

Solution Brief

# Juniper Networks NetScreen-IDP's Enterprise Security Profiler (ESP)

---

*How ESP Compares to Traditional Technologies*

Sarah Sorensen  
Product Marketing Manager



Juniper Networks, Inc.  
1194 North Mathilda Avenue  
Sunnyvale, CA 94089 USA  
408 745 2000 or 888 JUNIPER  
[www.juniper.net](http://www.juniper.net)

Part Number: 351040-001

---

## Contents

Introduction.....	3
Vulnerability Scanners.....	3
Drawbacks:.....	3
How ESP Compares? .....	4
Statistical Anomaly Detection,.....	5
Drawbacks:.....	5
How ESP Compares? .....	5
Conclusion .....	6

## Introduction

Administrators rely on a hodgepodge of technologies to try to help them identify potential threats and stem any impact they may have to the network's security. Mitigation is often achieved through the policies of the security solutions deployed on the network. These policies dictate what traffic does and does not pose a threat to the organization, by defining a series of characteristics that, when matched, represent traffic that should be "allowed" or "denied."

While security policies are an intuitive and powerful approach to management, they imply a level of understanding about what is going on in the network and what the threats are to the network. An administrator must know that they are vulnerable to something before they can create a security policy to protect against it. Some organizations try to address the potential vulnerabilities associated with what is "unknown" by setting a firewall policy to accept only the traffic expected to and from known hosts and servers. The problem is an administrator must still somehow keep track of all of the known entities on the network.

Most organizations will employ a variety of technologies to try to stay current on the network's activities, so they can more effectively refine their policies and efficiently address specific security concerns. These technologies may include a concert of vulnerability assessment tools (scanners) and intrusion detection and/or intrusion prevention solutions with statistical anomaly or network behavior anomaly detection (NBAD) capabilities. The following is a quick analysis of some these traditional technologies and how Juniper Networks NetScreen-IDP's ESP compares.

## Vulnerability Scanners

Vulnerability scanners proactively scan systems and services on the network to identify vulnerabilities at that point in time. They remotely probe to identify which servers are connected to the network and which services/applications, including versions and patch numbers, they are running to create a picture of the available servers and open services that an attacker could access and exploit. This information can then be used to verify that current policies are adequately protecting the resources on the network and facilitate quick adjustments to reflect any changes to the network environment.

### Drawbacks:

1. Represents a single moment in time: Focuses only on what is available at that particular time, missing ongoing changes and limiting its ability to identify something new as soon as it happens.
2. Doesn't track usage: There is no context on what is actually being used in the network to help administrator understand the risk of a vulnerability to the organization. Without this context, it is hard to know how to prioritize or assess the most immediate threats to the organization.

3. Only identifies server applications: They make the assumption that all vulnerabilities are on servers and server applications, not the clients. This is a risky assumption to make because attacks target clients too, e.g. someone might be running a vulnerable version of IE or using an old SSH client. These can be attacked if the user accidentally makes connections to malicious servers.
4. Can be intrusive: Depending upon the vulnerability for which the system is scanning, it is possible that the active scan can bring down the destination system or application that the administrator is trying to protect.

### How ESP Compares?

ESP works all the time, as opposed to running at discrete times. It monitors network activity and collects the information on all the servers, server applications and clients it sees. This information is then available to administrators through its on-demand searchable database. When something new dynamically appears on the network, a security administrator will be able to use ESP to identify it and then modify security policies to protect these new systems. Another advantage is that ESP works passively, so ESP does not increase the risk of crashing a server.

The only major advantage scanners have over ESP is they can detect applications that have been loaded on a server, but have not communicated over the network, which is not a common case. While scanners may provide patch level information that ESP doesn't collect, this level of information is often too much for security administrators to process. What they really want to know is if they are at risk when a vulnerability is announced, which requires only the knowledge of the software version that ESP supplies.

	ESP	Vulnerability Scanners
<b>How</b>	Passive	Active
<b>When</b>	All the Time	Discrete Events
<b>Systems</b>	Clients & Servers	Servers available when scanning is employed
<b>Impact on network</b>	Minimal	Very High
<b>Manpower Resources required</b>	Low	High
<b>Network security posture</b>	Strong	Strong only when scanned

## Statistical Anomaly Detection,

Statistical anomaly detection, sometimes called **network behavior anomaly detection (NBAD)**, is used by intrusion detection and/or prevention solutions to alert administrators to anomalous behavior that could represent a threat to the network. These solutions apply “statistical usage profiling” to try to identify changes to the network by comparing the baseline (long term usage) to a current point in time (short term usage). To detect anomalous behavior, the system compares the short-term usage to the long-term profile and reports deviations that are considered “statistically significant” as potential attacks. The system further blends the short-term observed usage into the long-term usage profile to realize adaptation.

### Drawbacks:

1. Translating data into action: The main problem with statistical anomaly or NBAD solutions is that it is hard to interpret the attack reporting and translate it into an action. For example, what does an administrator do with an alert simply reporting on a spike in e-mail activity?
2. False positives: These solutions tend to generate a lot of false alarms, which adds to the management burden. An alert on a spike in e-mail usage could represent malicious virus activity or a harmless e-mail campaign launched by the marketing department. The burden is on the administrator to investigate, in a reactive manner, exactly what is going on, analyze the activity and, if it is an attack, potentially refine the security policy to respond.
3. Dynamic nature of network traffic: Network traffic in large organizations is constantly changing, making it virtually impossible to establish a baseline. And without a baseline, the data there is no basis for a valid comparison. Plus, attacks can be contained within the baseline and an organization would never know; ironically, if an attack contained within the baseline ends, the system may actually alert on the drop/change in traffic as an attack.
4. Attackers circumvent the solution: Attackers can create attacks that appear as normal traffic to the system so that the solution would never alert on it.

### How ESP Compares?

ESP provides specific information about the network that is actionable. It doesn't present a “mean variance” to represent anomalous behavior. With ESP administrators have immediate access to specific data on changes to the network. They don't have to try to extrapolate from trending or statistical data what these interactions mean to their security stance or wade through each and every log to look for a specific data point, which can consume significant resources, considering the number of logs generated on any given day in a busy network could potentially escalate into the hundreds or thousands.

	<b>ESP</b>	<b>NBAD</b>
<b>How</b>	Searchable database on layer 3, 4 and 7 data that is active on the network	Alerts on activity that is "Statistically Significant"
<b>False Alarms</b>	N/A	High
<b>Manpower Resources required</b>	Low	High
<b>Network security posture</b>	Strong	Strong only when information correctly interpreted

## Conclusion

While vulnerability scanners and statistical anomaly detection can provide some information that could potentially offer insight into the dynamics of the network, these technologies place the burden on the administrator to manually correlate and then investigate the significance of the vulnerability or "deviation." What administrators really want is an actionable posture assessment at the enterprise-level, so they can ensure the most appropriate security measures are in place. Administrators need something that can detect when something new is on the network and alert them to the change, so they can quickly assess whether any adjustments need to be made to their policies to keep their security stance in force. This is what Juniper Networks NetScreen-IDP's Enterprise Security Profiler delivers.

---

Copyright © 2004 Juniper Networks, Inc. All rights reserved.

Juniper Networks, the Juniper Networks logo, NetScreen, NetScreen Technologies, GigaScreen, and the NetScreen logo are registered trademarks of Juniper Networks, Inc. NetScreen-5GT, NetScreen-5XP, NetScreen-5XT, NetScreen-25, NetScreen-50, NetScreen-100, NetScreen-204, NetScreen-208, NetScreen-500, NetScreen-5200, NetScreen-5400, NetScreen-Global PRO, NetScreen-Global PRO Express, NetScreen-Remote Security Client, NetScreen-Remote VPN Client, NetScreen-IDP 10, NetScreen-IDP 100, NetScreen-IDP 500, GigaScreen ASIC, GigaScreen-II ASIC, and NetScreen ScreenOS are trademarks of Juniper Networks, Inc. All other trademarks and registered trademarks are the property of their respective companies.

Information in this document is subject to change without notice.

No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without receiving written permission from:

Juniper Networks, Inc.  
1194 N. Mathilda Ave. Sunnyvale, CA 95014 ATTN: General Counsel