

**Solution Brief**

# **IDP and SIM systems**

---

## **Interoperability with Third Party Security Information Managers**

Nick Jeremica  
Sr. CSE – Emerging Technologies - Security



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

## Introduction

As networks continue to increase in complexity there has been a growing need for centralization of security device log data from dissimilar network security devices. In recent years there have been a number of products brought to market that address this need. As organizations deploy Security Information Management systems (SIMS) they require assurances their investments in networking and security products will be compatible with their SIMS.

SIM products differ from traditional network management products in that they offer, in general, features to better make use of data from security devices. In many cases, this means sophisticated correlation of log data.

This document attempts to outline the mechanisms of interoperability with SIM products that Juniper Networks supports in the IDP family of products. Also, this document makes note of which SIM vendors have developed features to make integration with Juniper's products more successful.

## Interoperability Mechanisms

Today's SIM products accept logs via one or more of the following mechanisms;

- SYSLOG
- SNMP
- Proprietary agent

Juniper's IDP products have been designed with interoperability in mind. Both the stand alone IDP systems and the integrated platforms (ISG with Security Modules) support forwarding events in the form of either SNMP traps or SYSLOG. Through these mechanisms IDP can support integration with virtually any SIM product. To provide additional value, some vendors have developed additional features to enhance interoperability with Juniper IDP.

As of the writing of this document, no proprietary agents for SIM products had been tested with Juniper IDP.

## List of SIM vendors

The following table shows a list of vendors that offer SIM tools the IDP can interoperate with.

<i>Vendor</i>	<i>Accept SNMP</i>	<i>Accept SYSLOG</i>	<i>J-Partner Security Alliance member</i>	<i>Developed features/templates for Juniper IDP</i>
<i>ArcSight</i>	✓	✓	✓	
<i>E-Security</i>	✓	✓		
<i>Micromuse</i>	✓	✓	✓ <sup>1</sup>	
<i>Network Intelligence</i>	✓	✓	✓	✓
<i>netForensics</i>	✓	✓	✓	
<i>Cisco Mar<sup>2</sup>s (formerly Protego)</i>	✓	✓		
<i>LogLogic</i>	✓	✓	✓	
<i>NetIQ</i>	✓	✓	✓	
<i>Q1 Labs</i>	✓	✓	✓	✓
<i>Computer Associates eTrust</i>	✓	✓		

## Summary

Juniper's support of SNMP and SYSLOG for event forwarding ensures that IDP family of products will be able to interoperate with SIM products.

Copyright © 2005 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.

<sup>1</sup> Alliance partnership was with Guarded Net which Micromuse purchased in July of 2005.

<sup>2</sup> This product was formerly known as Protego before acquisition by Cisco.

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

Part Number: 351127-001 August 2005