

A Comparison of VPN Solutions: SSL VS IPSec

A Netilla Networks White Paper



Netilla Networks, Inc.

347 Elizabeth Avenue

Somerset, NJ 08873

Phone: 732.652.5200

Fax: 732.764.8862

www.netilla.com

Part No.3.0.2.5.02 V 3.1.2.NR



Table of Contents

INTRODUCTION	3
WHAT IS A VPN?	3
<i>What are Cryptographic Protocols?</i>	3
WHAT IS AN IPSEC VPN?	3
IPSEC DRAWBACKS	3
TOP 4 IPSEC VPN OBSTACLES	4
1. <i>Client Software is Required</i>	4
2. <i>IPSec VPNs are IT Resource Intensive</i>	4
3. <i>Performance Drawbacks</i>	4
4. <i>Security Concerns</i>	4
WHAT IS AN SSL VPN?	5
WHAT IS AN SSL PROXY?	5
<i>SSL Proxies Provide Authentication</i>	5
<i>SSL Proxies Provide Increased Security</i>	6
WHY SSL PROXIES ARE A BETTER CHOICE	6
<i>Client free remote access</i>	6
<i>Easy to use and support Web interface</i>	6
<i>End-to-End vs. End-to-Edge Security</i>	6
<i>Extended Remote Access</i>	6
<i>Centralized Application Use Further Reduces IT Support Costs</i>	6
SSL VPN and IPSec VPN Comparison	7
WHICH TECHNOLOGY IS RIGHT FOR ME?	7
<i>SSL vs. IPSec VPN Considerations</i>	7
SUMMARY	8
FOR MORE INFORMATION, CONTACT NETILLA NETWORKS:	8
<i>Domestic U.S.: 877-Netilla</i>	8
<i>International: 732-652-5200</i>	8

Introduction

Traditional remote access approaches - such as leased lines and dial-up remote access servers (RAS) - have fallen out of favor for many reasons. Chief among these are deployment complexities, high phone charges, poor security implementations, and ongoing maintenance costs. These reasons have led many organizations to consider alternatives.

As a result, Virtual Private Networks (VPN) have emerged as the logical choice for providing cost effective, secure access to corporate resources from a remote location. VPNs allow organizations to extend access to internal networks for external employees and partners over standard Internet public networks, reducing private network and dial-up phone communication costs. With this approach, mission-critical corporate applications and data are made available to authorized users regardless of location.

A common misconception is that VPNs are always based on the Internet Protocol Security (IPSec) protocol. In fact, there are many encryption and security protocols that are used to secure the connection between remote users and the enterprise network. This paper describes the top two competing VPN solutions – traditional IPSec (Internet Protocol Security) VPNs and Web-based, application layer SSL (Secure Sockets Layer) VPNs.

What is a VPN?

A VPN is a secure, private connection that uses the Internet - a public network - to connect remote sites or users to company resources. VPNs employ various data protection technologies via a virtual “tunnel” between the client and the network. VPNs, in essence, use the Internet as an inexpensive transport bridge to eliminate the high costs once associated with using dedicated private networks based on leased lines, ATM or frame relay, while still providing the security and functionality that enterprises require. By capitalizing 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.

What are Cryptographic Protocols?

Cryptographic protocols are security protocols that use encryption – the process of using mathematical techniques – to encode data to ensure privacy. SSL and IPSec are cryptographic protocols that are used to transmit data securely.

Encryption, the core of any security protocol, provides three fundamental advantages over ‘clear-text’ or unencrypted data:

- **Data privacy:** The ability to hide the data that is being transmitted.
- **Data authenticity and integrity:** The ability to ensure that data has not been modified or damaged.
- **Non-repudiation:** The ability to prove an act occurred.

What is an IPSec VPN?

IPSec is the security protocol once commonly associated with a VPN. As an encryption protocol, IPSec provides for secure encrypted data transmission at the network layer across the Internet. Two parties who wish to create an IPSec tunnel must first negotiate on a standard way to communicate. Since IPSec supports several modes of operation, both sides must first decide on the security policy and mode to use, which encryption algorithms they wish to communicate with, and what type of authentication method to use. Once an IPSec tunnel is created, all protocols - such as TCP, UDP, and HTTP - are encrypted between the two communicating parties regardless of whether or not they have built in security and encryption.

IPSec VPNs operate at the network layer (layer three) of the Open System Interconnection (OSI) network architecture model. By operating at the network layer, IPSec VPNs allow clients to securely access a corporate network as if the remote client was located in the office, affording the same level of access from remote locations.

IPSec Drawbacks

Because IPSec operates at the network layer, all network traffic is encrypted, but the user also gains access to all company resources as if they were physically resident in the office connected to that LAN. You may or may not want partners or temporary remote employees to have total access

to your network. You may only want to expose a small portion of the enterprise resources to remote users. And, you may not want to encrypt everything from the remote client to the corporate network.

IPSec VPNs are thus best suited for site-to-site connections that require large, constant data transfers. They are also a good choice for tying remote LANs together over distances where network access is limited to IT-controlled personal computers (PCs). However, when used for distributed users that need access to centralized applications from numerous remote locations, and when access is required from PCs that are not easily accessible by IT staff members, IPSec VPNs can present significant obstacles.

Top 4 IPSec VPN Obstacles

1. Client Software is Required

IPSec requires special-purpose client software, which in most cases replaces or augments the client systems TCP/IP stack. In many systems this introduces the risk of compatibility issues with other system software as well as the security risk of Trojan Horses being loaded - especially if the client software is downloaded through the Web and not installed by an IT staff member. Because of the way IPSec was created - generally lacking conformance to a standard - nearly all IPSec implementations are not compatible with each other.

Installing software to geographically dispersed users or remote workers only adds to the deployment challenge. IT staff must not only install and maintain VPN clients, but their responsibilities extend to the actual software applications themselves.

In some cases IPSec runs on a network hardware appliance. In many cases, these types of solutions require both sides to have the same hardware to communicate with each other. The same compatibility issues with the client software apply to the IPSec enabled hardware.

IPSec clients are bound to a specific laptop or desktop system. This limits the mobility of the users, as they cannot connect to the VPN without an IPSec client first being loaded on

the client system they use to access the network.

2. IPSec VPNs are IT Resource Intensive

IPSec VPNs are IT-resource intensive for both implementation and long term maintenance. Individual VPN clients must be installed and maintained on every PC that requires access, and each remote client must be reconfigured every time the corporate network grows or changes its access approach.

IPsec VPNs impose IP address administration burdens on the VPN Administrator that are not inherent in an SSL-based solution, such as Netilla's. In an IPSec environment, administrators must worry about whether IP addresses are dynamically or statically assigned, from what IP address pool, and how routing and security policies are affected by such assignment.

For an organization with hundreds or thousands of remote users, managing a field of such clients is a significant undertaking, particularly when an IT staff does not have easy access to remote sites or PCs. Large corporations are often forced to designate several helpdesk personnel specifically devoted to supporting their IPSec-based remote employees.

3. Performance Drawbacks

An IPSec VPN does little to alleviate or circumvent the bandwidth constraints typical of most remote users. In practice, VPNs are processor-intensive and bandwidth-heavy. Moreover, access can be slow, even with cable and DSL connections. The overhead associated with IPSec eliminates some of the broadband advantages end-users have come to expect.

4. Security Concerns

When IPSec VPNs are used to extend company resources to remote users, security itself becomes a concern. IPSec VPNs lack support for asymmetric client authentication based on tokens or mainstream challenge-response methods that many enterprise customers have implemented.

While a VPN may satisfy security requirements for sending information over the Internet, the source data itself, often residing on laptops or other remote devices, remains vulnerable to loss and theft. With over one million laptops stolen each year worldwide, businesses cannot afford to have mission-critical data and proprietary applications residing on every PC that accesses the network.

Worse yet, because they operate at the network level, IPSec VPNs effectively provide the remote PC with full network visibility as if it were a computer located on the corporate Local Area Network (LAN). Consequently, there is no easy way for network administrators to control or monitor where users go or what they see. Hackers who use the remote VPN connection to gain unauthorized access to corporate network resources can exploit this hole to visualize the network topology, and possibly gain access to the network.

What is an SSL VPN?

Secure Sockets Layer (SSL) is an application layer protocol used most often to secure web-based communications over the Internet. SSL provides server authentication, data encryption and message integrity, typically over TCP/IP connections. Since originally developed by Netscape to secure electronic commerce transactions, SSL - also referred to as IETF standard Transport Layer Security (TLS) - has evolved into one of the leading security protocols throughout the Web. The integrated security afforded by SSL ensures confidence in business-critical data transfers. As a result, SSL has become the de facto standard for supporting private transactions such as credit card purchases and online stock trading and banking.

SSL uses encryption and authentication much like IPSec. However, SSL only encrypts the traffic between the two applications that wish to speak to each other. This contrasts IPSec, which operates independent of the application. SSL does not encrypt all the traffic from one host to another. For most client applications, encrypting all of the traffic from one system to another is not required, and a solution that just encrypts the application data is more appropriate.

An application must be “SSL aware” to be able to speak SSL. Common applications, which are “SSL aware” today, are Web browsers such as Internet Explorer and Netscape; email applications such as Outlook and Eudora include a feature called ESMTP or SMTP over SSL.

An SSL VPN uses the SSL protocol to access a private network via the Internet. An SSL VPN

functions as an “application layer” VPN that operates at layers four through seven of the OSI model. By operating at the application layer, SSL VPNs provide visibility into application data, affording network administrators new opportunities to enforce security policy before the user’s traffic reaches the application server at the data center. In this way, remote clients are allowed access only to the applications and services they are authorized to use, as opposed to the entire subnet.

What is an SSL Proxy?

An SSL proxy is an SSL-enabled network appliance that serves as a buffer between the public Internet and a private network. An SSL proxy allows for careful control of information between the public Internet and the private network-located servers. Using an SSL proxy - rather than communicating directly from a client to an SSL-enabled resource - provides both authentication and increased security, as explained below.

SSL Proxies Provide Authentication

The traditional SSL protocol lacks built-in authentication methods. SSL does include cryptographic authentication for both the server and the client. However, all of that security is based on one premise: The client’s cryptographic “private-key” was kept secure. If the key has been compromised or left unattended, the client may no longer be trusted. It may be necessary to add additional authentication methods on top of SSL to ensure the user or client is who they say they are.

An SSL proxy, however, strongly authenticates the clients before they are allowed to connect to the back end resource. Many web servers today do not natively support authentication methods other than SSL. SSL proxies therefore enforce much stronger authentication methods than a backend resource could ever support natively.

For instance, the Netilla Security Platform (NSP), an SSL VPN appliance from Netilla Networks, provides organizations with a vehicle to “enforce” strict access policies that control how and when a remote user gains access to an enterprise domain within the enterprise perimeter. Netilla’s SecureRealm™ architecture integrates authentication, authorization, and policy building blocks to control access on an individual, role, or group basis. Netilla’s dynaTRUST™ operating system builds on this policy enforcement

architecture to enable the real-time provisioning of “dynamic trust” privileges that are based on the identity, entitlements, and endpoint integrity of the user and/or service.

SSL Proxies Provide Increased Security

The SSL VPN proxy protects internal resources by ‘intermediating’ the connection between remote client requests and server-based applications, terminating incoming connections from the remote user at the application layer. By analyzing terminated-application information and enforcing the appropriate security policy, an SSL proxy acts as a secure “sentry” between the public Internet and the enterprise network. An SSL proxy can poll external authentication and policy servers - such as Active Directory - and validate user credentials to authorize specific application access.

Once a user is granted access, the SSL proxy processes and translates the data to the appropriate backend application protocol such as:

- Remote Desktop Protocol (RDP) for Windows applications residing on Windows Terminal Servers.
- X.11 over SSH for UNIX or Linux applications.
- 3270 over Telnet for mainframe and AS/400 applications.
- HTTP/HTTPS for web servers.

Why SSL Proxies are a Better Choice

Client-free Remote Access

A key advantage to an SSL proxy is that neither hardware nor client software is needed for the remote user base. SSL proxies can use standard Web browsers and email clients, which are already enabled to use SSL.

Web-based Interface

Web browsers and SSL-enabled email clients exist in many form factors today; Windows PC’s, Macintosh computers, Linux/UNIX clients, PDAs and even cell phones all can communicate securely via SSL. Little training is required; even the least technically savvy end user is immediately comfortable using a browser.

End-to-End vs. End-to-Edge Security

One of the major disadvantages of IPSec is that it only creates a secure tunnel between a client and an edge VPN Server. When a client requests access to a resource the client is treated as if it were a member of that same network in which the resource resides. The only secure connection is the one between the client and the edge of the corporate network; however all the data running over the internal network is in the clear, including any passwords and sensitive data that are sent.

With an SSL VPN, a secure tunnel is established directly from the client to the resource that the client is accessing. No data is sent in the clear neither on the internal network nor on the Internet. Everything from the client to the resource is securely authenticated and encrypted.

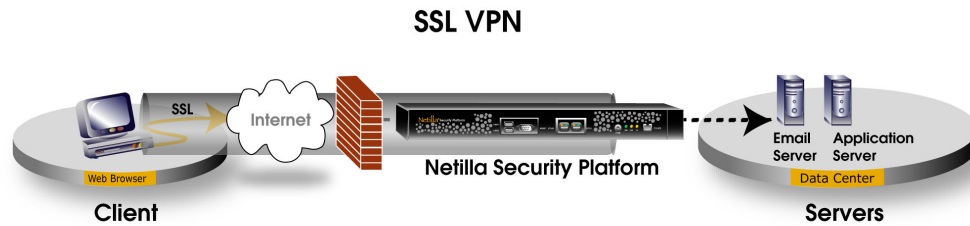
Extended Remote Access

Because SSL VPNs operate on top of TCP/UDP transports, SSL can traverse Network Address Translation (NAT) devices easily, without requiring router reconfiguration, thereby extending remote access to a wider range of network resources from any authorized client with a standard Web browser.

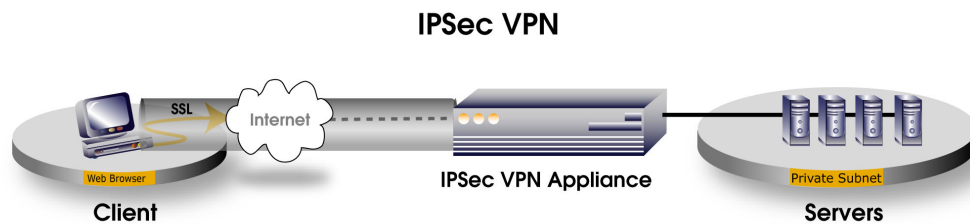
Centralized Application Use Further Reduces IT Support Costs

With SSL VPN appliances, users are not required to have applications or clients installed on their local machine. By centralizing applications in the data center, enterprises realize further reductions in IT support costs, while enhancing security and further extending business-critical applications and data. IT departments are not required to install, update and maintain applications at every remote desktop; instead, users access necessary applications remotely.

SSL VPN and IPsec VPN Comparison



SSL VPNs provide secure end to end communications. Client requests to the Netilla Security Platform are sent via SSL. The Netilla Security Platform verifies that the client is authorized to access the requested resource and obtains the requested information over a secure connection to the private server providing end to end security from the client to the remote server.



IPsec VPNs provide secure communications from the client to the edge of the private network. Upon proper authorization, a client is granted access to the entire private subnet. Data running over the private network is in clear text including passwords and other sensitive data.

Which technology is right for me?

The following table lists the main considerations for decision makers regarding various types of VPNs, and includes the capabilities and limitations of SSL and IP Sec-based VPNs for each of these key criteria.

SSL vs. IPsec VPN Considerations

Key Criteria	SSL VPN Features	IPsec VPN Features
Authentication Supported	<ul style="list-style-type: none"> - One way authentication tokens - Two way authentication tokens - Digital certificates 	<ul style="list-style-type: none"> - Two way authentication using tokens - Digital certificates
Encryption	<ul style="list-style-type: none"> - Strong Encryption - Browser based 	<ul style="list-style-type: none"> - Strong Encryption - Depends on implementation
Overall Security Coverage	<ul style="list-style-type: none"> - End to End security - Client to Resource encrypted 	<ul style="list-style-type: none"> - Edge to client - Client to VPN gateway only encrypted
Accessibility	<ul style="list-style-type: none"> - Anywhere anytime access to broadly distributed user base 	<ul style="list-style-type: none"> - Access limited to well-defined and controlled user base
Access Control	<ul style="list-style-type: none"> - Access is controlled per user and granted only to specific ports, URLs or applications on the private server 	<ul style="list-style-type: none"> - Access granted to trusted users to entire private server
Cost	<ul style="list-style-type: none"> - Low - No additional client software needed 	<ul style="list-style-type: none"> - High - Managed client software required

Installation	<ul style="list-style-type: none"> - Plug and play installation - No additional client-side software or hardware installation 	<ul style="list-style-type: none"> - Often long deployments - Requires client-side software or hardware
Simplicity for user	<ul style="list-style-type: none"> - Very user friendly - uses familiar Web browsers - No end user training required 	<ul style="list-style-type: none"> - Challenging for non-technical users - Requires training
Client Software Required	<ul style="list-style-type: none"> - Standard Web browser 	<ul style="list-style-type: none"> - IPSec client software
Applications Supported	<ul style="list-style-type: none"> - Web-enabled applications - Legacy applications (Windows, UNIX, Linux 3270 Mainframe and 5250 AS/400) - Desktop client/server connection via SSL tunneling - File sharing - E-mail 	<ul style="list-style-type: none"> - All IP-based services
Scalability	<ul style="list-style-type: none"> - Easily deployed and scalable 	<ul style="list-style-type: none"> - Scalable on server side - Difficult to scale clients
Users	<ul style="list-style-type: none"> - Customers, partners, employees, remote users, vendors etc 	<ul style="list-style-type: none"> - More suited for internal company use

Summary

This white paper examined the major differences between IPSec based VPNs and SSL based VPNs, and explored the advantages and disadvantages of each. Choosing a remote access strategy is often not based not on the superiority of one technology over another, but rather deciding which solution best fits the needs of your organization.

For more information, contact Netilla Networks:

Domestic U.S.: 877-Netilla
International: 732-652-5200

www.netilla.com
info@netilla.com

Copyright ©Netilla Networks, Inc. 2003
All rights reserved. Use, duplication and disclosure are subject to restrictions.

Netilla Networks, Inc. is the sole proprietor of this document and the material contained herein. This document, or any parts hereof, may not be reprinted or reproduced in any form, by any method, without written permission. For conditions of use and/or reproduction, or permissions to use these materials for publication, contact Netilla Networks, Inc.

Netilla Networks, Inc. reserves the right to revise and improve its products and manuals as it deems necessary. This document provides an accurate description of the product at the time of printing, and may not necessarily be accurate for future releases.

Trademarks
Netilla Networks and the Netilla Stylized figure are registered trademarks and dynaTRUST is a trademark of Netilla Networks.