



## Product Overview

The need for a scalable and distributed security management solution grows more important every day. Security threats and vulnerabilities are increasing at an unprecedented rate. To reduce business risk, organizations must be able to deploy security policies easily and quickly across their entire networks. Juniper Networks Network and Security Manager Central Manager (NSM CM) combined with Juniper Networks NSMXpress allows administrators to create a hierarchical security posture that pushes mandatory security rules to localized regional servers. This allows organizations to scale and respond faster to security threats, ensuring compliance and business continuity. In addition, the NSM Central Manager appliance saves installation and deployment time by offering the Network and Security Manager preloaded onto a dedicated hardware platform.

## Product Description

NSM Central Manager (NSM CM) is an appliance version of Juniper Networks<sup>®</sup> Network and Security Manager (2007.2 or later). It simplifies the complexity of deploying global security policies and objects across all Network and Security Manager regional servers (running 2007.2 or later). This robust hardware management system installs in minutes with full high availability (HA) support, and makes it easy to maintain, scale and deploy.

## Architecture and Key Components

NSM Central Manager focuses on three key areas: global policy enforcement, ease of deployment, and scalability.

### Global Policy Enforcement

NSM Central Manager introduces global policy enforcement by allowing administrators to deploy mandatory corporate policies across their entire network. These global policies can be added prior to or after local customer rules without the ability to modify them. This hierarchical approach provides flexibility and scalability from a centralized location leveraging commonalities across the infrastructure.

### Enterprise

It is a challenge for large enterprises to create and deploy corporate policies throughout the organization. Employees are using new applications like Skype, Instant Messaging, and P2P, which can impact productivity and revenue. By deploying global policies, enterprises can enforce mandatory corporate policies through their network and ensure compliance. NSM Central Manager provides a unified interface that allows administrators to create mandatory policy rules that can be pushed down locally and globally. Enterprises typically have a separate networking and security group. NSM Central Manager does not override or replace existing policies; it just appends mandatory rules before and after existing rules. This ensures business continuity and autonomy within the organization. Administrators in local areas or departments like finance, marketing, and HR can still manage their day-to-day operations while ensuring compliance.

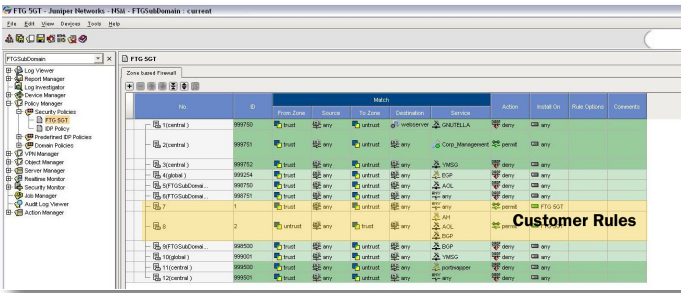


Figure 1: NSM Central Manager allows you to append Mandatory policies before and after Customer Rules

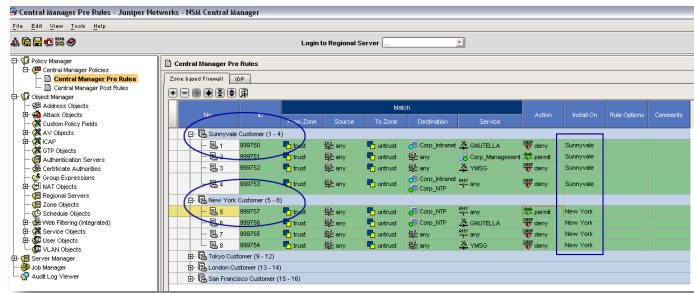


Figure 2: NSM Central Manager allows you to create and deploy customer specific policies from a single unified interface

**Service Providers**

Service providers and Managed Service Security Providers (MSSP) are looking for ways to offer new and better services to their customers. NSM Central Manager allows them to extend their services by deploying global services to all customers. For example, an MSSP with a combination of NSM Central Manager and NSMXpress can not only reduce total cost of ownership (TCO), but also lower configuration and installation costs. From a single centralized location, MSSPs can then push down services like firewall/VPN and IDP policies to their customer NSM Regional servers. These services can be preconfigured for each customer and pushed down to them when their server becomes reachable. For example, an MSSP can offer recommended IDP policies as a service and mandatory firewall/VPN rules virus protection (see Figure 2).

**Scalability**

NSM Central Manager gives administrators a consolidated view of all their managed Network and Security Manager regional servers. By simply clicking on the desired Network and Security Manager regional server, NSM Central Manager will automatically log administrators into that particular server. You can also scale to a large number of managed devices by stacking up NSMXpress and Network and Security Manager regional servers with one single management console. Each regional server can be configured to collect their own logs from their managed Juniper devices, thereby reducing the usage of resources like bandwidth (see Figure 3).

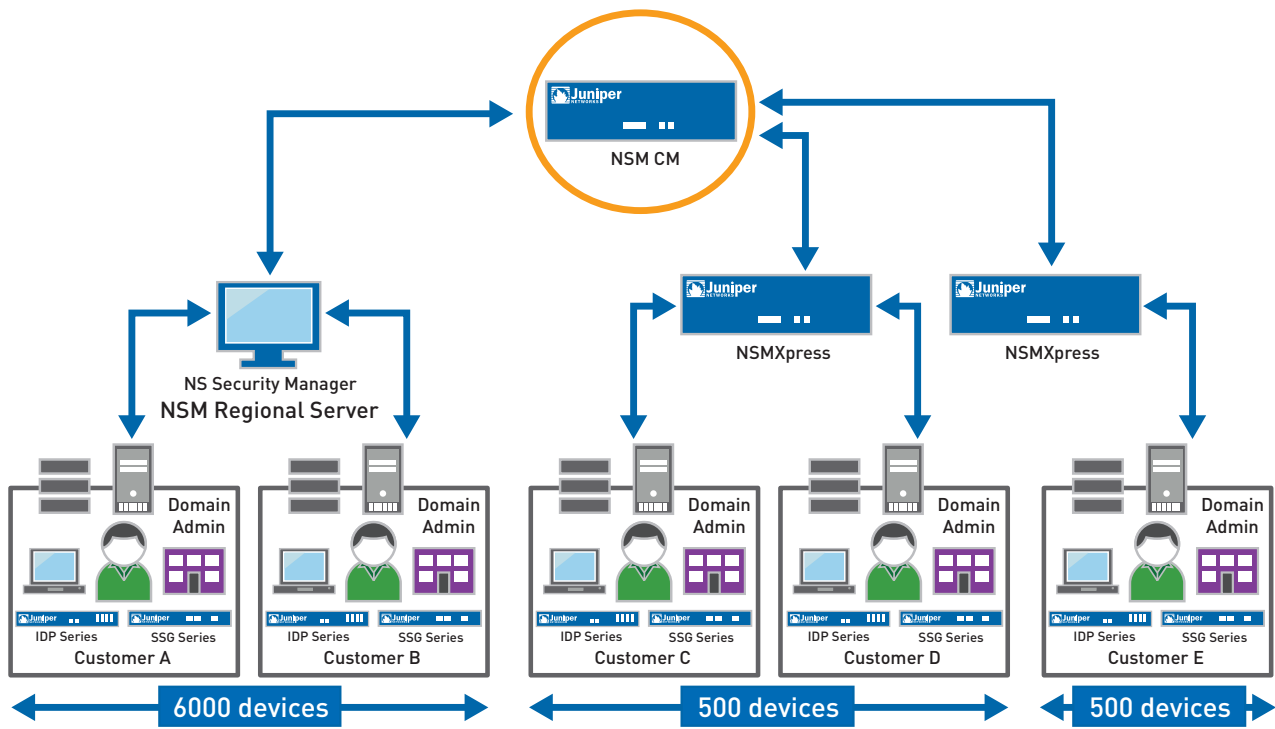


Figure 3: NSM Central Manager can scale to large number of devices by combining NSMXpress and NSM Regional Server support

## Features and Benefits

FEATURES	FEATURE DESCRIPTION	BENEFITS
Hardened OS	Juniper's security team monitors and maintains NSM Central Manager OS which is optimized for performance and security.	Users don't have to worry about security vulnerabilities, support, or patch management for the OS.
Web management	Intuitive Web UI for managing and maintaining NSM Central Manager.	Allows users to configure common NSM Central Manager parameters and tasks like network settings, scheduling updates, troubleshooting, utilities and backups via a Web interface.
Pre/post rules	Ability to create and deploy global policies that could be applied before or after customer rules across all Network and Security Manager regional servers. It supports all firewall/VPN and IDP rules.	Global administrators can push mandatory firewall/VPN and IDP policies across their entire network. It increases response time to threats and allows quick remediation.
Polymorphic objects and services	Ability to create global objects and services that can be pushed down to individual regional servers. These objects are empty container that can be populated and mapped to existing local objects.	Object management and consistency is maintained across the network. It makes it easy to deploy global objects to all your Network and Security Manager regional servers.
Single sign-on	Allows users to login to Network and Security Manager regional servers without entering credentials through a single NSM Central Manager client.	Users don't have to launch individual UI's and enter login information one by one. It saves times and allows a quick view into Network and Security Manager regional servers.
Self-sufficiency	NSM Central Manager will still function if Network and Security Manager regional servers are unavailable.	Enables business continuity by allowing users to configure all aspects of NSM Central Manager without depending on the regional servers.
Validation process	Real-time validation of configurations done through NSM Central Manager.	Users will be able to verify their configurations in real time and avoid errors as they happen.
Adaptability	NSM Central Manager can support both the hardware and software version of Network and Security Manager (2007.2 or later).	Existing users running software version of Network and Security Manager can also benefit from NSM Central Manager. It also allows them to scale by adding NSMExpress.
Easy and quick install	Wizard-driven quick setup of NSM Central Manager appliance.	In a couple of steps users can install and manage Network and Security Manager regional servers out-of-the-box.
Centralized updates	One place to get all the updates. NSM Central Manager can perform automatic downloads of latest OS and Network and Security Manager updates.	Users don't have to worry about maintaining server updates and patches.
One-stop support	Juniper Networks Technical Assistance Center (JTAC) supports all aspects of NSM Central Manager.	Users don't have to go to several vendors to get support.
Management of up to 10 regional servers	NSM Central Manager can manage up to 10 regional servers. It can be a combination of hardware or software version of Network and Security Manager.	Flexibility and adaptability. Users can easily deploy NSM Central Manager in their existing environment without changing hardware.
Single management client	The same Network and Security Manager client used with Network and Security Manager regional server (NSMExpress) can be used to log into NSM Central Manager.	Users don't have to download two different clients for NSM Central Manager and Network and Security Manager regional servers.
Dedicated HA support	NSM Central Manager comes with an option to get a dedicated HA box for full redundancy.	Users can easily deploy Network and Security Manager in full HA mode with hot standby configuration.



NSM CM

## Specifications

### Dimensions and Power

Dimensions (W x H x D)	16.7 x 3.5 x 16.2 in (42.42 x 8.89 x 41.15 cm)
Weight	28.5 lb (12.94 kg) typical (unboxed)
Rack mountable	Yes, 19"
A/C power supply	100-240 VAC, 50-60 Hz, 2.5 A 260 Watts
System battery	CR2032 3 V lithium coin cell
Efficiency	65% minimum, at full load
MTBF	78,000 Hours
Material	18 gauge (.048") cold-rolled steel
Fans	2 externally accessible, hot swappable ball-bearing fans

### Panel Display

Front panel power button	Yes
Power and temperature LEDs	Yes
Power supply failure LED	Yes
HDD activity	Yes

### Ports

Traffic	Two RJ-45 Ethernet-10/100/1000 full or half duplex (auto-negotiation)
Management	One RJ-45 Ethernet-10/100/1000 full or half-duplex (auto-negotiation)
Fast Ethernet	IEEE 802.3u compliant
Gigabit Ethernet	IEEE 802.3z or IEEE 802.3ab compliant
Console	One 9-pin serial console port

### Environment

Operating	50° to 95° F (10° C to 35° C)
Storage	-40° to 158° F (-40° C to 70° C)

### Environment (continued)

Relative humidity (operating)	8% to 90% non-condensing
Relative humidity (storage)	5% to 90% non-condensing
Altitude (operating)	-50 to 10,000 ft (3,000 m)
Altitude (storage)	-50 to 35,000 ft (10,600 m)

### Power Consumption

Thermal dissipation	416 BTU/hr (typical)
Thermal dissipation	470 BTU/hr (max single power supply)
Thermal dissipation	559 BTU/hr (max dual power supply)
Peak inrush current	50A Max. @ 115VAC, 80A Max. @ 230VAC

### Certifications

Safety certifications	EN60950-1:2001+ A11, UL60950-1:2003, CSA C22.2 No. 60950-1, IEC 60950-1:2001
Emissions certifications	FCC Class A, VCCI Class A, CE class A
Warranty	90 Days

## 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](http://www.juniper.net/products-services).

## Ordering Information

MODEL NUMBER	MODEL NAME AND DESCRIPTION
NS-SM-A-CM	NSM Central Manager

## 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](http://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

### 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  
Fax: 35.31.8903.601

Copyright 2009 Juniper Networks, Inc. All rights reserved. Juniper Networks, the Juniper Networks logo, JUNOS, NetScreen, and ScreenOS are registered trademarks of Juniper Networks, Inc. in the United States and other countries. "Engineered for the network ahead" and JUNOS are trademarks of Juniper Networks, Inc. All other trademarks, service marks, registered marks, or registered service marks are the property of their respective owners. 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.

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