Netilla® Security Platform

Technical Data Sheet

Application Gateway for the Modern Enterprise

The Netilla® Security Platform (NSP) is a clientless, 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 infrastructures, 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 Web-based intranet resources, remotely located client/server applications, and local client/server desktop applications. Access is controlled through the flexible Netilla SecureRealm Framework®, 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. Clientless access to remote client/server applications
2. Secure intranet access to Web-based applications and portals
3. Desktop client/server connection via SSL tunneling

1 Access Remote Client/Server Applications

The NSP incorporates Web-enabling technology directly within the platform, providing clientless remote access to legacy applications. This means remote access to centralized Windows, UNIX, Linux, 3270 mainframe, and 5250 AS/400 application without sacrificing speed or security and without third-party server-based software.

- Java-based, integrated thin-client application protocol
- Application Layer Proxy: termination, policy and translation in the DMZ
- Universal application access to centralized Windows, UNIX/Linux, 3270 mainframe and AS/400
- Single applications portal consolidates application access and control into a single secure gateway, simplifying management
- Proprietary data compression ensures optimal performance over any Internet connection, including dial-up

2 Access Web-based Applications and Portals

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.

- Browser-based access to Web resources
- 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
- Filtering of unwanted Web-objects (Java, ActiveX, JavaScript)
- Session control delivers automatic session time-outs

3 Exchange and Synchronize Data From Desktop Applications:

Users who need to work offline on their local PC-based TCP and UDP applications - such as Outlook, CRM, sales tools, productivity applications, and multimedia programs - can update their files and exchange data with corporate servers through Netilla's desktop access for client/server applications. Netilla facilitates a connection by establishing a secure SSL tunnel with the remote server whenever a user has Internet access. Netilla's virtual adapter, seamlessly downloaded upon initial login, gives users full functionality of their desktop applications, while ensuring timely updates to remain "in sync" with centrally hosted data.

- Broad application support: UDP and TCP
- Dynamic session-based firewall provides application port availability on a session-by-session basis
- Transparent Netilla virtual adapter: No application configuration required
- Network Address Translation (NAT) compatible

Security

Netilla's breadth of security features keeps your business-critical resources safe from potential risks. From browser-embedded SSL encryption to the Netilla SecureRealm Framework, the NSP can leverage security solutions already in place, such as leading 2-factor authentication systems and the prevailing policy engines used in today's enterprise environment. To further guard private network resources, the NSP incorporates a dynamic, session-based and stateful inspection firewall, along with application-layer proxy technology that prevents exposure of information to unauthorized users. Plus, the Netilla Upgrade GeNIE ensures fast deployment of security and feature updates.

Security

General
- 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
- Automated security patches and system software updates

Authorization
- Support for local groups
- Compatible with Microsoft® Windows 2000 Global groups
- Compatible with Microsoft Active Directory
- Application access control by user or groups

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

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

Operating Architecture
- Application layer proxy
- Hardened Linux O/S
- Hardened Apache® Web-server

Firewall
- Internal dual-Ethernet protection option
- Stateful-inspection technology
- Firewall transversal to limit port openings
- Ideal for multi-layer firewall designs
- Session-based for controlling desktop application access

Management and Reporting
- Firewall logs and diagnostic tools
- User audit trails by application
- No client software or local configuration of applications
- Non-intrusive deployment
- Only requires port 443
- Compatible with third-party access and Authentication protocols

Platform

Network Requirements
- Dedicated Internet access with static IP address
- Bandwidth requirements for remote desktop- Minimum 28.8 kbps/connection
- 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 3270 emulation support

Browser Requirements
- Microsoft Internet Explorer 5.0 or higher
- Netscape version 4.7
- Java-enabled browser for thin client access
- ActiveX-enabled browser (Windows 98+) for desktop client/server access

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. equipment rack.
Weight: 15 lbs. (6.8 kg)

Power Requirements
Input rating 100-240 V, 50/60 Hz
Power Consumption: 5.3 amps

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

Operating Environment
32oF to 95oF (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 - CSA

Application

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

E-mail
- Microsoft Exchange or other IMAPe-mail servers
- Outlook Web client or other Web-based e-mail
- Optional Netilla e-mail client
- Real-time e-mail access (No synchronization)
- Client Drive Mapping

Printing
- Redirection to local or network printers
- Session printer management

User Interface
- Customizable login page
- Service access tabs tailored to individual needs
- Full desktop display mode
- Print command controls to pause or stop 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 software
- Application server session load balancing
- Fail-over & redundancy

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

Netilla®
Making the remote accessible®

Tel: 732-652-5200 Web: www.netilla.com

© 2003 Netilla Networks, Inc. All rights reserved.
Netilla and Making the remote accessible are registered trademarks of Netilla Networks, Inc. All other brand or product names are trademarks or registered trademarks of their respective holders. **SST050103-2**

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
Optimal Use	Extranet Partners Branch Facilities ASP/MSP Solutions Internal Security Gateway Thin-Client Terminals Mobile Workers	Extranet Partners Internal Security Gateway Branch Facilities Thin-Client Terminals Mobile Workers Internet Kiosks	Sales and Field Personnel Who Need Offline Access Trusted Employees Network Administrators
Supported Applications	Microsoft Windows UNIX® X Window System Character-based UNIX Linux™ Mainframe 3270 AS/400 5250	Web-based applications Intranet applications Enterprise portals	Windows-based TCP applications Windows-based UDP applications