independent design and fully transparent data and application access work in favor of this approach and more than offset the additional installation efforts. Astaro's solution is characterized by its range of features, but above all by the software's efficient and convenient means of distribution. As a cost-free solution, economic benefits are added to the technological advantages, making it an ideal completion to existing site-to-site VPNs.

Contact



Europe, Middle East, Africa

Astaro AG
Amalienbadstrasse 36
76227 Karlsruhe Germany
T: +49 721 255 16 0
F: +49 721 255 16 200
emea@astaro.com

www.astaro.com

The Americas

Astaro Corporation
3 New England Executive
Park
Burlington, MA 01803
USA
T: +1 781 345 5000
F: +1 781 345 5100
americas@astaro.com

Asia Pacific Region

Astaro K.K.
12/F Ark Mori Building
1-12-32 Akasaka Minato-ku
Tokio 107-6012, Japan
T: +81 3 4360 8350
apac@astaro.com

This document may not be copied or distributed by any means, electronically or mechanically, in whole or in part, for any reason, without the express written permission of Astaro AG.

© 2008 Astaro AG. All rights reserved. Astaro Security Gateway, Astaro Command Center and WebAdmin are trademarks of Astaro AG. All further trademarks are the property of their respective owners. No guarantee is given for the correctness of the information contained in this document.