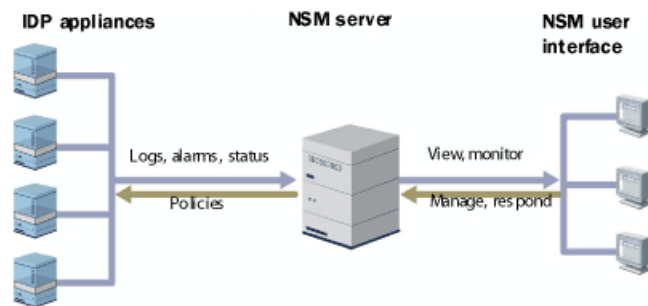


Centralized Management with NSM Overview

Juniper Networks Network and Security Manager (NSM) is a central management server capable of managing hundreds of IDP appliances and other Juniper Networks devices, such as ScreenOS firewalls, SA Series appliances, and IC Series appliances. You typically deploy NSM in a management subnet accessible to the NSM-managed devices.

Figure 1 illustrates the flow of information between the tiers of the central management solution: the NSM user interface, the NSM server, and IDP appliances.

Figure 1: IDP-NSM Communication



The IDP configuration, security policies, attack objects, and log records are stored in NSM server databases and administered using the NSM user interface. Communication between the NSM server and IDP appliances, and between the NSM server and the NSM user interface, is encrypted and authenticated.

For IDP deployments, centralized management provides the following benefits:

- Centralized management for IDP appliances and other network devices
- Consolidated logs from different devices in a single repository
- Centralized management of enterprise security policies
- Simplified management for attack signature updates
- Role-based administration

For information about installing NSM and using NSM distributed management features, management objects (such as address objects, service objects, and templates), and navigational and display features, see the NSM documentation.

Related Topics The following related topics are included in the *IDP Concepts and Examples Guide*:

- J-Security Center Updates Overview
- IDP Series Network Interfaces Overview

The following related topics are included in the *IDP Administration Guide*:

- NSM Device Configuration Management Task Summary
- IDP Logs and Reports in NSM Task Summary

Published: 2010-01-12