

Achieving **Versatility** and **Network Protection** in an SSL VPN

Protection

Versatility



- 1 Introduction**
- 1 Traditional Solutions Fall Short**
- 2 Introducing Netilla Security Platform**
- 2 Versatility:**
 - 2 **SSL VPNs:** Application Gateways for the Enterprise
 - 2 Clientless Access to Remote Client/Server Applications
 - 3 Secure Intranet Access to Web-based Applications and Portals
 - 4 **Desktop Application Access:** Client/Server over SSL Tunneling
- 6 Network Protection:**
 - 6 **Policy and Network Security:** The Application Layer Proxy
 - 6 **The Termination Zone:** Policy at the Network Edge
- 7 Remote Access to Legacy Applications: SSL VPN's are Not Alike**
- 8 Manageable Authentication and Policy: Netilla's Secure Realm Framework**
- 9 Conclusion**

Achieving Versatility and Network Protection in an SSL VPN

Introduction

Secure Sockets Layer (SSL) Virtual Private Networks (VPNs) are quickly gaining popularity as serious contenders in the remote-access marketplace. Analysts predict that products based on SSL VPN technology will rival - or even replace - IP Security Protocol (IPSec) VPNs as remote-access solutions. Meta Group has declared, "SSL VPNs will be the dominant method for remote access, with 80% of users utilizing SSL."¹ Infonetics predicts close to a \$1 billion SSL VPN marketplace by 2005². A recent Tolly Group survey of enterprise network security specialists indicates that SSL-based VPNs are likely to replace IPSec VPNs for remote access.³ Clearly, SSL VPNs are primed for exponential growth.

A number of factors are fueling the demand for SSL VPNs. These include:

- Federal mandates, such as the Health Insurance Portability and Accountability Act (HIPAA) for the healthcare industry and Gramm-Leach-Bliley Act (GLBA) for financial institutions. These mandates are driving key market segments to protect the privacy of distributed electronic information.
- The increasing use of extranets - the granting of non-employees and business partners secure access to internal networks - which have become a "must have" requirement of conducting business.
- Government and private interest towards Homeland Security initiatives, which is building momentum for security implementations on the whole.

It's not surprising that SSL VPNs are benefiting from these developments. SSL VPNs are uniquely suited to meet the diverse remote-access needs of today's enterprise, with their low costs, application access flexibility, high security, and overall simplicity. This paper describes an SSL VPN, how it operates, and the benefits of the Netilla Security Platform (NSP), a leading SSL VPN appliance from Netilla Networks, Inc.

For a detailed TCO comparison of SSL VPNs versus IPSec VPNs, refer to "A Functional and Cost Comparison of VPN Solutions: SSL Vs. IPSec" available from Netilla Networks, Inc.

1 Meta Group, 2002
2 Infonetics, 2002
3 Tolly Group, January 2002

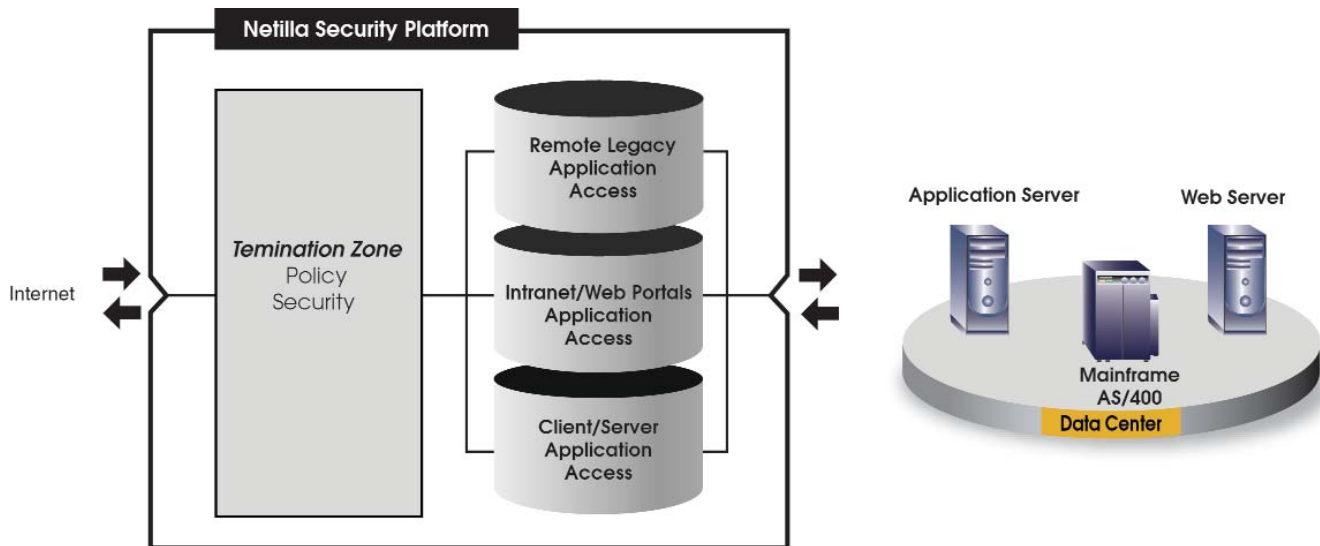


Figure 1: Multiple Application Access Modes

Introducing the Netilla Security Platform

The NSP is a clientless, SSL VPN that provides remote access to a wide range of corporate applications using a Web browser as a ready-made access client. As a dedicated network appliance, the NSP integrates into existing network and security designs seamlessly by offering rapid deployment, easy installation, minimal maintenance, and high security. With the NSP, remote users need only a computer and a Web browser to access virtually any business application on the corporate network. This approach leverages the global reach of the Internet for streamlined delivery of business-critical information to partners, suppliers, and employees, with strong security, privacy, and network protection.

Versatility

SSL VPNs: Application Gateways for the Enterprise

The modern enterprise network is a dynamic environment. Inevitably, corporations deploy an ever-changing variety of applications - residing on a variety of platforms - for a diverse community of users. These heterogeneous data centers may comprise legacy and client/server applications on Windows Terminal Servers, UNIX/Linux servers, or mainframes and AS/400 machines, as well as Web applications that reside on intranet Web servers.

Historically, opening up this complex realm to remote partners, suppliers, and employees, while ensuring network protection, has been one of the great hurdles to a successful remote-access deployment. As a result, enterprises are turning towards SSL-based VPNs, such

as the NSP from Netilla Networks, to satisfy the demands of today's more multifaceted arrangements. SSL VPNs simplify and secure multi-user, multi-application remote-access environments, reducing the time, cost, and complexities once required.

Taking this approach one step further, the NSP offers additional advantages over other SSL VPNs by combining three application-access technologies into a single gateway device:

- Clientless, browser-based access to remote legacy applications
- Secure intranet access to Web-based applications and portals
- Desktop access for client/server applications over SSL tunneling

Clientless Access to Remote Client/Server Applications

The Web revolution promises to radically alter the landscape of the enterprise network. Web-enabled applications - those specifically written for direct browser access - create new opportunities for collaboration and improved information accessibility.

These advantages notwithstanding, non-Web-enabled, legacy client/server applications - those residing on centralized Windows, UNIX/Linux, mainframes and AS/400 machines - form a vital core of the business applications used today. The challenge is to leverage these crucial legacy applications in a simple way that provides the same on-demand access to centralized information as their Web-enabled counterparts.

The NSP solves this dilemma, providing clientless, remote access to legacy applications by incorporating Web-enabling technology directly within the platform. This integrated approach, unique to Netilla among SSL VPN vendors, eliminates the need for enterprises to deploy and maintain server-based “middleware” and associated remote-access clients.

In the NSP model, both the client and server portions of an application are centrally hosted in the corporate data center. The advantage of this approach is that end users need only a browser to access these remotely located applications; no additional software or configuration of the remote computer is needed. Access to key legacy applications are available from any location, at any time.

With the NSP, legacy applications are made available to remote users through the Web, allowing companies to leverage their existing legacy application infrastructure without costly application re-development or installing and configuring remote PCs. Any program, running on any platform - Windows, UNIX and LINUX, or 3270 mainframe and 5250 AS/400 - can be made available to a multitude of concurrent remote users.

In this application-layer access model, the NSP uses a built-in screen-scraping protocol that splits the emulation and display processing so that only the application's display is sent to the remote user's Web browser. The NSP supports this capability through a browser enhancement (a small Java applet). This applet is downloaded to the user's browser when the user initially logs in to access legacy applications. The applet routes application information (screen, key strokes, and mouse clicks) between the remote user's browser and the network's application server. The remote application protocol monitors, measures, and adapts to the ways that data is transferred between server-based applications and client devices, and dynamically adjust to changing conditions as needed. As a result, the user experiences the application with optimal performance over any connection, just as if the application was installed and running on the user's local machine.

The application itself has the same resources available in the office, including server-based files, client drive mapping, and local and remote printing. Likewise, the remotely located application can fetch files from the client PC and print at the client's site, creating a truly seamless branch- or home-office experience.

This key functionality - clientless, browser-based access to centralized applications - establishes the NSP as the only fully integrated SSL VPN appliance that meets the demand for secure, cost-effective access to business applications from any remote computer, through the simplicity of a Web browser.

Notably, many alternative SSL VPN appliances lack this integrated remote application access protocol, and are forced to provide remote access to legacy applications via third-party middleware running over

an SSL tunnel. In fact, most SSL VPN vendors employ SSL tunneling as the sole means with which to access remote legacy applications. SSL tunneling is appropriate only for very specific scenarios, where trusted employees must synchronize select, locally installed applications with a remote server.

The NSP also offers SSL tunneling by deploying innovative strategies that overcome the security limitations of many SSL tunneling products. *Refer to Netilla: SSL Tunneling with Many Benefits.*

Secure Intranet Access to Web-based Applications and Portals

While organizations continue to rely on legacy applications as part of their application strategy, enterprises are also developing or acquiring applications intended for direct Web browser access. Sometimes these are re-written or “Webified” versions of legacy applications, such as Microsoft Outlook Web Client. They may also be proprietary applications specifically designed for the company's intranet use.

Remote Access Challenges

There is little doubt that Web-enabled applications vastly improve the accessibility of business information. However, sharing such information over the Web can lead to security risks that must be carefully addressed. IT departments given the unenviable task of extending Web-based applications to off-site partners, suppliers, and employees face abundant challenges:

- Web-enabled resources typically reside on a company's secure intranet, and use internal Domain Name System (DNS) that cannot be resolved by the public Internet. There are two main drawbacks to this situation:
 - Internet users cannot easily access these private network resources.
 - Making these DNS names resolvable by the public Internet provides potential attackers with insight into how a company partitions its business logic and processes.
- Web servers must often reside in the Demilitarized Zone (DMZ) or another security zone for public access; securing this environment is a risky and high-maintenance undertaking
- Web-enabled applications often run on servers that are either intrinsically insecure or known to have ongoing vulnerabilities (Microsoft IIS, for example)
- Keeping public-facing Web servers hardened, patched, and updated is an ongoing administrative challenge; if not constantly kept up-to-date, network susceptibility increases with each new vulnerability

The NSP allows organizations to overcome these obstacles and safely open intranet Web applications to authorized users via the Internet. The NSP provides clientless, browser-based access to Web-based resources using HyperText Transfer Protocol (HTTP) reverse-proxy technology. Unlike a forward proxy, which operates between a corporate intranet user and an Internet Web site, a reverse proxy operates between a remote user on the Internet and an enterprise Web site. With this approach, a single point of entry over the Internet - the NSP itself - lets remote users access back-end, intranet Web servers securely through a Web browser.

Some advantages of Netilla's approach include:

Accessibility

- Authorized remote users gain instant, clientless access to internal -Web applications from any location
- Internal DNS addresses that do not resolve publicly can be accessed securely over the Internet.

Security

- Company Web servers remain safe behind the firewall, in a highly secure portion of the private network, without the cost and maintenance of locking each server down for public access
- Administrators gain granular access control to directories, servers, and paths on a user or group basis
- Organizations can conceal their internal network topology from unauthorized users
- Because all requested pages are re-written by the NSP reverse proxy before being presented to the end user, filtering can be applied to block potentially malicious code based on type (JavaScript, ActiveX, Java applets)

This approach delivers fast, secure, on-demand access to Web-based information, with a highly scalable solution that can easily grow to authorize users on a global scale.

Desktop Application Access: Client/Server over SSL Tunneling

The NSP's clientless, remote access to legacy applications and secure intranet access to Web-based applications and portals meet the access needs of most remote users. However, some members of a company's organization may also rely on local client/server applications that are already installed on their computers. These productivity tools - typically email or Customer Relationship Management (CRM) programs - are local applications that interact over a network with a server in the private network. Many of these client/server applications support "off-line" usage in addition to online synchronization. For example, a user can continue to work with email messages via his/her local Outlook application while on a flight, and send and receive data via the Internet to the email server after landing. These applications often reside on computers "owned" by the company and are relatively accessible to MIS staff. In this case, a network-layer type access - similar to that provided by IPsec VPNs - is appropriate. The NSP provides this desktop application access via SSL tunneling.

How the NSP SSL Tunneling Works

The NSP desktop application access is supported through a VPN adapter that is downloaded and installed the first time a user logs into the NSP for client/server access. The virtual adapter negotiates the secure SSL tunnel via the user's Web browser. No changes to the client/server application itself are required; if the network administrator has authorized an application for a user, that application can be used over the SSL tunnel, without needing special configuration or help-desk intervention. In fact, the only action required by the user is to login to the NSP and initiate the SSL tunnel. At that point, all authorized traffic designated for the remote private network is encapsulated with SSL and sent over the Internet.

Netilla: SSL Tunneling with Many Benefits

Securing and managing the link between remote desktops and company data centers is a paramount concern of any MIS department. Relying on tunneling technology to meet the remote access needs of every member of an organization's user base - including "un-trusted" extranet partners and suppliers - is an ill-advised strategy that fails to provide adequate protection over private network resources.

Yet many SSL VPNs that lack the NSP's integrated legacy application protocol are forced to deploy SSL tunneling technology to deliver remote access to legacy applications for every remote user. Administrators therefore need the flexibility to limit tunneling solutions to the crucial client/server applications that select employees depend on every day - such as locally installed email clients - without compromising network security.

The NSP is well suited for these client/server arrangements, providing the necessary data transfer capabilities of an IPsec VPN, while delivering many additional benefits:

IPsec DRAWBACK: Network-layer IPsec VPNs create a peer-to-network connection between remote users and the corporate network, without easy application authentication and authorization.

NSP SOLVES: Netilla's integrated dynamic firewall limits access to the client/server applications that a user is allowed to use. Access can be restricted to authorized servers that host authorized client/server applications. This unique dynamic firewall functionality is not matched by traditional IPsec solutions.

IPsec DRAWBACK: IPsec VPNs require multiple firewall ports opened on the corporate network

NSP SOLVES: Netilla's SSL tunneling solution multiplexes all traffic over a single port, 443, which is already open to secure Web traffic. The result is no firewall configuration and less complexity.

IPsec DRAWBACK: IPsec VPNs do not work well with NAT-enabled devices

NSP SOLVES: The NSP's secure SSL tunnel communicates over Network Address Translation (NAT) connections easily, without requiring router re-configuration.

IPSec DRAWBACK: IPSec VPNs require that the client's private key/shared secret or certificate be installed and maintained on the PC.

NSP SOLVES: A successful login to the NSP creates a secure token for authenticating the SSL tunnel via the user's browser on a per-session basis, simplifying security management.

IPSec DRAWBACK: IPSec VPNs do not support split tunneling.

NSP SOLVES: With the NSP, users may transfer data to other Internet sites while communicating across the SSL tunnel to their private network.

Drawbacks to SOCKS Proxy Approaches

Some SSL VPNs employ a "SOCKS Proxy" approach for client/server data transfers. The NSP supports key features not available from SSL VPN vendors that employ SOCKS Proxy technology. These features include:

SOCKS LIMITATION: Support for any client/server application

NETILLA SOLVES: The NSP works with both UDP and TCP applications over SSL tunneling. Support is not limited to applications with "easily predictable TCP ports". Rather, any authorized TCP or UDP application works with the Netilla solution.

SOCKS LIMITATION: Re-configuration of client applications

All traffic that passes over the secure tunnel - both UDP and TCP - is encrypted with 128-bit SSL. UDP SSL encryption is not included with the SOCKS proxy specification.

Netilla SSL VPN adapter automatically downloads; no user intervention required

Client applications work over the NSP's SSL tunnel without any additional application or operating system re-configuration

SOCKS LIMITATION: Multiple-Subnet Environments

NETILLA SOLVES: The NSP lets users access application servers located on different subnets of the corporate network.

SOCKS LIMITATION: Dynamic Session-based Firewall

NETILLA SOLVES: The NSP controls access to specific desktop client/server applications based on group membership.

Security is further enhanced by the NSP's unique ability to enforce strong policy control over client/server access via the Netilla SecureRealm Framework (*see Manageable Authentication and Policy: Netilla's SecureRealm Framework for more information.*)

Versatility Means Meeting Every Access Requirement

By merging three access technologies into a single appliance, the NSP provides a full-spectrum remote-access solution that meets EVERY application access type. The result is a powerful tool - one that delivers a high level of flexibility for network administrators, who can arm their remote users with a wide range of applications based on changing conditions and needs, while protecting the company's critical business assets.

Different Needs for Different Users

To understand how the NSP is uniquely suited to meet the diverse user base of the modern enterprise, consider that today's remote access user base can be distilled into three classes:

- Extranet Users - Non-employees, partners and suppliers who need secure, controlled network access from computers not "owned" by the enterprise's MIS staff
- Employees - Members of the company's organization with a higher level of trust than extranet partners and are thus allowed access to more, but not all, network resources
- Administrators - The most "trusted" members, these users require full access to all network resources at all times

Serving the Extranet

Extranet users pose a different type of risk to the organization, and impose the greatest challenge. Extranet partners use machines that are inaccessible to MIS. They are poor candidates for traditional client/server applications - those that are locally installed and synchronized with a remote server - because MIS departments lack the ability to install and configure such applications. Further, extranet users cannot be trusted with the full network-layer access emblematic of traditional VPNs.

In this case, the NSP meets extranet user requirements through thin-client access to legacy applications and HTTP reverse proxy to Web applications. Both access modes leverage centralized applications, so there is no need to "touch" the remote computer. All applications in this model are accessed simply through a browser, while the enterprise network is safely protected behind the NSP.

Meeting Employee Needs

The second class of users, employees, are generally more trusted than extranet users, although with varied needs that call for a sophisticated application-access strategy. Employees likely have local client/server applications, such as email or CRM. However, having these applications installed on their computers does not mean they should always be granted the capability of using them.

In this case, network administrators need to control access over several application approaches. Some employees require client/server applications along with HTTP reverse proxy to some Web applications and parts of the intranet, and thin-client access to some legacy applications. The NSP, which provides access to all three application types, is well suited here, with flexible access management to control a variety of application approaches.

Access for Network Administrators

Network administrators are the most "trusted" users with the most comprehensive application access requirements. Such users need access to every legacy application and every level of the intranet structure, and the capability to use any client/server application that resides on their desktop. The NSP meets the needs of network administrators well.

In reality, few organizations have user bases that fall neatly into three categories. Inevitably, there are subgroups comprised of degrees of trust and application access requirements. For example, sales members need different application subsets than finance members, although they both are trusted employees. The NSP's flexible Netilla SecureRealm Framework can be tailored to meet an organization's unique requirements and diverse environments, as described later in this paper.

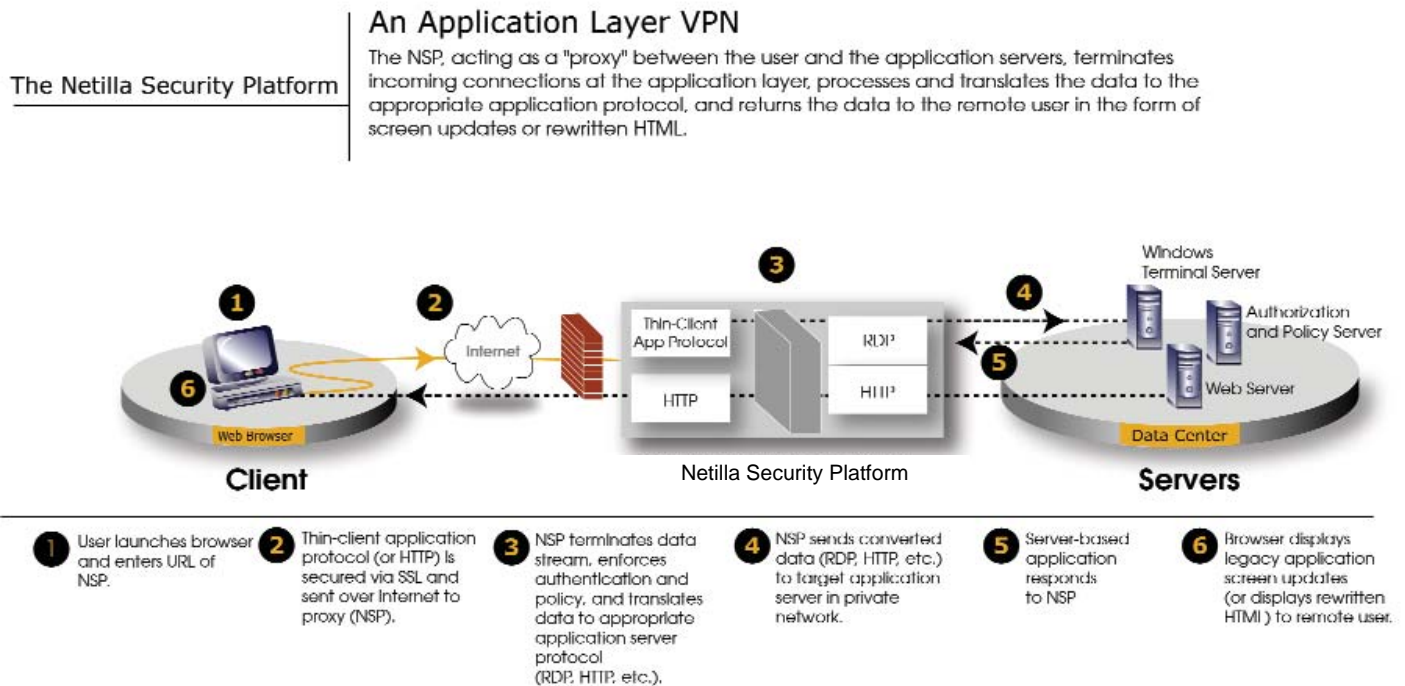


Figure 2: Application Layer Proxy

Network Protection

Policy and Network Security: The Application Layer Proxy

When supporting clientless access to legacy applications and operating as an HTTP reverse proxy for Web applications, SSL VPNs such as the NSP can deliver their rich set of application-access modes as an "Application Layer Proxy". SSL VPNs are so-called because they operate at layer seven - the application layer - of the Open Systems Interconnection (OSI) model. IPsec VPNs, by comparison, operate at the network layer. The NSP approach provides distinct network-protection advantages not available with other remote-access solutions. Operating at the application layer provides 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, the NSP can implement dynamic policy-based access to application resources from a single point of administration.

SSL VPNs empower organizations to avoid deploying application and Web servers in a DMZ or other security zone, where they would have to be exposed to the public Internet. Instead, with SSL VPNs, application servers remain safe on the private network, behind the firewall, and are never directly exposed to the public network. The NSP, which functions as a proxy for the end user, acts as a hardened barrier to protect mission-critical resources.

As **Figure 2** shows, the NSP protects resources by "intermediating" the connection between remote-client requests and server-based applications, terminating incoming connections from the remote user at the application layer. Once the incoming request is terminated (the "termination zone"), the NSP processes and translates the data to the appropriate back-end application protocol. Examples of back-end protocols include:

- 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

By acting as an intermediary between remote users and private network resources, negotiating the remote user's input with the back-end application's responses, the NSP allows remote users to access a variety of applications - both Web and remote legacy client/server - directly through a Web browser.

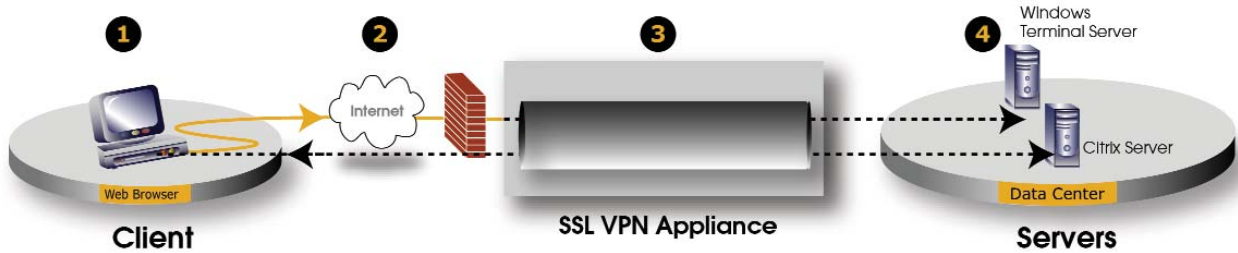
The Termination Zone: Policy at the Network Edge

During the NSP's "termination zone" - the period between terminating and translating incoming data - a unique opportunity exists to poll external authentication and policy servers, such as Active Directory or Lightweight Directory Access Protocol (LDAP), and credential user identities to authorize specific application access. By analyzing terminated-application information and applying the appropriate security policy, the NSP acts as a gatekeeper between the Internet and the private network.

Circuit-level VPN Drawbacks:

SSL Tunneling for Legacy Applications

SSL VPNs that lack the NSP's integrated remote application access protocol must rely on SSL tunnelling for remote access to legacy applications. These solutions do not perform data termination, policy and translation in the DMZ, at the network edge. Instead, such SSL VPNs apply security at the application server, INSIDE the private network.



- 1** User launches browser and logs into URL of SSL VPN appliance.
User launches third-party client to access server-based software.
- 2** Request for remote server-based applications made over the Internet.
- 3** SSL VPN appliance passes data directly through to private network.
- 4** Authentication and policy applied at the application server, INSIDE the private network.

This arrangement establishes a 3-tier communication model:

Tier 1:	Application data is sent from the browser to the NSP via screen-scraping technology.
Tier 2:	The NSP terminates and translates the data to the appropriate back-end resource, (e.g., RDP for Windows applications, 3270 for mainframes, X.11 for UNIX/Linux, HTTP for Web, etc.).
Tier 3:	The NSP delivers the translated data to the back-end application server.

This proxy approach is also well suited for Web-based intranet applications and portals, allowing secure remote access to Web-based resources, without exposing non-hardened intranet servers to outside attack. In this case, the NSP terminates, examines, and rewrites HTTP requests. Remote users are then presented with Web-application resources as defined by policy and security.

This scenario is an application-layer VPN in action - the user messages are not sent directly to the application server on the private network, but rather terminated by the NSP, processed with policy and security, translated to the appropriate back-end protocol, and transmitted via a new connection to the application server. The NSP enforces authentication and policy before allowing the data streams to reach the application server, protecting private network resources in a uniquely effective way unmatched by traditional remote-access solutions.

Remote Access to Legacy Applications: SSL VPNs are Not Alike

SSL VPNs support access to remote legacy applications in a variety of ways. As previously shown, the Netilla solution operates as a true application layer proxy for remote-access to legacy applications and Web applications. Legacy applications are delivered via a unique protocol between the remote browser and the NSP, which terminates, examines, and converts the data to a back-end legacy protocol. Web applications are terminated and re-written by the NSP's reverse proxy. This process occurs during the NSP's "termination zone."

However, not all SSL VPNs act as true application-layer proxies for all protocols all the time. For remote legacy-application access, alternative SSL VPNs do not function as application-layer proxies, but instead use SSL tunneling, operating as "circuit-layer" VPNs. **Figure 3** shows a drawback to this approach: Third-party remote clients must be installed and configured on each PC, essentially eliminating the "clientless" advantages that many users expect from an SSL VPN.

Security is another drawback. Such "tunneling-based" VPN solutions create a direct connection from the third-party client via the SSL VPN to an application server that hosts the target application. In this case, there is no intermediation and data translation. Instead, application data enters the network without having been analyzed by the SSL VPN appliance. In this scenario, authorization and policy occurs at the application server inside the private network, rather than in the security zone at the network edge, where it might have been processed and controlled. Such arrangements do not gain the advantages of an integrated policy, authentication, and authorization frame-

work as defined by the appliance, and leave target-application servers vulnerable to attack.

The NSP, by contrast, terminates legacy application and Web data streams in the DMZ. The result is greater protection over network resources. By sitting at the network's edge, policy and authorization are enforced before data streams are allowed onto the back-end application server. For instance, if a user requests a Windows application, the NSP translates incoming data to RDP only if the network rules permit access to the requested application. Otherwise, the NSP disconnects the data stream.

The NSP: A True Application Layer Proxy

The NSP can be considered a true application-layer proxy for both remote access to legacy applications and remote access to Web applications.

This arrangement provides greater network protection over a company's investment and mission-critical data, leading inevitably to a more secure solution.

The NSP's SSL tunneling for client/server applications mimics a network-layer VPN by design and cannot, by definition, be considered an application-layer proxy. However, even these network-layer applications can be uniquely secured by the NSP. For these applications, Netilla employs a dynamic firewall that overcomes the security drawbacks typical of a network-layer VPN, as explained later in this document.

Manageable Authentication and Policy: Netilla's SecureRealm Framework

One of the core technologies that differentiates the NSP from other SSL VPNs is Netilla's SecureRealm Framework for authentication and policy. Using the Netilla SecureRealm Framework, an organization can implement a dynamic application-layer policy enforcement point located in a DMZ or security zone, and enforce that policy before the user's traffic reaches the application server in the data center. This policy engine at the edge of the network allows the NSP to function as a secure barrier to private network resources.

Netilla's SecureRealm Framework combines authorization schemes (RSA SecurID®, Vasco DigiPass, Kerberos, RADIUS, Windows SMB, for example) as authentication building blocks, while integrating various policy mechanisms (Windows Group, Local Policy) as policy building blocks. These layers are arranged into logical groups, or realms, that represent clusters of authentication and authorization protocols. Each realm can be used to control access on an individual or group-by-group basis.

The key concept is not the number of authentication types supported by the NSP, but the fact that they can be logically stacked into a conglomerate scheme for levels of trusted users. Bolstering this functionality is the NSP's unique ability to pull policy information at each authentication stage, further refining the user's capabilities. This allows, for example, Windows Security Group membership to be

incorporated into the NSP's policy decision making in combination with non-Windows schemes for policy or authentication (such as RSA SecurID). Combining these capabilities into an organized access framework defines the synergistic power of the Netilla approach.

For example, an organization may want finance users to access only financial applications using a single sign-on against a single authentication server. At the same time, extranet users may need to access several applications, but with multiple layers of authentication - RSA SecurID, followed by Active Directory. All users, however, enter the network through a single NSP in the DMZ.

Each of these user types can be placed in a unique realm comprised of a unique subset of authentication and policy. A single NSP can support 1000 realms.

The result is a flexible and powerful security 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 way not easily matched by IPSec or SSL VPN alternatives.

SSL VPNs: Flexible and Manageable Security

Security is the cornerstone of any remote-access implementation; it is axiomatic that good security is easily managed security. SSL VPN appliances can quickly integrate into the network, providing companies with a rapid-deployment solution without modifications or interruptions to existing application servers and security mechanisms. The NSP blends key security features into a unified, hardened appliance. Security elements including authentication, policy, and encryption are bundled into the Netilla platform for fast and reliable deployment. The result is a low-maintenance, easily managed solution whose rich feature set cannot be matched by other integrated VPN offerings.

Netilla's security benefits include:

- A single-appliance solution that acts as a secure application gateway for diverse types of applications and browser-based access methods, while providing a single point of management
- Application Layer Proxy-application servers remain safe on the private LAN and are never directly accessed
- The Netilla SecureRealm Framework provides simplified granular identity and policy access management by using multiple authentication and authorization user realms that integrate seamlessly into existing security infrastructures
- Flexible, multi-stage authentication works with standard security technologies: RADIUS, RSA SecurID®, Windows 2000 and Active Directory, LDAP⁴, Vasco, ActivCard
- Netilla Software Update GeNIE™ provides instant remote security and update patches
- 128-bit SSL encryption protects all data transmissions and digital certificates provide site authentication
- Dual-interface, integrated stateful inspection firewall protects both internal and external threats to the platform

- No new firewall ports: All traffic is multiplexed over a single port to eliminate complex firewall implementations
- Automated failover/redundancy, with data replication for high availability
- Extensive monitoring utilities logs user access by application or service, time/date, and session duration

Conclusion: Versatility in One Platform

As shown, SSL VPNs like the NSP represent an excellent solution for accessing business-critical applications and resources. They allow enterprises to extend their Web-based resources easily and with confidence. With a rich variety of access modes, dynamic policy protection over network resources, and overall ease of use, the NSP boosts business productivity, revenue potential, and customer reach by integrating the broadest array of application-delivery access, user management, and network protection into a single, 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. 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, Netilla Security Platform, and the Netilla Stylized figure are registered trademarks of Netilla Networks, Inc.