DATASHEET

# NETWORK AND SECURITY MANAGER

## Product Overview

Juniper Networks Network and Security Manager (NSM) is a unified device management solution for Juniper's network infrastructure of routing, switching and security devices. The Network and Security Manager provides centralized, end-to-end device lifecycle management, granular policy configuration and comprehensive monitoring, reporting and investigative tools to enable you to improve IT management and cost efficiencies and to maximize the security of your network. The Network and Security Manager is highly scalable. Enterprise customers can leverage NSM globally to scale from branch to data center, and Service Providers can use it for carrier-class deployments.

## Product Description

Juniper Networks® Network and Security Manager (NSM) takes a new approach to network and security management by providing IT departments with an easy-to-use solution that controls all aspects of Juniper Networks routing, switching, firewall/VPN, and intrusion detection and prevention devices, including device configuration, network settings, and security policy management. Unlike solutions that require the use of multiple management tools to control a single device, Network and Security Manager not only enables IT departments to control the entire device life cycle with a single centralized solution, but also provides visibility with a complete set of investigative and reporting tools. Using NSM, device technicians, network administrators, and security administrators can work together to improve management efficiency and security, reduce overhead, and lower network operating costs.

## Architecture and Key Components

NSM's architecture is comprised of a device server, a GUI server, and a user interface (UI). To maintain flexibility and performance, all device interactions and log storage are 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 they can 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.

Network and Security Manager with Juniper Networks NSM Central Manager (NSM CM) can manage up to 10 regional NSM servers and solves scalability problems by allowing management for up to 6,000 routers, 3,000 switches, 6,000 firewall/VPN devices, or 2,000 firewall/VPN devices with 100 Juniper Networks IDP Series Intrusion Detection and Protection Appliances per regional server. While the NSMXpress is primarily geared towards small to mid market with the capability to manage up to 500 devices, NSM3000 scales to the requirements of large enterprise customers with the capability to manage up to 1500 devices. Together, these provide an overall solution to scale for large enterprise and service provider environments.

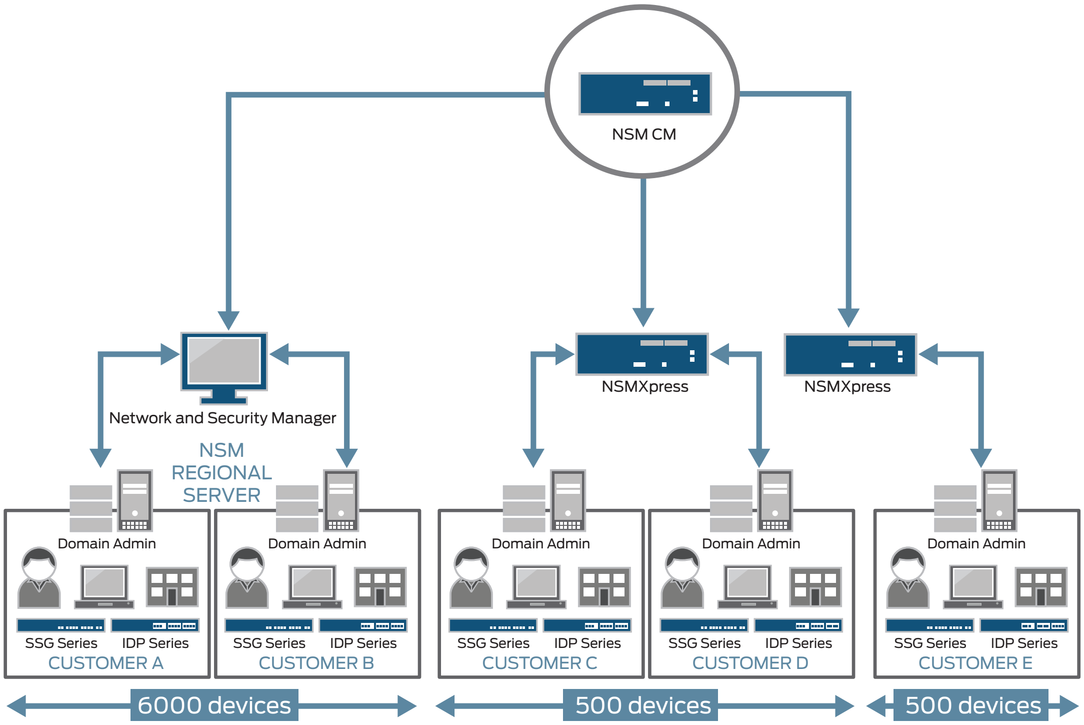


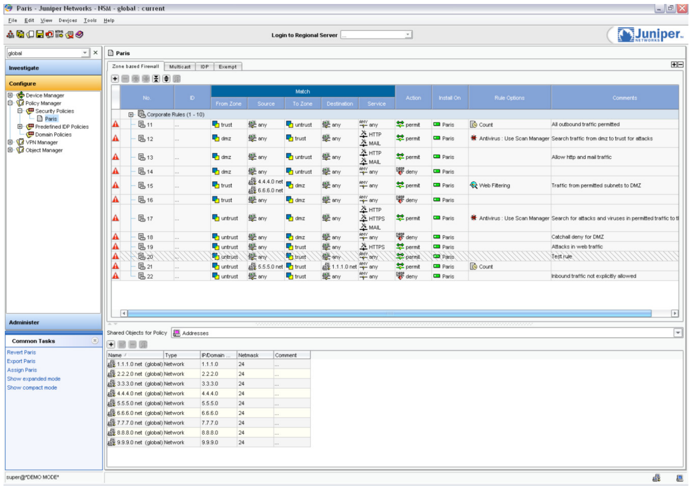
Figure 1: Network and Security Manager provides comprehensive device management with centralized security policy management, provisioning, logging and reporting

## Centralized Policy Management

NSM introduces a global policy feature that allows security administrators to create one master policy that can be applied to all regional management servers. This feature allows security administrators to enforce mandatory corporate policies across all devices in the network efficiently, and it ensures uniform security across the enterprise.

At the regional level, security administrators can create region- or device-specific policy rules. Overall, this hierarchical approach provides flexibility and scalability from a centralized location while leveraging commonalities across the infrastructure.

**Note:** For additional information, please refer to the NSM Central Manager and the Network and Security Manager Appliances (NSMXpress and NSM3000) datasheets.



| No. | ID | Match | | | | | Action | Install On | Rule Options | Comments |
|---|---|---|---|---|---|---|---|---|---|---|
| | | From Zone | Source | To Zone | Destination | Service | | | | |
| Corporate Rules (1 - 10) | | | | | | | | | | |
| 11 | ... | trust | any | untrust | any | any | permit | Paris | Count | All outbound traffic permitted |
| 12 | ... | dmz | any | trust | any | HTTP<br>MAIL | permit | Paris | Antivirus : Use Scan Manager | Search traffic from dmz to trust for attacks |
| 13 | ... | dmz | any | untrust | any | HTTP<br>MAIL | permit | Paris | | Allow http and mail traffic |
| 14 | ... | dmz | any | untrust | any | any | deny | Paris | | |
| 15 | ... | trust | 4.4.4.0 net<br>6.6.6.0 net | dmz | any | any | permit | Paris | Web Filtering | Traffic from permitted subnets to DMZ |
| 16 | ... | trust | any | dmz | any | any | deny | Paris | | |
| 17 | ... | untrust | any | dmz | any | HTTP<br>HTTPS<br>MAIL | permit | Paris | Antivirus : Use Scan Manager | Search for attacks and viruses in permitted traffic to t |
| 18 | ... | untrust | any | dmz | any | any | deny | Paris | | Catchall deny for DMZ |
| 19 | ... | untrust | any | trust | any | HTTPS | permit | Paris | | Attacks in web traffic |
| 20 | ... | untrust | any | trust | any | any | permit | Paris | | Test rule |
| 21 | ... | untrust | 5.5.5.0 net | trust | 1.1.1.0 net | any | permit | Paris | Count | |
| 22 | ... | untrust | any | trust | any | any | deny | Paris | | Inbound traffic not explicitly allowed |

| Name | Type | IP/Domain ... | Netmask | Comment |
|---|---|---|---|---|
| 1.1.1.0 net (global) | Network | 1.1.1.0 | 24 | ... |
| 2.2.2.0 net (global) | Network | 2.2.2.0 | 24 | ... |
| 3.3.3.0 net (global) | Network | 3.3.3.0 | 24 | ... |
| 4.4.4.0 net (global) | Network | 4.4.4.0 | 24 | ... |
| 5.5.5.0 net (global) | Network | 5.5.5.0 | 24 | ... |
| 6.6.6.0 net (global) | Network | 6.6.6.0 | 24 | ... |
| 7.7.7.0 net (global) | Network | 7.7.7.0 | 24 | ... |
| 8.8.8.0 net (global) | Network | 8.8.8.0 | 24 | ... |
| 9.9.9.0 net (global) | Network | 9.9.9.0 | 24 | ... |

## Template-Based Configuration

NSM provides a hierarchical, tree-based device configuration window. To streamline the design and deployment process in an IT environment, configuration templates are available that can be used to deploy either full or partial device configurations to one or several Juniper Networks switches. These templates can be newly created or they can use select parts of “golden configurations” that are vetted in a lab environment. IT administrators can also track which switches are associated with each configuration template.

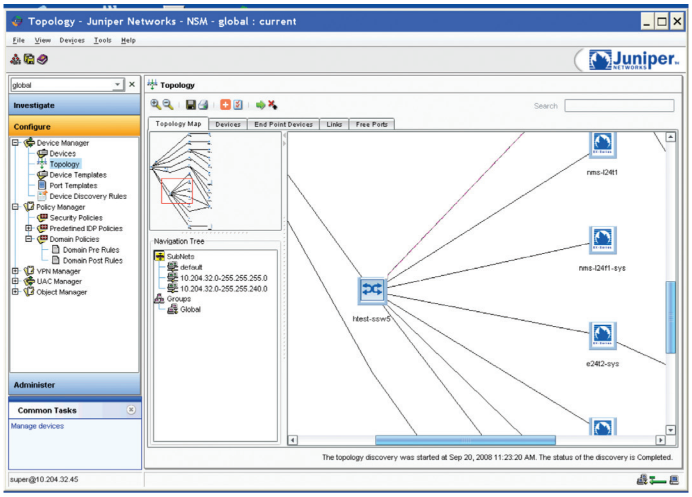
## Port Templates

NSM allows easy deployment of port-level configurations to Juniper Networks EX Series Ethernet Switches. The templates are based on best practice configurations for the most frequently used roles of Ethernet switch ports. They are well tested in a laboratory environment, thus saving valuable deployment time for network administrators. Network administrators can use one of the standard port templates (desktop, VoIP phone, access point, and so on) and apply them to one or more ports on multiple switches. Furthermore, network administrators can view a list of all ports that have a specific port template configured on them.

## Topology-Based Management

Network and Security Manager introduces a topology manager module that allows network administrators to visualize a layer 2 view of the network. The topology view allows hierarchical segmentation based on the sub network, and it shows the layer 2 connections between the sub networks and within each sub network.

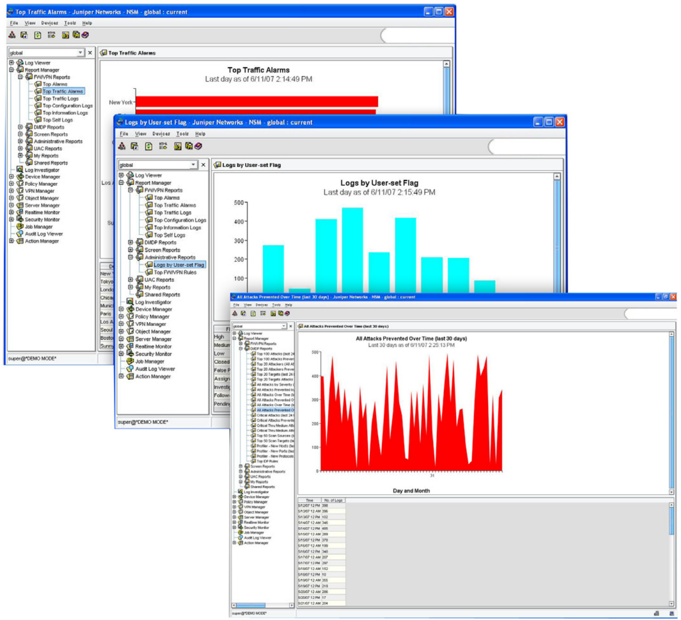
The topology view's zoom in and zoom out capability enables easy screen navigation for viewing the details on various devices in a network. Furthermore, the topology of devices is displayed in a tabular form for detailed information search of a specific device. Network administrators can print or save the tabular and graphical display of the network. They can also search for a device, in the topology view, based on system name, or IP address, or media access control (MAC) address. The topology view provides a tabular listing of not only the endpoints (hosts, etc.) connected to a switch, but also the switch ports that are free in the network.



The topology discovery was started at Sep 20, 2008 11:23:20 AM. The status of the discovery is Completed.

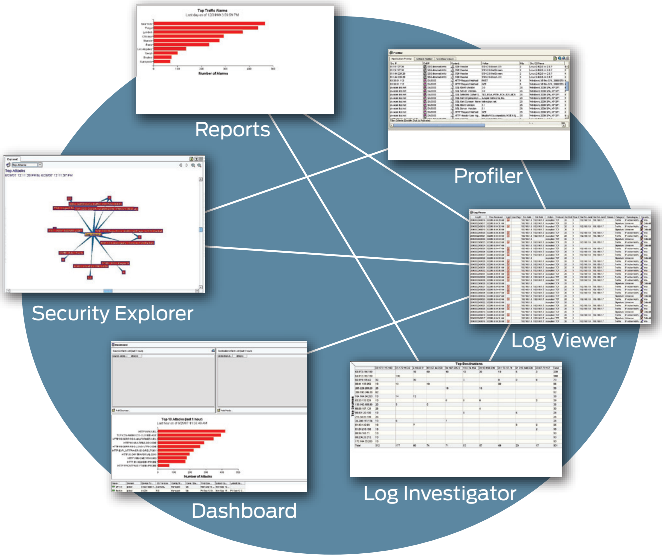
## Visibility and Reporting

Network and 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.


Top Traffic Alarms - Juniper Networks - NSM - global : current
Top Traffic Alarms
Last day as of 6/11/07 2:14:49 PM
Logs by User-set Flag - Juniper Networks - NSM - global : current
Logs by User-set Flag
Last day as of 6/11/07 2:15:49 PM
All Attacks Prevented Over Time (last 30 days) - Juniper Networks - NSM - global : current
All Attacks Prevented Over Time (last 30 days)
Last 30 days as of 6/11/07 2:25:13 PM
Day and Month
Log Viewer
Report Manager
Log Investigator
Device Manager
Policy Manager
VPN Manager
Object Manager
Server Manager
Realtime Monitor
Security Monitor
Job Manager
Audit Log Viewer
Action Manager
super@"DEMO MODE"

Logs that are stored within NSM can be analyzed in the following ways:

- **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** provides Top-N predefined reports, and it allows an administrator to generate, view, and export reports that summarize logs and alarms originating from the managed Juniper devices. Some examples of these include: Top Destinations for Juniper Networks Unified Access Control, Top Configuration Changes for EX Series Ethernet Switches, Top 20 Attackers for Juniper Networks SSG Series Secure Services Gateways, Top Authorization Failures for Juniper Networks SA Series SSL VPN Appliances, and Top 20 Attacks Prevented by IDP Series Devices. For more in-depth reporting, Juniper Networks STRM Series Security Threat Response Managers are the recommended solution.
- **Profiler Manager** (for IDP Series Sensors and Integrated Security Gateway Appliances) helps administrators view baseline network activity and quickly identifies new hosts and applications.
- Other tools include a dashboard and Log Investigator.



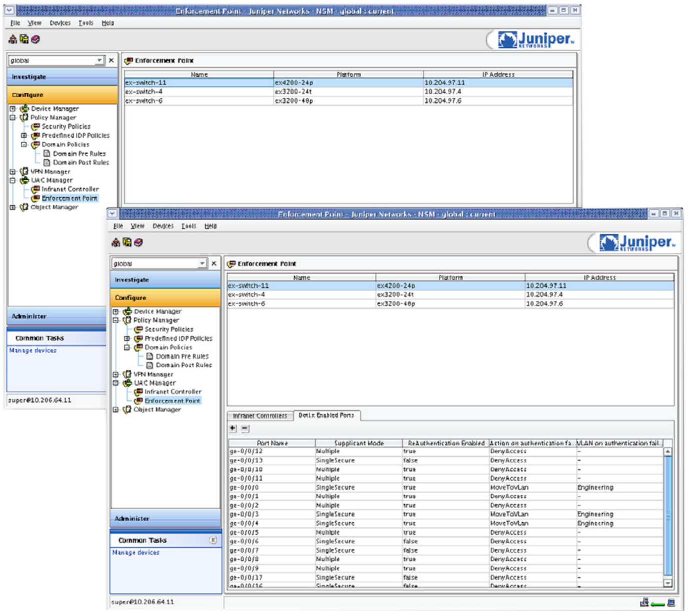
## Delegation of Administrative Rights

NSM allows enterprise IT departments to delegate appropriate levels of administrative access to specific users locally or via RADIUS for a wide range of tasks. Using role-based administration, enterprises can provide or restrict system permissions to different individuals or constituencies within the organization, based on skill set or responsibility.

Role-based administration can be accomplished using the predefined roles within NSM, or by creating a custom role from more than 100 assignable tasks within the system.

## Unified Access Control Management

NSM allows a centralized configuration of all Juniper Networks IC Series Unified Access Control Appliances and L2 enforcement points (EX Series switches) in the managed network. The UAC manager module enables network administrators to not only associate IC Series UAC Appliances and EX Series switches, but also to manage individual switch ports for 802.1X authentication.

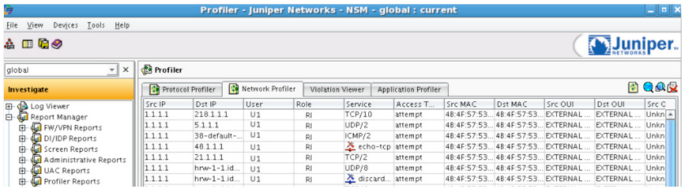


| Name | Platform | IP Address |
|---|---|---|
| ex-switch-11 | ex4200-24p | 10.204.97.11 |
| ex-switch-4 | ex3200-24t | 10.204.97.4 |
| ex-switch-6 | ex3200-48p | 10.204.97.6 |

| Port Name | Supplicant Mode | ReAuthentication Enabled | Action on authentication fa... | VLAN on authentication fail... |
|---|---|---|---|---|
| ge-0/0/12 | Multiple | true | DenyAccess | - |
| ge-0/0/13 | SingleSecure | false | DenyAccess | - |
| ge-0/0/10 | Multiple | true | DenyAccess | - |
| ge-0/0/11 | Multiple | true | DenyAccess | - |
| ge-0/0/0 | SingleSecure | true | MoveToVLan | Engineering |
| ge-0/0/1 | Multiple | true | DenyAccess | - |
| ge-0/0/2 | Multiple | true | DenyAccess | - |
| ge-0/0/3 | SingleSecure | true | MoveToVLan | Engineering |
| ge-0/0/4 | SingleSecure | true | MoveToVLan | Engineering |
| ge-0/0/5 | Multiple | true | DenyAccess | - |
| ge-0/0/6 | SingleSecure | false | DenyAccess | - |
| ge-0/0/7 | SingleSecure | false | DenyAccess | - |
| ge-0/0/8 | Multiple | true | DenyAccess | - |
| ge-0/0/9 | Multiple | true | DenyAccess | - |
| ge-0/0/17 | SingleSecure | false | DenyAccess | - |
| ge-0/0/16 | SingleSecure | false | DenyAccess | - |

## User-Specific Application Visibility

NSM provides a common interface that enables a network administrator to correlate which users are using what applications and display this data in Profiler Manager.



| Src IP | Dst IP | User | Role | Service | Access T... | Src MAC | Dst MAC | Src OUI | Dst OUI | Src C |
|---|---|---|---|---|---|---|---|---|---|---|
| 1.1.1.1 | 218.1.1.1 | U1 | RI | TCP/10 | attempt | 48:4F:57:53... | 48:4F:57:53... | EXTERNAL ... | EXTERNAL ... | Unkn |
| 1.1.1.1 | 5.1.1.1 | U1 | RI | UDP/2 | attempt | 48:4F:57:53... | 48:4F:57:53... | EXTERNAL ... | EXTERNAL ... | Unkn |
| 1.1.1.1 | 38-default-... | U1 | RI | ICMP/2 | attempt | 48:4F:57:53... | 48:4F:57:53... | EXTERNAL ... | EXTERNAL ... | Unkn |
| 1.1.1.1 | 48.1.1.1 | U1 | RI | echo-tcp | attempt | 48:4F:57:53... | 48:4F:57:53... | EXTERNAL ... | EXTERNAL ... | Unkn |
| 1.1.1.1 | 21.1.1.1 | U1 | RI | TCP/2 | attempt | 48:4F:57:53... | 48:4F:57:53... | EXTERNAL ... | EXTERNAL ... | Unkn |
| 1.1.1.1 | hrw-1-1.id... | U1 | RI | UDP/8 | attempt | 48:4F:57:53... | 48:4F:57:53... | EXTERNAL ... | EXTERNAL ... | Unkn |
| 1.1.1.1 | hrw-1-1.id... | U1 | RI | discard... | attempt | 48:4F:57:53... | 48:4F:57:53... | EXTERNAL ... | EXTERNAL ... | Unkn |

## Features and Benefits

### Network and Security Manager Features and Benefits

| APPLICATION | APPLICATION DESCRIPTION | BENEFIT |
|---|---|---|
| Device configuration management | Centralized interface to quickly and easily deploy one or more devices provides a similar, intuitive interface across all device types and versions, along with complete support for all device features. Device templates enable administrators to define and maintain commonly used configurations in one place. | Centralized configuration interface reduces overall configuration time for large or small network deployments. Templates enforce a common configuration per corporate policy and minimize configuration errors. |
| Policy management | Provides an intuitive, rule-based approach for all device families being managed, with a complete view of rule behaviors and options and powerful filtering capabilities. Allows network objects and services to be dragged and dropped directly into the policy rules from within the Policy or Object Manager window. | Centralized policy interface allows policy to be shared across one or more devices with built-in intelligence to update correct rule sets based on device type, allowing users to quickly and easily deploy policies across the entire network. |
| VPN management | An interface enables administrators to define topologies with just a few clicks. The system automatically creates the required VPN configuration, with an option to fine-tune a configuration if required. | Simple, accelerated VPN configuration and deployment. |
| Centralized object management | Shared Object manager allows central administration of network, service, Network Address Translation (NAT), attack, antivirus/deep inspection objects from one interface that can be used by one or more policies. | Reduces overall configuration time for large or small network deployments. |
| Real-time monitoring | Enables administrators to actively monitor the status of large numbers of firewall/VPN and IDP Series devices, clusters, and VPN tunnels. | Ability to view overall status from one centralized location. |

## Features and Benefits (continued)

| APPLICATION | APPLICATION DESCRIPTION | BENEFIT |
|---|---|---|
| Intelligent security updates | Juniper's security team adds coverage for new threats and selects recommended attack signatures. An automatic, scheduled process updates the NSM attack object database, and new attack object databases can be automatically pushed to security devices. | Coverage for the latest attacks without the need to spend time on threat analysis. Coverage for new protocols and contexts without service interruption. Time is saved through automation. |
| Version control | Global policy version control for NSM security policies. | Users can keep track of all changes made to their security policies with the ability to compare between versions and even roll back to previous working versions, if needed. |
| Topology view | Centralized interface to discover and visualize a layer 2 topology on an Ethernet switched network. Discovered topology is automatically organized into sub networks, and network administrators can view the topology of each sub network as well as view the topology between sub networks. The zoom in and zoom out capability allows network administrators to easily navigate through the various parts of the network. Network administrators can print/save the topology and search/locate capabilities based on various parameters. The topology view also lists the various end hosts connected to the switch. | Ease of use in visualizing the network and quickly zeroing in on devices in a topology using parameters. The powerful capability of visualizing layer 2 topology in a sub network on a single screen. |
| Log and report management | High-performance log storage mechanism allows collection and monitoring of 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. | Integrated log management and reporting provides visibility by quickly identifying areas of investigation, and improves control through direct access of policy management. |
| Software image management | Allows management of different versions of device software from a central location to perform software upgrades on one or more devices. | Reduces overall maintenance tasks for large or small networks. |
| User activity management | 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 complete. Audit logs provide a record of configuration changes, supporting central oversight of business policy compliance. | Allows multiple administrators to log in simultaneously and tracks every action taken, thus ensuring business continuity. |
| Disaster recovery and high availability | System provides several methods of disaster recovery:<br>• Local backup: Automatically backs up NSM database for up to past 7 days.<br>• High availability: High availability configuration of NSM servers provides automatic database synchronization between the primary and secondary servers with automatic failover to secondary. | Robust management system offers nonstop operation. |
| North Bound Interface (NBI) | XML in SOAP/HTTPS Open interface that allows key NSM functions like:<br>• List of managed devices<br>• Creation, deletion, modification of objects and policies<br>• Update and pushes | Allows users to access all key functions of NSM without using the UI. Customers can utilize and leverage their existing infrastructure and build tools that can be easily integrated with NSM's NBI. |
| Inventory management | NSM provides inventory management for all supported devices which include:<br>• Hardware/software<br>• Licensing<br>• Serial numbers<br>• Ports and network interface cards (NICs) | Allows users to track both hardware and software inventory across their Juniper network, giving IT and other decision makers insights into how their equipment is running. |
| Schema updates | Schema driven application that allows users to support updates and new devices quickly. | Near zero-day support for new device features without reloading or upgrading NSM. |
| Template promotion | Promote existing device configuration to a master template for quick, globally consistent distribution of configuration. | Allows users to import an existing configuration and promote a section or the entire configuration to a master template so that it can be shared among all similar devices. |

## Juniper Networks Services and Support

Juniper Networks is the leader in performance-enabling services and support, which are designed to accelerate, extend, and optimize your high-performance network. Our services allow you to bring revenue-generating capabilities online faster so you can realize bigger productivity gains and faster rollouts of new business models and ventures. At the same time, Juniper Networks ensures operational excellence by optimizing your network to maintain required levels of performance, reliability, and availability. For more details, please visit **www.juniper.net/us/en/products-services/**.

## Minimum System Requirements

### User Interface

Operating systems supported include Microsoft Windows 2000, Windows NT, Windows XP, Red Hat Enterprise Linux 3.0, Red Hat Enterprise Linux 4.0.

### Management Server

Operating systems supported include Solaris 10, Red Hat Enterprise Linux 3.0, Red Hat Enterprise Linux 4.0. and 5.0.

## Ordering Information

| MODEL NUMBER | DESCRIPTION |
|---|---|
| NS-SM-A-BSE | NSMXpress, 25 devices |
| NS-SM-A-HA | NSMXpress, High Availability |
| NS-SM-A-CM | Network and Security Manager, Central Manager |
| NS-SM-S-BSE | Network and Security Manager, 25 devices |
| NS-SM-ADD-50 | Network and Security Manager, additional 50 devices |
| NS-SM-ADD-100 | Network and Security Manager, additional 100 devices |
| NS-SM-ADD-500 | Network and Security Manager, additional 500 devices |
| NS-SM-ADD-1K | Network and Security Manager, additional 1000 devices |
| NS-SM-XL-A-BSE | NSM3000 , 25 devices |

## Juniper Networks Device and Software Support

- **EX Series Ethernet Switches:**
  EX3200 line, EX4200 line, EX8200 line
- **IC Series Unified Access Control  Appliances:**
  IC4000, IC4500, IC6000, IC6500
- **ISG Series Integrated Security Gateways:**
  ISG1000, ISG1000 w/IDP, ISG2000, ISG2000 w/IDP
- **IDP Series Intrusion Detection and Prevention Appliances:**
  IDP10, IDP50, IDP75, IDP100, IDP200, IDP250, IDP500, IDP600, IDP800, IDP1000, IDP1100, IDP8200
- **J Series Services Routers:**
  J2320, J2350, J4350, J6350
- **M Series Multiservice Edge Routers:**
  M7i, M10i, M40e, M120 and M320
- **MX Series 3DUniversal Edge Routers:**
  MX240, MX480 and MX960
- **SRX Series Services Gateways:**
  SRX100, SRX210, SRX240, SRX650, SRX3400, SRX3600, SRX5600 and SRX5800
- **NetScreen Series Security Systems:**
  NetScreen-Hardware Security Client (HSC), NetScreen-5GT, NetScreen-5GT ADSL, NetScreen-5XP, NetScreen-5XT, NetScreen-25, NetScreen-50, NetScreen-204, NetScreen-208, NetScreen-500, NetScreen-500 GPRS, NetScreen-5200, NetScreen-5400
- **SA Series SSL VPN Appliances:**
  SA2000, SA2500, SA4000, SA4000 FIPS, SA4500, SA4500 FIPS, SA6000, SA6000 FIPS, SA6500, SA6500 FIPS
- **SSG Series Secure Services Gateways:**
  SSG5, SSG20, SSG140, SSG320M, SSG350M, SSG520, SSG520M, SSG550, SSG550M
- **Junos® Operating System Support:**
  Junos OS version 9.0 and above; forward support for Junos OS 9.6 software through schema update
- **ScreenOS® Support:**
  ScreenOS version 5.0.0 and above
- **IDP Series Support:**
  IDP Series version 4.0 and above
- **IVE Support:**
  SA Series version 6.3 and above
- **IC Series Support:**
  IC Series version 2.2 and above

## About Juniper Networks

Juniper Networks, Inc. is the leader in high-performance networking. Juniper offers a high-performance network infrastructure that creates a responsive and trusted environment for accelerating the deployment of services and applications over a single network. This fuels high-performance businesses. Additional information can be found at **www.juniper.net**.

Corporate and Sales Headquarters
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

APAC Headquarters
Juniper Networks (Hong Kong)
26/F, Cityplaza One
1111 King's Road
Taikoo Shing, Hong Kong
Phone: 852.2332.3636
Fax: 852.2574.7803

EMEA Headquarters
Juniper Networks Ireland
Airside Business Park
Swords, County Dublin, Ireland
Phone: 35.31.8903.600
EMEA Sales: 00800.4586.4737
Fax: 35.31.8903.601

To purchase Juniper Networks solutions, please contact your Juniper Networks representative at 1-866-298-6428 or authorized reseller.

1100018-003-EN    Nov 2009

♻ Printed on recycled paper