

Juniper Networks NetScreen-SA Central Manager



Streamline administration

- Central management for deployments of Juniper Networks NetScreen Secure Access SSL VPNs
- Highly efficient and scalable architecture makes expanding deployments easy to maintain

Optimize performance

- Real-time system/cluster use data
- Automated appliance software updates
- Back-up and restore for rapid disaster recovery

Ensure consistent security policy enforcement

- Synchronization automates propagation of changes within a cluster
- Push technology eliminates incomplete security policy enforcement by sending information to other gateways or clusters

Comprehensive, actionable auditing

- Rich log filtering capabilities for quick searches of critical events
- Detailed archives for easy comparisons

The Juniper Networks NetScreen Secure Access family of appliances has consistently led the SSL VPN market, providing secure access to remote/mobile employees, business partners, and customers. As SSL VPN deployments grow both in cluster size and in breadth of geographic reach, so too has the challenge in providing streamlined, efficient management. Juniper Networks has extended its core competence in the SSL VPN marketplace with the introduction of the Juniper Networks 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. Enterprises can now employ all the benefits of Juniper's award-winning NetScreen Secure Access appliances even more easily and cost-effectively, with scalable, centralized device configuration and maintenance.

Eliminate repetitive admin tasks while enforcing security policies
One of the primary requirements of a strong security policy is its uniform deployment throughout the enterprise. The time-consuming task of replicating and maintaining these policies manually, which is also inherently prone to error, can significantly erode the benefits of a secure access solution no matter how easy that solution is to deploy. NetScreen SA-Central Manager enables consistent security policy enforcement by automating many repetitive tasks, while addressing the complex administration needs of enterprises extending their SSL VPNs to user constituencies around the campus or around the world. NetScreen SA-Central Manager uses sophisticated synchronization mechanisms between NetScreen Secure Access appliances to propagate security access, authentication, and authorization policies as well as device configuration throughout the cluster. Software updates can also be conducted via an automated process that enables maximum system uptime.

Improve performance while expediting capacity planning

With NetScreen-SA Central Manager, administrators also get access to detailed network utilization and performance information from a graphical System Dashboard. The System Dashboard gives a real-time view of capacity utilization graphs as well as system-wide metrics, so administrators can identify usage patterns and better plan for scale. The "snapshot" feature facilitates the archiving of system configurations, providing an overview of past conditions.

Local and global recovery system built-in

In the unlikely event of a failure, Central Manager provides another layer of recovery to the robust solution within the Secure Access appliances themselves. Local backup and restore features give administrators the ability to save configurations in whole or in part so that reverting an appliance or cluster to an earlier configuration state can be accomplished quickly. This same utility gives historical context to configuration changes and administrator access. The Deterministic Cluster Recovery feature optimizes system resilience. By assigning ranks to the nodes within the cluster, administrators can ensure that the most desired configuration state prevails throughout the cluster. Should there be a disruption in member communications, the node with the highest assigned rank propagates the correct cluster state once connectivity is restored.

Centralized functionality that is also cost effective

NetScreen SA-Central Manager is deployed as a software upgrade to existing clusters, rather than as a stand-alone server (an architecture much better suited to large scale networks with many clusters). Even smaller deployments can now get the benefits of centralized management with just the click of a button, and no infrastructure changes. Central Manager runs as an overlay to the existing Secure Access appliance Administrator Console, providing rich functionality in a familiar Web-based user interface. NetScreen SA-Central Manager works seamlessly with the Secure Access and Secure Meeting appliance software to provide one of the most powerful, flexible management portfolios in the SSL VPN industry.



**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-Series, Instant Virtual Extranet, Internet Processor, J2300, J4300, J6300, JProtect, J-series, JWeb, JUNOS, JUNOScope, JUNOScript, JUNOSe, M5, M7i, M10, M10i, M20, M40, M40e, M160, M320, M-series, MMD, NetScreen-SGT, NetScreen-SXP, NetScreen-5XT, 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.