

IDP Series

Deployment Scenarios

Release



Published: 2011-04-26
Part Number: , Revision 02

Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, California 94089
USA
408-745-2000
www.juniper.net

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, 1993, 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, Junos, Steel-Belted Radius, NetScreen, and ScreenOS are registered trademarks of Juniper Networks, Inc. in the United States and other countries. The Juniper Networks Logo, the Junos logo, and JunosE are trademarks 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.

IDP Series IDP Series Deployment Scenarios
Copyright © 2011, Juniper Networks, Inc.
All rights reserved.

Revision History
April 2011—Revision 02

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 OS 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 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 and regulations of any United States and any applicable foreign agency or authority, and not to 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 III) 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 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

	Preface	xiii
	Objectives	xiii
	Audience	xiii
	Documentation Conventions	xiii
	Related Documentation	xv
	Requesting Technical Support	xvi
	Self-Help Online Tools and Resources	xvi
	Opening a Case with JTAC	xvii
Chapter 1	Out-of-Path Deployments	1
	Sniffer Mode Overview	1
	Topology	1
	Purpose	2
	Limitations	2
	Configuration Overview	3
Chapter 2	In-Path Deployments	5
	Transparent Mode Overview	5
	Topology	5
	Purpose	6
	Link Aggregation	7
	Limitations	9
	Configuration Overview	9
	Mixed Mode Overview	10
	Topology	10
	Purpose	11
	Limitations	11
	Configuration Overview	11
	Simulation Mode Overview	12
	Topology	12
	Purpose	12
	Configuration Overview	13
	Logging	13
	In-Path Deployments: Bypass and PPM Features	15
	Layer 2 Bypass	15
	Internal Bypass	16
	External Bypass	17
	Peer Port Modulation	18

Chapter 3	Redundant Path Deployments (Failover)	21
	Third-Party High Availability Support and Limitations	21
	Third-Party High Availability Overview	21
	State Synchronization	21
	Link State Signaling	22
	Third-Party High Availability Requirements	23
	State Sync Limitations	24
	IDP Series HA Signaling Script Log Messages	25
	Example: IDP Series HA Design with Juniper Networks ScreenOS Firewalls	26
	Topology	26
	Deployment Steps	27
	Example: IDP Series HA Design with Juniper Networks EX Series Switches	32
	Topology	32
	Deployment Steps	34
	Example: IDP Series HA Design with Cisco Catalyst Switches	37
	Topology	37
	Deployment Steps	39
	Workflow: Upgrading an IDP OS 4.1r4 Cluster to IDP OS 5.1	44
Chapter 4	Coordinated Threat Control	49
	Deploying IDP Series with Juniper Networks Access Control Devices for	
	Coordinated Threat Control	49
	Purpose	49
	Topology	49
	Configuration Overview	52
	Integration Notes	53
Chapter 5	User-Role-Based Security Policies	55
	Deploying IDP Series with an IC Series Device to Implement User-Role-Based	
	Security Policies	55
	Purpose	55
	Topology	56
	Understanding Communication Between IC Series and IDP Series	
	Devices	57
	Configuration Overview	58

List of Figures

Chapter 1	Out-of-Path Deployments	1
	Figure 1: Network Diagram: Sniffer Mode	2
	Figure 2: ACM Configure Virtual Routers Page	3
Chapter 2	In-Path Deployments	5
	Figure 3: Network Diagram: Transparent Mode	6
	Figure 4: Example: Link Aggregation and Asymmetric Routes	8
	Figure 5: ACM Configure Virtual Routers Page	10
	Figure 6: Mixed Deployment Mode	11
	Figure 7: Packet Processing in Simulation Mode	13
	Figure 8: NSM Log Viewer: Simulation Mode Logs	14
	Figure 9: Internal Bypass	16
	Figure 10: External Bypass	18
	Figure 11: Peer Port Modulation	19
Chapter 3	Redundant Path Deployments (Failover)	21
	Figure 12: Redundant Path Design: IDP Series HA Depends on NSRP (Juniper Networks SSG Series)	27
	Figure 13: ACM Third-Party HA Pages	29
	Figure 14: NSM Device Cluster	30
	Figure 15: Redundant Path Design: IDP Series HA Depends on STP (Juniper Networks EX Series)	33
	Figure 16: ACM Third-Party HA Pages	35
	Figure 17: NSM Device Cluster	36
	Figure 18: Redundant Path Design: IDP Series HA Depends on STP (Cisco Catalyst Switch)	38
	Figure 19: ACM Third-Party HA Pages	42
	Figure 20: NSM Device Cluster	43
Chapter 4	Coordinated Threat Control	49
	Figure 21: Coordinated Threat Control Deployment Diagram: SA Series Split Deployment	50
	Figure 22: Coordinated Threat Control Deployment Diagram: SA Series Internal Deployment	51
	Figure 23: Coordinated Threat Control Deployment Diagram: IC Series Deployment	52
	Figure 24: ACM: Generating a One-Time Password for the Connection from an SA Series or IC Series Appliance	53
	Figure 25: IC Series Admin Console: Configuring the Connection to the IDP Series Appliance	53
Chapter 5	User-Role-Based Security Policies	55

Figure 26: Coordinated Threat Control Deployment Diagram: IC Series Deployment	56
Figure 27: Communication Among User-Role-Based Policy Deployment Components	57
Figure 28: ACM: Generating a One-Time Password for the Connection from an IC Series Device	58
Figure 29: IC Series Admin Console: Configuring the Connection to the IDP Series Appliance	58

List of Tables

	Preface	xiii
	Table 1: Notice Icons	xiv
	Table 2: Text Conventions	xiv
	Table 3: Syntax Conventions	xv
	Table 4: Related IDP Series Documentation	xv
Chapter 1	Out-of-Path Deployments	1
	Table 5: Sniffer Mode: Features and Limitations	3
Chapter 2	In-Path Deployments	5
	Table 6: Transparent Mode: Features and Limitations	9
Chapter 3	Redundant Path Deployments (Failover)	21
	Table 7: Third-Party HA Requirements	23
	Table 8: IDP Series HA Failover Cluster: Processing by the Standby Device	24
	Table 9: IDP Series HA Signaling Script Log Messages	25
	Table 10: IDP Series Configuration Guidelines	28
	Table 11: IDP Series Configuration Guidelines	35
	Table 12: IDP Series Configuration Guidelines	42

Preface

- Objectives on page xiii
- Audience on page xiii
- Documentation Conventions on page xiii
- Related Documentation on page xv
- Requesting Technical Support on page xvi

Objectives

The purpose of this guide is to provide complete procedures for the administration tasks related to the use of Juniper Networks IDP Series Intrusion Detection and Prevention (IDP) appliances.

For descriptions of features, limitations, and examples, see the *IDP Series Concepts and Examples Guide*.

For details on using Network and Security Manager centralized management and user interface features, see the NSM documentation.

Audience

This guide is intended for network administrators who are familiar with TCP/IP networks and network security issues.

Documentation 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

Icon	Meaning	Description
	Informational note	Indicates important features or instructions.
	Caution	Indicates a situation that might result in loss of data or hardware damage.
	Warning	Alerts you to the risk of personal injury or death.
	Laser warning	Alerts you to the risk of personal injury from a laser.

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

Table 2: Text Conventions

Convention	Description	Examples
Bold typeface like this	<ul style="list-style-type: none"> Represents commands and keywords in text. Represents keywords Represents UI elements 	<ul style="list-style-type: none"> Issue the clock source command. Specify the keyword exp-msg. Click User Objects
Bold typeface like this	Represents text that the user must type.	user input
<code>fixed-width font</code>	Represents information as displayed on the terminal screen.	<pre>host1# show ip ospf Routing Process OSPF 2 with Router ID 5.5.0.250 Router is an area Border Router (ABR)</pre>
Key names linked with a plus (+) sign	Indicates that you must press two or more keys simultaneously.	Ctrl + d
<i>Italics</i>	<ul style="list-style-type: none"> Emphasizes words Identifies variables 	<ul style="list-style-type: none"> The product supports two levels of access, <i>user</i> and <i>privileged</i>. <i>clusterID</i>, <i>ipAddress</i>.
The angle bracket (>)	Indicates navigation paths through the UI by clicking menu options and links.	Object Manager > User Objects > Local Objects

Table 3 on page xv defines syntax conventions used in this guide.

Table 3: Syntax Conventions

Convention	Description	Examples
Words in plain text	Represent keywords	terminal length
Words in italics	Represent variables	<i>mask, accessListName</i>
Words separated by the pipe () symbol	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.	diagnostic line
Words enclosed in brackets ([])	Represent optional keywords or variables.	[internal external]
Words enclosed in brackets followed by and asterisk ([]*)	Represent optional keywords or variables that can be entered more than once.	[level1 level2 11]*
Words enclosed in braces ({ })	Represent required keywords or variables.	{ permit deny } { in out } { clusterId ipAddress }

Related Documentation

Table 4 on page xv lists related IDP Series documentation.

Table 4: Related IDP Series Documentation

Document	Description
Release notes	Contains information about what is included in a specific product release: supported features, unsupported features, changed features, known problems, and resolved problems. If the information in the release notes differs from the information found in the documentation set, follow the release notes.
IDP Detector Engine release notes	Provides information about IDP Detector Engine releases, including new features, changed features, fixed problems, and known issues.
J-Security Center Attack Signatures	Lists predefined attack signatures developed by J-Security Center.
J-Security Center Application Signatures	Lists predefined application signatures developed by J-Security Center.
IDP Series installation guides	Describes IDP Series hardware and provides instructions for installing, configuring, updating, and servicing the device.
IDP Series Feature Documentation	A collection of topics from the <i>IDP Series Administration Guide</i> and <i>IDP Series Concepts and Examples Guide</i> , in HTML.
IDP Series Administration Guide	Provides procedures for completing IDP Series administration tasks with the Network and Security Manager (NSM) central management program; with the IDP Series device Appliance Configuration Manager (ACM); and with the IDP Series device command-line interface (CLI).
IDP Series Concepts and Examples Guide	Explains IDP Series features and provides examples of how to use the system.

Table 4: Related IDP Series Documentation (*continued*)

Document	Description
<i>IDP Series Custom Attack Objects Reference and Examples Guide</i>	Provides examples and reference information for creating custom attack objects.
<i>IDP Reporter User's Guide</i>	Describes how to use IDP Reporter, an on-box reporting platform that includes predefined reports on attack detection and application usage. You can also use IDP Reporter to schedule regular publication of reports that are of interest to you or your stakeholders.

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.

- JTAC policies—For a complete understanding of our JTAC procedures and policies, review the *JTAC User Guide* located at <http://www.juniper.net/us/en/local/pdf/resource-guides/7100059-en.pdf>.
- Product warranties—For product warranty information, visit <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/>
- Search for known bugs: <http://www2.juniper.net/kb/>
- Find product documentation: <http://www.juniper.net/techpubs/>
- Find solutions and answer questions using our Knowledge Base: <http://kb.juniper.net/>
- Download the latest versions of software and review release notes: <http://www.juniper.net/customers/csc/software/>
- Search technical bulletins for relevant hardware and software notifications: <http://www.juniper.net/alerts/>
- Join and participate in the Juniper Networks Community Forum: <http://www.juniper.net/company/communities/>
- Open a case online in the CSC Case Management tool: <http://www.juniper.net/cm/>

To verify service entitlement by product serial number, use our Serial Number Entitlement (SNE) Tool: <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> .

CHAPTER 1

Out-of-Path Deployments

- Sniffer Mode Overview on page 1

Sniffer Mode Overview

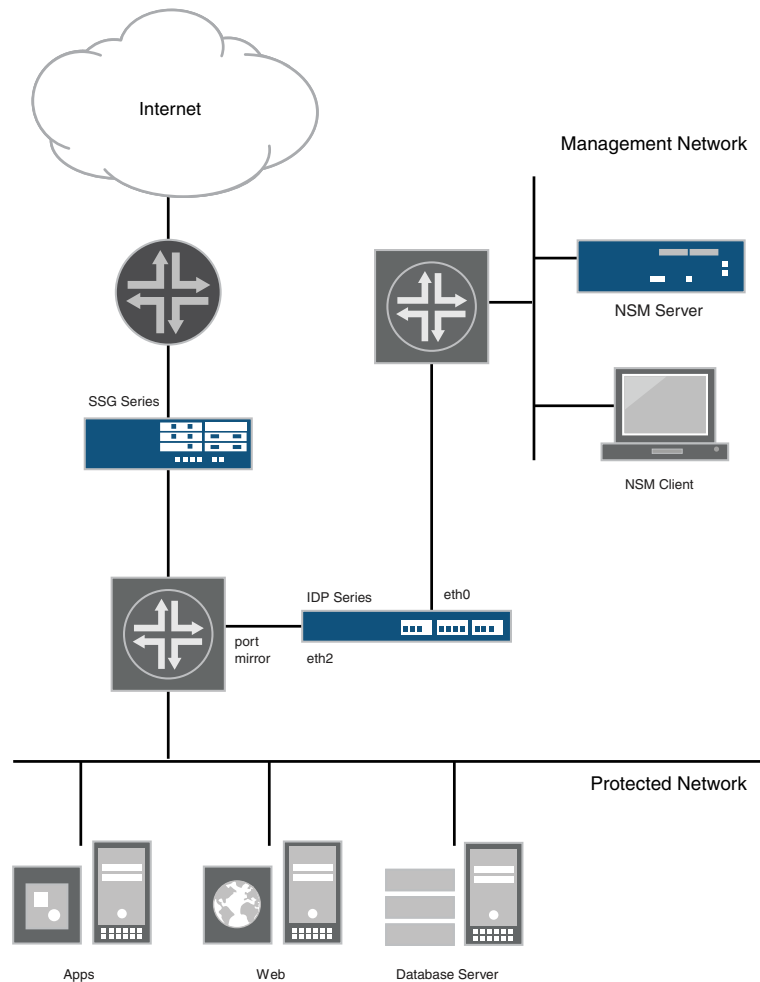
The following sections give an overview of sniffer mode deployments:

- Topology on page 1
- Purpose on page 2
- Limitations on page 2
- Configuration Overview on page 3

Topology

Figure 1 on page 2 shows a basic topology for a sniffer mode deployment. The IDP Series device is not in the forwarding path of network traffic and cannot become a point-of-failure.

Figure 1: Network Diagram: Sniffer Mode



In sniffer mode, the IDP Series device is not directly involved with packet flow. You connect an IDP Series device traffic interface to a port mirror or Switched Port Analyzer (SPAN) port. The IDP Series device analyzes the mirrored traffic based on your security policy and logs matching traffic. For some attacks, the IDP Series device can send TCP resets. However, this action does not guarantee protection, as attacks might have already happened before the reset or the attacker might persist.

Purpose

You deploy the IDP Series device in sniffer mode if you want to learn about security threats in your network but not disrupt connections.

Limitations

Table 5 on page 3 lists the features and the limitations of sniffer mode.

Table 5: Sniffer Mode: Features and Limitations

Features	Limitations
<ul style="list-style-type: none"> Replaces the current intrusion detection with minimal effort Does not create an additional point-of-failure gateway Detects attacks according to your security policy rules Performs the following security policy actions: <ul style="list-style-type: none"> Close Client and Server Close Client Close Server IP Close IP Notify 	<ul style="list-style-type: none"> Requires a hub or the SPAN port of a network switch Cannot perform the following security policy actions: <ul style="list-style-type: none"> Drop Packet Drop Connection Mark Diffserv Rate limit IP actions, such as IP block Does not inspect HTTPS traffic that requires interdiction with the SSL forward-proxy feature Does not support SYN Protector rulebase in relay mode Does not support Network Honeypot rulebase

Configuration Overview

You enable sniffer mode with the Appliance Configuration Manager (ACM). In a sniffer mode deployment, you typically connect only a single IDP Series interface to the switch port. However, in ACM, you only have the option to configure interface pairs. Hence, you use ACM to enable sniffer mode for the pair of interfaces that includes the sniffer interface.

Figure 2 on page 3 shows the ACM Configure Virtual Routers page. Note that bypass settings are not applicable to sniffer mode because sniffer mode interfaces are not in the path of network traffic.

Figure 2: ACM Configure Virtual Routers Page

Configure Virtual Routers

In this step, you must configure the interfaces that the IDP Sensor will use to handle traffic.

For each pair of interfaces, select the mode you want each pair to run in.

Active?	Interfaces	Virtual Router	Mode	NIC State (after system unavailability)	NIC State (after graceful shutdown)
<input checked="" type="checkbox"/>	eth2,eth3	vr0	<input type="radio"/> Transparent <input checked="" type="radio"/> Sniffer	NICs off	NICs off
<input checked="" type="checkbox"/>	eth4,eth5	vr1	<input type="radio"/> Transparent <input checked="" type="radio"/> Sniffer	NIC bypass	NIC bypass
<input checked="" type="checkbox"/>	eth6,eth7	vr2	<input checked="" type="radio"/> Transparent <input type="radio"/> Sniffer	NIC bypass	NIC bypass
<input checked="" type="checkbox"/>	eth8,eth9	vr3	<input checked="" type="radio"/> Transparent <input type="radio"/> Sniffer	NIC bypass	NIC bypass
<input checked="" type="checkbox"/>	eth10,eth11	vr4	<input checked="" type="radio"/> Transparent <input type="radio"/> Sniffer	NIC bypass	NIC bypass

☒ Enable layer2 bypass

☐ Enable Peer Port Modulator

Failover timeout value: 1

[Next Step](#)

Related Documentation

- Transparent Mode Overview on page 5
- Mixed Mode Overview on page 10
- Simulation Mode Overview on page 12

CHAPTER 2

In-Path Deployments

- Transparent Mode Overview on page 5
- Mixed Mode Overview on page 10
- Simulation Mode Overview on page 12
- In-Path Deployments: Bypass and PPM Features on page 15

Transparent Mode Overview

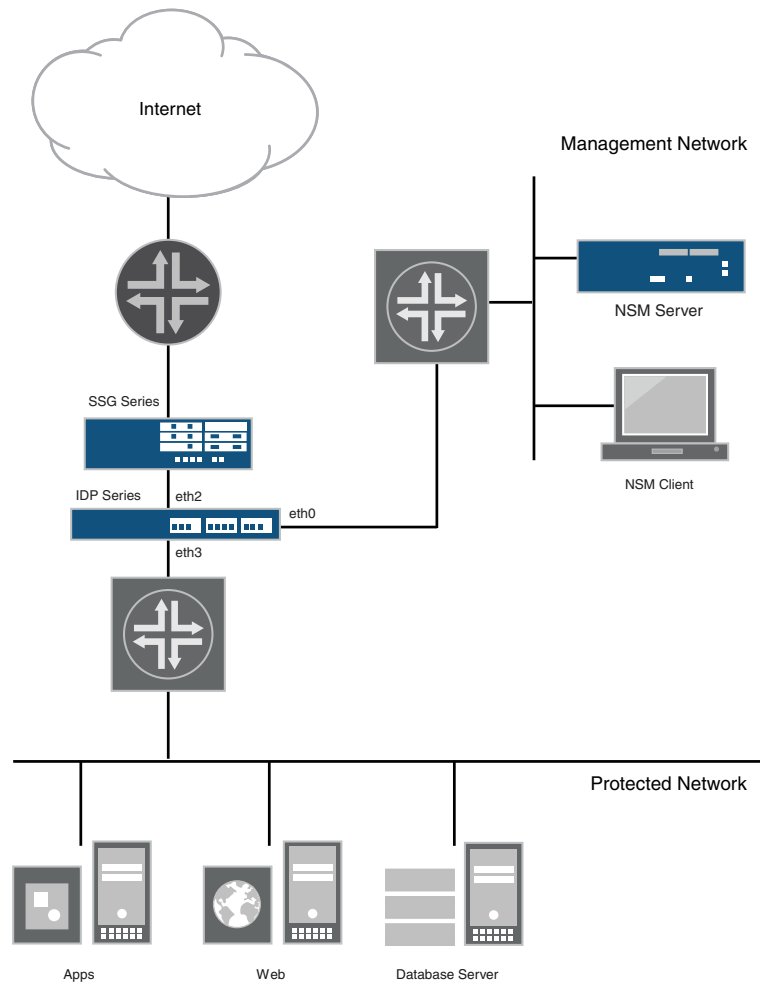
The following sections give an overview of transparent mode deployments:

- Topology on page 5
- Purpose on page 6
- Link Aggregation on page 7
- Limitations on page 9
- Configuration Overview on page 9

Topology

Figure 3 on page 6 shows a basic topology for a transparent mode deployment.

Figure 3: Network Diagram: Transparent Mode



In transparent mode, you deploy the IDP Series device in the path of network traffic. You connect the IDP Series device traffic interfaces directly to network devices, such as firewalls or switches. You do not have to configure the firewall or switch devices to be aware of the IDP Series device.

Purpose

You deploy an IDP Series device in transparent mode when you are ready to take action against network attacks. In transparent mode, the IDP Series device drops or forwards traffic according to your configuration and IDP security policy. In particular:

- **Layer 2**—Drops or passes through Layer 2 traffic according to your Layer 2 bypass setting.

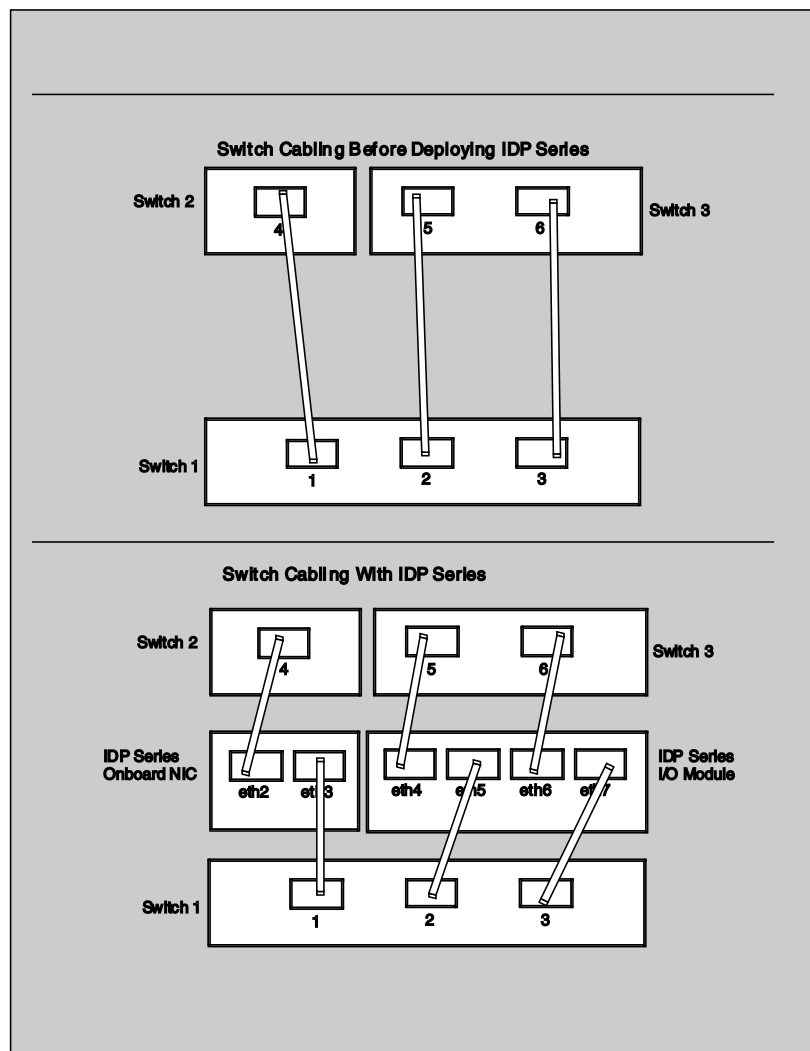
- Layer 3—Sets up a flow and processes according to two types of rules:
 - Implicit rules—Performs packet header checks and drops nonconforming traffic.
 - Security policy rules—Inspects traffic and processes the rules you specify to determine whether to drop, forward, or apply a DSCP code point to the traffic.
- Encapsulated and encrypted traffic—Passes it through by default. You can enable decapsulation and decryption to inspect GRE, GTP, IPsec ESP NULL, MPLS, and SSL.

Link Aggregation

In a transparent mode deployment, link aggregation and asymmetric routes are also transparent to the IDP Series device. In other words, you do not need to perform any special configuration on either the IDP Series device or surrounding network device to handle these cases.

In Figure 4 on page 8, Switch 1 passes traffic with Switch 2 and Switch 3. Assume VLAN 10 is the path Switch 1: Port 1 and Switch 2: Port 4; VLAN 20 is the path Switch 1: Port 2 and Switch 3 Port 5; and VLAN 30 is the path Switch 1: Port 3 and Switch 3: Port 6.

Figure 4: Example: Link Aggregation and Asymmetric Routes



The IDP Series device does not affect how your network handles link aggregation. In the example above with 3 network paths, you can aggregate switch interfaces and throughput so that one or all three paths are used, as long as the throughput is not greater than the maximum supported by the IDP Series device.

The IDP Series device handles asymmetric routes transparently. Let's consider an HTTP transaction where the client request traverses Switch 1:Port 1 > eth3 > eth2 > Switch 2:Port 4 and ultimately to a Web server farm. Assume the Web servers are load balanced in such a way that the server response traverses Switch 3:Port 5 > eth4 > eth5 Switch 1:Port 2 to the client. Because the IDP Series virtual routers belong to one subscriber, the

flow and security policy modules are aware that these client-to-server and server-to-client segments belong to the same session. If an attack is detected in a client-to-server flow, and the rule action is to close the client and server connection, then the client-side RST packet is sent through eth2 and the server-side RST packet is sent through eth3. Likewise, if the attack detected belongs to a server-to-client flow, then the client-side RST packet is sent through eth4, and the server-side RST packet is sent through eth5.

Limitations

Table 6 on page 9 lists the features and limitations of transparent mode.

Table 6: Transparent Mode: Features and Limitations

Features	Limitations
<ul style="list-style-type: none"> • Simple, transparent deployment • No changes to routing tables or network equipment • Supports all IDP security policy rulebases and all rule actions • Optionally passes through Layer 2 traffic • Passes through non-IP and non-ARP traffic • Passes through heartbeats used in deployments with an external bypass unit • Passes through bridge protocol data unit (BPDU) packets used in deployments with Spanning Tree Protocol (STP) • Internal bypass, flow bypass under congestion, and autorecovery features minimize risk that the IDP Series appliance will be a point of failure 	<ul style="list-style-type: none"> • Cannot connect IP networks with different address spaces

Configuration Overview

You enable transparent mode with the Appliance Configuration Manager (ACM). With ACM, you configure a deployment mode for each pair of interfaces. (In ACM, a pair of interfaces is referred to as a virtual router.)

Figure 5 on page 10 shows the ACM Configure Virtual Routers page.

Figure 5: ACM Configure Virtual Routers Page

Configure Virtual Routers

In this step, you must configure the interfaces that the IDP Sensor will use to handle traffic.

For each pair of interfaces, select the mode you want each pair to run in.

Active?	Interfaces	Virtual Router	Mode	NIC State (after system unavailability)	NIC State (after graceful shutdown)
<input checked="" type="checkbox"/>	eth2,eth3	vr0	<input checked="" type="radio"/> Transparent <input type="radio"/> Sniffer	NICs off	NICs off
<input checked="" type="checkbox"/>	eth4,eth5	vr1	<input checked="" type="radio"/> Transparent <input type="radio"/> Sniffer	NIC bypass	NIC bypass
<input checked="" type="checkbox"/>	eth6,eth7	vr2	<input checked="" type="radio"/> Transparent <input type="radio"/> Sniffer	NIC bypass	NIC bypass
<input checked="" type="checkbox"/>	eth8,eth9	vr3	<input checked="" type="radio"/> Transparent <input type="radio"/> Sniffer	NIC bypass	NIC bypass
<input checked="" type="checkbox"/>	eth10,eth11	vr4	<input checked="" type="radio"/> Transparent <input type="radio"/> Sniffer	NIC bypass	NIC bypass

☒ Enable layer2 bypass

☐ Enable Peer Port Modulator

Failover timeout value: 1

[Next Step](#)

Related Documentation

- In-Path Deployments: Bypass and PPM Features on page 15
- Sniffer Mode Overview on page 1
- Mixed Mode Overview on page 10
- Simulation Mode Overview on page 12

Mixed Mode Overview

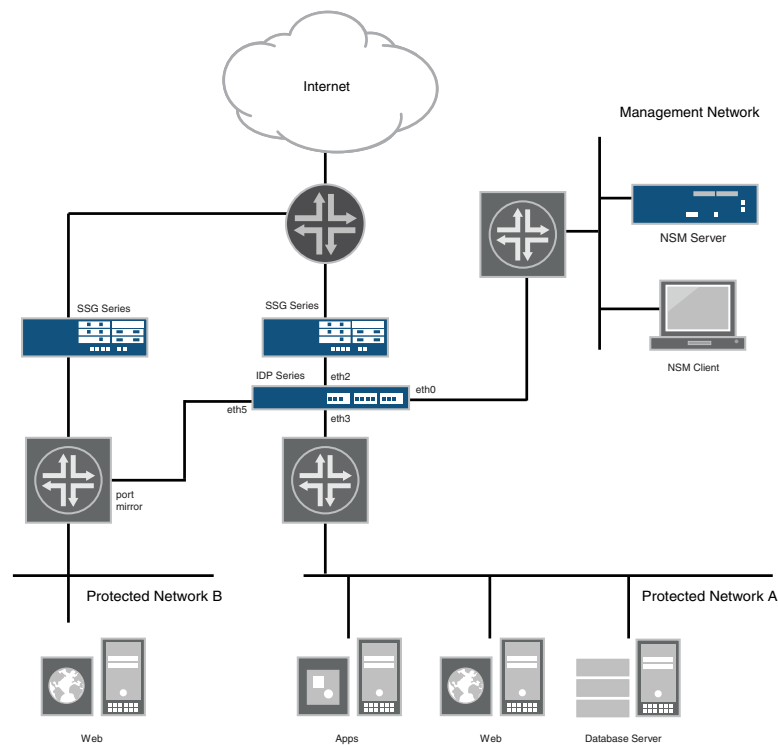
The following sections give an overview of a mixed mode deployment:

- Topology on page 10
- Purpose on page 11
- Limitations on page 11
- Configuration Overview on page 11

Topology

Figure 6 on page 11 shows a network design where the eth2 and eth3 interface pair is deployed as a virtual router in the path of Network A servers. The eth5 interface is deployed as a sniffer interface to inspect traffic mirrored from Network B.

Figure 6: Mixed Deployment Mode



Purpose

In a mixed mode deployment, you deploy the IDP Series device in the network path just like a transparent mode deployment. The mixed mode feature allows you to configure an “extra” virtual interface as a sniffer mode interface and use it to sniff traffic that traverses a different network segment.

Limitations

Be sure your deployment does not cause the IDP Series to examine the same network segment twice.

Configuration Overview

You use the Appliance Configuration Manager (ACM) to configure interface settings for each pair of interfaces. In ACM, a pair of interfaces is referred to as a virtual router. In a mixed mode deployment, you use ACM to designate that one or more pairs are deployed in transparent mode and one or more pairs in sniffer mode.

- Related Documentation**
- [Sniffer Mode Overview on page 1](#)
 - [Transparent Mode Overview on page 5](#)
 - [Simulation Mode Overview on page 12](#)

Simulation Mode Overview

Simulation mode is not a deployment mode, but rather an operational mode. The following sections give an overview of simulation mode:

- [Topology on page 12](#)
- [Purpose on page 12](#)
- [Configuration Overview on page 13](#)
- [Logging on page 13](#)

Topology

The purpose of simulation mode is to enable you to evaluate expected results when you deploy the IDP Series device in transparent mode or sniffer mode. Therefore, in your network topology, you install and connect the IDP Series device where you intend to deploy it in transparent (in-path) or sniffer mode (out-of-path).

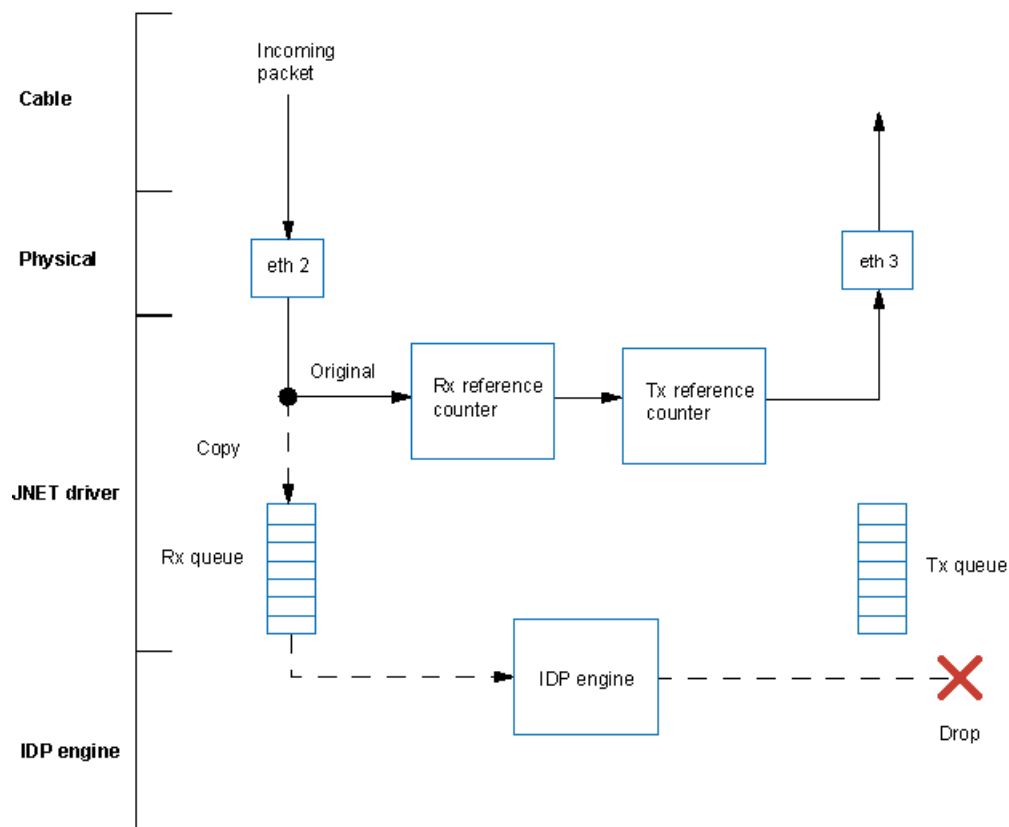
Purpose

You operate an IDP Series device in simulation mode in the following situations:

- When you first deploy the IDP Series device in your network and you want to evaluate the security actions it takes without disrupting traffic.
- When you implement a new feature or change a security policy and you want to evaluate the impact without disrupting traffic.
- As a workaround to avoid traffic outages when IDP processing is resulting in crashes and other failures.

In simulation mode, when the IDP Series device receives a packet, it makes a copy. It transmits the original packet uninspected through the egress interface and enqueues the duplicate packet into the JNET driver receive queue to be processed by the IDP engine. The IDP engine inspects the traffic against your security policy rules and implicit rules, and it generates logs when rules match. The IDP engine then drops the copy of the packet. Figure 7 on page 13 illustrates packet processing in simulation mode.

Figure 7: Packet Processing in Simulation Mode



NOTE: Because of packet queueing, when simulation mode is turned on, a few packets that are queued for processing and forwarding might be dropped. This results in retransmission depending on Layer 4 or Layer 7 behavior. When simulation mode is turned off, a few duplicate packets might be forwarded.

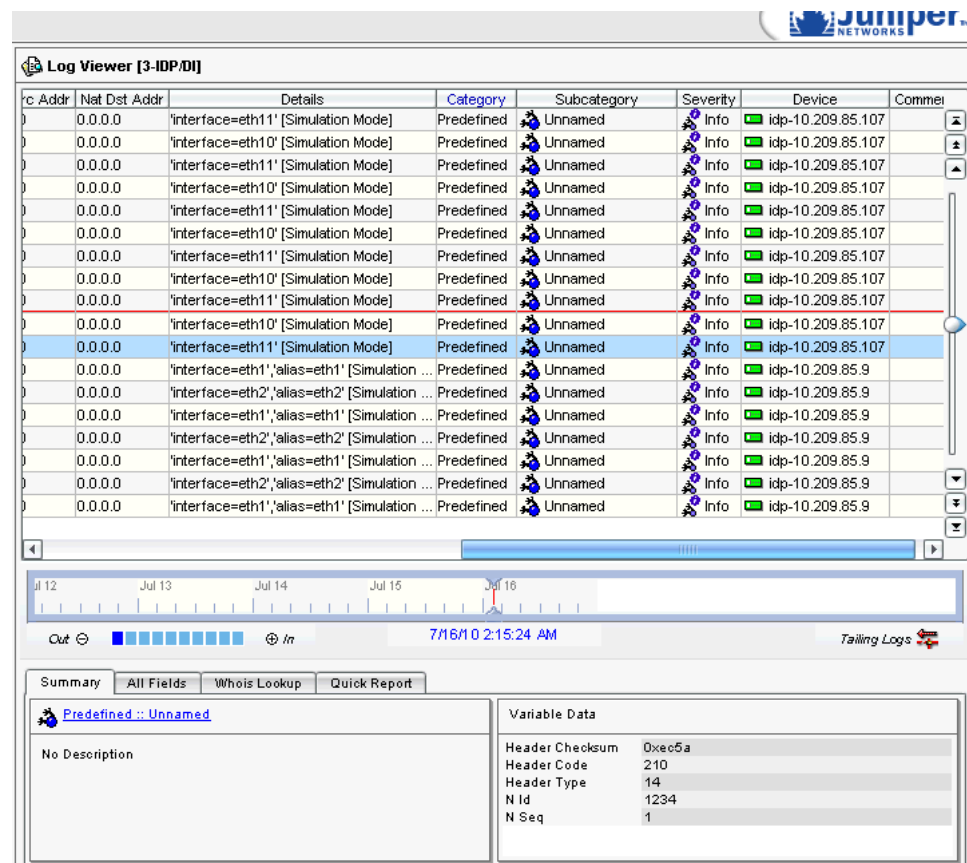
Configuration Overview

You use the CLI to enable or disable simulation mode. Simulation mode is disabled by default. You do not need to restart the IDP engine (`idp.sh`) or push a policy to enable or disable simulation mode.

Logging

In logs, the string [Simulation Mode] appears in the Details column, along with the details of the event. Figure 8 on page 14 shows a simulation mode log in the NSM log viewer. You can use NSM log and report filters to create log views and reports that filter for (or filter out) simulation mode logs.

Figure 8: NSM Log Viewer: Simulation Mode Logs



Related Documentation

The following related topics are included in *IDP Series Deployment Scenarios*:

- Sniffer Mode Overview on page 1
- Transparent Mode Overview on page 5

The following related topics are included in the *IDP Series Concepts and Examples Guide*

- Example: Getting Started with Simulation Mode
- Example: Using Simulation Mode to Maximize Uptime

The following related topic is included in the *IDP Series Administration Guide*

- Simulation Mode Task Summary

In-Path Deployments: Bypass and PPM Features

In an in-path deployment, the IDP Series device is deployed transparently “in the wire” between two network devices. Consequently, the IDP Series device can become a point-of-failure for the network path. We support a number of features to address the potential point-of-failure. You can:

- Deploy the IDP Series devices in a redundant path, failover topology.
- Enable internal or external bypass.
- Enable peer port modulation.

The following topics describe the bypass and PPM features:

- Layer 2 Bypass on page 15
- Internal Bypass on page 16
- External Bypass on page 17
- Peer Port Modulation on page 18

Layer 2 Bypass

You enable or disable Layer 2 bypass to determine how the IDP Series device handles Layer 2 packets.

When the IDP Series appliance is deployed in the path of network traffic, it can take three types of actions on the packets it receives:

- Drop it.
- Pass it through.
- Process it according to IDP OS rules to determine whether to drop it, forward it, rate limit, and so forth.

The IDP Series appliance processes Layer 2 traffic as follows:

- Processes address resolution protocol (ARP) and Layer 2 packets related to internet protocol (IPv4) traffic.
- Drops all other Layer 2 traffic, unless the Layer 2 bypass setting is enabled.
- When Layer 2 bypass is enabled, the IDP Series device passes through Layer 2 packets related to bypass and high availability deployments (such as heartbeats or Bridge Protocol Data Unit (BPDU) packets), and non-IPv4 packets and packets related to switching and routing protocols, such as IPv6, internetwork packet exchange (IPX), Cisco Discovery Protocol (CDP), and interior gateway routing protocol (IGRP), and so forth.

The IDP Series appliance processes TCP/IP traffic according to implicit rules related to traffic anomaly detection and explicit rules specified in the security policy.

Internal Bypass

The Internal Bypass feature is intended for deployments where a network security policy privileges availability over security. In the event of failure or graceful shutdown, traffic bypasses the IDP processing engine and is passed through the IDP Series device uninspected.

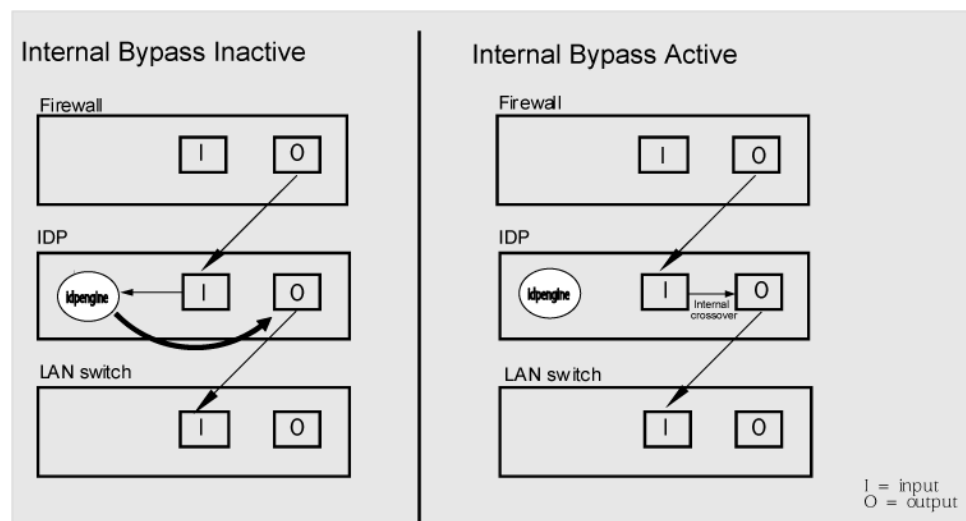
The Internal Bypass feature operates through a timing mechanism. When enabled, the timer on traffic interfaces counts down to a bypass trigger point. When the IDP Series appliance is turned on and available, it sends a reset signal to the traffic interface timer so that it does not reach the bypass trigger point. If the IDP OS encounters failure, then it fails to send the reset signal, the timer counts down to the trigger point, and the traffic interfaces enter a bypass state. If the IDP Series appliance is shut down gracefully, the traffic interfaces immediately enter bypass.

With copper NICs, the bypass mechanism joins the interfaces mechanically to form a circuit that bypasses IDP processing. Packets traverse the IDP Series device as if the path from eth2 (receiving interface) to eth3 (transmitting interface) were a crossover cable. No packet inspection or processing occurs.

With fiber NICs, the bypass mechanism uses optical relays instead of copper relays. During normal operations, the optical relays send light to the built-in optical transceivers. When bypass is triggered, the relays flip state, and the light signal is redirected to optically connect the two external ports.

Figure 9 on page 16 compares the data path when Internal Bypass is enabled but not activated with the data path when Internal Bypass is activated.

Figure 9: Internal Bypass



When the IDP OS resumes healthy operations, it sends a reset signal to the traffic interfaces, and the interfaces resume normal operation.



BEST PRACTICE: Our field engineers report that bypass occurs faster when copper NICs are configured with *fixed* speed and duplex settings. In contrast, when copper NICs have been set to *auto*, they must renegotiate with peers when recovering from bypass. We recommend you configure fixed speed and duplex settings. Be careful to observe the cabling guidelines (straight-through or cross-over) provided in the installation documentation [\[link\]](#). Be careful to set the same speed and duplex settings for the IDP Series interfaces and the network devices to which they are directly connected. To check speed and duplex settings, use the Linux `ethtool` or `dmesg | grep -i duplex` commands [\[link\]](#). (Do not use the `mii-tool` command. On IDP OS, `mii-tool` results are not reliable.) To configure NIC speed and duplex settings, use the ACM Configure Network Interface Hardware page [\[link\]](#).

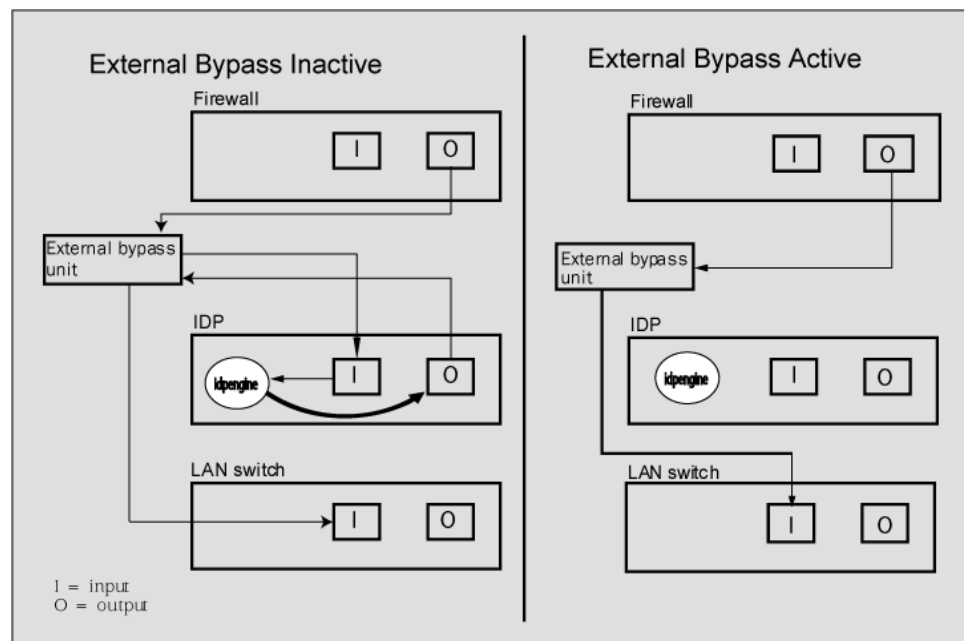


NOTE: You can enable bypass for all copper interface cards (onboard or I/O module) and for select fiber interface cards that support bypass. Refer to the product datasheets or installation documentation for information on which fiber interface cards support bypass.

External Bypass

The External Bypass setting supports third-party external bypass units. Deployments with external bypass units depend on the functionality of the external bypass unit to check the status of the IDP Series appliance and make the determination whether to send packets through or around the IDP Series device. Most external bypass units test for availability by sending heartbeat packets through the device. If the packets reach the expected destination, the external bypass unit allows the traffic to continue through the IDP Series appliance. If the packets fail to reach the expected destination, the external bypass unit determines the IDP Series is unavailable, so it forwards traffic around the IDP Series device. The IDP Series supports external bypass solutions by allowing the heartbeat traffic to pass through the device regardless of the Layer 2 Bypass setting. In other words, if you disable Layer 2 Bypass and enable External Bypass, most Layer 2 traffic will be dropped but the heartbeat traffic used in the external bypass deployment will be passed through. Figure 10 on page 18 compares the data path when External Bypass is enabled but not activated with the data path when External Bypass is activated.

Figure 10: External Bypass

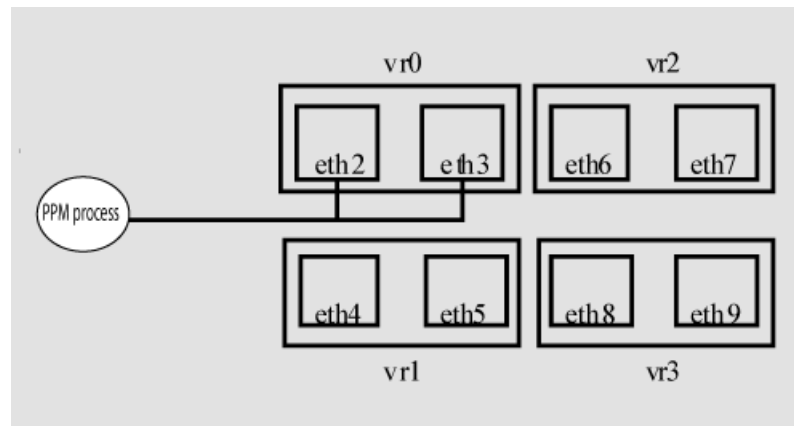


Peer Port Modulation

The peer port modulation (PPM) feature supports deployments where routers monitor link state to make routing decisions. In these deployments, a router might be set to monitor link state on only one side of the IDP Series device. Suppose, for example, the router monitors only the IDP inbound interface. Suppose the inbound interface remains up but the outbound interface goes down. The router watching the inbound link would detect an available link and forward traffic to the IDP Series device. Traffic would be dropped at the point of failure—the outbound link. PPM propagates a link loss state for one traffic interface to all interfaces in the IDP virtual router.

When PPM is enabled, a PPM daemon monitors the health of IDP traffic interfaces belonging to the same virtual router. If a traffic interface loses link, the PPM process turns off any associated network interfaces in the same virtual router so that other network devices detect that the virtual router is down and route around it. For example, assume you have enabled PPM and configured IDP virtual routers as shown in Figure 11 on page 19.

Figure 11: Peer Port Modulation



Suppose there is a network problem and eth3 goes down. The PPM daemon detects this and turns off the other interface in vr0: eth2. The interfaces in vr1, vr2, and vr3 are unaffected. After you fix the problem with eth3, the PPM daemon detects this, and turns on eth2.



NOTE: The PPM feature is independent of the bypass feature (NIC state setting). PPM is related to the *status of the link*, not the status of the IDP operating system. A link can be down even when the IDP operating system is healthy. Note, however, that PPM runs as a control plane process and operates only when the IDP Series device is turned on and the control plane is available. If the IDP operating system is unavailable, the PPM feature is also unavailable, regardless of the setting for the NIC state.



BEST PRACTICE: Network issues are easier to diagnose and correct when the link state is the same on both links in an interface pair. We recommend you enable PPM for (non-redundant) in-path deployments.

Related Documentation

The following related topics are included in the *IDP Series Deployment Scenarios* guide:

- Third-Party High Availability Support and Limitations on page 21

The following related topics are included in the *IDP Series Concepts and Examples Guide*:

- IDP Series Network Interfaces Overview
- IDP Series Operating System Overview

The following related topic is included in the *IDP Series Administration Guide*:

- Configuring Virtual Routers (ACM Procedure)

CHAPTER 3

Redundant Path Deployments (Failover)

- Third-Party High Availability Support and Limitations on page 21
- IDP Series HA Signaling Script Log Messages on page 25
- Example: IDP Series HA Design with Juniper Networks ScreenOS Firewalls on page 26
- Example: IDP Series HA Design with Juniper Networks EX Series Switches on page 32
- Example: IDP Series HA Design with Cisco Catalyst Switches on page 37
- Workflow: Upgrading an IDP OS 4.1r4 Cluster to IDP OS 5.1 on page 44

Third-Party High Availability Support and Limitations

The following sections describe IDP Series support for high availability deployments:

- Third-Party High Availability Overview on page 21
- Third-Party High Availability Requirements on page 23
- State Sync Limitations on page 24

Third-Party High Availability Overview

IDP OS Release 5.1 supports high availability in network designs where you have deployed redundant network paths and use the failure detection features of a firewall, router, or switch to manage the cutover from the primary path to the backup path in cases of failure. In these deployments, you implement:

- State synchronization between the primary and the standby IDP Series devices.
- Link state signaling. The IDP Series device must signal failure so that it can be predictably identified by the third-party failure detection mechanism.

The following sections provide details:

- State Synchronization on page 21
- Link State Signaling on page 22

State Synchronization

You establish state synchronization between the primary and the standby IDP Series device by connecting the IDP Series HA interfaces (eth1) with a crossover cable. In addition, you must use the Appliance Configuration Manager (ACM) to enable the Third-Party HA

setting. You can use the **sctop** command-line utility to monitor state and flow synchronization.

Link State Signaling

You enable an IDP Series link state signaling mechanism so that it responds as expected to the third-party device link checking mechanism. You have the following choices:

- Layer 2 bypass for Bridge Protocol Data Unit (BPDU) packets. In deployments that use spanning tree protocol (STP), the IDP Series device must be able to pass BPDU packets. Use ACM to enable Layer 2 bypass so that BPDU packets are passed through and not dropped. When the IDP engine is in a healthy state, it passes through the BPDU packets. When the IDP engine is shut down or in a failed state, it cannot pass BPDU packets. An STP switch deployment detects this and chooses an alternate path.
- Interface signaling. In deployments that use other link status detection methods, you can enable the interface signaling setting (setting `ha_interface_signal = 1`) so that all IDP Series interfaces are brought down when there is a problem with the device. The interface signaling script monitors the state of traffic interfaces (`eth2`, `eth3`, and so on) and IDP engines (`idpengine0`, `idpengine1`, and so on). In case of interface failure, the script brings down all peer interfaces so that the third-party link detection mechanism can properly detect failure. In case of IDP engine failure, the autorecovery feature attempts to restart the IDP engine. If the IDP engine cannot be restarted after six attempts, the auto-recovery process runs an **idp.sh stop** command. The interface signaling script then brings down all traffic interfaces.

After bringing down the traffic interfaces, the interface signaling script sleeps for 30 seconds to avoid link flapping issues. After 30 seconds, the script checks the state of the interface that had encountered the failure or the state of the IDP engine. When the underlying problem has been resolved, the interface signaling script brings up the peer interfaces.

Even when the interface signaling setting is disabled (setting `ha_interface_signal = 0`), the HA feature monitors the status of IDP engines. If an IDP engine fails, any remaining IDP engines are signaled to disregard the Layer 2 bypass setting and drop Layer 2 traffic, including BPDUs.

- Peer port modulation (PPM). If your IDP Series deployment uses only one pair of traffic interfaces, you can use PPM to monitor and propagate link state for the interface pair. In contrast to interface signaling, which propagates a failed state to all traffic interfaces, the PPM daemon propagates link state only to the paired interface on the other side (for example, `eth2` to `eth3`). If you enable both PPM and interface signaling, the PPM daemon is shut down to avoid conflicts.



NOTE: Due to a hardware limitation with 10 gigabyte fiber interface modules, interface signaling and PPM are not supported for the IDP8200 10 gigabyte fiber I/O module.

Third-Party High Availability Requirements

Table 7 on page 23 summarizes deployment component requirements. We support deployment of active-passive, failover pairs. We do not support active-active deployments.

Table 7: Third-Party HA Requirements

Component	Requirement
IDP Series devices	Hardware – same model.
	Software – same version.
	Same configuration and same security policy.
	Autorecovery enabled (default). HA can function if auto-recovery is disabled, but we recommend you leave it enabled so that easily recoverable conditions do not result in unnecessary failover operations.
	Traffic interfaces. Virtual routers (interface pairs) must be set to transparent mode. We have not tested and do not support HA state sync when virtual routers are configured in sniffer mode or when the device is deployed in mixed mode.
	You must enable one virtual router named vr0. When you enable HA with ACM, the HA interface (eth1), gets added to vr0. The eth1 interface is not involved in traffic forwarding. It must belong to vr0 as a system requirement.
	NOTE: The HA feature monitors interface status, so unplugging and plugging in interface cables is significant. Use the CLI hasignal.sh restart command to reinitialize HA interface monitoring any time you plug in or unplug a traffic interface.
	Simulation mode. Simulation mode is not a deployment mode, rather it is an operational mode. The simulation mode setting does not preclude your ability to enable HA or deploy the devices as an HA active-passive cluster. Note, however, that a device deployed in simulation mode is not likely to encounter failure.
	Layer 2 bypass enabled.
	NIC bypass set to Nics off . This setting is enforced by ACM. If you enable HA, you cannot enable NIC bypass.
HA interface	The eth1 interfaces must be connected directly with a cross-over cable (so must be physically close).
Third-party HA mechanism	<ul style="list-style-type: none"> • Juniper Networks ScreenOS firewalls, running NetScreen Redundancy Protocol (NSRP)* • Juniper Networks EX Series switches, running a spanning tree protocol: STP, MSTP, RTSP, or VSTP** • Other vendors' firewalls, running Virtual Router Redundancy Protocol (VRRP) • Other vendors' switches, running STP*** • Routers running Hot Standby Redundancy Protocol (HSRP)
<p>* IDP OS 5.1 was tested with Juniper Networks ISG1000 running ScreenOS version 5.4.0R3. ** IDP OS 5.1 was tested with Juniper Networks EX4200 running Junos OS 10.2R1. *** IDP OS 5.1 was tested with Cisco Catalyst C3500XL running version 12.0.</p>	

State Sync Limitations

When an IDP Series device receives network traffic, it sets up a flow of related packets so that it can inspect the network transaction for anomalies and attack signatures. When state synchronization between two IDP Series devices is enabled, the primary device sends TCP flow information to the standby IDP Series device whenever it sets up a new flow. As processing continues, the primary device sends application identification results to the standby device, populating the backup device application identification cache.

In the event of failure along the primary path, the switch or firewall cuts over to the redundant path, and the standby IDP Series device begins receiving traffic. Table 8 on page 24 describes limitations to state synchronization for the immediate “failover traffic” and for new sessions.

Table 8: IDP Series HA Failover Cluster: Processing by the Standby Device

Category	Limitations
Failover Traffic	<p>The initial load processed by the standby device might include retransmitted and midstream packets. Let's call these packets “failover traffic.” Because the standby device has accumulated state sync data, it attempts to correlate the failover traffic packets with the session data. When processing failover traffic, the standby device is able to match and enforce APE rules, but the following limitations are expected:</p> <ul style="list-style-type: none"> • Nested applications and custom applications. Due to a current limitation, the application cache results for nested applications and custom applications are not synchronized from primary to standby (PR 550567). Consequently, when the standby device performs APE rulebase processing for failover traffic, nested applications and custom applications are not identified using application identification feature methods. Instead, these are identified by service and standard port. • Intrusion detection. Neither flow-based or packet-based intrusion detection is possible (PR 559087). IDP rulebase rules cannot be enforced on failover traffic. The packets are passed through, uninspected.
New Traffic	<p>When the standby device receives new sessions, it creates a new flow them and processes them no differently from the primary device. However, be aware of the following observations:</p> <ul style="list-style-type: none"> • The IP Action table (such as IP block actions) is not synchronized. The standby device enforces its own IP Action table. Ultimately, this does not effect the security stance of the device. Instead of blocking the source IP immediately, the IDP Series device blocks the source IP after rule matching. • User session table. If you have implemented user-role-based policies, note that the user session table is not synchronized. Make sure you configure each device to receive user role information from the IC Series UAC device.

Related Documentation

- Example: IDP Series HA Design with Juniper Networks ScreenOS Firewalls on page 26
- Example: IDP Series HA Design with Juniper Networks EX Series Switches on page 32
- Example: IDP Series HA Design with Cisco Catalyst Switches on page 37
- Workflow: Upgrading an IDP OS 4.1r4 Cluster to IDP OS 5.1 on page 44

IDP Series HA Signaling Script Log Messages

HA signaling log messages are written to `/var/idp/device/sysinfo/logs/hasignal.timestamp`. HA signaling log messages are not sent to NSM or syslog servers. Table 9 on page 25 explains the conditions that generate HA signaling log messages.

Table 9: IDP Series HA Signaling Script Log Messages

Example Log	When Triggered
20101210001730:[WARN]:The UP & RUNNING nics are eth2 eth3 eth4 eth5 eth8 eth9 eth12 eth13	<p>Every time the IDP engine is restarted, IDP device rebooted, ACM configuration changed, or HA interface signaling script restarted, the HA signaling script generates a pair of logs listing traffic interfaces.</p> <p>This log lists the interfaces currently monitored by the HA interface signaling script.</p>
20101210001730:[WARN]:The considered nics are eth2 eth3 eth4 eth5 eth6 eth7 eth8 eth9 eth10 eth11 eth12 eth13	<p>Every time the IDP engine is restarted, IDP device rebooted, ACM configuration changed, or HA interface signaling script restarted, the HA signaling script generates a pair of logs listing traffic interfaces.</p> <p>The log lists the forwarding interfaces enabled in the ACM Configuring Virtual Routers page.</p>
20101210001730:[WARN]:Disabling HA signalling for engine failure, since auto-recovery is enabled	When auto recovery is enabled.
20101210005113:[WARN]:SIGNAL handler:HA signalling script gracefully getting terminated	Every time the IDP engine is restarted, IDP device rebooted, ACM configuration changed, or HA interface signaling script restarted, the HA signaling script is stopped and restarted.
20101210010839:[WARN]:NIC monitoring: One or more interfaces are down due to hw/sw failure	When interfaces are brought down.
20101210010839:[WARN]:NIC monitoring: About to bring down all the up & running interfaces	When any traffic interface goes down or IDP engine goes down (autorecovery disabled), all traffic interfaces are brought down (interface signaling enabled).
20101212224853:[WARN]:NIC monitoring: Interfaces with hw/sw issue are now up & running	When the downed interface comes up and the active node resumes (interface signaling enabled).
20101210010839:[WARN]:NIC monitoring: Blocking STP or similar such traffic	When interface signaling is disabled and a failover condition happens.
20101212224853:[WARN]:NIC monitoring: Allowing STP or similar such traffic	When the downed interface comes up and the active node resumes (interface signaling disabled).
20101212224853:[WARN]:ENGINE monitoring:IDP engine 2 terminated, about to signal third-party HA device	When autorecovery is disabled and one of the IDP engines goes down.
20101212224864:[WARN]:ENGINE monitoring:Bringing down any up & running interfaces	When autorecovery is disabled, interface signaling is enabled, and one of the IDP engines goes down.

Table 9: IDP Series HA Signaling Script Log Messages (*continued*)

Example Log	When Triggered
20101212224864:[WARN]:ENGINE monitoring:Blocking STP or similar such traffic	When autorecovery is disabled, interface signaling is disabled, and one of the IDP engines goes down.
20101212225126:[WARN]:Peer port modulator is being deliberately stopped.	If PPM and interface signaling are both enabled, this message warns you that the interface signaling script has stopped the PPM daemon.

Related Documentation • [Third-Party High Availability Support and Limitations on page 21](#)

Example: IDP Series HA Design with Juniper Networks ScreenOS Firewalls

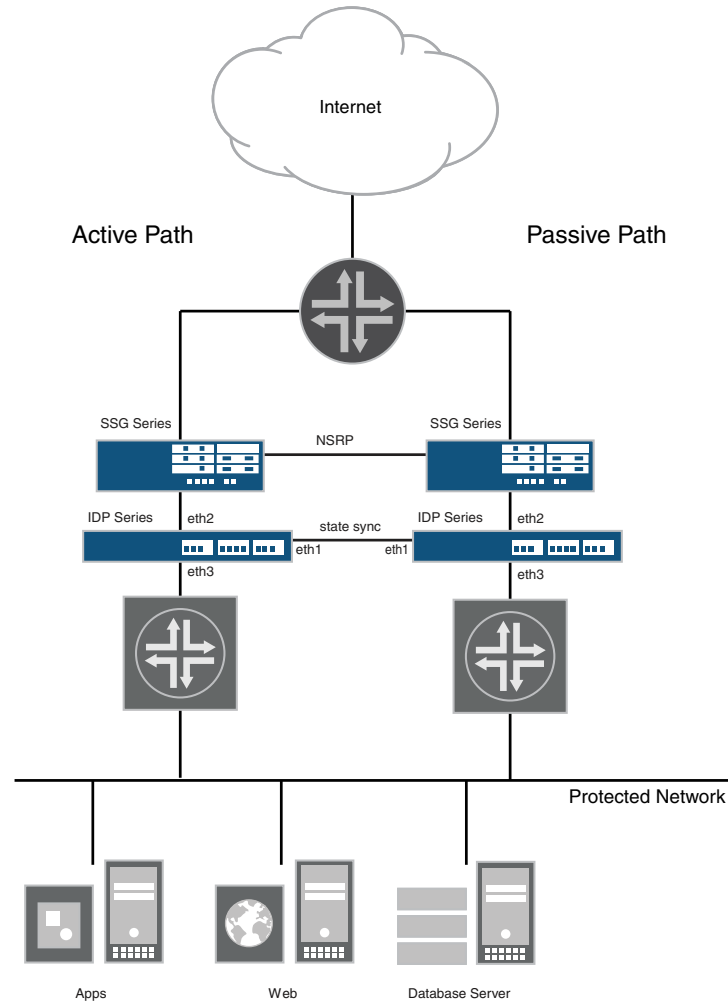
The following sections describe an example redundant path deployment where the Juniper Networks NetScreen Redundancy Protocol (NSRP) feature monitors the health of the network path:

- [Topology on page 26](#)
- [Deployment Steps on page 27](#)

[Topology](#)

Figure 12 on page 27 shows a network topology where there are redundant paths to the Internet. One path is active and the other is passive.

Figure 12: Redundant Path Design: IDP Series HA Depends on NSRP (Juniper Networks SSG Series)



In the deployment with IDP Series, the ScreenOS Track IP feature monitors the link state of the connection to the switch. If the IDP Series device encounters failure and cannot forward traffic, it causes the IP Track probe to the switch to fail. The firewall then forces traffic to the other path.

Deployment Steps

To deploy this solution, follow these basic steps:

1. Set up and configure the ScreenOS firewalls using the documentation that came with your firewall. Note the following requirements:
 - Hardware—Essentially, deploy the ScreenOS devices in an active-passive HA cluster as you normally would (without regard to the IDP Series devices).

- Failure detection mechanism—To establish a preferred primary and secondary path, you use NSRP priorities, with preemption. You can use one of the following NSRP methods to detect failure along the network path:

- Layer 2 path monitoring functions by checking that the physical ports are active and connected to other network devices. When you configured the redundant paths for the firewall deployment, you configured NSRP to monitor the status of its own interfaces and the devices to which those interfaces are connected. The interface monitoring feature can detect a down state of a connected IDP Series interface.

The firewall decides to failover to the redundant path only when all interfaces in the monitored zone are down. Therefore, in deployments where you have multiple interfaces connected, we recommend that you enable interface signaling on the IDP Series device.

- Layer 3 path monitoring, or IP tracking, functions by sending ping or ARP requests to up to 16 specified IP addresses at user-determined intervals and then monitoring if the targets respond. If you have not done so already, configure the firewall to use Track IP to monitor connection failure between itself and a list of Track IP hosts. The Track IP features sends ARP and ping traffic to the target hosts. If the value of the Track IP failure exceeds the user-specified threshold, the firewall decides the path is unavailable and initiates failover to the redundant path. Configure Track IP targets on the other side of the IDP Series device. When the IDP Series device is down, the ARP or ping traffic will fail, signaling to the firewall that the path is unavailable.

When the configured Track IP failure threshold is reached, the firewall initiates failover. All sessions (old sessions initiated before the failover and new sessions initiated after the failover) are forced to the other path.

Due to a hardware limitation, you cannot use interface signaling for an IDP8200 with 10 gigabyte fiber interfaces. In those deployments, use NSRP Layer 3 path monitoring.

For information about NSRP features, see the [ScreenOS Concepts and Examples Guide volume on high availability](#). For NSRP troubleshooting information, see the Juniper Networks [Knowledge Base](#).

2. Set up and configure the IDP Series devices. Note the following requirements.

Table 10: IDP Series Configuration Guidelines

Component	Guideline
IDP Series device hardware	Use a cross-over cable to connect one device HA port to the other HA port.

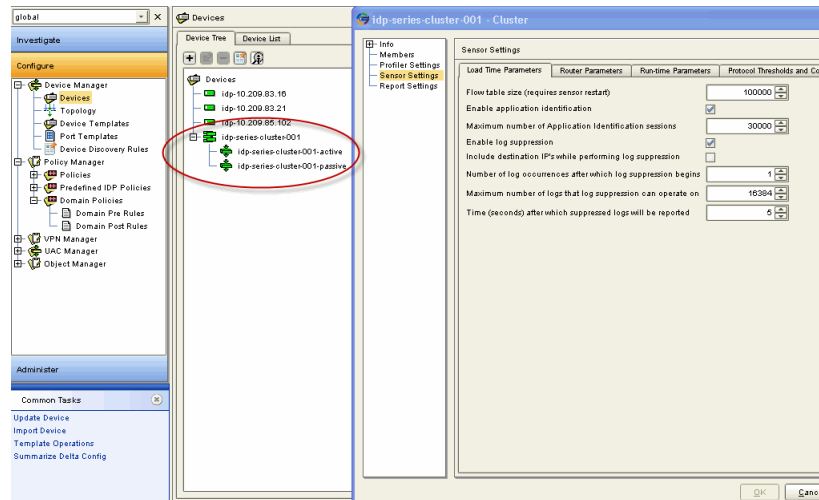
Table 10: IDP Series Configuration Guidelines (*continued*)

Component	Guideline
State sync	<p>Use ACM to enable Third-Party HA and assign each device an identifier.</p> <p>Figure 13: ACM Third-Party HA Pages</p> <p>The figure consists of three screenshots of the IDP configuration interface, labeled 1, 2, and 3.</p> <p>Step 1: The 'Configuration Status' section shows that configuration has been saved and applied, and a reboot is not needed. The 'Main Options' section lists several actions, including 'Reconfigure this IDP via the ACM wizard'. The 'ACM menu' section lists various configuration options, with 'Reconfigure HA (inline modes only)' highlighted in yellow.</p> <p>Step 2: The 'High Availability' tab is selected. The 'Co' section explains that the user specifies whether the IDP Sensor will support party HA. The 'Enable Third-Party HA' radio button is selected and highlighted in yellow. A 'Next Step' button is visible.</p> <p>Step 3: The 'High Availability' tab is selected. The 'Config' section explains that the user assigns the IDP sensor a unique cluster identifier. The 'Choose a unique identifier for this Sensor' dropdown menu is highlighted in yellow, showing '0' as the selected value. A 'Next Step' button is visible.</p>

Table 10: IDP Series Configuration Guidelines (*continued*)

Component	Guideline
Cluster	In NSM, create a cluster object and then add the IDP Series devices to NSM as cluster members. Whenever you push updates (such as OS version updates, detector engine updates, or security policy updates), select the cluster object as the target. NSM pushes updates to members in sequence: member A and then member B.

Figure 14: NSM Device Cluster



NOTE: For third-party high availability deployments, the cluster status displayed in the NSM Realtime Monitor > IDP Cluster Monitor always indicates failure. Disregard this status. You cannot use the NSM Cluster Monitor to display status.

Table 10: IDP Series Configuration Guidelines (*continued*)

Component	Guideline
Interface signaling	<p>If you use the NSRP Layer 3 Track IP method, do not enable interface signaling.</p> <p>If you use NSRP Layer 2 path monitoring, enable interface signaling on the IDP Series devices. In the user_funcs file, change the value of the ha_interface_signal setting to 1, as highlighted in the following example:</p> <pre>##### # VARIABLES ##### [...] #Enable or disable interface based third-party HA signaling #Enable or disable interface based third-party HA signaling #Setting this variable to 1,indicated that interface based #HA signaling should be used, and setting it to 1 indicates #to block STP and similar kind of traffic to enable traffic #switch-over by third-party HA devices. export ha_interface_signal=1 # 'max_intf_rcv_failed_cnt_nicbypass' - The maximum count value for any # data interface indicating the number of times the packet could not # be received by that interface. If the count for any interface reaches # this value nicBypass gets triggered. # **WARNING**: Changing the value would require running 'idp.sh restart'. export max_intf_rcv_failed_cnt_nicbypass=18 # Define SCIO SCIO=/usr/idp/device/bin/scio</pre>
Layer 2 Bypass	Use ACM to enable Layer 2 bypass.
Peer port modulation	Do not enable.

- On the IDP Series device, you can use the synchronization details in **sctop** flow tables and the device log files to verify and troubleshoot the HA deployment. Logs related to HA communication are written locally to /var/idp/device/sysinfo/logs/hasignal.log.

Related Documentation

The following related topics are included in *IDP Series Deployment Scenarios*:

- IDP Series HA Signaling Script Log Messages on page 25
- Third-Party High Availability Support and Limitations on page 21
- Workflow: Upgrading an IDP OS 4.1r4 Cluster to IDP OS 5.1 on page 44

The following additional related topics are included in the *IDP Series Administration Guide*:

- Adding IDP Series Devices to NSM Device Manager
- Understanding sctop Flow Table Reports

- Connecting to ACM
- Configuring Virtual Routers (ACM Procedure)

Example: IDP Series HA Design with Juniper Networks EX Series Switches

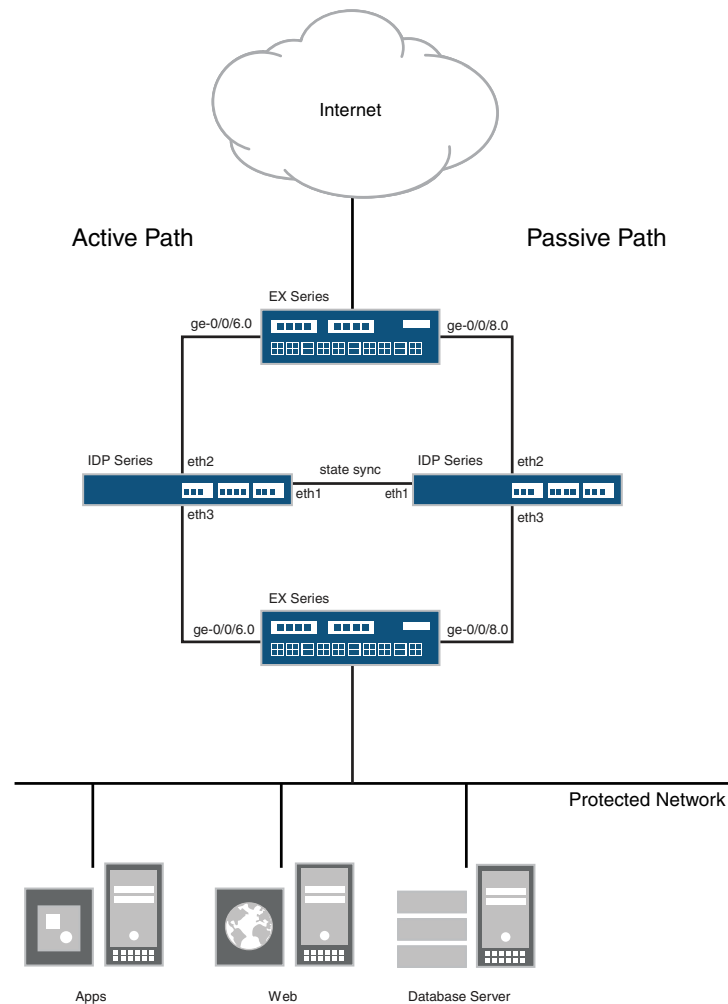
The following sections describe an example redundant path deployment where the Juniper Networks EX Series switch deployment uses Spanning Tree Protocol (STP) to select the active path:

- Topology on page 32
- Deployment Steps on page 34

Topology

Figure 15 on page 33 shows a network topology where there are redundant paths to the Internet. One path is active and the other is passive.

Figure 15: Redundant Path Design: IDP Series HA Depends on STP (Juniper Networks EX Series)



STP uses bridge protocol data unit (BPDU) packets to exchange information with other switches. BPDUs send hello packets out at regular intervals to exchange information across bridges and detect loops in a network topology. STP uses the information provided by the BPDUs to elect a root bridge, identify root ports for each switch, identify designated ports for each physical LAN segment, and prune specific redundant links to create a loop-free tree topology. All leaf devices calculate the best path to the root device and place their ports in blocking or forwarding states based on the best path to the root. The resulting tree topology provides a single active Layer 2 data path between any two end stations.

The IDP Series device does not participate in STP. Rather, when Layer 2 bypass is enabled, the IDP Series devices pass through the BPDU packets so the switches can communicate with each other. If Layer 2 bypass is not enabled, the IDP Series device drops the BPDU packets and the route cannot be chosen. The same is true when the IDP Series device is

gracefully shutdown or encounters failure. The IDP Series device cannot forward the BPDU packets, so STP forwards traffic through the backup path.

Deployment Steps

To deploy this solution, follow these basic steps:

1. Set up and configure the EX Series devices using the documentation that came with your switch. Note the following requirements:
 - Hardware—Connect the EX switch ports to IDP Series traffic interface pairs so that the IDP Series deployment is transparent to the original network path. If your original path connected ge-0/0/6 on one switch with ge-0/0/6 on the other, you undo that cabling and place the IDP Series device in between. You connect the switch on one side to IDP Series eth2 and the switch on the other side to IDP Series eth3.
 - Failure detection mechanism—Implement STP. For information on Junos OS spanning tree protocol, see the [EX Series documentation](#). The following command sample shows the commands use to configure an EX Series switch shown in the example network:

```
root# show | display set

set version 10.2R1.8
set system root-authentication encrypted-password
"$1$KeXQ4XiR$kqfcT.Fxc6GPw1ts7KVBm."
set system syslog user * any emergency
set system syslog file messages any notice
set system syslog file messages authorization info
set system syslog file interactive-commands interactive-commands any
set interfaces ge-0/0/6 unit 0 family ethernet-switching port-mode access
set interfaces ge-0/0/6 unit 0 family ethernet-switching vlan members
vlan200
set interfaces ge-0/0/7 unit 0 family ethernet-switching port-mode access
set interfaces ge-0/0/7 unit 0 family ethernet-switching vlan members
vlan200
set interfaces ge-0/0/8 unit 0 family ethernet-switching port-mode access
set interfaces ge-0/0/8 unit 0 family ethernet-switching vlan members
vlan200
set protocols igmp-snooping vlan all
set protocols stp bridge-priority 40k
set protocols stp max-age 20
set protocols stp hello-time 3
set protocols stp forward-delay 15
set protocols stp interface ge-0/0/6.0 cost 200000
set protocols lldp interface all
set protocols lldp-med interface all
set ethernet-switching-options storm-control interface all
set vlans vlan200 vlan-id 60
set vlans vlan200 interface ge-0/0/6.0
set vlans vlan200 interface ge-0/0/7.0
set vlans vlan200 interface ge-0/0/8.0
set poe interface all

{master:0}[edit]
root#
```

- Set up and configure the IDP Series devices. Consider the following configuration notes.

Table 11: IDP Series Configuration Guidelines

Component	Guideline
IDP Series device hardware	Use a cross-over cable to connect one device HA port to the other HA port.

State sync Use ACM to enable Third-Party HA and assign each device an identifier.

Figure 16: ACM Third-Party HA Pages

The figure displays three sequential screenshots of the IDP configuration web interface, specifically the 'High Availability' section.

Step 1: ACM menu
The first screenshot shows the 'ACM menu' with a list of options. The option 'Reconfigure HA (inline modes only)' is highlighted in yellow.

Step 2: Cofiguration Status
The second screenshot shows the 'Cofiguration Status' page. It includes a 'Main Options' section with links like 'Reconfigure this IDP via the ACM wizard' and 'View/Apply Current Configuration'. Below this, the 'Reconfigure HA (inline modes only)' option is highlighted in yellow.

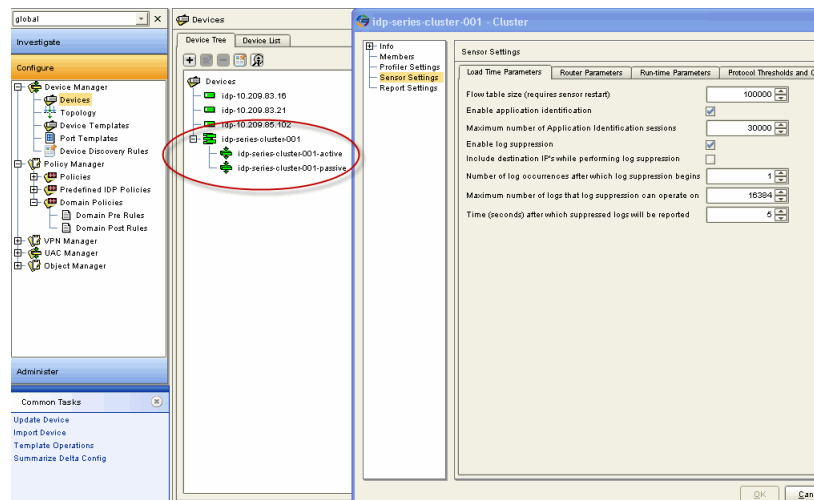
Step 3: Enable Third-Party HA
The third screenshot shows the 'Enable Third-Party HA' configuration page. It instructs the user to specify whether the IDP Sensor will support HA. The 'Enable Third-Party HA' radio button is selected and highlighted in yellow.

Step 4: Choose a unique identifier for this Sensor
The fourth screenshot shows the 'Choose a unique identifier for this Sensor' page. It instructs the user to assign a unique cluster identifier. The dropdown menu is set to '0' and is highlighted in yellow.

Table 11: IDP Series Configuration Guidelines (*continued*)

Component	Guideline
Cluster	In NSM, create a cluster object and then add the IDP Series devices to NSM as cluster members. Whenever you push updates (such as OS version updates, detector engine updates, or security policy updates), select the cluster object as the target. NSM pushes updates to members in sequence: member A and then member B.

Figure 17: NSM Device Cluster



NOTE: For third-party high availability deployments, the cluster status displayed in the NSM Realtime Monitor > IDP Cluster Monitor always indicates failure. Disregard this status. You cannot use the NSM Cluster Monitor to display status.

Layer 2 bypass	Use ACM to enable Layer 2 bypass.
Interface signaling	Do not enable. When interface signaling is disabled, the HA feature monitors the state of IDP engines. If an IDP engine fails, any remaining IDP engines are signaled to disregard the Layer 2 bypass setting and drop Layer 2 traffic, including BPDUs.
Peer port modulation	Do not enable.

- On the IDP Series device, you can use the synchronization details in **sctop** flow tables and the device log files to verify and troubleshoot the HA deployment. Logs related to HA communication are written locally to `/var/idp/device/sysinfo/logs/hasignal.log`.

Related Documentation

The following related topics are included in *IDP Series Deployment Scenarios*:

- IDP Series HA Signaling Script Log Messages on page 25
- Third-Party High Availability Support and Limitations on page 21
- Workflow: Upgrading an IDP OS 4.1r4 Cluster to IDP OS 5.1 on page 44

The following additional related topics are included in the *IDP Series Administration Guide*:

- Adding IDP Series Devices to NSM Device Manager

- Understanding sctop Flow Table Reports
- Connecting to ACM
- Configuring Virtual Routers (ACM Procedure)

Example: IDP Series HA Design with Cisco Catalyst Switches

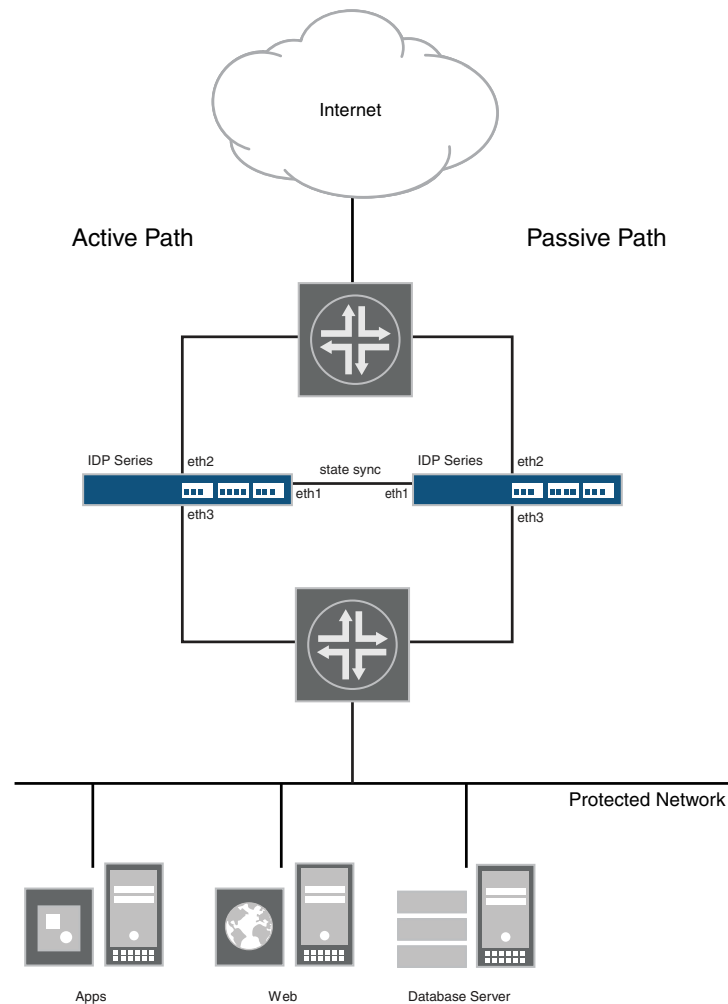
The following sections describe an example redundant path deployment where the Cisco Catalyst switch deployment uses Spanning Tree Protocol (STP) to select the active path:

- Topology on page 37
- Deployment Steps on page 39

Topology

Figure 18 on page 38 shows a network topology where there are redundant paths to the Internet. One path is active and the other is passive.

Figure 18: Redundant Path Design: IDP Series HA Depends on STP (Cisco Catalyst Switch)



The IDP Series device does not participate in STP. Rather, when Layer 2 bypass is enabled, the IDP Series devices pass through the BPDU packets so the switches can communicate with each other. If Layer 2 bypass is not enabled, the IDP Series device drops the BPDU packets and the route cannot be chosen. The same is true when the IDP Series device is gracefully shutdown or encounters failure. The IDP Series device cannot forward the BPDU packets, so STP forwards traffic through the backup path.

Deployment Steps

To deploy this solution, follow these basic steps:

1. Set up and configure the Catalyst switch using the documentation that came with your switch. Note the following requirements.
 - Hardware—Connect the switch ports to IDP Series traffic interface pairs so that the IDP Series deployment is transparent to the original network path. You connect the switch on one side to IDP Series eth2 and the switch on the other side to IDP Series eth3.
 - Failure detection mechanism—Implement spanning tree protocol (STP). For information on Cisco spanning tree protocol, see the [Cisco Catalyst documentation](#). The following command sample shows the configuration of a switch in this example:

```
Switch# show configuration

Using 3285 out of 32768 bytes
!
version 12.0
no service pad
service timestamps debug uptime
service timestamps log uptime
service password-encryption
!
hostname Switch
!
enable secret 5 $1$dupS$SVj8h0WfUzqDeJe.887TQ0
enable password 7 06080A355F4D1B1C001952
!
ip subnet-zero
no ip domain-lookup
!
!
!
interface FastEthernet0/1
  switchport access vlan 17
  no cdp enable
!
interface FastEthernet0/2
  switchport access vlan 51
  no cdp enable
!
interface FastEthernet0/3
  switchport access vlan 19
  no cdp enable
!
interface FastEthernet0/4
  switchport access vlan 21
  no cdp enable
!
interface FastEthernet0/5
  switchport access vlan 15
  no cdp enable
!
interface FastEthernet0/6
  switchport access vlan 15
  no cdp enable
```

```
!  
interface FastEthernet0/7  
  switchport access vlan 17  
  no cdp enable  
!  
interface FastEthernet0/8  
  switchport access vlan 17  
  no cdp enable  
!  
interface FastEthernet0/9  
  switchport access vlan 19  
  no cdp enable  
!  
interface FastEthernet0/10  
  switchport access vlan 19  
  no cdp enable  
!  
interface FastEthernet0/11  
  switchport access vlan 21  
  no cdp enable  
!  
interface FastEthernet0/12  
  switchport access vlan 21  
  no cdp enable  
!  
interface FastEthernet0/13  
  switchport access vlan 31  
  no cdp enable  
!  
interface FastEthernet0/14  
  switchport access vlan 33  
  no cdp enable  
!  
interface FastEthernet0/15  
  switchport access vlan 27  
  no cdp enable  
!  
interface FastEthernet0/16  
  switchport access vlan 29  
  no cdp enable  
!  
interface FastEthernet0/17  
  switchport access vlan 27  
  no cdp enable  
!  
interface FastEthernet0/18  
  switchport access vlan 27  
  no cdp enable  
!  
interface FastEthernet0/19  
  switchport access vlan 29  
  no cdp enable  
!  
interface FastEthernet0/20  
  switchport access vlan 29  
  no cdp enable  
!  
interface FastEthernet0/21  
  switchport access vlan 31  
  no cdp enable  
!
```

```

interface FastEthernet0/22
  switchport access vlan 31
  no cdp enable
!
interface FastEthernet0/23
  switchport access vlan 33
  no cdp enable
!
interface FastEthernet0/24
  switchport access vlan 33
  no cdp enable
!
interface GigabitEthernet0/1
  switchport access vlan 51
  no cdp enable
!
interface GigabitEthernet0/2
  switchport access vlan 51
  no cdp enable
!
interface VLAN1
  no ip directed-broadcast
  no ip route-cache
  shutdown
!
interface VLAN7
  ip address 10.209.95.14 255.255.240.0
  no ip directed-broadcast
  no ip route-cache
!
interface VLAN9
  no ip directed-broadcast
  no ip route-cache
  shutdown
!
ip default-gateway 10.209.95.254
mac-address-table aging-time 10
no cdp run
!
line con 0
  exec-timeout 0 0
  transport input none
  stopbits 1
line vty 0 4
  exec-timeout 0 0
  password 7 1419171F1F07382E2126
  login
line vty 5 15
  exec-timeout 0 0
  password 7 1419171F1F07382E2126
  login
!
end

```

2. Set up and configure the IDP Series devices. Consider the following configuration notes.

Table 12: IDP Series Configuration Guidelines

Component	Guideline
IDP Series device hardware	Use a cross-over cable to connect one device HA port to the other HA port.
State sync	Use ACM to enable Third-Party HA and assign each device an identifier.

Figure 19: ACM Third-Party HA Pages

Configuration Status

- Configuration has been saved and applied.
- The IDP does not need a reboot at this time.

Main Options

- Reconfigure this IDP via the ACM wizard
- View/Apply Current Configuration
- File Download Manager
- Upload and replace ACM configuration file

ACM menu

- Reset root/admin Passwords
- Change Host/Domain name
- **Reconfigure HA (inline modes only)**
- Reconfigure Radius
- Reconfigure Network Interface Hardware
- Reconfigure Virtual Routers
- Reconfigure IP Networking

Co

In this step, you specify whether the IDP Sensor will support third-party HA. Sniffer mode sensors do not support HA.

☐ Disable HA

☒ **Enable Third-Party HA**

Next Step

Config

In this step, you assign the IDP sensor a unique cluster identifier. We recommend you follow a convention where the device identifier is followed by the sensor identifier.

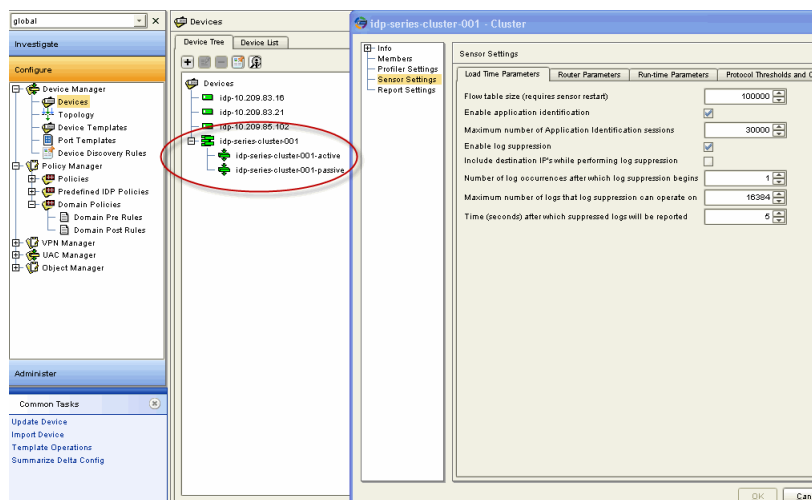
3 Choose a unique identifier for this Sensor: 0

Next Step

Table 12: IDP Series Configuration Guidelines (*continued*)

Component	Guideline
Cluster	In NSM, create a cluster object and then add the IDP Series devices to NSM as cluster members. Whenever you push updates (such as OS version updates, detector engine updates, or security policy updates), select the cluster object as the target. NSM pushes updates to members in sequence: member A and then member B.

Figure 20: NSM Device Cluster



NOTE: For third-party high availability deployments, the cluster status displayed in the NSM Realtime Monitor > IDP Cluster Monitor always indicates failure. Disregard this status. You cannot use the NSM Cluster Monitor to display status.

Layer 2 bypass	Use ACM to enable Layer 2 bypass.
Interface signaling	Do not enable. When interface signaling is disabled, the HA feature monitors the state of IDP engines. If an IDP engine fails, any remaining IDP engines are signaled to disregard the Layer 2 bypass setting and drop Layer 2 traffic, including BPDUs.
Peer port modulation	Do not enable.

- On the IDP Series device, you can use the synchronization details in **sctop** flow tables and the device log files to verify and troubleshoot the HA deployment. Logs related to HA communication are written locally to `/var/idp/device/sysinfo/logs/hasignal.log`.

Related Documentation

The following related topics are included in *IDP Series Deployment Scenarios*:

- IDP Series HA Signaling Script Log Messages on page 25
- Third-Party High Availability Support and Limitations on page 21
- Workflow: Upgrading an IDP OS 4.1r4 Cluster to IDP OS 5.1 on page 44

The following additional related topics are included in the *IDP Series Administration Guide*:

- Adding IDP Series Devices to NSM Device Manager

- Understanding sctop Flow Table Reports
- Connecting to ACM
- Configuring Virtual Routers (ACM Procedure)

Workflow: Upgrading an IDP OS 4.1r4 Cluster to IDP OS 5.1

The upgrade from IDP OS 4.1r4 to IDP OS 5.1 is a major task. It is not a matter of simply pushing the new OS to the cluster members. You must perform the following steps in the order shown.

When you upgrade from IDP OS 4.1r4 to IDP OS 5.1, you are reimaging the disk with a new operating system. All partitions except `/var/idp` are rewritten.

The upgrade process restores your license and most of your previous settings. The following settings are not preserved:

- The upgrade does not retain your deployment mode or virtual router configuration. In IDP OS 5.1, you use the ACM virtual routers page to configure a deployment mode per interface.
- The upgrade does not retain settings that are no longer supported in IDP OS 5.1.
- The upgrade process saves a backup of your previous `/usr/idp/device/bin/user_funcs` file, but installs a new `user_funcs` file in order to provide appropriate content for IDP OS 5.1.

The upgrade process preserves packet log files in `/usr/idp/device/var/pktlogs/0/`. Packet log files in other directories will be lost upon upgrade. If you have been using the option to maintain packet data locally and send to NSM on demand, copy logs from `/usr/idp/device/var/pktlogs/1/` and higher numbered log directories to a remote location before you upgrade. This action is not required if you have been using the option to always include packet data when NSM sends the event log.

We have verified upgrade from an IDP OS 4.1r4 cluster where the IDP Series devices are deployed in transparent mode or sniffer mode. If the devices are deployed in bridge, proxy-arp, or router mode, you must redeploy them in IDP OS 4.1r4 transparent mode or sniffer mode before you can upgrade to IDP OS 5.1. Note, however, that HA is not applicable to sniffer mode deployments. Your target is a transparent mode deployment, so migration to IDP OS 5.1 might involve network topology replanning. In transparent mode, an HA cluster is an active-passive, failover pair. You deploy the IDP Series devices in redundant paths and rely on third-party link detection mechanisms to choose the active path.

To upgrade an active-passive, failover pair:

1. Disconnect the HA interface cable.
2. Upgrade the device deployed in the inactive path first.
 - a. Log into the CLI and run the **idp.sh stop** command to stop the IDP engine.
 - b. Upgrade the OS using either NSM or the CLI:
 - In NSM, push the software to the device, not the cluster. If you push to the cluster, you will disrupt traffic in the primary path.
 - From the CLI, execute the `reimage shar` file.

During the upgrade, the console might display messages similar to the following:

```
Critical: sc_flow.c:4020 sc_flow_ha_handle_msg: received
SC_HA_MSG_TYPE_SYNC_FLOW_TABLE from major = 5 minor = 1 buid = 137260, my
major = 4 my minor = 1 my build = 134028
```

You can disregard these messages.

- c. Use ACM and the CLI to configure new and changed features:
 - On the ACM Configure High Availability page, enable Third-Party HA.
 - On the ACM Configure HA State-Sync page, assign the backup device ID 1.
 - On the ACM virtual routers page:
 - Assign interface pairs to virtual routers. Because HA was enabled on your IDP OS 4.1r4 configuration, the upgrade process creates a virtual router named `vr0` that contains `eth1` (the HA interface). One of the system requirements for HA is that a virtual router named `vr0` contain `eth1`.
 - Specify transparent mode.
 - Specify **Nics Off** in case of failure or graceful shutdown.
 - Enable Layer 2 bypass.
 - (Optional) Enable PPM.
 - Log into the CLI and edit the `user_funcs` file:
 - Use the backup copy generated by the OS upgrade to add your custom settings back into the operative file: `/usr/idp/device/bin/user_funcs`.
 - (Optional) If you want to enable interface signaling, edit the `user_funcs` file and change the value of the `ha_interface_signal` setting to 1, as highlighted in the following example:

```
#####
#          VARIABLES
#####
```

```
[...]
#Enable or disable interface based third-party HA signaling

#Enable or disable interface based third-party HA signaling
#Setting this variable to 1,indicated that interface based
#HA signaling should be used, and setting it to 1 indicates
#to block STP and similar kind of traffic to enable traffic
#switch-over by third-party HA devices.

export ha_interface_signal=1

# 'max_intf_rcv_failed_cnt_nicbypass' - The maximum count value for any
# data interface indicating the number of times the packet could not
# be received by that interface. If the count for any interface reaches
# this value nicBypass gets triggered.
# **WARNING**: Changing the value would require running 'idp.sh restart'.

export max_intf_rcv_failed_cnt_nicbypass=18

# Define SCIO
SCIO=/usr/idp/device/bin/scio
```

d. Verify the device functions as expected:

- Display interface statistics to verify traffic flow.
- Run **scio getsystem** and verify that HA is enabled:

```
[root@defaulthost ~]# scio getsystem
```

```
Product Name:  NS-IDP-200
Serial Number: 0146082005000328
Software Version: 5.1.137260
IDP Mode: transparent
HA Mode: Enabled
Detector Version: 5.1.110101209
Software License: Permanent
Software Expiration Date: never
```

- Run **idp.sh status** and verify the status of the hasignal.sh process.
- Run **sctop** to see if the eth1 interface is displayed as the sync interface.
- Run **scio vr list** to verify that eth1 is listed in vr0.

```
[root@defaulthost ~]# scio vr list
```

```
Attached Virtual Routers:
V-Router  V-Circuit  NIC
-----  -
vr0      eth1      eth1
         eth3      eth3
         eth2      eth2
```

- Check for the logs in `/var/idp/device/sysinfo/logs/hasignal.timestamp`:


```
20101210030431:[WARN]:The UP & RUNNING nics are eth2 eth3 eth6 eth7
20101210030431:[WARN]:The considered nics are eth2 eth3 eth4 eth5 eth6
eth7 eth8 eth9 eth10 eth11
```

Every time the IDP engine is restarted, IDP device rebooted, ACM configuration changed, or HA interface signaling script restarted, the HA signaling script generates a pair of logs listing traffic interfaces.

In the example above, the first line (UP & RUNNING nics) indicates the traffic interfaces monitored by the interface signaling script. The second line (considered nics) indicates all the traffic interfaces that have been enabled through the ACM Configure Virtual Routers page. If the first line does not include all the interfaces you expect to be monitored, run the **hasignal.sh restart** command and check the new logs.

3. Upgrade the OS for the primary device.

- a. Log into the CLI and run the **idp.sh stop** command to stop the IDP engine. Stopping the IDP engine signals unavailability to firewalls or routers monitoring the links and cause traffic to cutover to the redundant path.
- b. Upgrade the OS using either NSM or the CLI:
 - In NSM, push the software to the device.
 - From the CLI, execute the installation shar file.
- c. Use ACM and the CLI to configure new and changed features:
 - On the ACM Configure High Availability page, enable Third-Party HA.
 - On the ACM Configure HA State-Sync page, assign the primary device ID 0.
 - On the ACM virtual routers page:
 - Assign interface pairs to virtual routers. Because HA was enabled on your IDP OS 4.1r4 configuration, the upgrade process creates a virtual router named vr0 that contains eth1 (the HA interface). One of the system requirements for HA is that a virtual router named vr0 contain eth1.
 - Specify transparent mode.
 - Specify **Nics Off** in case of failure or graceful shutdown.
 - Enable Layer 2 bypass.
 - (Optional) Enable PPM.
 - Log into the CLI and edit the user_funcs file:
 - Use the backup copy generated by the OS upgrade to add your custom settings back into the operative file: /usr/idp/device/bin/user_funcs.
 - (Optional) In the user_funcs file, change the value of the ha_interface_signal setting to 1 if you want to enable interface signaling.

- d. Verify the device functions as expected.
4. Reconnect the HA interface cable.
5. Use the **sctop** utility flow tables to verify state sync; and examine device logs to verify HA operations. Logs related to HA communication are written locally to `/var/idp/device/sysinfo/logs/hasignal.timestamp`.
6. (If necessary), use NSM to push the latest detector engine to the cluster.
7. Use NSM to push the same security policy to the cluster.

Related Documentation

The following related topics are included in *IDP Series Deployment Scenarios*:

- IDP Series HA Signaling Script Log Messages on page 25
- Third-Party High Availability Support and Limitations on page 21

The following additional related topics are included in the *IDP Series Administration Guide*:

- Updating IDP OS Software (NSM Procedure)
- Connecting to ACM
- Configuring Virtual Routers (ACM Procedure)
- Understanding sctop Flow Table Reports

CHAPTER 4

Coordinated Threat Control

The following topic provides an overview of coordinated threat control deployments:

- Deploying IDP Series with Juniper Networks Access Control Devices for Coordinated Threat Control on page 49

Deploying IDP Series with Juniper Networks Access Control Devices for Coordinated Threat Control

The Juniper Networks coordinated threat control solution is an secure access solution deployment that leverages event logs collected by IDP Series devices. The following sections provide an overview of the solution:

- Purpose on page 49
- Topology on page 49
- Configuration Overview on page 52
- Integration Notes on page 53

Purpose

When the IDP Series appliance detects a security event (be it a threat or any traffic that breaks an administrator configured policy), it can, in addition to blocking that threat, send the event log to a Juniper Networks SA Series or IC Series device in real time.

The SA Series or IC Series device can then use the log data to identify the user session that is the source of the undesired traffic. It can take appropriate actions on the endpoint, such as notifying the administrator, terminating the user session, disabling the user account, or mapping the user to a quarantine role.

Administrators can configure the quarantine role to provide users with a lower level of access and inform them why they have been quarantined and what they should do next. During remediation, administrators can enforce additional endpoint security checks or push additional endpoint protection software.

Topology

In a coordinated threat control deployment, Juniper Networks devices communicate using Transport Layer Security (TLS).

Figure 21 on page 50 shows a *split deployment*, where the SA Series appliance has been deployed for extended enterprise access and the IDP Series appliance for security for all perimeter traffic including, but not limited to, the traffic coming from the SA Series appliance.

Figure 21: Coordinated Threat Control Deployment Diagram: SA Series Split Deployment

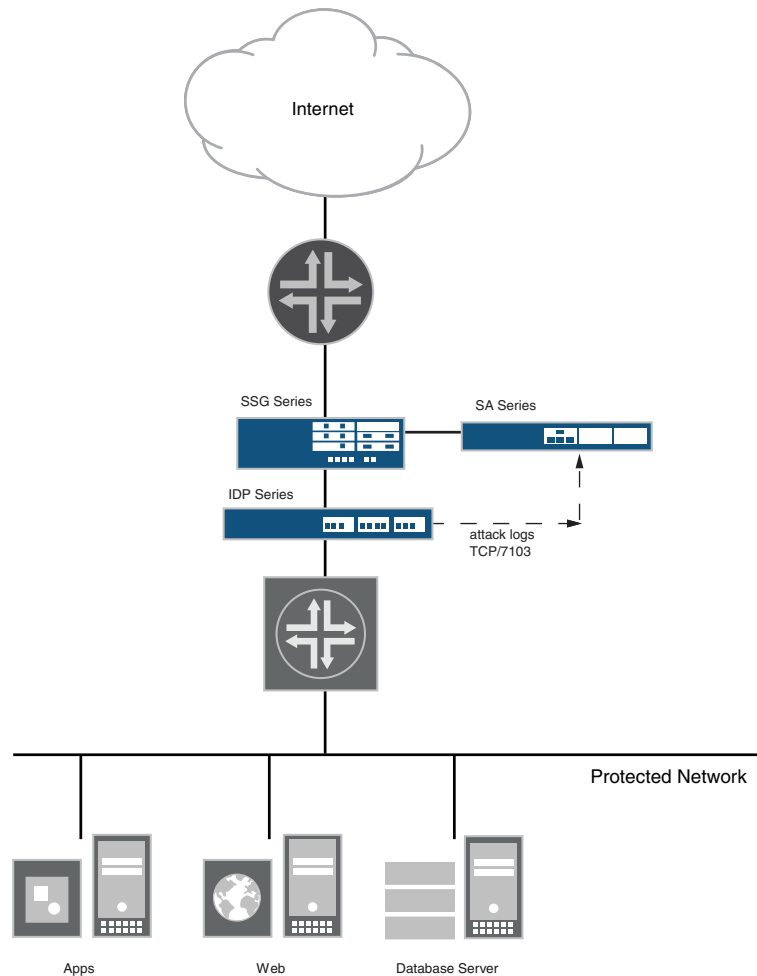


Figure 22 on page 51 shows an *internal deployment*, where only encrypted SSL traffic terminated at the SA Series appliance has access to the protected network and the IDP Series appliance is deployed to inspect only traffic coming through the SA Series appliance.

Figure 22: Coordinated Threat Control Deployment Diagram: SA Series Internal Deployment

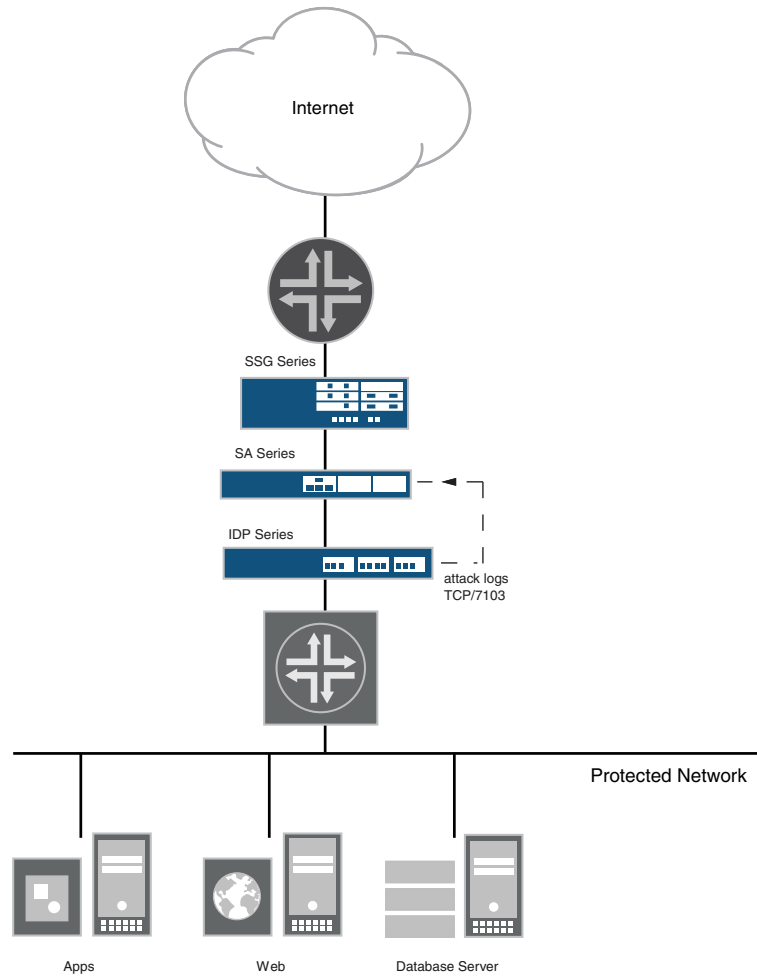
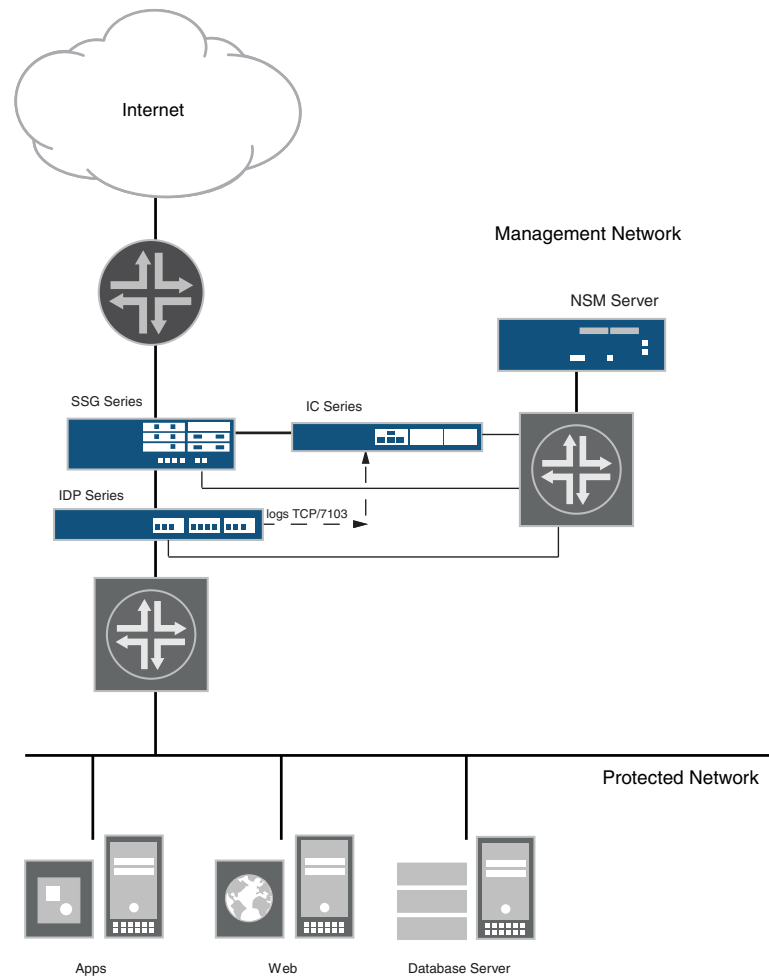


Figure 23 on page 52 shows deployment with an IC Series UAC device.

Figure 23: Coordinated Threat Control Deployment Diagram: IC Series Deployment



Configuration Overview

From the IDP Series side, you use the Appliance Configuration Manager (ACM) to generate a one-time password the SA Series or IC Series device will use to connect to the IDP Series device. Figure 24 on page 53 shows the ACM page used to generate a password.

Figure 24: ACM: Generating a One-Time Password for the Connection from an SA Series or IC Series Appliance

The screenshot shows the 'Configure NetScreen-Security Manager Communication' page in the IDP configuration interface. The page has a navigation bar with 'Setup', 'Networking', 'System', and 'Management' tabs. The 'Management' tab is active. The page title is 'Configure NetScreen-Security Manager Communication'. Below the title, there is a paragraph explaining that this step is for configuring the sensor to use a NetScreen-Security Manager. It mentions that configuration fields are optional and that a one-time password can be reset. A form follows with fields for 'Reset One Time Password' (checkbox), 'New One Time Password' (text box), 'Device ID' (text box with a long alphanumeric string), 'Primary NetScreen-Security Manager IP' (text box with '10.150.99.52'), 'Secondary NetScreen-Security Manager IP' (text box), 'Port No' (text box with '7803'), and 'Port No' (text box with '7803'). Below this, there is a section titled 'Configure IDP IVE Server Communication' with a paragraph explaining that the IVE one-time password (IVE OTP) can be reset. It includes a 'Reset IVE OTP?' checkbox and a 'Next Step' button.

From the SA Series or IC Series side, you configure the connection to the IDP Series device, specifying the IP address, port 7103, and the one-time password. Figure 25 on page 53 shows the IC Series Admin Console Sensor Configuration page. The SA Series Admin Console Sensor Configuration page is similar.

Figure 25: IC Series Admin Console: Configuring the Connection to the IDP Series Appliance

The screenshot shows the 'Infranet Controller' Admin Console. The left sidebar contains a tree view with categories: System, Configuration, Authentication, Administrators, Users, UAC, and Maintenance. The 'Configuration' category is expanded, showing sub-items: Licensing, Security, Certificates, DMI Agent, Sensors, Sensor Event Policies, and Sensors. The 'Sensors' sub-item is selected, and the 'Sensor Event Policies' sub-item is also selected. The main content area shows the 'Sensor Event Policies' configuration page. It has a navigation bar with 'Security', 'Certificates', 'DMI Agent', and 'Sensors' tabs. The 'Sensors' tab is active. Below the tabs, there is a table with columns: Sensor, Address, Enabled, Status, and Notes. The table is currently empty. Above the table, there are buttons for 'Enable', 'Disable', 'Reconnect', and 'Refresh'.

Integration Notes

To avoid issues with integration:

- Log suppression for the IDP Series appliance must be disabled. The coordinated threat control solution depends on notification of each event to the SA Series or IC Series appliance. If log suppression is enabled, the IDP Series appliance might report only one occurrence for numerous virtual connections coming through the SA Series or IC Series appliance.

- Relevant security policy rules must have logging enabled (configure notification options).
- IP actions (such as IP Block and IP Close) are not advised in policies that examine traffic from an SA Series or IC Series appliance. Closing or blocking a connection based on IP address might shut down numerous VPN sessions.

**Related
Documentation**

The following related topics are included in the *IDP Series Administration Guide*:

- Connecting to ACM
- Configuring Log Suppression (NSM Procedure)
- Specifying Rule Notification Options (NSM Procedure)
- Specifying IP Action (NSM Procedure)

CHAPTER 5

User-Role-Based Security Policies

The following topics provide an overview of deployment requirements to support user-role-based security policies:

- Deploying IDP Series with an IC Series Device to Implement User-Role-Based Security Policies on page 55

Deploying IDP Series with an IC Series Device to Implement User-Role-Based Security Policies

The IDP Series user role-based policy feature depends on integration with the Juniper Networks IC Series Unified Access Control (UAC) appliance. The following sections provide an overview of the deployment requirements:

- Purpose on page 55
- Topology on page 56
- Understanding Communication Between IC Series and IDP Series Devices on page 57
- Configuration Overview on page 58

Purpose

The user role-based policy feature enables you to specify user roles as match criteria in IDP rulebase and application policy enforcement (APE) rulebase rules. Matching based on user role rather than IP address both simplifies and finely tunes your rules. In many networks, the IP address is dynamically assigned. To protect your network, you would have to cast a wide net for traffic sources. In most cases, you would specify a subnet mask or specify **Any** source (in the latter case, this means you really are not matching on source). For the purpose of intrusion detection and prevention, a wide net is not necessarily a bad thing: you do want to inspect any session that could potentially contain an attack. Use of role-based rules with a terminal match, however, will improve performance by providing faster matching with specific source targets and rulebase termination. In addition, you are likely to find that user role-based logs are easier to analyze because they provide visibility into the user role associated with an attack event or application usage.

UAC integration with IDP Series devices also improves end user experience authenticating to your network. In a UAC deployment, you use the Host Checker feature to quarantine users with vulnerable hosts. Instead of using a firewall to shut down access to network

resources, you can use IDP security policies to enable access and inspect the traffic to guard against threats.

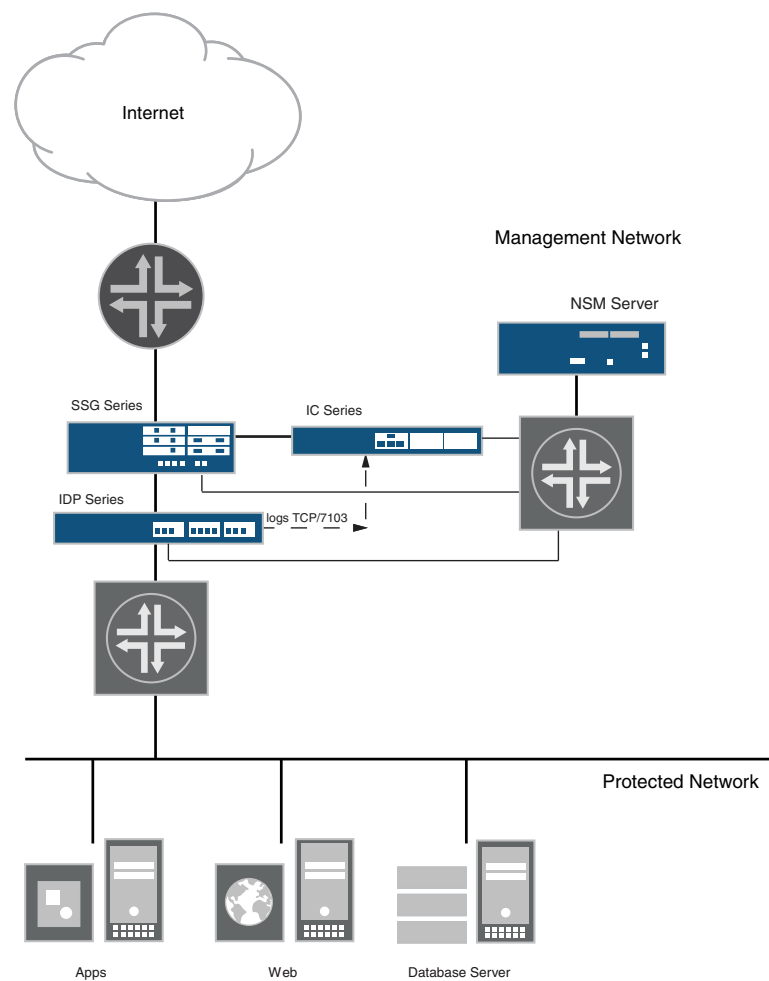
In the APE rulebase, role-based rules are indispensable to supporting the business cases that demand a nuanced approach to application policy enforcement. They enable you to enforce business policies such as “Contractors, Part-Time, and Temporary employees may not use peer-to-peer filesharing applications; full-time employees may use them, but only with a limited pool of bandwidth.”

Topology

In a user-role-based policy deployment, the Juniper Networks devices communicate using Transport Layer Security (TLS).

Figure 26 on page 56 shows an IDP Series deployment with an IC Series UAC device.

Figure 26: Coordinated Threat Control Deployment Diagram: IC Series Deployment

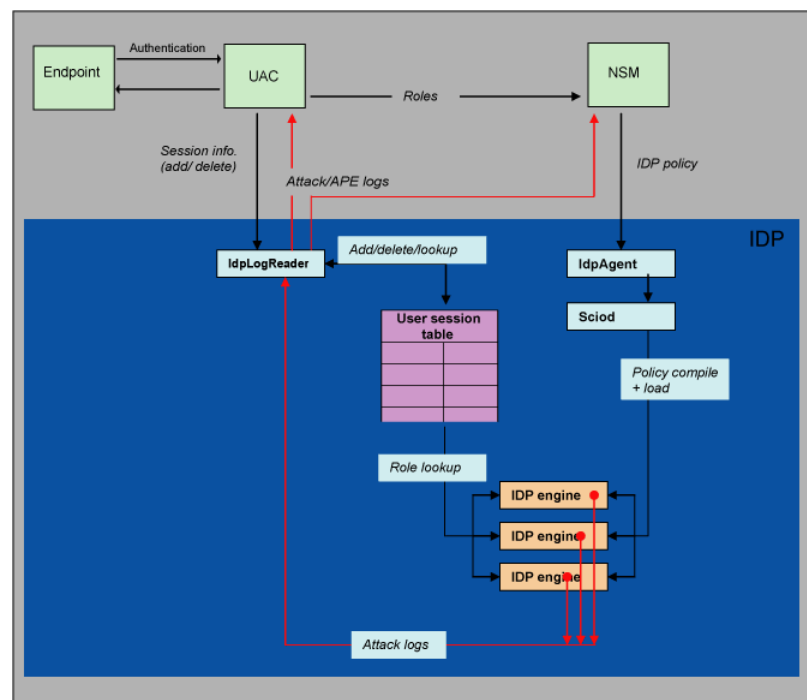


Understanding Communication Between IC Series and IDP Series Devices

When an endpoint client authenticates to the network through the IC Series device, the IC Series device assigns a role to the authenticated user and sends session information to the IDP Series device. Session information includes IP address, username, and the roles to which the user is assigned.

When you configure communication between IC Series and IDP Series devices, the IC Series device sends its session table to the IDP Series device. Figure 27 on page 57 illustrates the communication between IDP Series and IC Series devices.

Figure 27: Communication Among User-Role-Based Policy Deployment Components



If the user IP address changes, user role changes, or the session is deleted, the IC Series device sends updates to the IDP Series session table.

Assuming you also have configured communication between the IC Series device and NSM, the IC Series device sends user role information to the NSM via the IC Series — NSM connection. You use NSM to configure policy rules that match user roles and then push the policy from NSM to the IDP Series device.

When the user traffic traverses the IDP Series device, the IDP system inspects the session to see if there is a match. If the security policy has user-role-based rules, the IDP system looks up the IP address in the session table to see if the IP address is a match for any role. If any role matches, the IDP system uses the role and other matching criteria to attempt to match user-role-based rules. If no user-role-based rule matches, the IDP system attempts to match the IP address-based rules.

If you have enabled logging, the IDP Series device sends logs to both the IC Series device and NSM.

Configuration Overview

From the IDP Series side, you use the Appliance Configuration Manager (ACM) to generate a one-time password the IC Series device will use to connect to the IDP Series device. Figure 28 on page 58 shows the ACM page used to generate a password.

Figure 28: ACM: Generating a One-Time Password for the Connection from an IC Series Device

From the IC Series side, you configure the connection to the IDP Series device, specifying the IP address, port 7103, and the one-time password. Figure 29 on page 58 shows the IC Series Admin Console Sensor Configuration page.

Figure 29: IC Series Admin Console: Configuring the Connection to the IDP Series Appliance

**Related
Documentation**

The following related topics are included in the *IDP Series Concepts and Examples Guide*:

- User-Role-Based Policy Feature Overview
- IDP Rulebase Example: User-Role-Based Policies
- APE Rulebase Example: Aggregate and Per-Subscriber Rate Limits

The following related topics are included in the *IDP Series Administration Guide*:

- Connecting to ACM
- Verifying Integration with an IC Series Unified Access Control Appliance
- Configuring Advanced Settings for the User-Role-Based Policy Feature

