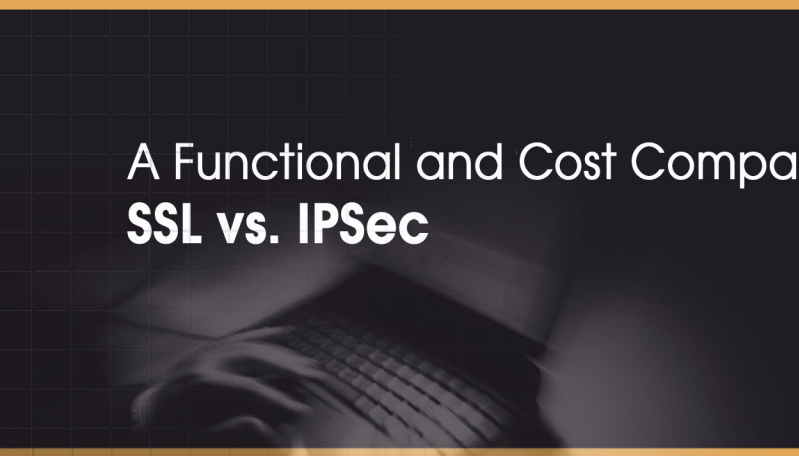
A Functional and Cost Comparison of VPN Solutions: **SSL vs. IPSec**



Netilla®
Making the remote accessible

Netilla Networks, Inc.
347 Elizabeth Avenue
Somerset, NJ 08873
Phone: 732.652.5200
Fax: 732.764.8862
www.netilla.com

Table of Contents

Introduction

The increasing demand for secure corporate data exchange over the Internet is driving an exploding market for Virtual Private Networks (VPNs). This need for secure transmissions is being fueled by federal regulations such as the Health Insurance Portability and Accountability Act (HIPAA) for the healthcare industry and the Gramm-Leach-Bliley Act for financial transactions. These regulations require organizations to safeguard the privacy of electronic information. In addition, the trend towards decentralized facilities and the growth of mobile workforces increases the need for secure access to company data. The virtualization of the enterprise is underway, and VPNs are helping to make the new business landscape more secure and trusted.

The numbers are impressive: According to International Data Corporation (IDC) research, the VPN product market, excluding services, will grow from $5 billion in 2001 to $9.7 billion by 2005, representing a four year Compound Annual Growth Rate of 18%. As these numbers show, VPNs are poised for dramatic growth.

At the same time, shrinking Information Technology (IT) budgets and reductions in management information systems (MIS) staff are challenging IT departments to do more with less. Given this dilemma, companies must find solutions that ensure utmost security with maximum functionality while limiting Total Cost of Ownership (TCO).

Traditional remote access approaches—leased lines, dial-up remote access servers (RAS), and client/server-based computing—have proven inadequate to the task. Phone charges, poor security implementations, deployment complexity, ongoing maintenance costs, lack of scalability and bandwidth limitations have led many corporations to consider alternatives.

As a result, Virtual Private Networks (VPN) have emerged as the logical choice for extending corporate resources securely and cost effectively. VPNs allow an organization to reduce private network and dial-up phone communication costs, while making mission-critical corporate applications and data available to authorized users regardless of location.

This paper describes two VPN solutions—traditional IPSec (Internet Protocol Security) VPNs and Web-based, application layer SSL (Secure Sockets Layer) VPNs. When the critical elements—including initial deployment costs, help-desk time, end-user training, and ongoing IT maintenance—are considered, we will show that the SSL Web-based approach emerges with a significant TCO advantage.

Overview: What is a VPN?

Essentially, a VPN is a secure, private connection that uses a public network, such as the Internet, 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 cost of 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.

VPNs fall into several categories. Some VPNs use IPSec and operate at the network layer (layer three) of the Open System Interconnection (OSI) network architecture model. Other VPNs use SSL technology, and function as "application layer" VPNs that operate at layers four through seven of the OSI model. While both VPN models leverage the Internet, the SSL application layer approach offers compelling cost and ease-of-use benefits over IPSec-based networks.

IPSec VPNs: Distributed Complexity for Remote Access

IPSec VPNs use the IPSec protocol to provide secure exchange of IP packets. An IPSec-compliant device can be either hardware or software based. Typically, these devices sit between the public and private network at both ends of the communication points. 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.

IPSec VPNs are 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, IPSec VPNs present significant drawbacks.

High Maintenance, Hidden Costs

Ironically, the very nature of a remote access VPN—providing secure access to distributed users at numerous remote locations—introduces a new set of deployment and maintenance concerns that threaten to undermine the potential savings promised by IPSec-based VPN implementations.

For one, IPSec VPNs are IT-resource intensive. 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. 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. Consider a physician's office that needs secure access to a hospital network. Configuring and managing VPN clients at each caregiver's remote computer in this extranet deployment leads to a strain on MIS resources that few organizations can bear.

Initiating an IPSec connection is not as easy as launching a Web browser (the mechanism for SSL-based VPNs). Navigating the typical IPSec VPN complexities of IP addresses and other network settings can be difficult for non-technical users. This can lead to greater help-desk intervention for training and troubleshooting, while significantly impacting and diminishing end-user acceptance.

Another challenge is the incompatibility between Network Address Translation (NAT) and IPSec. NAT is a protocol that converts the individual IP addresses of a host of users to a single address, essentially hiding individual addresses from outside access. This useful security feature is often employed in enterprise and home-based locations. However, NAT does not interoperate well with IPSec; the changes made to each IP packet through NAT appear to the receiving VPN device as altered and potentially malicious data, causing the packets to be rejected upon arrival.

The lack of a standard among competing IPSec VPN vendors is also a concern, one that becomes more serious when working with a variety of partners and suppliers. The IT department tasked with integrating VPNs from competing vendors is faced with complex interoperability hurdles.

Firewall traversal, particularly for outgoing connections, can create further difficulties with IPSec. Internal firewalls often require additional configuration to permit outgoing IPSec traffic to pass through the firewall. This extra step adds to growing support requirements, particularly given home users' growing reliance on firewalls.

Remote Application Installation Challenges

IPSec VPNs are also not adept at delivering shared application services or centralized databases for real-time access. Rather, individual client copies of applications must be purchased and installed, and updated versions maintained, on each remote machine. Installing software to geographically dispersed users or remote teleworkers 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. One all-too-typical scenario involves non-technical end uses faced with having to configure their remote PCs – replete with various operating systems, patches, and driver configurations – without the benefit of onsite IT assistance.

Performance Drawbacks

An IPSec VPN does little to alleviate or circumvent the bandwidth constraints typical of most remote users. In practice, VPNs are processor-intense 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.

Security Concerns

When IPSec VPNs are used to extend company resources to remote users, security itself becomes a concern. 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 the network.

SSL VPNs: A Better Remote Access Choice

The drawbacks associated with IPSec VPNs have led enterprises to consider alternatives. Increasingly, businesses are attracted to the advantages brought by appliances that incorporate SSL along with additional Internet technology. The Netilla Service Platform is such an appliance.

SSL is an open-standard Web protocol that provides server authentication, data encryption, and message integrity 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. All transactions, from passwords and email access to application and file sharing can be secured with SSL, making eavesdropping on communications and stealing user passwords extremely difficult.

Client-less Advantages

SSL VPNs provide a number of advantages over traditional IPSec VPNs. One advantage is the ubiquity of ready-made SSL clients: the Web browsers built into every modern computer. By taking advantage of this "client-less" deployment, SSL VPNs minimize the need to configure and maintain remote computers. Little training is required; even the least technically savvy end user is immediately comfortable using a browser.

Netilla Service Platform: Thin Client Use of Shared Applications

Taking the "client-less" deployment one step further, the Netilla Service Platform provides an additional key benefit: easy access to legacy (Windows, UNIX/Linux, and mainframe) applications quickly and easily over the Internet through thin-client technology. This crucial functionality differentiates the Netilla platform from the various SSL VPN approaches, some of which are often limited to Web applications or network file access only.

With the Netilla Service Platform, the applications that end users access reside not on the remote PC, but rather on the application servers located in the main corporate network. This is an ideal way to provide extranet partners, branch offices, remote facilities, or mobile employees with secure, cost-effective and easy access to virtually any type of business application, without requiring the time and effort of an onsite visit to install client copies of each program.

In this thin-client model, application processing is performed on the server in the corporate data center, while the end user's machine—whether a full PC or a "smart" client such as a Wyse Winterm™—handles only the input and output data (keystrokes, mouse clicks, and graphical display). End users interface with the

virtual representations of the applications through screens, not directly with the applications themselves – although the application works just as it would if it were installed directly on the PC.

One advantage of this secure, "application layer proxy" arrangement – so called because the SSL appliance generates a proxy, or a representation of the application, rather than the application itself – is that remote users can access various applications through native protocols – such as Remote Desktop Protocol (RDP) data for Windows-based applications, X11 data for UNIX applications, or telnet data for IBM mainframe applications – via a single protocol, secure http (https).

For example, end users access the URL of the Netilla platform over https. The Netilla platform then sends the appropriate protocol to each application server on the backend as a proxy for the end user. The advantage is that the end user has only to launch a Web browser to access any application that has been provided for them by the Netilla administrator, and is not required to have native protocol applications or clients on their location machine.

By centralizing applications in this way, 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. This thin-client approach delivers a fast Return on Investment (ROI) and reduces initial and ongoing MIS costs dramatically (refer to *Table 1: 3-Year TCO* for analysis).

There are also marked advantages to deploying an SSL VPN by using a dedicated network appliance, rather than multiple pieces of software that must be installed on the application servers. One obvious benefit is the elimination of overhead on each application server that is required for software-based approaches.

Contrasting IPSec, SSL traverses standard firewall ports that are already open to allow Web traffic. The advantage is that unlike IPSec VPNs, SSL VPNs seldom require firewalls to be reconfigured.

Key advantages such as these translate into a long-term cost savings leading to a significant reduction in IT maintenance costs, both initially and ongoing. Refer to *Table 3: Annual Operations* for a comparison of maintenance costs on a yearly basis.

Table 2: 3 Year TCO

Netilla Vs. IPSec VPNs: A Significant Cost Savings
Three Year TCO: 100 Concurrent Users

Product	VPN Concentrator	Netilla-ESP
Equipment & Software	$28,700	$31,200
3 Year's Maintenance & Support Costs	$93,900	$37,500
3 Year TCO	$122,600	$68,700
Netilla Advantage		*44% Savings*

Equipment and Software: Initial hardware costs
Three Years' Maintenance and Support Cost: The Annual Maintenance Cost per User x100 users for three years. Annual Maintenance is described in Table 2, below.

Table 2: Annual Operations

Netilla Vs. IPSec VPNs: Significant Maintenance Savings
Annual Operations Cost: 100 Concurrent Users

Product	VPN Concentrator	Netilla-ESP
IT Support ($150/hour)	$30,000 2 hours per year, per user	$7,500 .5 hours per year, per user
Annual Platform Maintenance	$1,345	$5,000
Total Annual Maintenance	$31,345	$12,500
Annual Maintenance/User	$313	$125
Netilla Advantage		*60% Savings*

IT Support:
For VPN: Conservatively assumes two hours IT support per user, per month.
For NSP: Assumes .5 hours IT support per month.
Annual Platform Maintenance:
Netilla Maintenance Plus provides 24x7 support and includes appliance and software.
VPN Concentrator maintenance provides 24x7 support for hardware, and 100 VPN clients.

The Netilla Service Platform: Thin Client Performance through Browser-based Applet

The Internet technology built into the Netilla Service Platform monitors network load and the processing power of the end user's device, incorporating thin-client remote access functionality into a downloadable Java® applet. This browser-based applet communicates with the appropriate legacy application on the corporate network through terminal sessions, which are sent via the Netilla Service Platform.

Netilla's advanced technology for communicating with applications and resources is called Adaptive Internet Protocol (AIP). AIP splits the emulation and display

processing so that only the display is sent over the network. AIP constantly monitors available bandwidth and dynamically adapts to changes in the user environment. This ensures optimal performance for all users, regardless of their connection speed.

The AIP protocol is designed to work with a range of clients and connection types over complex network routes with varying bandwidths. It employs sophisticated heuristic mechanisms to continually monitor, measure and adapt to the ways in which data is transferred between applications and client devices, and adjusts to changing conditions such as Internet latency.

The result is greater efficiency when running remote applications. Any program, running on any platform – whether commercial software for Windows, UNIX and Linux, or complex proprietary or mainframe applications – all are made immediately and easily accessible to a multitude of concurrent, remote users.

The remotely accessed application itself can draw upon the same resources available in the main office, such as server-based files and office printers. Likewise, the remotely located application can pull files from client PCs and perform remote printing at the client's site, creating a truly seamless office experience. Unlike IPSec VPNs, there is no need to expose all network resources to the entire user base: network administrators can set user permissions and policies to limit access to specific applications for specified users.

Netilla Service Platform: Practical and Manageable Security

The Netilla Service Platform has been designed from the ground up for powerful security, IT simplification, and ease of use.

It blends a suite of key security features into a unified, hardened platform. The result is a low-maintenance, easily managed solution that cannot be easily matched by other integrated VPN offerings.

This arrangement delivers benefits quickly and without complexity. It's easier to enable new applications, add new users and manage new user accounts.

Security elements including authentication, policy, and encryption are bundled into the Netilla platform for reliable and quick deployment. Netilla's security benefits include:

- Hardened Linux platform with hardened Apache Web server
- Application Layer Proxy—application servers remain safe on the private LAN and are never directly accessed
- X.509 digital certificate for site authentication with Web-based certificate management GUI
- Dual-interface firewall protects both internal and external threats to the platform
- No new firewall ports: SSL traverses standard https ports already open for Web traffic
- Flexible, multi-stage authentication works with numerous protocols: RADIUS, RSA SecurID®, Windows® 2000 and Active Directory, LDAP, Vasco, and ActivCard

Manageable Authentication and Policy: Netilla's Realm-based Framework

One of the core technologies that differentiates the Netilla Service Platform from other SSL VPN aproaches is Netilla's unique "realm-based" framework for authentication and policy. This portable framework allows administrators to stack multiple authorization policies and authentication stages existing on external directories into logical groups, or realms, which represent clusters of authentication and authorization protocols. Each realm can then be used to control access on a group-by-group basis.

Netilla's Realm Framework begins by utilizing various authentication schemes (RSA SecurID®, Vasco DigiPass, Kerberos, RADIUS, Windows SMB, LDAP, etc.) as authentication building blocks, while integrating various policy mechanisms (Windows Group, Local Policy, LDAP, etc.) as policy building blocks. The Netilla platform then takes these building blocks and melds them into an authentication and policy realm.

When a realm member logs in to the Netilla Service Platform, the realm polls its associated authorization and authentication servers, and stores a user profile that is referenced via a Web-based token. This token is used to extract the user credentials from the profile that needs to be forwarded to each of the

backend servers on behalf of the user. Examples of backend servers include Windows Terminal Servers, Unix Servers, or mainframes.

The result is a flexible and powerful authentication and policy framework that delivers granular control over access to network resources, allowing administrators to group different types of users according to their level of trust or needs, in a manner not easily matched by IPSec or SSL VPN alternatives.

For example, consider a hospital that needs to provide patient information to remotely located physicians. The physician, who is not an employee of the facility, must be given limited access to network resources as a "less-trusted" Netilla user. In this case, the physician might be required to pass multiple stages of authentication, such as RADIUS and 2-factor SecurID; be given access only to particular healthcare applications according to an external Windows Group policy server; and be challenged for credentials upon each subsequent attempt to access the hospital network file directory through file sharing.

Such a profile, built by integrating various authentication schemes with authorization and policy databases, can be grouped together into a Netilla realm called "physicians," and applied to new users as needed.

In another example, a company's sales manager, who as a member of the private IP network is granted a higher level of trust, would have wholly different access requirements. This user might need to pass only Windows NT authentication; be given access to a suite of applications from multiple application servers according to an external LDAP policy server; and have his or her credentials continuously presented to the appropriate resource for single sign-on functionality. All of these authentication and policy variables can be combined into a realm called "Sales."

Table 3: Initial Deployment Costs

Netilla Vs. IPSec VPNs: Deployment Costs
Initial Deployment: 100 Concurrent Users

Product	VPN Concentrator	Netilla-ESP
Initial Platform Purchase	$12,500	$30,000
Hardware Installation ($150/hour)	$1,200 (8 hours)	$1,200 (8 hours)
Remote PC Configuration	$15,000 1 hour/User	$0
Total Deployment Cost	$28,700	$31,200
Deployment/Concurrent User	$287	$312
Percentage Difference	-8%	

Initial Platform Purchase:
Based on 100 user platform; includes licenses, power supply and stateful inspection internal firewall.

Remote PC Configuration:
For VPN: Conservatively assumes 1 hour per PC for VPN client install and configuration, driver and/or PC updates, travel to each remote site, end-user training, and application software installations.
Netilla server-based appliance utilizes browser-based SSL, and requires no client or software installation.

Easier Management

The result of this synergy is a robust policy and authentication framework that forms the core of the Netilla offering. Multiple external authentication and policy protocols are easily integrated and applied to a variety of users and user groups from a single Netilla platform, which acts as a gateway to network resources as a central point of management.

TCO Comparison

As shown, IPSec VPNs, with their high maintenance and deployment requirements, lead inevitably to a higher cost solution. The data reveals that while initial deployment costs are essentially the same (refer to *Table 3, Initial Deployment Costs)*, when the other costs required for a remote access implementat ion are considered, including help-desk time, end-user training, and ongoing IT maintenance, the Netilla Service Platform emerges with more than 40% TCO savings over three years.

Conclusion

The Netilla Service Platform delivers significant cost savings in a complete and comprehensive remote-access solution compared to IPSec VPN alternatives. The Netilla Service Platform provides a high value of security with low maintenance and support requirements through Web-based SSL technology. Quick to deploy, reliable and affordable, the Netilla platform boosts business productivity, revenue potential, and customer reach by integrating application-delivery access, user management, and network security into a single and cost-effective IT solution.

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. 2002
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, Netilla Service Platform, and the Netilla Stylized figure are registered trademarks of Netilla Networks, Inc.