Juniper Networks **NetScreen-Security Manager**

- Centralized, end-to-end lifecycle management for granular control of device configuration, network settings and security policies
- Delegation of administrative roles provides information access to those who need it
- Intuitive GUI simplifies complex tasks such as device configuration, policy creation, and VPN deployment
- Three-tiered architecture maximizes performance and flexibility

Product overview

Juniper Networks NetScreen-Security Manager takes a new approach to security management by providing IT departments with an easy-to-use solution that controls all aspects of the NetScreen device including device configuration, network settings, and security policy. Unlike some solutions that require the use of multiple management tools to control a single device, NetScreen-Security Manager enables IT departments to control the entire device lifecycle with a single, centralized solution. Using NetScreen-Security Manager, device technicians, network administrators and security administrators can work together to improve management efficiency, reduce overhead, and lower operating costs.

Delegation of administrative rights

NetScreen-Security Manager allows enterprise IT departments to delegate appropriate levels of administrative access to specific users for a wide range of tasks, ranging from read-only to full-edit capabilities. Enterprises can provide or restrict information to different individuals or constituencies within the organization, allowing employees to make role-appropriate decisions. Similarly, by enabling—or limiting—system permissions based on skill set, enterprises can support role-based administration where permissions and tasks correspond directly to the enterprise's ideal team structure. Role-based administration can be achieved using the pre-defined roles within NetScreen-Security Manager or by creating a custom role from over fifty assignable tasks within the system. In addition, NetScreen-Security Manager includes several other features to help make the security team more effective.

- Object locking allows multiple administrators to safely modify different policies or devices concurrently
- Comment fields for logs and policies allow the administrative team to communicate the intention of the rules and status of incidents
- Job Manager provides centralized status for all device updates whether in progress or completed

With NetScreen's management approach, enterprises can empower each group or individual responsible for a specific phase of the device lifecycle to make critical security-related decisions with confidence, enhancing security by ensuring that users can only access the required and authorized information.

Simplified management of complex tasks

A key design philosophy of NetScreen-Security Manager is to simplify the complexity of security device administration while maintaining the flexibility to address each organization's diverse needs. To that end, NetScreen-Security Manager provides a single, integrated management interface that allows every device parameter to be controlled from a centralized location. With a few clicks of a mouse, an administrator can configure a device, create a security policy or manage a firmware update. All aspects of a device that can be configured through CLI can be managed through NetScreen-Security Manager. Some of the tools included in NetScreen-Security Manager include:

- Role templates to simplify the creation and management of user permissions
- Device templates to minimize configuration errors by managing any or all aspects of a device or group of devices via a template
- VPN manager to accelerate VPN deployments by creating all the necessary rules after a basic topology has been defined

Logging and reporting

NetScreen-Security Manager includes a high performance log storage mechanism that allows an IT department to collect and monitor detailed historical information on key criteria such as network traffic and security events. Using the built-in reporting capabilities, administrators can quickly generate reports for investigative or compliance purposes. For more extensive analysis, log files can be exported to a third party reporting tool or database. Real-time monitoring includes VPN and device up/down status and high availability cluster monitoring. Logs that are stored within NetScreen-Security Manager can be analyzed in the following manner.

- Log Viewing allows logs stored within the system to be viewed in real time. User-defined filters allow an administrator to perform rapid analysis of security status and events
- Log Investigator provides the ability to correlate high-level log information to look for trends and anomalies
- Log Reporting allows an administrator to generate, view and export reports summarizing logs and alarms originating from the managed firewall/VPN devices

Juniper Networks NetScreen-Security Manager

Architecture

NetScreen-Security Manager's architecture is comprised of a Device Server, a GUI Server, and a lightweight user interface (UI). To address the diverse management needs of the IT staff while maintaining flexibility and performance, a fundamental architectural design decision was made to place all device related functions on the Device Server, while placing all centralized configuration functions in the GUI Server. This separation of Device Server and GUI Server enables performance and flexibility. Both device and GUI components can reside on the same server where cost and/or simplicity are the primary requirements, or reside on separate servers where performance and deployment flexibility are more important. Independent of the chosen deployment of the Device and GUI Servers, the UI provides the single point of access for the administrator to all of the information and capabilities of the system. By utilizing the computational capabilities of the GUI Server for most of the load, the impact on the end-user's system is minimized.

All tiers within NetScreen-Security Manager are connected via a TCP-based communication channel, secured through AES encryption and SHA-1 authentication. By embedding security similar to an IPSec VPN in the communication channel, secure management can be easily deployed in most any network environment.

Feature Overview

Configuration

- Device templates with overrides
- Configure all aspects of device
- Full device import
- Device configuration validation
- Report on configuration differences
- VPN modeling tool
- Route-based and policy-based VPN management
- Full mesh, hub & spoke, combination VPN topologies
- Shared policies
- Rule-based management of antivirus
- Rule-based management of Deep Inspection
- Policy validation
- Shared objects

Logging

- Integrated real-time and historical logs
- Full filtering capabilities
- Saved views per user
- Log flagging/comments for team coordination

Administration

- Role-based administration
- Object locking
- Audit logging
- Domains
- Automated domain versioning
- Job Manager for tracking update status

3rd Party Integration

- Syslog on per-rule basis
- SNMP on per-rule basis

Real-Time Monitoring

- Firewall devices
- VPNs
- NSRP (HA) clusters
- GUI Server CPU usage
- Device Server CPU usage

Reporting

- Firewall reports
- Deep Inspection reports (attacks)
- Screen reports (attacks)
- Administrative reports
- HTML export
- Log Investigator to correlate log information

Secure Communications

- Secure communications at all tiers
- TCP-based communications mechanism
- Encryption: AES, 256 bit
- Authentication: SHA-1

Minimum System Requirements

User Interface	
Operating System Support	Microsoft Windows 2000, Windows NT, and Windows XP
Minimum CPU	400 mHz Pentium II or equivalent
Minimum RAM	256 MB RAM, 512 MB recommended
Minimum Available Disk Space	100 MB
Minimum Connectivity to Server	384kbps (DSL) or LAN
Management Server (GUI Server and Device Server combined)	
Minimum CPU	1 GHz*
Minimum RAM	1 GB*
Minimum Hard Disk	10K rpm disk with at least 18GB
disk space (logs are estimated to	be an average of 100 bytes each)*
Minimum NIC	100 Mbs*
Operating System Support	Solaris 8, Solaris 9, Red Hat Linux 8.0, Red Hat Linux 9.0
Maximum devices managed per server	1000

*Global Pro or Global Pro Express appliance also supported

Device Support

- Juniper Networks NetScreen-5XP
- Juniper Networks NetScreen-5XT
- Juniper Networks NetScreen-5GT
- Juniper Networks NetScreen-25
- Juniper Networks NetScreen-50
- Juniper Networks NetScreen-100
- Juniper Networks NetScreen-204
- Juniper Networks NetScreen-208
- Juniper Networks NetScreen-500
- Juniper Networks NetScreen-5200
- Juniper Networks NetScreen-5400

NetScreen ScreenOS support

- Juniper Networks ScreenOS 4.0.0
- Juniper Networks ScreenOS 4.0.0 DIAL2
- Juniper Networks ScreenOS 4.0.1
- Juniper Networks ScreenOS 4.0.3
- Juniper Networks ScreenOS 5.0.0 and up

Ordering Information

Product	Part Number
Juniper Networks NetScreen-Security Manager, 10 devices	NS-SM-10
Juniper Networks NetScreen-Security Manager, 25 devices	NS-SM-25
Juniper Networks NetScreen-Security Manager, 50 devices	NS-SM-50
Juniper Networks NetScreen-Security Manager, 100 devices	NS-SM-100
Juniper Networks NetScreen-Security Manager, 200 devices	NS-SM-200
Juniper Networks NetScreen-Security Manager, 500 devices	NS-SM-500
Juniper Networks NetScreen-Security Manager, 1000 devices	NS-SM-100

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

Part Number: 110018-001 Apr 2004