Juniper Networks **NetScreen-SA 3000 Series**

The Juniper Networks NetScreen-SA 3000 Series of SSL VPNs enable mid-to-large-sized organizations to provide cost effective remote access, partner extranet, and intranet security. Users can securely access corporate applications and resources from any standard Web browser. Based on the award-winning Instant Virtual Extranet (IVE) platform, the NetScreen-SA 3000 Series appliances feature rich access privilege management functionality that can be used to create secure customer/partner extranets with no infrastructure changes, no DMZ deployments, and no software agents. This functionality also allows the enterprise to secure access to the corporate intranet, so that different employee and visitor populations can utilize exactly the resources that they need while adhering to enterprise security policies.

NetScreen-SA 3000 Series products can be purchased with either Baseline or Advanced software feature sets. Baseline software encompasses the streamlined feature set that an enterprise would need to deploy secure remote access, as well as a basic customer/partner extranet or secure intranet. The Advanced products have additional sophisticated features that meet the needs of more complex deployments with diverse audiences and use cases.

Value Summary

Rich Access Privilege Management Capabilities
- Dynamic, controlled access at the URL, file, application and server level, based on a variety of session-specific variables including identity, device, security control and network trust level

Provision by Purpose
- Three different access methods allow administrators to balance security and access on a per-user, per-session basis

End-to-End Layered Security
- Numerous security options from the end user device, to the application data and servers

High Availability
- Cluster pair deployment option, for high availability across the LAN and the WAN

Lower Total Cost of Ownership
- Secure remote access with no client software deployments or changes to servers, and virtually no ongoing maintenance
- Secure extranet access with no DMZ buildout, server hardening, resource duplication, or incremental deployments to add applications or users

Streamlined Manageability
- Central management option for unified administration
- User self service features enhance productivity while lowering administrative overhead

Access Privilege Management Capabilities

The NetScreen-SA 3000 Series appliances provide dynamic access privilege management capabilities without infrastructure changes, custom development, or software deployment/maintenance. This facilitates the easy deployment and maintenance of secure remote access, as well as secure extranets and intranets.

When a user logs in to the NetScreen-SA 3000, they pass through pre-authentication assessment, and then are dynamically mapped to the session role that combines established network, device, identity and session policy settings. Granular resource authorization policies further ensure exact compliance to security strictures.

Feature	Benefit
Hybrid role- / resource-based policy model	Administrators can tailor access to dynamically ensure that security policies reflect dynamic business requirements
Pre-authentication assessment	Network and device attributes, including presence of Host Checker/Cache Cleaner, source IP, browser type and digital certificates, can be examined even before login is allowed and results are used in dynamic policy enforcement decisions
Dynamic authentication policy	Leverages the enterprise's existing investment in directories, PKI, and strong authentication, enabling administers to establish a dynamic authentication policy for each user session
Dynamic role mapping	Combines network, device and session attributes to determine which of three different types of access is allowed, allowing the administrator to provision by purpose for each unique session
Resource authorization	Enables extremely granular access control to the URL, server, or file level to tailor security policies to specific resources
Granular auditing and logging	Fine-grained auditing and logging capabilities in a clear, easy-to-understand format to the per-user, per-resource, and per-event level can be used for security purposes as well as capacity planning
Custom expressions *Advanced software feature set*	Enable the dynamic combination of attributes on a "per-session" basis, at the role definition/mapping rules and the resource authorization policy level.
Web-based Single Sign-On - BASIC Auth & NTLM	Alleviates the need for end users to enter and maintain multiple sets of credentials for Web-based and Microsoft applications
Web-based Single Sign-On - forms-based and header-variable-based *Advance software feature set*	In addition to BASIC Auth and NTLM SSO, the advanced feature set provides the ability to pass user name, credentials and other customer defined attributes to the authentication forms of other products and as header-variables, to enhance user productivity and provide a customized experience

Provision by Purpose

The NetScreen-SA 3000 Series includes three different access methods. These different methods are selected as part of the user's role, so the administrator can enable the appropriate access on a per-session basis, taking into account user, device, and network attributes in combination with enterprise security policies.

Feature	Benefit
Clientless core Web access	Access to Web-based applications, including complex JavaScript apps and Java applets that require a socket connection, as well as standards-based e-mail, files and telnet/SSH hosted applications. Provides the most easily accessible form of application and resource access, and enables extremely granular security control options
Secure Application Manager (SAM)	A lightweight Java or Windows-based download enables access client/server applications using just a Web browser
Network Connect	Provides complete network-layer connectivity via an automatically provisioned Windows-based download for those users that require it, using a Web browser

End-to-End Layered Security

The NetScreen-SA 3000 series provides complete end-to-end layered security, including endpoint client, device, data and server layered security controls. These include:

Feature	Benefit
Native Host Checker	Client computers can be checked at the beginning and throughout the session to verify an acceptable security posture by checking the registry for pre-defined files, processes and ports, with MD5 hash checksum validation to verify the authenticity of the applications
Host Checker API Hardened security appliance and Web server	Created in partnership with best-of-breed endpoint security vendors, checks that specified security services are running at login and throughout the session, protecting both the network and the user.
Security services employ kernel-level packet filtering and safe routing.	Hardened security infrastructure, audited by 3rd party security experts including TruSecure, effectively protects internal resources and lowers total cost of ownership by minimizing the need to patch servers on an ongoing basis.
Cache Cleaner	Ensures that unauthenticated connection attempts, such as malformed packets or DOS attacks are filtered out.
Data trap & cache control	All proxy downloads and temp files installed at login are erased at logout, ensuring that no data is left behind.
FIPS - Cryptographic key handling in a certified module	Prevents sensitive meta-data (cookies, headers, form entries, etc) from leaving the network, and allows for rendering of content in a non-cacheable format Purpose built appliances, incorporating a FIPS 140-2 level 3 certified Hardware Security Module (HSM), adheres to US Federal government procurement guidelines, as per NSTISSP No. 11

Lower Total Cost of Ownership

In addition to enterprise-class security benefits, the NetScreen-SA 3000 Series has a wealth of features that enable low total cost of ownership.

Feature	Benefit
Uses SSL, available in all standard Web browsers	Secure remote access with no client software deployment and no changes to existing servers
Based on industry-standard protocols and security methods	The investment in the NetScreen-SA 3000 Series can be leveraged across many applications and resources over time
User self-service features	Increases end user productivity, greatly simplifies administration of large diverse user groups, and lowers support costs, with features that include including password management integration and Web Single Sign-On
Multiple Hostname Support Advanced software feature set	Provides the ability to host different virtual extranet Websites from a single NetScreen-SA 3000 Series appliance, saving the cost of incremental servers, easing management overhead and providing a transparent user experience with differentiated entry URLs
Customizable User Interface Advanced software feature set	Allows the creation of completely customized sign-in pages to give an individualized look for specified roles, streamlining the user experience

High Availability

The NetScreen-SA 3000 Series includes a variety of capabilities for the availability and redundancy required for mission-critical access in demanding enterprise environments.

Feature	Benefit
Stateful peering	Units that are part of a cluster pair synchronize system-state, user profile-state, and session-state data among a group of appliances in the cluster for seamless failover with minimal user downtime and loss of productivity
Clustering	Cluster pairs multiply aggregate throughput to handle unexpected burst traffic as well as resource-intensive application use. Clusters can be deployed in either Active/Passive or Active/Active modes, as well as in a single site or across multiple Points of Presences (POPs). Cluster pairs can be deployed across the LAN or across the WAN for superlative scalability with a large number of user licenses, which scales access as the user base grows.

Juniper Networks NetScreen-SA 3000 Series

Streamlined Management and Administration

The NetScreen-SA 3000 includes a variety of features available from a central management console at the click of a button. These benefits are extended across clustered devices, with the addition of NetScreen-SA Central Manager, a robust product with an intuitive Web-based UI designed to facilitate the task of configuring, updating and monitoring Secure Access appliances whether within a single cluster or across a global cluster deployment.

Feature	Benefit
Central Manager	Cluster pairs can be seamlessly managed from an integrated central management console, making administration convenient and efficient. The Central Manager allows administrators to track cluster-wide metrics, push configurations and updates, and provide backup and recovery for local and clustered appliances.
Role-based delegation *Advanced software feature set*	Granular role-based delegation lessens IT bottlenecks by allowing administrators to delegate control of diverse internal and external user populations to the appropriate parties, associating real-time control with business, geographic, and functional needs.
Easy-to-edit role mapping and resource authorization policies	Administrators can copy and re-use existing policies, simplifying the process of setting up complex multi-variable polices or administration for multiple types of groups/roles
Customizable audit log data	Using NetScreen-SA Central Manager, log data can be compiled in standard formats including W3C or WELF, as well as tailored for input into proprietary report packages
SNMP	Enhanced monitoring with standards-based integration to third party management systems

Specifications

Upgrade Options

- Secure Application Manager Upgrade Option
- Network Connect Upgrade Option
- High Availability Clustering Options
- Secure Meeting Upgrade Option

Technical Specifications

NetScreen-Chassis SA 3000

- Dimensions: 17.72”W x 1.74”H x 19”D (45.00cmW x 4.41cmH x 48.26cmD)
- Weight: 18.5lb 8.3916(kg) typical (unboxed)
- Material: 18 gauge (.048”) cold-rolled steel
- Fans: 4 ball-bearing exhaust fans, plus 1 CPU blower

Panel Display

- Front Panel Power Switch
- Power LED

Ports

Network

- Two RJ-45 Ethernet
- 10/100 full or half-duplex (auto-negotiation)
- IEEE 802.3 compliant

Console

- One 9-pin serial console port

Power

- Input Voltage and Current 90-264 VAC Full Range
- 6A (RMS) at 115 VAC
- 3A (RMS) at 230 VAC
- Input Frequency 47 - 63Hz
- Efficiency 65% min, at full load
- Peak Inrush Current 60A max. for 115 VAC
- 90A max. for 230 VAC
- Output Power 350w
- Fans 2 ball-bearing exhaust fans
- Power Supply MTBF 100,000 hours at 25°C

Environmental

- Temperature Range Operating: 5C to 30C (41F to 86F)
- Operating (short term): 0C to 50C (32F to 122F)
- Non-Operating: -30C to 60C (-22F to 140F)
- Relative Humidity Operating: 20% to 80% non-condensing
- Non-Operating: 5% to 95% non-condensing
- Altitude: to 3,000m (10,000ft)
- Shock Operating: 2G at 11ms
- Non-Operating: 30G at 11ms

Safety and Emissions Certification

- Safety: CB to IEC 60950: 1999, 3rd edition; TUV GS mark to EN60950: 2000; TUV C-US to UL60950: 2000; CAN/CSA-C22.2 No 60950: 2000
- Emissions: FCC Class B, VCCI Class B, CE class B

Warranty

- 90 days - can be extended with support contract

Juniper NETWORKS

1194 North Mathilda Avenue Sunnyvale, CA 94089 USA
Phone: 888-JUNIPER (888-586-4737) or 408-745-2000
Fax: 408-745-2100

Part Number: 110016-001 Apr 2004