

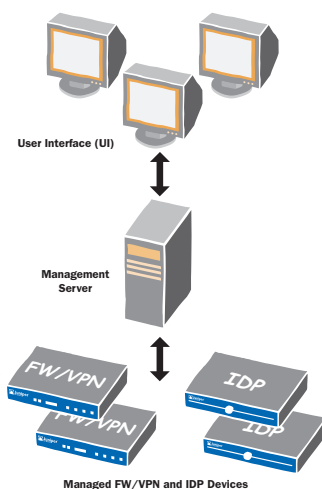
Juniper Networks NetScreen-Security Manager

- Centralized, end-to-end device lifecycle management for granular control of configuration, network settings and security policies
- Delegation of administrative roles provides relevant access to those who need it
- Ease of use and operational efficiency deliver lower TCO

- Complete set of investigative tools provides visibility into what is happening in the network
- Robust architecture provides performance, flexibility and fault tolerance

Product overview

Juniper Networks NetScreen-Security Manager takes a new approach to network and security management by providing IT departments with an easy-to-use solution that controls all aspects of the Juniper Networks FW/VPN and IDP devices 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 and security, 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. 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 or responsibility, 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 one hundred 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
- Job Manager provides centralized status for all device updates whether in progress or completed
- Audit logs provide a record of configuration changes, supporting central oversight of business policy compliance

With Juniper’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.

Ease of use and lower TCO

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. Other tasks, such as security updates on devices, can be automated. Some of the tools included in NetScreen-Security Manager include:

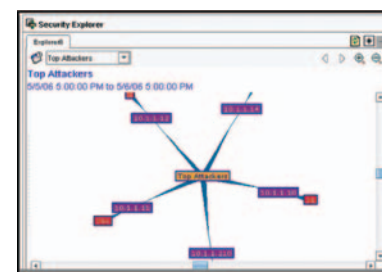
- Device templates to minimize configuration errors by managing any or all aspects of a device or group of devices via a template
- VPN manager to accelerate VPN deployments by creating all the necessary rules after a basic topology has been defined

In addition, managing FW/VPN devices and IDP Sensors through one central system greatly reduces administrative costs.

Complete set of investigative tools

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 complete set of built-in analysis tools, administrators can quickly generate reports for investigative or compliance purposes. For integration into existing tools, logs can be forwarded to a third party reporting tool or database. Logs that are stored within NetScreen-Security Manager can be analyzed in the following manner.

- Log Viewer allows logs to be viewed in real time; user-defined filters allow an administrator to perform rapid analysis of security status and events
- Security Explorer presents an interactive graphical view of the relationships between hosts, networks, services, and attacks
- Report Manager allows an administrator to generate, view and export reports summarizing logs and alarms originating from the managed firewall/VPN and IDP devices
- Profiler (for IDP Sensors) helps administrators baseline network activity and quickly identify new hosts and applications
- Other tools include a dashboard and Log Investigator



NetScreen-Security Manager's Security Explorer

Architecture

NetScreen-Security Manager's architecture is comprised of a Device Server, a GUI Server, and a user interface (UI). To maintain flexibility and performance, all device interaction and log storage is handled by the Device Server, while all configuration information is placed on the GUI Server. 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.

Feature Overview

Configuration

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

Redundancy

- Full High Availability with automatic synchronization and failover

Scalability

- NSM can manage up to 6,000 devices and be deployed in almost any scenario

Logging

- Up to 30,000 logs per second
- Full filtering capabilities
- Saved views per user
- Log flagging/comments for team coordination
- Export logs: XML, CSV

Administration

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

3rd Party Integration

- Log forwarding via Syslog, SNMP, email, scripts, XML, CSV

Real-Time Monitoring

- Firewall and IDP devices
- VPNs
- NSRP (HA) clusters
- Management Server, CPU, memory, disk usage

Reporting and Analysis Tools

- 32 pre-defined report templates
- User customizable reports
- Reports can be scheduled and delivered via email or FTP
- Security Explorer for a graphical view of relationships between hosts, networks, services and attacks
- Log Investigator to correlate log information
- Profiler for application visibility with IDP
- Dashboard
- Statistical Report Server product available as add-on module for SLA and other statistical reports

Architecture

- High Availability
- Secure communications at all tiers
- Flexibility for large and small deployments

Minimum System Requirements

User Interface

Operating System Support	Microsoft Windows 2000, Windows NT, Windows XP, Red Hat Enterprise Linux 3.0, Red Hat Enterprise Linux 4.0
--------------------------	--

Management Server (GUI Server and Device Server combined)

Operating System Support	Solaris 8, Solaris 9, Red Hat Enterprise Linux 3.0, Red Hat Enterprise Linux 4.0
--------------------------	--

Ordering Information

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

Juniper Networks Firewall/VPN and Intrusion Detection and Prevention Device Support

NetScreen-Hardware	SSG 520	IDP 10
Security Client (HSC)	SSG 550	IDP 50
NetScreen-5XP	NetScreen-500	IDP 100
NetScreen-5XT	NetScreen-500 GPRS	IDP 200
NetScreen-5GT	ISG 2000	IDP 500
NetScreen-5GT ADSL	ISG 2000 w/IDP	IDP 600
NetScreen-25	ISG 1000	IDP 1000
NetScreen-50	ISG 1000 w/IDP	IDP 1100
NetScreen-204	NetScreen-5200	
NetScreen-208	NetScreen-5400	

NetScreen ScreenOS Support

ScreenOS 5.4.0	ScreenOS 5.1/5.2/5.3-GPRS	ScreenOS 4.0.3
ScreenOS 5.3.0	ScreenOS 4.0.1	ScreenOS 4.0.1-SBR
ScreenOS 5.2.0	ScreenOS 4.0.1-MCAST	ScreenOS 4.0.1-SIBR
ScreenOS 5.1.0	ScreenOS 4.0.0-DIAL2	ScreenOS 4.0.0
ScreenOS 5.0.0		

