



IPSec vs SSL Virtual Private Networks

- an eB2Bcom White Paper



Date: 19 August 2005

Version: 1.0

Prepared By: eB2Bcom Pty Ltd
Suite 3, 935 Station St
Box Hill Nth, Vic 3129 Australia
Phone: +61-39896 7800
Fax: +61-39896 7801

DOCUMENT DETAILS

Author: Lisa Vuu BA InfoSys Phone: +61 3 9896 7800

DOCUMENT SECURITY

This document contains intellectual property of eB2Bcom, and is provided on a COMMERCIAL-IN-CONFIDENCE basis to the party ("Client") named on the front page. It is solely for the use by the staff of Client for the consideration and evaluation of eB2Bcom's proposals. It must not be provided in whole or in part to third parties without the express approval of an authorised officer of eB2Bcom.

REVIEW

Reviewed by: Alistair Nelson, Andrew Sciberras, and Trevor Hancock eB2Bcom

DOCUMENT HISTORY

Version	Comment	Date
0.1	First draft – Lisa Vuu	09 August 2005
0.2	Second draft – Andrew Sciberras	11 August 2005
0.3	Third draft – Andrew Ferguson	13 August 2005
0.4	Fourth draft - Teow Hin	17 August 2005
0.5	Fifth draft – Rene Poot	18 August 2005
1.0	Approved – Andrew Ferguson	19 August 2005

TABLE OF CONTENTS

DOCUMENT DETAILS	2
DOCUMENT SECURITY	2
REVIEW	2
DOCUMENT HISTORY	2
TABLE OF CONTENTS.....	3
CREDENTIALS.....	4
BACKGROUND	4
INTRODUCTION.....	4
WHAT IS A VPN?.....	5
TYPES OF VPN	5
3.1 SSL	5
3.2 IPSec	5
ADVANTAGES AND DISADVANTAGES	7
4.1 IPSec VPN	7
4.2 SSL VPN	8
COST COMPARISON	9
HOW TO CHOOSE - RECOMMENDATION	9
CONCLUSION	9
REFERENCES.....	10

CREDENTIALS

eB2Bcom specialises in security, identity management, and associated infrastructure. We are an established provider of software and services to Defence, Intelligence, Police and Government Agencies as well as the private sector. eB2Bcom has offices and works with a range of partners throughout South East Asia, Australia and New Zealand.

BACKGROUND

This eB2Bcom White Paper attempts to provide the reader with an explanation of modern Virtual Private network (VPN) technologies and attempts to explain the advantages and disadvantages in the deployment of IPSec (Internet Protocol Security) versus SSL (Secure Sockets Layer) VPN technology.

INTRODUCTION

An organisations data communications strategy is no longer just an option in today's highly competitive business environment. It has become a necessity. Connecting remote users to corporate resources – securely- is not a new problem for IT. But today's end users with changing work styles, new computing and communication devices and ever increasing expectations are driving demand for expanded remote access. Therefore communication channels connecting remote offices, mobile users and business partners are essential to the efficient and effective functioning of organisations.

Virtual Private Networks (VPNs) enable a range of individuals to securely communicate over the wide area through one or more data networks. (Odhner, 2003)

The two competing VPN options that businesses of today choose to implement are Internet Protocol Security (IPSec) and Secure Sockets Layer (SSL) virtual private networks. IPSec and SSL are both encryption protocols that protect IP based data streams over any IP network. Both IPSec and SSL can provide secure access to network applications and both have their own unique features, strengths and limitations. IPSec is a protocol all on its own. SSL VPNs on the other hand make use of HTTPs which is TCP based.

This paper describes two VPN solutions –IPSec and SSL VPNs. This paper takes a balanced approach in comparing both VPNs in terms of advantages and disadvantages.

WHAT IS A VPN?

A VPN is a secure private data network that makes use of a public network, such as the Internet, to connect company resources or remote sites. VPNs use the Internet as the means to provide connectivity and to eliminate the high cost of using dedicated private networks based on leased lines while still providing the security and functionality that organisation require.

By capitalising on the ubiquity of the public Internet, VPNs eliminate "private" network, access costs and represent a cost effective, secure networking alternative to expensive dedicated networks.

TYPES OF VPN

The two main competing VPN options used today are IPSec and SSL VPNs. Essentially IPSec and SSL are encryption and authentication technologies designed for data transit. Both VPN types deliver secure, enterprise-level remote access, but their architectural and operational approaches differ considerably. These differences should be considered when choosing a VPN as well as factors such as organisation overall security architecture and network security policy.

Originally SSL VPNs were suppose to compensate for the shortfalls of IPSec VPNs; installation of client software and complex client configuration or administration.

3.1 SSL

SSL was originally developed by Netscape communication for the World Wide Web (WWW) who aimed to provide a single solution for all their communication problems including web, mail and new traffic. SSL works by using a public key to encrypt data that is transferred over the SSL connection. It is an open standard web protocol that offers privacy, server and client authentication and message integrity over TCP/IP connection. SSL was designed specifically to secure the HTTP protocol. SSL is a higher-layer security protocol, sitting closer to the application. This close connection to application layers means that compared to IPSec, SSL can more easily provide the granular access control that remote access and extranet VPNs require. IPSec is part of the network protocol in the lower network layer.

Most browsers support SSL, and many websites use the protocol to obtain confidential user information, such as credit card numbers. IPSec requires specific client software while SSL uses any SSL enabled browser as the client. The key success of SSL is its mobility because it only has to rely on the browser.

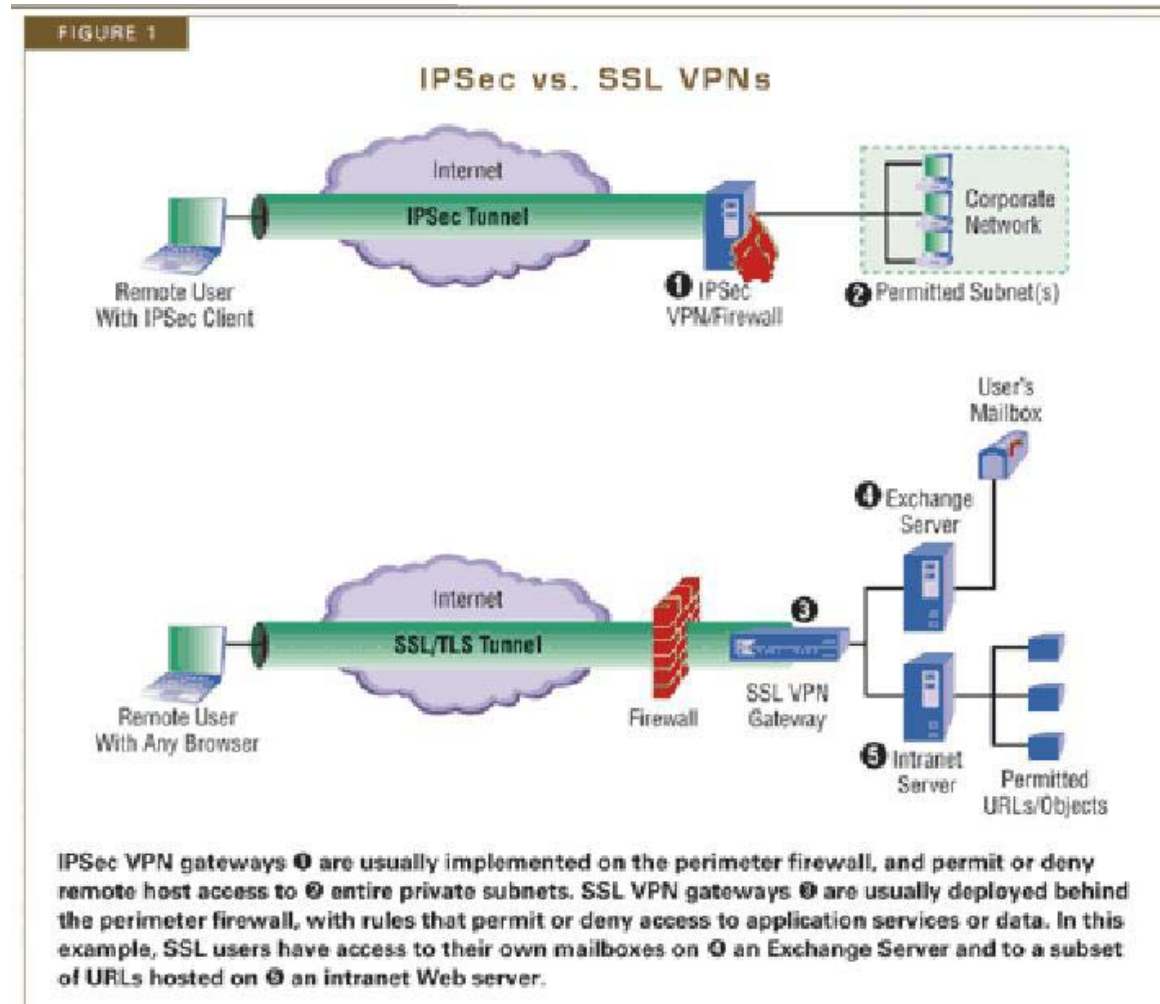
3.2 IPSec

IPSec is a series of protocols developed by the Internet Engineering Tasks Force (IETF) to deliver symmetric key encryption and authentication services at the IP layer. It offers organisations a great amount of flexibility in supporting network configurations and application.

IPSec VPNs operate at the network layer of the Open System Interconnection (OSI) network architecture model. IPSec VPNs use the IPSec protocol to provide secure exchange of IP packets. Typically these devices sit between the public and private network at both ends of the communication points. But can also be utilised to

provide secure internal LAN traffic. Information sent from the private network passes through the device, where it is encrypted, sent over the public network and accepted by the remote side. These days, IPSec solutions have powerful central management. This means that each application must be confirmed and adapted relative to its SSL VPN capability.

Figure 1 - Comparison between IPSec and SSL.



Source: TechTarget

ADVANTAGES AND DISADVANTAGES

4.1 IPsec VPN

4.1.1 Advantages

IPsec VPNs are no longer generally best suited to just site-to-site connections that require large, constant data transfers and provides seamless remote access for end users. IPsec has been expanded with numerous different "additions" that allow it to be used in a remote access environment with dynamically assigned IP addresses.

IPsec VPNs eliminate "private" network access costs and represents a cost effective, secure networking alternative to expensive dedicated networks.

IPsec offers flexibility and support for offline work. Users with laptops can connect back to the company network provided they have a connection to the Internet.

Another advantage of IPsec is the seamless experience for accessing files and Internet sites. A remote user has seamless access to email, files and Intranet sites from their PC if the IPsec VPN is properly implemented. "Network drives can be mapped directly into the end users computer, providing for integrated access to network-based files from any application as if they are physically in the office and connected to the LAN.

Currently vendors are able to provide better solution where the client dictates what type of data is permitted and what type of data is denied to travel through the VPN tunnel through a personal firewall which is dynamic and adapts to different situations. Also clients must not allow traffic originating from other sources to be routed through the client to the remote network.

4.1.2 Disadvantages

A main drawback with IPsec is the hidden costs where initiating an IPsec connection is not as easy as launching a web browser (the mechanism for SSL based VPNs). With an IPsec VPN, the Information Technology Department personnel must install and maintain individual VPN clients on each PC from which a user needs access, and changes to the desktop may be required, although with some VPN software vendors the possibility exists to do remote administration and configuration without the need to do individual changes to the desktop. This is sometimes called EndPoint configuration and security.

In some cases IPsec VPNs can increase security risks when they are used to extend company resources to remote users. These concerns means IPsec VPNs can be prone to vulnerability when IT administrators choose non PKI certificate options such as password or tokens for authentication rather than using Public Key Infrastructure (PKI) certificates for dual factor authentication where the use of the certificate requires knowledge of a secret PIN.

Companies run the risks that crackers can use the remote IPsec VPN network tunnel to gain unauthorised access to the corporate network. IPsec establishes and authenticates a network link but doesn't establish an identity of the user. However IPsec combined with PKI overcomes this issue (as long as the end user keeps their PKI certificates secret). (Note many PCs and PDAs today have security and encryption software loaded which require pre-boot or signature based authentication

to re-enforce the end point security. Thus IPsec **with PKI** and **local encryption** for remote users can be extremely secure.

4.2 SSL VPN

4.2.1 Advantages

SSL has emerged as the leader in the remote access VPN space. However the increasing attention on SSL VPNs does not eliminate the value of traditional IPsec VPN solutions.

Without the burden of configuring, managing, and supporting complex IPsec clients for each user, SSL VPNs are easier and less expensive to support and are faster to deploy than IPsec VPNs. Therefore little training is required, even the least technically savvy end user is immediately comfortable using a browser. Furthermore, SSL is also included in standard browsers like Microsoft Internet Explorer and Mozilla FireFox.

There is increased security with SSL because end user access to any given resource is restricted unless authorised. SSL VPNs provide a secure, proxied connection to only those resources the user is authorised to access. This lack of a direct network connection, combined with split tunnelling in which users have access to the Internet and corporate resources at the same time tend to be safer.

SSL is also easy for IT and end users because ongoing administration is simpler with an SSL VPN than with an IPsec VPN. Also SSL does not require complex or intrusive clients i.e. installation of software on end user computers, which means easier installation, maintenance, and higher cost savings. Also SSL VPN is ideal when the user could be a casual access user for instance from an airport departure lounge or Internet café where use of personal tokens would be impossible or extremely dangerous from a security point of view. For some application and situation casual access may be fine but for other important situation this would not be a good idea.

SSL also when combined with Mobile security (one time passwords issued by Secure SMS) can be an effective way to allow secure access to remote users.

4.2.2 Disadvantages

One downside of most SSL VPN solutions is that they provide access only to web applications, while failing to address the needs of companies whose users require access to client/server applications. If Internet connectivity is not available, the remote user will not have an independent means of getting work done. While failing to address the needs of companies whose users require access to client/server application.

Web enabled SSL VPN connections have most problems when it comes to using PKI based authentication schemes especially when it comes to two factor authentication. However most vendors push this as being an issue that has to be dealt with by the browser not the SSL VPN.

When using an SSL VPN, one also has an insecure connection to the Internet. This means that the remote access user's machine is vulnerable to attack.

COST COMPARISON

When comparing the range of costs associated with IPSec and SSL VPNs, administrators should base their assessments on the costs at both the host and remote site. In general there are three cost categories to consider for each respective VPN type: equipment costs, deployment costs and ongoing support costs.

An organisation must consider the up-front capital cost of the networking equipment required for successful deployment. IPSec and SSL VPNs both require equipment at the hub location to terminate the encrypted tunnels from the network location. The cost of hub location servers and VPN gateways is typically higher for SSL VPNs than it is for IPSec VPNs. But IPSec VPNs with their high maintenance and deployment requirements lead inevitably to a high cost solution.

HOW TO CHOOSE - RECOMMENDATION

Whether an SSL or IPSec is the right choice for a company really depends on the organisational needs. Traditional IPSec VPN technology is designed for site-to-site VPNs and does the job well. SSL VPN technology on the hand, works much better for secure remote access and extranet implementation.

A careful examination of the data being transferred, its level of sensitivity to the organisation, and the impact of unauthorised disclosure are key factors that should be considered when deciding between which architecture to use when implementing a VPN. Certain types of businesses with specific goals for employees and customers, however, will find one more beneficial than the other. For some situation the use of an IPSec based VPN is too much for an organisation and for other situation, SSL VPNs might not be sufficient.

The organisation must examine as many aspects of the various technologies and their associated costs as possible. These elements include initial capital outlay, deployment, ongoing maintenance & support, security, flexibility and scalability with the weight of each category varying by enterprise and specific wide area data communications needs.

CONCLUSION

Deciding between IPSec Vs SSL VPN is not the appropriate question. Both are often necessary to support the different types of work that must be done. Choosing the right solution that enables employees to be productive while working remotely in a secure environment is the important decision. Whether an SSL VPN is the right choice for a company really depends on the enterprises needs.

Both compliment each other and should not really be viewed as "one or the other". Different requirements require different solution. The IPSec VPN offers a transparent solution offering a true network connection which is the role of the VPN. On the other hand, SSL VPNs have another approach and does not offer a network connection and instead offers a secure interface that allows users to access resources.

REFERENCES

Bradley. T (2003) "**VPN's: IPSec vs SSL – Which Technology Is Right For You?**"
November 2003

Clayton, N (year) "**VPN over IPSec**"

Lynch, D (2004) "Following Protocol", SC Magazine, 29th September 2004

Odhner. N, (2003) "**Face Off: IPSec vs SSL VPN's**", Faulkner Information Services

Sorensen. E, Bregman, T, (2004) "**How to Choose IPSec or SSL VPN's**" MCI

Van, D (2001) "**SSL VPN vs IPSec VPN: A Study and Comparison**" Xceedium,
Inc.

Aventail (2004) "**Comparing Secure Remote Access Options: IPSec VPNs vs
SSL VPNs**"

Positive Networks (2002) "**IPSec Vs SSL VPNs – Don't choose**", November



Sydney: +61-2-9779-1597
Melbourne: +61-3 -9896-7800
Brisbane: +61-7-3871-1440
Singapore: +65-6841-7374
email: sales@eb2bcom.com
Web: www.eb2bcom.com