

Juniper Networks NetScreen-SA 5000 Series



The Juniper Networks NetScreen-SA 5000 Series of SSL VPNs are designed for medium to large enterprises, and feature best-in-class performance, scalability, and redundancy for organizations with high volume secure access and authorization requirements. The NetScreen-SA 5000 Series hardware platform is designed to scale to the largest enterprise deployments and optimize application delivery. The NetScreen-SA 5000 Series appliance, like all products built on the Instant Virtual Extranet (IVE) platform, use Secure Socket Layer (SSL) available in all Web browsers as a means of secure transport. This enables the enterprise to provide remote access to mobile employees and contractors without deploying client software, as well secure extranet or intranet access with no DMZ buildout, server hardening, Web agent deployments, or ongoing maintenance.

NetScreen-SA 5000 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 to 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 Layer Security

- Numerous security options from the end user device, to the application data and servers
- Juniper's Endpoint Defense Initiative includes native functionality as well as client- and server-side APIs for effective enforcement and unified administration of best-of-breed endpoint security

Performance Scalability

- A variety of hardware-based performance enhancing features, including GZIP compression, SSL acceleration, and clustering provide optimal scalability

High Availability

- Various stateful clustering options, offering high availability across the LAN and the WAN

Streamlined Manageability

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

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

Access Privilege Management Capabilities

The NetScreen-SA 5000 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 5000, they pass through a pre-authentication assessment, 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 administrators 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 <i>Advanced software feature set</i>	Enable the dynamic combination of attributes on a "per-session" basis, at the role definition/mapping rules and the resource authorization policy level

Juniper Networks NetScreen-SA5000 Series

Access Privilege Management Capabilities Cont'd

Feature	Benefit
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, Header Variable-based, SAML-based <i>Advanced software feature set</i>	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. SAML-based integration for authentication and authorization

Provision by Purpose

The NetScreen-SA 5000 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 to client/server applications using just a Web browser. Also provides native access to terminal server applications without the need for a pre-installed client
Network Connect	Provides complete network-layer connectivity via an automatically provisioned Windows-based download for those users that require it, using just a Web browser

End-to-End Layered Security

The NetScreen-SA 5000 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 requiring or restricting network ports; checking files/process and validating their authenticity with MD5 hash checksums. Performs version checks on security applications, and carries out pre-authentication checks and enforcement. Enables enterprises to write their own host check method to customize the policy checks
Host Checker API	Created in partnership with best-of-breed endpoint security vendors, enables enterprises to enforce an endpoint trust policy for managed PCs that have personal firewall, antivirus clients, or other installed security clients, and quarantine non-compliant endpoints
Host Check Server Integration API	Enables enterprises to deliver and update third party security agents from the NS-SA 5000, which reduces public-facing infrastructure, enables consolidated reporting of security events, and enables policy-based remediation of non-compliant clients
Policy-based enforcement	Allows the enterprise to establish trustworthiness of non-API-compliant hosts without writing custom API implementations, or locking out external users such as customers or partners that run other security clients
Hardened security appliance and Web server	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
Security services employ kernel-level packet filtering and safe routing	Ensures that unauthenticated connection attempts, such as malformed packets or DOS attacks are filtered out
Cache Cleaner	All proxy downloads and temp files installed at login are erased at logout, ensuring that no data is left behind
Data Trap & cache controls	Prevents sensitive meta-data (cookies, headers, form entries, etc) from leaving the network, and allows for rendering of content in a non-cacheable format

Performance Scalability

The NetScreen-SA 5000 Series hardware platform is specifically designed to accommodate large numbers of users with complex application needs, and provides application performance optimization via compression algorithms. These features allow the appliance to process large, simultaneous transaction loads while minimizing perceptible latency to users.

Feature	Benefit
Hardware-based GZIP HTTP compression	Hardware-based compression of HTTP and file content for faster application performance, particularly for users on low speed, "last mile" connections
Hardware-based SSL acceleration	Offloads compute-intensive encrypt/decrypt process from the CPU, enhancing performance
Dual Gigabit Ethernet interfaces	Enables strong performance in the highest speed enterprise networks
Clustering	Cluster pairs or multi-unit clusters 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

High Availability

The NetScreen-SA 5000 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 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

Streamlined Management and Administration

The NetScreen-SA 5000 Series 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 <i>Advanced software feature set</i>	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 policies 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

Lower Total Cost of Ownership

In addition to enterprise-class security benefits, the NetScreen-SA 5000 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 5000 Series can be leveraged across many applications and resources over time.
Extensive directory integration & broad interoperability	Existing directories can be leveraged for authentication and authorization. Standard-based interfaces and APIs provide seamless integration with 3rd party products
User self-service features	Increases end user productivity, greatly simplifies administration of large diverse user groups, and lowers support costs, with features that include password management integration and Web Single Sign-On
Multiple Hostname Support <i>Advanced software feature set</i>	Provides the ability to host different virtual extranet Websites from a single NetScreen-SA 5000 appliance, saving the cost of incremental servers, easing management overhead and providing a transparent user experience with differentiated entry URLs
Customizable User Interface <i>Advanced software feature set</i>	Allows the creation of completely customized sign-in pages to give an individualized look for specified roles, streamlining the user experience

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 5000

- Dimensions: 17.72"W x 3.5"H x 19"D (45.00cmW x 8.89cmH x 48.26cmD)
- Weight: 23lb 10.45(kg) typical (unboxed)
- Material: 18 gauge (.048") cold-rolled steel
- Fans: 3 ball-bearing exhaust fans, plus 2 CPU chillers

Panel Display

- Front Panel Power Switch
- Power LED

Ports

Network

- Two RJ-45 Ethernet
- 10/100/1000 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



CORPORATE HEADQUARTERS AND SALES HEADQUARTERS FOR NORTH AND SOUTH AMERICA
 Juniper Networks, Inc.
 1194 North Mathilda Avenue
 Sunnyvale, CA 94089 USA
 Phone: 888-JUNIPER (888-586-4737) or 408-745-2000
 Fax: 408-745-2100
www.juniper.net

EAST COAST OFFICE
 Juniper Networks, Inc.
 10 Technology Park Drive
 Westford, MA 01886-3146 USA
 Phone: 978-589-5800
 Fax: 978-589-0800

ASIA PACIFIC REGIONAL SALES HEADQUARTERS
 Juniper Networks (Hong Kong) Ltd.
 Suite 2507-11, Asia Pacific Finance Tower
 Citibank Plaza, 3 Garden Road
 Central, Hong Kong
 Phone: 852-2332-3636
 Fax: 852-2574-7803

EUROPE, MIDDLE EAST, AFRICA REGIONAL SALES HEADQUARTERS
 Juniper Networks (UK) Limited
 Juniper House
 Guildford Road
 Leatherhead
 Surrey, KT22 9JH, U. K.
 Phone: 44(0)1372-385500
 Fax: 44(0)1372-385501

Copyright 2004, Juniper Networks, Inc. All rights reserved. Juniper Networks, the Juniper Networks logo, NetScreen, NetScreen Technologies, the NetScreen logo, NetScreen-Global Pro, ScreenOS, and GigaScreen are registered trademarks of Juniper Networks, Inc. in the United States and other countries. The following are trademarks of Juniper Networks, Inc.: ERX, ESP E-series, Instant Virtual Extranet, Internet Processor, J2300, J4300, J6300, JProtect, Jseries, JWeb, JUNOS, JUNOScope, JUNOScript, JUNOSe, M5, M71, M10, M10i, M20, M40, M40e, M160, M320, M-series, MMD, NetScreen-SGT, NetScreen-SXP, NetScreen-SXT, NetScreen-25, NetScreen-50, NetScreen-204, NetScreen-208, NetScreen-500, NetScreen-5200, NetScreen-5400, NetScreen-IDP 10, NetScreen-IDP 100, NetScreen-IDP 500, NetScreen-Remote Security Client, NetScreen-Remote VPN Client, NetScreen-SA 1000 Series, NetScreen-SA 3000 Series, NetScreen-SA 5000 Series, NetScreen-SA Central Manager, NetScreen Secure Access, NetScreen-SM 3000, NetScreen-Security Manager, NMC-RX, SDX, Stateful Signature, T320, T640, and T-series. All other trademarks, service marks, registered trademarks, or registered service marks are the property of their respective owners. All specifications are subject to change without notice. Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.