

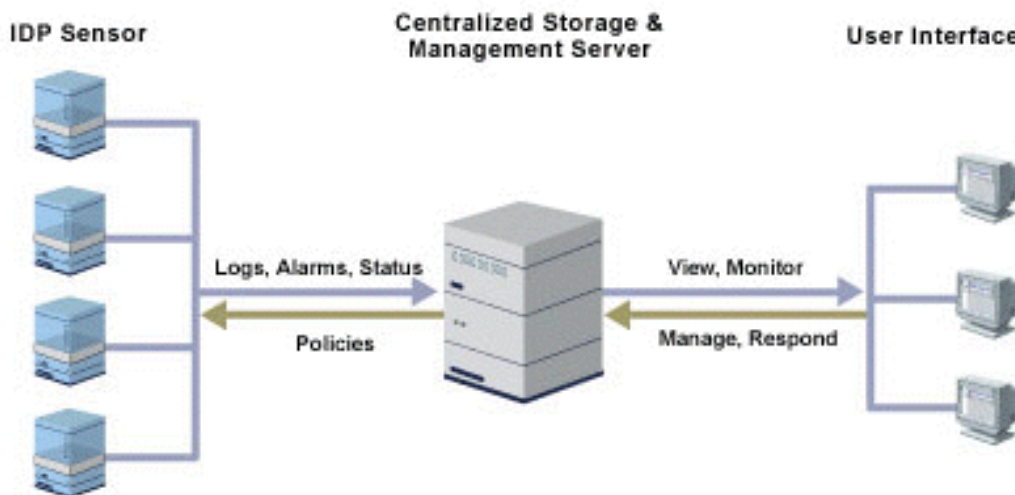
Architecture Overview

Juniper Networks IDP was designed from the ground up to deliver a solution that is flexible in its deployment and management. Administrators have complete control over the system, determining exactly how they want it deployed and to behave on the network. This is achieved via the architecture of Juniper Networks IDP, which makes it simple to install, configure and maintain. Juniper Networks IDP offers several distinguishing features, such as:

- 3-Tier management
- Rule-based policy management
- Numerous deployment options, including High Availability

Three-Tier Architecture

The Juniper Networks IDP system uses a three-tier architecture to logically separate the management functions associated with the system. This gives the IT team the flexibility to access the system from anywhere and accomplish remote management. The central management server stores all log and policy information in one database. Policies are loaded on individual sensors, but are also stored in the management server to facilitate central access. Logs from sensors are collected in the same database allowing administrators to quickly view and investigate threats from anywhere in the organization. If necessary, security policies can be edited and updated with a single action, further reducing management overhead.



Rule-Based Policy Management

Juniper Networks IDP gives administrators granular control over how the system behaves, without introducing complexity. To do this, Juniper Networks IDP uses a rule-based configuration mechanism, in which the individual rules that make up the security policy for the entire organization are created. This single security

policy is a logical and powerful configuration method that provides complete control over which traffic the Juniper Networks IDP examines and how it responds when intrusions are detected.

Another advantage of rulebases is that new updates of signatures can be installed on all required sensors by the rules defined in the rulebase. This reduces the tremendous burden associated with regular signature updates, since the system automatically knows which signatures should be distributed to which sensor, each and every time the policy is downloaded to the sensor.

Deployment Options

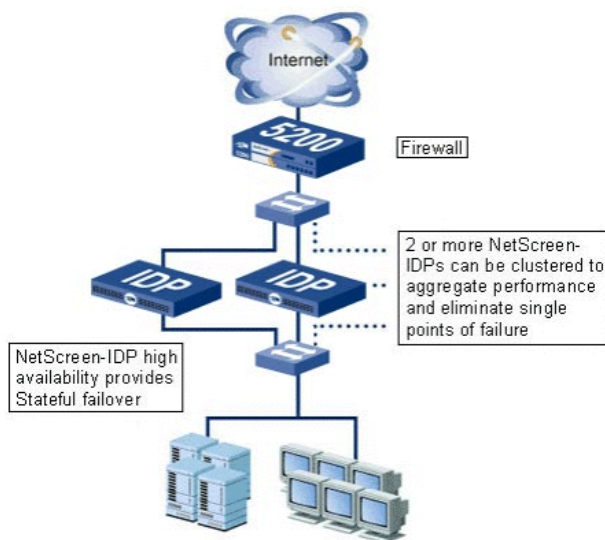
The Juniper Networks IDP system operates either as a non-intrusive sniffer or in an active gateway mode. The non-intrusive sniffer mode provides the ability to substitute a passive IDS system with Juniper Networks IDP and immediately reap the benefits of improved intrusion detection accuracy and simplified management. The active gateway mode allows administrators to protect their network from attacks, by dropping malicious packets to eliminate any potential impact.

Different deployment options give enterprises the flexibility to control how actively the network is being protected. The list below describes some sample configurations:

- Replace current IDS systems as a passive and non-intrusive sniffer, but with improved alarm accuracy, anti-evasion capabilities and simplified management
- Install in gateway mode, but only use the alarming capability to notify administrators of threats. This can improve evasion protection and allow users to build confidence in the system before dropping traffic
- Install in gateway mode and use the ability to drop traffic only sparingly, based on the level of the perceived threat
- Install in gateway mode with full packet-dropping capabilities
- Install in gateway mode in a high availability configuration, eliminating a single point of failure

Resiliency

For high traffic networks, multiple Juniper Networks IDPs can be run in parallel or as a cluster to increase performance capacity. Juniper Networks IDP clusters automatically divide the network load, without the need to deploy third party load balancers, to provide multi-gigabit performance to effectively protect the most trafficked network segments. Juniper Networks IDP clustering enables stateful, standalone high availability minimizing the risk of a single point of failure and maximizing network protection.



Copyright © 2005 Juniper Networks, Inc. All rights reserved. Juniper Networks, the Juniper Networks logo, NetScreen, NetScreen Technologies, the NetScreen logo, NetScreen-Global Pro, ScreenOS, and GigaScreen are registered trademarks of Juniper Networks, Inc. in the United States and other countries.

The following are trademarks of Juniper Networks, Inc.: ERX, ESP, E-series, Instant Virtual Extranet, Internet Processor, J2500, J4300, J6300, J-Protect, J-series, J-Web, JUNOS, JUNOScope, JUNOScript, JUNOSe, M5, M7i, M10, M10i, M20, M40, M40e, M160, M320, M-series, MMD, NetScreen-5GT, NetScreen-5XP, NetScreen-5XT, NetScreen-25, NetScreen-50, NetScreen-204, NetScreen-208, NetScreen-500, NetScreen-5200, NetScreen-5400, NetScreen-IDP 10, NetScreen-IDP 100, NetScreen-IDP 500, NetScreen-Remote Security Client, NetScreen-Remote VPN Client, NetScreen-SA 1000 Series, NetScreen-SA 3000 Series, NetScreen-SA 5000 Series, NetScreen-SA Central Manager, NetScreen Secure Access, NetScreen-SM 3000, NetScreen-Security Manager, NMC-RX, SDX, Stateful Signature, T320, T640, and T-series. All other trademarks, service marks, registered trademarks, or registered service marks are the property of their respective owners. All specifications are subject to change without notice.

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.