This product includes the Envoy SNMP Engine, developed by Epilogue Technology, an Integrated Systems Company. Copyright © 1986-1997, Epilogue Technology Corporation. All rights reserved. This program and its documentation were developed at private expense, and no part of them is in the public domain.

This product includes memory allocation software developed by Mark Moraes, copyright © 1988, 1989, 1995, University of Toronto.

This product includes FreeBSD software developed by the University of California, Berkeley, and its contributors. All of the documentation and software included in the 4.4BSD and 4.4BSD-Lite Releases is copyrighted by the Regents of the University of California. Copyright © 1979, 1980, 1983, 1986, 1988, 1989, 1991, 1992, 1993, 1994. The Regents of the University of California. All rights reserved.

GateD software copyright © 1995, the Regents of the University. All rights reserved. Gate Daemon was originated and developed through release 3.0 by Cornell University and its collaborators. GateD is based on Kirton’s EGP, UC Berkeley’s routing daemon (routed), and DCN’s HELLO routing protocol. Development of Gated has been supported in part by the National Science Foundation. Portions of the GateD software copyright © 1988, Regents of the University of California. All rights reserved. Portions of the GateD software copyright © 1991, D. L. S. Associates.

This product includes software developed by Maker Communications, Inc., copyright © 1996, 1997, Maker Communications, Inc.

Juniper Networks, the Juniper Networks logo, JUNOS, NetScreen, ScreenOS, and Steel-Belted Radius are registered trademarks of Juniper Networks, Inc. in the United States and other countries. JUNOSe is a trademark of Juniper Networks, Inc. All other trademarks, service marks, registered trademarks, or registered service marks are the property of their respective owners.

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.

Products made or sold by Juniper Networks or components thereof might be covered by one or more of the following patents that are owned by or licensed to Juniper Networks: U.S. Patent Nos. 5,473,599, 5,905,725, 5,909,440, 6,192,051, 6,333,650, 6,359,479, 6,406,312, 6,429,706, 6,459,579, 6,493,347, 6,538,518, 6,538,899, 6,552,918, 6,567,902, 6,578,186, and 6,590,785.

Network and Security Manager Configuring Intrusion Detection and Prevention Devices Guide
Release 2009.1
Copyright © 2009, Juniper Networks, Inc.
All rights reserved. Printed in USA.

Revision History
24 August 2009—01

The information in this document is current as of the date listed in the revision history.

YEAR 2000 NOTICE

Juniper Networks hardware and software products are Year 2000 compliant. The JUNOS Software has no known time-related limitations through the year 2038. However, the NTP application is known to have some difficulty in the year 2036.
END USER LICENSE AGREEMENT

READ THIS END USER LICENSE AGREEMENT ("AGREEMENT") BEFORE DOWNLOADING, INSTALLING, OR USING THE SOFTWARE. BY DOWNLOADING, INSTALLING, OR USING THE SOFTWARE OR OTHERWISE EXPRESSING YOUR AGREEMENT TO THE TERMS CONTAINED HEREIN, YOU (AS CUSTOMER OR IF YOU ARE NOT THE CUSTOMER, AS A REPRESENTATIVE/AGENT AUTHORIZED TO BIND THE CUSTOMER) CONSENT TO BE BOUND BY THIS AGREEMENT. IF YOU DO NOT OR CANNOT AGREE TO THE TERMS CONTAINED HEREIN, THEN (A) DO NOT DOWNLOAD, INSTALL, OR USE THE SOFTWARE, AND (B) YOU MAY CONTACT JUNIPER NETWORKS REGARDING LICENSE TERMS.

1. The Parties. The parties to this Agreement are (i) Juniper Networks, Inc. (if the Customer’s principal office is located in the Americas) or Juniper Networks (Cayman) Limited (if the Customer’s principal office is located outside the Americas) (such applicable entity being referred to herein as “Juniper”), and (ii) the person or organization that originally purchased from Juniper or an authorized Juniper reseller the applicable license(s) for use of the Software (“Customer”) (collectively, the “Parties”).

2. The Software. In this Agreement, “Software” means the program modules and features of the Juniper or Juniper-supplied software, for which Customer has paid the applicable license or support fees to Juniper or an authorized Juniper reseller, or which was embedded by Juniper in equipment which Customer purchased from Juniper or an authorized Juniper reseller. “Software” also includes updates, upgrades and new releases of such software. “Embedded Software” means Software which Juniper has embedded in or loaded onto the Juniper equipment and any updates, upgrades, additions or replacements which are subsequently embedded in or loaded onto the equipment.

3. License Grant. Subject to the payment of the applicable fees and the limitations and restrictions set forth herein, Juniper grants to Customer a non-exclusive and non-transferable license, without right to sublicense, to use the Software, in executable form only, subject to the following use restrictions:

   a. Customer shall use Embedded Software solely as embedded in, and for execution on, Juniper equipment originally purchased by Customer from Juniper or an authorized Juniper reseller.

   b. Customer shall use the Software on a single hardware chassis having a single processing unit, or as many chassis or processing units for which Customer has paid the applicable license fees, provided, however, with respect to the Steel-Belted Radius or Odyssey Access Client software only, Customer shall use such Software on a single computer containing a single physical random access memory space and containing any number of processors. Use of the Steel-Belted Radius or IMS AAA software on multiple computers or virtual machines (e.g., Solaris zones) requires multiple licenses, regardless of whether such computers or virtualizations are physically contained on a single chassis.

   c. Product purchase documents, paper or electronic user documentation and/or the particular licenses purchased by Customer may specify limits to Customer’s use of the Software. Such limits may restrict use to a maximum number of seats, registered endpoints, concurrent users, sessions, calls, connections, subscribers, clusters, nodes, realms, devices, links, ports or transactions, or require the purchase of separate licenses to use particular features, functionalities, services, applications, operations, or capabilities, or provide throughput, performance, configuration, bandwidth, interface, processing, temporal, or geographical limits. In addition, such limits may restrict the use of the Software to managing certain kinds of networks or require the Software to be used only in conjunction with other specific Software. Customer’s use of the Software shall be subject to all such limitations and purchase of all applicable licenses.

   d. For any trial copy of the Software, Customer’s right to use the Software expires 30 days after download, installation or use of the Software. Customer may operate the Software after the 30-day trial period only if Customer pays for a license to do so. Customer may not extend or create an additional trial period by re-installing the Software after the 30-day trial period.

   e. The Global Enterprise Edition of the Steel-Belted Radius software may be used by Customer only to manage access to Customer’s enterprise network. Specifically, service provider customers are expressly prohibited from using the Global Enterprise Edition of the Steel-Belted Radius software to support any commercial network access services.

The foregoing license is not transferable or assignable by Customer. No license is granted herein to any user who did not originally purchase the applicable license(s) for the Software from Juniper or an authorized Juniper reseller.

4. Use Prohibitions. Notwithstanding the foregoing, the license provided herein does not permit the Customer to, and Customer agrees not to and shall not: (a) modify, unbundle, reverse engineer, or create derivative works based on the Software; (b) make unauthorized copies of the Software (except as necessary for backup purposes); (c) rent, sell, transfer, or grant any rights in and to any copy of the Software, in any form, to any third party; (d) remove any proprietary notices, labels, or marks on or in any copy of the Software or any product in which the Software is embedded; (e) distribute any copy of the Software to any third party, including as may be embedded in Juniper equipment sold in the secondhand market; (f) use any ‘locked’ or key-restricted feature, function, service, application, operation, or capability without first purchasing the applicable license(s) and obtaining a valid key from Juniper, even if such feature, function, service, application, operation, or capability is enabled without a key; (g) distribute any key for the Software provided by Juniper to any third party; (h) use the Software in any manner that extends or is broader than the uses purchased by Customer from Juniper or an authorized Juniper reseller; (i) use Embedded Software on non-Juniper equipment; (j) use Embedded Software (or make it available for use) on Juniper equipment that the Customer did not originally purchase from Juniper or an authorized Juniper reseller; (k) disclose the results of testing or benchmarking of the Software to any third party without the prior written consent of Juniper; or (l) use the Software in any manner other than as expressly provided herein.

5. Audit. Customer shall maintain accurate records as necessary to verify compliance with this Agreement. Upon request by Juniper, Customer shall furnish such records to Juniper and certify its compliance with this Agreement.
6. Confidentiality. The Parties agree that aspects of the Software and associated documentation are the confidential property of Juniper. As such, Customer shall exercise all reasonable commercial efforts to maintain the Software and associated documentation in confidence, which at a minimum includes restricting access to the Software to Customer employees and contractors having a need to use the Software for Customer’s internal business purposes.

7. Ownership. Juniper and Juniper’s licensors, respectively, retain ownership of all right, title, and interest (including copyright) in and to the Software, associated documentation, and all copies of the Software. Nothing in this Agreement constitutes a transfer or conveyance of any right, title, or interest in the Software or associated documentation, or a sale of the Software, associated documentation, or copies of the Software.

8. Warranty, Limitation of Liability, Disclaimer of Warranty. The warranty applicable to the Software shall be as set forth in the warranty statement that accompanies the Software (the “Warranty Statement”). Nothing in this Agreement shall give rise to any obligation to support the Software. Support services may be purchased separately. Any such support shall be governed by a separate, written support services agreement. TO THE MAXIMUM EXTENT PERMITTED BY LAW, JUNIPER SHALL NOT BE LIABLE FOR ANY LOST PROFITS, LOSS OF DATA, OR COSTS OR PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES, OR FOR ANY SPECIAL, INDIRECT, OR CONSEQUENTIAL DAMAGES ARISING OUT OF THIS AGREEMENT, THE SOFTWARE, OR ANY JUNIPER OR JUNIPER-SUPPLIED SOFTWARE. IN NO EVENT SHALL JUNIPER BE LIABLE FOR DAMAGES ARISING FROM UNAUTHORIZED OR IMPROPER USE OF ANY JUNIPER OR JUNIPER-SUPPLIED SOFTWARE. EXCEPT AS EXPRESSLY PROVIDED IN THE WARRANTY STATEMENT TO THE EXTENT PERMITTED BY LAW, JUNIPER DISCLAIMS ANY AND ALL WARRANTIES IN AND TO THE SOFTWARE (WHETHER EXPRESS, IMPLIED, STATUTORY, OR OTHERWISE), INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NONINFRINGEMENT. IN NO EVENT DOES JUNIPER WARRANT THAT THE SOFTWARE, OR ANY EQUIPMENT OR NETWORK RUNNING THE SOFTWARE, WILL OPERATE WITHOUT ERROR OR INTERRUPTION, OR WILL BE FREE OF VULNERABILITY TO INTRUSION OR ATTACK. In no event shall Juniper’s or its suppliers’ or licensors’ liability to Customer, whether in contract, tort (including negligence), breach of warranty, or otherwise, exceed the price paid by Customer for the Software that gave rise to the claim, or if the Software is embedded in another Juniper product, the price paid by Customer for such other product. Customer acknowledges and agrees that Juniper has set its prices and entered into this Agreement in reliance upon the disclaimers of warranty and the limitations of liability set forth herein, that the same reflect an allocation of risk between the Parties (including the risk that a contract remedy may fail of its essential purpose and cause consequential loss), and that the same form an essential basis of the bargain between the Parties.

9. Termination. Any breach of this Agreement or failure by Customer to pay any applicable fees due shall result in automatic termination of the license granted herein. Upon such termination, Customer shall destroy or return to Juniper all copies of the Software and related documentation in Customer’s possession or control.

10. Taxes. All license fees payable under this Agreement are exclusive of tax. Customer shall be responsible for paying Taxes arising from the purchase of the license, or importation or use of the Software. If applicable, valid exemption documentation for each taxing jurisdiction shall be provided to Juniper prior to invoicing, and Customer shall promptly notify Juniper if their exemption is revoked or modified. All payments made by Customer shall be net of any applicable withholding tax. Customer will provide reasonable assistance to Juniper in connection with such withholding taxes by promptly: providing Juniper with valid tax receipts and other required documentation showing Customer’s payment of any withholding taxes; completing appropriate applications that would reduce the amount of withholding tax to be paid; and notifying and assisting Juniper in any audit or tax proceeding related to transactions hereunder. Customer shall comply with all applicable tax laws and regulations, and Customer will promptly pay or reimburse Juniper for all costs and damages related to any liability incurred by Juniper as a result of Customer’s non-compliance or delay with its responsibilities herein. Customer’s obligations under this Section shall survive termination or expiration of this Agreement.

11. Export. Customer agrees to comply with all applicable export laws and restrictions of any United States and any applicable foreign agency or authority, and to not export or re-export the Software or any direct product thereof in violation of any such restrictions, laws or regulations, or without all necessary approvals. Customer shall be liable for any such violations. The version of the Software supplied to Customer may contain encryption or other capabilities restricting Customer’s ability to export the Software without an export license.

12. Commercial Computer Software. The Software is “commercial computer software” and is provided with restricted rights. Use, duplication, or disclosure by the United States government is subject to restrictions set forth in this Agreement and as provided in DFARS 227.7201 through 227.7202-4, FAR 12.212, FAR 27.405(b)(2), FAR 52.227-19, or FAR 52.227-14(ALT II) as applicable.

13. Interface Information. To the extent required by applicable law, and at Customer’s written request, Juniper shall provide Customer with the interface information needed to achieve interoperability between the Software and another independently created program, on payment of applicable fee, if any. Customer shall observe strict obligations of confidentiality with respect to such information and shall use such information in compliance with any applicable terms and conditions upon which Juniper makes such information available.

14. Third Party Software. Any licensor of Juniper whose software is embedded in the Software and any supplier of Juniper whose products or technology are embedded in (or services are accessed by) the Software shall be a third party beneficiary with respect to this Agreement, and such licensor or vendor shall have the right to enforce this Agreement in its own name as if it were Juniper. In addition, certain third party software may be provided with the Software and is subject to the accompanying license(s), if any, of its respective owner(s). To the extent portions of the Software are distributed under and subject to open source licenses obligating Juniper to make the source code for such portions publicly available (such as the GNU General Public License (“GPL”) or the GNU Library General Public License (“LGPL”)), Juniper will make such source code portions (including Juniper modifications, as appropriate) available upon request for a period of up to three years from the date of distribution. Such request can be made in writing to Juniper Networks, Inc., 1194 N. Mathilda Ave., Sunnyvale, CA 94089, ATTN: General Counsel. You may obtain a copy of the GPL at http://www.gnu.org/licenses/gpl.html, and a copy of the LGPL at http://www.gnu.org/licenses/lgpl.html.

15. Miscellaneous. This Agreement shall be governed by the laws of the State of California without reference to its conflicts of laws principles. The provisions of the U.N. Convention for the International Sale of Goods shall not apply to this Agreement. For any disputes arising under this Agreement, the Parties hereby consent to the personal and exclusive jurisdiction of, and venue in, the state and federal courts within Santa Clara County, California. This Agreement constitutes the entire and sole agreement between Juniper and the Customer with respect to the Software, and supersedes all prior and contemporaneous agreements.
agreements relating to the Software, whether oral or written (including any inconsistent terms contained in a purchase order), except that the terms of a separate written agreement executed by an authorized Juniper representative and Customer shall govern to the extent such terms are inconsistent or conflict with terms contained herein. No modification to this Agreement nor any waiver of any rights hereunder shall be effective unless expressly assented to in writing by the party to be charged. If any portion of this Agreement is held invalid, the Parties agree that such invalidity shall not affect the validity of the remainder of this Agreement. This Agreement and associated documentation has been written in the English language, and the Parties agree that the English version will govern. (For Canada: Les parties aux présentes confirment leur volonté que cette convention de même que tous les documents y compris tout avis qui s’y rattache, soient rédigés en langue anglaise. (Translation: The parties confirm that this Agreement and all related documentation is and will be in the English language).)
# Table of Contents

## About This Guide

- Objectives ......................................................... xiii
- Audience ............................................................... xiii
- Conventions ............................................................ xiii
- List of Technical Publications .................................. xv
- Requesting Technical Support .................................. xvi
  - Self-Help Online Tools and Resources ..................... xvi
  - Opening a Case with JTAC .................................... xvii

## Part 1  Getting Started

### Chapter 1  Intrusion Detection and Prevention Device and NSM Installation Overview

- Intrusion Detection and Prevention Device Installation Overview ................. 3
- NSM Installation Overview ............................................. 3

### Chapter 2  Understanding Intrusion Detection and Prevention Device Configuration and Integration Overview

- NSM and Intrusion Detection and Prevention Device Management Overview ................................................................. 5
- Intrusion Detection and Prevention Services and Device Configurations Supported in NSM ............................................................. 6
- Adding Intrusion Detection and Prevention Devices in NSM Overview .......... 8
- Adding Intrusion Detection and Prevention Clusters in NSM Overview ......... 8
- Using Templates and Configuration Groups in NSM Overview .................. 8

## Part 2  Configuring Intrusion Detection and Prevention Devices

### Chapter 3  Configuring Profiler Settings

- Configuring Profiler Options (NSM Procedure) ............................................. 13
  - Specifying General Options ......................................................... 14
  - Specifying Tracked Hosts .............................................................. 16
### Chapter 4  
#### Configuring Security Policies  

- Intrusion Detection and Prevention Devices and Security Policies  
  - Overview .............................................. 29  
- Configuring Predefined Security Policies (NSM Procedure) ..................... 31  
- Creating a New Security Policy (NSM Procedure) ................................. 32  
- Modifying IDP Rulebase Rules (NSM Procedure) ..................................... 34  
  - Specifying Rule Match Conditions .................................................... 35  
  - Specifying IDP Rulebase Attack Objects ............................................ 37  
  - Specifying Rule Session Action ......................................................... 38  
  - Specifying Rule IP Action ................................................................. 39  
  - Specifying Rule Notification Options ................................................ 40  
  - Specifying Rule VLAN Matches ....................................................... 41  
  - Specifying Rule Targets ................................................................. 41  
  - Specifying Rule Severity ................................................................. 42  
  - Specifying Rule Optional Fields ...................................................... 42  
  - Specifying Rule Comments ............................................................ 43  
- Configuring Exempt Rulebase Rules (NSM Procedure) ........................... 43  
- Configuring Backdoor Rulebase Rules (NSM Procedure) ....................... 45  
- Configuring SYN Protector Rulebase Rules (NSM Procedure) ............... 48  
- Configuring Traffic Anomalies Rulebase Rules (NSM Procedure) .......... 51  
- Configuring Network Honeypot Rulebase Rules (NSM Procedure) .......... 54  
- Configuring Application Rulebase Rules (NSM Procedure) .................... 57
<table>
<thead>
<tr>
<th>Chapter 5</th>
<th>Working with Attack Objects</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attack Objects in Intrusion Detection and Prevention Security Policies</td>
<td></td>
</tr>
<tr>
<td>Overview .................................................................................................................61</td>
<td></td>
</tr>
<tr>
<td>Loading J-Security-Center Updates (NSM Procedure) .................................................62</td>
<td></td>
</tr>
<tr>
<td>Viewing Predefined Attack Objects (NSM Procedure) ..................................................64</td>
<td></td>
</tr>
<tr>
<td>Working with Attack Groups (NSM Procedure) ..............................................................64</td>
<td></td>
</tr>
<tr>
<td>Creating Dynamic Groups ............................................................................................65</td>
<td></td>
</tr>
<tr>
<td>Creating Static Groups ..................................................................................................66</td>
<td></td>
</tr>
<tr>
<td>Creating Custom Attack Objects (NSM Procedure) ..........................................................67</td>
<td></td>
</tr>
<tr>
<td>Configuring General Properties for Attack Objects .........................................................67</td>
<td></td>
</tr>
<tr>
<td>Creating a Signature Attack Object .................................................................................69</td>
<td></td>
</tr>
<tr>
<td>Verifying the Attack Object Database Version (NSM Procedure) .......................................75</td>
<td></td>
</tr>
<tr>
<td>Updating the IDP Detector Engine (NSM Procedure) ........................................................76</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Chapter 6</th>
<th>Configuring SNMP and Syslog Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuring an SNMP Agent (NSM Procedure) ...............................................................79</td>
<td></td>
</tr>
<tr>
<td>Configuring Syslog Collection (NSM Procedure) ...........................................................80</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Chapter 7</th>
<th>Configuring Anti-Spoof Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuring Antispoof Settings in Intrusion Detection and Prevention Devices (NSM Procedure) ...................................................................................................83</td>
<td></td>
</tr>
<tr>
<td>Example: Applying Antispoof to a Web Server and Database Server (NSM Procedure) ..............................................................................................................84</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Chapter 8</th>
<th>Configuring Intrusion Detection and Prevention Device Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuring Load-Time Parameters (NSM Procedure) .....................................................87</td>
<td></td>
</tr>
<tr>
<td>Configuring Run-Time Parameters (NSM Procedure) ........................................................88</td>
<td></td>
</tr>
<tr>
<td>Configuring Router Parameters (NSM Procedure) ............................................................94</td>
<td></td>
</tr>
<tr>
<td>Configuring Protocol Handling (NSM Procedure) ............................................................95</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Chapter 9</th>
<th>Configuring Additional Intrusion Detection and Prevention Features</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuring Additional Intrusion Detection and Prevention Features Overview .................................................................111</td>
<td></td>
</tr>
<tr>
<td>Enabling Intrusion Detection and Prevention Processing of Encrypted and Encapsulated Traffic (NSM Procedure) ..........................................................111</td>
<td></td>
</tr>
<tr>
<td>Enabling SSL Decryption ................................................................................................112</td>
<td></td>
</tr>
<tr>
<td>Enabling GRE Decapsulation ............................................................................................112</td>
<td></td>
</tr>
<tr>
<td>Enabling GTP Decapsulation ............................................................................................113</td>
<td></td>
</tr>
<tr>
<td>Part 3</td>
<td>Managing Intrusion Detection and Prevention Devices</td>
</tr>
<tr>
<td>--------</td>
<td>-----------------------------------------------------</td>
</tr>
<tr>
<td>Chapter 10</td>
<td>Managing Security Policies in Intrusion Detection and Prevention Devices</td>
</tr>
<tr>
<td></td>
<td>Assigning a Security Policy in an Intrusion Detection and Prevention Device (NSM Procedure) ..........................................................</td>
</tr>
<tr>
<td></td>
<td>Validating a Security Policy (NSM Procedure) ..................</td>
</tr>
<tr>
<td></td>
<td>Troubleshooting Security Policy Validation Errors (NSM Procedure) ...........</td>
</tr>
<tr>
<td></td>
<td>Pushing Security Policy Updates to an IDP Device (NSM Procedure) ........</td>
</tr>
<tr>
<td></td>
<td>Troubleshooting Configuration Push Errors (NSM Procedure) ............</td>
</tr>
<tr>
<td></td>
<td>Disabling Rules (NSM Procedure) .......................................</td>
</tr>
<tr>
<td></td>
<td>Exporting Security Policies (NSM Procedure) ..........................</td>
</tr>
<tr>
<td>Chapter 11</td>
<td>Managing Profiler Settings in Intrusion Detection and Prevention Devices</td>
</tr>
<tr>
<td></td>
<td>Managing Profiler Settings ..................................................</td>
</tr>
<tr>
<td></td>
<td>Updating Profiler Settings ..................................................</td>
</tr>
<tr>
<td></td>
<td>Starting the Profiler ............................................................</td>
</tr>
<tr>
<td></td>
<td>Stopping the Profiler ............................................................</td>
</tr>
<tr>
<td>Part 4</td>
<td>Monitoring Intrusion Detection and Prevention Devices</td>
</tr>
<tr>
<td>Chapter 12</td>
<td>Working with NSM Logs and Reports</td>
</tr>
<tr>
<td></td>
<td>NSM Logs and Reports Overview .............................................</td>
</tr>
<tr>
<td></td>
<td>Viewing Logs ............................................................................</td>
</tr>
<tr>
<td></td>
<td>IDP Logs ................................................................................</td>
</tr>
<tr>
<td></td>
<td>Using NSM Log Investigator ....................................................</td>
</tr>
<tr>
<td></td>
<td>Using NSM Audit Log Viewer ...................................................</td>
</tr>
<tr>
<td></td>
<td>Viewing Device Status ............................................................</td>
</tr>
<tr>
<td></td>
<td>Viewing NSM Predefined Reports ..............................................</td>
</tr>
<tr>
<td></td>
<td>Creating NSM Custom Reports ..................................................</td>
</tr>
<tr>
<td></td>
<td>Configuring Log Suppression ....................................................</td>
</tr>
<tr>
<td>Chapter 13</td>
<td>Working with Intrusion Detection and Prevention Reporter Reports</td>
</tr>
<tr>
<td></td>
<td>Intrusion Detection and Prevention Reporter Overview ..................</td>
</tr>
</tbody>
</table>
Part 5

Index

Index ........................................................................................................... 147
About This Guide

- Objectives on page xiii
- Audience on page xiii
- Conventions on page xiii
- List of Technical Publications on page xv
- Requesting Technical Support on page xvi

Objectives

Network and Security Manager (NSM) is a software application that centralizes control and management of your Juniper Networks devices. With NSM, Juniper Networks delivers integrated, policy-based security and network management for all security devices.

Intrusion Detection and Prevention (IDP) series uses eight detection methods to detect malicious network traffic. It is able to drop attacks to prevent damage to your network and can operate inline as a forwarding gateway, directly in the path of traffic coming and going on your network.

This guide provides the various steps to configure and manage IDP devices using NSM. This guide also helps in understanding of how to configure basic and advanced NSM functionality, including adding new devices, deploying new device configurations, updating device firmware, viewing log information, and monitoring the status of IDP devices.

Audience

This guide is intended for the system administrators who are responsible for configuring IDP devices.

Conventions

This section provides all the documentation conventions that are followed in this guide. Table 1 on page xiv defines notice icons used in this guide.
Table 1: Notice Icons

<table>
<thead>
<tr>
<th>Icon</th>
<th>Meaning</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Informational note" /></td>
<td>Informational note</td>
<td>Indicates important features or instructions.</td>
</tr>
<tr>
<td><img src="image" alt="Caution" /></td>
<td>Caution</td>
<td>Indicates a situation that might result in loss of data or hardware damage.</td>
</tr>
<tr>
<td><img src="image" alt="Warning" /></td>
<td>Warning</td>
<td>Alerts you to the risk of personal injury or death.</td>
</tr>
<tr>
<td><img src="image" alt="Laser warning" /></td>
<td>Laser warning</td>
<td>Alerts you to the risk of personal injury from a laser.</td>
</tr>
</tbody>
</table>

Table 2 on page xiv defines text conventions used in this guide.

Table 2: Text Conventions

<table>
<thead>
<tr>
<th>Convention</th>
<th>Description</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Bold typeface like this</strong></td>
<td>Represents commands and keywords in text. Represents keywords Represents UI elements</td>
<td>Issue the <code>clock source</code> command. Specify the keyword <code>exp-msg</code>. Click <strong>User Objects</strong></td>
</tr>
<tr>
<td><strong>Bold typeface like this</strong></td>
<td>Represents text that the user must type.</td>
<td><strong>user input</strong></td>
</tr>
<tr>
<td><strong>fixed-width font</strong></td>
<td>Represents information as displayed on the terminal screen.</td>
<td><code>host1# show ip ospf</code> Routing Process OSPF 2 with Router ID 5.5.0.250 Router is an area Border Router (ABR)</td>
</tr>
<tr>
<td><strong>Key names linked with a plus (+) sign</strong></td>
<td>Indicates that you must press two or more keys simultaneously.</td>
<td>Ctrl + d</td>
</tr>
<tr>
<td><strong>Italics</strong></td>
<td>Emphasizes words Identifies variables</td>
<td>The product supports two levels of access, <code>user</code> and <code>privileged</code>. <code>clusterID</code>, <code>ipAddress</code>.</td>
</tr>
<tr>
<td><strong>The angle bracket (&gt;)</strong></td>
<td>Indicates navigation paths through the UI by clicking menu options and links.</td>
<td><strong>Object Manager &gt; User Objects &gt; Local Objects</strong></td>
</tr>
</tbody>
</table>

Table 3 on page xv defines syntax conventions used in this guide.
### Table 3: Syntax Conventions

<table>
<thead>
<tr>
<th>Convention</th>
<th>Description</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>Words in plain text</td>
<td>Represent keywords</td>
<td>terminal length</td>
</tr>
<tr>
<td>Words in italics</td>
<td>Represent variables</td>
<td>mask, accessListName</td>
</tr>
<tr>
<td>Words separated by the pipe (</td>
<td>) symbol</td>
<td>Represent a choice to select one keyword or variable to the left or right of this symbol. The keyword or variable can be optional or required.</td>
</tr>
<tr>
<td>Words enclosed in brackets ([ ])</td>
<td>Represent optional keywords or variables.</td>
<td>[ internal</td>
</tr>
<tr>
<td>Words enclosed in brackets followed by and asterisk ([ ]*)</td>
<td>Represent optional keywords or variables that can be entered more than once.</td>
<td>[ level1</td>
</tr>
<tr>
<td>Words enclosed in braces ({ })</td>
<td>Represent required keywords or variables.</td>
<td>{ permit</td>
</tr>
</tbody>
</table>

### List of Technical Publications

This section provides the list of the documentations required for any additional information.

### Table 4: Network and Security Manager and IDP Device Publications

<table>
<thead>
<tr>
<th>Publication</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network and Security Manager Installation Guide</td>
<td>Details the steps to install the NSM management system on a single server or on separate servers. It also includes information on how to install and run the NSM user interface. This guide is intended for IT administrators responsible for the installation and/or upgrade to NSM.</td>
</tr>
<tr>
<td>Network and Security Manager Administration Guide</td>
<td>Describes how to use and configure key management features in the NSM. It provides conceptual information, suggested workflows, and examples where applicable. This guide is best used in conjunction with the NSM Online Help, which provides step-by-step instructions for performing management tasks in the NSM UI. This guide is intended for application administrators or those individuals responsible for owning the server and security infrastructure and configuring the product for multi-user systems. It is also intended for device configuration administrators, firewall and VPN administrators, and network security operation center administrators.</td>
</tr>
<tr>
<td>Network and Security Manager Configuring Firewall/VPN Devices Guide</td>
<td>Describes NSM features that relate to device configuration and management. It also explains how to configure basic and advanced NSM functionality, including deploying new device configurations, managing Security Policies and VPNs, and general device administration.</td>
</tr>
<tr>
<td>Network and Security Manager Online Help</td>
<td>Provides task-oriented procedures describing how to perform basic tasks in the NSM user interface. It also includes a brief overview of the NSM system and a description of the GUI elements.</td>
</tr>
<tr>
<td>IDP Installation Guide</td>
<td>Details the physical features of Juniper Networks Intrusion Detection and Prevention (IDP) series. It also explains how to install, configure, update/reimage, and service the IDP system.</td>
</tr>
</tbody>
</table>
**Table 4: Network and Security Manager and IDP Device Publications (continued)**

<table>
<thead>
<tr>
<th>Publication</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>IDP Concepts &amp; Examples Guide</td>
<td>Details about the Juniper Networks Intrusion Detection and Prevention (IDP) series that uses multiple methods to detect and prevent network attacks. IDP is designed to reduce false positives to ensure that only actual malicious traffic is detected and stopped.</td>
</tr>
<tr>
<td>IDP Reporter User's Guide</td>
<td>Details about the IDP Reporter that enables you to analyze your enterprise network thoroughly so you can assess attacks, attackers, and resource utilization.</td>
</tr>
<tr>
<td>IDP ACM Online Help</td>
<td>Details about how to complete the IDP QuickStart and ACM Wizard which is available through the IDP Appliance Configuration Manager (ACM) as context-sensitive online help.</td>
</tr>
<tr>
<td>IDP Detector Engine Release Notes</td>
<td>Details about IDP Detector Engine features and resolved issues in the recent releases. It also helps you to decide to update the IDP Detector Engine version in your deployment.</td>
</tr>
</tbody>
</table>

**Requesting Technical Support**

Technical product support is available through the Juniper Networks Technical Assistance Center (JTAC). If you are a customer with an active J-Care or JNASC support contract, or are covered under warranty, and need post-sales technical support, you can access our tools and resources online or open a case with JTAC.

- **Product warranties**—For product warranty information, visit [http://www.juniper.net/support/warranty/](http://www.juniper.net/support/warranty/).
- **JTAC hours of operation**—The JTAC centers have resources available 24 hours a day, 7 days a week, 365 days a year.

**Self-Help Online Tools and Resources**

For quick and easy problem resolution, Juniper Networks has designed an online self-service portal called the Customer Support Center (CSC) that provides you with the following features:

- **Find CSC offerings**: [http://www.juniper.net/customers/support/](http://www.juniper.net/customers/support/)
- **Search for known bugs**: [http://www2.juniper.net/kb/](http://www2.juniper.net/kb/)
- **Find product documentation**: [http://www.juniper.net/techpubs/](http://www.juniper.net/techpubs/)
- **Find solutions and answer questions using our Knowledge Base**: [http://kb.juniper.net/](http://kb.juniper.net/)
- **Download the latest versions of software and review release notes**: [http://www.juniper.net/customers/csc/software/](http://www.juniper.net/customers/csc/software/)
- **Search technical bulletins for relevant hardware and software notifications**: [https://www.juniper.net/alerts/](https://www.juniper.net/alerts/)
- **Join and participate in the Juniper Networks Community Forum**: [http://www.juniper.net/company/communities/](http://www.juniper.net/company/communities/)
- **Open a case online in the CSC Case Management tool**: [http://www.juniper.net/cm/](http://www.juniper.net/cm/)
To verify service entitlement by product serial number, use our Serial Number Entitlement (SNE) Tool located at https://tools.juniper.net/SerialNumberEntitlementSearch/.

**Opening a Case with JTAC**

You can open a case with JTAC on the Web or by telephone.

- Use the Case Management tool in the CSC at http://www.juniper.net/cm/.
- Call 1-888-314-JTAC (1-888-314-5822 toll-free in the USA, Canada, and Mexico).

For international or direct-dial options in countries without toll-free numbers, see http://www.juniper.net/support/requesting_support.html
Part 1

Getting Started

- Intrusion Detection and Prevention Device and NSM Installation Overview on page 3
- Understanding Intrusion Detection and Prevention Device Configuration and Integration Overview on page 5
Chapter 1
Intrusion Detection and Prevention Device and NSM Installation Overview

Intrusion Detection and Prevention Device Installation Overview

The Intrusion Detection and Prevention (IDP) series consists of hardware and software components. You can install the IDP device and start configuring your system using the following steps:

1. Decide on the physical location of the device.
2. Install the device into your equipment rack.
3. Connect power cables and power on.
4. Perform some initial configuration steps.
5. Install the device license key.

See the installation documentation for your IDP model to install, configure, update, and service a Juniper Networks IDP device.

Related Topics
- NSM Installation Overview on page 3
- NSM and Intrusion Detection and Prevention Device Management Overview on page 5

NSM Installation Overview

NSM is a software application that enables you to integrate and centralize management of your Juniper Networks environment. You need to install two main software components to run NSM: the NSM management system and the NSM user interface (UI).

See the Network Security Manager Installation Guide for the steps to install the NSM management system on a single server or on separate servers. It also includes information on how to install and run the NSM user interface. The Network Security Manager Installation Guide is intended for IT administrators responsible for installing or upgrading to the NSM.
Related Topics

- Intrusion Detection and Prevention Device Installation Overview on page 3
- NSM and Intrusion Detection and Prevention Device Management Overview on page 5
Chapter 2

Understanding Intrusion Detection and Prevention Device Configuration and Integration Overview

- NSM and Intrusion Detection and Prevention Device Management Overview on page 5
- Intrusion Detection and Prevention Services and Device Configurations Supported in NSM on page 6
- Adding Intrusion Detection and Prevention Devices in NSM Overview on page 8
- Adding Intrusion Detection and Prevention Clusters in NSM Overview on page 8
- Using Templates and Configuration Groups in NSM Overview on page 8

NSM and Intrusion Detection and Prevention Device Management Overview

NSM is the Juniper Networks network management tool that allows distributed administration of network appliances. You can use the NSM application to centralize status monitoring, logging, and reporting, and to administer IDP Series configurations.

IDP technology detects and stops attacks when deployed inline to your network. Unlike intrusion detection service (IDS), IDP uses multiple methods to detect attacks against your network and to prevent attackers from gaining access and damaging your system. IDP drops malicious packets or connections before the attacks enter your network. IDP is designed to reduce false positives and ensure that only actual malicious traffic is detected and stopped. You can also deploy IDP as a passive sniffer, similar to a traditional IDS, but with greater accuracy and manageability.

NSM is the sole means for configuring and managing IDP on the ISG1000, ISG2000, and standalone IDP Sensors running IDP 4.x. Standalone IDP sensors running IDP 3.x and earlier are managed using the IDP management server and UI.

The ISG1000 and ISG2000 security modules have an optional component installed that provides IDP functionality. If you have purchased an ISG1000 or ISG2000 device that does not have IDP capability, you can upgrade the device to be an IDP-capable system by replacing the memory chip in the CPU. You install up to three security modules and insta the Advanced and IDP license keys for IDP.

With NSM, you can manage most of the parameters that you can configure through the IDP admin console. The configuration screens rendered through NSM are similar
to the screens in the IDP admin console. NSM incorporates a broad configuration management framework that allows co-management using other methods.

After you have completed installation, follow these steps to get started with managing an IDP device with NSM:

1. Add the IDP device to NSM. When you first add the IDP device to NSM in first instance, NSM pushes the policy named Recommended to the device.
2. Update the IDP detector engine and attack object database.
3. Update software version (if necessary).
4. Run the Profiler.
5. Examine the logs.
6. Create address objects for IDP rulebase rules.
7. Optionally, configure additional rulebases.
8. If adding this device changes your plan to distribute administrative responsibility, create NSM users with the access privileges.

An administrator (a user of NSM or IDP) has a specific level of permission. You can create multiple administrators with specific roles to control access to the devices in each domain.

Related Topics
- Intrusion Detection and Prevention Services and Device Configurations Supported in NSM on page 6
- Adding Intrusion Detection and Prevention Devices in NSM Overview on page 8

Intrusion Detection and Prevention Services and Device Configurations Supported in NSM

The Intrusion Detection and Prevention (IDP) device supports the following services in NSM:

- Inventory management service—NSM enables upgrading license and management of the IDP hardware details. Adding or deleting licenses or upgrading or downgrading software are not supported.

- Status monitoring service—Allows the IDP device’s status to be obtained, including name, domain, OS version, synchronization status, connection details, current alarms, CPU, memory, and swap.

- Logging service—Allows the IDP device’s logs to be obtained in a time-generated order. Logging configuration details that are set on the IDP device will apply to NSM.

- Packaging log files or debug files for remote analysis

- Managing interface settings such as setting IP addresses, settings IDP device host and network information, interoperability with NSM, Infranet Controllers, Secure Access devices, settings deployment mode, enabling layer 2 processing, and so on. For more information see the ACM online Help.
The following device configurations are not supported:

- Editing licensing information, although licenses can be viewed
- Rebooting the IDP device

On standalone IDP sensors and ISG security module settings inspects the following protocols using Table 5 on page 7.

### Table 5: Intrusion Detection and Prevention: Supported Protocols

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>AIM</td>
<td>HTTP</td>
<td>Oracle</td>
<td>SMTP</td>
</tr>
<tr>
<td>CHARGEN</td>
<td>ICMP</td>
<td>POP3</td>
<td>SNMP/Trap</td>
</tr>
<tr>
<td>DHCP</td>
<td>IDENT</td>
<td>PortMapper</td>
<td>SQL Mon</td>
</tr>
<tr>
<td>DISCARD</td>
<td>IKE</td>
<td>RADIUS</td>
<td>SSH</td>
</tr>
<tr>
<td>DNS</td>
<td>IMAP</td>
<td>Rexec</td>
<td>SSL</td>
</tr>
<tr>
<td>ECHO</td>
<td>IRC</td>
<td>rlogin</td>
<td>Syslog</td>
</tr>
<tr>
<td>FINGER</td>
<td>LDAP</td>
<td>SunRPC</td>
<td>TELNET</td>
</tr>
<tr>
<td>FTP</td>
<td>LPR</td>
<td>Rsh</td>
<td>TFTP</td>
</tr>
<tr>
<td>GNUTELLA</td>
<td>MSN</td>
<td>RTSP</td>
<td>VNC</td>
</tr>
<tr>
<td>Gopher</td>
<td>MSRPC</td>
<td>NBNAME</td>
<td>WHOIS</td>
</tr>
<tr>
<td>GRE*</td>
<td>MS-SQL</td>
<td>NFS</td>
<td>Yahoo Messenger</td>
</tr>
<tr>
<td>H.225**</td>
<td>GTP</td>
<td>NNTOP</td>
<td></td>
</tr>
<tr>
<td>NTP</td>
<td>Rusers</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SMB</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

* GRE inspection are supported only for IP (protocol 0x0800) and PPP for CDMA A10 channel (protocol 0x8881). PPP is a Layer 2 protocol, which can carry any Layer 3 protocols. Within PPP, IDP inspects IP and Van Jacobson compressed TCP.

** Standalone IDP only.

** Related Topics **

- Adding Intrusion Detection and Prevention Clusters in NSM Overview on page 8
- Using Templates and Configuration Groups in NSM Overview on page 8
- NSM and Intrusion Detection and Prevention Device Management Overview on page 5
Adding Intrusion Detection and Prevention Devices in NSM Overview

Before NSM can manage IDP devices, you must first add the IDP devices to the management system using the NSM UI. To add an IDP device, you create an object in the UI that represents the physical device, and then create a connection between the UI object and the device so that their information is linked. When you make a change to the UI device object, you can push that information to the real device so the two remain synchronized. You can add a single IDP device at a time or add multiple IDP devices all at once.

For complete details on adding IDP devices, see the Network and Security Manager Administration Guide.

Related Topics
- Adding Intrusion Detection and Prevention Clusters in NSM Overview on page 8
- Using Templates and Configuration Groups in NSM Overview on page 8

Adding Intrusion Detection and Prevention Clusters in NSM Overview

In IDP, maximum of two clusters join together to ensure continued network uptime. The device configurations are synchronized, meaning all cluster members share the same configuration settings, enabling an IDP device to handle traffic for another if one device fails.

Adding a cluster is a two-stage process:
- Add the cluster device object.
- Add the members of the cluster to the cluster device object.

For complete details on adding IDP clusters, see the Network and Security Manager Administration Guide.

Related Topics
- Using Templates and Configuration Groups in NSM Overview on page 8
- NSM and Intrusion Detection and Prevention Device Management Overview on page 5

Using Templates and Configuration Groups in NSM Overview

Use templates to define an IDP device configuration and then reuse that configuration information across multiple IDP devices. In a template, you need to define only those configuration parameters that you want to set; you do not need to specify a complete device configuration.

Templates provide these benefits:
- You can configure parameter values for an IDP device by referring to one or more templates when configuring the device.
When you change a parameter value in a template and save the template, the value also changes for all the IDP device configurations that refer to that template, unless specifically overridden in the device object.

For complete details on using device templates and configuration groups, see the Network and Security Manager Administration Guide.

Related Topics
- NSM and Intrusion Detection and Prevention Device Management Overview on page 5
- Intrusion Detection and Prevention Services and Device Configurations Supported in NSM on page 6
Part 2
Configuring Intrusion Detection and Prevention Devices

- Configuring Profiler Settings on page 13
- Configuring Security Policies on page 29
- Working with Attack Objects on page 61
- Configuring SNMP and Syslog Settings on page 79
- Configuring Anti-Spoof Settings on page 83
- Configuring Intrusion Detection and Prevention Device Settings on page 87
- Configuring Additional Intrusion Detection and Prevention Features on page 111
Chapter 3

Configuring Profiler Settings

Before configuring security, you must first enable and set up the Profiler. The Profiler is a network analysis tool that helps you learn about your internal network, enabling you to create effective security policies and minimize unnecessary log records. After you configure the Profiler, it automatically learns about your internal network and the elements that comprise it, including hosts, peers (communication between two hosts), ports (non-IP protocols, TCP/UDP ports, RPC programs), and Layer-7 data that uniquely identifies hosts, applications, commands, users, and filenames.

The Profiler is supported in all IDP modes and HA configurations, and also queries and correlates information from multiple devices. For details on analyzing your network, see the Network and Security Manager Administration Guide. This chapter provides information on setting up the Profiler and configuring antivirus settings, including antispam and Web filtering.

- Configuring Profiler Options (NSM Procedure) on page 13
- Viewing Profiler Logs (NSM Procedure) on page 20
- Modifying Profiler Settings (NSM Procedure) on page 25
- Configuring Profiler Database Preferences (NSM Procedure) on page 26
- Displaying Profiler Database Information (NSM Procedure) on page 27
- Querying the Profiler Database (NSM Procedure) on page 28
- Purging the Profiler Database (NSM Procedure) on page 28

Configuring Profiler Options (NSM Procedure)

Profiler option settings are valid for standalone IDP sensors only. For more information, see the NSM online Help.

To configure the Profiler on a given IDP sensor, open the Device window and select Profiler Settings.

You configure Profiler options to enable Profiler features, set network addresses and applications subject to profiling, and set alerts.

Setting Up the Profiler

Using the Profiler involves the following steps:

- Collecting specific information about your internal network
Starting the Profiler to enable your device to begin collecting data
Customizing Profiler preferences

You configure your device to collect specific information and compile it into the Profiler database.

Configuring the Profiler

You can configure the Profiler using the Profiler settings available on the device settings in the Device Manager. Using the Device Manager, double-click to access a device managed in NSM, and click Profiler Settings.

The Profile Configuration dialog box appears with the General tab selected. Once you select the device for profiling, you can configure the options for the device to collect data from your internal network.

The following topics describe the steps to configure Profiler options:

- Specifying General Options on page 14
- Specifying Tracked Hosts on page 16
- Specifying Context Targets on page 17
- Specifying Alert Options on page 18

Specifying General Options

In this tab, indicate whether you want to enable Application Profiling and Probe and Attempt and whether Non-tracked IP Profiles will be included in the profiling. Also indicate the size of the Profiler database and whether to enable OS fingerprinting.

You configure Profiler general options to enable Profiler features.

OS fingerprinting passively detects the operating system of an end-host by analyzing TCP handshake packets. To ensure that this works, you need to verify that OS fingerprinting is first enabled on the profiled device. After you have configured the Profiler with the tracked hosts and contexts, you must update the device.

OS fingerprinting works only for packets that contain a full-fledged TCP connection, that is the TCP connection should have a SYN, SYN/ACK, and a FIN connection. OS fingerprinting only works for operating systems that are supported on the device. A list of the supported operating systems is available on the device in a file called fingerprints.set at the following location:

/usr/idp/device/cfg/fingerprints.set

Configuring Network Objects

The first part of configuring the Profiler is to inform the device which network objects you want the device to profile. When you start the Profiler, the device begins collecting data from the selected hosts.
To specify Profiler general options:
1. From Device Manager, double-click a device and then click Profiler Settings.
2. Click the General tab.
3. Configure Profiler general options using Table 6 on page 15.
4. Click Apply.

Table 6: Profiler Settings: General Tab

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Profiling</td>
<td>Enables the Profiler.</td>
</tr>
<tr>
<td>Enable Application Profiling</td>
<td>Enables the Profiler to collect and track application data. This setting can</td>
</tr>
<tr>
<td></td>
<td>be started when you disable it in the profiler setting.</td>
</tr>
<tr>
<td>Enable Application Volume Tracking</td>
<td>Enables the Profiler to perform application volume tracking.</td>
</tr>
<tr>
<td>Include Probe and Attempt</td>
<td>Enables the Profiler to collect and track specific probes and attempts.</td>
</tr>
<tr>
<td>Include Non-tracked IP Profiles</td>
<td>Enables the Profiler to collect and track data from external hosts.</td>
</tr>
<tr>
<td>db limit (in MB)</td>
<td>Specifies maximum database size for the Profiler on each device. By default,</td>
</tr>
<tr>
<td></td>
<td>the maximum database size is set to 3GB.</td>
</tr>
<tr>
<td>Enable OS fingerprinting</td>
<td>Enables the Profiler to perform passive OS fingerprinting to determine the</td>
</tr>
<tr>
<td></td>
<td>operating system of an end host.</td>
</tr>
<tr>
<td></td>
<td>OS fingerprinting detects the operating system of an end host by analyzing</td>
</tr>
<tr>
<td></td>
<td>TCP handshake packets.</td>
</tr>
<tr>
<td></td>
<td>The OS fingerprinting process depends on an established TCP connection (one</td>
</tr>
<tr>
<td></td>
<td>that has a SYN and a SYN/ACK).</td>
</tr>
<tr>
<td></td>
<td>The OS fingerprinting process is capable of detecting the operating systems</td>
</tr>
<tr>
<td></td>
<td>listed in /usr/idp/device/cfg/fingerprints.set.</td>
</tr>
<tr>
<td>Refresh Interval(in secs)</td>
<td>Specifies the time interval (in seconds) that the Profiler refreshes OS</td>
</tr>
<tr>
<td></td>
<td>fingerprinting. By default, the Profiler refreshes OS fingerprinting data</td>
</tr>
<tr>
<td></td>
<td>every 3600 seconds (60 minutes).</td>
</tr>
</tbody>
</table>

NOTE: If you change Profiler settings, you must push a configuration update to the device before the new settings take effect. From the Device Manager, right-click the device, select Update Device, select the Restart IDP Profiler After Device Update checkbox, and click OK.
Specifying Tracked Hosts

Select the known hosts you want to track in the Tracked Hosts tab. Select Object Manager > Address Objects to add entries to the hosts list.

In the Tracked Hosts tab, select the Network Objects that represent your internal hosts. The device collects detailed information about traffic that passes between internal hosts, and then groups traffic that does not match an internal host in a special IP: 73.78.69.84. Communication between an internal host and an external host is recorded only once. For example, the device records internal host A communicating to www.yahoo.com and www.cnn.com as one entry in the Profiler database. You can select unlimited internal network objects. You can also use the Exclude List tab to select the Network Objects that represent internal hosts that you do not want to include in IDP profiling. You might want to exclude a host from the Profiler if you select a group of network objects in the Tracked Host tab. Also, you might want to exclude specific members of that group.

You configure Profiler tracked host and excluded host settings to determine the network segments where the Profiler gathers data.

To configure the tracked host and exclude lists:
1. From Device Manager, double-click a device and then click Profiler Settings.
2. Click the Tracked Hosts tab.
3. Click the + icon and then select Add Host > Add Network or Add Group. A dialog box appears where you create your tracked hosts list.
4. Configure Profiler tracked host settings using Table 7 on page 16.

Table 7: Profiler Tracked Hosts/Exclude List Dialog Boxes

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add Host</td>
<td>Name—Enter the name of the host.</td>
</tr>
<tr>
<td></td>
<td>Color—Select any color from the drop-down list.</td>
</tr>
<tr>
<td></td>
<td>Comment—Enter any additional comments.</td>
</tr>
<tr>
<td></td>
<td>IP/IP Address—Enter the IP address when you select IP.</td>
</tr>
<tr>
<td></td>
<td>Domain/Domain name—Enter the domain name when you select domain name.</td>
</tr>
<tr>
<td></td>
<td>Resolve—Resolve the domain name with the IP and vice versa.</td>
</tr>
</tbody>
</table>
Table 7: Profiler Tracked Hosts/Exclude List Dialog Boxes (continued)

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add Network</td>
<td>Name—Enter the name of the host.</td>
</tr>
<tr>
<td></td>
<td>IP Address—Enter the IP address of the network.</td>
</tr>
<tr>
<td></td>
<td>Use Wildcard Mask—Enable this feature if you want to use wildcard mask.</td>
</tr>
<tr>
<td></td>
<td>Netmask—Enter the netmask for the IP.</td>
</tr>
<tr>
<td></td>
<td>Color—Select any color from the drop-down list.</td>
</tr>
<tr>
<td></td>
<td>Comment—Enter any additional comments.</td>
</tr>
<tr>
<td>Add Group</td>
<td>Name—Enter the name of the group.</td>
</tr>
<tr>
<td></td>
<td>Color—Select any color from the drop-down list.</td>
</tr>
<tr>
<td></td>
<td>Comment—Enter any additional comments.</td>
</tr>
<tr>
<td></td>
<td>Member List—Add or remove the members from the non-members list.</td>
</tr>
</tbody>
</table>

5. Click the Exclude List tab.
6. Click the + icon and then select Add Host > Add Network or Add Group. A dialog box appears where you create your exclude list.

Table 7 on page 16 describes these dialog box settings.
7. Configure Profiler settings using Table 7 on page 16.
8. Click Apply.

**NOTE:** If you change Profiler settings, you must push a configuration update to the device before the new settings take effect. From the Device Manager, right-click the device, select Update Device, select the Restart IDP Profiler After Device Update check box, and click OK.

**Specifying Context Targets**

Select the contexts you want to profile in the Context Targets tab. Next, determine which contexts you want the device to record. In the Contexts to Profile tab, the context list includes only the contexts that can clearly identify a host, a user, and/or an application. When you start the Profiler, the device begins collecting data on traffic that matches the selected contexts. For example, To track FTP logins, usernames, and commands, select the FTP contexts in the Contexts to Profile tab. After the Profiler is started, the device begins collecting information about FTP logins, usernames, and commands, enabling you to quickly identify the users using FTP on your network and the actions they perform over that protocol.
When you first configure the Profiler, select all contexts. This enables the device to collect data about every context on your network, giving you a complete view of your network traffic. Later, when you have analyzed your traffic, you can eliminate contexts that you know will not be used on your network.

Select **Profile Context** to include context information. If you clear **Profile Context**, IDP profile data only includes high-level traffic data such as source, destination, and service. If you want Profiler information to include context values and network probes (for example, port scans), also configure the Profiler to include probes and attempts.

You configure Profiler context settings to determine whether Profiler logs include not only host and application data but also data pulled from application contexts. For example, if you specify context targets for FTP usernames, the Profiler logs will include the username specified for the FTP connection in addition to the hostname and service (FTP).

To specify Profiler context targets:
1. From Device Manager, double-click a device and then click **Profiler Settings**.
2. Click the **Contexts To Profile** tab.
3. Browse and select from the predefined list of contexts.
4. Click **Apply**.

**NOTE:** If you change Profiler settings, you must push a configuration update to the device before the new settings take effect. From the Device Manager, right-click the device, select **Update Device**, check **Restart IDP Profiler After Device Update**, and click **OK**.

---

## Specifying Alert Options

Specify which Profiler events you want to generate alerts for in the Alert Options tab. Use this tab to configure the Profiler to indicate the appearance of a new host, protocol, or port on your internal network. When you select **New Host Detected**, **New Protocol Detected**, or **New Port Detected**, the device generates a specific log record, such as PROFILER_NEW_HOST, in the Profiler Logs section of the Log Viewer when the device discovers a new host, protocol, or port.

If you are configuring the Profiler for the first time, do not enable the new host, protocol, or port alerts. As the Profiler runs, the device views all network components as new, which can generate unnecessary log records. After the Profiler has learned about your network and has established a baseline of network activity, you should reconfigure the device to record new hosts, protocols, or ports discovered on your internal network. For details, see the Network and Security Manager Administration Guide.

Select the **Database Limit Exceeded** alert to indicate when you have reached the maximum limit of the database size. You can configure the maximum limit of the Profiler database using the dbLimit parameter in the General tab of the Profiler Configuration dialog box. The default is 500 MB; the minimum-maximum range is
0 to 500 MB. After a device reaches this limit, it begins purging the database. For example, a network host performs the normal connections required for Internet connectivity (SMTP, POP3, HTTP, and so on). If the host is infected by a worm, it begins making outbound connections on an arbitrary port. The device logs the unique event and generates PROFILER_NEWPROTO and PROFILER_NEWPORT log records. The system immediately e-mails these log records to the security administrator, who can investigate the worm and take action to contain it.

Repeat the configuration process for each device in your network. When you have configured all devices on your network, you are ready to start the Profiler.

You configure Profiler alert options to determine whether you receive alerts when Profiler detects new hosts, protocols, or ports in use.

If you are configuring the Profiler for the first time, do not enable the new host, protocol, or port alerts. As the Profiler runs, the device views all network components as new, which can generate unnecessary log records. After the Profiler has learned about your network and has established a baseline of network activity, you should reconfigure the device to record new hosts, protocols, or ports discovered on your internal network.

To specify Profiler alert options:
1. From Device Manager, double-click a device and then click Profiler Settings.
2. Click the Alert tab.
3. Configure alert settings using Table 8 on page 19.
4. Click Apply.
5. Click OK.

### Table 8: Profiler Alert Tab

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>New Host Detected</td>
<td>Sends an alert when Profiler detects a new host.</td>
</tr>
<tr>
<td>New Protocol Detected</td>
<td>Sends an alert when Profiler detects a new protocol. New Protocol detection alerts are used only for Layer 3 protocols.</td>
</tr>
<tr>
<td>New Port Detected</td>
<td>Sends an alert when Profiler detects a new port.</td>
</tr>
<tr>
<td>Database Limit Exceeded</td>
<td>Sends an alert to indicate the maximum database size has been reached. After a device reaches this limit, it begins purging the database.</td>
</tr>
</tbody>
</table>

**NOTE:** If you change Profiler settings, you must push a configuration update to the device before the new settings take effect. From the Device Manager, right-click the device, select Update Device, select the Restart IDP Profiler After Device Update checkbox, and click OK.
Viewing Profiler Logs (NSM Procedure)

The Profiler Viewer contains multiple tabs with different views of Profiler data. The following topics describe these views:

- Application Profiler on page 20
- Protocol Profiler on page 22
- Network Profiler on page 23
- Violation Viewer on page 24

Application Profiler

The Application Profiler tab displays Application Volume Tracking (AVT) data. The Application Profiler tab is a table of information such as the NSM Log Viewer which enables you to view and analyze dynamic application (Layer-7) traffic within a specific context.

The Application Profiler view is divided into two sections:

- In the left pane, the Application Profiler tab displays a hierarchical tree of application categories. Applications are grouped by common functionality. For example, Peer-to-Peer applications include Chat and File Sharing applications. Under Chat, you can display Yahoo messenger, MSN, and AIM; under File Sharing, you can display Kazaa, Bittorrent, and Gnutella.

- The left pane also displays aggregate statistics for volume (bytes) and packet count for the application category, application group, or application you select in the tree.

- In the right pane, the Application Profiler tab displays tables of session logs related to the application category or application you select in the left pane.

Table 9 on page 20 describes Application Profiler session table.

**Table 9: Application Profiler Session**

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Src IP</td>
<td>Source IP address of the traffic profiled.</td>
</tr>
<tr>
<td>Dst IP</td>
<td>Destination IP address of the traffic profiled.</td>
</tr>
<tr>
<td>User</td>
<td>The user associated with the traffic profiled.</td>
</tr>
</tbody>
</table>
Table 9: Application Profiler Session  (continued)

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Role</td>
<td>The role group to which the user that is associated with the traffic profiled belongs.</td>
</tr>
<tr>
<td>Context</td>
<td>All contexts of traffic that the devices selected in the Device table recorded.</td>
</tr>
<tr>
<td>Value</td>
<td>When you select a context, the values that your devices recorded for a selected context.</td>
</tr>
<tr>
<td>Src MAC</td>
<td>Source MAC addresses of traffic profiled.</td>
</tr>
<tr>
<td>Dst MAC</td>
<td>Destination MAC addresses of traffic profiled.</td>
</tr>
<tr>
<td>Src OUI</td>
<td>Source OUIs of traffic profiled.</td>
</tr>
<tr>
<td>Dst OUI</td>
<td>Destination OUIs of traffic profiled.</td>
</tr>
<tr>
<td>Src OS Name</td>
<td>Operating-system version running on the source IP of the traffic profiled.</td>
</tr>
<tr>
<td>Dst OS Name</td>
<td>Operating-system version running on the destination IP of the traffic profiled.</td>
</tr>
<tr>
<td>Hits</td>
<td>Number of occurrences that match the traffic profiled.</td>
</tr>
<tr>
<td>First Time</td>
<td>Timestamp for the first time the device logged the event (within the specified time interval).</td>
</tr>
<tr>
<td>Last Time</td>
<td>Timestamp for the last time the device logged the event (within the specified time interval).</td>
</tr>
<tr>
<td>Domain</td>
<td>Domain in which the device is managed in NSM.</td>
</tr>
<tr>
<td>Device</td>
<td>Device that profiled the data displayed.</td>
</tr>
</tbody>
</table>

NOTE: The Organizationally Unique Identifier (OUI) value is a mapping of the first three bytes of the MAC address and the organization that owns the block of MACs. You can obtain a list of OUIs at [http://standards.ieee.org/regauth/oui/oui.txt](http://standards.ieee.org/regauth/oui/oui.txt).

By default, the Application Profiler view contains only the data collected during the configured time interval.

To display the Application Profiler view:
2. Click the Application Profiler tab.

TIP: You can jump from the Application Profiler tab to the APE rulebase editor by right-clicking an application in the left pane and selecting a policy editor option. For information about using NSM features to sort, filter, and drill down on records, see the NSM online help.
Protocol Profiler

The Protocol Profiler tab displays information about applications that are running on your network.

Table 10 on page 22 describes the protocol profiler data.

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Src IP</td>
<td>Source IP address of the session.</td>
</tr>
<tr>
<td><strong>NOTE:</strong></td>
<td>Profiler tracks all traffic through the IDP appliance, including traffic for hosts not in your tracked hosts list. It records a value of 73.78.69.84 for the IP address for hosts not defined in the Tracked Hosts tab, such as external hosts you would not know and therefore could not configure.</td>
</tr>
<tr>
<td>Dst IP</td>
<td>Destination IP address.</td>
</tr>
<tr>
<td><strong>NOTE:</strong></td>
<td>Communication between an internal host and an external host is recorded only once. For example, the device records internal host A communicating to <a href="http://ca.yahoo.com">http://ca.yahoo.com</a> and <a href="http://edition.cnn.com">http://edition.cnn.com</a> as one entry in the Profiler DB.</td>
</tr>
<tr>
<td>User</td>
<td>The user associated with the session.</td>
</tr>
<tr>
<td>Role</td>
<td>The role to which the user belongs.</td>
</tr>
<tr>
<td>Context</td>
<td>Matching contexts.</td>
</tr>
<tr>
<td>Value</td>
<td>Value retrieved from matching context.</td>
</tr>
<tr>
<td>Src MAC</td>
<td>Source MAC addresses.</td>
</tr>
<tr>
<td>Dst MAC</td>
<td>Destination MAC addresses.</td>
</tr>
<tr>
<td>Src OUI</td>
<td>Source OUI.</td>
</tr>
<tr>
<td><strong>NOTE:</strong></td>
<td>The Organizationally Unique Identifier (OUI) value is a mapping of the first three bytes of the MAC address and the organization that owns the block of MACs. You can obtain a list of OUIs at <a href="http://standards.ieee.org/regauth/oui/oui.txt">http://standards.ieee.org/regauth/oui/oui.txt</a>.</td>
</tr>
<tr>
<td>Dst OUI</td>
<td>Destination OUI.</td>
</tr>
<tr>
<td>Src OS Name</td>
<td>Operating-system version running on the source IP.</td>
</tr>
<tr>
<td>Dst OS Name</td>
<td>Operating-system version running on the destination IP.</td>
</tr>
<tr>
<td>Hits</td>
<td>Number of occurrences that match the session.</td>
</tr>
<tr>
<td>First Time</td>
<td>Timestamp for the first time the device logged the event (within the specified time interval).</td>
</tr>
<tr>
<td>Last Time</td>
<td>Timestamp for the last time the device logged the event (within the specified time interval).</td>
</tr>
<tr>
<td>Domain</td>
<td>NSM domain.</td>
</tr>
</tbody>
</table>
Table 10: Protocol Profiler Data (continued)

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device</td>
<td>Device through which the session was forwarded.</td>
</tr>
</tbody>
</table>

By default, the Protocol Profiler tab contains only the data collected during the configured time interval.

To display the Protocol Profiler tab:
1. In the NSM navigation tree, select Investigate > Security Monitor > Profiler.
2. Click the Protocol Profiler tab.

TIP: For information about using NSM features to sort, filter, and drill down in records, see the NSM online Help.

Network Profiler

The Network Profiler view is a table of information such as the NSM Log Viewer which enables you to view and analyze data related to static traffic (Layer-3, Layer-4, and RPC protocols, ports, and program numbers) within the context of data corresponding to peer, host, and operating system.

Table 11 on page 23 describes Network Profiler data.

Table 11: Network Profiler Data

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Src IP</td>
<td>Source IP address of the traffic profiled.</td>
</tr>
<tr>
<td>Dst IP</td>
<td>Destination IP address of the traffic profiled.</td>
</tr>
<tr>
<td>User</td>
<td>The user associated with the traffic profiled.</td>
</tr>
<tr>
<td>Role</td>
<td>The role group to which the user that is associated with the traffic profiled belongs.</td>
</tr>
<tr>
<td>Service</td>
<td>All services of traffic profiled.</td>
</tr>
<tr>
<td>Access Type</td>
<td>Type of the traffic profiled:</td>
</tr>
<tr>
<td>-</td>
<td>Access indicates a successful connection, during which the device recorded valid requests and responses from the server to a client.</td>
</tr>
<tr>
<td>-</td>
<td>Attempt indicates a request that did not receive a reply. The device recorded a packet from a client to a server, but never saw a reply.</td>
</tr>
<tr>
<td>-</td>
<td>Probe indicates a request that does not expect a reply. For non-TCP sessions, the device recorded an ICMP error; for TCP sessions, the device recorded a SYN packet from the client followed by a RST from the server.</td>
</tr>
</tbody>
</table>
Table 11: Network Profiler Data (continued)

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Src MAC</td>
<td>Source MAC addresses of traffic profiled.</td>
</tr>
<tr>
<td>Dst MAC</td>
<td>Destination MAC addresses of traffic profiled.</td>
</tr>
<tr>
<td>Src OUI</td>
<td>Source OUIs of traffic profiled.</td>
</tr>
<tr>
<td>Dst OUI</td>
<td>Destination OUIs of traffic profiled.</td>
</tr>
<tr>
<td>Src OS Name</td>
<td>Operating-system version running on the source IP of the traffic profiled.</td>
</tr>
<tr>
<td>Dst OS Name</td>
<td>Operating-system version running on the destination IP of the traffic profiled.</td>
</tr>
<tr>
<td>Hits</td>
<td>Number of occurrences that match the traffic profiled.</td>
</tr>
<tr>
<td>First Time</td>
<td>Timestamp for the first time the device logged the event (within the specified time interval).</td>
</tr>
<tr>
<td>Last Time</td>
<td>Timestamp for the last time the device logged the event (within the specified time interval).</td>
</tr>
<tr>
<td>Domain</td>
<td>Domain in which the device is managed in NSM.</td>
</tr>
<tr>
<td>Device</td>
<td>Device that profiled the data displayed.</td>
</tr>
</tbody>
</table>

To display the Network Profiler view:
2. Click the Network Profiler tab.

**TIP:** For information about using NSM features to sort, filter, and drill down on records, see the NSM online Help.

**Violation Viewer**

The Violation Viewer is a filtered view of the Network Profiler view. In the Violation Viewer, you configure permitted objects. Permitted objects are filtered from the display, allowing you to focus on unpermitted traffic.

To configure permitted objects:
2. Click the Violation Viewer tab.
3. Click on the + icon that appears on the top of the right-hand window to display the New Permitted Object dialog box.
4. Type a name for the permitted object.

5. Within the New Permitted Object dialog box, click the + icon to add a rule to match source, destination, and services values for the permitted object.

6. To change the source, destination, or service value from Any, right-click the value and select Add Source, Add Destination, or Add Service.

7. Use the selection controls to select the desired address objects or service objects and click OK.

8. Click OK to save the permitted object.

   The object appears in the filters windows within the Violation Viewer tab.

9. Select the object and click Apply to hide all matching objects from the Violation Viewer.

TIP: For information about using additional NSM features to sort, filter, and drill down on records, see the NSM online Help.

Related Topics
- Configuring Profiler Options (NSM Procedure) on page 13
- Displaying Profiler Database Information (NSM Procedure) on page 27
- Querying the Profiler Database (NSM Procedure) on page 28

Modifying Profiler Settings (NSM Procedure)

You can use the Profiler Settings dialog box to modify Profiler database settings and default settings for application volume tracking reports.

To modify profiler database and application volume tracking settings:

1. From the NSM main menu, select Tools > Preferences. The New Preferences dialog box is displayed.

2. Click Profiler Settings.

3. Modify settings as described in Table 12 on page 25.

4. Click OK.

Table 12: Profiler Settings

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Purge profiler database if size exceeds (in MB)</td>
<td>Removes the profiler database for the selected size in MB. The default value is 1000 MB.</td>
</tr>
<tr>
<td>Max profiler database size after purging (in MB)</td>
<td>Specifies the maximum size of the purged profiler database. The default value is 750 MB.</td>
</tr>
<tr>
<td>Profiler query timeout (in seconds)</td>
<td>Specifies the timeout entry for a profiler query. The default value is 120 seconds.</td>
</tr>
</tbody>
</table>
Table 12: Profiler Settings (continued)

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hour of day to perform db optimization</td>
<td>Specifies the time to perform the database optimization. The default value is 00:00 GMT.</td>
</tr>
<tr>
<td>(local time)</td>
<td></td>
</tr>
<tr>
<td>Number of sessions to display per application</td>
<td>Determines the number of sessions displayed in the Application Profiler application volume tracking session tables. The default value is 10 sessions. You can specify from 5 to 10,000 sessions.</td>
</tr>
<tr>
<td>Hours of session data to display from present time</td>
<td>Determines the hours of application volume tracking data displayed in the Application Profiler tab session tables. The default value is 1 hour. You can specify from 1 to 24 hours.</td>
</tr>
<tr>
<td></td>
<td>This setting is also a data retention policy. By default, data older than 1 hour is deleted. If your change to 12 hours, data older than 12 hours is deleted.</td>
</tr>
</tbody>
</table>

**Related Topics**
- Configuring Profiler Options (NSM Procedure) on page 13
- Querying the Profiler Database (NSM Procedure) on page 28

**Configuring Profiler Database Preferences (NSM Procedure)**

ScreenOS 6.2 supports application volume tracking (AVT), a feature that enables NSM to track network bandwidth usage on a per-application basis. The security device sends the NSM server periodic update messages containing details about port activity. NSM listens and processes these periodic update messages and maintains a cumulative count for each port. NSM displays this count on the console. NSM provides reports about application volume tracking. The AVT feature has the following limitations:

- Periodic updates maintained per port for each active session can slightly affect CPU performance.
- Accuracy of AVT data is dependent on communication with the NSM server. NSM, however, lacks a mechanism to ensure that periodic updates sent by AVT from ScreenOS are received, which may result in a lag between traffic instances and reporting of those instances. NSM maintains a cumulative count for all traffic on each port regardless of session, node, or protocol. The count displayed is a total across all sessions. Because updates are periodic, the currently displayed number of bytes in NSM may be inaccurate until the next update.
- You must use NSM to view the enhanced logging provided by AVT.

For more details on AVT, see the *Network and Security Manager Administration Guide*.

Use the Profiler Settings under the Tools menu to configure the Profiler preferences mentioned in Table 12 on page 25. You can use the Profiler Settings dialog box to modify Profiler database settings and default settings for application volume tracking reports.

Data discovered by Profiler is stored in a database located on the NSM GUI server.
To modify profiler database preferences and application volume tracking settings:

1. From the NSM main menu, select **Tools > Preferences**. The New Preferences dialog box is displayed.
2. Click **Profiler Settings**.
3. Modify settings as described in Table 12 on page 25.
4. Click **OK**.

### Table 13: Profiler Database Preferences

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Purge profiler database if size exceeds (in MB)</td>
<td>NSM purges the profiler database size if it exceeds 4 GB (4000 MB) by default.</td>
</tr>
<tr>
<td>Max profiler database size after purging (in MB)</td>
<td>If the database size exceeds its maximum limit, NSM purges the Profiler database size until the size reaches 3 GB (3000 MB) by default.</td>
</tr>
<tr>
<td>Profiler query timeout (in seconds)</td>
<td>Specifies the timeout entry for a profiler query. The default value is 120 seconds.</td>
</tr>
<tr>
<td>Hour of day to perform db optimization (local time)</td>
<td>Specifies the time to perform the database optimization. The default value is 00:00 GMT.</td>
</tr>
<tr>
<td>Number of sessions to display per application</td>
<td>Determines the number of application volume tracking sessions displayed in the Application Profiler tab session tables. The default value is 10 sessions. You can specify from 5 to 10,000 sessions.</td>
</tr>
<tr>
<td>Hours of session data to display from present time</td>
<td>Determines the hours of application volume tracking data displayed in the Application Profiler tab session tables. The default value is 1 hour. You can specify from 1 to 24 hours. This setting is also a data retention policy. By default, data older than 1 hour is deleted. If your change to 12 hours, data older than 12 hours is deleted.</td>
</tr>
</tbody>
</table>

### Related Topics
- Configuring Profiler Options (NSM Procedure) on page 13
- Displaying Profiler Database Information (NSM Procedure) on page 27
- Viewing Profiler Logs (NSM Procedure) on page 20

### Displaying Profiler Database Information (NSM Procedure)

**Purpose**
Data discovered by Profiler is stored in a database located on the NSM GUI server. Use the steps in this procedure to display information about the Profiler database.

**Action**
To display Profiler database information:

1. In the NSM Navigation tree select **Investigate > Security Monitor > Profiler**.
2. Click the **Show DB Information** icon in the upper right corner to view specific details about the Profiler database, including the database size.
**Querying the Profiler Database (NSM Procedure)**

**Purpose**
Data discovered by Profiler is stored in a database located on the NSM GUI server. Use the steps in this procedure to query the Profiler database.

**Action**
To query records in the database:

1. Log into the NSM GUI server as the Postgres SQL user. By default, the Postgres SQL user is `netscreen`.
2. Navigate to the directory where the Profiler DB is located: `/usr/local/nsmpsql/bin`.
3. Run any Postgres SQL command. For example, you can type the following command:
   
   ```
   ./psql -d profilerDb
   ```

**Related Topics**
- Configuring Profiler Options (NSM Procedure) on page 13
- Configuring Profiler Database Preferences (NSM Procedure) on page 26
- Querying the Profiler Database (NSM Procedure) on page 28

---

**Purging the Profiler Database (NSM Procedure)**

Data discovered by Profiler is stored in a database located on the NSM GUI server. When the database reaches a maximum size (4 GB by default), it begins purging records (oldest first) automatically. The Profiler stops purging records when it reaches a certain set minimum size (3 GB by default).

Use the steps in this procedure to purge the Profiler database, if needed.

To change automatic purge settings, from the NSM main menu select **Tools > Preferences** and modify the Profiler database settings.

To manually purge the database:

1. In the NSM Navigation tree, select **Investigate > Security Monitor > Profiler**.
2. Click the **Clear All DB** icon in the upper right corner.

**Related Topics**
- Configuring Profiler Options (NSM Procedure) on page 13
- Configuring Profiler Database Preferences (NSM Procedure) on page 26
- Displaying Profiler Database Information (NSM Procedure) on page 27
- Querying the Profiler Database (NSM Procedure) on page 28
Chapter 4
Configuring Security Policies

Intrusion Detection and Prevention Devices and Security Policies Overview

An IDP security policy defines how the IDP device handles network traffic. It allows you to enforce various attack detection and prevention techniques on traffic that traverses your network.

For a detailed explanation of security policy features and components, and for examples, see the IDP Concepts & Examples Guide.

To create an effective security policy, follow these basic steps:

1. Run the New Policy wizard to create a new security policy object. The new security policy can be based on a predefined template.

2. Use the Security Policy editor to add one or more rulebases.

A rulebase is an ordered set of rules that use a particular detection method to identify and prevent attacks.

Table 14 on page 30 describes the IDP security policy rulebases. A security policy can contain only one instance of any rulebase type.
Table 14: IDP Security Policy Rulebases

<table>
<thead>
<tr>
<th>Rulebase</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application Rulebase</td>
<td>Enables you to limit bandwidth for specified users and applications and thus helps to manage network traffic. APE rules do not use attack objects.</td>
</tr>
<tr>
<td>IDP Rulebase</td>
<td>Protects your network from attacks by using attack objects to detect known and unknown attacks. Juniper Networks provides predefined attack objects that you can use in IDP rules. You can also configure your own custom attack objects.</td>
</tr>
<tr>
<td>Exempt Rulebase</td>
<td>You configure rules in this rulebase to exclude known false positives or to exclude a specific source, destination, or source/destination pair from matching an IDP rule. If traffic matches a rule in the IDP rulebase, IDP attempts to match the traffic against the Exempt rulebase before performing the action specified.</td>
</tr>
<tr>
<td>Backdoor Rulebase</td>
<td>Protects your network from mechanisms installed on a host computer that facilitates unauthorized access to the system. Attackers who have already compromised a system typically install backdoors (such as Trojans) to make future attacks easier. When attackers send and retrieve information to and from the backdoor program (as when typing commands), they generate interactive traffic that IDP can detect.</td>
</tr>
<tr>
<td>SYN Protector Rulebase</td>
<td>Protects your network from SYN-floods by ensuring that the three-way handshake is performed successfully for specified TCP traffic. If you know that your network is vulnerable to a SYN-flood, use the SYN-Protector rulebase to prevent it.</td>
</tr>
<tr>
<td>Traffic Anomalies Rulebase</td>
<td>Protects your network from attacks by using traffic flow analysis to identify attacks that occur over multiple connections and sessions (such as scans).</td>
</tr>
<tr>
<td>Network Honeypot Rulebase</td>
<td>Protects your network by impersonating open ports on existing servers on your network, alerting you to attackers performing port scans and other information-gathering activities.</td>
</tr>
</tbody>
</table>

3. Within rulebases, configure rules.

*Rules* are instructions that provide context to detection methods. Rules specify:

- A source/destination/service match condition that determines which traffic to inspect
- Attack objects that determine what to look for (IDP rulebase and Exempt rulebase)
- Actions that determine what to do when an attack is detected
- Notification options, including logs, alerts, and packet captures

Each rulebase can contain up to 40,000 rules.

4. Fine-tune your security policy as you learn more about your network and security requirements and IDP capabilities.

**Related Topics**

- Configuring Predefined Security Policies (NSM Procedure) on page 31
- Creating a New Security Policy (NSM Procedure) on page 32
Configuring Predefined Security Policies (NSM Procedure)

The highly respected Juniper Networks Security Center team (J-Security Center) provides the default IDP security policy—named Recommended. We advise that you use this policy to protect your network from the likeliest and most dangerous attacks.

Table 15 on page 31 summarizes the properties of the Recommended security policy.

Table 15: Recommended Security Policy Definition

<table>
<thead>
<tr>
<th>Property</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rulebase</td>
<td>IDP Rulebase</td>
</tr>
<tr>
<td>Rules</td>
<td>9 rules, distinguished by attack object</td>
</tr>
<tr>
<td>Traffic source</td>
<td>Any</td>
</tr>
<tr>
<td>Service</td>
<td>Default, meaning the matching property is based on the service bindings of the attack object specified by the rule</td>
</tr>
<tr>
<td>Destination</td>
<td>Any</td>
</tr>
<tr>
<td>Attacks</td>
<td>Recommended IP, Recommended TCP, Recommended ICMP, Recommended HTTP, Recommended SMTP, Recommended DNS, Recommended FTP, Recommended POP3, Recommended IMAP, Recommended Trojan, Recommended Virus, Recommended Worm</td>
</tr>
<tr>
<td>Action</td>
<td>Recommended, meaning the action is specified by the attack object</td>
</tr>
<tr>
<td>Notification</td>
<td>Logging</td>
</tr>
</tbody>
</table>

If you prefer, you can copy this security policy and use it as a template for a custom security policy tailored for your network.

Table 16 on page 31 describes other IDP security policy templates.

Table 16: IDP Security Policy Templates

<table>
<thead>
<tr>
<th>Template</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>all_with_logging</td>
<td>Includes all attack objects and enables packet logging for all rules.</td>
</tr>
<tr>
<td>all_without_logging</td>
<td>Includes all attack objects but does not enable packet logging.</td>
</tr>
<tr>
<td>dmz_services</td>
<td>Protects a typical DMZ environment.</td>
</tr>
<tr>
<td>dns_server</td>
<td>Protects DNS services.</td>
</tr>
</tbody>
</table>
Table 16: IDP Security Policy Templates (continued)

<table>
<thead>
<tr>
<th>Template</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>file_server</td>
<td>Protects file sharing services, such as SMB, NFS, FTP, and others.</td>
</tr>
<tr>
<td>getting_started</td>
<td>Contains very open rules. Useful in controlled lab environments, but should not be deployed on heavy traffic live networks.</td>
</tr>
<tr>
<td>idp_default</td>
<td>Contains a good blend of security and performance.</td>
</tr>
<tr>
<td>web_server</td>
<td>Protects HTTP servers from remote attacks.</td>
</tr>
</tbody>
</table>

If you use these templates, we advise you customize them for your deployment. At a minimum, you should change the destination IP setting from Any to the IP addresses for specific servers you want to protect. For more information, see the IDP Concepts & Examples guide.

Related Topics
- Intrusion Detection and Prevention Devices and Security Policies Overview on page 29
- Creating a New Security Policy (NSM Procedure) on page 32
- Assigning a Security Policy in an Intrusion Detection and Prevention Device (NSM Procedure) on page 117
- Modifying IDP Rulebase Rules (NSM Procedure) on page 34

Creating a New Security Policy (NSM Procedure)

You use the security policy wizard to create a new security policy. The security policies you create with the wizard must have a new name but can be based on existing policies or templates.

To create a new security policy:
1. In the NSM navigation tree, select Policy Manager > Security Policies.
2. Select File > New Policy to display the New Policy wizard.
3. On the first page, complete the settings and then click Next. Table 17 on page 32 describes page one fields.

Table 17: New Policy Wizard: Page One

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>A string to identify the policy.</td>
</tr>
<tr>
<td>Comments</td>
<td>Text to further identify the policy. In the security policy list, you can sort on comments.</td>
</tr>
</tbody>
</table>

4. On the second page, complete the settings and then click Next. Table 18 on page 33 describes page two settings.
Table 18: New Policy Wizard: Page Two

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create new Policy for</td>
<td>Select this option to create a new security policy.</td>
</tr>
<tr>
<td></td>
<td>If you select this option, the wizard displays the following set of device types:</td>
</tr>
<tr>
<td></td>
<td>- Firewall/VPN</td>
</tr>
<tr>
<td></td>
<td>- Firewall/VPN with IDP</td>
</tr>
<tr>
<td></td>
<td>- Standalone IDP</td>
</tr>
<tr>
<td></td>
<td>Select Standalone IDP</td>
</tr>
</tbody>
</table>

| Use Existing Policy          | Use this option to assign an existing policy to one or more IDP devices.    |
|                              | If you select this option, the wizard displays a drop-down list of existing policies. |
|                              | Select a policy from the list.                                             |
|                              | **NOTE:** This procedure involves creating a new policy. For this procedure, do not select Use Existing Policy. |

5. On the next pages, complete pre-configuration options. Table 19 on page 33 describes your choices. Click **Next** to advance through the pages.

Table 19: New Policy Wizard: Pre-configuration Options

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use Predefined Policy Template</td>
<td>Select this option to create a new security policy based on a predefined template.</td>
</tr>
<tr>
<td></td>
<td>If you select this option, the wizard displays a drop-down list of predefined templates.</td>
</tr>
<tr>
<td></td>
<td>Select one and click <strong>Next</strong>.</td>
</tr>
</tbody>
</table>

| Configure IDP Policy            | Select this option and complete the rule properties on the next page to generate a policy with the following features: |
|                                  | - IDP rulebase                                                              |
|                                  | - Multiple rules matching any source, any destination, and default services |
|                                  | - Multiple rules are distinguished by the attack object severity group, action, and notification option you configure in the next wizard page. |

| Empty Policy                    | Select this option to create an empty policy that you can later modify.     |

6. On the next to last page, select IDP devices for which you are designing this policy. Then click **Next**.

7. Click **Finish** to save the policy.
The new policy appears in the security policy list. After you have created a security policy, you can add rules to the new policy. Rules include IPv6, VPN, and also VPN link. For more information, see the IDP Concepts & Examples guide

Related Topics
- Intrusion Detection and Prevention Devices and Security Policies Overview on page 29
- Configuring Predefined Security Policies (NSM Procedure) on page 31
- Modifying IDP Rulebase Rules (NSM Procedure) on page 34
- Assigning a Security Policy in an Intrusion Detection and Prevention Device (NSM Procedure) on page 117

Modifying IDP Rulebase Rules (NSM Procedure)

This procedure assumes you have used the New Policy wizard to create a basic policy that you can modify.

The primary IDP security policy rulebase is the IDP rulebase. The IDP rulebase enables the IDP process engine to inspect matching traffic for signs of an attack.

For background on and examples of IDP rulebase rules, see the IDP Concepts & Examples Guide.

To modify IDP rulebase rules:
1. In the NSM navigation tree, select Configure > Policy Manager > Security Policies.
2. Select the security policy you want to edit.
3. In the security policy pane, select IDP tab to display the IDP rulebase table.
4. To add, delete, copy, or reorder rules, right-click the table cell for the rule number and make your selection.
5. To modify the property of a rule, right-click the table cell for the property and make your selection. Table 20 on page 34 lists the rule properties you can modify and provides references documentation for these properties.

### Table 20: IDP Rulebase Rule Properties

<table>
<thead>
<tr>
<th>Property</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID</td>
<td>Identification number of the IDP rules that you add.</td>
</tr>
<tr>
<td>Match</td>
<td>You can select the zone from which the source sends traffic to the destination zone.</td>
</tr>
<tr>
<td>Look For</td>
<td>You can select the attacks that you want add IDP to match in the monitored traffic.</td>
</tr>
<tr>
<td>Action</td>
<td>Specifies the action you want IDP to perform against the current connection.</td>
</tr>
<tr>
<td>IP Action</td>
<td>Specifies the action you want IDP to perform against future connections that use the same IP address.</td>
</tr>
</tbody>
</table>
Table 20: IDP Rulebase Rule Properties (continued)

<table>
<thead>
<tr>
<th>Property</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Notification</td>
<td>You can choose none, or enable logging and select the logging options that are appropriate for your network.</td>
</tr>
<tr>
<td>VLAN Tag</td>
<td>Specifies the VLAN tags you want to match in applying the rule.</td>
</tr>
<tr>
<td>Severity</td>
<td>You can use the default severity settings of the selected attack objects, or you can choose a specific severity for your rule.</td>
</tr>
<tr>
<td>Install On</td>
<td>Specifies the selected source and destination zone that are available on the security device.</td>
</tr>
<tr>
<td>Optional Fields</td>
<td>Specifies the optional fields that you can configure in the rule.</td>
</tr>
<tr>
<td>Comments</td>
<td>Describes any additional comments about the rule.</td>
</tr>
</tbody>
</table>

Following are the updates that you can perform on an IDP rulebase rule:

- Specifying Rule Match Conditions on page 35
- Specifying IDP Rulebase Attack Objects on page 37
- Specifying Rule Session Action on page 38
- Specifying Rule IP Action on page 39
- Specifying Rule Notification Options on page 40
- Specifying Rule VLAN Matches on page 41
- Specifying Rule Targets on page 41
- Specifying Rule Severity on page 42
- Specifying Rule Optional Fields on page 42
- Specifying Rule Comments on page 43

Specifying Rule Match Conditions

To specify rule match conditions, right-click the table cell and select your setting.

Table 21 on page 35 describes match condition columns for IDP rulebase rules.

Table 21: IDP Rulebase Match Condition Settings

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>From zone / To zone</td>
<td>Not applicable for standalone IDP devices.</td>
</tr>
</tbody>
</table>
### Table 21: IDP Rulebase Match Condition Settings (continued)

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Source</strong></td>
<td><strong>Select Address</strong>—Display the Select Address dialog box where you can select address objects for traffic sources.</td>
</tr>
<tr>
<td></td>
<td><strong>Any</strong>—Matches any source of traffic. To guard against incoming attacks, you typically specify Any.</td>
</tr>
<tr>
<td></td>
<td><strong>Negate</strong>—Matches any except those specified.</td>
</tr>
<tr>
<td></td>
<td>To use address negation:</td>
</tr>
<tr>
<td></td>
<td>1. Add the address object.</td>
</tr>
<tr>
<td></td>
<td>2. Right-click the address object and select Negate.</td>
</tr>
<tr>
<td><strong>User Role</strong></td>
<td><strong>Select User Role</strong>—Displays the Select User Role dialog box where you can select or configure user role matches.</td>
</tr>
<tr>
<td></td>
<td>If a value for User Role matches, the Source parameter is not consulted.</td>
</tr>
<tr>
<td></td>
<td>User role-based rules are evaluated before IP source rules. If a user role matches, and if the other match criteria are met, the rule is applied and IP address-based rules are not consulted.</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> Matching based on user role depends on integration with Juniper Networks Infranet Controllers.</td>
</tr>
<tr>
<td><strong>Destination</strong></td>
<td><strong>Select Address</strong>—Display the Select Address dialog box where you can select address objects for destination servers.</td>
</tr>
<tr>
<td></td>
<td><strong>Any</strong>—Matches any destination address.</td>
</tr>
<tr>
<td></td>
<td><strong>Negate</strong>—Specifies any except those specified.</td>
</tr>
<tr>
<td></td>
<td>To use address negation:</td>
</tr>
<tr>
<td></td>
<td>1. Add the address object.</td>
</tr>
<tr>
<td></td>
<td>2. Right-click the address object and select Negate.</td>
</tr>
<tr>
<td><strong>Service</strong></td>
<td><strong>Default</strong>—Matches the service(s) specified in the rule attack object(s).</td>
</tr>
<tr>
<td></td>
<td>If you have enabled the Application Identification (AI) feature, the IDP process engine identifies services even if they are running on nonstandard ports.</td>
</tr>
<tr>
<td></td>
<td>If you have not enabled AI and specify Default, the IDP process engine assumes that standard ports are used for the service.</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> If you do not enable AI and your service uses nonstandard ports, you must create a custom service objects.</td>
</tr>
<tr>
<td></td>
<td><strong>Any</strong>—Matches any service.</td>
</tr>
<tr>
<td></td>
<td><strong>Select Service</strong>—Display the Select Service dialog box where you can select predefined or custom service objects.</td>
</tr>
</tbody>
</table>
Table 21: IDP Rulebase Match Condition Settings (continued)

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Terminate</td>
<td><strong>Enable</strong> or <strong>Disable</strong>—Marks the rule a terminal rule (or clears the mark). If a session matches a terminal rule, the IDP process engine does not load any subsequent rules. It takes action, if any, according to the terminal rule.</td>
</tr>
</tbody>
</table>

Specifying IDP Rulebase Attack Objects

To add attack objects:

1. Right-click the table cell for attacks and select **Select Attacks**.
2. In the All Attacks/Groups box, expand **Attack Groups**.
3. To add attack objects recommended by Juniper Networks Security Center (J-Security Center), expand **Recommended Attacks**, browse groups, and select groups or individual attack objects.
4. To add other predefined attack objects, expand **All Attacks**, browse groups, and select groups or individual attack objects.
5. To add attack objects that belong to custom groups, expand the node for the custom group, browse subgroups, and select groups or individual attack objects.
6. To add custom attack objects that do not belong to groups, expand **Attack List** and select from custom attack objects.
7. Click **OK**.

Table 22 on page 37 describes the attack object group hierarchy for recommended and predefined attack objects provided by J-Security Center.

Table 22: Attack Object Group Hierarchy

<table>
<thead>
<tr>
<th>Group</th>
<th>Contents</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attack Type</td>
<td>Contains two subgroups: anomaly and signature. Within each subgroup, attack objects are grouped by severity.</td>
</tr>
<tr>
<td>Category</td>
<td>Contains subgroups based on category. Within each category, attack objects are grouped by severity.</td>
</tr>
<tr>
<td>Operating System</td>
<td>Contains the following subgroups: BSD, Linux, Solaris, and Windows. Within each operating system, attack objects are grouped by services and severity.</td>
</tr>
<tr>
<td>Severity</td>
<td>Contains the following subgroups: Critical, Major, Minor, Warning, Info. Within each severity, attack objects are grouped by category.</td>
</tr>
<tr>
<td>Web Services</td>
<td>Contains subgroups based on Web services. Within services, attacked objects are grouped by severity.</td>
</tr>
<tr>
<td>Miscellaneous</td>
<td>Contains attack objects that have a significant affect on IDP performance.</td>
</tr>
</tbody>
</table>

**NOTE:** Our severity rating is not based on CVSS (Common Vulnerability Scoring System). We do include data from Bugtraq (Symantec) and CVE (Common Vulnerabilities and Exposures).
Specifying Rule Session Action

Actions are responses to sessions that match the source/destination condition and attack object pattern. Actions protect your network from attacks.

If a packet triggers multiple rule actions, the IDP device takes the most severe action. For example, if the rules dictate that a packet will receive a DiffServ marking and be dropped, and then the packet will be dropped.

To specify a rule action, right-click the table cell and select your setting.

Table 23 on page 38 describes the actions you can set for IDP rulebase rules.

Table 23: IDP Rulebase Actions

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Recommended</td>
<td>Predefined attack objects include a recommended action. The recommended action is related to severity. Table 24 on page 39 lists the recommended actions by severity.</td>
</tr>
<tr>
<td>None</td>
<td>IDP inspects for attacks but takes no action against the connection if an attack is found.</td>
</tr>
<tr>
<td>Ignore</td>
<td>IDP does not inspect for attacks and ignores the connection.</td>
</tr>
<tr>
<td>DiffServ Marking</td>
<td>IDP assigns the indicated service-differentiation value to the packet, and then passes it on normally. Set the service-differentiation value in the dialog box that appears when you select this action in the rulebase.</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> The marking has no effect in sniffer mode.</td>
</tr>
<tr>
<td>Drop Packet</td>
<td>IDP drops a matching packet before it can reach its destination but does not close the connection. Use this action to drop packets for attacks in traffic that is prone to spoofing, such as UDP traffic. Dropping a connection for such traffic could result in a DoS that prevents you from receiving traffic from a legitimate source address.</td>
</tr>
<tr>
<td>Drop Connection</td>
<td>IDP drops the connection without sending an RST packet to the sender, preventing the traffic from reaching its destination. Use this action to drop connections for traffic that is not prone to spoofing.</td>
</tr>
<tr>
<td>Close Client and Server</td>
<td>IDP closes the connection and sends an RST packet to both the client and the server. If IDP is in sniffer mode, IDP sends an RST packet to both the client and server but does not close the connection.</td>
</tr>
<tr>
<td>Close Client</td>
<td>IDP closes the connection to the client but not to the server.</td>
</tr>
<tr>
<td>Close Server</td>
<td>IDP closes the connection to the server but not to the client.</td>
</tr>
</tbody>
</table>

Table 24 on page 39 describes the logic applied to the value Recommended, a setting coded in predefined attack objects provided by Juniper Networks Security Center.
Table 24: IDP Rulebase Actions: Recommended Actions by Severity

<table>
<thead>
<tr>
<th>Severity</th>
<th>Description</th>
<th>Recommended Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Critical</td>
<td>Attacks attempt to evade an IPS, crash a machine, or gain system-level privileges.</td>
<td>Drop Packet, Drop Connection</td>
</tr>
<tr>
<td>Major</td>
<td>Attacks attempt to crash a service, perform a denial of service, install or use a Trojan, or gain user-level access to a host.</td>
<td>Drop Packet, Drop Connection</td>
</tr>
<tr>
<td>Minor</td>
<td>Attacks attempt to obtain critical information through directory traversal or information leaks.</td>
<td>None</td>
</tr>
<tr>
<td>Warning</td>
<td>Attacks attempt to obtain noncritical information or scan the network. They can also be obsolete attacks (but probably harmless) traffic.</td>
<td>None</td>
</tr>
<tr>
<td>Info</td>
<td>Attacks are normal, harmless traffic containing URLs, DNS lookup failures, and SNMP public community strings. You can use informational attack objects to obtain information about your network.</td>
<td>None</td>
</tr>
</tbody>
</table>

**NOTE:** Our severity rating is not based on CVSS (Common Vulnerability Scoring System). We do include data from Bugtraq (Symantec) and CVE (Common Vulnerabilities and Exposures).

**Specifying Rule IP Action**

If the IDP device matches an attack, it can take action not only against the current session but also against future network traffic that uses the same IP address. Such actions are called *IP actions*. By default, the specified IP action is permanent (timeout = 0). If you prefer, you can set a timeout.

To specify an IP action, right-click the table cell and configure options.

Table 25 on page 40 describes IDP rulebase IP actions.
Table 25: IDP Rulebase IP Actions

<table>
<thead>
<tr>
<th>IP Action</th>
<th>Description</th>
</tr>
</thead>
</table>
| IP Block  | IDP blocks the matching connection and future connections that match combinations of the following properties you specify:  
| Source IP address  |  
| Source subnet  |  
| Protocol  |  
| Destination IP Address  |  
| Destination Subnet  |  
| Destination Port  |  
| From Zone  |  |
| IP Close  | IDP closes the matching connection and future connections that match combinations of the following properties you specify:  
| Source IP address  |  
| Source subnet  |  
| Protocol  |  
| Destination IP Address  |  
| Destination Subnet  |  
| Destination Port  |  
| From Zone  | |
| IP Notify  | IDP does not take any action against future traffic but logs the event or sends an alert.  |

Specifying Rule Notification Options

Notification options determine how events that match the rule are logged.

To specify notification options, right-click the table cell and configure options.

Table 26 on page 40 describes IDP rulebase notification options.

Table 26: IDP Rulebase Notification Options

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
</table>
| Event logs and alerts          | You can enable the following delivery and handling options for logs:  
|                                 | Send to NSM Log Viewer  
|                                 | Send to NSM Log Viewer and flag as an alert  
|                                 | Send to an e-mail address list  
|                                 | Send to syslog  
|                                 | Send to SNMP trap  
|                                 | Save in XML format  
|                                 | Save in CVS format  
|                                 | Process with a script  |
### Table 26: IDP Rulebase Notification Options *(continued)*

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Packet captures</td>
<td>Viewing the packets used in an attack on your network can help you determine the extent of the attempted attack, its purpose, whether or not the attack was successful, and any possible damage to your network. If multiple rules with packet capture enabled match the same attack, IDP captures the maximum specified number of packets. For example, you configure rule 1 to capture 10 packets before and after the attack, and you configure rule 2 to capture 5 packets before and after the attack. If both rules match the same attack, IDP attempts to capture 10 packets before and after the attack. You can capture up to 256 packets before the event and 256 packets after the event. <strong>NOTE:</strong> If necessary, you can improve performance by logging only the packets received after the attack.</td>
</tr>
</tbody>
</table>

### Specifying Rule VLAN Matches

If you deploy an IDP device in a virtual local area network (VLAN), you can specify VLAN tags for traffic in IDP rulebase rules.

Normally, rules match source, destination, and service. If your rule specifies a VLAN tag, then the rule must also match the VLAN tag.

To specify that rules match a VLAN tag, right-click the table cell and configure your setting.

Table 27 on page 41 describes VLAN tag settings.

### Table 27: IDP Rulebase VLAN Tag Settings

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>Matches only traffic that has no VLAN tag</td>
</tr>
<tr>
<td>Any</td>
<td>Matches traffic with any or no VLAN tag (default).</td>
</tr>
<tr>
<td>Select VLAN Tags</td>
<td>Displays the Select VLAN Tags dialog box where you can set a single VLAN tag or a range of VLAN tags.</td>
</tr>
<tr>
<td>Delete VLAN Tags</td>
<td>Displays a dialog box that prompts you to confirm you want to delete the VLAN tag match setting.</td>
</tr>
</tbody>
</table>

### Specifying Rule Targets

By default, IDP security policy rules can be applied to any IDP device. If you desire, you can specify that the rule applies to only specified IDP devices.

To specify that the rule only applies to specified devices, right-click the table cell and select **Select Target** to display the Select Targeted Devices dialog box, where you can select the specify devices on which the rule is to be applied.
Specifying Rule Severity

Severity is a rating of the danger posed by the threat the rule is designed to prevent.

To specify a rule severity, right-click the table cell and select a severity.

Table 28 on page 42 describes rule severity settings.

### Table 28: IDP Rulebase Severity

<table>
<thead>
<tr>
<th>Severity</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>Select <strong>Default</strong> to inherit severity from that specified in the attack object.</td>
</tr>
<tr>
<td>Critical</td>
<td>Attacks that attempt to evade an IPS, crash a machine, or gain system-level privileges. We recommend that you drop the packets or drop the connection for such attacks.</td>
</tr>
<tr>
<td>Major</td>
<td>Attacks that attempt to crash a service, perform a denial of service, install or use a Trojan, or gain user-level access to a host. We recommend that you drop the packets or drop the connection for such attacks.</td>
</tr>
<tr>
<td>Minor</td>
<td>Attacks that attempt to obtain noncritical information through directory traversal or information leaks. We recommend that you log such attacks.</td>
</tr>
<tr>
<td>Warning</td>
<td>Attacks that attempt to obtain noncritical information or scan the network. They can also be obsolete attacks (but probably harmless) traffic. We recommend that you log such attacks.</td>
</tr>
<tr>
<td>Info</td>
<td>Attacks that are normal, harmless traffic containing URLs, DNS lookup failures, and SNMP public community strings. You can use informational attack objects to obtain information about your network. We recommend that you log such attacks.</td>
</tr>
</tbody>
</table>

**NOTE:** Our severity rating is not based on CVSS (Common Vulnerability Scoring System). We do include data from Bugtraq (Symantec) and CVE (Common Vulnerabilities and Exposures).

Specifying Rule Optional Fields

Optional fields are user-defined name-value pairs you can configure if you want to be able to sort rules based on these fields. Optional fields do not affect the functionality of the security policy rule.
To specify optional fields, right-click the table cell and select Edit Options to display the Select Policy Custom Options dialog box, where you can configure name-value pairs.

**Specifying Rule Comments**

Comments are notations about the rule. Comments do not affect the functionality of the security policy rule.

To specify comments, right-click the table cell and select Edit Comments to display the Edit Comments dialog box, where you can enter a comment up to 1024 characters in length.

**Related Topics**
- Intrusion Detection and Prevention Devices and Security Policies Overview on page 29
- Configuring Predefined Security Policies (NSM Procedure) on page 31
- Configuring Exempt Rulebase Rules (NSM Procedure) on page 43
- Assigning a Security Policy in an Intrusion Detection and Prevention Device (NSM Procedure) on page 117

**Configuring Exempt Rulebase Rules (NSM Procedure)**

The exempt rulebase contains rules that prevent rules in the Intrusion Detection and Prevention (IDP) rulebase from matching specific source or destination pairs for specific attack objects.

The exempt rulebase works in conjunction with the IDP rulebase. Before you can create exempt rules, you must first create rules in the IDP rulebase. If traffic matches a rule in the IDP rulebase, the IDP sensor attempts to match the traffic against the exempt rulebase before performing the specified action or creating a log record for the event.

**NOTE:** The exempt rulebase is a non-terminal rulebase. The IDP device checks all rules in the exempt rulebase and executes all matches.

To configure an exempt rulebase rule:
1. In the NSM navigation tree, select **Policy Manager > Security Policies**.
2. Select and double-click the security policy for which you want to add an exempt rulebase rule.
3. Click **New** in the upper right corner of the policy viewer and select **Add Exempt Rulebase**.
4. Click the **New** button within the rules viewer to add a rule.
5. Modify the property of the rule by right-clicking the table cell for the property and making your modifications.

6. Configure or modify the rule using the settings described in Table 29 on page 44.

Table 29: Exempt Rulebase Rule Properties

<table>
<thead>
<tr>
<th>Option</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>Specifies if you want to add, delete, copy, or reorder rules.</td>
<td>Right-click the table cell for the rule number and make your required modifications.</td>
</tr>
<tr>
<td>Match &gt; From Zone</td>
<td>Specifies the zone from where the source sends traffic.</td>
<td>Select one or more zones for the source zone, or you can specify any for all source zones.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>NOTE:</strong> The selected zone must be available on the security device specified in the Install On column.</td>
</tr>
<tr>
<td>Match &gt; Source</td>
<td>Specifies the address object that is the source of the traffic.</td>
<td>Select any to monitor network traffic originating from any IP address.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>NOTE:</strong> You can also negate one or more address objects to specify all sources except the excluded object.</td>
</tr>
<tr>
<td>Match &gt; To Zone</td>
<td>Specifies the destination zone.</td>
<td>Select the destination zone.</td>
</tr>
<tr>
<td>Match &gt; Destination</td>
<td>Specifies the address object that is the destination of the traffic, typically a server or other device on your network.</td>
<td>Select the destination object.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>NOTE:</strong> You can also negate one or more address objects to specify all destinations except the excluded object.</td>
</tr>
<tr>
<td>Attacks</td>
<td>Specifies the attack(s) you want the IDP to exempt for the specified source or destination addresses.</td>
<td>Select the attack objects or groups.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>NOTE:</strong> You must include at least one attack object in an exempt rule.</td>
</tr>
</tbody>
</table>
### Table 29: Exempt Rulebase Rule Properties (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN Tag</td>
<td>Specifies that you can configure a rule to only apply to messages in certain VLANs.</td>
<td>Set a value by selecting any of the following options:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ <em>Any</em>—This rule is applied to messages in any VLAN and to messages without a VLAN tag.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ <em>None</em>—This rule is applied only to messages that do not have a VLAN tag.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ <em>Select VLAN Tags</em>—This rule specifies which VLAN tags the rule applies to.</td>
</tr>
<tr>
<td>Install On</td>
<td>Specifies the security devices or templates that receive and use this rule.</td>
<td>Select the target security device.</td>
</tr>
<tr>
<td>Comments</td>
<td>Specifies any miscellaneous comment about the rule's purpose.</td>
<td>Enter any additional comments about the rule.</td>
</tr>
</tbody>
</table>

For more information, see the *IDP Concepts & Examples guide*.

**Related Topics**
- Intrusion Detection and Prevention Devices and Security Policies Overview on page 29
- Creating a New Security Policy (NSM Procedure) on page 32
- Assigning a Security Policy in an Intrusion Detection and Prevention Device (NSM Procedure) on page 117
- Configuring Backdoor Rulebase Rules (NSM Procedure) on page 45

**Configuring Backdoor Rulebase Rules (NSM Procedure)**

The backdoor rulebase detects if there exists any interactive traffic introduced during backdoor attacks.

To configure a backdoor rulebase rule:
1. In the NSM navigation tree, select *Policy Manager > Security Policies*.
2. Select and double-click the security policy to which you want to add the backdoor rulebase rule.
3. Click **New** in the upper right corner of the policy viewer and select **Add Backdoor Rulebase**.
4. Click the **New** button within the rules viewer to add a rule.
5. Modify the property of the rule by right-clicking the table cell for the property and making your modifications.

6. Configure or modify the rule using the settings described in Table 30 on page 46.

### Table 30: Backdoor Rulebase Rule Properties

<table>
<thead>
<tr>
<th>Option</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>Specifies if you want to add, delete, copy, or reorder rules.</td>
<td>Right-click the table cell for the rule number and make your required modifications.</td>
</tr>
<tr>
<td>Match &gt; Source</td>
<td>Specifies the address object that is the source of the traffic.</td>
<td>Select any to monitor network traffic originating from any IP address.</td>
</tr>
<tr>
<td></td>
<td>NOTE: You can also negate one or more address objects to specify all sources except the excluded object.</td>
<td></td>
</tr>
<tr>
<td>Match &gt; Destination</td>
<td>Specifies the address object that is the destination of the traffic, typically a server or other device on your network.</td>
<td>Select the destination object.</td>
</tr>
<tr>
<td></td>
<td>NOTE: You can also negate one or more address objects to specify all destinations except the excluded object.</td>
<td></td>
</tr>
<tr>
<td>Match &gt; Service</td>
<td>Specifies service objects in rules to service an attack to access your network.</td>
<td>Set a service by selecting any of the following options:</td>
</tr>
<tr>
<td></td>
<td>■ Any—Sets any service.</td>
<td>■ Default—Accepts the service specified by the attack object.</td>
</tr>
<tr>
<td></td>
<td>■ Select Service—Chooses specific services from the list of defined service objects.</td>
<td></td>
</tr>
<tr>
<td>Operation</td>
<td>Specifies whether to detect or ignore the backdoor traffic.</td>
<td>Select either Detect or Ignore.</td>
</tr>
<tr>
<td>Action</td>
<td>Specifies an action of the IDP to detect any interactive traffic.</td>
<td>Select any type of action.</td>
</tr>
<tr>
<td>Notification</td>
<td>Allows you to create log records with attack information that you can view real-time in the Log Viewer.</td>
<td>Select Configure to create log records.</td>
</tr>
</tbody>
</table>
Table 30: Backdoor Rulebase Rule Properties (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN Tag</td>
<td>Specifies that you can configure a rule to</td>
<td>Set a value by selecting any of the following options:</td>
</tr>
<tr>
<td></td>
<td>only apply to messages in certain VLANs.</td>
<td>■ <strong>Any</strong>—This rule is applied to messages in any VLAN and to messages</td>
</tr>
<tr>
<td></td>
<td></td>
<td>without a VLAN tag.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ <strong>None</strong>—This rule is applied only to messages that do not have a VLAN</td>
</tr>
<tr>
<td></td>
<td></td>
<td>tag.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ <strong>Select VLAN Tags</strong>—This rule specifies which VLAN tags the rule applies</td>
</tr>
<tr>
<td></td>
<td></td>
<td>to.</td>
</tr>
<tr>
<td>Severity</td>
<td>Specifies if you can override the inherent</td>
<td>Set the severity to <strong>Default</strong>, <strong>Info</strong>, <strong>Warning</strong>, <strong>Minor</strong>, <strong>Major</strong>,</td>
</tr>
<tr>
<td></td>
<td>attack severity on a per-rule basis within</td>
<td>or <strong>Critical</strong>.</td>
</tr>
<tr>
<td></td>
<td>the IDP rulebase.</td>
<td><strong>NOTE:</strong> This column only appears when you view the Security Policy in</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Expanded Mode.</td>
</tr>
<tr>
<td>Install On</td>
<td>Specifies the security devices or templates</td>
<td>Select the target security device.</td>
</tr>
<tr>
<td></td>
<td>that receive and use this rule.</td>
<td><strong>NOTE:</strong> You can also select multiple security devices on which to install</td>
</tr>
<tr>
<td></td>
<td></td>
<td>the rule.</td>
</tr>
<tr>
<td>Comments</td>
<td>Specifies any miscellaneous comment about the</td>
<td>Enter any additional comments about the rule.</td>
</tr>
<tr>
<td></td>
<td>rule's purpose.</td>
<td></td>
</tr>
</tbody>
</table>

For more information, see the *IDP Concepts & Examples guide*.

**Related Topics**
- Intrusion Detection and Prevention Devices and Security Policies Overview on page 29
- Modifying IDP Rulebase Rules (NSM Procedure) on page 34
- Configuring SYN Protector Rulebase Rules (NSM Procedure) on page 48
- Assigning a Security Policy in an Intrusion Detection and Prevention Device (NSM Procedure) on page 117
Configuring SYN Protector Rulebase Rules (NSM Procedure)

The SYN protector rulebase protects your network from malicious SYN-flood attacks.

To configure a SYN protector rulebase rule:
1. In the NSM navigation tree, select Policy Manager > Security Policies.
2. Select and double-click the security policy to which you want to add the SYN protector rulebase rule.
3. Click New in the upper right corner of the policy viewer and select Add SYN Protector Rulebase.
4. Click the New button within the rules viewer to add a rule.
5. Modify the property of the rule by right-clicking the table cell for the property and making your modifications.
6. Configure or modify the rule using the settings described in Table 31 on page 48.

Table 31: SYN Protector Rulebase Rule Properties

<table>
<thead>
<tr>
<th>Option</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>Specifies if you want to add, delete, copy, or reorder rules.</td>
<td>Right-click the table cell for the rule number and make your required modifications.</td>
</tr>
<tr>
<td>Match &gt; Source</td>
<td>Specifies the address object that is the source of the traffic.</td>
<td>Select any to monitor network traffic originating from any IP address.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>NOTE:</strong> You can also negate one or more address objects to specify all sources except the excluded object.</td>
</tr>
<tr>
<td>Match &gt; Destination</td>
<td>Specifies the address object that is the destination of the traffic, typically a server or other device on your network.</td>
<td>Select the destination object.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>NOTE:</strong> You can also negate one or more address objects to specify all destinations except the excluded object.</td>
</tr>
<tr>
<td>Match &gt; Service</td>
<td>Specifies service objects in rules to service an attack to access your network.</td>
<td>Set a service by selecting any of the available options.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>NOTE:</strong> We recommend that you do not change the default value, TCP-ANY.</td>
</tr>
</tbody>
</table>
Table 31: SYN Protector Rulebase Rule Properties (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mode</td>
<td>Specifies the mode that indicates how IDP handles TCP traffic.</td>
<td>Select any of the following options:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- None—Specifies that IDP takes no action and does not participate in the three-way handshake.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Relay—Specifies that IDP acts as the middleman or relay, for the connection establishment, performing the three-way handshake with the client host on behalf of the server.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Passive—Specifies that IDP handles the transfer of packets between the client host and the server, but does not actively prevent the connection from being established.</td>
</tr>
</tbody>
</table>

**NOTE:** Relay mode might not work as expected for MPLS traffic. When the IDP engine processes MPLS traffic, it stores the MPLS label information for traffic in each direction. In the case of traffic that matches SYN Protector rules in relay mode, the IDP appliance is programmed to send a SYN-ACK before the traffic has reached the server. In these cases, the IDP engine does not have server-to-client MPLS label information. Therefore, the SYN-ACK packet does not include an MPLS label. Some MPLS routers can add packets without a label to an existing MPLS tunnel; others drop such packets.
Table 31: SYN Protector Rulebase Rule Properties (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Notification</td>
<td>Allows you to create log records with attack information that you can view real-time in the Log Viewer.</td>
<td>Select Configure to create log records.</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> For more critical attacks, you can also set an alert flag to appear in the log record.</td>
<td><strong>NOTE:</strong> The Configure menu option does not appear if the Mode column is set to None.</td>
</tr>
<tr>
<td>VLAN Tag</td>
<td>Specifies that you can configure a rule to only apply to messages in certain VLANs.</td>
<td>Set a value by selecting any of the following options:</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> Specifies that you can configure a rule to only apply to messages in certain VLANs.</td>
<td>■ Any—This rule is applied to messages in any VLAN and to messages without a VLAN tag.</td>
</tr>
<tr>
<td></td>
<td>■ None—This rule is applied only to messages that do not have a VLAN tag.</td>
<td>■ Select VLAN Tags—This rule specifies which VLAN tags the rule applies to.</td>
</tr>
<tr>
<td></td>
<td>■ Select VLAN Tags—This rule specifies which VLAN tags the rule applies to.</td>
<td>Set the severity to Default, Info, Warning, Minor, Major, or Critical.</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> This column only appears when you view the Security Policy in Expanded Mode.</td>
<td>For more critical attacks, you can also set an alert flag to appear in the log record.</td>
</tr>
<tr>
<td>Install On</td>
<td>Specifies the security devices or templates that receive and use this rule.</td>
<td>Select the target security device.</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> You can also select multiple security devices on which to install the rule.</td>
<td>For more information, see the IDP Concepts &amp; Examples guide.</td>
</tr>
<tr>
<td>Comments</td>
<td>Specifies any miscellaneous comment about the rule’s purpose.</td>
<td>Enter any additional comments about the rule.</td>
</tr>
</tbody>
</table>
Configuring Traffic Anomalies Rulebase Rules (NSM Procedure)

The traffic anomalies rulebase employs a traffic flow analysis method to detect attacks that occur over multiple connections and sessions (such as scans).

To configure a traffic anomalies rulebase rule:
1. In the NSM navigation tree, select Policy Manager > Security Policies.
2. Select and double-click the security policy to which you want to add the traffic anomalies rulebase rule.
3. Click New in the upper right corner of the policy viewer and select Add Traffic Anomalies Rulebase.
4. Click the New button within the rules viewer to add a rule.
5. Modify the property of the rule by right-clicking the table cell for the property and making your modifications.
6. Configure or modify the rule using the settings described in Table 32 on page 51.

Table 32: Traffic Anomalies Rulebase Rule Properties

<table>
<thead>
<tr>
<th>Option</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>Specifies if you want to add, delete, copy, or reorder rules.</td>
<td>Right-click the table cell for the rule number and make your required modifications.</td>
</tr>
<tr>
<td>Match &gt; Source</td>
<td>Specifies the address object that is the source of the traffic.</td>
<td>Select any to monitor network traffic originating from any IP address.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>NOTE:</strong> You can also negate one or more address objects to specify all sources except the excluded object.</td>
</tr>
<tr>
<td>Match &gt; Destination</td>
<td>Specifies the address object that is the destination of the traffic, typically a server or other device on your network.</td>
<td>Select the destination object.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>NOTE:</strong> You can also negate one or more address objects to specify all destinations except the excluded object.</td>
</tr>
</tbody>
</table>
### Table 32: Traffic Anomalies Rulebase Rule Properties (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Match &gt; Service</td>
<td>Specifies service objects in rules to service an attack to access your network.</td>
<td>Set a service by selecting any of the available options.</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> We recommend that you do not change the default value, TCP-ANY.</td>
<td></td>
</tr>
<tr>
<td>Traffic Anomaly</td>
<td>Specifies how IDP is to treat the matching traffic.</td>
<td>Select any of the following options:</td>
</tr>
<tr>
<td></td>
<td>■ <strong>Ignore</strong>—IDP ignores this traffic. This option excludes traffic from trusted sources that might be falsely construed as a scan.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ <strong>Detect</strong>—IDP matches this traffic and takes the IP action that you have set. When you select this option, the Traffic Anomalies dialog box appears. Select the scans or sweep you want to detect and enter values for Port Count and Time Threshold (in seconds) or Session Count.</td>
<td></td>
</tr>
<tr>
<td>IP Action</td>
<td>Allows you to log, drop, or close the current connection for each attack that matches a rule.</td>
<td>Select <strong>Configure</strong> to do any one of the following actions:</td>
</tr>
<tr>
<td></td>
<td>■ <strong>Enabled</strong>—Enables IP actions.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ <strong>Action</strong>—Specifies the action you want the IDP to take.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ <strong>Block</strong>—Specifies which parameters IDP will use to close or block further connections from the drop down list.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ <strong>Logging</strong>—Specifies the log action for a matching event.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ <strong>Timeout (sec)</strong>—Specifies the number of seconds that this action remains in effect on IDP after a traffic match.</td>
<td></td>
</tr>
</tbody>
</table>
### Table 32: Traffic Anomalies Rulebase Rule Properties (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Notification</td>
<td>Allows you to create log records with attack information that you can view real-time in the Log Viewer. NOTE: For more critical attacks, you can also set an alert flag to appear in the log record.</td>
<td>Select <strong>Configure</strong> to create log records. <strong>NOTE:</strong> The Configure menu option does not appear if the Mode column is set to None. ■ Select <strong>Logging</strong> to have a log record created each time the rule is matched. ■ Select <strong>Alert</strong> to have an alert flag placed in the Alert column of the Log Viewer for the matching log record. ■ In the Log Actions tab, select desired log actions, if any.</td>
</tr>
<tr>
<td>VLAN Tag</td>
<td>Specifies that you can configure a rule to only apply to messages in certain VLANs.</td>
<td>Set a value by selecting any of the following options: ■ <strong>Any</strong>—This rule is applied to messages in any VLAN and to messages without a VLAN tag. ■ <strong>None</strong>—This rule is applied only to messages that do not have a VLAN tag. ■ <strong>Select VLAN Tags</strong>—Specifies which VLAN tags the rule applies to.</td>
</tr>
<tr>
<td>Severity</td>
<td>Specifies if you can override the inherent attack severity on a per-rule basis within the IDP rulebase.</td>
<td>Set the severity to <strong>Default</strong>, <strong>Info</strong>, <strong>Warning</strong>, <strong>Minor</strong>, or <strong>Critical</strong>. <strong>NOTE:</strong> This column only appears when you view the Security Policy in Expanded Mode.</td>
</tr>
<tr>
<td>Install On</td>
<td>Specifies the security devices or templates that receive and use this rule.</td>
<td>Select the target security device. <strong>NOTE:</strong> You can also select multiple security devices on which to install the rule.</td>
</tr>
<tr>
<td>Comments</td>
<td>Specifies any miscellaneous comment about the rule's purpose.</td>
<td>Enter any additional comments about the rule.</td>
</tr>
</tbody>
</table>

For more information, see the **IDP Concepts & Examples guide**.

**Related Topics**
- Intrusion Detection and Prevention Devices and Security Policies Overview on page 29
- Modifying IDP Rulebase Rules (NSM Procedure) on page 34
Configuring Network Honeypot Rulebase Rules (NSM Procedure)

The network honeypot rulebase is a method to detect investigation activities.

To configure a network honeypot rulebase rule:
1. In the NSM navigation tree, select Policy Manager > Security Policies.
2. Select and double-click the security policy to which you want to add the network honeypot rulebase rule.
3. Click New in the upper right corner of the policy viewer and select Add Network Honeypot Rulebase.
4. Click the New button within the rules viewer to add a rule.
5. Modify the property of the rule by right-clicking the table cell for the property and making your modifications.
6. Configure or modify the rule using the settings described in Table 33 on page 54.

Table 33: Network Honeypot Rulebase Rule Properties

<table>
<thead>
<tr>
<th>Option</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>Specifies if you want to add, delete, copy, or reorder rules.</td>
<td>Right-click the table cell for the rule number and make your required modifications.</td>
</tr>
<tr>
<td>Source Address</td>
<td>Specifies the address object that is the source of the traffic.</td>
<td>Select any source address or group.</td>
</tr>
<tr>
<td>Impersonate &gt; Destination</td>
<td>Specifies the address object that is the destination of the traffic, typically a server or other device on your network.</td>
<td>Select the destination object. <strong>NOTE:</strong> You can also negate one or more address objects to specify all destinations except the excluded object.</td>
</tr>
<tr>
<td>Impersonate &gt; Service</td>
<td>Specifies the services running on your network.</td>
<td>Select the services you want to monitor.</td>
</tr>
</tbody>
</table>
### Table 33: Network Honeypot Rulebase Rule Properties (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Operation</strong></td>
<td>Specifies whether or not IDP fakes open ports.</td>
<td>Select any of the following options:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ <strong>Ignore</strong>—This option allows free passage on your network when creating rules for trusted traffic.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ <strong>Impersonate</strong>—IDP creates a fake port open to the public based on the destination IP addresses and service you selected.</td>
</tr>
<tr>
<td><strong>IP Action</strong></td>
<td>Allows you to log, drop, or close the current connection for each attack that matches a rule.</td>
<td>Select <strong>Configure</strong> to do any one of the following actions:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ <strong>Enabled</strong>—Enable IP actions.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ <strong>Action</strong>—Specifies the action you want the IDP to take.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ <strong>Block</strong>—Specifies which parameters IDP will use to close or block further connections from the drop-down list.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ <strong>Logging</strong>—Specifies the log action for a matching event.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ <strong>Timeout (sec)</strong>—Specifies the number of seconds that this action remains in effect on IDP after a traffic match.</td>
</tr>
<tr>
<td><strong>Notification</strong></td>
<td>Allows you to create log records with attack information that you can view real-time in the Log Viewer.</td>
<td>Select <strong>Configure</strong> to create log records.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>NOTE:</strong> The Configure menu option does not appear if the Mode column is set to None.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ Select <strong>Logging</strong> to have a log record created each time the rule is matched.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ Select <strong>Alert</strong> to have an alert flag placed in the Alert column of the Log Viewer for the matching log record.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ In the Log Actions tab, select desired log actions, if any.</td>
</tr>
</tbody>
</table>
Table 33: Network Honeypot Rulebase Rule Properties (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN Tag</td>
<td>Specifies that you can configure a rule to only apply to messages in certain VLANs.</td>
<td>Set a value by selecting any of the following options:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ Any—This rule is applied to messages in any VLAN and to messages without a VLAN tag.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ None—This rule is applied only to messages that do not have a VLAN tag.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ Select VLAN Tags—This rule specifies which VLAN tags the rule applies to.</td>
</tr>
<tr>
<td>Severity</td>
<td>Specifies if you can override the inherent attack severity on a per-rule basis within the IDP rulebase.</td>
<td>Set the severity to Default, Info, Warning, Minor, Major, or Critical.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>NOTE:</strong> This column only appears when you view the Security Policy in Expanded Mode.</td>
</tr>
<tr>
<td>Install On</td>
<td>Specifies the security devices or templates that receive and use this rule.</td>
<td>Select the target security device.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>NOTE:</strong> You can also select multiple security devices on which to install the rule.</td>
</tr>
<tr>
<td>Comments</td>
<td>Specifies any miscellaneous comment about the rule's purpose.</td>
<td>Enter any additional comments about the rule.</td>
</tr>
</tbody>
</table>

**NOTE:** The IDP drops MPLS traffic that matches a Network Honeypot rule. When the IDP engine processes MPLS traffic, it stores the MPLS label information. It stores separate labels for client-to-server and server-to-client communication. In the case of traffic that matches Network Honeypot rules, there is no genuine server-to-client communication, so the IDP engine does not have server-to-client MPLS label information. Therefore, the impersonation operation is not supported.

For more information, see the *IDP Concepts & Examples guide*.

**Related Topics**  
- Intrusion Detection and Prevention Devices and Security Policies Overview on page 29  
- Modifying IDP Rulebase Rules (NSM Procedure) on page 34  
- Assigning a Security Policy in an Intrusion Detection and Prevention Device (NSM Procedure) on page 117  
- Validating a Security Policy (NSM Procedure) on page 118
Configuring Application Rulebase Rules (NSM Procedure)

The Application Policy Enforcement (APE) rulebase enables you to limit bandwidth for specified users and/or applications. You can configure APE rules to detect network traffic based on application signatures. The APE rules are sent as part of the IDP rulebase, and the attacks are mapped from the corresponding application. The user can define custom application signatures to be used in the APE rules. The custom application is included as part of the policy update for IDP 5.0 and later supported devices (devices that have application identification support).

To configure an APE rulebase rule:

1. In the NSM navigation tree, select Policy Manager > Security Policies.
2. Select and double-click the security policy to which you want to add the APE rulebase rule.
3. Click New in the upper right corner of the policy viewer and select Add Application Rulebase.
4. Click the New button within the rules viewer to add a rule.
5. Modify the property of the rule by right-clicking the table cell for the property and making your modifications.
6. Configure or modify the rule using the settings described in Table 34 on page 57.
7. Click OK to save your changes.

Table 34: APE Rulebase Rule Properties

<table>
<thead>
<tr>
<th>Option</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>No.</td>
<td>Specifications if you want to add, delete, copy, or reorder rules. Right-click the table cell for the rule number and make your required modifications.</td>
<td></td>
</tr>
<tr>
<td>Match &gt; Source</td>
<td>Specifies the address object that is the source of the traffic. Select any to monitor network traffic originating from any IP address. <strong>NOTE:</strong> For guidelines on specifying match parameters, see the IDP Concepts and Examples Guide.</td>
<td></td>
</tr>
<tr>
<td>Match &gt; User Role</td>
<td>Specifies the user roles to match the session for the rule to be applied. If a value for User Role matches, the Source parameter is not consulted. Right-click the table cell to select user roles. Matching based on user role depends on integration with a compatible Juniper Networks IC Series Unified Access Control appliance.</td>
<td></td>
</tr>
</tbody>
</table>
Table 34: APE Rulebase Rule Properties (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Match &gt; Destination</td>
<td>Specifies the address object that is the destination of the traffic, typically a server or other device on your network.</td>
<td>Select the destination object.</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> You can also negate one or more address objects to specify all destinations except the excluded object.</td>
<td></td>
</tr>
<tr>
<td>Match &gt; Service</td>
<td>Requires one of the specified services to match the session for the rule to be applied. Services are Application Layer protocols that define how data is structured as it travels across the network. The IDP engine can inspect services that use TCP, UDP, RPC, and ICMP transport layer protocols. If the application running on the destination server uses standard ports, you can select from predefined services. If the application running on the destination server uses nonstandard ports, you must create a custom service object.</td>
<td>Right-click the table cell and select any one of the required options.</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> To apply an APE action to all traffic matching source and destination parameters, set both the service parameter and the application parameter to <strong>Any</strong>.</td>
<td></td>
</tr>
<tr>
<td>Match &gt; Application</td>
<td>Requires one of the specified applications to match the session for the rule to be applied. The predefined list of applications is populated by the application identification feature. The application identification feature identifies the application regardless of port. Port-independent application identification simplifies rule configuration and ensures that you do not miss applications running on nonstandard ports. Hence it is recommended to use the application parameter instead of the service parameter whenever possible.</td>
<td>Right-click the table cell and make your required modifications.</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> To apply an APE action to all traffic matching source and destination parameters, set both the service parameter and the application parameter to <strong>Any</strong>.</td>
<td></td>
</tr>
</tbody>
</table>
Table 34: APE Rulebase Rule Properties (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Action</td>
<td>Specifies which actions to perform against attacks that match rules in your security policy.</td>
<td>Right-click the table cell and select any one of the following options:</td>
</tr>
<tr>
<td></td>
<td>■ None — IDP takes no action against the connection.</td>
<td>■ None — IDP takes no action against the connection.</td>
</tr>
<tr>
<td></td>
<td>■ Drop Packet — IDP drops a matching packet before it can reach its destination but does not close the connection.</td>
<td>■ Drop Packet — IDP drops a matching packet before it can reach its destination but does not close the connection.</td>
</tr>
<tr>
<td></td>
<td>■ Drop Connection — IDP drops the connection without sending an RST packet to the sender, preventing the traffic from reaching its destination.</td>
<td>■ Drop Connection — IDP drops the connection without sending an RST packet to the sender, preventing the traffic from reaching its destination.</td>
</tr>
<tr>
<td></td>
<td>■ Close Client — IDP closes the connection to the client and not to the server.</td>
<td>■ Close Client — IDP closes the connection to the client and not to the server.</td>
</tr>
<tr>
<td></td>
<td>■ Close Server — IDP closes the connection to the server and not to the client.</td>
<td>■ Close Server — IDP closes the connection to the server and not to the client.</td>
</tr>
<tr>
<td></td>
<td>■ Close Client and Server — IDP closes the connection and sends a RST packet to both the client and the server.</td>
<td>■ Close Client and Server — IDP closes the connection and sends a RST packet to both the client and the server.</td>
</tr>
<tr>
<td></td>
<td>■ Diffserv Marking — Assigns the service differentiation value indicated to the packet, then passes it on normally.</td>
<td>■ Diffserv Marking — Assigns the service differentiation value indicated to the packet, then passes it on normally.</td>
</tr>
<tr>
<td></td>
<td>■ Rate Limiting — IDP enforces a rate limit for all current sessions that match the rule (separate limits for client-to-server and server-to-client traffic). If the limit has not been reached, IDP forwards the packets. If the limit has been reached, IDP behaves as if no bandwidth is available.</td>
<td>■ Rate Limiting — IDP enforces a rate limit for all current sessions that match the rule (separate limits for client-to-server and server-to-client traffic). If the limit has not been reached, IDP forwards the packets. If the limit has been reached, IDP behaves as if no bandwidth is available.</td>
</tr>
<tr>
<td>Notification</td>
<td>Specifies logging options. Packet capture is not applicable for APE rulebase rules.</td>
<td>Right-click the table cell and select Configure to display a dialog box where you can configure logging options.</td>
</tr>
<tr>
<td>VLAN Tag</td>
<td>Specifies rules to traffic on certain VLANs. Normally, for a rule to take effect, it must match the packet source, destination, service, and attack objects. If the VLAN cell is populated with a value other than any, then the rule will also consider the packet’s VLAN tag when determining a match.</td>
<td>Right-click the table cell to assign a VLAN object to a rule or to set the VLAN tag value to none.</td>
</tr>
<tr>
<td>Install On</td>
<td>Specifies target IDP devices for the rule. By default, IDP security policy rules can be applied to any IDP device.</td>
<td>Right-click the table cell and select Select Target to display a dialog box to specify the IDP devices to which the rule can be installed.</td>
</tr>
<tr>
<td>Comments</td>
<td>Adds notations about the rule. This setting is optional and does not affect the functionality of the security policy rule.</td>
<td>Right-click the table cell and select Edit Comments to display a dialog box where you can make notations about the rule.</td>
</tr>
</tbody>
</table>

You can verify the APE rulebase functionality in your lab and view APE related statistics in the Command-Line Interface (CLI). It is recommended that you retain defaults for APE rulebase. By default:

Configuring Application Rulebase Rules (NSM Procedure)
IDP does not limit the rate of sessions that do not match APE rules. Rate limiting is done by service based till application is identified in the session i.e. default services running on the port.

When the application identification feature fails to identify the application, IDP does not try to match the rule but instead applies the default rate limit (if any). You can modify this so that in cases where application identification fails, IDP attempts to match the session to the standard protocol and port for the application.

For more information, see the *IDP Concepts & Examples guide*.

**Related Topics**
- Intrusion Detection and Prevention Devices and Security Policies Overview on page 29
- Modifying IDP Rulebase Rules (NSM Procedure) on page 34
Chapter 5
Working with Attack Objects

- Attack Objects in Intrusion Detection and Prevention Security Policies Overview on page 61
- Loading J-Security-Center Updates (NSM Procedure) on page 62
- Viewing Predefined Attack Objects (NSM Procedure) on page 64
- Working with Attack Groups (NSM Procedure) on page 64
- Creating Custom Attack Objects (NSM Procedure) on page 67
- Verifying the Attack Object Database Version (NSM Procedure) on page 75
- Updating the IDP Detector Engine (NSM Procedure) on page 76

**Attack Objects in Intrusion Detection and Prevention Security Policies Overview**

You use the NSM Object Manager to manage NSM administrative objects, including the attack objects used in IDP security policies.

For more explanation of attack objects and examples, see the *Network and Security Manager Administration Guide*.

For details on how to use NSM Object Manager features to copy objects, find references to objects, search for unused objects, or configure object versions, see the *NSM online Help*.

IDP administration using attack objects can include the following tasks related to attack objects:
- Updating IDP detector engine and the NSM attack database
- Viewing predefined attack object definitions
- Viewing attack object groups
- Creating custom attack objects
- Updating predefined IDP attack objects and groups

**Related Topics**
- Working with Attack Groups (NSM Procedure) on page 64
- Viewing Predefined Attack Objects (NSM Procedure)
- Loading J-Security-Center Updates (NSM Procedure) on page 62
Loading J-Security-Center Updates (NSM Procedure)

The Juniper Networks Security Center (J-Security Center) routinely makes important updates available to IDP security policy components, including updates to the IDP detector engine and NSM attack database.

The IDP detector engine is a dynamic protocol decoder that includes support for decoding more than 60 protocols and more than 500 service contexts. You should update IDP detector engine when you first install the IDP device, whenever you upgrade, and whenever alerted to do so by Juniper Networks.

The NSM attack database stores data definitions for the attack objects that are key components of IDP security policies. Updates can include new attack objects, revised severity settings, or removed attack objects. You should schedule daily updates to the NSM attack database.

After you have completed the update, any new attack objects are available in the security policy editor. If you use dynamic groups to your IDP rulebase rules and a new attack object belongs to the dynamic group, the rule automatically inherits the new attacks.

Table 35 on page 62 provides procedures for updating IDP detector engine and the NSM attack database.

Table 35: IDP Detector Engine and NSM Attack Database Update Procedures

<table>
<thead>
<tr>
<th>Task</th>
<th>Procedure</th>
</tr>
</thead>
</table>
| To download IDP detector engine and NSM attack database updates to the NSM GUI server | From the NSM main menu, select **Tools > View/Update NSM attack database** and complete the wizard steps.  
**NOTE:** The default URL from which to obtain updates is https://services.netscreen.com/restricted/sigupdates/nsm-updates/NSM-SecurityUpdateInfo.dat. If you encounter connection errors, ensure this setting has not been inadvertently changed.  
1. From the NSM main menu, select **Tools > Preferences**.  
2. Click **Attack Object**.  
3. Click **Restore Defaults**.  
   NSM restores the URL in the **Download URL for ScreenOS Devices** text box.  
4. Click **OK**. |
| To push an IDP detector engine update from the NSM GUI server to IDP devices | From the NSM main menu, select **Devices > IDP Detector Engine > Load IDP Detector Engine for ScreenOS** and complete the wizard steps.  
**NOTE:** Updating the IDP detector engine on a device does not require a reboot of the device. |
Table 35: IDP Detector Engine and NSM Attack Database Update Procedures (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Procedure</th>
</tr>
</thead>
</table>
| To push predefined attack object updates from the NSM GUI server to IDP devices | 1. From the NSM main menu, select **Devices > Configuration > Update Device Config.**  
2. Select the devices that you want to push configuration updates to and to set update job options on.  
3. Click **OK.**  

**NOTE:** Only the attack objects that are used in IDP rules for the device are pushed from the GUI server to the device. |
| To schedule regular updates                                           | 1. Log in to the NSM GUI server command line.  
2. Change directory to `/usr/netscreen/GuiSvr/utils`.  
3. Create a shell script called `attackupdates.sh` with the following contents:  
   - Set the `NSMUSER` environment variable with an NSM domain/user pair. The command for setting environment variables depends on your OS. Example:  
     ```bash  
     export NSMUSER=domain/user  
     ```  
   - Set the `NSMPASSWD` environment variable with an NSM password. The command for setting environment variables depends on your OS and shell. Example:  
     ```bash  
     export NSMPASSWD=password  
     ```  
   - Specify a guiSvrCli command string. Example:  
     ```bash  
     ```  
4. Make the script executable by the user associated with the cron job:  
   ```bash  
   chmod 700 attackupdates.sh  
   ```  
5. Run the crontab editor:  
   ```bash  
   crontab -e  
   ```  
6. Add an entry for the shell script:  
   ```bash  
   minutes_after_hour  
   hour * * * /usr/netscreen/GuiSvr/utils/attackupdates.sh  
   ```  
   During the update, the guiSvrCli utility updates the attack object database, then performs the post actions. After updating and executing actions, the system generates an exit status code of 0 (no errors) or 1 (errors). |

**Related Topics**  
- Attack Objects in Intrusion Detection and Prevention Security Policies Overview on page 61  
- Viewing Predefined Attack Objects (NSM Procedure)  
- Working with Attack Groups (NSM Procedure) on page 64
Viewing Predefined Attack Objects (NSM Procedure)

**Purpose**  
Juniper Networks Security Center (J-Security Center) develops predefined attack objects and attack object groups for IDP rulebase rules.

In most cases, the predefined attack objects are the only attack objects you need to protect your network.

The predefined attack object list in the NSM Object Manager provides the following summary of each attack object:
- Name of the attack object
- Severity of the attack: critical, major, minor, warning, info
- Category
- Keywords
- Common Vulnerabilities and Exposures database (CVE) number
- Security Focus Bugtraq database number

**Action**  
To view predefined attack object details:

1. In the Object Manager, click **Attack Objects > IDP Objects** to display the IDP Objects dialog box.
2. Click either the **Predefined Attacks** or **Predefined Attack Groups** tab to view the predefined attack object list.
3. Double-click the table row entry for the attack object to display its details.

**NOTE:** You cannot create, edit, or delete predefined attack objects.

**Related Topics**  
- Attack Objects in Intrusion Detection and Prevention Security Policies Overview on page 61
- Working with Attack Groups (NSM Procedure) on page 64
- Loading J-Security-Center Updates (NSM Procedure) on page 62
- Viewing Predefined Attack Objects (NSM Procedure)

Working with Attack Groups (NSM Procedure)

NSM groups are administrative objects that facilitate configuration and monitoring tasks. You can add attack groups or individual attack objects to IDP rulebase rules and Exempt rulebase rules.

- Creating Dynamic Groups on page 65
- Creating Static Groups on page 66
Creating Dynamic Groups

A dynamic group contains attack objects that are automatically added or deleted based on specified criteria for the group. The NSM Object Manager includes predefined dynamic groups that work with recommended attack objects, predefined attack objects, the recommended security policy, and predefined policy templates.

When you run an NSM attack database update job, the process automatically performs the following tasks:

- For all new attack objects, compares the predefined attributes of each attack object to each dynamic group criteria and adds the attack objects that match.
- For all updated attack objects, removes attack objects that no longer meet their dynamic group criteria.
- Reviews updated attack objects to determine if they now meet any other dynamic group criteria, and adds them to those groups if necessary.
- For all deleted attack objects, removes the attack objects from their dynamic groups.

Use of dynamic groups eliminates the need to review each new signature to determine if you need to use it in your existing security policy.

A predefined or custom dynamic group can contain only attack objects and not attack groups. Dynamic group members can be either predefined or custom attack objects.

To create a custom dynamic group:

1. In Object Manager, select **Attack Objects > IDP Objects** to display the IDP Objects dialog box.
2. Click the **Custom Attack Groups** tab, then click the **+** icon and select **Add Dynamic Group** to display the New Dynamic Group dialog box.
3. Enter a name and description for the static group. Select a color for the group icon.
4. In the Filters tab, click the **+** icon and add select filters that determine which attack objects should be in the group using Table 36 on page 65.
2. Click the **Members** tab to view the attack objects now belonging to the group.
3. Click **OK** to save your settings.

Table 36: Dynamic Attack Group Filters

<table>
<thead>
<tr>
<th>Filter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add Products Filter</td>
<td>Filters attack objects based on the application that is vulnerable to the attack.</td>
</tr>
</tbody>
</table>
Table 36: Dynamic Attack Group Filters (continued)

<table>
<thead>
<tr>
<th>Filter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add Severity Filter</td>
<td>Filters attack objects based on attack severity.</td>
</tr>
<tr>
<td><strong>NOTE:</strong></td>
<td>All predefined attack objects are assigned a severity level by Juniper Networks. However, you can edit this setting to match the needs of your network.</td>
</tr>
<tr>
<td>Add Category Filter</td>
<td>Filters attack objects based on category.</td>
</tr>
<tr>
<td>Add Last Modified Filter</td>
<td>Filters attack objects based on their last modification date.</td>
</tr>
<tr>
<td>Add Recommended Filter</td>
<td>Filters attack objects based on whether they have been marked Recommended.</td>
</tr>
</tbody>
</table>

Creating Static Groups

A static group contains a specific, finite set of attack objects or groups. There are two types of static groups: predefined static groups and custom static groups.

A custom static group can include the same members as a predefined static group (predefined attack objects, predefined static groups, and predefined dynamic groups), plus the following members:

- Custom attack objects
- Custom dynamic groups
- Other custom static groups

Use static groups to define a specific set of attacks to which you know your network is vulnerable, or to group custom attack objects. For example, you might want to create a group for a specific set of informational attack objects that keep you aware of what is happening on your network.

Static groups require more maintenance than dynamic groups because you must manually add or remove attack objects in a static group to change the members. However, you can include a dynamic group within a static group to automatically update some attack objects. For example, the predefined attack object group Operating System is a static group that contains four predefined static groups: BSD, Linux, Solaris, and Windows. The BSD group contains the predefined dynamic group BSD-Services-Critical, to which attack objects can be added during an attack database update.

To create a custom static group:

1. In Object Manager, select **Attack Objects > IDP Objects** to display the IDP Objects dialog box.
2. Click the **Custom Attack Groups** tab, then click the + icon and select **Add Static Group** to display the New Static Group dialog box.
3. Enter a name and description for the static group.
4. Select a color for the group icon.
5. Select the attack or group from the Attacks/Group list and click Add.
6. Click OK.

Related Topics
- Attack Objects in Intrusion Detection and Prevention Security Policies Overview on page 61
- Creating Custom Attack Objects (NSM Procedure) on page 67
- Viewing Predefined Attack Objects (NSM Procedure)
- Verifying the Attack Object Database Version (NSM Procedure) on page 75

Creating Custom Attack Objects (NSM Procedure)

This section includes the following:
- Configuring General Properties for Attack Objects on page 67
- Creating a Signature Attack Object on page 69

Configuring General Properties for Attack Objects

To create a custom attack object:
1. In the Object Manager, click Attack Objects > IDP Objects to display the IDP Objects dialog box.
2. Click the Custom Attacks tab.
3. Click the + icon to display the Custom Attack dialog box.
4. Configure general attack object settings using Table 37 on page 67 on the General tab.

Table 37: Custom Attack Dialog Box: General Tab Settings

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
</table>
| Name      | Specifies the name to be displayed in the UI.  
**TIP:** You might want to include the protocol the attack uses as part of the attack name. |
| Description | Specifies details about the attack. Entering a description is optional when creating a new attack object, but it can help you remember important information about the attack. View the attack descriptions for predefined attacks for examples. |
| Severity  | Specifies a severity rating: Info, Warning, Minor, Major, or Critical. Critical attacks are the most dangerous—typically these attacks attempt to crash your server or gain control of your network. Informational attacks are the least dangerous and typically are used by network administrators to discover holes in their own security system. |
| Category  | Specifies a predefined category or defines a new category. |
| Keywords  | Specifies keywords—unique identifiers that can be used to search and sort log records. |
Table 37: Custom Attack Dialog Box: General Tab Settings (continued)

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Recommended</td>
<td>Specifies that this attack object is part of your highest risk set of attack objects. Later, when you add this attack object to dynamic groups, you can specify whether only recommended attack objects will be included.</td>
</tr>
<tr>
<td>Attack Versions</td>
<td>Skip this for now.</td>
</tr>
<tr>
<td>Detection Performance</td>
<td>Select High, Medium, Low, or Not Defined.</td>
</tr>
</tbody>
</table>

5. On the Extended tab, using Table 38 on page 68. Configure additional attack details.

Table 38: Custom Attack Dialog Box: Extended Tab Settings

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Primary URL</td>
<td>Enter up to three URLs (primary, secondary, tertiary) for external references you used when researching the attack.</td>
</tr>
<tr>
<td>Secondary URL</td>
<td></td>
</tr>
<tr>
<td>Tertiary URL</td>
<td></td>
</tr>
<tr>
<td>CVE</td>
<td>Common Vulnerabilities and Exposures (CVE) is a standardized list of vulnerabilities and other information security exposures. The CVE number is an alphanumeric code, such as CVE-2209</td>
</tr>
<tr>
<td>Bugtraq</td>
<td>A moderated mailing list that discusses and announces computer security vulnerabilities. The BugTraq ID number is a three-digit code, such as 831 or 120.</td>
</tr>
<tr>
<td>Impact</td>
<td>Enter details about the impact of a successful attack, including information on system crashes and access granted to the attacker.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description of the custom attacks.</td>
</tr>
<tr>
<td>Tech Info</td>
<td>Enter details on the vulnerability, the commands used to execute the attack, which files are attacked, registry edits, and other low-level information.</td>
</tr>
<tr>
<td>Patches</td>
<td>List any patches available from the product vendor, as well as information on how to prevent the attack.</td>
</tr>
</tbody>
</table>

6. Return to the General tab.
7. Under Attack Versions, click the + icon to display the New Attack wizard.
8. On the Target Platform and Type page, select a device platform (IDP 4.0, for example) and attack type.

Table 39 on page 69 summarizes attack types and provides references to the next steps required to implement the technical configuration of the attack objects for each type.
Table 39: Attack Object Types

<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Signature</td>
<td>Uses a stateful attack signature (a pattern that always exists within a specific section of the attack) to detect known attacks. Stateful signature attack objects also include the protocol or service used to perpetrate the attack and the context in which the attack occurs. If you know the exact attack signature, the protocol, and the attack context used for a known attack, select this option.</td>
</tr>
<tr>
<td>Protocol Anomaly</td>
<td>Detects unknown or sophisticated attacks that violate protocol specifications (RFCs and common RFC extensions). You cannot create new protocol anomalies, but you can configure a new attack object that controls how the security device handles a predefined protocol anomaly when detected. If you do not know that exact attack signature, but you do know the protocol anomaly that detects the attack, select this option.</td>
</tr>
<tr>
<td>Compound Attack</td>
<td>Detects attacks that use multiple methods to exploit a vulnerability. This object combines multiple signatures and/or protocol anomalies into a single attack object, forcing traffic to match all combined signatures and/or anomalies within the compound attack object before traffic is identified as an attack. By combining and even specifying the order in which signatures or anomalies must match, you can be very specific about the events that need to take place before IDP identifies traffic as an attack. If you need to detect an attack that uses several benign activities to attack your network, or if you want to enforce a specific sequence of events to occur before the attack is considered malicious, select this option.</td>
</tr>
</tbody>
</table>

9. Click Ok.

Creating a Signature Attack Object

To configure a signature attack object:

1. Configure general attack object properties. For information, see “Configuring General Properties for Attack Objects” on page 67.

   On the Target Platform and Type page, select Signature and click Next.

2. On the Custom Attack–General Properties page, configure the settings described in Table 40 on page 69.

Table 40: Custom Attack – General Properties

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>False Positives</td>
<td>Select the frequency that the attack object produces a false positive on your network: Unknown, Rarely, Occasionally, Frequently.</td>
</tr>
</tbody>
</table>
Table 40: Custom Attack – General Properties (continued)

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service Binding</td>
<td><strong>Any</strong>—If you are unsure of the correct service, select Any to match the signature in all services. Because some attacks use multiple services to attack your network, you might want to select the Any service binding to detect the attack regardless of which service the attack selects for a connection. <strong>NOTE:</strong> You must select a service binding other than Any if you want to select a context for the attack.</td>
</tr>
<tr>
<td></td>
<td><strong>IP</strong>—If you are not sure of the correct service, but know the IP protocol type, select IP protocol type for the service binding. Specify the protocol type number. If you select this option, you should also specify an attack pattern and IP header values later in the wizard. However, if you use a context binding of first packet, you must leave the attack pattern empty.</td>
</tr>
<tr>
<td></td>
<td><strong>TCP, UDP, or ICMP</strong>—Attacks that do not use a specific service might use a specific protocol to attack your network. Some TCP and UDP attacks use standard ports to enter your network and establish a connection. For TCP and UDP protocol types, specify the port ranges.</td>
</tr>
<tr>
<td></td>
<td><strong>RPC</strong>—The remote procedure call (RPC) protocol is used by distributed processing applications to handle interaction between processes remotely. When a client makes a remote procedure call to an RPC server, the server replies with a remote program; each remote program uses a different program number. To detect attacks that use RPC, configure the service binding as RPC and specify the RPC program ID.</td>
</tr>
<tr>
<td></td>
<td><strong>Service</strong>—Most attacks use a specific service to attack your network. If you select Service, the wizard displays a second selection box where you specify the service used for the attack. If you select this option, you are restricted to general attack contexts (packet, first packet, stream, stream 256, or line context).</td>
</tr>
<tr>
<td>Time Binding</td>
<td><strong>Enable</strong>—Time attributes control how the attack object identifies attacks that repeat for a certain number of times. <strong>Scope</strong>—Select the scope within which the count occurs:</td>
</tr>
<tr>
<td></td>
<td>■ <strong>Source</strong>—Detects attacks from the source IP address for the specified number of times, regardless of the destination IP address.</td>
</tr>
<tr>
<td></td>
<td>■ <strong>Destination</strong>—Detects attacks to the destination IP address for the specified number of times, regardless of the source IP address.</td>
</tr>
<tr>
<td></td>
<td>■ <strong>Peer</strong>—Detects attacks between source and destination IP addresses of the sessions for the specified number of times. <strong>Count/Min</strong>—Enter the number of times per minute that the attack object must detect an attack within the specified scope before the device considers the attack object to match the attack.</td>
</tr>
</tbody>
</table>
Click **Next**.

3. On the Custom Attack – Attack Patterns page, configure the settings described in Table 41 on page 71.

**Table 41: Custom Attack – Attack Patterns**

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pattern</td>
<td>\0 &lt; octal_number &gt;</td>
</tr>
<tr>
<td></td>
<td>For a direct binary match.</td>
</tr>
<tr>
<td></td>
<td>\X &lt; hexadecimal-number &gt; \X</td>
</tr>
<tr>
<td></td>
<td>For a direct binary match.</td>
</tr>
<tr>
<td></td>
<td>[ &lt; character-set &gt; ]</td>
</tr>
<tr>
<td></td>
<td>For case insensitive matches.</td>
</tr>
<tr>
<td></td>
<td>.</td>
</tr>
<tr>
<td></td>
<td>To match any symbol.</td>
</tr>
<tr>
<td></td>
<td>*</td>
</tr>
<tr>
<td></td>
<td>To match 0 or more symbols.</td>
</tr>
<tr>
<td></td>
<td>+</td>
</tr>
<tr>
<td></td>
<td>To match 1 or more symbols.</td>
</tr>
<tr>
<td></td>
<td>?</td>
</tr>
<tr>
<td></td>
<td>To match 0 or 1 symbols.</td>
</tr>
<tr>
<td></td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>Grouping of expressions.</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Alternation. Typically used with ().</td>
</tr>
<tr>
<td></td>
<td>[ &lt; start &gt; - &lt; end &gt; ]</td>
</tr>
<tr>
<td></td>
<td>Character range.</td>
</tr>
<tr>
<td></td>
<td>[^ &lt; start &gt; - &lt; end &gt; ]</td>
</tr>
<tr>
<td></td>
<td>Negation of character range.</td>
</tr>
<tr>
<td>Negate</td>
<td>Select this option to negate the attack pattern.</td>
</tr>
</tbody>
</table>
Table 41: Custom Attack – Attack Patterns (continued)

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Context</td>
<td>Select the context used by the attack to enter your network.</td>
</tr>
<tr>
<td></td>
<td>If you know the service and the specific service context, select that service and then select the appropriate service contexts.</td>
</tr>
<tr>
<td></td>
<td>If you know the service, but are unsure of the specific service context, select <strong>Other</strong> and then select one of the following general contexts:</td>
</tr>
<tr>
<td></td>
<td>■ <strong>Packet</strong>—Detects the pattern at the packet level. When you select this option, you should also specify the Service Binding (in the General tab) and define the service header options (in the Header Match tab). Although not required, specifying these additional parameters helps to improve the accuracy of the attack object.</td>
</tr>
<tr>
<td></td>
<td>■ <strong>First Packet</strong>—Inspects only the first packet of a stream. When the flow direction for the Attack Object is set to any, IDP checks the first packet of both the server-to-client (STC) and client-to-server (CTS) flows. If you know that the attack signature appears in the first packet of a session, choosing first packet instead of packet reduces the amount of traffic the security device needs to monitor, which improves performance.</td>
</tr>
<tr>
<td></td>
<td>■ <strong>Stream Select</strong>—Reassembles packets and extracts the data to search for a pattern match. However, IDP does not recognize packet boundaries for stream contexts, so data for multiple packets is combined. Select this option only when no other context option contains the attack.</td>
</tr>
<tr>
<td></td>
<td>■ <strong>Stream 256</strong>—Reassembles packets and searches for a pattern match within the first 256 bytes of a traffic stream. When the flow direction is set to any, DI checks the first 256 bytes of both the STC and CTS flows. If you know that the attack signature will appear in the first 256 bytes of a session, choosing stream 256 instead of stream reduces the amount of traffic that the security device must monitor and cache, improving performance.</td>
</tr>
<tr>
<td></td>
<td>■ <strong>Line</strong>—Detects a pattern match within a specific line within your network traffic.</td>
</tr>
<tr>
<td>Direction</td>
<td>Select the direction in which to detect the attack:</td>
</tr>
<tr>
<td></td>
<td>■ <strong>Client to Server</strong>—Detects the attack only in client-to-server traffic.</td>
</tr>
<tr>
<td></td>
<td>■ <strong>Server to Client</strong>—Detects the attack only in server-to-client traffic.</td>
</tr>
<tr>
<td></td>
<td>■ <strong>Any</strong>—Detects the attack in either direction.</td>
</tr>
<tr>
<td>Flow</td>
<td>Select the flow in which to detect the attack:</td>
</tr>
<tr>
<td></td>
<td>■ <strong>Control</strong>—Detects the attack in the initial connection that is established persistently to issue commands, requests, and so on.</td>
</tr>
<tr>
<td></td>
<td>■ <strong>Auxiliary</strong>—Detects the attack in the response connection established intermittently to transfer requested data.</td>
</tr>
<tr>
<td></td>
<td>■ <strong>Both</strong>—Detects the attack in the initial and response connections.</td>
</tr>
<tr>
<td><strong>TIP:</strong></td>
<td>Using a single flow (instead of Both) improves performance and increases detection accuracy.</td>
</tr>
</tbody>
</table>

Click **Next**.

4. On the Custom Attack – IP Settings and Header Matches page, specify signature settings as described in Table 42 on page 73.
NOTE: The IP tab specifies the contents of the IP header in a malicious packet. You cannot specify IP header contents if you selected a line, stream, stream 256, or a service context in the Attack Patterns tab.

TIP: If you are unsure of the IP flags and IP fields for the malicious packet, leave all fields blank. If not values are set, IDP attempts to match the signature for all IP header contents.

Table 42: Custom Attack: IP Settings and Header Matches

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type of Service</td>
<td>Enter the service type. Common service types are:</td>
</tr>
<tr>
<td></td>
<td>■ 0000 Default</td>
</tr>
<tr>
<td></td>
<td>■ 0001 Minimize Cost</td>
</tr>
<tr>
<td></td>
<td>■ 0002 Maximize Reliability</td>
</tr>
<tr>
<td></td>
<td>■ 0003 Maximize Throughput</td>
</tr>
<tr>
<td></td>
<td>■ 0004 Minimize Delay</td>
</tr>
<tr>
<td></td>
<td>■ 0005 Maximize Security</td>
</tr>
<tr>
<td>Total Length</td>
<td>Enter the number of bytes in the packet, including all header fields and the data payload.</td>
</tr>
<tr>
<td>ID</td>
<td>Enter the unique value used by the destination system to reassemble a fragmented packet.</td>
</tr>
<tr>
<td>Time-to-live</td>
<td>Enter the time-to-live (TTL) value of the packet. This value represents the number of routers the packet can pass through. Each router that processes the packet decrements the TTL by 1; when the TTL reaches 0, the packet is discarded.</td>
</tr>
<tr>
<td>Protocol</td>
<td>Enter the protocol used in the attack.</td>
</tr>
<tr>
<td>Source</td>
<td>Specify the IP address of the attacking device.</td>
</tr>
<tr>
<td>Destination</td>
<td>Specify the IP address of the attack target.</td>
</tr>
<tr>
<td>RB</td>
<td>Reserved bit. Specifies that IDP looks for a pattern match whether or not the IP flag is set (none), only if the flag is set (set), or only if the flag is not set (unset).</td>
</tr>
<tr>
<td>MF</td>
<td>More fragments. Specifies that IDP looks for a pattern match whether or not the IP flag is set (none), only if the flag is set (set), or only if the flag is not set (unset).</td>
</tr>
<tr>
<td>DF</td>
<td>Don’t fragment. Specifies that IDP looks for a pattern match whether or not the IP flag is set (none), only if the flag is set (set), or only if the flag is not set (unset).</td>
</tr>
</tbody>
</table>

5. If you selected TCP for Service Binding and packet or first-data-packet as the Context, click the Protocols tab, select TCP packet header fields, and configure TCP Header Match settings as described in Table 43 on page 74.
### Table 43: TCP Header Match Settings

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source Port</td>
<td>The port number on the attacking device.</td>
</tr>
<tr>
<td>Destination Port</td>
<td>The port number of the attack target.</td>
</tr>
<tr>
<td>Sequence Number</td>
<td>The sequence number of the packet. This number identifies the location of the data in relation to the entire data sequence.</td>
</tr>
<tr>
<td>ACK Number</td>
<td>The ACK number of the packet. This number identifies the next sequence number; the ACK flag must be set to activate this field.</td>
</tr>
<tr>
<td>Header Length</td>
<td>The number of bytes in the TCP header.</td>
</tr>
<tr>
<td>Window Size</td>
<td>The number of bytes in the TCP window size.</td>
</tr>
<tr>
<td>Data Length</td>
<td>The number of bytes in the data payload. For SYN, ACK, and FIN packets, this field should be empty.</td>
</tr>
<tr>
<td>Urgent Pointer</td>
<td>The data in the packet is urgent; the URG flag must be set to activate this field.</td>
</tr>
<tr>
<td>URG Bit</td>
<td>When set, the urgent flag indicates that the packet data is urgent.</td>
</tr>
<tr>
<td>ACK Bit</td>
<td>When set, the acknowledgment flag acknowledges receipt of a packet.</td>
</tr>
<tr>
<td>PSH Bit</td>
<td>When set, the push flag indicates that the receiver should push all data in the current sequence to the destination application (identified by the port number) without waiting for the remaining packets in the sequence.</td>
</tr>
<tr>
<td>RST Bit</td>
<td>When set, the reset flag resets the TCP connection, discarding all packets in an existing sequence.</td>
</tr>
<tr>
<td>FIN Bit</td>
<td>When set, the final flag indicates that the packet transfer is complete and the connection can be closed.</td>
</tr>
<tr>
<td>R1 Bit, R2 Bit</td>
<td>Reserved bit. Unused.</td>
</tr>
</tbody>
</table>

6. If you selected UDP for Service Binding and packet or first-data-packet as the Context, click the Protocols tab, select UDP packet header fields, and configure UDP Header Match settings as described in Table 44 on page 74.

### Table 44: UDP Header Match Settings

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source Port</td>
<td>Enter the port number on the attacking device.</td>
</tr>
<tr>
<td>Destination Port</td>
<td>Enter the port number of the attack target.</td>
</tr>
<tr>
<td>Data Length</td>
<td>Enter the number of bytes in the data payload.</td>
</tr>
</tbody>
</table>
7. If you selected ICMP for Service Binding and packet or first-data-packet as the Context, click the Protocols tab, select ICMP packet header fields, and configure ICMP Header Match settings as described in Table 45 on page 75.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ICMP Type</td>
<td>Enter the primary code that identifies the function of the request/reply.</td>
</tr>
<tr>
<td>ICMP Code</td>
<td>Enter the secondary code that identifies the function of the request/reply within a given type.</td>
</tr>
<tr>
<td>Sequence Number</td>
<td>Enter the sequence number of the packet. This number identifies the location of the request/reply in relation to the entire sequence.</td>
</tr>
<tr>
<td>ICMP ID</td>
<td>Enter the identification number which is a unique value used by the destination system to associate requests and replies.</td>
</tr>
</tbody>
</table>

8. Click Finish.

**Related Topics**
- Attack Objects in Intrusion Detection and Prevention Security Policies Overview on page 61
- Working with Attack Groups (NSM Procedure) on page 64
- Viewing Predefined Attack Objects (NSM Procedure)
- Updating the IDP Detector Engine (NSM Procedure) on page 76

**Verifying the Attack Object Database Version (NSM Procedure)**

**Purpose**
New attack objects are added to the attack object database server frequently; downloading these updates and installing them on your managed devices regularly ensures that your network is protected against the latest threats. As new attack objects are added to the attack object database server, the version number of the database increments by 1. When you download a version of the attack object database from the server, NSM stores the version number of that database.

**Action**
Automatic Verification

The management system uses the database version number to detect and notify you when the stored attack object database on the GUI server is:
- Older than the most recent database available from the attack object database server.
- Newer than the attack object database currently installed on your ScreenOS 5.1 and later managed devices.

When NSM detects that the managed device contains an older attack object database version than the one stored on the GUI server, the UI displays a warning for that device, indicating that you should update the attack object database on the device.
**Manual Verification**

You can also check to see if the attack object database on the server is more recent than the one on the security device.

To check the attack object database version:

1. From the Device Manager, select **Security Updates > Check Attack Database Server Version**. The Check Attack Database Server Version dialog box appears.
2. Select the devices or group of devices to be checked.
3. Click **OK**. The Job Information window displays the status of the version check.

**Related Topics**

- Attack Objects in Intrusion Detection and Prevention Security Policies Overview on page 61
- Creating Custom Attack Objects (NSM Procedure) on page 67
- Loading J-Security-Center Updates (NSM Procedure) on page 62
- Viewing Predefined Attack Objects (NSM Procedure)

---

**Updating the IDP Detector Engine (NSM Procedure)**

The IDP detector engine is dynamically changeable firmware that runs on ISG security devices running ScreenOS 5.0.0-IDP1, standalone IDP sensors, J-series devices, and SRX-series devices. Automatic updates to the IDP detector engine occur when you:

- Upgrade security device firmware.
- Load a new detector engine—New detector engines may be downloaded with normal attack object updates. You must load the new detector engine onto the device.

**NOTE:** You cannot downgrade the IDP detector engine version on the device.

To update the IDP detector engine for an IDP device:

1. From the Device Manager, select **Security Updates > Update ScreenOS/IDP Device Detector**. The Load IDP Detector Engine wizard starts.
2. Click **Next**, and then follow the instructions in the wizard to update the IDP detector engine on the selected device.

**NOTE:** Updating the IDP detector engine on a device does not require a reboot of the device.

For more information, see *Network and Security Manager Administration Guide*. 
Related Topics

- Attack Objects in Intrusion Detection and Prevention Security Policies Overview on page 61
- Working with Attack Groups (NSM Procedure) on page 64
- Loading J-Security-Center Updates (NSM Procedure) on page 62
- Viewing Predefined Attack Objects (NSM Procedure)
Chapter 6
Configuring SNMP and Syslog Settings

Use Global Settings to specify syslog and SNMP servers. In device templates, find these settings under IDP Device Settings. In an individual device, find these settings under Global Settings.

This chapter includes the following topics:
- Configuring an SNMP Agent (NSM Procedure) on page 79
- Configuring Syslog Collection (NSM Procedure) on page 80

Configuring an SNMP Agent (NSM Procedure)

The IDP sensor creates and sends a log entry whenever one of the following statistics reaches 90%. It also sends a log when the value drops below 90%. Logs are sent no more than once a minute. The log entry specifies the value of the setting at the time the log is sent.

- **CPU Usage**—Log entry generated when CPU usage reaches 90%.
- **Hard Disk Usage**—Log entry generated when disk space reaches 90%.
- **Memory Usage**—Log entry generated when memory usage reaches 90%.
- **Session Count**—Log entry generated when session count reaches 90% of the total possible session count. (Maximum total session count for each device is specified on that device’s product sheet.)

These logs are generated and sent to NSM automatically. However, you can also set the sensor to send the entries to your SNMP server. To do so, enable SNMP and specify the server’s community and IP address, and then load the new configuration onto the sensor.

You configure an SNMP agent if you want to send device event logs to an SNMP server.

You have the option of configuring an SNMP agent for NSM (if you want to send the NSM collection to SNMP) or configuring an SNMP agent for each IDP device.

To configure an SNMP agent for NSM, see the NSM online Help.
To configure an SNMP agent for a single IDP device:

1. In the NSM Device Manager, double-click the IDP device to display the device configuration editor.
2. Click Report Settings.
3. Add or modify the settings in the SNMP Settings grid as described in the Table 46 on page 80.
4. Click OK.

Table 46: IDP Configuration: SNMP Settings

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable SNMP</td>
<td>Enables forwarding to a network management system that reads SNMP.</td>
</tr>
<tr>
<td>SNMP Read Only Community</td>
<td>Specifies a string. The SNMP read-only community string resembles a password used for the exchange between the IDP device and the network management system.</td>
</tr>
<tr>
<td>SNMP Manager IP</td>
<td>Specifies the IP address of the SNMP server.</td>
</tr>
<tr>
<td>SNMP Contact</td>
<td>Specifies an e-mail address for the IDP administrator contact to be included in SNMP communications. If the network management system encounters a problem with the SNMP communication, it can use the contact information to follow up.</td>
</tr>
<tr>
<td>SNMP Location</td>
<td>Specifies a location of the IDP device to be included in SNMP communications.</td>
</tr>
<tr>
<td>New SNMP allowed hosts</td>
<td>Specifies the network/host IP address and the network/host netmask for the agent.</td>
</tr>
</tbody>
</table>

Related Topics
- Configuring Syslog Collection (NSM Procedure) on page 80
- NSM Logs and Reports Overview on page 129

Configuring Syslog Collection (NSM Procedure)

You configure syslog settings if you want to forward a copy of IDP logs to a syslog server.

You have the option of configuring NSM to forward a copy of its log collection to a syslog server or configuring syslog settings for each IDP device.

To have all IDP logs sent to a Syslog server, select the check box and specify the syslog server IP address. Then load the new configuration onto the sensor.

To configure syslog forwarding for NSM, see the NSM online Help.

To configure syslog forwarding for a single IDP device:

1. In the NSM Device Manager, double-click the IDP device to display the device configuration editor.
2. Click Report Settings.
3. Select **Enable Syslog**.
4. Specify the syslog server IP address.
5. Specify whether to forward packet logs to the syslog server.
6. Click **OK**.

**Related Topics**
- NSM Logs and Reports Overview on page 129
- Viewing Logs on page 129
- Configuring an SNMP Agent (NSM Procedure) on page 79
Chapter 7

Configuring Anti-Spoof Settings

- Configuring Antispoof Settings in Intrusion Detection and Prevention Devices (NSM Procedure) on page 83
- Example: Applying Antispoof to a Web Server and Database Server (NSM Procedure) on page 84

Configuring Antispoof Settings in Intrusion Detection and Prevention Devices (NSM Procedure)

Antispoof settings are valid for standalone IDP sensors only. You can assign address objects to specific interfaces on your sensor. You can set the sensor to log or drop any connections that do not match the permitted address objects for that interface.

In addition, you can set the sensor to check incoming IP addresses against the permitted address objects for other interfaces. If the sensor detects an IP address entering the wrong interface, it can log or drop that connection.

To configure antispoof settings:
1. In NSM Device Manager, double-click the IDP device you want to configure antispoof settings. The device configuration editor appears.
2. Click Anti-Spoof Settings.
3. Click New to display the Anti-Spoof Settings dialog box.
4. Configure antispoof settings using Table 47 on page 83.
5. Click OK.

Table 47: IDP Device Configuration: Anti-Spoof Settings

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface Name</td>
<td>Select a forwarding interface to configure.</td>
</tr>
<tr>
<td>Logging</td>
<td>Enable logging for spoofed IP address.</td>
</tr>
<tr>
<td>Alarm</td>
<td>Enable alerts for spoofed IP addresses.</td>
</tr>
<tr>
<td>Check Other Interfaces</td>
<td>Indicate whether the device should check the status of other interfaces when determining spoofing.</td>
</tr>
<tr>
<td>Action</td>
<td>Specify the action for the IDP device to take: None or Drop Packet.</td>
</tr>
</tbody>
</table>
Table 47: IDP Device Configuration: Anti-Spoof Settings (continued)

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network Objects</td>
<td>Browse and select the address objects you associate with the selected interface.</td>
</tr>
</tbody>
</table>

Related Topics

- Configuring Additional Intrusion Detection and Prevention Features Overview on page 111
- Adding Intrusion Detection and Prevention Devices in NSM Overview on page 8
- NSM and Intrusion Detection and Prevention Device Management Overview on page 5

Example: Applying Antispoof to a Web Server and Database Server (NSM Procedure)

To apply antispoof settings to a Web server and a database server:

1. Add your Web server and database server to the list of address objects.
2. Connect the Web server to the Sensor through eth2. Connect the database server to the Sensor through eth4.
3. Open the device in Device Manager.
4. Click Anti-Spoof Settings.
5. Click New to add a new entry to the antispoof table. In the dialog box that opens, configure the following settings:
   a. Select eth4 as the forwarding interface for the database server.
   b. Check both the Logging and Alert check boxes because your database server is important.
   c. Select None from the Action list.
   d. Select your database server from the list of address objects.
   e. Click OK.
   f. Click New again to add your Web server.
   g. Select eth2 as the interface.
   h. Select the Logging check box.
   i. Select the Check other interfaces check box.
      If this check box is selected, the sensor compares each IP address to the list of addresses known to be assigned to other interfaces. In other words, if the database server IP address appears at this interface, you want the sensor to let you know.
   j. Select None from the Action list. You just want to log this event.
   k. Select the Web server as the address object assigned to this interface.
Related Topics

- Configuring Antispoof Settings in Intrusion Detection and Prevention Devices (NSM Procedure) on page 83
- Intrusion Detection and Prevention Services and Device Configurations Supported in NSM on page 6
Chapter 8
Configuring Intrusion Detection and Prevention Device Settings

The IDP SM and sensor settings specify how the security module(s) on the ISG Series devices and IDP sensors handle traffic. When you add IDP, default values for all security module parameters are used. As you fine-tune a security policy to fit network traffic, you may want to edit these default values. If you make changes to the default settings, the changes only affect that device to which the security module settings apply. For detailed information on fields, refer to the NSM online Help or the IDP Concepts and Examples Guide.

- Configuring Load-Time Parameters (NSM Procedure) on page 87
- Configuring Run-Time Parameters (NSM Procedure) on page 88
- Configuring Router Parameters (NSM Procedure) on page 94
- Configuring Protocol Handling (NSM Procedure) on page 95

Configuring Load-Time Parameters (NSM Procedure)

Load-time parameters include options for tuning IDP performance. In general, you modify these settings only if you encounter performance issues. These options control the security module functions when it first powers on.

To configure load-time parameters:

1. In NSM Device Manager, double-click the IDP device for which you want to configure load-time parameters. The device configuration editor appears.
2. Click Sensor Settings.
3. Click the Load Time Parameters tab.
4. Configure load-time parameters using Table 48 on page 88.
5. Click Apply.
6. Click OK.
Table 48: IDP Device Configuration: Load Time Parameters

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Flow table size (requires sensor restart)</td>
<td>For improved IDP performance, set the flow table size to limit the size of the connection table. This setting should reflect the maximum number of concurrent flows you expect to have at any one time. A TCP connection has about two flows per session, and a UDP connection has about three flows per session. The default setting is 100,000 concurrent flows. If you change this value, you have to restart the IDP device.</td>
</tr>
<tr>
<td>Enable log suppression</td>
<td>Log suppression reduces the number of logs displayed in the Log Viewer by displaying a single record for multiple occurrences of the same event. NOTE: If the reporting interval is set too high, log suppression can negatively impact IDP performance.</td>
</tr>
<tr>
<td>Include destination IP’s while performing log suppression</td>
<td>When log suppression is enabled, multiple occurrences of events with the same source IP, service, and matching attack object generate a single log record with a count of occurrences. If you enable this option, log suppression combines log records for events with the same destination IP.</td>
</tr>
<tr>
<td>Number of log occurrences after which log suppression begins</td>
<td>This number represents the number of identical log records received before suppression starts. The default is 1 (meaning log suppression begins with the first redundancy).</td>
</tr>
<tr>
<td>Maximum number of logs that log suppression can operate on</td>
<td>When log suppression is enabled, IDP must cache log records so that it can identify when multiple occurrences of the same event occur. This number represents the number of log records in the IDP management server that IDP tracks for log suppression. The default is 16,384 log records.</td>
</tr>
<tr>
<td>Time (seconds) after which suppressed logs will be reported</td>
<td>When log suppression is enabled, the IDP device maintains a count of multiple occurrences of the same event. This number represents the number of seconds that pass before IDP reports a single log entry containing the count of occurrences. The default is 10 seconds.</td>
</tr>
<tr>
<td>Enable application identification</td>
<td>The application identification feature is used to detect the session application regardless of port. We recommend you disable this feature only when troubleshooting.</td>
</tr>
<tr>
<td>Maximum number of Application Identification sessions</td>
<td>Specifies the maximum number of sessions where application identification is in use. The default is 100,000. Valid values are 0 - 200,000. We recommend you tune this setting only if you encounter issues.</td>
</tr>
<tr>
<td>Enable policy sharing</td>
<td>This option allows two CPUs on a security module to share a policy. This enables the policy with all attacks to withhold maximum memory. Also the memory usage increases while the attacks database grows.</td>
</tr>
</tbody>
</table>

**Related Topics**
- Pushing Security Policy Updates to an IDP Device (NSM Procedure) on page 119
- Troubleshooting Configuration Push Errors (NSM Procedure) on page 121
- Configuring Run-Time Parameters (NSM Procedure) on page 88

**Configuring Run-Time Parameters (NSM Procedure)**

Run-time parameters include options for tuning IDP detection methods. In general, you modify these settings only if you encounter false positives or performance issues. These options control the security module operations.
To configure run-time parameters:

1. In NSM Device Manager, double-click the IDP device for which you want to configure run-time parameters. The device configuration editor appears.

2. Click Sensor Settings.

3. Click the Run-time Parameters tab.

4. Configure run-time settings using Table 49 on page 89.

5. Click Apply.

6. Click OK.

### Table 49: IDP Device Configuration: Run-Time Parameters

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Backdoor Detection</td>
<td><strong>Minimum interval between consecutive small packets (microseconds)</strong> / <strong>Maximum interval between consecutive small packets (microseconds)</strong>—Controls the minimum and maximum intervals (in microseconds) between the arrival of two consecutive small packets in suspected interactive traffic. If the IDP device sees small packets arrive in less than the minimum or more than the maximum number of microseconds, it does not consider the traffic to be interactive. The defaults are 20,000 and 2,00,000. This means that consecutive small packets must arrive within 20,000 to 2,00,000 microseconds to be considered interactive.</td>
</tr>
<tr>
<td>Byte threshold for packet sizes in a backdoor connection—Controls the maximum number of bytes a TCP packet must contain before the IDP device uses the packet for backdoor detection heuristics. The default is 20 bytes.</td>
<td></td>
</tr>
<tr>
<td>Minimum number of data carrying TCP packets—Controls the minimum number of data-carrying TCP packets in suspected interactive traffic. The default is 20 packets.</td>
<td></td>
</tr>
<tr>
<td>Minimum percentage of back-to-back small packets—Controls the minimum percentage of consecutive small packets in suspected interactive traffic. If the IDP device sees less than this percentage, it does not report a backdoor event. The default is 20%.</td>
<td></td>
</tr>
<tr>
<td>Ratio of small packets to the total packets (percentage)—Controls the minimum percentage of small packets that the IDP device uses for backdoor detection heuristics. If the IDP device sees less than this minimum, it does not report a backdoor event. The default is 20%.</td>
<td></td>
</tr>
</tbody>
</table>
### Table 49: IDP Device Configuration: Run-Time Parameters (continued)

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Flow Management</strong></td>
<td><strong>Timeout (seconds) for non-UDP/TCP/ICMP flows</strong>—Each connection through the security module typically has two non-UDP/TCP/ICMP flows, one in each direction. If IDP does not see flow activity for the specified timeout, it removes the idle flow from the flow table. The default is 30 seconds.</td>
</tr>
<tr>
<td></td>
<td><strong>Timeout (seconds) for UDP flows</strong>—Each connection through the security module typically has two UDP flows, one in each direction. If IDP does not see flow activity for the specified timeout, it removes the idle flow from the flow table. The default is 30 seconds.</td>
</tr>
<tr>
<td></td>
<td><strong>Timeout (seconds) for TCP flows</strong>—Each connection through the security module typically has two TCP flows, one in each direction. If IDP does not see flow activity for the specified timeout, it removes the idle flow from the flow table. The default is 30 seconds.</td>
</tr>
<tr>
<td></td>
<td><strong>Timeout (seconds) for ICMP flows</strong>—Each connection through the security module typically has two ICMP flows, one in each direction. If IDP does not see flow activity for the specified timeout, it removes the idle flow from the flow table. The default is 30 seconds.</td>
</tr>
<tr>
<td></td>
<td><strong>Maximum TCP Sessions</strong>—Controls the maximum number of TCP sessions that IDP maintains. If IDP reaches the maximum, it drops all new sessions and writes a SESSION_LIMIT_EXCEEDED log. Defaults vary according to model.</td>
</tr>
<tr>
<td></td>
<td><strong>Maximum UDP Sessions</strong>—Controls the maximum number of UDP sessions that IDP maintains. If IDP reaches the maximum, it drops all new sessions and writes a SESSION_LIMIT_EXCEEDED log. Defaults vary according to model.</td>
</tr>
<tr>
<td></td>
<td><strong>Maximum ICMP Sessions</strong>—Controls the maximum number of ICMP sessions that IDP maintains. If IDP reaches the maximum, it drops all new sessions and writes a SESSION_LIMIT_EXCEEDED log. Defaults vary according to model.</td>
</tr>
<tr>
<td></td>
<td><strong>Maximum IP (non-UDP/TCP/ICMP) sessions</strong>—Controls the maximum number of IP sessions that IDP maintains. If IDP reaches the maximum, it drops all new sessions and writes a SESSION_LIMIT_EXCEEDED log. Defaults vary according to model.</td>
</tr>
<tr>
<td><strong>IP Actions</strong></td>
<td><strong>Reset block table with policy load/unload</strong>—Allows the IDP device to reset the block table. The block table maintains the state of active IP actions each time a security policy loads or unloads. This setting is enabled by default.</td>
</tr>
<tr>
<td><strong>Log flow related errors</strong></td>
<td>Enables logging for flow-related errors. This setting is not enabled by default.</td>
</tr>
</tbody>
</table>

### Table 49: IDP Device Configuration: Run-Time Parameters *(continued)*

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
</table>
| Intrusion Detection      | **Buffer Overflow emulator** – Turns on buffer overflow emulation. \[ Attack matches per packet when Signature Hierarchy (0 to disable) take effect **– Sets the threshold for activating Signature Hierarchy calculations.** \]

Common attack can be composed of several known vulnerabilities. Each vulnerability has an attack object, and each would generate a separate log entry if the signature hierarchy feature were disabled.

For example, for a policy with critical, high, medium, low, and info attacks and logging enabled, a single detection of HTTP:IIS:COMMAND-EXEC attack generates the following logs:

- HTTP:IIS:COMMAND-EXEC [wininnt\system32\cmd.exe] (medium)
- HTTP:WIN-CMD:WIN-CMD-EXE [cmd.exe] (medium)
- HTTP:REQERR:REQ-MALFORMED-URL [anomaly for %xx] (medium)
- HTTP:DIR:TRAVERSE-DIRECTORY (anomaly for ..) (medium)
- HTTP:REQERR:REQ-LONG-UTF8CODE (anomaly for oe) (medium)
- TCP:AUDIT:BAD-SYN-NONSYN (info)
- HTTP:AUDIT:URL (info)
- TCP:AUDIT:BAD-SYN-NONSYN (info)

If the number of attacks in a packet exceeds the set value, then IDP examines its signature hierarchy to see if some attacks are actually part of a larger attack. If so, then only the parent attack is displayed in the logs. In this example, if the value was set to 9 or lower, then only a log for HTTP:IIS:COMMAND-EXEC would be generated.

An attack in the signature hierarchy may have multiple parents or multiple children. If a child attack is part of two discovered parents, IDP takes action based on the parent with the highest severity.

Specify 0 to disable.
<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Run-time Parameters</td>
<td><strong>RPC program timeout (seconds)</strong>—IDP performs a stateful inspection of all RPC messages on port 111, then builds a table of program-to-port mapping for each RPC server that it finds on the network. This setting indicates how long an entry in the table is maintained. The default is 300 seconds.</td>
</tr>
<tr>
<td></td>
<td><strong>RPC transaction timeout (Seconds)</strong>—All RPC messages (port 111) are based on a request/response protocol. When the IDP receives a request, it adds the request to a request table. If IDP does not receive an RPC reply in the specified timeout, the RPC entry times out. The default is 5 seconds.</td>
</tr>
<tr>
<td></td>
<td><strong>Exempt management server flows</strong>—Exempts NSM connections from IDP processing. This setting is enabled by default.</td>
</tr>
<tr>
<td></td>
<td><strong>Fragment timeout (seconds)</strong>—Controls when IDP drops an incomplete fragment chain because one or more fragments did not arrive. If IDP does not receive missing fragments in the specified timeout, it generates a log (FRAGMENT_TIME_EXCEEDED). The default is 5 seconds.</td>
</tr>
<tr>
<td></td>
<td><strong>Minimum fragment size (bytes)</strong>—IDP drops all IP fragments less than the specified size (bytes). The default is 0 bytes (no fragments are dropped).</td>
</tr>
<tr>
<td></td>
<td><strong>Maximum fragments per IP datagram</strong>—An IP datagram can be broken into many fragments which, when assembled, should not exceed 64 K. Because IP fragment processing is CPU and memory intensive, this setting controls the size of the IP fragment chain. If the number of fragments in a chain exceeds this number, IDP drops the entire fragment chain. The default is 65,535 bytes.</td>
</tr>
<tr>
<td></td>
<td><strong>Maximum concurrent fragments in queue</strong>—IDP can perform pseudo reassembly of IP fragment chains. This setting controls the maximum number of reassembled fragment chains. Once this limit is reached, IDP drops all new IP fragment chains and generates a log (TOO_MANY_FRAGMENTS). If your network produces a large number of IP fragments, such as those produced by Network File System (NFS), increase the number of fragments per chain to eliminate unnecessary logs. The default is 16 fragments.</td>
</tr>
<tr>
<td></td>
<td><strong>Log fragment related errors</strong>—Logs fragment related errors. This setting is not enabled by default.</td>
</tr>
<tr>
<td></td>
<td><strong>Enable GRE decapsulation support</strong>—Enables IDP to decode generic routing encapsulation (GRE) tunnels where IP-in-GRE or PPP-in-GRE encapsulation is used. This allows IDP to inspect the packet in its original form. GRE decapsulation is not enabled by default.</td>
</tr>
<tr>
<td></td>
<td><strong>Enable GTP decapsulation support</strong>—Enables GPRS Tunneling Protocol (GTP) decapsulation. IDP supports decapsulation of UDP GTPv0 and GTPv1 only. GTP decapsulation is not enabled by default.</td>
</tr>
<tr>
<td></td>
<td><strong>Enable SSL decryption support</strong>—Enables SSL inspection. SSL decryption is not enabled by default.</td>
</tr>
</tbody>
</table>
### Table 49: IDP Device Configuration: Run-Time Parameters (continued)

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>SYN Protector</strong></td>
<td><strong>Timeout for half-open SYN protected flows</strong>—A half-open SYN flow occurs during the TCP three-way handshake, after the client has sent a SYN/ACK packet to the server. The half-open connection is now in the SYN_RECV state, and is placed into a connection queue while it waits for an ACK or RST packet. The connection remains in the queue until the connection-establishment timeout expires and the half-open connection is deleted. This setting controls the connection establishment timer, which determines the number of seconds that the security module maintains a half-open SYN protected flow. The default is 5 seconds.</td>
</tr>
<tr>
<td></td>
<td><strong>Lower SYN’s-per-second threshold below which SYN Protector will be deactivated</strong> / <strong>Upper SYN’s-per-second threshold above which SYN Protector will be activated</strong>—The SYN Protector rulebase is activated when the number of SYN packets per second is greater than the sum of the lower SYNs-per-second threshold and the upper SYNs-per-second threshold.</td>
</tr>
<tr>
<td></td>
<td>The SYN Protector rulebase is deactivated when the number of SYN packets per second is less than the lower SYNs-per-second threshold.</td>
</tr>
<tr>
<td></td>
<td>The defaults are 1000 and 20. The SYN Protector is activated when SYNs-per-second reach 1020 and deactivated when SYNs-per-second fall below 1000.</td>
</tr>
<tr>
<td><strong>TCP Reassembler</strong></td>
<td><strong>Ignore packets in TCP flows where a SYN hasn’t been seen (recommended)</strong>—The absence of SYN flags in TCP flows is suspect, yet still a very common occurrence. IDP can ignore packets within TCP flows that do not yet contain a SYN flag. This is enabled by default.</td>
</tr>
<tr>
<td></td>
<td><strong>Close flows as soon as a FIN is seen</strong>—Enables when a TCP connection closes, IDP sees a FIN packet from each side of the connection followed by an ACK packet from each side of the connection. However, TCP does not guarantee delivery of the final ACK.</td>
</tr>
<tr>
<td></td>
<td>Enables IDP to quickly close a TCP connection after receiving a FIN packet. When enabled, IDP maintains a connection waiting for a final ACK for 5 seconds, then closes the connection. This is enabled by default and recommended.</td>
</tr>
<tr>
<td></td>
<td><strong>Timeout for connected, idle TCP flows (seconds)</strong>—Controls the number of seconds that IDP maintains connected (but idle) TCP flows. The default is 3600 seconds.</td>
</tr>
<tr>
<td></td>
<td><strong>Timeout for closed TCP flows (seconds)</strong>—Controls when IDP sees a RST packet or FIN/FIN+ACK packets on a TCP connection, it closes the connection flows. IDP drops any further packets for the closed flow, but does not delete existing, closed flows from the flow table. Controls the number of seconds that closed TCP flows are maintained in the flow table. The default is 5 seconds.</td>
</tr>
<tr>
<td></td>
<td><strong>Timeout for CLOSE-WAIT/LAST-ACK TCP flows (seconds)</strong>—Controls when a TCP connection closes, IDP sees a FIN packet from each side of the connection followed by an ACK packet from each side of the connection. However, TCP does not guarantee delivery of the final ACK.</td>
</tr>
<tr>
<td></td>
<td>Controls the number of seconds a connection is maintained while waiting for the final ACK.</td>
</tr>
<tr>
<td></td>
<td>To improve IDP performance during heavy loads, decrease the timeout—this reduces the size of the flow table by closing connections sooner. The default is 120 seconds.</td>
</tr>
</tbody>
</table>
Table 49: IDP Device Configuration: Run-Time Parameters (continued)

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Traffic Signatures</td>
<td><strong>Byte threshold for suspicious flows</strong>—Specifies a threshold for what IDP considers a small packet. A scan typically uses small packets to access its targets. You can exclude suspicious flows that contain large packets to prevent false positives when detecting scans. If IDP sees more than this maximum, it does not consider the connection to be a scan. The default is 20 bytes.</td>
</tr>
<tr>
<td><strong>Reporting frequency when scan is in progress</strong>—Controls how often IDP generates &quot;in progress&quot; logs for a stealthy scan. Attackers can perform blatant scans very quickly, mapping your network in just a few seconds, but these scans typically trigger IDSes and leave evidence behind. Stealthy scans are performed over much longer time periods, lasting hours, days, or even weeks, making them more difficult to detect. The default is 30 seconds.</td>
<td></td>
</tr>
<tr>
<td><strong>The number of IP tracked for session rate</strong>—Controls the number of IP addresses tracked by the session rate counter. If IDP sees more addresses than the maximum, it does not track the additional IP addresses. The default is 32,767 IP addresses.</td>
<td></td>
</tr>
</tbody>
</table>

**Related Topics**
- Updating the IDP Detector Engine (NSM Procedure) on page 76
- Configuring SYN Protector Rulebase Rules (NSM Procedure) on page 48
- Configuring Router Parameters (NSM Procedure) on page 94

**Configuring Router Parameters (NSM Procedure)**

Router parameters control how the security module handles address resolution protocol (ARP) requests/replies and media access control (MAC) address issues. These settings apply to proxy-ARP and bridge mode deployments. These options control packet handling for specific protocols. Use these options to control IDP Sensor routing, if applicable.

To configure router parameters:
1. In NSM Device Manager, double-click the IDP device for which you want to configure router parameters. The device configuration editor appears.
2. Click **Sensor Settings**.
3. Click the **Router Parameters** tab.
4. Configure the router parameters using Table 50 on page 95.
5. Click **Apply**.
6. Click **OK**.
Table 50: IDP Device Configuration: Router Parameter Settings

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ARP timeout (seconds)</td>
<td>When the virtual router is in proxy-ARP mode, this setting controls how long an ARP entry is maintained in the virtual router. If IDP does not receive an ARP reply before the timeout expires, the ARP entry times out. The default is 3600 seconds.</td>
</tr>
<tr>
<td>ARP proxy timeout (seconds)</td>
<td>In proxy-ARP mode, IDP sends out proxy ARPs on all interfaces except the one on which an ARP request was received. This setting indicates how long the original ARP entry is maintained in the virtual router if IDP does not receive an ARP reply through that interface. The default is 20 seconds.</td>
</tr>
<tr>
<td>Log ARP attacks</td>
<td>When selected, IDP detects and logs all spoofed ARP requests/replies and other ARP anomalies. This setting is enabled by default.</td>
</tr>
<tr>
<td>MAC timeout (seconds)</td>
<td>When the virtual router is in bridge mode, this setting controls how long a MAC entry is maintained in the virtual router. The default is 3600 seconds.</td>
</tr>
<tr>
<td>MAC proxy timeout (seconds)</td>
<td>In bridge mode, IDP performs MAC discovery if the target MAC address is not in its MAC table. This setting controls how long the entry is maintained in the virtual router until a reply comes back. The default is 20 seconds.</td>
</tr>
</tbody>
</table>

Related Topics
- Configuring Protocol Handling (NSM Procedure) on page 95
- Configuring Load-Time Parameters (NSM Procedure) on page 87

Configuring Protocol Handling (NSM Procedure)

The protocol anomaly detection methods identify traffic that deviates from RFC specifications. In general, you modify protocol thresholds and configuration settings only if you encounter false positives or performance issues.

To tune protocol anomaly detection thresholds:
1. In NSM Device Manager, double-click the IDP device that you want to modify. The device configuration editor appears.
2. Click Sensor Settings.
3. Click the Protocol Thresholds and Configuration tab.
4. Configure the protocol thresholds using Table 51 on page 96.
5. Click Apply.
6. Click OK.
### Table 51: IDP Device Configuration: Protocol Thresholds and Configuration Settings

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AIM</td>
<td><strong>Maximum header length</strong>—Raises a protocol anomaly if IDP detects a header containing more bytes than the specified maximum. The default is 10,000 bytes.</td>
</tr>
<tr>
<td></td>
<td><strong>Maximum type-length-value length</strong>—Raises a protocol anomaly if IDP detects an AIM/ICQ type-length-value (TLV) containing more bytes than the specified maximum. A TLV is a tuple used for passing typed information to the protocol. The default is 8000 bytes.</td>
</tr>
<tr>
<td></td>
<td><strong>Maximum inter-client-message-block length</strong>—Raises a protocol anomaly if IDP detects an AIM/ICQ inter-client-message-block (ICMB) containing more bytes than the specified maximum. The default is 2000 bytes.</td>
</tr>
<tr>
<td></td>
<td><strong>Maximum filename length</strong>— Raises a protocol anomaly if IDP detects an AIM/ICQ file name containing more bytes than the specified maximum. The default is 10,000 bytes.</td>
</tr>
<tr>
<td>DHCP</td>
<td><strong>Check to see if the source port of client’s packets is 68</strong>— Raises a protocol anomaly if IDP detects DHCP traffic that originates from a port other than 68. This setting is not enabled by default.</td>
</tr>
<tr>
<td>DNS</td>
<td><strong>Report unknown DNS parameters (high noise)</strong>—Detects and reports unknown DNS parameters. You must also configure an IDP rulebase rule to detect DNS anomalies. This setting is not enabled by default.</td>
</tr>
<tr>
<td></td>
<td><strong>Report unexpected DNS parameters (high noise)</strong>—Detects and reports unexpected DNS parameters. This setting is not enabled by default.</td>
</tr>
<tr>
<td></td>
<td><strong>Maximum length of a DNS UDP packet</strong>— Raises a protocol anomaly if IDP detects a DNS UDP packet containing more bytes than the specified maximum. The default is 512 bytes.</td>
</tr>
<tr>
<td></td>
<td><strong>Maximum size of a NXT resource record</strong>— Raises a protocol anomaly if IDP detects an NXT resource record in a DNS request or response message of a greater size. The default is 4096 bytes.</td>
</tr>
<tr>
<td></td>
<td>This setting tunes the following protocol anomaly attack object: DNS_BIND_NXT_OVERFLOW (key is DNS:OVERFLOW:NXT-OVERFLOW).</td>
</tr>
<tr>
<td></td>
<td><strong>Maximum time of a dns cache</strong>— Controls the maximum amount of time for a DNS query and reply. The default is 60 seconds.</td>
</tr>
<tr>
<td></td>
<td><strong>Maximum number of logs in a session</strong>—Controls the maximum number of DNS queries kept to match a reply. The default is 1000 queries.</td>
</tr>
</tbody>
</table>
Table 51: IDP Device Configuration: Protocol Thresholds and Configuration Settings (continued)

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>FTP</td>
<td>Maximum Line length–Raises a protocol anomaly if IDP detects an FTP username containing more bytes than the specified maximum. The default is 32 bytes.</td>
</tr>
<tr>
<td></td>
<td>Maximum Username length–Raises a protocol anomaly if IDP detects an FTP password containing more bytes than the specified maximum. The default is 64 bytes.</td>
</tr>
<tr>
<td></td>
<td>Maximum Password length – Raises a protocol anomaly if IDP detects an FTP pathname containing more bytes than the specified maximum. The default is 512 bytes.</td>
</tr>
<tr>
<td></td>
<td>Maximum Pathname length– Raises a protocol anomaly if IDP detects an FTP pathname containing more bytes than the specified maximum. The default is 512 bytes.</td>
</tr>
<tr>
<td></td>
<td>Maximum Sitestring length – Raises a protocol anomaly if IDP detects an FTP sitestring containing more bytes than the specified maximum. The default is 512 bytes.</td>
</tr>
<tr>
<td></td>
<td>Maximum number of login failures per-minute– Raises a protocol anomaly if IDP detects more FTP login failures in one minute than the specified maximum. The default is 4 FTP login failures per minute.</td>
</tr>
<tr>
<td>GNUTELLA</td>
<td>Maximum TTL hops– Raises a protocol anomaly if IDP detects a number of TTL hops that is higher than the specified maximum. The default is 8 TTL hops.</td>
</tr>
<tr>
<td></td>
<td>Maximum Line length– Raises a protocol anomaly if IDP detects, in a Gnutella connection, a line that contains more bytes than the specified maximum. The default is 2048 bytes.</td>
</tr>
<tr>
<td></td>
<td>Maximum Query size– Raises a protocol anomaly if IDP detects a Gnutella client query that contains more bytes than the specified maximum. The default is 256 bytes.</td>
</tr>
<tr>
<td>GOPHER</td>
<td>Maximum line length – Raises a protocol anomaly if IDP detects, in a Gopher server-to-client connection, a line sent by a Gopher server to a client that contains more bytes than the specified maximum. The default is 512 bytes.</td>
</tr>
<tr>
<td></td>
<td>Maximum hostname length– Raises a protocol anomaly if IDP detects, in a Gopher server-to-client connection, a hostname that contains more bytes than the specified maximum. The default is 64 bytes.</td>
</tr>
</tbody>
</table>
Table 51: IDP Device Configuration: Protocol Thresholds and Configuration Settings (continued)

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP Maximum Request length</td>
<td>Raises a protocol anomaly if IDP detects an HTTP request that contains more bytes than the specified maximum. The default is 8192 bytes.</td>
</tr>
<tr>
<td>HTTP Maximum Header length</td>
<td>Raises a protocol anomaly if IDP detects an HTTP header that contains more bytes than the specified maximum. The default is 8192 bytes.</td>
</tr>
</tbody>
</table>
| HTTP Maximum Cookie length       | Raises a protocol anomaly if IDP detects a cookie that contains more than the specified maximum. The default is 8192 bytes.  
Cookies that exceed the cookie length setting can match the protocol anomaly "r:HTTP-HEADER-OVERFLOW" and produce unnecessary log records. If you are getting too many log records for the HTTP-HEADER-OVERFLOW protocol anomaly, increase the maximum cookie length. |
| HTTP Maximum Authorization length| Raises a protocol anomaly if IDP detects an HTTP header authorization line that contains more bytes than the specified maximum. The default is 512 bytes.  
Use this setting to tune results from the Auth Overflow attack object (key is HTTP-OVERFLOW:AUTH-OVFLW). |
| HTTP Maximum Content-type length | Raises a protocol anomaly if IDP detects an HTTP header content-type that contains more bytes than the specified maximum. The default is 512 bytes. |
| HTTP Maximum User-agent length   | Raises a protocol anomaly if IDP detects an HTTP header user-agent that contains more bytes than the specified maximum. The default is 256 bytes. |
| HTTP Maximum Host length         | Raises a protocol anomaly if IDP detects an HTTP header host that contains more bytes than the specified maximum. The default is 64 bytes. |
| HTTP Maximum Referrer length     | Raises a protocol anomaly if IDP detects an HTTP header referrer that contains more bytes than the specified maximum. The default is 8192 bytes.  
Use alternate ports as http service—If selected, the security module watches for HTTP traffic on the following ports in addition to tcp/80: 7001; 8000; 8001; 8100; 8200; 8080; 8888; 9080. This setting is enabled by default. |
| ICMP Maximum Packets per second to trigger a flood | Raises a protocol anomaly if IDP detects more ICMP packets than the specified maximum. The default is 250 packets per second. |
| ICMP Minimum time interval (in seconds) between packets | Raises a protocol anomaly if IDP detects ICMP packets that have less than the specified minimum time interval between them. The default is 1 second.  
Use this setting to tune the Flood attack object (ICMP:EXPLOIT:FLOOD). |
<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IDENT</td>
<td><strong>Maximum requests per session</strong>—Raises a protocol anomaly if IDP detects more IDENT (identification protocol) requests than the specified maximum. The default is 1 request per session.</td>
</tr>
<tr>
<td></td>
<td>This setting tunes the Too Many Requests attack object (key is IDENT:OVERFLOW:REQUEST-NUM).</td>
</tr>
<tr>
<td></td>
<td><strong>Maximum Request length</strong>—Raises a protocol anomaly if IDP detects an IDENT request containing more bytes than the specified maximum. The default is 15 bytes.</td>
</tr>
<tr>
<td></td>
<td>This setting tunes the Request Too Long attack object (key is IDENT:OVERFLOW:REQUEST).</td>
</tr>
<tr>
<td></td>
<td><strong>Maximum Reply length</strong>—Raises a protocol anomaly if IDP detects an IDENT reply containing more bytes than the specified maximum. The default is 128 bytes.</td>
</tr>
<tr>
<td></td>
<td>This setting tunes the Reply Too Long attack object (key is IDENT:OVERFLOW:REPLY).</td>
</tr>
<tr>
<td>IKE</td>
<td><strong>Maximum number of payloads in an IKE message</strong>—Raises a protocol anomaly if IDP detects an IKE message with a higher number of payloads. The default is 57 payloads.</td>
</tr>
<tr>
<td></td>
<td>This setting tunes detection with the TOO-MANY-PAYLOADS attack object (key is IKE:MALFORMED:2MANY-PAYLOAD).</td>
</tr>
<tr>
<td>IMAP</td>
<td><strong>Maximum Line length</strong>—Raises a protocol anomaly if IDP detects an IMAP line containing more bytes than the maximum. The default is 2048 bytes.</td>
</tr>
<tr>
<td></td>
<td><strong>Maximum Username length</strong>—Raises a protocol anomaly if IDP detects an IMAP username containing more bytes than the maximum. The default is 64 bytes.</td>
</tr>
<tr>
<td></td>
<td><strong>Maximum Password length</strong>—Raises a protocol anomaly if IDP detects an IMAP password containing more bytes than the specified maximum. The default is 64 bytes.</td>
</tr>
<tr>
<td></td>
<td><strong>Maximum Mailbox length</strong>—Raises a protocol anomaly if IDP detects an IMAP mailbox containing more than the maximum. The default is 64 bytes.</td>
</tr>
<tr>
<td></td>
<td><strong>Maximum Reference length</strong>—Raises a protocol anomaly if IDP detects an IMAP reference containing more bytes than the specified maximum. The default is 64 bytes.</td>
</tr>
<tr>
<td></td>
<td><strong>Maximum Flag length</strong>—Raises a protocol anomaly if IDP detects an IMAP flag containing more bytes than the specified maximum. The default is 64 bytes.</td>
</tr>
<tr>
<td></td>
<td><strong>Maximum Literal length</strong>—Raises a protocol anomaly if IDP detects a literal with more octets than the specified maximum. In IMAP4 protocol, a string can be in one of two forms: literal and quoted. As defined in RFC 2060 4.3, a literal is a sequence of zero or more octets (including CR and LF), prefix-quoted with an octet count in the form of an open brace (&quot;{&quot;), the number of octets, close brace (&quot;}&quot;), and CRLF. Valid range is 1 to 1,67,77,215. The default is 65,535 bytes.</td>
</tr>
<tr>
<td></td>
<td>This setting tunes detection with the imap_literal_length_overflow attack object (key is IMAP:OVERFLOW:LIT_LENGTH_OVERFLOW).</td>
</tr>
<tr>
<td></td>
<td><strong>Maximum number of login failures per-minute</strong>—Raises a BRUTE_FORCE protocol anomaly if IDP detects more login failures than the maximum. The default is 4 IMAP login failures per minute.</td>
</tr>
</tbody>
</table>
Table 51: IDP Device Configuration: Protocol Thresholds and Configuration Settings *(continued)*

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IRC</td>
<td><strong>Maximum Password length</strong> – Raises a protocol anomaly if IDP detects an Internet Relay Chat (IRC) password containing more bytes than the specified maximum. The default is 16 bytes.</td>
</tr>
<tr>
<td>IRC</td>
<td><strong>Maximum Username length</strong> – Raises a protocol anomaly if IDP detects an IRC username containing more bytes than the specified maximum. The default is 16 bytes.</td>
</tr>
<tr>
<td>IRC</td>
<td><strong>Maximum Channel length</strong> – Raises a protocol anomaly if IDP detects an IRC channel name containing more bytes than the specified maximum. The default is 64 bytes.</td>
</tr>
<tr>
<td>IRC</td>
<td><strong>Maximum Nickname length</strong> – Raises a protocol anomaly if IDP detects an IRC nickname containing more bytes than the specified maximum. The default is 16 bytes.</td>
</tr>
<tr>
<td>Setting</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>LDAP</strong></td>
<td><strong>Maximum length of Integer representation in BER encoding</strong>—Raises a protocol anomaly if IDP detects an integer field of the LDAP BER containing more bytes than the specified maximum. The default is 4 bytes.</td>
</tr>
<tr>
<td></td>
<td><strong>Maximum number of left zeros for tag in BER encoding</strong>—Raises a protocol anomaly if IDP detects more left zeros in any tag in LDAP BER encoding than the specified maximum. The default is 4 left zeros.</td>
</tr>
<tr>
<td></td>
<td><strong>Maximum value of any LDAP tag in BER encoding</strong>— Raises a protocol anomaly if IDP detects a value for a tag that can be seen in the LDAP BER encoding that is greater than the specified maximum. LDAP tags are represented using 1 byte, with the top 3 bits reserved. The default is 31.</td>
</tr>
<tr>
<td></td>
<td><strong>Maximum number of left zeros for length in BER encoding</strong>— Raises a protocol anomaly if IDP detects more left zeros in any length field in LDAP BER encoding than the specified maximum. The default is 64 left zeros.</td>
</tr>
<tr>
<td></td>
<td><strong>Maximum number of search results requested by LDAP client</strong>— Raises a protocol anomaly if IDP detects an LDAP client request for more matching entries than the specified maximum. The default is 0 (indicating no limit).</td>
</tr>
<tr>
<td></td>
<td><strong>Maximum timelimit for search result requested by LDAP client</strong>— Raises a protocol anomaly if IDP detects a time limit greater than the specified maximum. The time limit is the number of seconds before a client request times out waiting for a response from the server. The default is 0 (indicating no limit).</td>
</tr>
<tr>
<td></td>
<td><strong>Maximum length of an LDAP Attribute Descriptor</strong>— Raises a protocol anomaly if IDP detects a length of an attribute descriptor field in an LDAP message containing more bytes than the specified maximum. The default is 512 bytes.</td>
</tr>
<tr>
<td></td>
<td><strong>Maximum length of an LDAP Distinguished Name</strong>— Raises a protocol anomaly if IDP detects a length of a distinguished name field in the LDAP message containing more bytes than the specified maximum. The default is 512 bytes.</td>
</tr>
<tr>
<td></td>
<td><strong>Maximum value of Message ID in any LDAP Message</strong>— Raises a protocol anomaly if IDP detects a message ID greater than the specified maximum. The default is 2,14,74,83,647.</td>
</tr>
<tr>
<td></td>
<td><strong>Maximum length of an LDAP message</strong>— Raises a protocol anomaly if IDP detects a LDAP message that will be processed by the LDAP subsystem larger than the specified maximum. The default is 8100 bytes.</td>
</tr>
<tr>
<td></td>
<td>This setting tunes the MESSAGE_TOO_LONG attack object. If IDP raises this anomaly, it logs the event and skips the message.</td>
</tr>
<tr>
<td></td>
<td><strong>Maximum number of nested operators in an LDAP search request</strong>— Raises a protocol anomaly if IDP detects a number of nested levels allowed in an LDAP search request filter argument greater than the specified maximum. The default is 8 nested operators.</td>
</tr>
<tr>
<td></td>
<td><strong>Maximum Number of login failures per-minute</strong>— Raises a BRUTE_FORCE protocol anomaly if IDP detects more login failures than the maximum. The default is 4 LDAP login failures per minute.</td>
</tr>
</tbody>
</table>
Table 51: IDP Device Configuration: Protocol Thresholds and Configuration Settings (continued)

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>LPR</strong></td>
<td><strong>Maximum Sub-command length in RECEIVE-JOB Command</strong>—Raises a protocol anomaly if IDP detects in an Line Printer Protocol (LPR) control file a sub command line containing more bytes than the specified maximum. LPR is a TCP-based print server protocol used by line printer daemons (client and server) to communicate over networks. An LPR client uses the LPR protocol to send a print command to an LPR server (a line printer) at TCP/515. After the print command is received by the server, the client can issue subcommands to the server and send control and data files. Control files tell the line printer which functions to perform when printing the file; data files carry the payload. The default is 256 bytes.</td>
</tr>
<tr>
<td><strong>Maximum Reply length from server</strong>— Raises a protocol anomaly if IDP detects an LPR control filename containing more bytes than the specified maximum. The default is 64 bytes.</td>
<td></td>
</tr>
<tr>
<td><strong>Maximum Control filename length</strong>— Raises a protocol anomaly if IDP detects an LPR control filename containing more bytes than the specified maximum. The default is 64 bytes.</td>
<td></td>
</tr>
<tr>
<td><strong>Maximum Data filename length</strong>— Raises a protocol anomaly if IDP detects a data filename containing more bytes than the specified maximum. The default is 64 bytes.</td>
<td></td>
</tr>
<tr>
<td><strong>Maximum Control file size</strong>— Raises a protocol anomaly if IDP detects an LPR control file size greater than the specified maximum. The default is 1024 bytes.</td>
<td></td>
</tr>
<tr>
<td><strong>Maximum Data file size</strong>— Raises a protocol anomaly if IDP detects an LPR data file size greater than the specified maximum. The default is 64 bytes.</td>
<td></td>
</tr>
<tr>
<td><strong>Maximum Banner string length</strong>— Raises a protocol anomaly if IDP detects an LPR banner string containing more bytes than the specified maximum. A banner string is typically the filename of the print job. The default is 32 bytes.</td>
<td></td>
</tr>
<tr>
<td><strong>Maximum E-mail length</strong>— Raises a protocol anomaly if IDP detects an LPR control file e-mail address containing more bytes than the specified maximum. After the file has printed, it is sent to the e-mail address specified in the control file. The default is 32 bytes.</td>
<td></td>
</tr>
<tr>
<td><strong>Maximum Symbolic link length</strong>— Raises a protocol anomaly if IDP detects in an LPR control file a symbolic link containing more bytes than the specified maximum. A symbolic link is a file that points to another file (entry) in a UNIX file system, but does not contain the data in the target file. When the LPR protocol receives a symbolic link command in a control file, it records the symbolic link data for the print job filename to prevent directory entry changes from reprinting the file. The default maximum is 128 bytes.</td>
<td></td>
</tr>
<tr>
<td><strong>Maximum font length</strong>— Raises a protocol anomaly if IDP detects in an LPR control file a font name containing more bytes than the specified maximum. The default is 64 bytes.</td>
<td></td>
</tr>
<tr>
<td><strong>Maximum filename length for format related sub commands</strong>— Raises a protocol anomaly if IDP detects in an LPR control file a format-related file name containing more bytes than the specified maximum. The default is 32 bytes.</td>
<td></td>
</tr>
<tr>
<td>Setting</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>MSN</td>
<td><strong>Maximum Username length</strong>—Raies a protocol anomaly if IDP detects an MSN (Microsoft Instant Messaging) username containing more bytes than the specified maximum. The default is 84 bytes.</td>
</tr>
<tr>
<td></td>
<td><strong>Maximum Display name length</strong>—Raies a protocol anomaly if IDP detects an MSN display name containing more bytes than the specified maximum. The default is 128 bytes.</td>
</tr>
<tr>
<td></td>
<td><strong>Maximum Group name length</strong>—Raies a protocol anomaly if IDP detects an MSN group name containing more bytes than the specified maximum. The default is 84 bytes.</td>
</tr>
<tr>
<td></td>
<td><strong>Maximum User state length</strong>—Raies a protocol anomaly if IDP detects an MSN user state containing more bytes than the specified maximum. A user state is a three-letter code that indicates the status of the user’s connection (online, offline, idle, and so on). The default is 10 bytes.</td>
</tr>
<tr>
<td></td>
<td><strong>Maximum Phone number length</strong>—Raies a protocol anomaly if IDP detects a phone number containing more bytes than the specified maximum. The default is 20 bytes.</td>
</tr>
<tr>
<td></td>
<td><strong>Maximum Length of IP:port</strong>—Raies a protocol anomaly if IDP detects an IP:port parameter containing more bytes than the specified maximum. An IP:port parameter indicates the IP address and port number of the MSN server for a switchboard session. The default is 30 bytes.</td>
</tr>
<tr>
<td></td>
<td><strong>Maximum URL length</strong>—Raies a protocol anomaly if IDP detects a URL containing more bytes than the specified maximum. The default is 1024 bytes.</td>
</tr>
<tr>
<td></td>
<td><strong>Maximum tower data length in endpoint mapper messages</strong>—Raies a protocol anomaly if IDP detects an endpoint mapper message with a tower data length greater than the specified maximum. The default is 8192.</td>
</tr>
<tr>
<td></td>
<td><strong>Maximum number of entries in an insert message</strong>—Raies a protocol anomaly if IDP detects an MSRPC insert message with more entries than the specified maximum. The default is 100 entries.</td>
</tr>
<tr>
<td>MSRPC</td>
<td><strong>Maximum fragment length in MSRPC message</strong>—Raies a protocol anomaly if IDP detects an MSRPC (Microsoft Remote Procedure Call) message with a fragment length greater than the specified maximum. The default is 8192.</td>
</tr>
<tr>
<td>NFS</td>
<td><strong>Maximum Name length</strong>—Raies a protocol anomaly if IDP detects an NFS packet name containing more bytes than the specified maximum. The default is 256 bytes.</td>
</tr>
<tr>
<td></td>
<td><strong>Maximum Path length</strong>—Raies a protocol anomaly if IDP detects an NFS packet pathname containing more bytes than the specified maximum. The default is 1024 bytes.</td>
</tr>
<tr>
<td></td>
<td><strong>Maximum buffer length for read/write</strong>—Raies a protocol anomaly if IDP detects an NFS read/writer buffer larger than the specified maximum. The default is 52,768 bytes.</td>
</tr>
</tbody>
</table>
### Table 51: IDP Device Configuration: Protocol Thresholds and Configuration Settings (continued)

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>NTP</strong></td>
<td><strong>Minimum time (in seconds) between two requests</strong>– Raises a protocol anomaly if IDP detects the time between two client-to-server NTP requests is greater than the specified maximum. Valid values range from 64 to 1024 seconds. The default is 0 seconds (which turns the feature off).</td>
</tr>
<tr>
<td><strong>Maximum length for NTPv3 message</strong>– Raises a protocol anomaly if IDP detects an NTPv3 message containing more bytes than the specified maximum. The default is 68 bytes.</td>
<td></td>
</tr>
<tr>
<td><strong>Maximum length for NTPv4 message</strong>– Raises a protocol anomaly if IDP detects an NTPv4 message containing more bytes than the specified maximum. The default is 68 bytes.</td>
<td></td>
</tr>
<tr>
<td><strong>Maximum stratum value for any NTP peer</strong>– Raises a protocol anomaly if IDP detects a stratum value larger than the specified maximum. The default is 15 bytes.</td>
<td></td>
</tr>
<tr>
<td><strong>Maximum time since last update of Reference clock</strong>– Raises a protocol anomaly if IDP detects that the NTP reference clock has not been updated in more time than the specified maximum. The default is 86,400 seconds.</td>
<td></td>
</tr>
<tr>
<td><strong>Match timestamps on NTP request and response</strong>– Enables IDP to perform timestamp matching on client requests and server responses. With this setting enabled, IDP expects the server response original timestamp to match the client request transmit timestamp; otherwise IDP considers the packet a possible protocol anomaly. This setting is enabled by default.</td>
<td></td>
</tr>
<tr>
<td><strong>Maximum Authorization field length in NTP control message</strong>– Raises a protocol anomaly if IDP detects that the length of the Authentication fields in an NTP control message is larger than the specified maximum. The default is 20 bytes.</td>
<td></td>
</tr>
<tr>
<td><strong>Maximum length of any NTP control variable</strong>– Raises a protocol anomaly if IDP detects that the length of NTP control data variable name is larger than the specified maximum. The default is 128 bytes.</td>
<td></td>
</tr>
<tr>
<td><strong>Maximum length of any NTP variable value</strong>– Raises a protocol anomaly if IDP detects that the length of any NTP control data variable value is larger than the specified maximum. The default is 255 bytes.</td>
<td></td>
</tr>
<tr>
<td><strong>Maximum length of buffer to store between control packets</strong>– NTP control messages can be split across multiple UDP packets. This setting is the maximum number of characters that IDP stores in memory to ensure continuity from one packet to the other. The default is 255 bytes.</td>
<td></td>
</tr>
<tr>
<td><strong>Maximum time for an NTP Symmetric passive association to dissolve</strong>– A symmetric passive association between two NTP peers must be dissolved after sending one reply. This setting is the time in seconds after which IDP considers such an association as expired. The default is 900 seconds.</td>
<td></td>
</tr>
<tr>
<td>Setting</td>
<td>Description</td>
</tr>
<tr>
<td>----------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>POP3</td>
<td><strong>Maximum Line length</strong>—Raises a protocol anomaly if IDP detects a POP3 line containing more bytes than the specified maximum. The default is 512 bytes.</td>
</tr>
<tr>
<td></td>
<td><strong>Maximum Username length</strong>—Raises a protocol anomaly if IDP detects a POP3 username containing more bytes than the specified maximum. The default is 64 bytes.</td>
</tr>
<tr>
<td></td>
<td><strong>Maximum Password length</strong>—Raises a protocol anomaly if IDP detects a POP3 password containing more bytes than the specified maximum. The default is 64 bytes.</td>
</tr>
<tr>
<td></td>
<td><strong>Maximum APOP length</strong>—Raises a protocol anomaly if IDP detects an APOP containing more bytes than the specified maximum. The default is 100 bytes.</td>
</tr>
<tr>
<td></td>
<td><strong>Maximum message number</strong>—Raises a protocol anomaly if IDP detects a POP3 message number that is higher than the specified maximum. The default is 10,00,000.</td>
</tr>
<tr>
<td></td>
<td><strong>Maximum number of login failures per-minute</strong>—Raises a BRUTE_FORCE protocol anomaly if IDP detects more login failures than the specified maximum. The default is 4 POP3 login failures per minute.</td>
</tr>
<tr>
<td>RADIUS</td>
<td><strong>Maximum number of authenticated failures per-minute</strong>—Raises a BRUTE_FORCE protocol anomaly if IDP detects more login failures than the specified maximum. The default is 4 RADIUS login failures per minute.</td>
</tr>
<tr>
<td>SIP</td>
<td><strong>Max-Forwards threshold</strong>—Raises a protocol anomaly if IDP detects maximum number of thresholds.</td>
</tr>
<tr>
<td>SMB</td>
<td><strong>Maximum registry key length</strong>—Raises a protocol anomaly if IDP detects an SMB registry key containing more bytes than the specified maximum. The default is 8192 bytes.</td>
</tr>
<tr>
<td></td>
<td><strong>Maximum number of login failures per-minute</strong>—Raises a BRUTE_FORCE protocol anomaly if IDP detects more login failures than the specified maximum. The default is 4 SMB login failures per minute.</td>
</tr>
</tbody>
</table>
## Table 51: IDP Device Configuration: Protocol Thresholds and Configuration Settings (continued)

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SMTP</td>
<td><strong>Maximum Number of mail recipients</strong>—Raises a protocol anomaly if IDP detects an SMTP message containing more recipients than the specified maximum. The default is 100 recipients.</td>
</tr>
<tr>
<td></td>
<td><strong>Maximum Username length in RCPT and MAIL</strong>—Raises a protocol anomaly if IDP detects an SMTP message with a username containing more bytes than the specified maximum. The default is 256 bytes.</td>
</tr>
<tr>
<td></td>
<td><strong>Maximum Domain name length in RCPT and MAIL</strong>—raises a protocol anomaly if IDP detects an SMTP message with a domain name containing more bytes than the specified maximum. The default is 64 bytes.</td>
</tr>
<tr>
<td></td>
<td><strong>Maximum Path length in RCPT and MAIL</strong>—Raises a protocol anomaly if IDP detects an SMTP message with a pathname containing more bytes than the specified maximum. The default is 256 bytes.</td>
</tr>
<tr>
<td></td>
<td><strong>Maximum Command line length (before DATA)</strong>—Raises a protocol anomaly if IDP detects an SMTP message with a command-line entry containing more bytes than the specified maximum. The default is 1024 bytes.</td>
</tr>
<tr>
<td></td>
<td><strong>Maximum Reply line length from server (default)</strong>—Raises a protocol anomaly if IDP detects an SMTP message with a reply line from the server containing more bytes than the specified maximum. The default is 512 bytes.</td>
</tr>
<tr>
<td></td>
<td><strong>Maximum Text line length (after DATA)</strong>—Raises a protocol anomaly if IDP detects an SMTP text line containing more bytes than the specified maximum. The default is 1024 bytes.</td>
</tr>
<tr>
<td></td>
<td><strong>Maximum number of nested mime multi-part attachments</strong>—Raises a protocol anomaly if IDP detects more nested attachments than the specified maximum. The default is 4 nested mime multi-part attachments.</td>
</tr>
<tr>
<td></td>
<td><strong>Maximum number of base-64 bytes to decode</strong>— Raises a protocol anomaly if IDP detects more bytes of encoded mime data than the specified maximum. The default is 64 bytes.</td>
</tr>
<tr>
<td></td>
<td><strong>Maximum length of the value for content-type’s name attribute</strong>—Raises a protocol anomaly if IDP detects a name attribute in the content-type header containing more bytes than the specified maximum. The default is 128 bytes.</td>
</tr>
<tr>
<td></td>
<td><strong>Maximum length of the value for the content-disposition’s filename attribute</strong>— Raises a protocol anomaly if IDP detects a filename attribute in the content-disposition header containing more bytes than the specified maximum. The default is 128 bytes.</td>
</tr>
<tr>
<td></td>
<td><strong>Look for email headers in message data</strong>—Controls whether IDP looks for e-mail headers in the message data, which can occur when a bounced email contains an attachment. This setting is not enabled by default.</td>
</tr>
<tr>
<td>SYSLOG</td>
<td><strong>Validate RFC-3164 compliant timestamp format</strong>—If selected, the security module checks the timestamp in syslog traffic to ensure that it is compliant with RFC 3164. If the timestamp is not compliant, the security module considers the traffic a possibly anomaly. This setting is not enabled by default.</td>
</tr>
<tr>
<td>TELNET</td>
<td><strong>Maximum number of login failures per-minute</strong>— Raises a protocol anomaly if IDP detects more login failures than the specified maximum. The default is 4 TELNET login failures per minute.</td>
</tr>
<tr>
<td>TFTP</td>
<td><strong>Maximum Filename length</strong>— Raises a protocol anomaly if IDP detects a filename containing more bytes than the specified maximum. The default is 128 bytes.</td>
</tr>
</tbody>
</table>
Table 51: IDP Device Configuration: Protocol Thresholds and Configuration Settings (continued)

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>VNC</strong></td>
<td><strong>Maximum Reason string length</strong>—Raises a protocol anomaly if IDP detects a VNC (Virtual Network Computing) reason string length greater than the specified maximum. A reason string contains the text that describes why a connection between a VNC server and client failed. The default is 512 bytes.</td>
</tr>
<tr>
<td></td>
<td><strong>Maximum Display name length</strong>—Raises a protocol anomaly if IDP detects a VNC display name containing more bytes than the specified maximum. The default is 128 bytes.</td>
</tr>
<tr>
<td></td>
<td><strong>Maximum cut text length</strong>—Raises a protocol anomaly if IDP detects a VNC cut text buffer containing more bytes than the specified maximum. The default is 4096 bytes.</td>
</tr>
<tr>
<td></td>
<td><strong>Verify message after the initial handshake</strong>—Enables the security module to verify VNC connections after the initial handshake. This setting is not enabled by default.</td>
</tr>
<tr>
<td></td>
<td><strong>Maximum number of login failures per-minute</strong>—Raises a BRUTE_FORCE protocol anomaly if IDP detects more login failures than the specified maximum. The default is 4 VNC login failures per minute.</td>
</tr>
<tr>
<td><strong>WHOIS</strong></td>
<td><strong>Maximum Request length</strong>—Raises a protocol anomaly if IDP detects a WHOIS request containing more bytes than the specified maximum. The default is 128 bytes.</td>
</tr>
</tbody>
</table>
### Table 51: IDP Device Configuration: Protocol Thresholds and Configuration Settings (continued)

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>YMSG</td>
<td><strong>Maximum Message length</strong>—Raises a protocol anomaly if IDP detects a Yahoo! Messenger message with a header that indicates more bytes for the total message than the specified maximum. The default is 8192 bytes.</td>
</tr>
<tr>
<td></td>
<td><strong>Maximum Username length</strong>—Raises a protocol anomaly if IDP detects a Yahoo! Messenger ID containing more bytes than the specified maximum. The default is 84 bytes.</td>
</tr>
<tr>
<td></td>
<td><strong>Maximum Groupname length</strong>—Raises a protocol anomaly if IDP detects a Yahoo! Messenger group name containing more bytes than the specified maximum. The default is 84 bytes.</td>
</tr>
<tr>
<td></td>
<td><strong>Maximum Crypt length</strong>—Raises a protocol anomaly if IDP detects a Yahoo! Messenger encrypted password containing more bytes than the specified maximum. The default is 124 bytes.</td>
</tr>
<tr>
<td></td>
<td><strong>Maximum Instant message length</strong>—Raises a protocol anomaly if IDP detects a Yahoo! Messenger message containing more bytes than the specified maximum. The default is 1024 bytes.</td>
</tr>
<tr>
<td></td>
<td><strong>Maximum Activity string length</strong>—Raises a protocol anomaly if IDP detects a Yahoo! Messenger activity data type containing more bytes than the specified maximum. The default is 8000 bytes.</td>
</tr>
<tr>
<td></td>
<td><strong>Maximum Challenge length</strong>—Raises a protocol anomaly if IDP detects a Yahoo! Messenger challenge containing more bytes than the specified maximum. The default is 15 bytes.</td>
</tr>
<tr>
<td></td>
<td><strong>Maximum Cookie length</strong>—Raises a protocol anomaly if IDP detects a Yahoo! Messenger cookie containing more bytes than the specified maximum. The default is 84 bytes.</td>
</tr>
<tr>
<td></td>
<td><strong>Maximum URL length</strong>—Raises a protocol anomaly if IDP detects a Yahoo! Messenger Web Name containing more bytes than the specified maximum. The default is 400 bytes.</td>
</tr>
<tr>
<td></td>
<td><strong>Maximum Conference message length</strong>—Raises a protocol anomaly if IDP detects a Yahoo! Messenger join conference message containing more bytes than the specified maximum. The default is 1024 bytes.</td>
</tr>
<tr>
<td></td>
<td><strong>Maximum Conference name length</strong>—Raises a protocol anomaly if IDP detects a Yahoo! Messenger conference name containing more bytes than the specified maximum. The default is 1024 bytes.</td>
</tr>
<tr>
<td></td>
<td><strong>Maximum E-mail length</strong>—Raises a protocol anomaly if IDP detects a Yahoo! Messenger new e-mail alert containing an e-mail that has more bytes than the specified maximum. The default is 84 bytes.</td>
</tr>
<tr>
<td></td>
<td><strong>Maximum E-mail subject length</strong>—Raises a protocol anomaly if IDP detects an Yahoo! Messenger subject line containing more bytes than the specified maximum. The default is 128 bytes.</td>
</tr>
<tr>
<td></td>
<td>This setting tunes the Mail Subject Overflow attack object (key is CHAT:YIM:OVERFLOW:MAIL-SUBJECT).</td>
</tr>
<tr>
<td></td>
<td><strong>Maximum Filename length</strong>—Raises a protocol anomaly if IDP detects a Yahoo! Messenger file transfer containing a filename that has more bytes than the specified maximum. The default is 1000 bytes.</td>
</tr>
<tr>
<td></td>
<td><strong>Maximum Chatroom name length</strong>—Raises a protocol anomaly if IDP detects a Yahoo! Messenger chat room name containing more bytes than the specified maximum. The default is 1024 bytes.</td>
</tr>
<tr>
<td></td>
<td><strong>Maximum Chatroom message length</strong>—Raises a protocol anomaly if IDP detects a Yahoo! Messenger chat room message containing more bytes than the specified maximum. The default is 2000 bytes.</td>
</tr>
<tr>
<td></td>
<td><strong>Maximum buddy list length</strong>—Raises a protocol anomaly if IDP detects a Yahoo! Messenger buddy list containing more bytes than the specified maximum. The default is 8000 bytes.</td>
</tr>
</tbody>
</table>
### Table 51: IDP Device Configuration: Protocol Thresholds and Configuration Settings (continued)

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum webcam key length</td>
<td>Raises a protocol anomaly if IDP detects an Yahoo! Messenger Webcam key containing more bytes than the specified maximum. The default is 124 bytes.</td>
</tr>
</tbody>
</table>

**Related Topics**
- Updating the IDP Detector Engine (NSM Procedure) on page 76
- Configuring Traffic Anomalies Rulebase Rules (NSM Procedure) on page 51
Chapter 9
Configuring Additional Intrusion Detection
and Prevention Features

- Configuring Additional Intrusion Detection and Prevention Features Overview on page 111
- Enabling Intrusion Detection and Prevention Processing of Encrypted and Encapsulated Traffic (NSM Procedure) on page 111

Configuring Additional Intrusion Detection and Prevention Features Overview

You can configure additional IDP features in NSM, including enabling IDP processing of encrypted and encapsulated traffic. For more information on configuring the following features, see the IDP ACM online Help.

- Traffic interfaces
- IDP in advanced deployment modes
- Enable Spanning Tree Protocol
- High availability deployments
- Interoperability with Secure Access devices and Infranet Controllers

Related Topics
- NSM and Intrusion Detection and Prevention Device Management Overview on page 5
- Configuring Antispoof Settings in Intrusion Detection and Prevention Devices (NSM Procedure) on page 83
- Enabling Intrusion Detection and Prevention Processing of Encrypted and Encapsulated Traffic (NSM Procedure) on page 111

Enabling Intrusion Detection and Prevention Processing of Encrypted and Encapsulated Traffic (NSM Procedure)

You can enable IDP processing of encrypted and encapsulated traffic through NSM.
1. Enabling SSL Decryption on page 112
2. Enabling GRE Decapsulation on page 112
3. Enabling GTP Decapsulation on page 113
**Enabling SSL Decryption**

You can enable inspection of SSL traffic by first adding keys for the target SSL servers to the IDP keystore and then enabling the IDP SSL decryption feature.

For an overview of the IDP SSL decryption feature and lists of supported encryption algorithms and SSL ciphers, see the *IDP Concepts & Examples Guide*.

To add keys for target SSL servers to the IDP keystore:

1. Use SCP or FTP to copy your private key file to the IDP device. IDP does not run an FTP server, so you have to initiate the FTP session from the IDP device.
2. Add the key to the IDP keystore.
3. Retrieve the key ID from the IDP keystore.
4. Add any other servers that use the same key.

To enable SSL decryption:

1. In the NSM Device Manager, double-click the IDP device to display the device configuration editor.
2. Click **Sensor Settings**.
3. Click the **Run-Time Parameters** tab.
4. Expand the **Run-Time Parameters** group.
5. Select **Enable SSL decryption support**.
6. Click **OK**.

**Enabling GRE Decapsulation**

To enable GRE decapsulation:

1. In the NSM Device Manager, double-click the IDP device to display the device configuration editor.
2. Click **Sensor Settings**.
3. Click the **Run-Time Parameters** tab.
4. Expand the **Run-Time Parameters** group.
5. Select **Enable GRE decapsulation support**.
6. Click **OK**.
**Enabling GTP Decapsulation**

To enable GTP decapsulation:

1. In the NSM Device Manager, double-click the IDP device to display the device configuration editor.
2. Click **Sensor Settings**.
3. Click the **Run-Time Parameters** tab.
4. Expand the **Run-Time Parameters** group.
5. Select **Enable GTP decapsulation support**.
6. Click **OK**.

**Related Topics**

- Configuring Additional Intrusion Detection and Prevention Features Overview on page 111
- NSM and Intrusion Detection and Prevention Device Management Overview on page 5
Part 3
Managing Intrusion Detection and Prevention Devices

- Managing Security Policies in Intrusion Detection and Prevention Devices on page 117
- Managing Profiler Settings in Intrusion Detection and Prevention Devices on page 125
Chapter 10
Managing Security Policies in Intrusion Detection and Prevention Devices

Assigning a Security Policy in an Intrusion Detection and Prevention Device (NSM Procedure)

After you have created the necessary firewall and IDP rules within the security policy, you must perform the following steps to assign a security policy.

To assign an existing policy to the IDP device:
1. In the NSM navigation tree, select Policy Manager > Security Policies.
2. In Device Manager, right-click the IDP device and select Policy > Assign Policy.
3. From the Security Policy Name list, select the security policy you just created.
4. Click OK.

For more information, see the IDP Concepts & Examples Guide or Network and Security Manager Administration Guide.
Validating a Security Policy (NSM Procedure)

Validating a security policy can identify potential problems before you install it.

To validate a security policy:
1. In the navigation tree, select Device Manager. The Device manager appears.
2. Select Validate > Validate IDP Policy and select the device. A Job Manager window displays job information and progress.
3. Click OK.

For more information, see either the IDP Concepts & Examples Guide or the Network and Security Manager Administration Guide.

Related Topics
- Intrusion Detection and Prevention Devices and Security Policies Overview on page 29
- Assigning a Security Policy in an Intrusion Detection and Prevention Device (NSM Procedure) on page 117
- Troubleshooting Security Policy Validation Errors (NSM Procedure) on page 118

Troubleshooting Security Policy Validation Errors (NSM Procedure)

Problem
If NSM identifies a problem in the policy during policy validation, it displays information about the problem at the bottom of the selected rulebase. For example, if you included a non-IDP capable security device in the Install On column of an IDP rule, policy validation displays an error message. You can validate those errors and troubleshoot them.

Table 52 on page 118 describes security policy validation errors and how to resolve them.

Table 52: Troubleshooting: Security Policy Validation Errors

<table>
<thead>
<tr>
<th>Error</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rule Duplication</td>
<td>Rule appears more than once.</td>
</tr>
<tr>
<td></td>
<td>To resolve this problem, delete the duplicate.</td>
</tr>
<tr>
<td>Rule Shadowing</td>
<td>Rule shadowing occurs when two rules are designed to detect the same attack, and the first rule is either a terminal match rule or contains a more severe action than the second rule. In these cases, the second rule will never be applied.</td>
</tr>
<tr>
<td></td>
<td>To resolve this problem, modify or delete one of the rules.</td>
</tr>
</tbody>
</table>
Table 52: Troubleshooting: Security Policy Validation Errors (continued)

<table>
<thead>
<tr>
<th>Error</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protocol Mismatches</td>
<td>Protocol mismatches occur when a service object that is specified in the Service column of the security policy uses a different protocol from that specified by the default service binding of the attack object for that rule. Remember that the service binding specifies the service and port that the attack uses. Because two different protocols are specified, IDP cannot match attacks for the attack object. To resolve this problem, set Service to Default.</td>
</tr>
<tr>
<td>Any-Any-None Rules</td>
<td>Any-Any-None rules are rules that specify any for the source and destination and none for attacks. Because IDP must log all packets for all connections, this rule can cause severe IDP performance penalties. To resolve this problem, specify network objects for the destination and attack objects for the attacks.</td>
</tr>
<tr>
<td>Any-Any-One Rules</td>
<td>Any-Any-One rules are rules that specify any for the source and destination and a single attack object for attacks. Because IDP must look at all network traffic, this rule can cause severe IDP performance penalties. To resolve this problem, specify network objects for the destination.</td>
</tr>
<tr>
<td>Unsupported Options</td>
<td>Rule contains options that are not supported on the target device. To resolve this problem, upgrade the target device or remove the option from the rule.</td>
</tr>
</tbody>
</table>

Related Topics

- Intrusion Detection and Prevention Devices and Security Policies Overview on page 29
- Assigning a Security Policy in an Intrusion Detection and Prevention Device (NSM Procedure) on page 117
- Validating a Security Policy (NSM Procedure) on page 118

Pushing Security Policy Updates to an IDP Device (NSM Procedure)

You must run a device configuration update job (also called pushing an update) in the following cases:

- After you have revised the security policy assigned to an IDP device. The configuration changes you make in NSM do not affect the IDP device until you have successfully pushed the configuration to the IDP device.
- If you have deleted the device from NSM and reinstall it. In these cases, the IDP device does not retain the previous security policy assignment.
- If you use the NSM Device Manager to change IDP device settings.

To push configuration updates to multiple IDP devices:

1. Select Devices > Configuration > Update Device Config to display the Update Devices Options dialog box.
2. Select the devices that you want to push configuration updates to and to set update job options on. Table 53 on page 120 describes devices update job options.

3. Click OK.

### Table 53: Devices Update Job Options

<table>
<thead>
<tr>
<th>Tab</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>General</td>
<td>Run Summarize Delta Config—Summarizes and runs the delta change in the configuration.</td>
</tr>
</tbody>
</table>
| Netconf                    | Lock configuration during update—Locks configuration while updating device configuration.  
                                | Update to candidate config first before commit to running config—Updates the configuration before committing.  
                                | Use confirmed commit—Enables commit confirmed.  
                                | Rollback candidate config to running config in error—Rollbacks when there is error generated during the configuration.  
                                | Discard uncommitted changes when exclusive lock is available—Discards any uncommitted changes during exclusive lock.  |
| ScreenOS and IDP           | Show unconnected devices—Lists all devices that are not connected.  
                                | Update when device connects—Updates configuration when the devices are connected.  
                                | Firewall Device Options—Not applicable.  
                                | Standalone IDP device options—Includes the following option:  
                                | ■ Restart IDP Profiler after Device Update—Restarts the Profiler.  
                                | ISG Device Options—Not applicable.  |

To push an update to a specific, single device:

1. In Device Manager, right-click the device that you want to push the update to and select **Update Device** to display the Update Device Options dialog box.

2. Set update job options using Table 54 on page 120.

3. Click OK.

### Table 54: Device Update Job Options

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Update When Device Connects</td>
<td>Updates the device whenever there exist a connection between the devices.</td>
</tr>
<tr>
<td>Restart IDP Profiler After Device Update</td>
<td>Restarts the profiler when the device gets updated.</td>
</tr>
<tr>
<td>Update IDP Rulebase Only</td>
<td>Updates IDP rulebase only.</td>
</tr>
</tbody>
</table>
Table 54: Device Update Job Options (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Don’t Show This Dialog</td>
<td>Does not allow this dialog box to appear again.</td>
</tr>
</tbody>
</table>

For more information, see the IDP Concepts & Examples Guide.

**Related Topics**
- NSM and Intrusion Detection and Prevention Device Management Overview on page 5
- Troubleshooting Configuration Push Errors (NSM Procedure) on page 121

### Troubleshooting Configuration Push Errors (NSM Procedure)

**Problem**
Table 55 on page 121 provides tips for troubleshooting errors related to NSM configuration push jobs.

**Table 55: Troubleshooting: Configuration Push Errors**

<table>
<thead>
<tr>
<th>Error</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Timeout</td>
<td>The default timeout for IDP policy is 2400000 milliseconds (40 minutes).</td>
</tr>
<tr>
<td></td>
<td>When you first push a policy to a newly deployed IDP device, NSM must send a lot of information (mostly attack definitions). In some cases, the update job can time out before it completes.</td>
</tr>
<tr>
<td></td>
<td>To modify the timeout setting:</td>
</tr>
<tr>
<td></td>
<td>1. On the NSM Device Server, open the following file in a text editor:</td>
</tr>
<tr>
<td></td>
<td>/usr/netscreen/DevSvr/var/devSvr.cfg</td>
</tr>
<tr>
<td></td>
<td>2. Modify the following setting:</td>
</tr>
<tr>
<td></td>
<td>devSvrDirectiveHandler.idpPolicyPush.timeout 2400000</td>
</tr>
<tr>
<td>The following attacks/groups cannot be updated. Not supported for version.</td>
<td>Different versions of IDP use different detector engines. Not all attack objects are valid for all versions of the detector engine. IDP indicates which attack objects in the security policy were not valid for the loaded detector engine and, therefore, not loaded.</td>
</tr>
<tr>
<td></td>
<td>This message is for information purposes only and does not indicate a problem with the IDP device or the policy.</td>
</tr>
<tr>
<td>No firewall rules can be updated for device in assigned policy policyName.</td>
<td>You try to load a policy that contains a firewall rulebase onto a standalone IDP device.</td>
</tr>
<tr>
<td></td>
<td>This message just means that IDP cannot process the firewall rulebase. The IDP rulebases are still processed normally, assuming no other errors.</td>
</tr>
</tbody>
</table>
Table 55: Troubleshooting: Configuration Push Errors (continued)

<table>
<thead>
<tr>
<th>Error</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rule #: Packet logging with any/any rule has serious performance implications.</td>
<td>Setting the rule to log packets causes IDP to save packets until it is sure that they will not be needed for a log entry. A rule that has any in the Source IP column and any in the Destination IP column examines all traffic. So, IDP has to save a lot of packets all the time, which impacts performance.</td>
</tr>
<tr>
<td>Policy has not changed and hence will not be updated.</td>
<td>For performance reasons, IDP does not spend resources recompiling a security policy that has not changed.</td>
</tr>
<tr>
<td>Failed to update device. Failed to compile policy.</td>
<td>Something has gone wrong with the policy compilation. Other error messages may indicate why.</td>
</tr>
<tr>
<td>No license for idp.</td>
<td>The device does not have a valid license. Unlicensed devices do not accept policy uploads.</td>
</tr>
</tbody>
</table>

**Related Topics**
- NSM and Intrusion Detection and Prevention Device Management Overview on page 5
- Pushing Security Policy Updates to an IDP Device (NSM Procedure) on page 119

**Disabling Rules (NSM Procedure)**

You can disable a rule without deleting it in cases where you run tuning experiments, troubleshoot an issue, or otherwise need to make a quick or temporary modification.

To disable a rule, right-click inside the No. column (the first column) of the rule and select **Disable**. The rule remains in the rulebase, but a gray diagonal stripe indicates that it has been disabled. While the rule is disabled, NSM does not install the rule on any devices.

To enable a rule, right-click inside the No. column (the first column) of the rule and select **Disable** again to clear the check box. You can disable rule groups using the same method. For more information, see the *Network and Security Manager Administration Guide*.

---

**NOTE:** You cannot disable an entire security policy or a rulebase.

**Related Topics**
- NSM and Intrusion Detection and Prevention Device Management Overview on page 5
- Modifying IDP Rulebase Rules (NSM Procedure) on page 34

**Exporting Security Policies (NSM Procedure)**

You can export a security policy rulebase to an HTML file.
To export a security policy to an HTML file:

1. Select the security policy and select File > Export Policy to display the Export Policy dialog box.
2. Select the rulebases you want to export.
3. Select a directory in which to save the exported file.
4. Click Export to complete the operation.

Each export creates a new directory. The default directory name is `policyname_YYMMDD_HHMMSS`. The export process puts each rulebase in a separate HTML file in that directory.

Use an HTML browser to view the exported file. For more information, see the Network and Security Manager Administration Guide.

Related Topics
- Intrusion Detection and Prevention Devices and Security Policies Overview on page 29
- Assigning a Security Policy in an Intrusion Detection and Prevention Device (NSM Procedure) on page 117
Chapter 11
Managing Profiler Settings in Intrusion Detection and Prevention Devices

Managing Profiler Settings

- Managing Profiler Settings on page 125

Updating Profiler Settings

- Updating Profiler Settings on page 125
- Starting the Profiler on page 125
- Stopping the Profiler on page 125

Updating Profiler Settings

After you have finished configuring settings on the Profiler, you must update those settings on the device. You can do this in the Device Manager by right-clicking the device and selecting Update Device. The Device Update Options window appears and prompts you to restart IDP Profiler after the device updates. Click OK to confirm.

The Job Information window appears indicating the status of the update. After this is finished, the device begins collecting data for the Profiler database.

Starting the Profiler

To manually start the Profiler, use the Devices menu, and select IDP Profiler > Start Profiler. In the Start Profiler dialog box, select the devices you want to use for profiling, and then click OK. Alternatively, you can right-click any device from the Device Manager, and select IDP Profiler > Start Profiler.

As your devices begin profiling your internal network, they gather information about your network hosts, their peers, ports, and Layer-7 data.

Stopping the Profiler

To manually stop the Profiler, use the Devices menu, and select IDP Profiler > Stop Profiler. In the Stop Profiler dialog box, select the appropriate devices, and then click OK. Alternatively, you can right-click any device from the Device Manager, and select IDP Profiler > Stop Profiler.

Related Topics
- Configuring Profiler Options (NSM Procedure) on page 13
Modifying Profiler Settings (NSM Procedure) on page 25
Part 4
Monitoring Intrusion Detection and Prevention Devices

- Working with NSM Logs and Reports on page 129
- Working with Intrusion Detection and Prevention Reporter Reports on page 143
Chapter 12
Working with NSM Logs and Reports

- NSM Logs and Reports Overview on page 129
- Viewing Logs on page 129
- Viewing Device Status on page 132
- Viewing NSM Predefined Reports on page 135
- Creating NSM Custom Reports on page 137
- Configuring Log Suppression on page 140

NSM Logs and Reports Overview

IDP devices generate logs about device status based on built-in criteria and about security events based on the security policy notification settings. These logs are automatically sent to the NSM GUI server and can be viewed in the NSM log viewer.

IDP administration includes the following log-related tasks:

- Viewing device status, logs, and reports
- Configuring log suppression, if you want to reduce the number of identical log files

Related Topics
- Viewing Logs on page 129
- Configuring Syslog Collection (NSM Procedure) on page 80

Viewing Logs

NSM logging tools provide a high-level view of the activity on your network, enabling you to view summaries as well as detailed information. You can choose to view log entries for an event that occurs across domains. This section includes the following primary sections:

1. IDP Logs on page 130
2. Using NSM Log Investigator on page 130
3. Using NSM Audit Log Viewer on page 130
**IDP Logs**

NSM collects logs from managed IDP devices and stores them in a central log database. You can use NSM to view, manipulate, and export logs.

Table 56 on page 130 provides a reference of log views.

<table>
<thead>
<tr>
<th>Log Views</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>NSM Log Viewer / Log Investigator</td>
<td>Logs based on notification options you set for security policy rules.</td>
</tr>
<tr>
<td></td>
<td>Logs related to device events, such as changes in the state of a traffic interface.</td>
</tr>
<tr>
<td>NSM Log Viewer / Log Investigator</td>
<td>Logs produced by the Profiler feature.</td>
</tr>
<tr>
<td>NSM Security Monitor</td>
<td></td>
</tr>
<tr>
<td>NSM Audit Log Viewer</td>
<td>Logs generated by NSM related to the use of NSM to manage the IDP device.</td>
</tr>
<tr>
<td>statview utility</td>
<td>Logs produced by the application volume tracking (AVT) feature.</td>
</tr>
</tbody>
</table>

**Using NSM Log Investigator**

**Purpose**
You use the NSM Log Investigator to analyze aggregations of logs and drill down based on properties of interest.

**Action**
To display logs in NSM Log Investigator, select **Investigate > Log Investigator**.

*TIP:* For details on using NSM to modify aggregation or display options, see the NSM online Help.

**Using NSM Audit Log Viewer**

**Purpose**
You use the NSM Audit Log Viewer to track the administrative changes made to a managed device. Log-entry details include the administrator that performed the change, when the change occurred, and the job results.

**Action**
To display the NSM Audit Log Viewer table, select **Investigate > Audit Log Viewer**.

Table 57 on page 131 describes the columns in the Audit Log Viewer table.
### Table 57: NSM Audit Log Viewer Table

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time Generated</td>
<td>The time the object was changed. The Audit Log Viewer displays log entries in order of time generated by Greenwich Mean Time (GMT).</td>
</tr>
<tr>
<td>Admin Name</td>
<td>The name of the NSM administrator who changed the object.</td>
</tr>
<tr>
<td>Admin Login Domain</td>
<td>The name of the domain (global or subdomain) that contains the changed object.</td>
</tr>
<tr>
<td>Authorization Status</td>
<td>The final access-control status of activities is either success or failure.</td>
</tr>
<tr>
<td>Command</td>
<td>The command applied to the object or system, for example, sys_logout or modify.</td>
</tr>
<tr>
<td>Targets</td>
<td>For changes made to a device configuration or object, the Audit Log Viewer displays the object type, an object name, and object domain.</td>
</tr>
<tr>
<td>Devices</td>
<td>For changes made to a device, the Audit Log Viewer displays the device name, object type, and device domain.</td>
</tr>
<tr>
<td></td>
<td>For changes made to the management system, such as administrator login or logout, the Audit Log Viewer does not display target or device data.</td>
</tr>
<tr>
<td>Miscellaneous</td>
<td>Additional information that is not displayed in other audit log columns.</td>
</tr>
</tbody>
</table>

To display details of a configuration change, such as a changed IP address or renamed device, select the audit log entry for that change in the Audit Log table and view details in the Target View table, which appears below the Audit Log Viewer table.

Table 58 on page 131 describes the Target View table.

### Table 58: NSM Audit Log Viewer: Target View Table

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Target Name</td>
<td>To see additional details for a target view entry, double-click the entry. NSM displays the configuration screen that the change was made in and marks the changed field with a solid green triangle.</td>
</tr>
<tr>
<td>Table</td>
<td>To set the table details for the target view entry, double-click the table. Enter or update the options.</td>
</tr>
<tr>
<td>Domain ID</td>
<td>Specifies the domain ID of the target view.</td>
</tr>
</tbody>
</table>

To display details of a non-configuration event, such as adding the device, auto-detecting a device, or rebooting a device, select the audit log entry for that change in the Audit Log table and view details in the Device View table, which is displayed below the Audit Log Viewer table.

Table 59 on page 132 describes the Device View table.
**Table 59: NSM Audit Log Viewer: Device View Table**

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Name</td>
<td>To see additional details for a device view entry, double-click the entry. NSM displays the Job Manager information window for the job task.</td>
</tr>
<tr>
<td>Table</td>
<td>To set the table details for the device view entry, double-click the table. Enter or update the options.</td>
</tr>
<tr>
<td>Domain ID</td>
<td>Specifies the domain ID of the device view.</td>
</tr>
</tbody>
</table>

**Related Topics**
- Viewing Device Status on page 132
- NSM Logs and Reports Overview on page 129
- Configuring Syslog Collection (NSM Procedure) on page 80

**Viewing Device Status**

NSM keeps you up-to-date on the health of your network with the following information:

- View critical information about your devices and IDP sensors in the Device Monitor:
  - Configuration and connection status of your security devices
  - Individual device details, such as memory usage and active sessions
  - Device statistics
- View the status of your IDP clusters in the IDP Cluster Monitor.

Table 60 on page 132 lists and describes device information that you can view through the Device Monitor.

**Table 60: Device Status Information**

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Unique name assigned to the device in NSM.</td>
</tr>
<tr>
<td>Domain</td>
<td>Domain in NSM in which the device is managed.</td>
</tr>
<tr>
<td>Platform</td>
<td>Model number of the device.</td>
</tr>
<tr>
<td>OS Version</td>
<td>Operating system firmware version running on the device.</td>
</tr>
</tbody>
</table>
### Table 60: Device Status Information (continued)

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Config Status</td>
<td>Current configuration status of the device in NSM:</td>
</tr>
<tr>
<td>■ None</td>
<td>No state has been set (does not show in Device Monitor).</td>
</tr>
<tr>
<td>■ Modeled</td>
<td>The device exists in NSM, but a connection to the device has not yet been established.</td>
</tr>
<tr>
<td>■ RMA</td>
<td>Equivalent to bringing the device into the Modeled state. RMA results from an administrator selection in the UI when a device goes down.</td>
</tr>
<tr>
<td>■ Waiting for 1st connect</td>
<td>NSM is waiting for the device to connect. You must enter a command on the device to make it connect to NSM.</td>
</tr>
<tr>
<td>■ Import Needed</td>
<td>You must import the configuration of the device into NSM. When you add a device for the first time, verify that your status indicates “Import Needed” before you attempt to import the device. During migration, this state indicates that import of the security device configuration is still required.</td>
</tr>
<tr>
<td>■ OS Version Adjustment Needed</td>
<td>The firmware version detected running on the device is different from what was previously detected in NSM. This could happen in the event that the automatic adjustment option was cleared during a change device firmware directive or an Update Device directive was issued to an IDP device with a firmware version mismatch.</td>
</tr>
<tr>
<td>■ Platform Mismatch</td>
<td>The device platform selected when adding the DMI device in NSM does not match the device itself. A device in this state cannot connect to NSM.</td>
</tr>
<tr>
<td>■ Device Firmware Mismatch</td>
<td>The OS version selected when adding a DMI device does not match the OS version running on the device itself.</td>
</tr>
<tr>
<td>■ Device Type Mismatch</td>
<td>The type of device specified when adding the device in NSM does not match the device itself. The device type might indicate whether the device is part of a vsys device, part of a cluster, or part of a virtual chassis. A device in this state cannot connect to NSM.</td>
</tr>
<tr>
<td>■ Detected duplicate serial number</td>
<td>The device has the same sequence number as another managed device. A device in this state cannot connect to NSM.</td>
</tr>
<tr>
<td>■ Update Needed</td>
<td>An update to this device is required.</td>
</tr>
<tr>
<td>■ Managed</td>
<td>The device is currently being managed by NSM.</td>
</tr>
<tr>
<td>■ Managed, In Sync</td>
<td>The physical device configuration is synced with the modeled configuration in NSM.</td>
</tr>
</tbody>
</table>
### Table 60: Device Status Information (continued)

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Config Status (continued)</strong></td>
<td>Managed, Device Changed—The physical device configuration is out of sync with the modeled configuration in NSM. Changes were made to the physical device configuration (the configuration on the physical device is newer than the modeled configuration).</td>
</tr>
<tr>
<td></td>
<td>Managed, NSM Changed—The modeled device configuration is out of sync with the physical device configuration. Changes were made to the modeled configuration (the configuration on the NSM is newer than the physical device configuration).</td>
</tr>
<tr>
<td></td>
<td>Managed, NSM and Device Changed—Both device configurations (physical and modeled) are out of sync with each other. Changes were made to the physical device configuration and to the modeled configuration.</td>
</tr>
<tr>
<td></td>
<td>Managed, Sync Pending—Completion of the Update Device directive is suspended and waiting for the device to reconnect. This state occurs only for ScreenOS devices that have the Update When Device Connects option selected during the device update.</td>
</tr>
</tbody>
</table>

**Connection Status**

Connection status of the device in NSM:

- **Up**—Device is currently connected to NSM.
- **Down**—Device is not currently connected to NSM but has connected in the past.
- **Never Connected**—Device has never connected to NSM.

The Device Server checks the connection status of each device every 120 seconds by default. You can change this behavior by editing the value for the `devDaemon.deviceHeartbeatTimeout` parameter in the Device Server configuration file. Refer to the Network and Security Manager Installation Guide for more information on editing configuration files.

**NOTE:** If the network connection goes down for a period longer than six to eight minutes, the device connection will permanently time out. If this occurs and the device goes down for any reason, the device still appears as Up in the Device Monitor.

**Alarm**

Displays the current alarm status for each device in NSM:

- If device has any alarms, the most severe alarm severity is displayed (either Major or Minor).
- **None**—The device has no alarms.
- **Unknown**—The device status is unknown. For example, the device might not be connected.
- **N/A**—The device’s alarm is not pollable or discoverable, for example, this column shows “N/A” for ScreenOS and IDP devices.

**Alarm is colored:**

- Red for Major.
- Orange for Minor.
- Green for Ignore, None, Unknown, or N/A.
Table 60: Device Status Information (continued)

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>H/W Inventory Status</td>
<td>Displays the inventory status for hardware on the device:</td>
</tr>
<tr>
<td>■ In Sync</td>
<td>The inventory information in the NSM database is synchronized with the information on the device.</td>
</tr>
<tr>
<td>■ Out Of Sync</td>
<td>The inventory information in the NSM database is not synchronized with the information on the device.</td>
</tr>
<tr>
<td>■ N/A</td>
<td>The connected device is a ScreenOS or IDP device, or the device is not connected and imported.</td>
</tr>
<tr>
<td>S/W Inventory Status</td>
<td>Displays the inventory status for software on the device:</td>
</tr>
<tr>
<td>■ In Sync</td>
<td>The inventory information in the NSM database is synchronized with the software on the device.</td>
</tr>
<tr>
<td>■ Out Of Sync</td>
<td>The inventory information in the NSM database is not synchronized with the software on the device.</td>
</tr>
<tr>
<td>■ N/A</td>
<td>The connected device is a ScreenOS or IDP device, or the device is not connected and imported.</td>
</tr>
<tr>
<td>License Inventory Status</td>
<td>Displays the inventory status for software on the device:</td>
</tr>
<tr>
<td>■ In Sync</td>
<td>The inventory information in the NSM database is synchronized with the licenses on the device.</td>
</tr>
<tr>
<td>■ Out Of Sync</td>
<td>The inventory information in the NSM database is not synchronized with the licenses on the device.</td>
</tr>
<tr>
<td>■ N/A</td>
<td>The connected device is a ScreenOS or IDP device, or the device is not connected and imported.</td>
</tr>
<tr>
<td>First Connect</td>
<td>The first time the security device connected to the NSM device server.</td>
</tr>
<tr>
<td>Latest Connect</td>
<td>The last time the security device connected to the NSM device server.</td>
</tr>
<tr>
<td>Latest Disconnect</td>
<td>The last time the security device disconnected from the NSM device server.</td>
</tr>
</tbody>
</table>

Related Topics
- Creating NSM Custom Reports on page 137
- NSM Logs and Reports Overview on page 129

Viewing NSM Predefined Reports

You can use the predefined reports to validate the effectiveness of your security policies.

Table 61 on page 135 describes NSM DI/IDP predefined reports. These reports are related to attacks.

Table 61: NSM DI/IDP Predefined Reports

<table>
<thead>
<tr>
<th>Report</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Top 100 Attacks (last 24 hours)</td>
<td>Those attacks that are detected most frequently within the last 24 hours.</td>
</tr>
<tr>
<td>Report</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Top 100 Attacks Prevented (last 24 hours)</td>
<td>Those attacks that are prevented most frequently within the last 24 hours.</td>
</tr>
<tr>
<td>Top 20 Attackers (All Attacks - last 24</td>
<td>IP addresses that have most frequently been the source of an attack during</td>
</tr>
<tr>
<td>hours)</td>
<td>the last 24 hours.</td>
</tr>
<tr>
<td>Top 20 Attackers Prevented (All Attacks -</td>
<td>IP addresses that have most frequently been prevented from attacking the</td>
</tr>
<tr>
<td>last 24 hours)</td>
<td>network during the last 24 hours.</td>
</tr>
<tr>
<td>Top 20 Targets (last 24 hours)</td>
<td>IP addresses that have most frequently been the target of an attack during</td>
</tr>
<tr>
<td></td>
<td>the last 24 hours.</td>
</tr>
<tr>
<td>Top 20 Targets Prevented (last 24 hours)</td>
<td>IP addresses that have most frequently prevented attacks during the last 24</td>
</tr>
<tr>
<td></td>
<td>hours.</td>
</tr>
<tr>
<td>All Attacks by Severity (last 24 hours)</td>
<td>Number of attacks by severity level (set in attack objects).</td>
</tr>
<tr>
<td>All Attacks Prevented by Severity (last 24</td>
<td>Number of attacks prevented by severity level (set in attack objects).</td>
</tr>
<tr>
<td>hours)</td>
<td></td>
</tr>
<tr>
<td>All Attacks Over Time (last 7 days)</td>
<td>All attacks detected during the last 7 days.</td>
</tr>
<tr>
<td>All Attacks Prevented Over Time (last 7</td>
<td>All attacks prevented during the last 7 days.</td>
</tr>
<tr>
<td>days)</td>
<td></td>
</tr>
<tr>
<td>All Attacks Over Time (last 30 days)</td>
<td>All attacks detected during the last 30 days.</td>
</tr>
<tr>
<td>All Attacks Prevented Over Time (last 30</td>
<td>All attacks prevented during the last 30 days.</td>
</tr>
<tr>
<td>days)</td>
<td></td>
</tr>
<tr>
<td>Critical Attacks (last 24 hours)</td>
<td>All attacks categorized as “critical” detected during the past 24 hours.</td>
</tr>
<tr>
<td>Critical Attacks Prevented (last 24 hours)</td>
<td>All attacks categorized as “critical” prevented during the past 24 hours.</td>
</tr>
<tr>
<td>Critical through Medium Attacks (last 24</td>
<td>All attacks categorized as either “critical” or “medium” detected during</td>
</tr>
<tr>
<td>hours)</td>
<td>the past 24 hours.</td>
</tr>
<tr>
<td>Critical through Medium Attacks Prevented</td>
<td>All attacks categorized as either “critical” or “medium” prevented during</td>
</tr>
<tr>
<td>(last 24 hours) (last 24 hours)</td>
<td>the past 24 hours.</td>
</tr>
<tr>
<td>Top 50 Scan Sources (last 7 days)</td>
<td>IP addresses that have most frequently performed a scan of a managed device.</td>
</tr>
<tr>
<td>Top 50 Scan Targets (last 7 days)</td>
<td>IP addresses that have most frequently been the target of a scan over the</td>
</tr>
<tr>
<td></td>
<td>last 7 days.</td>
</tr>
<tr>
<td>Profiler - New Hosts (last 7 days)</td>
<td>New hosts listed in the Profiler over the last 7 days.</td>
</tr>
<tr>
<td>Profiler - New Ports (last 7 days)</td>
<td>New ports listed in the Profiler over the last 7 days.</td>
</tr>
<tr>
<td>Profiler - New Protocols (last 7 days)</td>
<td>New protocols listed in the Profiler over the last 7 days.</td>
</tr>
<tr>
<td>Top IDP Rules</td>
<td>The total number of log entries generated by specific rules in your IDP</td>
</tr>
<tr>
<td></td>
<td>policies. You can use the Top Rules report to identify those rules that are</td>
</tr>
<tr>
<td></td>
<td>generating the most log events. This enables you to better optimize your</td>
</tr>
<tr>
<td></td>
<td>rulebases by identifying those rules that are most and least effective. You</td>
</tr>
<tr>
<td></td>
<td>can then modify or remove those rules from your security policies.</td>
</tr>
</tbody>
</table>
Table 62 on page 137 describes Profiler predefined reports. These reports are related to activity by hosts in your network.

**Table 62: NSM Profiler Predefined Reports**

<table>
<thead>
<tr>
<th>Report</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Top 10 Peers by Count</td>
<td>Ten source and destination IP addresses that appeared most frequently in the Profiler logs.</td>
</tr>
<tr>
<td>Top 10 Peers with maximum hits</td>
<td>Ten source and destination IP addresses that had the highest number of hits in the Profiler logs.</td>
</tr>
</tbody>
</table>

Table 63 on page 137 describes the predefined application volume tracking reports. The reports are related to application use in your network.

**Table 63: NSM: Application Volume Tracking Reports**

<table>
<thead>
<tr>
<th>Report</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Top 10 Applications by Volume</td>
<td>Applications with the highest volume in bytes in the past 24 hours.</td>
</tr>
<tr>
<td>Top 10 Application Categories by Volume</td>
<td>Application categories with the highest volume in bytes in the past 24 hours.</td>
</tr>
<tr>
<td>Top 5 Applications by Volume over Time (last 1 hour)</td>
<td>Applications with the highest volume in bytes in the past 1 hour.</td>
</tr>
<tr>
<td>Top 5 Application Categories by Volume (last 1 hour)</td>
<td>Application categories with the highest volume in bytes in the past 1 hour.</td>
</tr>
<tr>
<td>Top 5 Source by Volume over Time (last 1 hour)</td>
<td>Source IP addresses with the highest volume in bytes in the past 1 hour.</td>
</tr>
<tr>
<td>Top 5 Destination by Volume over Time (last 1 hour)</td>
<td>Destination IP addresses with the highest volume in bytes in the past 1 hour.</td>
</tr>
</tbody>
</table>

**Related Topics**
- Creating NSM Custom Reports on page 137
- NSM Logs and Reports Overview on page 129

**Creating NSM Custom Reports**

**Purpose**
You use custom reports if you require a view of data not covered by predefined reports.

**Action**
To create a custom report:
1. In the NSM navigation tree, select **Investigate > Report Manager**.
2. Select a pre-defined report with data similar to what you ultimately want to save.
3. Select **File > Save As**.

4. Use pre-defined report as a template and example, complete the configuration options, and click **OK** to save the new report settings.

   Table 64 on page 139 describes configuration options.
### Table 64: Custom Report Configuration Options

<table>
<thead>
<tr>
<th>Tab</th>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>General</td>
<td>Name</td>
<td>Specify a name for the report as you would like it to appear in the NSM navigation tree.</td>
</tr>
<tr>
<td></td>
<td>Report Title</td>
<td>Specify a name for the report as you would like it to appear at the top of the report.</td>
</tr>
<tr>
<td>Type of Report</td>
<td>Select a report type:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>▪ Count-Based</td>
<td>Displays total current activity to date. For example, the Top Scan Targets report is a count-based report that displays the total number of scans currently recorded against a specified number of destination IP addresses.</td>
</tr>
<tr>
<td></td>
<td>▪ Time-Based</td>
<td>Displays activity over time. For example, the Attacks Over Time report is a time-based report that measures the top attacks recorded in log records over a specified period.</td>
</tr>
<tr>
<td></td>
<td>▪ Sum-Based</td>
<td>Displays the sum of the activities to date.</td>
</tr>
<tr>
<td>Columns for Report</td>
<td>In reports, columns are the same as log fields.</td>
<td></td>
</tr>
<tr>
<td>Time Period</td>
<td>You can configure a report to display all available data from either a specific date and time or during a specific time interval. For example, if you suspect that your network was attacked on September 15 at 6:00 PM, you could set the Starting At Time Period Duration report field in the options on a Top Screen Attacks report to that time, then generate the report. If you are not sure of the exact date or time of the attack, but know it occurred during the past 2 days, set the Duration field in the Time Period Duration report options on a Top Screen Attacks report to two days, then generate the report.</td>
<td></td>
</tr>
<tr>
<td>Data point count</td>
<td>Typically, the top 50 occurrences of each data type are displayed in each report. You can configure a report to display more or fewer data points depending upon the level of detail you need. For example, if you want to obtain a more precise view of the top occurrences of events, you would configure a lower data point count (such as 25).</td>
<td></td>
</tr>
<tr>
<td>Chart type</td>
<td>Select from the following choices:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>▪ Horizontal bar (default)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>▪ Pie</td>
<td></td>
</tr>
<tr>
<td></td>
<td>▪ Line</td>
<td></td>
</tr>
<tr>
<td></td>
<td>▪ Vertical bar</td>
<td></td>
</tr>
<tr>
<td>Save Report In</td>
<td>In the first selection box, specify whether to save in the My Reports or Shared Reports node.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>In the second box, select the Others folder or type a new folder name.</td>
<td></td>
</tr>
<tr>
<td>Filter</td>
<td>Columns for Report</td>
<td>The columns you selected on the General tab are passed through. Select the column with the cursor to display the corresponding Filter Settings controls.</td>
</tr>
<tr>
<td></td>
<td>Filter Settings</td>
<td>Specify filter values related to column settings.</td>
</tr>
</tbody>
</table>
TIP: For information on deleting custom reports, organizing report folders, exporting reports, and using the NSM guiSvrCli.sh command line utility and Linux cron utility to automate reporting jobs, see the NSM online Help.

Related Topics
- NSM Logs and Reports Overview on page 129
- Intrusion Detection and Prevention Reporter Overview on page 143

Configuring Log Suppression

You can configure log suppression if you want to reduce the number of logs displayed in the NSM log viewer. If you enable log suppression, NSM displays a single record for multiple occurrences of similar events, along with a count of all such occurrences.

To enable and configure log suppression:
1. In the NSM Device Manager, double-click the IDP device to display the configuration editor.
2. Click **Sensor Settings**.
3. Click **Load-Time Parameters**.
4. Complete the settings related to log suppression using Table 65 on page 140.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable log suppression</td>
<td>Log suppression is enabled by default. Use this setting to turn log suppression off and on.</td>
</tr>
<tr>
<td>Include destination IPs when performing log suppression</td>
<td>When log suppression is enabled, multiple occurrences of events with the same source IP, service, and matching attack object generate a single log record with a count of occurrences. If you enable this option, log suppression combines log records for events with the same destination IP.</td>
</tr>
<tr>
<td>Number of log occurrences after which log suppression begins</td>
<td>This number represents the number of identical log records received before suppression starts. The default is 1 (meaning log suppression begins with the first redundancy).</td>
</tr>
<tr>
<td>Maximum number of logs that log suppression can operate on</td>
<td>When log suppression is enabled, IDP must cache log records so that it can identify when multiple occurrences of the same event occur. This number represents the number of log records in the IDP Management Server that IDP tracks for log suppression. The default is 16384 log records.</td>
</tr>
<tr>
<td>Time (seconds) after which suppressed logs will be reported</td>
<td>When log suppression is enabled, the IDP device maintains a count of multiple occurrences of the same event. This number represents the number of seconds that pass before IDP reports a single log entry containing the count of occurrences. The default is 10 seconds.</td>
</tr>
<tr>
<td>Maximum number of logs that can be stored</td>
<td>Determines the limit for logs stored on the IDP device. The default is 50,000. The minimum value is 1,000. The maximum is 65,535.</td>
</tr>
</tbody>
</table>
Table 65: IDP Configuration: Log Suppression Settings *(continued)*

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
</table>
| Maximum number of packet captures that can be stored | Determines the limit for packet captures stored on the IDP device. The default is 10,000.  
The minimum value is 100; the maximum is 1,000 packets. The maximum is 65,535. |

**Related Topics**
- NSM Logs and Reports Overview on page 129
- Configuring Syslog Collection (NSM Procedure) on page 80
Chapter 13

Working with Intrusion Detection and Prevention Reporter Reports

- Intrusion Detection and Prevention Reporter Overview on page 143

Intrusion Detection and Prevention Reporter Overview

IDP reports are representations of log data, aggregated and sorted to facilitate network and security analysis. The standalone IDP solution supports both centralized, aggregated reporting through NSM and on-box reporting for a singular IDP device instance through IDP Reporter.

You can perform the following reporting tasks:

- View predefined reports on attacks.
- Generate reports based on criteria you specify
- Create jobs that regularly generate predefined or custom reports and e-mail them to customers or other third-party organizations.

For more information on using IDP Reporter, see the IDP Reporter User’s Guide.

Related Topics

- NSM Logs and Reports Overview on page 129
- Creating NSM Custom Reports on page 137
Part 5
Index

- Index on page 147
Index

C
customer support ........................................................xvi
  contacting JTAC.....................................................xvi

S
Security.................................................................13
  support, technical See technical support

T
  technical support
    contacting JTAC................................................xvi