

White Paper

Provision by Purpose

A Guide to Selecting NetScreen Secure Access SSL VPN Access Methods

Johnnie Konstantas
Senior Manager, Product
Management



Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, CA 94089 USA
408 745 2000 or 888 JUNIPER
www.juniper.net

Part Number: 200081-001 Apr 2004

Contents

Contents	2
Executive Summary	3
Access Methods Primer	3
Clientless: Core Access	3
Thin Client Application Proxy: Secure Application Manager (SAM)	4
Thin Client Network Proxy: Network Connect (NC)	5
Provisioning by Purpose	6
Business Example #1:	6
Business Example #2:	7
Business Example #3:	8
Summary	10

Executive Summary

Over the last two years, appliance-based SSL VPNs have completely redefined “remote access” and Juniper Network’s NetScreen Secure Access family of SSL VPNs (formerly Neoteris) have led the way. What was once expensive functionality reserved for corporate power users when traveling is now a business enabler (i.e. connectivity for diverse enterprise constituencies). Browser-based clientless access means IT professionals, including e-Business directors and enterprise administrators, can use the same solution to tailor resource access based on business directives. The NetScreen Secure Access SSL VPN product line uniquely enables secure access for corporate power users, telecommuters, business partners, customers and intranet users by combining multiple SSL-based access methods with powerful access privilege management and security controls. The flexibility of the broad array of options available with Juniper’s NetScreen SSL VPN products necessitates an understanding of how to best make use of all available functions. Options in access method and access controls mean associated tradeoffs in accessible resources, security, and cost of ownership.

This paper explains how enterprises can leverage Juniper’s NetScreen Secure Access appliances to maximize business opportunity while also reducing security risks and costs. It should be noted that although all NetScreen Secure Access connectivity and administrative controls are available for all use cases, there are certain combinations which best meet given business needs. The guidelines contained in this document define typical use cases and their constituent requirements. Based on these case studies, the optimal security, resource and cost combinations of NetScreen Secure Access functions and controls are put forth.

Access Methods Primer

Juniper Network’s NetScreen Secure Access solutions combine three SSL-based access methods within a single appliance. The three options, clientless Web-based access or “Core Access”, thin-client application proxy or Secure Application Manager (SAM), and thin-client full network connectivity or Network Connect (NC) combined with powerful access provisioning and management tools, specifically map to key enterprise requirements. These can be provisioned from a single appliance to serve various user constituencies and business needs.

Clientless: Core Access

Core Access uses the SSL support present in Web browsers and standards-based email clients, including PDAs and other handheld devices. Core Access represents the lowest total cost of ownership because there are no helpdesk or desktop support costs associated with deployment. Enterprises can provision access to the largest potential user base, including remote and mobile employees, business partners and temporary employees. Core Access has:

- No operating system (OS) dependencies,
- Works with different browsers and OSs

Since Core Access requires only a Web browser at the client it offers clear benefits:

- Minimum requirements: “standard” Web browser and internet connection

- No client-side or server-side changes required to existing applications or network infrastructure
- Access from any device (i.e. corporate PC, personal PC, kiosk, PDA, etc.)
- No software agent required
- No OS or JVM compatibility issues
- Security policy controls at the URL and parameter level
- Granular auditing at the URL, file and host level

Core Access (Clientless)			
Security	Resources	Pros	Cons
Strong Authentication <ul style="list-style-type: none"> • Password(Radius) • Tokens • Digital Certificates 	Web Apps: <ul style="list-style-type: none"> • Static HTML • Scripted: Javascript, DHTML, VBScript, etc... Java Apps: <ul style="list-style-type: none"> • TCP Sockets • HTTP/S 	<ul style="list-style-type: none"> • Lowest Overall TCO • Most Granular Access Controls • Broadest User/Device Accessibility 	Access limited to Web-based applications, file shares, standards based mail and terminal hosts
Granular Authorization <ul style="list-style-type: none"> • By user identity, role, device type, network type • To the file, URL, resource level 	File Shares: <ul style="list-style-type: none"> • Windows • Unix 		
Detailed Application Layer Auditing	Terminal Emulation: <ul style="list-style-type: none"> • SSH/Telnet (native) • Citrix JICA • MS TS • Tarantella, etc. 		

Thin Client Application Proxy: Secure Application Manager (SAM)

Secure Application Manager for Java (J-SAM) or Windows (W-SAM) acts as an application proxy for accessing client/server applications. This agent-based technology extends browser-based access to client/server applications in a transparent manner. Because it proxies applications by port forwarding traffic, capturing all traffic generated by an application, or by capturing all traffic bound for a range of internal hosts, it adds to the complexity of the deployment relative to Core Access. Utilizing J-SAM or W-SAM extends broad support for client/server applications to remote and mobile employees, partners and intranet users without the security risks or cost of traditional remote access VPNs. The NetScreen Secure Access SAM offers the following benefits:

- Minimal requirements: “standard” Web browser, Internet connection, and compatible Java VM (for J-SAM) or MS Windows OS (for W-SAM).
- Automatic and transparent provisioning of application connections to messaging servers, files servers, legacy servers, and other client-server resources
- No administrative changes required for enabling access to either the network, the network addressing scheme, or the applications being accessed

All Juniper access methods function across complex network topologies without Network Address Translation (NAT), firewall, or proxy-gateway traversal issues, but because SAM captures the complete application stream (rather than each application request as with Core Access) access controls are applied at the host level. The net result is that while access controls with Core Access can be applied at the file and URL level, SAM access controls are applied by resource name and IP address, an arguably less granular set of controls.

Enterprises can choose to provision Core Access for Web content and SAM connectivity for certain session types like access to proprietary messaging servers, server-based computing systems from Citrix or Microsoft, or legacy and custom applications. By leveraging the NetScreen Secure Access integration with the broadest set of authentication and directory stores, as well as the powerful administration tools provided with Secure Access gateways, administrators can define user groups and use cases that invoke SAM on an “as needed basis.”

Thin-Client Application Proxy: Secure Application Manager (SAM)			
Security	Resources	Pros	Cons
Strong Authentication <ul style="list-style-type: none"> • Password(Radius) • Tokens • Digital Certificates 	Client Server Applications <ul style="list-style-type: none"> • Static Port TCP • Dynamic Port TCP • NetBIOS Tunneling 	Access to popular mail programs and specialized applications	Adds some administrative complexity & cost Adds OS or JVM dependencies Less granular access controls
Host/Application level authorization & auditing <ul style="list-style-type: none"> • Client-side & Server-side ACLs • MD5 Checksum Validation 			

Thin Client Network Proxy: Network Connect (NC)

For employees and IT personnel that require unfettered resource access (as though “on the LAN”) Juniper’s Network Connect (NC) offers a lightweight agent-based network connection that can be provisioned to authenticated and authorized users “on the fly.” Network Connect extends the broadest form of remote connectivity without requiring desktop software installations because it uses protocols (PPP, SSL) and applications (Internet Explorer, browsers) already resident on most PCs. Network Connect is dynamically provisioned and transparently invoked creating a network layer tunnel between the access requestor and the Secure Access gateway. The method allows for the delivery of all types of functionality including server-initiated and UDP based applications to the network administrators and corporate power users that typically have need of them. However, since Network Connect provides a path to all corporate resources, it also represents a potential point of vulnerability that requires additional security provisioning. As with IPSec VPNs, this “tunnel” constitutes a theoretically exploitable path to sensitive resources. For this reason, Juniper recommends controlling access to employees connecting from managed devices as well as use of the end-point security mechanisms provided with the Secure Access products including the Host Checker API. It is advisable to use Network Connect in conjunction with personal firewall technologies that protect from U-turn attacks where a tunnel to the network is used to carry hacker traffic.

Thin-Client Network Proxy (NC)			
Security	Resources	Pros	Cons
Strong Authentication <ul style="list-style-type: none"> • Password(Radius) • Tokens • Digital Certificates 	Full IP Network Access	<ul style="list-style-type: none"> • Full network layer connectivity • Broadest access to any application & service • VPN w/out a client 	<ul style="list-style-type: none"> • Highest TCO • Adds Administrative complexity & OS dependencies • Least granular access controls
Authorization <ul style="list-style-type: none"> • IP address • Port range 			

Provisioning by Purpose

The Instant Virtual Extranet (IVE), platform on which the NetScreen Secure Access products are based, provides the functionality to meet all remote, intranet and extranet access use cases. Selecting the right configuration alternatives can bring together seemingly diametrically opposed goals: *maximizing security and breadth of access*. A process for doing this cost effectively starts with identifying the business purpose.

Business Example #1:

Providing access to business partners, contract and temporary employees and other non-employees of the corporation.

The key three requirements:

- Access to web
- User self service
- Ease of administration

Description: In this use scenario, focus is on extending Web-based resources like partner extranets to individuals whose devices and networks are not managed internally. Since connection requests are originating from untrusted entities, resource access is typically highly restricted. Strong authentication and endpoint security solutions cannot be assumed as requirements since the end users will have varying configurations based on the security policies of their organizations. This scenario likely serves large numbers of users whose identities and profiles are ever-changing, making ease of administration and user self-service key requirements for the enterprise which serves them. The chart below summarizes the security, resource and costs for SSL VPN access followed by the recommended Juniper Secure Access connectivity method.

Connecting Business Partners & Non-Corporate Employees		
SECURITY	RESOURCES	COST
Authentication <ul style="list-style-type: none"> <input checked="" type="checkbox"/> Password/Native <input type="checkbox"/> Two-factor <input type="checkbox"/> Digital Certificates 	Intranet <ul style="list-style-type: none"> <input checked="" type="checkbox"/> Web applications <input checked="" type="checkbox"/> Java applets 	<ul style="list-style-type: none"> <input checked="" type="checkbox"/> Secure Access Gateway appliance <input type="checkbox"/> Strong authentication architecture
Authorization Policy <ul style="list-style-type: none"> <input checked="" type="checkbox"/> Native <input checked="" type="checkbox"/> By file, URL, resource level 	<ul style="list-style-type: none"> <input checked="" type="checkbox"/> File Access/File Servers 	<ul style="list-style-type: none"> <input type="checkbox"/> Help-desk Support for thin-client <input type="checkbox"/> Administration of complex policies <input type="checkbox"/> External directory

<input type="checkbox"/> Host level Access Controls <input type="checkbox"/> LDAP <input type="checkbox"/> Active Directory <input type="checkbox"/> By IP address/port		
User Identity & Profile <input checked="" type="checkbox"/> By role <input checked="" type="checkbox"/> By group <input checked="" type="checkbox"/> Dynamic	Email Access <input checked="" type="checkbox"/> Webmail <input type="checkbox"/> Client-based	<input type="checkbox"/> Incremental End-point Security Software (i.e. personal firewall)
Network Attributes <input type="checkbox"/> Trusted <input checked="" type="checkbox"/> Untrusted	<input type="checkbox"/> Client-Server Applications	
Device Being Used <input checked="" type="checkbox"/> Unmanaged <input type="checkbox"/> Managed	Server-based computing <input checked="" type="checkbox"/> Vx00 Term. (native) <input checked="" type="checkbox"/> Citrix <input checked="" type="checkbox"/> MS TS <input checked="" type="checkbox"/> Tarantella, etc.	
End-Point Security <input checked="" type="checkbox"/> Web-based SSO <input checked="" type="checkbox"/> Cache controls <input checked="" type="checkbox"/> URL filters & encoding <input type="checkbox"/> Application integrity validation (MD5) <input type="checkbox"/> Cache cleaning <input type="checkbox"/> Host Check <input type="checkbox"/> 3 rd party product check <input type="checkbox"/> Session mobility/persistence	Network Access <input type="checkbox"/> Server Initiated Applications <input type="checkbox"/> VoIP <input type="checkbox"/> SIP/H.323 <input type="checkbox"/> Wireless LAN <input type="checkbox"/> Full IP Network Access	
Recommended Access Method: Core Access		

Business Example #2:

Providing access to telecommuters, mobile employees, kiosk and PDA users

Description: It is very often the case that enterprises extend intranet and email access to telecommuters and mobile employees. A common configuration includes access to proprietary mail servers (i.e. Exchange, Domino), ERP and CRM applications as well as some legacy or custom applications. Devices used to connect may vary from kiosks to Internet-enabled handhelds so both the endpoint devices and they networks on which they reside when requesting access are untrusted. There is, however, a higher degree of security confidence in this use case, if customers have deployed architectures for strong authentication (i.e. tokens, digital certificates) and/or end-point security tools (via Host Checker, Cache Cleaner, etc.). These groups can use SAM (WSAM or JSAM) for access to client/server applications. Core Access is also available to these same users where access to Web content and Web-mail is all that is required.

Connecting Remote Employees of the Enterprise		
SECURITY	RESOURCES	COST
Authentication <input type="checkbox"/> Password/Native <input checked="" type="checkbox"/> Two-factor <input checked="" type="checkbox"/> Digital Certificates	Intranet <input type="checkbox"/> Web applications <input type="checkbox"/> Java applets	<input checked="" type="checkbox"/> Secure Access Gateway appliance <input checked="" type="checkbox"/> Strong authentication architecture
Authorization Policy <input checked="" type="checkbox"/> Native <input type="checkbox"/> By file, URL, resource level <input checked="" type="checkbox"/> Host level Access Controls <input checked="" type="checkbox"/> LDAP <input checked="" type="checkbox"/> Active Directory <input type="checkbox"/> By IP address/port	<input type="checkbox"/> File Access/File Servers	<input checked="" type="checkbox"/> Help-desk Support for thin-client <input checked="" type="checkbox"/> Administration of complex policies <input checked="" type="checkbox"/> External directory
User Identity & Profile <input checked="" type="checkbox"/> By role <input checked="" type="checkbox"/> By group <input checked="" type="checkbox"/> Dynamic	Email Access <input type="checkbox"/> Webmail <input checked="" type="checkbox"/> Client-based	<input type="checkbox"/> Incremental End point Security Software(i.e. personal firewall)
Network Attributes <input type="checkbox"/> Trusted <input checked="" type="checkbox"/> Untrusted	<input checked="" type="checkbox"/> Client-Server Applications	
Device Being Used <input checked="" type="checkbox"/> Unmanaged <input checked="" type="checkbox"/> Managed	Server-based computing <input type="checkbox"/> Vx00 Term. (native) <input type="checkbox"/> Citrix <input type="checkbox"/> MS TS <input type="checkbox"/> Tarantella, etc.	
End-Point Security <input checked="" type="checkbox"/> Web-based SSO <input checked="" type="checkbox"/> Cache controls <input checked="" type="checkbox"/> URL filters & encoding <input checked="" type="checkbox"/> Application integrity validation (MD5) <input checked="" type="checkbox"/> Cache cleaning <input checked="" type="checkbox"/> Host Check <input checked="" type="checkbox"/> 3rd party product check <input checked="" type="checkbox"/> Session mobility/persistence	Network Access <input type="checkbox"/> Server Initiated Applications <input type="checkbox"/> VoIP <input type="checkbox"/> SIP/H.323 <input type="checkbox"/> Wireless LAN <input type="checkbox"/> Full IP Network Access	
Recommended Access Method: Secure Application Manager (SAM)		

Business Example #3:

Providing secure access to corporate employees located on the intranet, on Wireless LANs and to fixed telecommuters with home networks.

Description: Corporate “power users” (i.e. IT personnel, network administrators and directors as well as executive staff) often have need for robust network access including UDP-based applications which use dynamic ports. This user constituency, as well as those working on wireless LANs or the intranet, need a connectivity experience that is equivalent to being “on network” or, in other words, unfettered access to resources, services and applications of any type. For these users a full IP connection is appropriate. Strong authentication and careful Access Control List (ACL) creation are musts for provisioning users belonging to this group.

Connecting Remote Employees of the Enterprise		
SECURITY	RESOURCES	COST
Authentication <input type="checkbox"/> Password/Native <input checked="" type="checkbox"/> Two-factor <input type="checkbox"/> Digital Certificates	Intranet <input type="checkbox"/> Web applications <input type="checkbox"/> Java applets	<input checked="" type="checkbox"/> Secure Access Gateway appliance <input checked="" type="checkbox"/> Strong authentication architecture
Authorization Policy <input checked="" type="checkbox"/> Native <input type="checkbox"/> By file, URL, resource level <input type="checkbox"/> Host level Access Controls <input checked="" type="checkbox"/> LDAP <input checked="" type="checkbox"/> Active Directory <input checked="" type="checkbox"/> By IP address/port	<input type="checkbox"/> File Access/File Servers	<input checked="" type="checkbox"/> Help-desk Support for thin-client <input checked="" type="checkbox"/> Administration of complex policies <input checked="" type="checkbox"/> External directory
User Identity & Profile <input checked="" type="checkbox"/> By role <input checked="" type="checkbox"/> By group <input checked="" type="checkbox"/> Dynamic	Email Access <input type="checkbox"/> Webmail <input type="checkbox"/> Client-based	<input checked="" type="checkbox"/> Incremental End-point Security Software (i.e. personal firewall)
Network Attributes <input checked="" type="checkbox"/> Trusted <input type="checkbox"/> Untrusted	<input type="checkbox"/> Client-Server Applications	
Device Being Used <input type="checkbox"/> Unmanaged <input checked="" type="checkbox"/> Managed	Server-based computing <input type="checkbox"/> Vx00 Term. (native) <input type="checkbox"/> Citrix <input type="checkbox"/> MS TS <input type="checkbox"/> Tarantella, etc.	
End-Point Security <input checked="" type="checkbox"/> Web-based SSO <input checked="" type="checkbox"/> Cache controls <input checked="" type="checkbox"/> URL filters & encoding <input checked="" type="checkbox"/> Application integrity validation (MD5) <input checked="" type="checkbox"/> Cache cleaning <input checked="" type="checkbox"/> Host Check <input checked="" type="checkbox"/> 3rd party product check	Network Access <input checked="" type="checkbox"/> Server Initiated Applications <input checked="" type="checkbox"/> VoIP <input checked="" type="checkbox"/> SIP/H.323 <input checked="" type="checkbox"/> Wireless LAN <input checked="" type="checkbox"/> Full IP Network Access	

<input checked="" type="checkbox"/> Session mobility/persistence		
Recommended Access Method: Network Connect (NC)		

Summary

Once the business need has been identified, provisioning access is easy. Administrators need only create user groups that correspond to the business need (i.e. partners, contractors, temporary employees, telecommuters, wireless LAN users) and merely associate the access method and security controls which apply to each. When the security, resource and TCO concerns outlined above are assessed, it is very often the case that even large user groups can be mapped to a few major constituencies. Most importantly, Juniper Network's NetScreen Secure Access allows for dynamic provisioning of the connectivity type based on the need. Meaning that any of the three access methods can be applied for a given user or user group based on where the user is located, the type of network and device being used and the resources to which access is required.

It is important to note that while other vendors may provide some subset of functionality that is similar to the three Secure Access connectivity methods, none has equivalent product depth in the critical security and access management controls. Without these, access provisioning that is cost effective and commensurate with security best practices is not possible.

Copyright © 2004 Juniper Networks, Inc. All rights reserved.

Juniper Networks, the Juniper Networks logo, NetScreen, NetScreen Technologies, Neoteris, Neoteris-Secure Access, Neoteris-Secure Meeting, NetScreen-SA 1000, NetScreen-SA 3000, NetScreen-SA 5000, IVEGigaScreen, and the NetScreen logo are registered trademarks of Juniper Networks, Inc. NetScreen-5GT, NetScreen-5XP, NetScreen-5XT, NetScreen-25, NetScreen-50, NetScreen-100, NetScreen-204, NetScreen-208, NetScreen-500, NetScreen-5200, NetScreen-5400, NetScreen-Global PRO, NetScreen-Global PRO Express, NetScreen-Remote Security Client, NetScreen-Remote VPN Client, NetScreen-IDP 10, NetScreen-IDP 100, NetScreen-IDP 500, GigaScreen ASIC, GigaScreen-II ASIC, and NetScreen ScreenOS are trademarks of Juniper Networks, Inc. All other trademarks and registered trademarks are the property of their respective companies.

Information in this document is subject to change without notice.

No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without receiving written permission from:

Juniper Networks, Inc.
1194 N. Mathilda Ave.Sunnyvale, CA 95014 ATTN: General Counsel