

## Technical Data Sheet

### Application Gateway for the Modern Enterprise

The Netilla® Security Platform (NSP) is an SSL VPN appliance that offers secure, Web-browser access to a wide range of data-center resources. As a dedicated network device, the NSP integrates seamlessly into existing network and security infrastructure, while offering rapid deployment, easy installation, minimal maintenance, and unparalleled network protection.

**The NSP simplifies and secures multi-application remote-access environments for diverse users.** With the NSP, authorized users can work with an array of applications, including Microsoft Outlook Web access and other Web-based intranet applications, Windows Terminal Servers and server-based applications, and client/server applications over an SSL tunnel. Access is controlled through the powerful Netilla V-Realms, which manages privileges through multi-layer user authentication and dynamic policy enforcement from external servers. With any PC, laptop, or terminal, a mobile sales force, telecommuters, branch office employees, and business partners can quickly and securely reach the varied resources found in today's IT environment.

### 3 Versatile Ways to Access Your Network

With three SSL access technologies in a single appliance, the NSP provides a full-spectrum remote-access solution that meets every application access type:

- 1 Thin access for remote server-based applications
- 2 Web access for web-based applications and portals
- 3 Tunneling access for client/server applications

### 1 Remote Access to Server-based Applications

The NSP incorporates web-enabling technology directly within the platform, providing browser-based access to non web-enabled, server-based applications. This means simply secure access to Windows Terminal Servers, UNIX, Linux, and 3270 mainframe applications quickly and easily, and without third-party server-based software.

- Thin client computing model
- Java-based solution - No Admin rights needed
- Application Layer Proxy security: Termination, policy and translation in the DMZ
- Session persistence provides seamless continuity
- Proprietary data compression ensures optimal performance over any connection, including dial-up
- Supports both local or remote printing
- Drive mapping for seamless interactivity with local and remote data
- 24-bit color for Windows and X Windows

### 2 Remotely Access to Web-enabled Applications

The NSP's Secure Intranet Access enables suppliers, partners, and remote employees to access any internal Web application, corporate intranet, or portal securely through HTTP reverse proxy technology. Netilla's Secure Intranet Access empowers organizations to overcome the security and access challenges associated with deploying public-facing Web servers for remote-user access. With the NSP, intranet Web servers and network topology remain safely protected within the organization's private intranet, while fine-grained access policies limit access to paths, directories, servers, and Web components on a per-user or per-group basis.

- Reverse Web Proxy technology
- Browser-based access to Web resources
- Strong Web application security mitigates network threats
- Application Layer Proxy: Termination, policy and translation in the DMZ
- Gateway portal protection hides network topology from unauthorized viewing
- Granular access controls to directories, servers, and paths
- Powerful Java Applet Re-write Module for greater security

### 3 Remote Access for Client/Server Applications

Users who work offline on their local PC-based TCP and UDP applications - such as Outlook, CRM, sales tools, and other client/server programs - can update their files and exchange data with corporate servers through Netilla's network layer SSL Tunnel. The Netilla Virtual Adapter, seamlessly downloaded upon initial login, gives users full functionality of their local client/server applications, while ensuring timely updates to remain "in sync" with centrally hosted data.

- Layer 3 network connection
- Broad application support: UDP and TCP
- Dynamic session-based firewall - allow or deny application use over the tunnel
- Transparent Netilla Virtual Adapter: No application configuration required
- Network Address Translation (NAT) compatible

### Security



Netilla's breadth of security features means your business-critical resources remain safe from threats. From browser-embedded SSL encryption, to Netilla's V-Realms™ Client Identity engine, the NSP leverages security solutions already in place, such as leading 2-factor authentication and the prevailing policy engines used in today's enterprise. NSP client integrity options include a Secure Desktop that wipes all traces of a user's session, host integrity tools that validate the presence and patch levels of security software, adaptive policies for controlled endstation access, and cache cleaning functionality. Configurable session time-outs, Client Side Certificates with revocation list support, application-layer proxy protection, and a dynamic, session-based stateful inspection firewall add to Netilla security, while the Netilla Upgrade GeNIE ensures fast deployment of security and feature updates.

## Security

## Platform

## Application

### General

- Netilla Client Integrity options -
- Client side certificates with CRL -
- Granular control through dynamic policy-based authentication and authorization framework
- Compatible with existing security systems and external servers
- Application-Layer Proxy: Security at the network edge
- Authentication with multiple user-verification challenges
- Application usage audit trails
- Remote security patches and system software updates
- Configurable session timeout

### Authorization

- Groups support includes Microsoft® Windows 2000 Global groups, Active Directory (LDAP) groups, and local groups

### Authentication

- Single login enforcement
- Supports multiple authentication stages
- Supports multiple domains
- RADIUS® (RFC 2865)
- Microsoft Windows® NT/2000/2003
- Microsoft SMB
- Kerberos
- LDAP
- RSA SecurID® Ready / RSA Ace 5 Server Ready
- VASCO Ready Partner
- Aladdin eToken™ Enabled Partner
- X.509 digital certificate support

### Continuity and Productivity

- Netilla Hot Standby: Replication to backup platform
- Session persistence (for Windows Terminal Servers)

### Encryption

- 128-bit SSL 3.0 encryption
- Encryption of all authentication and session data
- Mandatory encryption levels

### Firewall

- Internal dual-Ethernet protection option
- Stateful-inspection technology
- Single firewall traversal limits port openings
- Ideal for multi-layer firewall designs
- Session-based for controlling desktop application access

### Management and Reporting

- SNMP and Syslog
- Web-based Administration GUI
- No Admin rights needed on local PC (for Thin and Web)
- Compatible with third-party access and Authentication protocols

### Network Requirements

- Dedicated Internet access with static IP address
- Bandwidth requirements for remote user - minimum 28.8 kbps/connection
- Available 10/100 BASE-T Ethernet connection/s

### Application Server Requirements

- Microsoft Windows-compatible applications require Windows Terminal Services
- X Window applications must be X11 compliant
- Character-based UNIX applications run in a terminal session
- Mainframe and AS/400 applications require optional Netilla 3270 emulation support

### Browser Recommendations

Microsoft Internet Explorer 6 or higher

### Platform Specifications

Netilla-powered SSL VPN solutions are available in B, E, and G platforms, depending on the capacity needs of your organization.

### Physical Specifications

- Dimensions: 17.75 in. x 15.25 in. x 1.75 in. (45.1 cm x 38.7 cm x 4.5 cm)
- Fits in a standard single-unit (1U), 19-in. rack.
- Weight: 15 lbs. (6.8 kg)

### Power Requirements

- B- and E-Class Platforms**
- Input rating 100-240 V, 50/60 Hz
- Power Consumption: 5.3 amps

### G-Class Platforms

- Input rating 100-240 V, 47/63 Hz
- Power Consumption: 6.0 amps

### Port Specification

- Two RJ-45 10/100 Ethernet
- Nine pin serial console port
- RJ-45 Failover Port

### Operating Environment

- 32°F to 95°F (0°C to 35°C)
- 10% to 90% humidity (non-condensing)

### Non-operating environment

- 14°F to 112°F (-10°C to 50°C)
- 5% to 93% humidity (non-condensing)

### Regulatory Approvals

- CISPR 22B
- UL
- CE
- FCC Part 15 B

### File Sharing

- Compatible with Microsoft Windows SMB
- Manage (copy, delete, rename) files from folders on the server
- Transfer files to/from local drive and remote server
- Client Drive Mapping

### E-mail

- Microsoft Exchange or other IMAP e-mail servers
- Outlook Web client or other Web-based e-mail
- Real-time e-mail access (No synchronization)

### Printing

- Redirection to local or network printers
- Session printer management
- Universal printer support

### User Interface

- Customizable login page
- Service access tabs tailored to individual needs
- Full desktop display mode
- Print command controls for local printing
- Help and notification text area per application
- Run multiple applications simultaneously

### Networking & Routing

- Multiple domains
- Private subnets
- Static routing
- Dual Interface configuration

### Performance

- Dynamic bandwidth optimization
- Application server session load balancing
- Fail-over & redundancy
- 24-bit color support

### Maintenance Features & Support

- Platform performance monitoring
- Application usage monitoring
- Remote automated updates and upgrades
- Netilla Upgrade GeNIE for secure updates



Tel: 732-652-5200 Web: [www.netilla.com](http://www.netilla.com)

© 2004 Netilla Networks, Inc. All rights reserved.  
Netilla is a registered trademark of Netilla Networks, Inc.  
All other brand or product names are trademarks or registered trademarks of their respective holders. SST050103

## Access Modes

### 1 Thin-Client Application Access

### 2 Secure Intranet Access

### 3 Desktop Access for Client/Server Applications

Technology	Browser-based Thin-Client Protocol	HTTP Reverse Proxy	SSL Tunneling
<b>Optimal Use</b>	Extranet Partners Branch Facilities ASP/MSP Solutions Internal Security Gateway Thin-Client Terminals Mobile Workers Internet Kiosks	Extranet Partners Internal Security Gateway Branch Facilities Thin-Client Terminals Mobile Workers Internet Kiosks	Sales and Field Personnel Needing Offline Access Trusted Employees Network Administrators
<b>Supported Applications</b>	Microsoft Windows UNIX® X Window System Linux™ and Character-based UNIX Mainframe 3270	Web-based applications Intranet applications Enterprise portals	Windows-based TCP applications Windows-based UDP applications