

Management & Reporting

Juniper Networks IDP uses a centralized, rule-based approach to simplify deployment, configuration and maintenance of IDP devices, enabling administrators to define and update security policies, as well as investigate and respond to attacks. As a result, Juniper Networks IDP makes it easy to deploy inline attack prevention to protect the network against the latest threats and attack trends.

Key features within Juniper Networks IDP management that can help accelerate inline prevention and facilitate attack investigative analysis include:

- Enterprise Security Profiler to gain insight into network and attack activity that accelerates inline deployment and facilitates attack investigation.
- Policy Editor to create and deploy security policies.
- Log Viewer to investigate specific security incidents.
- Fully customizable reporting to generate up to the minute status on network activity.

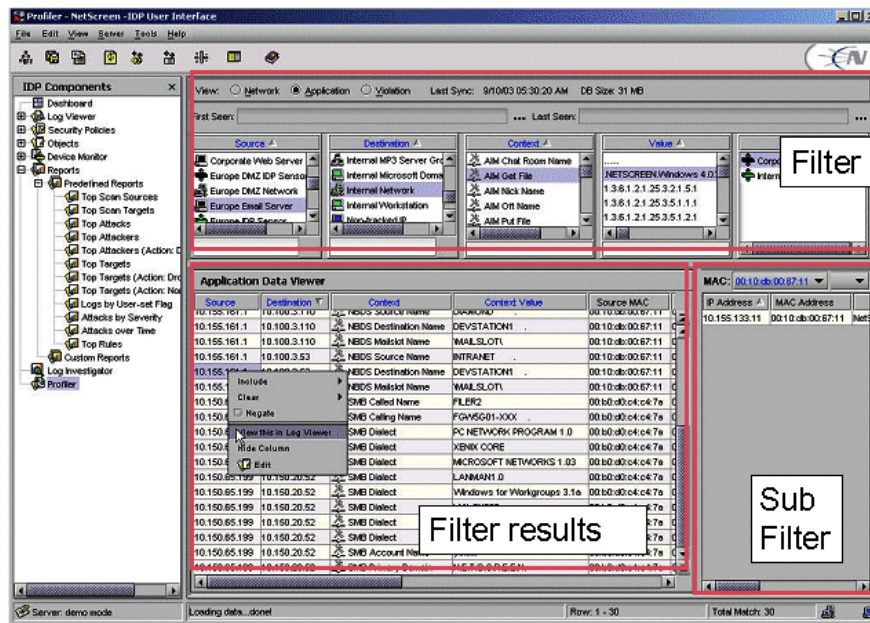
Enterprise Security Profiler

Enterprise Security Profiler (ESP) passively collects real-time network and application data to provide an on-demand view of the traffic that is actually traversing the network. Using built-in correlation tools within Juniper Networks IDP, administrators can translate that data into security policies that can accelerate the deployment of inline prevention. With the penetrating insight into network and application level activity that ESP provides, an IT team can quickly determine the root cause of the attack, regardless of where it was first detected. Once the root cause is detected, attack prevention and policy management tools can be used to immediately respond to the attack.

Network information collected by ESP includes items such as IP/MAC addresses (host connected to and from), and port number while application level info collected includes items such as: application used over network, version number, user name, and URL. With ESP, an administrator has the power to quickly answer questions such as:

- What Windows users have logged in from a specific IP address?
- What IP addresses have specific users logged in from? (Based on Windows User id, AIM Nick Name, MSN Nick Name, IRC Nick Name, etc.)
- What versions of SSH (clients & servers) have operated in the environment?

The combination of ESP and Juniper Networks IDP's inline attack prevention capabilities will ultimately help improve network security in a proactive manner. Any vulnerabilities or issues uncovered by ESP can be quickly translated into incremental changes to security policies resulting in tighter network security. Or if an attack has somehow gotten through, ESP can be used as a forensics tool to perform rapid attack investigative analysis using the intuitive GUI to drill down on an attack.



In this example, ESP provides a list of servers that have been targeted by network probes, a typical precursor to a Worm attack.

Policy Editor

The Juniper Networks IDP system is controlled using a rule-based security policy that provides granular control over what traffic to look at, what attacks to look for in that traffic and how to respond when an attack has been detected in that traffic. Juniper Networks IDP sensors are controlled using a single, logical Security Policy. Individual rules within the policy can be applied to one or more sensors, providing the ability to define an enterprise-wide Security Policy that can be distributed with the push of a button -- it's that easy. All relevant configuration and signature information is automatically sent to the Juniper Networks IDP Sensors. Updates are equally simple, since the system will automatically generate the appropriate configuration and signature. Juniper Networks IDP also keeps a copy of all of the

Security Policies that have been installed, so a history of revisions is always available.

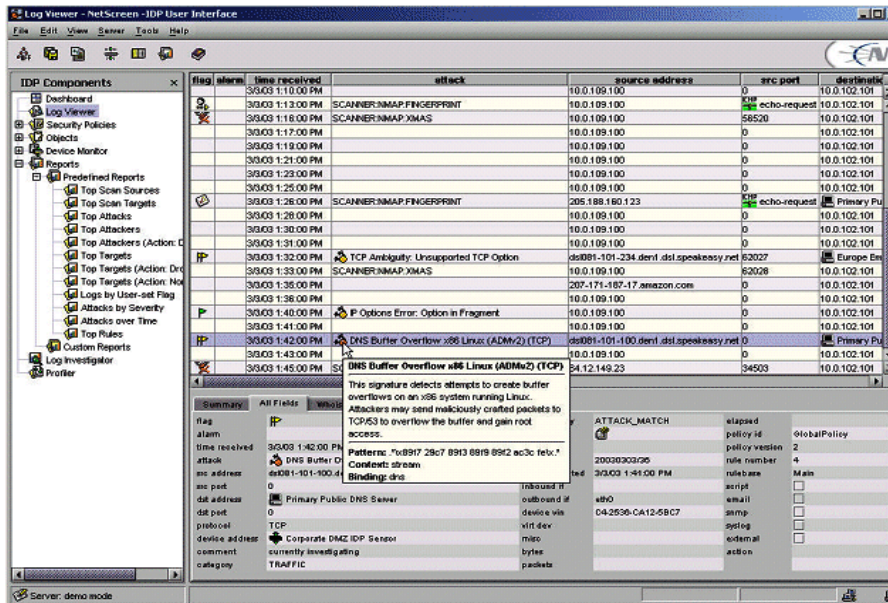
Log Viewer

The log viewer is designed to optimize administrative interaction with the system, providing the ability to customize the way information is processed within the system. Presentation of data within Juniper Networks IDP can be customized in the following ways:

- Display: Control of columns relative to display size and position to ensure it is easily understandable
- Column search: Search within specific columns or across all columns to find the information most pertinent to an investigation
- Filtered views: Apply filtering criteria against multiple columns and only display log records that match the criteria, reducing the data set to only that which is relevant at that moment
- Multiple views: Display multiple filtered views at the same time, all with the same context and real-time updates, so that it is easy to move from one to another to correlate information
- Saved views: Save log viewer settings into views to make it easy to retrieve certain sets of information during system interaction

The log viewer also contains contextual information that helps the security team prioritize which of the most serious threats they should focus on.

Attack details are linked to the logs so that an administrator can quickly drill into what triggered the attack and understand exactly what the attack did. Whenever an attack is detected, Juniper Networks IDP can do session packet captures, with a pre-trigger setting and a post-trigger setting defined in the rulebase. The pre-trigger setting determines how many packets preceding an attack to capture. This is useful in determining the activity immediately before an attack is detected. The post-trigger setting determines how many packets to capture after the attack has been detected.



Log Viewer provides detailed attack information, alarms that may have been triggered and the ability to quickly translate this data into a security policy modification.

Reporting

In addition to the feedback that ESP and Log Viewer provides, administrators can use several reporting mechanisms to generate management or compliance reports on current attack activity. Juniper Networks IDP includes three types of reporting:

- Pre-defined management level reports provide easily understood graphs that offer a complete picture of the network security and the actions taken to protect the network.
- Fully customizable reports provide up to the minute status on current network activity, both for incident management and for compliance reporting.
- Quick reports are context sensitive reports that can be generated directly from the log viewer, allowing rapid investigation of security incidents such as Day Zero attacks.