NETWORK AND SECURITY MANAGER

Product Overview

Network and Security Manager provides unparalleled capability for device and security policy configuration, comprehensive monitoring, reporting tools, and tools for investigating potential security threats in your network.

Juniper Networks NSM Central Manager (NSM CM) appliance enables scalable large scale deployments and the ability to do global policy enforcement via a hierarchical distribution of NSMXpress and NSM Central Manager.

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 IDP Series Intrusion Detection and Prevention Appliances, 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 Network and Security Manager, device technicians, network administrators, and security administrators can work together to improve management efficiency and security, reduce overhead, and lower operating costs.

Architecture and Key Components

Network and Security Manager's architecture is comprised of a device server, a GUI server, and a 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.

Network and Security Manager with Central Manager (NSM CM) can manage up to 10 regional Network and Security Manager servers and solves scalability problems by allowing management for up to 6000 routers, 3000 switches, 6,000 firewall/VPN devices or 2,000 firewall/VPN devices with 100 Juniper Networks IDP Series appliances per regional server. NSMXpress (NSM appliance) manages up to 100 routers, 150 switches and 500 firewall/VPN devices. Together, these provide an overall solution to scale for large enterprise and service provider environments.
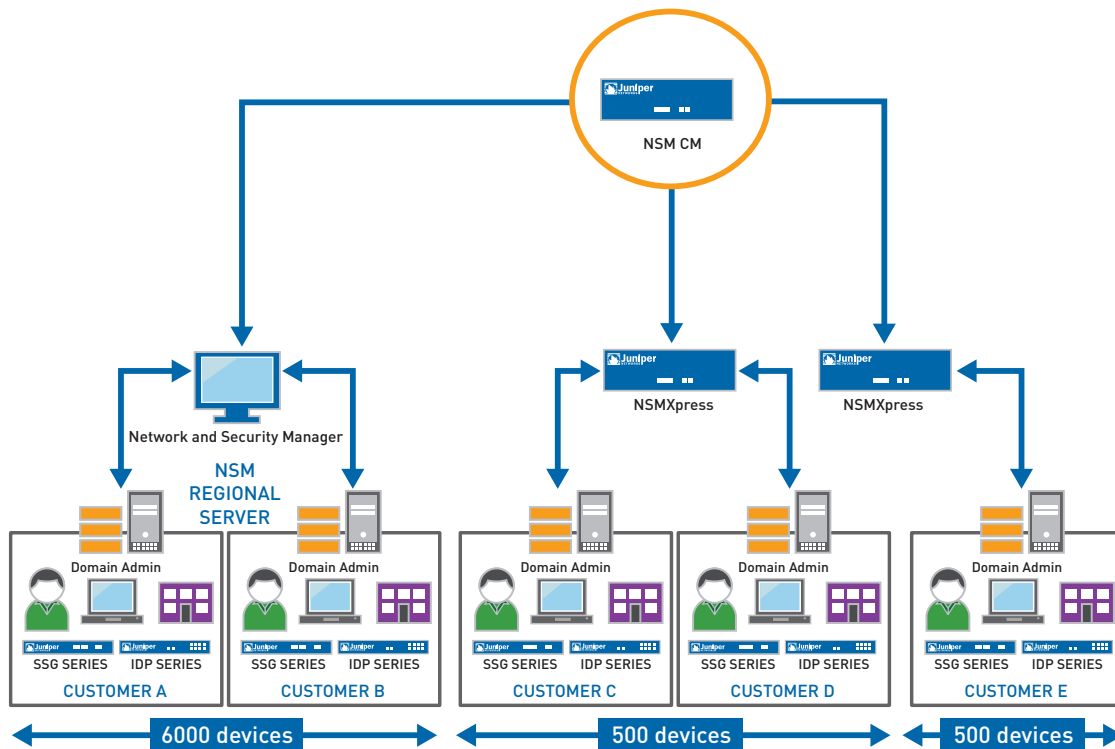
Figure 1: Network and Security Manager provides comprehensive device management with centralized security policy management, provisioning, logging and reporting

Centralized Policy Management

Network and Security Manager 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 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 infrastructure.

Note: For additional information refer to the NSM Central Manager and the NSMXpress datasheets.

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.
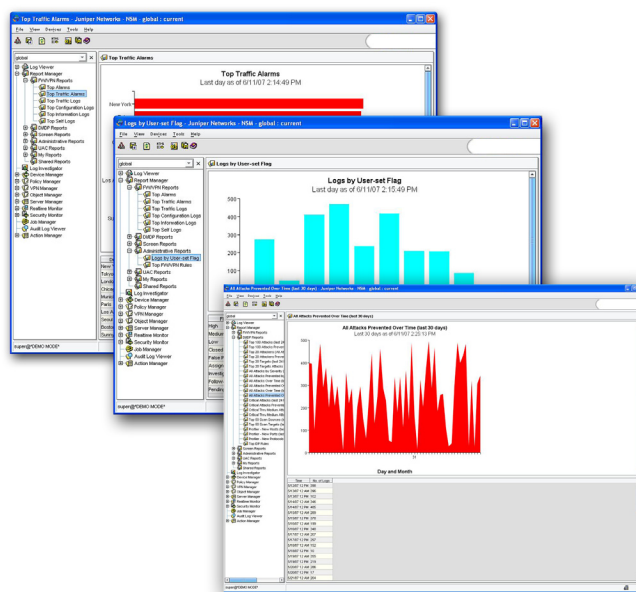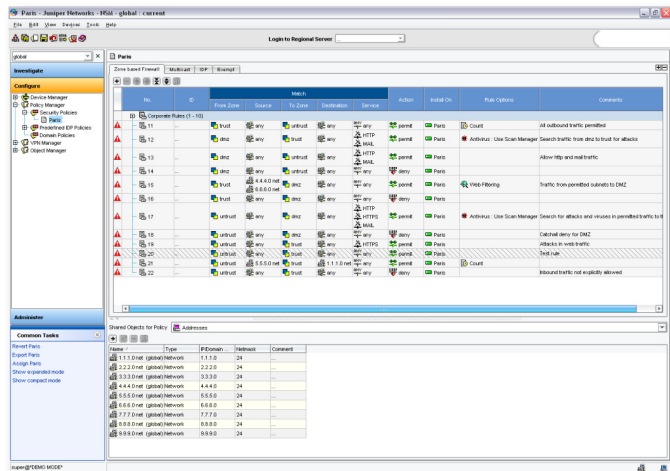
Logs that are stored within Network and Security Manager can be analyzed in the following ways:

- 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.
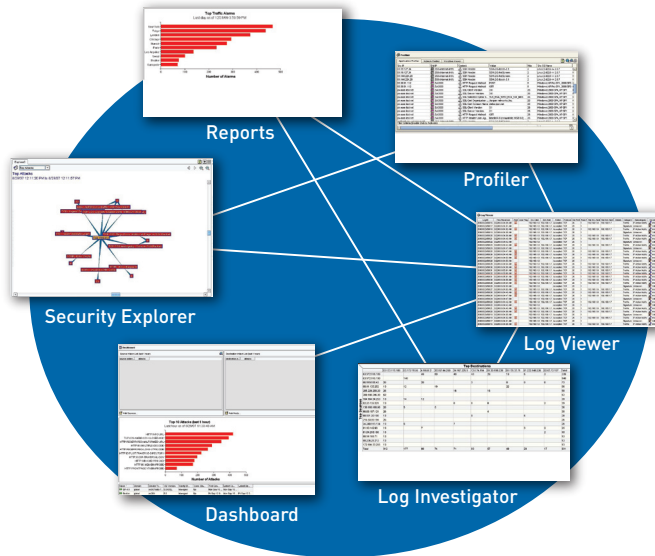
- Report Manager provides Top-N predefined reports and allows an administrator to generate, view, and export reports summarizing logs and alarms originating from the managed Juniper devices. For example: Top Destinations for UAC, Top Configuration changes for EX Series Ethernet Switches, Top 20 Attackers for SSG, Top Authorization Failures for SSL, and Top 20 Attacks Prevented for IDP Series. For more in-depth reporting, the Juniper Networks STRM Series Security Threat Response Managers is the recommended solution.
- Profiler Manager (for IDP Series Sensors and integrated security devices) 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

Network and Security Manager 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 Network and Security Manager or by creating a custom role from more than 100 assignable tasks within the system.

Features and Benefits

FEATURES	FEATURE DESCRIPTION	BENEFITS
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 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 configuration if required.	Simple, accelerated VPN configuration and deployment.
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.

FEATURES	FEATURE DESCRIPTION	BENEFITS
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.
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.
Real-time monitoring	Enables administrators to actively monitor the status of large numbers of firewall/VPN and IDP devices, clusters, and VPN tunnels.	Ability to view overall status from one centralized location.
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 login simultaneously and tracks every action taken thus ensuring business continuity.
Intelligent security updates	Juniper's security team adds coverage for new threats and selects recommended attack signatures. An automatic, scheduled process updates the Network and Security Manager attack object database and new attack object database 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.
Disaster recovery and high availability	System provides several methods of disaster recovery: • Local backup: Automatically backs up Network and Security Manager database for up to past 7 days. • High availability: High availability configuration of Network and Security Manager servers provides automatic database synchronization between the primary and secondary servers with automatic failover to secondary.	Robust management system offers nonstop operation.
Inventory management	NSM provides inventory management for all supported devices which includes: • Hardware/software • Licensing • Serial number • Ports and network interface cards (NICs)	Allows users to track both hardware and software inventory across their Juniper network and give IT and other decision makers an insight on how their equipment is running.
North Bound Interface (NBI)	XML in SOAP/HTTPS Open interface that allows key NSM functions like: • List of managed devices • Creation, deletion, modification of objects and policies • 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.
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.
Version control	Global policy version control for NSM security policies.	Users can keep track of all the changes made to their security policies with the ability to compare between versions and even roll back to previous working versions if needed.
Template promotion	Promote existing device configuration to a master template for quick global consistent distribution of configuration.	Allows users to import existing configuration and promote a section or the entire configuration to a master template so that it can share it among all similar devices.

Minimum System Requirements

User Interface

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

Performance-Enabling 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, faster rollouts of new business models and ventures, and greater market reach, while generating higher levels of customer satisfaction. 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/products-services.**

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

Juniper Networks Device & Software Support

- **Juniper Networks EX Series Ethernet Switches:**
  EX3200 line and EX4200 line
- **Juniper Networks IC Series Unified Access Control Appliances:**
  IC4000, IC4500, IC6000, IC6500
- **Juniper Networks ISG Series Integrated Security Gateways:**
  ISG1000, ISG1000 w/IDP, ISG2000, ISG2000 w/IDP
- **Juniper Networks IDP Series Intrusion Detection and Prevention Appliances:**
  IDP10, IDP50, IDP75, IDP100, IDP200, IDP250, IDP500, IDP600, IDP800, IDP1000, IDP1100, IDP8200
- **Juniper Networks J Series Services Routers:**
  J2320, J2350, J4350, J6350
- **Juniper Networks NetScreen Series Security Systems:**
  Juniper Networks 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
- **Juniper Networks SA Series SSL VPN Appliances:**
  SA2000, SA2500, SA4000, SA4000 FIPS, SA4500, SA4500 FIPS, SA6000, SA6000 FIPS, SA6500, SA6500 FIPS
- **Juniper Networks SSG Series Secure Services Gateways:**
  SSG5, SSG20, SSG140, SSG320M, SSG350M, SSG520, SSG520M, SSG550, SSG550M

Juniper Networks JUNOS® Software Support

- JUNOS software version 9.0 and above

Juniper Networks ScreenOS® Support

- ScreenOS version 5.0.0 and above

Juniper Networks IDP Series Support

- IDP Series version 4.0 and above

Juniper Networks IVE Support

- SA Series version 6.3 and above

Juniper Networks 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**.

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

Printed on recycled paper.

Engineered for the network ahead™