

Integrated Incident Management

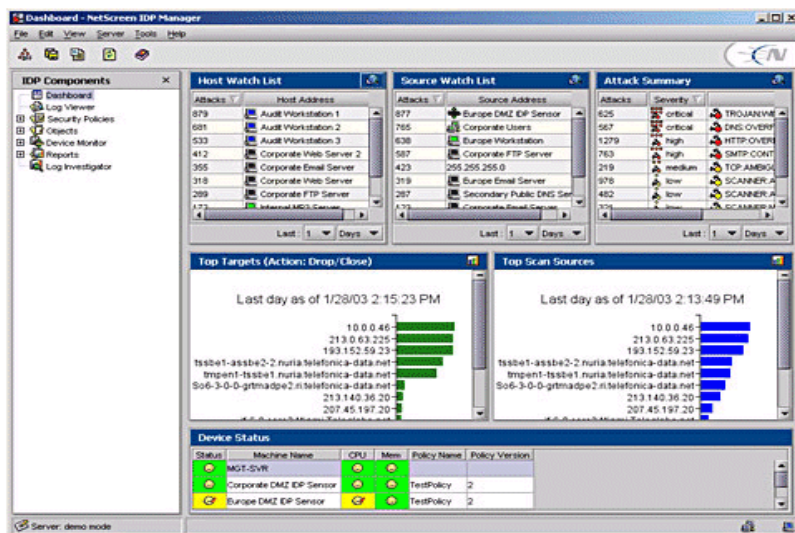
Juniper Networks IDP accelerates incident response with a closed loop investigative process that makes it easy to quickly see the big picture and then drill down to the appropriate level of detail to make informed security decisions. Through the Juniper Networks IDP management interface, an IT administrator can investigate security incidents by moving from top-level information, to attack specifics, to detailed forensic data, to the policy where any necessary adjustments can be made to ensure the network is protected. Juniper Networks IDP incident management mechanisms include:

- IDP Dashboard provides a quick, high-level view of all activity along with the ability to quickly drill down into a specific event.
- Enterprise Security Profiler provides detailed data on security policy violations and the ability to drill down into specific incidents to make incremental policy modifications.
- TruSecure IntelliShield Alert Manager integration provides immediate access to application vulnerability data to accelerate incident remediation.
- Log Investigator provides the ability to drill down into specific security incidents.

With Juniper Networks IDP, administrators will no longer need to manually sift through thousands, even millions of logs and try to correlate them to identify network incidents. Juniper Networks IDP does it automatically, organizing the information so that the IT team can systematically decrease the dataset to pinpoint the exact information needed, while increasing the ability to look at the data using multiple variables.

IDP Dashboard

The Juniper Networks IDP system aggregates all of the logs from the Sensors and correlates them to identify the key attack trends and top threats in the network. The Dashboard provides a complete top-level picture of which hosts are being targeted, by whom and what attacks they are using against the network. This summary information can be used to watch the top trends and then drill into anything that looks suspicious. The Dashboard allows an administrator to move from the summary information into more specifics, visually correlating the host, attack source and attack type to quickly identify what is at risk in the network.

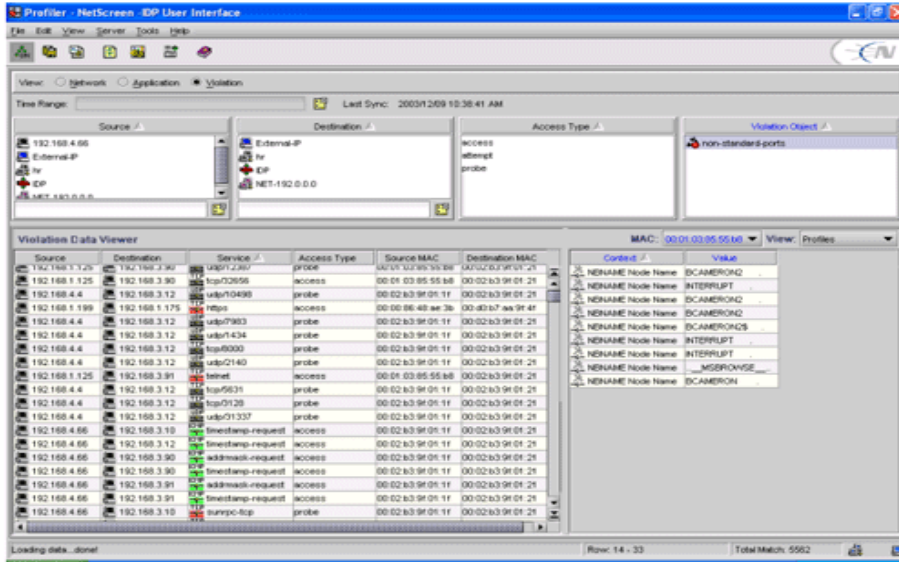


Enterprise Security Profiler

Enterprise Security Profiler not only provides the ability to help accelerate the deployment of inline prevention, it also facilitates the attack investigative process by providing additional network and application-level data on the attack source and target. Juniper Networks IDP's closed loop investigative process allows an IT team to view from many different levels, how an attack occurred, what systems were affected, and what applications were running on these systems, so that an informed security decision can be made to help improve network security.

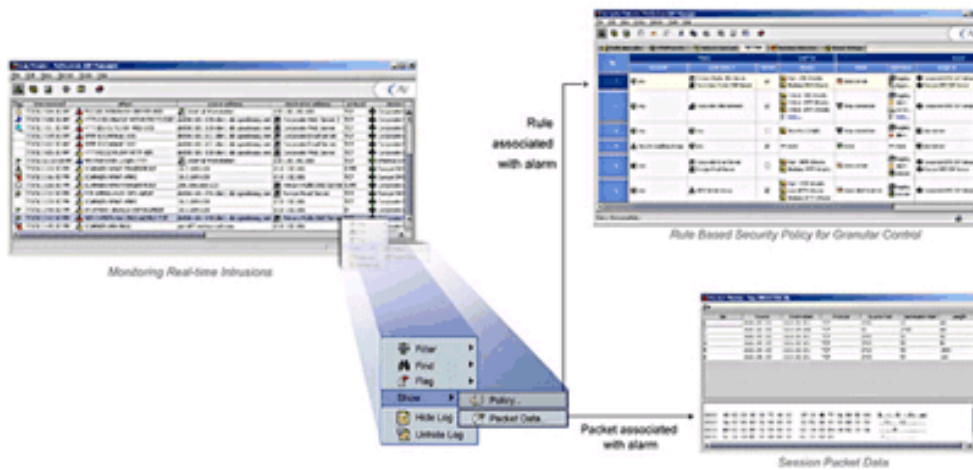
TruSecure IntelliShield Integration

To help accelerate the identification of vulnerabilities and attacks, the TruSecure IntelliShield Alert Manager has been integrated into the Juniper Networks IDP management console. TruSecure integration provides an administrator with immediate to relevant information on the vulnerability, patches available, and the affected operating systems and applications. In attack scenarios where minutes count, the integration of TruSecure IntelliShield data can mean the difference between a minor inconvenience and a full network outage.



Log Investigator

The Log Investigator provides the ability to drill into the three crucial pieces of information required to investigate any security incident: what traffic caused it, why it was triggered, and what to do about it. Juniper Networks IDP allows an administrator to navigate between the Log Viewer (which shows incidents), the Session Viewer (which shows associated packets), and the Policy Editor (which shows why the incident was triggered). Once the source of the attack is found, an administrator can jump directly to the rule that needs to be changed, make the necessary adjustments to the security policy and then quickly deploy it so that it cannot impact the network.



Juniper Networks IDP enables an IT team to set priorities and respond quickly, through its unique ability to drill into specific events to follow the course of the attack to simplify forensic investigations. Juniper Networks IDP also provides advanced incident tracking capabilities, including customizable annotation flags and user comment fields to ensure that everyone knows what is happening with each incident.

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.