

White Paper

# Centralized Security Management for Large Organizations

---



Juniper Networks, Inc.  
1194 North Mathilda Avenue  
Sunnyvale, California 94089  
USA  
408.745.2000  
1.888 JUNIPER  
[www.juniper.net](http://www.juniper.net)

**Table of Contents**

Introduction .....	3
The Security Management Challenge .....	4
The Device Lifecycle .....	4
Configuration Tasks .....	4
Administrative Rights .....	5
Complex Tasks.....	6
A Unified Approach to Security Management.....	6
Device Lifecycle Management .....	6
Multi-level Configuration Task Management.....	7
Use of Investigative Tools .....	8
Delegation of Administrative Rights.....	9
Simplified Management of Complex Tasks .....	10
Conclusion.....	10

## Introduction

As businesses increasingly turn to the Internet to extend their network resources, expand their revenue opportunities, enhance business relationships, and improve customer satisfaction, greater control through effective management of security threats becomes paramount. Striking the delicate balance between tight network security and consistently available network access is critical in enabling IT to contribute to the company's bottom line. Factors such as controlling access by internal and external users, ensuring the security of intellectual property and confidential data, and protecting customer privacy are key to ensuring that the enterprise meets its strategic business goals.

Effectively managing enterprise security and achieving this security-access balance requires all members of the IT organization to be working toward a common goal. While this may seem logical, it is anything but simple to execute, because members of the IT organization may have different objectives. Network and security teams often work at cross-purposes, resulting in less than desirable consequences. For example, in enabling network access, network administrators may inadvertently create security holes, thereby compromising the organization's overall security. Similarly, in creating security policies, security administrators may unknowingly block business critical traffic, impacting the flow of business operations and affecting customer or partner relationships – and the company's bottom-line.

IT organizations face the day-to-day challenges of managing complex network environments containing multiple types of security devices with different management systems. With each security device, there is a need to ensure network administrators have the right access to the appropriate systems and tools required for their specific job responsibilities, without enabling access to every management function on every device. To truly protect the network, it is imperative to deploy a management solution that offers tight integration of network application visibility and control, so that the context of information is preserved. This addresses the need to ensure that the right security measures are taken in a timely manner based on various security events as they occur. Unfortunately, most security management solutions today are disjointed and uncoordinated, exacerbating rather than alleviating these problems. A different approach to security management is required, one that will overcome these hurdles and allow network and security teams to work in unison, improving management efficiency, reducing overhead and operating costs, and enabling enterprises to more effectively leverage their technology assets to drive revenue and shareholder value.

## The Security Management Challenge

Let's take an in-depth look into the security management challenges faced by today's IT organizations. In a typical enterprise, the IT department must address each of the following four components of security management:

### The Device Lifecycle

Enterprises must manage network devices through their entire lifecycle, from initial deployment and configuration through maintenance and operating system/functionality upgrades. Depending on the size of the organization, multiple people in different sub-groups may be involved in this process. (see Figure 1)

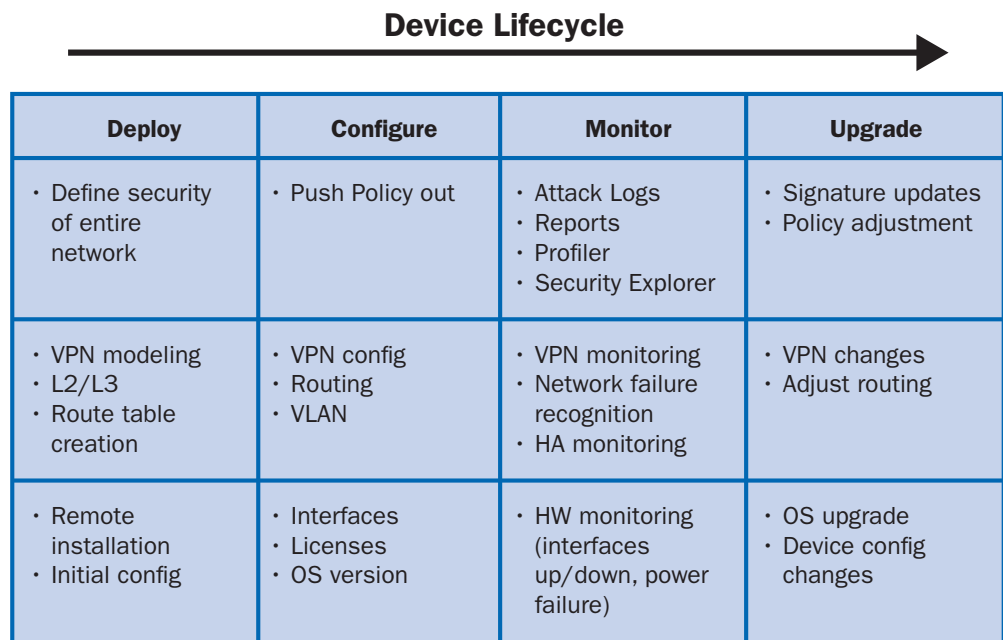


Figure 1: The complete device lifecycle includes four phases

### Configuration Tasks

As depicted in Figure 2, enterprises must not only manage the entire device lifecycle, they must also manage configuration tasks at the device, network, and security levels. Device technicians determine how a device fits into the enterprise environment, configuring and preparing it for initial deployment. Network administrators determine what traffic is allowed and where it is allowed to go by configuring the device to provide network access. Security administrators dictate what traffic is or is not allowed to traverse the network and the appropriate response when a violation occurs.

All three of these separate and distinct sets of tasks – device, network and security – must be managed effectively to ensure enterprise security. Conflicts or security risks may arise when the goals and objectives of each mandating group are not aligned or different tools are used to perform different management tasks.

	Deploy	Configure	Monitor	Upgrade
Security	<ul style="list-style-type: none"> <li>Define security of entire network</li> </ul>	<ul style="list-style-type: none"> <li>Push device-specific policy out</li> </ul>	<ul style="list-style-type: none"> <li>Attack Logs</li> <li>Reports</li> <li>Profiler</li> <li>Security Explorer</li> </ul>	<ul style="list-style-type: none"> <li>Signature updates</li> <li>Policy adjustment</li> </ul>
Network	<ul style="list-style-type: none"> <li>VPN modeling</li> <li>L2/L3</li> <li>Routing</li> </ul>	<ul style="list-style-type: none"> <li>VPN config</li> <li>Route tables</li> <li>Routing</li> <li>VLAN</li> </ul>	<ul style="list-style-type: none"> <li>VPN monitoring</li> <li>Network failure recognition</li> <li>HA monitoring</li> </ul>	<ul style="list-style-type: none"> <li>VPN changes</li> <li>Adjust routing</li> </ul>
Device	<ul style="list-style-type: none"> <li>Remote installation</li> <li>Initial config</li> </ul>	<ul style="list-style-type: none"> <li>Interfaces</li> <li>Licenses</li> <li>OS version</li> </ul>	<ul style="list-style-type: none"> <li>HW monitoring (interfaces up/down, power failure)</li> </ul>	<ul style="list-style-type: none"> <li>OS upgrade</li> <li>Device config changes</li> </ul>

Figure 2: Each device includes configuration tasks at device, network and security levels

### Administrative Rights

Enterprises have numerous individuals with differing technology, functional, and business expertise managing security (see Figure 3). These individuals may or may not understand the interdependencies between all aspects of configuration, yet they need access to the devices and the information contained within these devices to perform their jobs effectively. For example, executives may need status information for reporting and compliance issues but may not have the necessary rights, impacting their ability to perform their job responsibilities. Further complicating the device access issue is the fact that different employees may be using different systems to perform security management tasks in an uncoordinated manner, leading to potential breaches or security risks. By aligning security management with the IT organization’s structure, all groups can work in concert rather than at cross-purposes, enabling tighter security and compliance with corporate policies and government regulations, while utilizing corporate resources more efficiently.

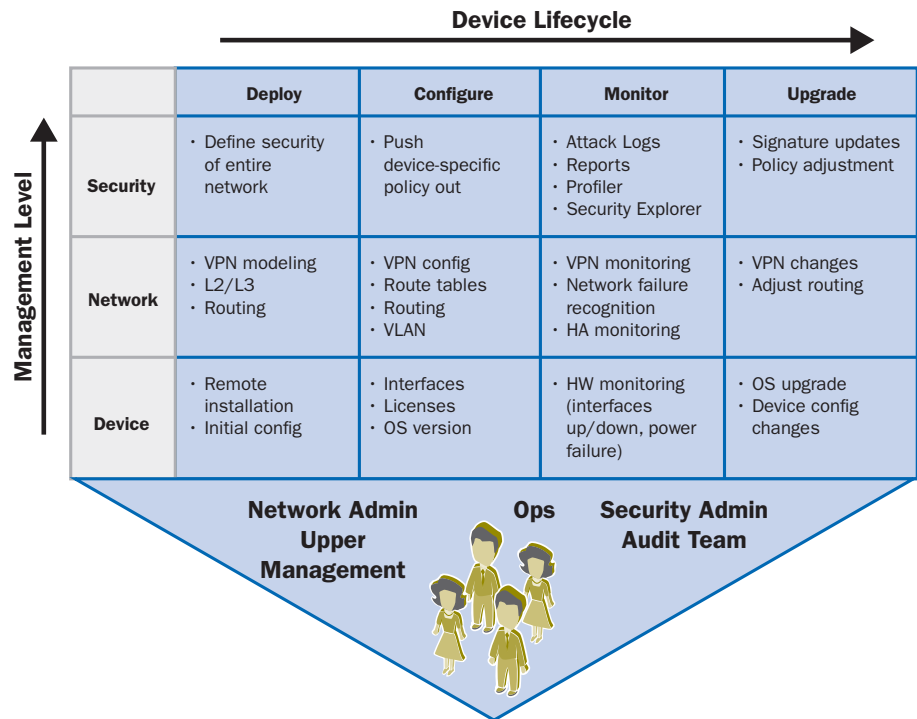


Figure 3: Each phase of the device lifecycle is the responsibility of a different group or individual within the IT organization

### **Complex Tasks**

Most IT administrators will admit that managing a network device can be exceedingly complex. Device, network and security aspects must be configured for deployment and monitored continuously, so they can be adjusted as needed. Today's management tools focus on one of two forms of access at opposite ends of the spectrum. Some provide granular access to the necessary configuration commands, while others focus on delivering a graphical user interface that only addresses high-level management of security. To effectively manage enterprise security, enterprises need a single tool that delivers the ability to easily manage the mundane tasks, such as group level access control, while simultaneously simplifying the complex tasks, such as full mesh VPN configurations.

It is the management of all four of these components – in a central, unified manner – that is required for effective management of enterprise security.

## **A Unified Approach to Security Management**

Juniper has taken a new approach to security management by addressing five key criteria in a single, centralized solution called Juniper Networks NetScreen-Security Manager. With NetScreen-Security Manager, organizations can:

- Centrally manage the device lifecycle of both firewall/IPSec VPN and Intrusion Prevention security devices
- Use a single, integrated management interface for granular control of configuration, network settings, and security policies
- Utilize a complete set of investigative tools that provide in-depth network visibility
- Give users access to the information required to fulfill their job responsibilities while controlling the administrative tasks they are allowed to execute
- Simplify the management of complex tasks with templates and other tools that incorporate all aspects of security.

The remainder of this paper will illustrate how Juniper Networks' NetScreen-Security Manager addresses these five criteria for effective, unified security management, and enables every member of an enterprise's IT organization to work together in a centralized and coordinated manner, to improve efficiency, reduce the administrative burden, and decrease operating costs associated with network security management.

### **Device Lifecycle Management**

NetScreen-Security Manager allows enterprises to control the entire device lifecycle from deployment and configuration to maintenance and upgrades. Beginning at the deployment phase, NetScreen-Security Manager allows initial configuration and assignment of interface characteristics via an intuitive graphical user interface. Once installed and configured, NetScreen-Security Manager allows administrators to establish network parameters and to monitor the organization's security policies using NetScreen-Security Manager's logging capabilities and other reporting tools. Security administrators can use NetScreen-Security Manager in the configuration phase to determine which devices to protect and how to protect them using the appropriate security policies. NetScreen-Security Manager also enhances the administrator's ability to troubleshoot and resolve problems during routine maintenance. Finally, NetScreen-Security Manager enables administrators to easily upgrade the devices with updates or new versions of operating software.

NetScreen-Security Manager's unified security management approach minimizes user error, reduces provisioning time, enhances team coordination, and allows enterprises to gain control of the entire security management process.

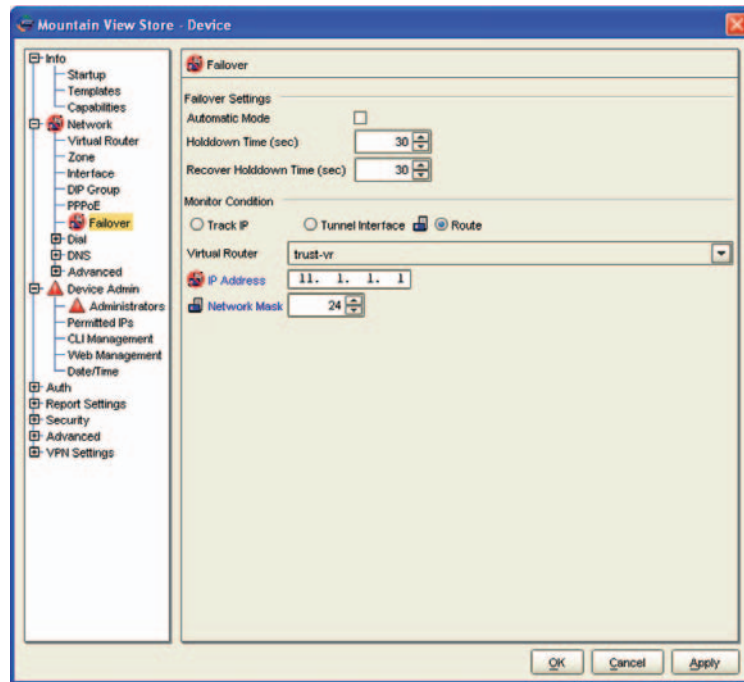


Figure 4: Device technicians use a similar, intuitive interface across all device types and versions; Device Templates minimize manual configurations by defining common settings

## Multi-level Configuration Task Management

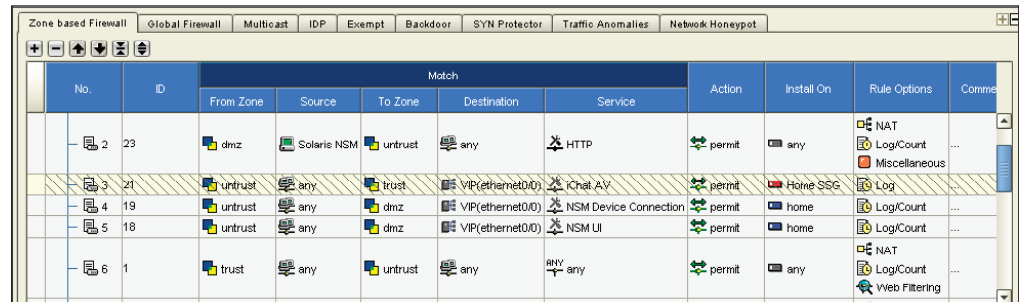
NetScreen-Security Manager uses a similar, intuitive management interface across all device types and provides complete support for all device features. Coupled with device templates that help minimize manual configurations by defining common settings, this unified interface minimizes the tension between operations, networking, and security groups. It enables every member of an enterprise's IT organization to configure all relevant settings using the same tool and update many devices at once, while providing an overall view of security – in real time.

NetScreen-Security Manager combines the flexibility of full-featured configuration management with the simplicity of rule-based management. Every task that can be performed in the command-line interface for a device is supported by NetScreen-Security Manager, allowing for the creation of general rules, as well as exceptions to rules where needed. With NetScreen-Security Manager, enterprises can, from a centralized location, configure, view, and manage all types of security policies, including:

- Zone-based Firewall
- Global Firewall
- Multicast
- IDP
- Backdoor
- SYN Protector
- Traffic Anomalies
- Network Honeypot

With NetScreen-Security Manager, security policy creation and management can also be managed using a single, intuitive interface (see Figure 5). Rules can be shared across many devices or, alternatively, administrators can create unique rules for each individual device in the network. For example, when setting up security zones across a widely distributed enterprise,

some devices may use the home/work zone feature of ScreenOS while others may not with all other rules being identical. With NetScreen-Security Manager, the individual policies can reflect these zone exceptions, minimizing individual device management.



No.	ID	Match					Action	Install On	Rule Options	Comments
		From Zone	Source	To Zone	Destination	Service				
2	23	dmz	Solaris NSM	untrust	any	HTTP	permit	any	NAT, Log/Count, Miscellaneous	
3	21	untrust	any	trust	VIP(ethernet0/0)	Chat AV	permit	Home SSG	Log	
4	19	untrust	any	dmz	VIP(ethernet0/0)	NSM Device Connection	permit	home	Log/Count	
5	18	untrust	any	dmz	VIP(ethernet0/0)	NSM UI	permit	home	Log/Count	
6	1	trust	any	untrust	any	any	permit	any	NAT, Log/Count, Web Filtering	

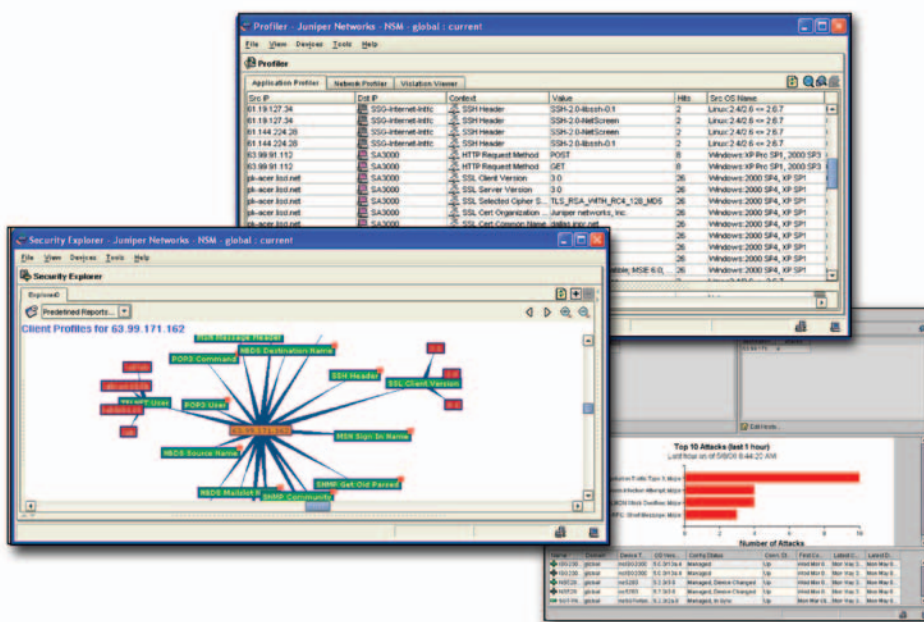
**Figure 5: NetScreen-Security Manager's Policy Management tool provides an intuitive, rule-based approach to setting policies across devices, powerful policy filtering capabilities and a complete view of rule behavior and options**

By giving organizations a single, real-time, system-level view by device type of both security policy and networking configurations, Juniper reduces user error and minimizes the discontinuity between security and networking administration. This improves management efficiency, enhances user productivity, and can significantly reduce overhead costs.

## Use 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 (see Figure 6). For integration into existing tools, logs can be forwarded to a third party reporting tool or database, and NetScreen-Security Manager provides a suite of tools that facilitate the analysis of stored logs:

- 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
- Log Investigator provides a quick way to statistically analyze security events and drill in on problem areas
- Dashboard shows a high-level overview of the status of the network including device status, top attacks, and attack statistics for key hosts



**Figure 6: NetScreen-Security Manager’s innovative, investigative tools, such as Profiler, Security Explorer and Dashboard, help pinpoint data that can be leveraged to fine tune security policies**

Having a complete and robust set of investigative tools provides broad visibility and the integration of security events and network traffic. It also provides multiple, interactive views for correlation and analysis enabling greater insight for more effective policy and overall security management. Links from the security events to the associated policies allow an administrator to tune security policy based information gathered during investigation.

### Delegation of Administrative Rights

Industry analyst firm META Group recommends that enterprises account for separation of duties in their policies, process definitions, and an organizational model for information security. Such alignment of security management with organizational structure enables all groups enterprise-wide to work in concert rather than at cross-purposes in the security management process.

NetScreen-Security Manager allows enterprise IT departments to delegate appropriate levels of role-based administrative access across different device types for a wide range of tasks, ranging from read-only to full-edit capabilities. In this way, Juniper provides users with access to the information required to fulfill their job responsibilities, while controlling the administrative tasks they are allowed to execute. Organizations can provide or restrict information to different individuals or constituencies, allowing users to make role-appropriate decisions. Similarly, by enabling or limiting system permissions based on skill set, organizations can support role-based administration where permissions and tasks correspond directly to an ideal team structure.

NetScreen-Security Manager includes a set of predefined templates for a wide range of roles within the enterprise. For example, templates for system administrators, domain administrators, and IDP administrators are available, and each template can be applied to an individual or a group of users. Role templates include read and write permissions as well as task-level authorization and can easily be modified and saved as a customized template to fit the needs of the organization. When a new administrator is added to the organization, specific permissions can be assigned by simply applying one or more of the predefined role templates.

NetScreen-Security Manager's domain functionality offers organizations a mechanism to logically separate devices, policies, reports, and objects. Domains can be set up to provide control at the business unit or geographical location level, allowing a balance of centralized and decentralized management.

With Juniper Networks management approach, organizations can empower each group or individual responsible for a specific phase of a device's 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 all device parameters 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 the software update.

To further simplify the management of complex tasks, NetScreen-Security Manager also includes a series of templates. These templates include pre-defined device configurations and security policies that automate repetitive tasks while minimizing both the time spent on configuration and the errors that may result from manual data entry. Device templates can be created and applied unilaterally, while other device-specific settings can be applied later to modify the configuration for specific requirements, such as geographical location. Multiple templates can be applied to each device. Templates and shared policies leverage commonalities to simplify the audit process.

By simplifying the management of complex tasks such as device and policy configurations and role assignment, NetScreen-Security Manager greatly improves the efficiency of the IT organization and can significantly reduce overhead and management costs.

## **Conclusion**

Juniper Networks' NetScreen-Security Manager provides IT departments with a comprehensive security management tool that centralizes the management of critical security components across multiple devices and device types. Using a single user interface that simplifies the management of complex tasks, NetScreen-Security Manager provides a unifying platform that aligns security management with the IT organization's structure so that all groups can work in concert as they control and administer configuration, network settings, and security policies. It gives users ready access to required information while controlling the administrative tasks they are allowed to execute. And it provides a complete set of investigative tools for in-depth network visibility and closed loop reporting. In short, NetScreen-Security Manager is a comprehensive and innovative approach to unified security management that can deliver significant business benefits to the enterprise by improving management efficiency, lowering operating costs, enhancing information security, and better aligning IT within the business.