



SRC Software

Sample Applications Guide

Release 3.2.x

Juniper Networks, Inc.

1194 North Mathilda Avenue
Sunnyvale, California 94089
USA

408-745-2000

www.juniper.net

Published: 2009-09-11

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

Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

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

SRC PE Software Sample Applications Guide

Release 3.2.x

Copyright © 2009, Juniper Networks, Inc.

All rights reserved. Printed in USA.

Writing: Linda Creed, Justine Kangas, Betty Lew, Helen Shaw

Editing: Fran Mues

Illustration: Nathaniel Woodward

Cover Design: Edmonds Design

Revision History

30 September 2009—Revision 1

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

YEAR 2000 NOTICE

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

SOFTWARE LICENSE

The terms and conditions for using this software are described in the software license contained in the acknowledgment to your purchase order or, to the extent applicable, to any reseller agreement or end-user purchase agreement executed between you and Juniper Networks. By using this software, you indicate that you understand and agree to be bound by those terms and conditions.

Generally speaking, the software license restricts the manner in which you are permitted to use the software and may contain prohibitions against certain uses. The software license may state conditions under which the license is automatically terminated. You should consult the license for further details.

For complete product documentation, please see the Juniper Networks Web site at www.juniper.net/techpubs.

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)).

Abbreviated Table of Contents

	About the Documentation	xxv
Part 1	Installing Applications	
Chapter 1	Installing the Sample SRC Applications	3
Part 2	Providing Network Security and Threat Mitigation	
Chapter 2	Mirroring Subscriber Traffic in the SRC Network	11
Chapter 3	Providing Endpoint Security with IVE	27
Part 3	Providing Threat Mitigation Services with IDP	
Chapter 4	Overview of IDP Integration	41
Chapter 5	Configuring Services and Subscriptions to Integrate IDP	49
Chapter 6	Sending E-Mail to Subscribers	63
Chapter 7	Monitoring Subsets of Subscriber Traffic	71
Chapter 8	Defining Actions to Be Taken for Subscriber Traffic	81
Chapter 9	Enabling SRC Actions from IDP Manager	91
Part 4	Integrating IP Address Managers	
Chapter 10	Integrating IP Address Managers with the SAE	97
Part 5	Integrating Prepaid Service Applications	
Chapter 11	Providing Prepaid Services	107
Part 6	Managing Access Portals for Residential Subscribers	
Chapter 12	Overview of the Residential Portal	117
Chapter 13	Installing and Configuring the Sample Residential Portal	121
Chapter 14	How Subscribers Use the Sample Residential Portal	133
Chapter 15	Developing a Residential Portal	153
Part 7	Designing Services for Enterprise Manager Portal	
Chapter 16	Reviewing and Configuring Policies and Services for Enterprise Manager Portal	161

Part 8	Managing Access Portals for Enterprise Subscribers	
Chapter 17	Overview of Enterprise Service Portals	189
Chapter 18	Planning Deployment for Enterprise Service Portals	199
Chapter 19	Installing and Configuring Enterprise Service Portals	205
Chapter 20	Managing Services with Enterprise Manager Portal	219
Chapter 21	Managing Enterprise Service Portals	285
Chapter 22	Using NAT Address Management Portal	291
Chapter 23	Using the Sample Enterprise Service Portal	295
Chapter 24	Developing an Enterprise Service Portal	305
Part 9	Index	
	Index	311

Table of Contents

About the Documentation xxv

SRC Documentation and Release Notes	xxv
Audience	xxv
Documentation Conventions	xxv
Obtaining Documentation	xxvii
Documentation Feedback	xxvii
Requesting Technical Support	xxviii
Self-Help Online Tools and Resources	xxviii
Opening a Case with JTAC	xxviii

Part 1

Installing Applications

Chapter 1

Installing the Sample SRC Applications 3

SRC Software for Sample and Demonstration Applications	3
Before You Install the Sample SRC Applications	4
Solaris Packages and Installation Folders for Sample and Demonstration Applications	5
Installing SRC Application Packages	5
Uninstalling SRC Packages	6
Installing Sample SRC Data for Sample and Demonstration Applications	6
Installing SRC Sample Web Applications	6
Installing Web Applications Inside the JBoss Application Server	7
Removing SRC Web Applications	7
Removing a Web Application from JBoss	7
Reviewing Port Settings for Sample SRC Applications	8

Part 2**Providing Network Security and Threat Mitigation**

Chapter 2**Mirroring Subscriber Traffic in the SRC Network 11**

Overview of Traffic Mirroring	11
Traffic-Mirroring Application	11
Configuring Traffic Mirroring	13
Configuring Scopes	13
Configuring Services for Mirroring	14
Configuring Services	16
Subscribing to the Aggregate Service	18
Configuring Subscriber Sessions	18
Subscriber Classification Scripts	18
Interface Classification Scripts	18
Managing Traffic Mirroring	19
Overview of the Traffic Mirroring Administration Portal	19
Accessing the Portal	19
Starting New Mirroring Tasks	20
Managing Mirroring Tasks	21
Configuring the Traffic Mirroring Administration Portal	23
Deploying the Traffic Mirroring Administration Portal	23
Configuring the Traffic-Mirroring Application	24
Configuring NIC Proxy	25
Configuring Logging	25

Chapter 3**Providing Endpoint Security with IVE 27**

Overview of IVE Host Checker Integration	27
Before You Integrate IVE into an SRC Environment	27
Sample Implementation for Integrating IVE Host Checker	29
Configuring Host Checking in an SRC Network	29
Configuring the Host Check Result Portal	30
Overview of the Sample Host Check Result Portal	30
Configuring Properties for the Sample Host Check Result Portal	32
Deploying the Sample Host Check Result Portal	36
Accessing the Portal	36
Configuring the Redirect Server to Redirect Traffic to the Captive Portal	36
Configuring Services for Subscribers	36
Scheduling Subscriber Host Checking	38

Part 3**Providing Threat Mitigation Services with IDP**

Chapter 4**Overview of IDP Integration 41**

Overview of IDP Integration	41
Before You Integrate IDP into an SRC Environment	42

Example: Integrating IDP into an SRC Environment	42
Sample Network Topologies	43
Components in Sample Data	44
Directing Subscriber Traffic to IDP for Monitoring	45
Surveillance Director	45
Router and Interface Subscriber Sessions	46
Subscriber Session to Host an Aggregate Service	46
Subscriber Session to Host a Core Interface Fragment Service	47
Subscriber Session to Host a Router Interface Fragment Service	47
Integrating IDP into an SRC Environment	47

Chapter 5

Configuring Services and Subscriptions to Integrate IDP **49**

Configuring Services and Subscriptions to Send Traffic to an IDP Sensor	49
Configuring Services to Policy-Route Traffic to IDP	50
Configuring Scopes When You Use Policy-Based Routing	50
Defining Services for Policy-Based Routing on JUNOS Routers	50
Configuring a Subscriber Interface Service	52
Configuring a Core Interface Service	52
Configuring an Aggregate Service	53
Configuring Services to Mirror Traffic to IDP	55
Configuring Scopes When Mirroring Traffic	55
Defining Services for Mirroring on JUNOS Routing Platforms	56
Subscribing to an Aggregate Service from a JUNOS Router	59
Classifying Subscribers for IDP Integration	60
Example: Router Subscriber Session to Host an Aggregate Service	60
Example: Interface Subscriber Session to Policy-Route Traffic to IDP	61
Example: Router Subscriber Session to Mirror Traffic to IDP	61
Classifying Interfaces for IDP Integration	61
Example: Interface Classification for Core Interfaces on a JUNOS	
Router	62
Example: Interface Classification for the Forwarding Interface on a JUNOS	
Routing Platform	62

Chapter 6

Sending E-Mail to Subscribers **63**

Overview of IDP E-Mailer	63
How IDP E-Mailer Responds to Incidents Reported by IDP	63
Configuring Deployment Properties for IDP E-Mailer	64
Configuring Application Properties for IDP E-Mailer	65
Configuring General Properties for IDP E-Mailer	65
IDP E-Mailer Fields	66
Configuring a NIC Proxy for IDP E-Mailer	66
Configuring Logging for IDP E-Mailer	67
Configuring E-Mail Properties for IDP E-Mailer	67
E-Mailer Configurations Fields	68
Deploying IDP E-Mailer	70

Chapter 7	Monitoring Subsets of Subscriber Traffic	71
	Overview of Surveillance Director	71
	Configuring Initial Properties for the Surveillance Director	71
	General Properties for Surveillance Director	72
	Java Properties for Surveillance Director	73
	Customizing How to Monitor Subsets of Subscriber Traffic	74
	Configuring Directory Properties for the Surveillance Director	75
	Network Field	76
	Configuring Logging for the Surveillance Director	76
	Configuring an Instance of the Surveillance Director	76
	Surveillance Director Fields	77
Chapter 8	Defining Actions to Be Taken for Subscriber Traffic	81
	Actions to Be Taken for Subscriber Traffic	81
	Redirecting Web Requests to an IDP Captive Portal	81
	Sequence for Redirecting Traffic	83
	About the Record Servlet	83
	Developing and Customizing the Sample IDP Captive Portal	84
	Configuring Properties for the Sample IDP Captive Portal	84
	Basic Portal Properties	85
	Locator Properties	87
	Deploying the Updated WAR File	88
	Accessing the IDP Captive Portal	88
	Configuring the Redirect Server to Redirect Traffic to the IDP Captive Portal	88
	Applying Services to Subscribers Associated with Problem Traffic	89
Chapter 9	Enabling SRC Actions from IDP Manager	91
	Overview of How to Enable Actions from IDP Manager	91
	Configuring Scripts for IDP	91
	Before You Configure Scripts	91
	Configuring Scripts	92
	Properties in the idpsdx.py File	92
	Sample idpsdx.py Script	94

Part 4 Integrating IP Address Managers

Chapter 10 Integrating IP Address Managers with the SAE 97

Overview of IP Address Manager Integration	97
Monitoring DHCP Messages	98
Monitoring RADIUS Messages	98
Installing Monitoring Agent	99
Configuring Monitoring Agent	99
Configuring Properties	99
Monitoring Agent Properties	99
Configuring NIC Proxy	101
Managing Monitoring Agent	102
Starting Monitoring Agent	102
Stopping Monitoring Agent	102
Displaying Monitoring Agent Status	103
Cleaning Monitoring Agent Logs	103

Part 5 Integrating Prepaid Service Applications

Chapter 11 Providing Prepaid Services 107

Overview of Prepaid Services Demo	107
Account Server	107
Time-Based Services	108
Volume-Based Services	108
Installing and Configuring the Prepaid Services Demo	109
Installing the Account Server	109
Configuring the Account Server	109
Publishing the Object References	110
Manual Configuration	110
Starting the Account Server	111
Stopping the Account Server	111
Configuring the SAE for the Prepaid Plug-In	111
Configuring the Prepaid Services	112
Deploying the Prepaid Account Administration Application	112
Configuring the Prepaid Account Administration Application	113
Managing Prepaid Accounts	113
Accessing the Prepaid Account Administration Application	113
Administering Accounts	113

Part 6 Managing Access Portals for Residential Subscribers

Chapter 12 Overview of the Residential Portal 117

How Subscribers Use a Residential Portal	117
Overview of a Residential Portal	118
Subscriptions to Services	118
Service Schedules in a Residential Portal	119
Equipment Registration for DHCP Login	119
Overview of the Sample Residential Portal	119
Web Application Architecture	119
Model Components	119
View Components	120
Control Components	120
Behaviors for the Sample Residential Portal	120

Chapter 13 Installing and Configuring the Sample Residential Portal 121

Before You Install and Configure the Sample Residential Portal	121
Configuring Equipment Registration and ISP Service Behaviors	121
Configuring Cable Behavior	122
Authenticating Subscribers Through RADIUS	122
Customizing How the Sample Residential Portal Handles Unrecognized IP Subscribers	123
Overview of Configuration Files for the Sample Residential Portal	123
WEB-INF/portalBehavior.properties	123
WEB-INF/struts-config.xml	125
WEB-INF/tiles-defs.xml	128
Installing the Sample Residential Portal	129
Preparing the Application for Customization	130
Configuring the Sample Residential Portal	130
Deploying the Updated WAR File	130
Testing a Portal Application	131
Removing Access to the Sample Residential Portal	131

Chapter 14 How Subscribers Use the Sample Residential Portal 133

Overview of the Sample Residential Portal	133
Before You Use the Sample Residential Portal	133
Logging In to the Sample Residential Portal Using a Simulated User Profile	133
Logging In to the Sample Residential Portal	134
Managing Services from the Sample Residential Portal	136
Starting and Stopping Services	137
Getting Usage Information	138
Setting Up the Type of Service Activation	139

Setting Up Service Schedules	140
Specifying Values for Times	142
Setting Times	142
Setting Actions	144
Subscribing to Services	145
Registering Equipment for DHCP Login	146
Disabling Equipment Registration	147
Logging Out of the Sample Residential Portal	149
Using the Sample Residential Portal from PDAs	150

Chapter 15

Developing a Residential Portal **153**

Before You Develop a Residential Portal	153
Development Tools to Create a Residential Portal	153
Virtual IP Address for Policies	154
Redirecting Traffic to a Captive Portal Web Page	154
Sequence for Redirecting Traffic	155
Configuring the SRC Software in a Multihop Environment	155
Managing Security for Public Wireless LAN Applications	156
Developing a Portal Based on the Sample Residential Portal	156
Preparing to Develop a Portal Based on the Sample Residential Portal	157
Creating a Portal Project	157
Building the Portal	158
Deploying the Portal	158
Testing a Portal Application	158

Part 7

Designing Services for Enterprise Manager Portal

Chapter 16

Reviewing and Configuring Policies and Services for Enterprise Manager Portal **161**

Overview of Services for Enterprise Manager Portal	161
Directory Structure	162
Priorities for Subscriptions	162
Before You Configure Services for Enterprise Manager Portal	162
Configuring Firewall Policies and Services for Enterprise Manager Portal	163
Types of Firewall Services	163
Overview of Basic Firewall Services and Policies	164
Tasks to Configure Firewall Policies and Services	165
Configuring Basic Firewall Policies	165
Configuring Basic Firewall Services	166
Reviewing the fwrule Policy Group for Exceptions to Stateful Firewalls	166
Reviewing the Firewall Rule Service for Exceptions to Stateful Firewalls	166

Reviewing Services for Exceptions to Stateless Firewalls	167
Parameter Values Used by Services for Exceptions to Stateless Firewalls	168
Planning Services for Custom Firewall Exceptions	169
Configuring Policies for Custom Firewall Exceptions	169
Configuring Services for Custom Firewall Exceptions	170
Configuring Priorities for Stateless or Stateful Firewall Services	170
Configuring Priorities to Have Enterprise Services Work Together	170
Configuring Priorities for Individual Scopes by Defining Them in Services	171
Using Stateless Firewall and BoD Applications Together	171
Configuring NAT Policies and Services for Enterprise Manager Portal	172
NAT Policies and Services in the SRC Sample Data	172
Configuring the dynsrcnat Policy Group	172
Reviewing the DynSrcNat Service	173
Configuring the staticdstnat Policy Group	173
Configuring the StaticDstNat Service	173
Configuring the staticsrcnat Policy Group	173
Configuring the StaticSrcNat Service	174
Configuring Bandwidth Policies and Services for Enterprise Manager Portal	174
Bandwidth-on-Demand Services for Enterprise Manager Portal	174
Parameter Values Used by BoD Services	175
Bandwidth Policies for Different Routing Platforms	176
Configuring Basic BoD Policies	176
Configuring Basic BoD Services	177
Configuring BoD Policies	178
Configuring BoD Services	179
Using BoD Services to Assign Traffic to Bandwidth Categories	179
Using BoD and Basic BoD Services Together to Supply Class of Service	180
Examples: Setting Up Forwarding Preferences	180
Setting Up Forwarding Preferences by Using CoS on JUNOS Routing Platforms	180
Setting Up Forwarding Preferences by Allocating a Percentage of a Link's Bandwidth to a Service	181
Enabling Schedules for Subscriptions for Enterprise Manager Portal	182
Configuring VPNs for Enterprise Manager Portal	182
Overview of VPN Management Through Enterprise Manager Portal	183
Before You Configure VPN Policies and Services	183
Configuring Policies for BoD Traffic Destined for VPNs	183
Configuring Services for BoD Traffic Destined for VPNs	184
Billing Subscribers Through SCU/DCU for JUNOS Routing Platforms	184

Part 8**Managing Access Portals for Enterprise Subscribers**

Chapter 17**Overview of Enterprise Service Portals 189**

Function of Enterprise Service Portals	189
Consistency of Data in the Directory	190
Privileges of IT Managers	190
Developing and Customizing Enterprise Service Portals	190
Identifying the SAE	190
Enterprise Service Portals Provided with the SRC Software	191
Sample Enterprise Service Portal	191
Enterprise Manager Portal	191
NAT Address Management Portal	191
Enterprise Service Portal Audit Plug-In	193
Network Information Collector with Enterprise Service Portals	193
Service Parameters	193
Substitutions and the Parameter Acquisition Path	194
Power of Substitutions	195
Substituting Values for Policy Parameters	195
Managing Subscriptions to Aggregate Services	196
Configuring Your Web Browser to Use an Enterprise Service Portal	196
Accessing Enterprise Service Portals	196

Chapter 18**Planning Deployment for Enterprise Service Portals 199**

Architecture of Enterprise Service Portals	199
Elements for an Enterprise Service Portal	199
Communication Protocols	200
Deployment Scenario for an Enterprise Service Portal	200
Deciding Which Enterprise Service Portal to Use	201
Planning Number of Instances of an Enterprise Service Portal	202
Planning Namespace Hierarchy for an Enterprise Service Portal	202

Chapter 19**Installing and Configuring Enterprise Service Portals 205**

Before You Install an Enterprise Service Portal	205
Setting Up Enterprise Service Portals	206
Preparing the Web Applications for Customization	206
Configuring Connections to the Directory	207
Initialization Properties for Enterprise Service Portals	207
Configuring Deployment Settings for Enterprise Manager Portal	209
Deployment Properties for Enterprise Manager Portal	209
Configuring the URL for an Enterprise Service Portal	215
Writing an Application to Allow a Machine to Provide Public IP Addresses for NAT	215
Configuring an Enterprise Service Portal Audit Plug-In	216

Chapter 20**Managing Services with Enterprise Manager Portal****219**

Overview of Enterprise Manager Portal	219
Getting Help on Enterprise Manager Portal	220
Setting the Configuration Level for Enterprise Manager Portal	220
Managing Schedules	221
Schedules in Enterprise Manager Portal	221
Enabling Scheduling for the Enterprise Manager Portal	222
Using Schedules in Enterprise Manager Portal	222
Creating a Schedule in Enterprise Manager Portal	222
Applying a Schedule to a Service in Enterprise Manager Portal	226
Disabling a Schedule for a Service in Enterprise Manager Portal	227
Changing Schedules in Enterprise Manager Portal	228
Managing Subscriptions to Bandwidth-on-Demand Services	228
Overview of Bandwidth-on-Demand Services	229
Planning Subscriptions to BoD Services	229
Creating a Subscription to BoD Services	230
Setting a Bandwidth Level	230
Adding Subscriptions to BoD Services	231
Modifying Rules for a Subscription to a BoD Service	242
Modifying the Bandwidth Level	242
Moving the Bandwidth Level	242
Deleting a Subscription for a BoD Service	242
Deleting the Bandwidth Level	243
Monitoring Use of Subscriptions to BoD Services	243
Integrating VPNs into an SRC Network Through Enterprise Manager Portal	244
Overview of VPNs in an SRC Network	244
Modifying Subscriber VPN Configuration	244
VPN Fields in Enterprise Manager Portal	245
Creating Extranets Through Enterprise Manager Portal	246
Deleting Extranets Through Enterprise Manager Portal	247
Sending Traffic to a VPN	247
Modifying the VPN to Which the Router Sends Traffic	247
Stopping the Router from Sending Traffic to VPNs	248
Classifying Traffic for Stateful Firewall Exceptions and NAT Rules	248
Overview of Traffic Classification for Firewall Exceptions and NAT Rules	248
Classifying Traffic	249
Traffic Classification Fields in Enterprise Manager Portal	250
Modifying Values for Traffic Classifications	253
Deleting Traffic Classifications	254

Subscribing to Firewall Services Through Enterprise Manager Portal	254
Overview of Firewall Services in Enterprise Manager Portal	254
Before You Configure Firewall Exception Rules	255
Creating Subscriptions to Firewall Services	255
Firewall Service Field in Enterprise Manager Portal	256
Creating Firewall Exceptions for Stateless Firewalls	256
Fields for Exceptions to Stateless Firewalls in Enterprise Manager Portal	259
Creating Firewall Exceptions for Stateful Firewalls	267
Fields for Exceptions to Stateful Firewalls in Enterprise Manager Portal	267
Adding a Schedule to a Firewall Exception	270
Schedule Field for a Firewall Exception	270
Modifying Firewall Exceptions	271
Deleting Firewall Exceptions	271
Deleting Basic Firewalls	271
Monitoring the Use of Subscriptions to Firewall Services	272
Working with IP Addressing and NAT Services	272
Requesting Public IP Addresses for NAT Services	273
Address Fields for NAT Addressing in Enterprise Manager Portal	274
Canceling Requests for Public IP Addresses	274
Returning Public IP Addresses to Service Providers	275
Applying NAT Rules to Traffic	275
Configuring Public IP Addresses for Outgoing Traffic	277
Outgoing Traffic Fields for NAT Addressing in Enterprise Manager Portal	277
Configuring Public IP Addresses for Incoming Traffic	278
Incoming Traffic Fields for NAT Addressing in Enterprise Manager Portal	278
Configuring Fixed Public Addresses for Outgoing Traffic	279
Modifying NAT Rules	280
Deleting NAT Rules	280
Monitoring the Status of Subscriptions	280
Troubleshooting Subscriptions That Are Not Functioning Correctly	283
Troubleshooting Subscriptions of Unknown Status	283

Chapter 21

Managing Enterprise Service Portals

285

Displaying Information About Your Control in the Enterprise Through the Enterprise Service Portal	285
Updating Data That the Enterprise Service Portal Displays	286
Managing Operators Through the Enterprise Service Portal	286
Creating Managers Through the Enterprise Service Portal	286
Managers Fields in the Enterprise Service Portal	287
Modifying Managers Through the Enterprise Service Portal	289
Deleting Managers Through the Enterprise Service Portal	289

Chapter 22	Using NAT Address Management Portal	291
	Overview of NAT Address Management Portal	291
	Assigning IP Addresses	291
	Acknowledging the Release of IP Addresses	292
Chapter 23	Using the Sample Enterprise Service Portal	295
	Overview of the Sample Enterprise Service Portal	295
	Starting the Sample Enterprise Service Portal	295
	Subscribing to Services	296
	Activating Subscriptions	297
	Deactivating Subscriptions	298
	Suspending Subscriptions	298
	Canceling Suspensions of Subscriptions	299
	Monitoring Use of Subscriptions	299
	Specifying Values for Service Parameters in Subscriptions	299
	Restoring Default Values for Service Parameters In Subscriptions	300
	Deleting Subscriptions	300
	Monitoring Service Sessions for a Subscription	300
	Defining Networks for Departments in an Enterprise	301
	Modifying Network Definitions for Departments in an Enterprise	302
	Deleting Network Definitions for Departments in an Enterprise	303
Chapter 24	Developing an Enterprise Service Portal	305
	Developing a Portal Based on the Sample Enterprise Service Portal	305
	Preparing to Develop a Sample-Based Enterprise Service Portal	305
	Creating a Portal Project for a Sample-Based Enterprise Service Portal	306
	Building a Sample-Based Enterprise Service Portal	306
	Deploying a Sample-Based Enterprise Service Portal	307
	Testing a Sample-Based Enterprise Service Portal	307
	Using a Virtual Address for the Portal	307
Part 9	Index	
	Index	311

List of Figures

Part 2

Providing Network Security and Threat Mitigation

Chapter 2	Mirroring Subscriber Traffic in the SRC Network	11
	Figure 1: Sample Network Topology with a JUNOSe Router and JUNOS Routing Platforms	12
	Figure 2: Scopes to Support Mirroring Traffic	14
	Figure 3: Services to Mirror Traffic	15
	Figure 4: Sample fragSubrIps Parameter Values for Mirroring Enterprise Traffic	15
	Figure 5: Sample fragSubrIps Parameter Value for Mirroring Subscriber Traffic	16
Chapter 3	Providing Endpoint Security with IVE	27
	Figure 6: Sample Retailer Configuration for Host Checking	38

Part 3

Providing Threat Mitigation Services with IDP

Chapter 4	Overview of IDP Integration	41
	Figure 7: Sample Network Topology with a JUNOSe Router	43
	Figure 8: Sample Network Topology with a JUNOSe Router and JUNOS Routing Platforms	44
Chapter 5	Configuring Services and Subscriptions to Integrate IDP	49
	Figure 9: Scopes to Support Policy-Based Routing of Traffic to an IDP Sensor	50
	Figure 10: Services to Policy-Route Traffic to an IDP Sensor	51
	Figure 11: Sample Values for SubrSubnet and SubrIps Parameters in Services for Policy-Based Routing of Traffic	52
	Figure 12: Scopes to Support Mirroring Traffic to an IDP Sensor	56
	Figure 13: Services to Mirror Traffic to an IDP Sensor	57
	Figure 14: Sample Values for SubrSubnet Parameter in Services for Mirroring	57
	Figure 15: Router and Interface Subscriptions for JUNOSe Routers	60

Part 8

Managing Access Portals for Enterprise Subscribers

Chapter 18	Planning Deployment for Enterprise Service Portals	199
	Figure 16: Elements and Communication Protocols for an Enterprise Service Portal	199
	Figure 17: Deployment for an Enterprise Service Portal	201
Chapter 20	Managing Services with Enterprise Manager Portal	219
	Figure 18: Bandwidth & VPNs Page	231
	Figure 19: Bandwidth & VPNs Page with a Bandwidth Level Set	232

	Figure 20: VPNs Page	245
	Figure 21: Applications Page	249
	Figure 22: Create Exception Dialog Box for Stateless Firewalls	257
	Figure 23: Firewall Page with Firewall Service Applied and Exceptions Configured	258
	Figure 24: Firewall Page with Firewall Service Applied	267
	Figure 25: Addresses Page Before Requesting Addresses	273
	Figure 26: Addresses Page After Requesting Addresses	274
	Figure 27: NAT Page	276
Chapter 21	Managing Enterprise Service Portals	285
	Figure 28: Manager's Page	287
Chapter 23	Using the Sample Enterprise Service Portal	295
	Figure 29: Subscriptions Page	298
	Figure 30: Departments Page	302

List of Tables

	About the Documentation	xxv
	Table 1: Notice Icons	xxvi
	Table 2: Text Conventions	xxvi
Part 1	Installing Applications	
Chapter 1	Installing the Sample SRC Applications	3
	Table 3: Sample Applications	3
	Table 4: Components to Support SRC Sample and Demonstration Applications	4
	Table 5: Solaris Packages and Installation Folders for Sample Applications	5
	Table 6: Solaris Packages and Installation Folders for Application Library	5
Part 3	Providing Threat Mitigation Services with IDP	
Chapter 4	Overview of IDP Integration	41
	Table 7: Network Configuration and Forwarding Method	45
	Table 8: Types of Fragment Services in an Aggregate Service	46
Part 6	Managing Access Portals for Residential Subscribers	
Chapter 14	How Subscribers Use the Sample Residential Portal	133
	Table 9: Navigation Pane for the Sample Residential Portal	136
Part 7	Designing Services for Enterprise Manager Portal	
Chapter 16	Reviewing and Configuring Policies and Services for Enterprise Manager Portal	161
	Table 10: Services Available from Enterprise Manager Portal	161
	Table 11: Basic Firewall Services and Policies	164
	Table 12: Stateless Firewall Services in Sample Data	167
	Table 13: Parameters for Stateless Firewall Services for Enterprise Manager Portal	168
	Table 14: NAT Services and Policies	172
	Table 15: Parameters for BoD Services for Enterprise Manager Portal	175
	Table 16: Integrated BoD and Basic BoD Services in Sample Data	181
	Table 17: Policies to Specify Forwarding Treatment for Specified Traffic Classes	182

Part 8**Managing Access Portals for Enterprise Subscribers**

Chapter 18	Planning Deployment for Enterprise Service Portals	199
	Table 18: Communication Protocols for an Enterprise Service Portal	200
	Table 19: Enterprise Service Applications	201
	Table 20: Namespaces for Enterprise Service Portals	202
Chapter 19	Installing and Configuring Enterprise Service Portals	205
	Table 21: Common Audit Plug-In Information	216
	Table 22: Events Reportable to the Audit Plug-In	216
Chapter 20	Managing Services with Enterprise Manager Portal	219
	Table 23: Portal Configuration Support for Services on Routers	219
	Table 24: Maximum Duration for Recurrence Patterns	225
	Table 25: Possible Subscription Status	282

About the Documentation

- SRC Documentation and Release Notes on page xxv
- Audience on page xxv
- Documentation Conventions on page xxv
- Obtaining Documentation on page xxvii
- Documentation Feedback on page xxvii
- Requesting Technical Support on page xxviii

SRC Documentation and Release Notes

For a list of related SRC documentation, see <http://www.juniper.net/techpubs/>.

If the information in the latest *SRC Release Notes* differs from the information in the SRC guides, follow the *SRC Release Notes*.

Audience

This documentation is intended for experienced system and network specialists working with routers running JUNOS® and JUNOSe Software in an Internet access environment. We assume that readers know how to use the routers, directories, and RADIUS servers that they will deploy in their SRC networks. If you are using the SRC software in a cable network environment, we assume that you are familiar with the PacketCable Multimedia Specification (PCMM) as defined by Cable Television Laboratories, Inc. (CableLabs) and with the Data-over-Cable Service Interface Specifications (DOCSIS) 1.1 protocol. We also assume that you are familiar with operating a multiple service operator (MSO) multimedia-managed IP network.

Documentation Conventions

Table 1 on page xxvi defines the notice icons used in this guide. Table 2 on page xxvi defines text conventions used throughout this documentation.

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: Text Conventions

Convention	Description	Examples
Bold text like this	<ul style="list-style-type: none"> Represents keywords, scripts, and tools in text. Represents a GUI element that the user selects, clicks, checks, or clears. 	<ul style="list-style-type: none"> Specify the keyword exp-msg. Run the install.sh script. Use the pkgadd tool. To cancel the configuration, click Cancel.
Bold text like this	Represents text that the user must type.	user@host# set cache-entry-age cache-entry-age
Fixed-width text like this	Represents information as displayed on your terminal's screen, such as CLI commands in output displays.	<pre> nic-locators { login { resolution { resolver-name /realms/ login/A1; key-type LoginName; value-type SaeId; } } } </pre>
Regular sans serif typeface	<ul style="list-style-type: none"> Represents configuration statements. Indicates SRC CLI commands and options in text. Represents examples in procedures. Represents URLs. 	<ul style="list-style-type: none"> system ldap server{ stand-alone; Use the request sae modify device failover command with the force option user@host# . . . http://www.juniper.net/techpubs/software/management/src/api-index.html
<i>Italic sans serif typeface</i>	Represents variables in SRC CLI commands.	user@host# set local-address local-address
Angle brackets	In text descriptions, indicate optional keywords or variables.	Another runtime variable is <gfwif> .
Key name	Indicates the name of a key on the keyboard.	Press Enter.

Table 2: Text Conventions (*continued*)

Key names linked with a plus sign (+)	Indicates that you must press two or more keys simultaneously.	Press Ctrl + b.
<i>Italic typeface</i>	<ul style="list-style-type: none"> ■ Emphasizes words. ■ Identifies book names. ■ Identifies distinguished names. ■ Identifies files, directories, and paths in text but not in command examples. 	<ul style="list-style-type: none"> ■ There are two levels of access: <i>user</i> and <i>privileged</i>. ■ <i>SRC PE Getting Started Guide</i> ■ <i>o = Users, o = UMC</i> ■ The <i>/etc/default.properties</i> file.
Backslash	At the end of a line, indicates that the text wraps to the next line.	Plugin.radiusAcct-1.class = \net.juniper.srmt.sae.plugin\RadiusTrackingPluginEvent
Words separated by the symbol	Represent a choice to select one keyword or variable to the left or right of this symbol. (The keyword or variable may be either optional or required.)	diagnostic line

Obtaining Documentation

To obtain the most current version of all Juniper Networks technical documents, see the products documentation page on the Juniper Networks Web site at <http://www.juniper.net/>.

To download complete sets of technical documentation to create your own documentation CD-ROMs or DVD-ROMs, see the CD-ROM and DVD-ROM Documentation page at

<http://www.juniper.net/techpubs/resources/cdrom.html>

Copies of the Management Information Bases (MIBs) are available at <http://www.juniper.net/>.

Documentation Feedback

We encourage you to provide feedback, comments, and suggestions so that we can improve the documentation. You can send your comments to techpubs-comments@juniper.net, or fill out the documentation feedback form at <https://www.juniper.net/cgi-bin/docbugreport/>. If you are using e-mail, be sure to include the following information with your comments:

- Document or topic name
- URL or page number
- Software release version (if applicable)

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/customers/support/downloads/710059.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: <https://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>

Part 1

Installing Applications

- Installing the Sample SRC Applications on page 3

Chapter 1

Installing the Sample SRC Applications

- SRC Software for Sample and Demonstration Applications on page 3
- Before You Install the Sample SRC Applications on page 4
- Solaris Packages and Installation Folders for Sample and Demonstration Applications on page 5
- Installing SRC Application Packages on page 5
- Uninstalling SRC Packages on page 6
- Installing Sample SRC Data for Sample and Demonstration Applications on page 6
- Installing SRC Sample Web Applications on page 6
- Removing SRC Web Applications on page 7
- Reviewing Port Settings for Sample SRC Applications on page 8

SRC Software for Sample and Demonstration Applications

You can access the software for the SRC sample and demonstration applications, associated documentation for some of the applications, component software to support applications, the SRC SDK, and the product *Release Notes* on the Juniper Networks Web site at: <https://www.juniper.net/support/csc/swdist-erx/src.html>. You can access the documentation for the Enterprise Manager Portal, the sample enterprise service portal, and the NAT Address Management Portal in the *SRC PE Subscribers and Subscriptions Guide*.

The sample applications are distributed either as Solaris packages or Web applications in the `/Demos+Sample_Applications` directory of the `SDK+AppSupport+Demos+Samples.tar.gz` file. Table 3 on page 3 lists the sample applications provided in this file.

Table 3: Sample Applications

Application	Type of Application	File or Directory in Archive File
Enterprise Manager Portal	Web application	/webapp/entmgr.war
IDP integration	Solaris package	UMCidp
Host Checker	Web application	/webapp/hostcheckPortal.war

Table 3: Sample Applications *(continued)*

Application	Type of Application	File or Directory in Archive File
Monitoring Agent application	Solaris package	UMCmagt
NAT Address Management Portal	Web application	/webapp/nataddr.war
Traffic Mirroring	Web application	/webapp/tmPortal.war
Prepaid Account Administration application	Web application	/webapp/accountAdmin.war
Prepaid services demonstration application	Solaris package	UMCpddemo
Sample Enterprise Service Portal	Web application	/webapp/tagsEntDemo.war
Sample residential portal	Web application	/webapp/ssportal.war

The archive file also contains components that support the sample and demonstration applications. Table 4 on page 4 lists the directory and Solaris packages under the /ApplicationSupport directory of the SDK+AppSupport+Demos+Samples.tar.gz file.

Table 4: Components to Support SRC Sample and Demonstration Applications

Component	Type of Application	File or Directory
Plug-ins for Configuration Editor	Plug-in	/ConfEd
Python Runtime Environment	Solaris package	/SMCpython
Configuration Editor	Solaris package	UMCecl
JBoss Application Server	Solaris package	UMCjboss
JAVA Runtime Environment	Solaris package	UMCjre
Python Libraries	Solaris package	UMCpyadd

Before You Install the Sample SRC Applications

Before you install Solaris packages, install the necessary Solaris patches to the installation host, make sure that you understand whether you want to root or nonroot users to have access to install and configure the application, and establish users and groups for software administration.

Table 5 on page 5 lists the components for each sample application, their Solaris package names, and the directories where each component is installed by default. In Table 5 on page 5, the directories listed are all subordinate to /opt/UMC.

Table 5: Solaris Packages and Installation Folders for Sample Applications

Application	Components Supplied with SRC	Package	Installation Directory
IDP Integration	■ IDP Integration components	■ UMCidp	■ idp
Monitoring Agent	■ Packet capture event integration	■ UMCmagt	■ monAgent
Prepaid services demonstration application	■ Prepaid services demonstration application	■ UMCpre	■ prepaid

Solaris Packages and Installation Folders for Sample and Demonstration Applications

Table 6 on page 5 lists the components for applications, their Solaris package names, and the directories where each component is installed by default. All directories listed are subordinate to /opt/UMC.

Table 6: Solaris Packages and Installation Folders for Application Library

Application	Components Supplied with SRC	Package	Installation Directory
IDP Integration	■ IDP Integration components	■ UMCidp	■ idp
Monitoring Agent	■ Packet capture event integration	■ UMCmagt	■ monAgent
Prepaid services demonstration application	■ Prepaid services demonstration application	■ UMCpre	■ prepaid

Installing SRC Application Packages

To install an application package:

1. On the UNIX host where you will install the application library software, log in as root.
2. Launch the **pkgadd** tool.

pkgadd -d /tmp/Demos+Sample_Applications

The tool displays the available Solaris packages.

3. Enter the desired package(s).

You can enter the name or number for a single package, multiple packages separated by spaces, or the keyword **all** to select all the packages.

The tool displays the license agreement.

4. Press Enter to move through the agreement, and then enter **y** to accept the license agreement when prompted by the tool.
5. Follow the prompt directions to accept the installation directory for the package, to permit the use of superuser scripts required for the package, and so on.



NOTE: You can use the UNIX **swmtool** command to install the application packages, but this method requires that you install each application separately. If you use **admintool** directly, you can install multiple applications at the same time.

Uninstalling SRC Packages

Use the **pkgrm** command to uninstall application library components. For example, to remove the Monitoring Agent package, issue the following command, and respond as prompted by the process:

```
pkgrm UMCmagt
```

Installing Sample SRC Data for Sample and Demonstration Applications

You can install sample data from the SRC CLI for the following applications:

- Intrusion Detection and Prevention (IDP) integration application
- Instant Virtual Extranet (IVE) Host Checker integration application
- Traffic-Mirroring Application
- Sample residential portal applications:
 - Equipment registration mode
 - Internet service provider (ISP) mode

For more information about loading sample data with the SRC CLI, see Loading Sample Data in to a Juniper Networks Database (SRC CLI).

Installing SRC Sample Web Applications

Web applications must be deployed in a Web application server. The exact way you install Web applications depends on the Web application server you are using and the particular Web application.

The following procedure provides general steps for installing a Web application:

1. Install the Web application server on the host.

2. If the Web application requires configuration of a properties file, complete the following procedure:
 - a. Copy the WAR file from the `SDK+AppSupport+Demos+Samples.tar.gz` file to a temporary folder on the host.
 - b. Unpack the WAR file.

For information about unpacking and packing WAR files, see

<http://java.sun.com/j2se/1.4/docs/guide/jar/>

- c. Edit the properties file for the Web application.
 - d. Repack the WAR file.
3. Deploy the WAR file by using the procedure appropriate for your Web application server.

For information about deploying WAR files, see the documentation for your Web application software.

Installing Web Applications Inside the JBoss Application Server

JBoss is an open-source Java application server that provides full support for J2EE application programming interfaces (APIs). To deploy a Web application inside JBoss:

1. Install the UMCjboss package from the `SDK+AppSupport+Demos+Samples/ApplicationSupport` directory.
2. During the installation, choose a JBoss configuration when prompted; typically choose the default configuration.
3. Customize the properties file for the Web application.
4. Deploy the WAR file by copying it into the JBoss `default/deploy` directory.

```
cp <filename>.war /opt/UMC/jboss/server/default/deploy
```

JBoss automatically starts the Web application when a new WAR file is copied into the deploy directory.

Removing SRC Web Applications

The way you remove a Web application depends on the Web application server that you are using. Refer to the documentation on removing Web applications for your server.

Removing a Web Application from JBoss

To undeploy a Web application from JBoss, remove the WAR file from the JBoss `default/deploy` directory.

Reviewing Port Settings for Sample SRC Applications

If you use firewall software within your internal network, ensure that firewall settings allow traffic to and from the ports for the sample applications that you implement in your environment. The prepaid services application that communicates between the prepaid services Web application and an account server uses TCP port 8803.

Part 2

Providing Network Security and Threat Mitigation

- Mirroring Subscriber Traffic in the SRC Network on page 11
- Providing Endpoint Security with IVE on page 27

Chapter 2

Mirroring Subscriber Traffic in the SRC Network

- Overview of Traffic Mirroring on page 11
- Configuring Traffic Mirroring on page 13
- Managing Traffic Mirroring on page 19

Overview of Traffic Mirroring

Traffic mirroring allows you to intercept subscriber traffic by configuring a service with the SRC software that applies policies on a JUNOS routing platform in a fashion similar to the application of firewall filters.

When the SAE activates a traffic-mirroring service session, the session applies filters to the forwarding table to mirror traffic using the preconfigured mirroring port and policy-specified filters. The process is similar to service activation on interfaces, but this service is activated on the forwarding table for a JUNOS routing platform and is applicable only to input.

By activating traffic-mirroring services in an SRC-managed environment, service providers can use the SRC software to simplify traffic mirroring on their network equipment. The SRC software can set up a policy to:

- Monitor subscriber traffic and intercept traffic from a particular source or to a particular destination.
- Take actions for subscribers with intercepted traffic by applying policies to the subscriber traffic.

You must deploy traffic mirroring on JUNOS routing platforms to monitor the subscriber traffic.

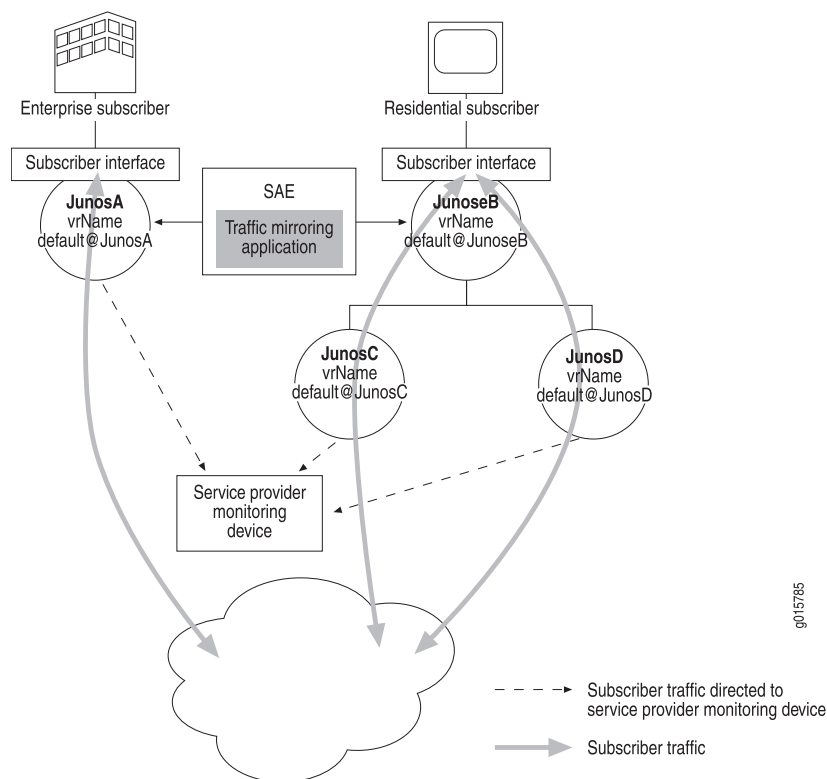
The traffic-mirroring application is not compatible with Web application server clusters; it should be run in a standalone Web application server.

Traffic-Mirroring Application

The SRC application library provides a traffic-mirroring application that can mirror subscriber traffic on any subscriber access platform supported by the SRC software. You set up traffic mirroring by configuring a service with the SRC software that

applies policies on a JUNOS routing platform to mirror subscriber traffic in the SRC-managed network. The traffic-mirroring application provides robust sample data for mirroring traffic. Figure 1 on page 12 illustrates a sample network configuration that contains JUNOSe routers and JUNOS routing platforms.

Figure 1: Sample Network Topology with a JUNOSe Router and JUNOS Routing Platforms



The implementation includes:

- Policies, services, router definitions, and SAE configuration in the sample data. Sample entries for traffic mirroring have the prefix TM.

For information about installing sample data, see “Installing the Sample SRC Applications” on page 3.

- Sample policies and services to mirror subscriber traffic.
- Traffic Mirroring Administration portal.

You can use the sample data to create a demonstration implementation. The traffic-mirroring router definitions, identified as TM <routername> in the sample data, can be configured to act as simulated routers for the demonstration environment. For information about setting up a simulated router, see Configuring Simulated Router Drivers (SRC CLI).

You can also customize the sample data to use traffic mirroring in your network, or you can use the samples as a guide to create your own implementation.

Configuring Traffic Mirroring

To support traffic mirroring in an SRC network, configure an aggregate service that can be activated to set up input filter policies on a JUNOS routing platform. The aggregate service defines the set of addresses to be mirrored, such as the subscriber's address or the list of addresses used by an enterprise. This aggregate service is activated for the subscriber whose traffic should be mirrored, and it also activates fragment services on the JUNOS routing platforms that perform the mirroring. One fragment is activated on each JUNOS routing platform that will process the subscriber's traffic for mirroring.

You must have preconfigured forwarding options on JUNOS routing platforms for port mirroring and next-hop-group. For complete information about how these features work on the router, see the *JUNOS Policy Framework Configuration Guide*.

To use the traffic-mirroring application, configure the following items:

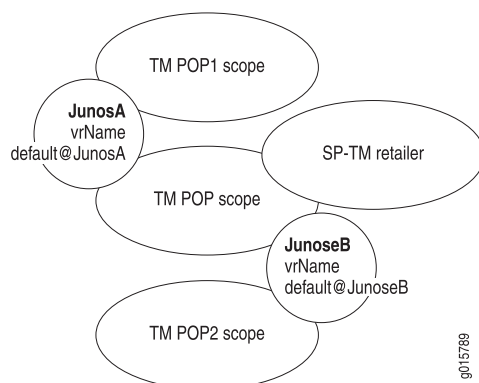
- Service scopes
- Services for mirroring traffic on routers in subscriber paths
- Subscription to service
- Subscriber sessions for forwarding interfaces

The following sections describe the tasks to incorporate traffic mirroring in your environment and provide references to entries in the sample data that demonstrate an implementation.

Configuring Scopes

You configure scopes to define the services to be activated for a specific SRC-managed network and the set of routers that handle subscriber traffic for a location, usually a point of presence (POP).

Figure 2 on page 14 shows the scopes and routers configured in the sample data. The TM POP scope is the scope assigned to all routers, and contains the aggregate and fragment services. Attaching this scope to the retailer (SP-TM) is the easiest way to define the services for all routers. The TM POP1 scope defines the list of JUNOS routing platforms that provide the mirroring service for the subscriber access router. The TM POP2 scope is the scope assigned to JUNOSe routers, and contains the aggregate and fragment services.

Figure 2: Scopes to Support Mirroring Traffic

To configure scopes for defining mirroring services:

1. In SDX Admin, create a general POP scope that defines the mirroring services (aggregate and fragment) to be activated for the network. For more information about defining the aggregate and fragment services, see “Configuring Services for Mirroring” on page 14.
2. Assign this scope to the retailer so that the mirroring services are available to all subscribers, including router subscribers. For an example, see *retailermame = SP-TM, o = Users, o = umc* in the sample data.

For a sample scope, see *l = TM, o = Scopes, o = umc* in the sample data.

To configure scopes for defining mirroring routers:

1. In SDX Admin, create a network-specific scope that lists the names of the mirroring routers in this POP.

This scope must contain a parameter specifying the virtual router names of the JUNOS routing platforms in the POP. By using this list, the SRC software activates the services in the JUNOS scope for each router listed.

2. Assign this scope to the virtual routers on the subscriber access router. For an example, see *virtualRouterName = default, orderedCimKeys = TMJunosA, o = Network, o = umc*. This scope is assigned to the routers to define which core routers transmit subscriber traffic.

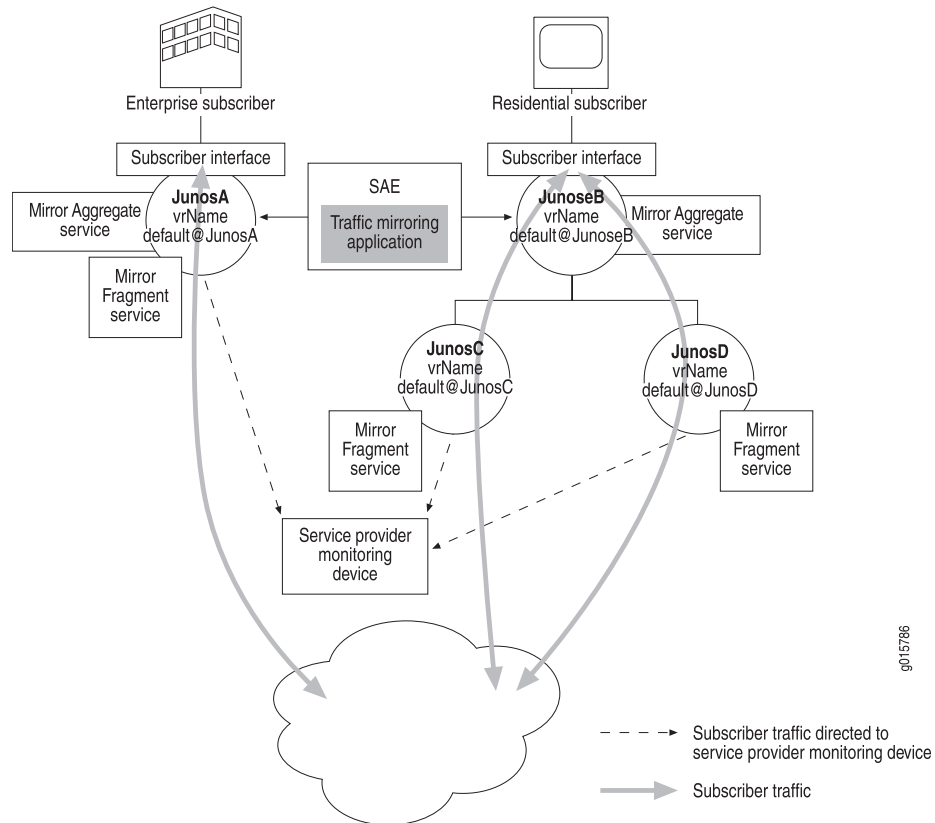
For a sample scope, see *l = TM-Pop1, o = Scopes, o = umc* in the sample data.

Configuring Services for Mirroring

Before you configure services to mirror subscriber traffic, make sure that the JUNOS routing platform is configured for mirroring, that SRC service policies specify which traffic to mirror, and that the router configuration specifies how to implement mirroring on that system. For information about port mirroring on a JUNOS routing platform, see the *JUNOS Policy Framework Configuration Guide*.

Figure 3 on page 15 illustrates the services in the sample data that mirror subscriber traffic from JUNOS routing platforms and shows the routers on which the services are activated.

Figure 3: Services to Mirror Traffic



The traffic-mirroring application passes the value of the `subrlps` parameter to the aggregate service; the aggregate service then substitutes the value of the `subrlps` parameter for the `fragSubrlps` parameter in the fragment services. For example, in Figure 4 on page 15, the enterprise IP addresses (112.2.1.13 and 112.2.1.14) that were entered are passed to the aggregate service. The aggregate service passes the value for the IP address to the fragment service for the local router (JunosA). Similarly, in Figure 5 on page 16, the Mirror Traffic of Subscriber's Current IP check box in the Traffic Mirroring Administration portal was selected, and the aggregate service passes the subscriber's current IP address in the subscriber session (111.1.2.6) to the fragment services for the JUNOS routing platforms in the same POP (JunosC and JunosD).

Figure 4: Sample fragSubrlps Parameter Values for Mirroring Enterprise Traffic

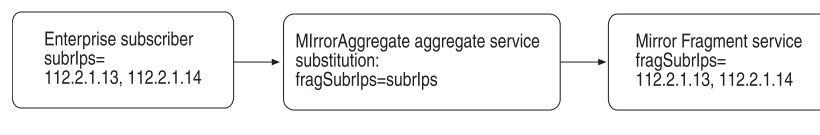
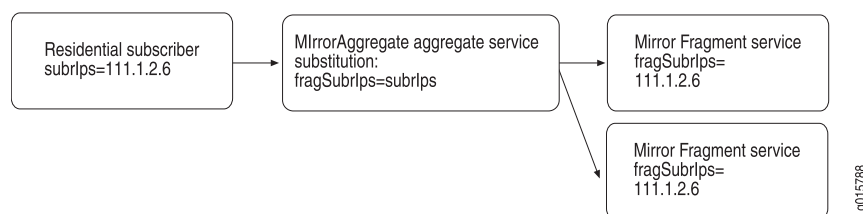


Figure 5: Sample fragSubIps Parameter Value for Mirroring Subscriber Traffic

Configuring Services

To configure services to mirror subscriber traffic:

1. Configure a policy to mirror traffic for a subscriber whose IP addresses are specified by the fragSubIps parameter.

For a mirroring policy, you specify policy rules for traffic sent to and received from the subscriber (the value of the fragSubIps parameter) that have the traffic-mirror action.

For a sample policy that implements mirroring, see *policyGroupName = mirror, ou = tm, o = Policies, o = umc* in the sample data.

2. Create a service for the scope that defines mirroring services, which is a router fragment service; set the type to normal, and specify the policy group configured in Step 1. This service is activated once for each router in a specified POP.

For a sample service, see *servicename = MirrorFragment, l = TM, o = Scopes, o = umc* in the sample data.

3. Create an aggregate service for the scope that defines mirroring services; set the type to aggregate; and define the fragment service in the Aggregate tab of the SSP Service pane by using the field descriptions in “Aggregate Service Fields for Mirroring Traffic” on page 16 to enter the information in the fields of the Service Fragment dialog box.

For a sample aggregate service, see *serviceName = MirrorAggregate, o = TM, o = Scopes, o = umc* in the sample data.

Aggregate Service Fields for Mirroring Traffic

Use the fields in this section to configure aggregate services in the Service Fragment dialog box.

Expression

- Subscriber reference expression to specify each mirroring router in the subscriber’s traffic paths and the interface name used to activate the service.
- Value—vr = " < - substitution.vrNames - > ",
interfaceName = "FORWARDING-INTERFACE"

- FORWARDING-INTERFACE is used to activate the fragment service for the forwarding table. The vrNames substitution must be defined in each separate POP-specific scope.

Service

- Service to be included in the aggregate service as a fragment service.
- Value—Service configured in Step 2 of “Configuring Services” on page 16.

Mandatory

- Specifies whether the fragment service is mandatory.
- Value
 - false
 - If there is a redundancy group, the application will show the mirroring task as pending until one of the mirroring routers becomes manageable by the SAE.
 - If there is no redundancy group, the application will show the mirroring tasks as pending only when it cannot contact the SAE managing the subscriber.
 - true—The application will show the mirroring task as pending until the SAE can activate the fragment service on all the mirroring routers.

Redundancy Group

- Group identifier for a redundant service.
- Value—Text
- Guidelines—Applicable only when Mandatory is false. If there is a redundancy group, then the mirroring task is considered active if the mirroring fragment is activated on at least one of the mirroring routers.

Subscription

- Specifies whether a remote subscriber session is required to subscribe to the fragment service.
- Value—False.

Substitutions

- List of IP addresses for subscribers.
- Value—fragSubrlps = subrlps
- Guidelines—Note that the fragSubrlps parameter is for the fragment service and can be changed to match the parameter used for the policy in Step 1 of “Configuring Services” on page 16. The subrlps parameter is for the aggregate service and cannot be changed. This substitution is used to resolve the value of the IP address in the context of a subscriber session and to pass the correct value to the fragment service.

Subscribing to the Aggregate Service

You subscribe to the aggregate service from a subscriber. To create a subscription to the aggregate service:

1. In SDX Admin, under Users select a retailer, and then create a subscriber folder for subscribers.
2. In the folder for subscribers, create each subscriber for which you want to mirror traffic.
3. Create a subscription to the aggregate service in the folder for subscribers.

For a sample subscription, see *serviceName = MirrorAggregate, ou = subscribers, retailermame = SP-TM, o = Users, o = umc* in the sample data.

Configuring Subscriber Sessions

To apply policies to the forwarding interfaces, you configure additional entries in the subscriber classification and interface classification scripts. For general information about classifying subscribers and interfaces, see Overview of Classification Scripts .

Subscriber Classification Scripts

In addition to the typical entries in the subscriber classification script, traffic mirroring requires the assignment of a subscriber profile for the forwarding interface on the JUNOS routing platform. For example:

```
[ou=routers,retailermame=SP-TM,o=Users,o=UMC??sub?(routerName=<virtualRouterName>)]
# host subscriber for JUNOS routers
interfaceName=="FORWARDING_INTERFACE"
```

To view the sample subscriber classifications referenced in this section, see *l = TrafficMirroring, l = SAE, ou = staticConfiguration, ou = Configuration, o = Management, o = umc* in the sample data.

Interface Classification Scripts

An entry is needed in the interface classification script to specify the default policy for forwarding interfaces. This default policy must forward all traffic; otherwise all traffic that is not mirrored is dropped. For example:

```
[policyGroupName=forwardIntfDefault,ou=tm,o=Policies,o=UMC]
# manage router interface for mirroring
interfaceName=="FORWARDING_INTERFACE"
```

To view the sample interface classifications referenced in this section and others, see the interface classification for the TM <routername> routers listed under *o = Network, o = umc* in the sample data.

Managing Traffic Mirroring

You can manage the mirroring of subscriber traffic with the Traffic Mirroring Administration portal. The *tmPortal.war* file comprises the files for the Traffic Mirroring Administration servlet. This file is on the SRC application library CD in the */webapp* directory.

Overview of the Traffic Mirroring Administration Portal

Through the Traffic Mirroring Administration portal, you can manage the traffic-mirroring tasks by:

- Specifying the subscriber whose traffic should be mirrored and the IP addresses of the traffic to be mirrored
- Managing currently active mirroring tasks
- Managing pending actions

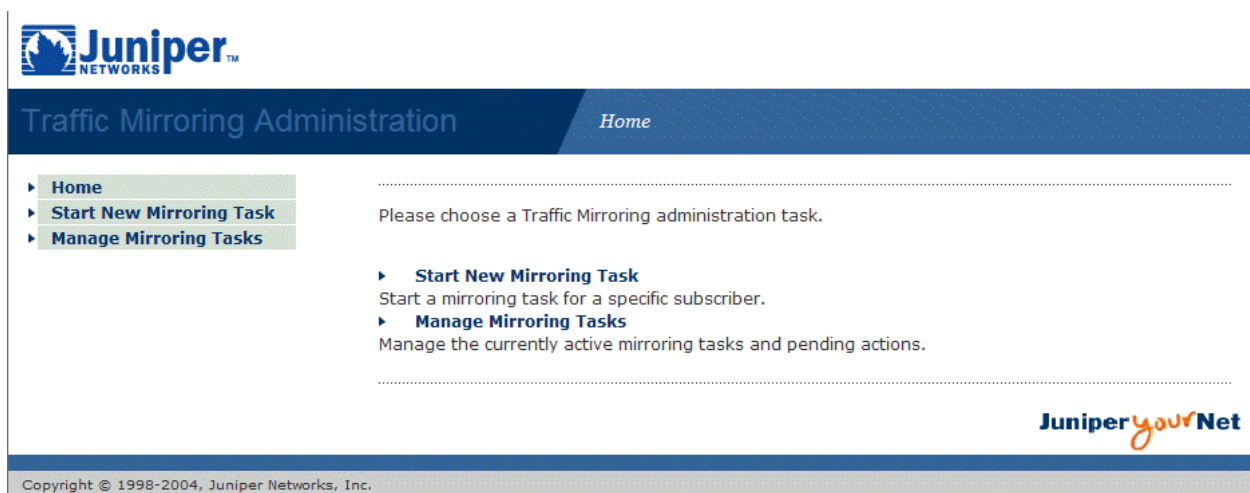
Accessing the Portal

To access the portal, enter the following URL in your Web browser.

http://<host>:<port>/tmPortal

- <host> —IP address or name of the host on which you installed the Traffic Mirroring Administration portal
- <port> —HTTP port for the J2EE application server

The Traffic Mirroring Administration portal appears.



Starting New Mirroring Tasks

To start a new traffic-mirroring task:

1. On the Traffic Mirroring Administration portal, click **Start New Mirroring Task**.

The Start New Mirroring Task page appears.

Start New Mirroring Task:

Specify the subscriber whose traffic should be mirrored, and the source/destination IPs of the traffic to be mirrored.

Subscriber ID Type: Login Name (dropdown)

Subscriber ID: [text input]

Mirror Traffic To/From Subscriber IPs: [text input]

Mirror Traffic of Subscriber's Current IP: ☐

[START] [RESET]

Juniper yourNet

Copyright © 1998-2004, Juniper Networks, Inc.

2. Using the field descriptions below, enter the information in the fields on the Start New Mirroring Task page.
3. Click **START** to perform the task or **RESET** to clear the fields.

If you click **START**, the Manage Mirroring Tasks page appears.

Subscriber ID Type

- Subscriber's ID type.
- Value
 - Login Name—Login name that the subscriber uses to log onto the network.
 - LDAP Distinguished Name—Distinguished name of the subscriber object in the directory. Applicable only when the subscriber objects are not shared by multiple subscribers so they can uniquely identify a subscriber, such as when the subscriber is an enterprise.
 - IP Address—Current IP address of the subscriber. Used when a router can provide subscriber addresses to the SRC software, such as when a JUNOSe

router manages subscribers that get their addresses using RADIUS or using the JUNOS local or external DHCP server.

Subscriber ID

- Value for the subscriber's ID based on the selected subscriber ID type.
- Value
 - <login name>
 - <LDAP distinguished name>
 - <IP address>
- Examples
 - joe@virneo.net
 - accessName=AcmeAccess, enterpriseName=Acme, ou=subscribers, retailername=SP
 - 62.3.21.4

Mirror Traffic To/From Subscriber IPs

- Subscriber's IP addresses.
- Value—IP address
- Guidelines—You can enter the subscriber's IP addresses in this field, and/or select the Mirror Traffic of Subscriber's Current IP check box.

Mirror Traffic of Subscriber's Current IP

- Subscriber's IP addresses.
- Value— < subscriber's IP addresses >
- Guidelines—You can select the Mirror Traffic of Subscriber's Current IP check box, or enter the subscriber's IP addresses in the Mirror Traffic To/From Subscriber IPs field, or both.

Managing Mirroring Tasks

To manage mirroring tasks:

1. On the Traffic Mirroring Administration portal, click **Manage Mirroring Tasks**.

The Manage Mirroring Tasks page appears and displays all active tasks and pending actions.



Traffic Mirroring Administration

Manage

- ▶ Home
- ▶ Start New Mirroring Task
- ▶ Manage Mirroring Tasks

Manage Mirroring Tasks:

This page shows the active mirroring tasks and the pending actions.
An active task can be stopped, and a pending start/stop action can be cancelled.

ACTIVE MIRRORING TASKS

ID Type	ID	IP Address	Mirroring Current User IP	Task Creation Time	Mirroring Start Time	Action
Login Name	joe@tm		true	Wed Mar 23 11:03:48 EST 2005	Wed Mar 23 11:03:48 EST 2005	<input type="button" value="STOP"/>

PENDING ACTIONS

No pending task available

Juniper yourNet

Copyright © 1998-2004, Juniper Networks, Inc.

2. In the Active Mirroring Tasks table, click **STOP** in the Action column to stop the task in that row.

The resulting action depends on whether the subscriber is online when you stop the task.

- If a subscriber is logged in, the mirroring task is removed from the Manage Mirroring Tasks page.
 - If a subscriber is logged out, the mirroring task is placed in a pending state and appears in the Pending Actions table.
3. In the Pending Actions table, the situation that results in a pending task determines the next step that can be taken.

- If the subscriber is not logged in when you start the mirroring task, then the task automatically becomes a pending action.

Click **CANCEL** in that row to remove the mirroring task from the Manage Mirroring Tasks page.

- If the subscriber is logged in when you start the mirroring task and the subscriber logs out before you click **STOP** in the Active Mirroring Tasks table, then the possible actions are determined by when the affected subscriber logs in again.
 - If the subscriber will never log in again, the task will never be removed from the Pending Actions table.

Click **Details** in the Pending Due To column to determine why the action is pending. To force the cleanup of any task in the pending stop state, use the **Force Cleanup** button in the Pending Actions table, which you get to by clicking the **Details** link.

Use the **Force Cleanup** button only when the traffic-mirroring service activation has been removed or the subscriber has been removed from the system and will never log in again.

- If the subscriber logs in again while the action is pending, the task is removed from the Manage Mirroring Tasks page.
- If you click **CANCEL** before the subscriber logs in again, the task becomes active and appears in the Active Mirroring Tasks table.

Configuring the Traffic Mirroring Administration Portal

The Traffic Mirroring Administration portal provided with the SRC software is designed to be used with the traffic-mirroring implementation in the sample data. To use the portal, edit the *WEB-INF/default.properties* file.

To customize properties for the Traffic Mirroring Administration portal:

1. Copy the *tmPortal.war* file to a temporary folder, and work in that folder.
2. Extract the *default.properties* file from the *tmPortal.war* file.

jar xvf tmPortal.war WEB-INF/default.properties

3. With a text editor, edit the *WEB-INF/default.properties* file.
 - This file provides the bootstrap properties. Change these values as needed to accommodate your SRC configuration. For example, the file specifies that the LDAP directory server is being used in the default port on the local system. To change the location of the directory server, edit the `Config.java.naming.provider.url` property.
 - This file provides the bootstrap configuration that specifies the configuration namespace for the application. By default, `/WebApplication/TrafficMirroring` is used as the namespace. If you are using another namespace, change the `tmConfigNamespace` and `loggingConfigNamespace` properties.
4. Replace the *WEB-INF/default.properties* file in the *tmPortal.war* file.

jar uvf tmPortal.war WEB-INF/default.properties

Deploying the Traffic Mirroring Administration Portal

To deploy the updated *tmPortal.war* file:

- Copy the file to the deployment directory for your Web server.

If you are using JBoss, copy the file to the `/opt/UMC/jboss/server/default/deploy` directory. JBoss automatically starts the Web application when a new WAR file is copied into the `deploy` directory.

Configuring the Traffic-Mirroring Application

To use the traffic-mirroring application, you must configure properties to specify how the application handles information about mirroring tasks and the aggregate service that the application activates to mirror traffic.

To configure these properties for the traffic-mirroring application:

1. In SDX Admin go to `l = TrafficMirroring`, `l = WebApplication`, `ou = staticConfiguration`, `ou = Configuration`, `o = Management`, `o = umc`.
2. In the Main tab for Configuration, modify the following properties.

directory

- Specifies the directory in the file system in which information about the mirroring tasks is stored. The application stores all tasks in a series of files that are considered live or dead. Live files record at least one active or pending task and include the word *live* in their names. Dead files record only tasks that have been canceled or stopped and include the word *dead* in their names. You can delete or archive dead files at any time. However, if you delete a live file, the application will not be able to access information about existing tasks.
- Value— <pathname>
- Guidelines—The application server must be able to write and modify files in this directory. If you use WEB-INF, you will lose all your data about the mirroring tasks whenever you undeploy or redeploy the traffic-mirroring application.
- Default—WEB-INF

retryInterval

- Time to wait before retrying a pending task that was unsuccessful.
- Value—Number of seconds
- Guidelines—Do not specify too small a value, because the number of service activation attempts could cause network overload.
- Default—900

serviceName

- Name of the aggregate service activated by the application to mirror subscriber traffic.
- Value— <service name>
- Default—MirrorAggregate

maxFileSize

- Maximum file size for files that store information about the pending and active tasks. A new file is created whenever the current file exceeds this setting.
- Value—Number of bytes
- Guidelines—This value should not need modification.
- Default—1000000 (1 MB)

Configuring NIC Proxy

To configure a NIC proxy for the traffic-mirroring application, see Overview of NIC Proxy Configuration.

Configuring Logging

To configure logging for the traffic-mirroring application, see Configuring System Logging (SRC CLI) or Configuring a Component to Store Log Messages in a File (SRC CLI).

Chapter 3

Providing Endpoint Security with IVE

- Overview of IVE Host Checker Integration on page 27
- Before You Integrate IVE into an SRC Environment on page 27
- Sample Implementation for Integrating IVE Host Checker on page 29
- Configuring Host Checking in an SRC Network on page 29

Overview of IVE Host Checker Integration

The IVE Host Checker feature simplifies secure remote access by ensuring endpoint security compliance. It can be used to verify third-party software compliance and application authenticity to prevent unauthorized access to the network. By integrating IVE into an SRC-managed environment, you can use the SRC software to monitor subscriber logins with the IVE to:

- Automatically authenticate the subscriber anonymously.
- Use the IVE's single sign-on (SSO) capability to forward the results of the host check to the Host Check Result portal.

Based on the host-checking results, the subscriber may be allowed full, limited, or no access to the Internet.

You can deploy IVE Host Checker in a network so that it is activated:

- Each time the subscriber logs in.
- When the Intrusion Detection and Prevention (IDP) system finds an anomaly in the subscriber's traffic. See "Overview of IDP Integration" on page 41.
- According to the service provider's schedule.

Before You Integrate IVE into an SRC Environment

Integrating IVE into an SRC-managed environment requires:

- The Host Check Result portal installed with your SRC application library software.
- SRC-managed JUNOSe routers or JUNOS routing platforms in the network.
- Working knowledge of the IVE platform. For the IVE OS product documentation, see <http://www.juniper.net/techpubs>

For complete information about IVE Host Checker features, see the *Juniper Networks Secure Access and Secure Meeting Administration Guide*.

Before you extend IVE host checking to SRC subscriber traffic, you would typically preconfigure IVE software as follows:

1. Define Host Checker policies to verify that the subscriber's system meets the service provider's requirements.



NOTE: We recommend that you specify one rule for each Host Checker policy to provide detailed results.

2. Create two roles, HCComplied (for subscribers complying to the policies) and HCViolated (for subscribers violating the policies), and set the Host Check Result portal as the start page for these roles.
3. Create an anonymous authentication realm for subscribers.
4. Assign the defined Host Checker policies to the realm as authentication policies.
5. Define role-mapping rules for the anonymous realm that map subscribers (complying or violating Host Checker policies) to different roles. The rules are evaluated in sequential order.
6. Define a sign-in policy that maps a URL to the anonymous authentication realm created in Step 3.
7. Define a remote SSO Form POST policy for both roles defined in Step 2 that includes the following information:
 - Resource: URL of the Host Check Result portal
 - Role: Policy applied to both roles
 - Action: POST performed as defined by the Post to URL and Post parameters values
 - Post to URL: URL of the Host Check Result portal servlet
 - Post parameters:
 - subscriberIp
 - IP address of the subscriber
 - Value— < sourceIp >
 - compliedPolicy < x >
 - The Host Checker policy assigned to the authentication realm. There must be a one-to-one correspondence between the compliedPolicy < x > parameter and each Host Checker policy.
 - Value— < hostCheckerPolicy[x] > , where x is an integer in the range 1 to the number of Host Checker policies assigned to the authentication realm.

8. Customize the *Logout.thtml* file, which is one of the sign-in pages for the authentication realm, to automatically redirect the subscriber to the Host Check Result portal. Add the following line to the `<head>` section of the *Logout.thtml* file:

```
<meta http-equiv="Refresh" Content="0; URL=<Portal URL>">
```

where `<Portal URL>` is the Host Check Result portal URL.

Sample Implementation for Integrating IVE Host Checker

The SRC application library provides a sample implementation for integrating IVE Host Checker into an SRC-managed network. The sample data demonstrates how subscriber traffic can activate host checking for a retailer in different scenarios.

The sample implementation includes:

- Policies, services, and SAE configuration in the sample data

For information about installing sample data, see “Installing the Sample SRC Applications” on page 3.

- Host Check Result portal

For information about using the Host Check Result portal, see “Configuring the Host Check Result Portal” on page 30.

- Sample SRC VTA application for scheduling subscriber host checking

You can use the sample data and applications to create a demonstration implementation. You can also customize the sample data and applications to integrate IVE Host Checker into your network, or you can use the samples as a guide to create your own implementation.

Configuring Host Checking in an SRC Network

When IVE processes subscriber sign-ons, it identifies compliance with the Host Checker policies that are configured within IVE. For SRC-managed subscriber traffic, you can configure the SRC software to:

- Activate a host-checking service on the subscriber interface to redirect the subscriber’s Web traffic to IVE Host Checker.
- Direct the subscriber’s next HTTP request to the IVE Single Sign-On page for checking the compliance policy of the subscriber’s machine.



NOTE: If connection to the Host Checker client program on the subscriber’s machine is not possible, the subscriber is considered to be violating Host Checker policy.

- Post host-checking results to the Host Check Result portal servlet that provides information about the host’s compliance to Host Checker policies.

- If the subscriber's system complies with the Host Checker policies, the SRC software deactivates the host-checking service so that the subscriber's next Web request will not be redirected to the IVE sign-on page.
- If the subscriber's system does not comply with the Host Checker policies, the SRC software deactivates the host-checking service and can do one of the following:
 - Activate a blocking service to redirect the subscriber's Web traffic to a captive portal until the subscriber's machine is in compliance.
 - Schedule the next host check using the service schedule specified by the result.

To support host checking in an SRC network, configure a service on the subscriber's interface that can be activated to redirect the subscriber's HTTP traffic to IVE Host Checker. You must have preconfigured Host Checker (see "Before You Integrate IVE into an SRC Environment" on page 27). For complete information about IVE Host Checker features, see the *Juniper Networks Secure Access and Secure Meeting Administration Guide*.

To use the host-checking application, perform the following tasks:

- "Configuring the Host Check Result Portal" on page 30
- "Configuring Services for Subscribers" on page 36

The following sections describe the tasks to incorporate IVE Host Checker into your environment and provide references to entries in the sample data that demonstrate an implementation.

Configuring the Host Check Result Portal

You can configure the SRC software to redirect subscriber Web requests to the captive portal page in response to IVE Host Checker policy compliance by a subscriber's machine. A captive portal is simply a Web page that receives redirected HTTP requests. The SRC application library provides a sample Host Check Result captive portal that is a Java 2 Platform, Enterprise Edition (J2EE) Web application. We provide the application for demonstration purposes.

The Host Check Result portal uses a policy-routing service and the redirect server to redirect traffic to the portal. This process is similar to the one used by the sample residential portal. See "Overview of the Residential Portal" on page 117.

You can use the sample Host Check Result portal as the basis for a captive portal for your environment, or you can develop a different captive portal based on the sample.

Overview of the Sample Host Check Result Portal

The sample Host Check Result portal provides:

- The subscriber's IP address.

- An explanation of the host-checking result for each Host Checker policy and the suggested action.
- The controls to reschedule the host-checking service (Remind me again in drop-down list) or to redirect the subscriber to the IVE Sign-In page (Check Again button).

About the HostCheckServlet

The HostCheckServlet receives messages from Host Checker and posts these messages to a specified URL to display the checking result. The default URL is

`http(s)://<hostname>:<port>/hostcheckPortal/HostCheck`

The Host Checker sends the following type of information to the HostCheckServlet.

- subscriberIP—Subscriber's IP address
- compliedPolicy < number > —Host Checker policy name that maps to this complied policy

In the following sample message, the parameter name appears to the left of the equal sign and the value to the right.

```
subscriberIP=10.127.1.137
compliedPolicy1=AcmeAVIsRunning
compliedPolicy2=AcmePFIsRunning
```

The HostCheckServlet maps each IP address to a list of complied policies for the subscriber as a record displayed on the Host Check Result portal.

Developing and Customizing the Sample Host Check Result Portal

The */webapp* directory on the SRC application library CD contains the *hostcheckPortal.war* file, which provides:

- Complete source code for the Host Check Result portal in the *WEB-INF/src* directory
- Documentation for the Java classes used in the sample Host Check Result portal in the */javadoc* directory

For information about customizing the sample Host Check Result portal, see “Configuring Properties for the Sample Host Check Result Portal” on page 32 .


Configuration Tasks to Deploy the Sample Portal

To deploy the sample Host Check Result portal, perform these tasks:

1. “Configuring Properties for the Sample Host Check Result Portal” on page 32
2. “Deploying the Sample Host Check Result Portal” on page 36

3. “Accessing the Portal” on page 36
4. “Configuring the Redirect Server to Redirect Traffic to the Captive Portal” on page 36

The following sample Host Check Result portal page identifies the Host Checker policy and the host-checking result as well as suggested actions. For example, if the correct firewall software is not running, the suggested action is to activate the firewall or follow the link to the site from which it can be purchased.



Virneo Host Check Result Portal

Host Check Result

Current Host IP Address: 172.28.32.143

This host violated one or more HostCheck policies.
You can choose a limited time to continue the web services and take necessary measures to secure your computer.
HostCheck will be re-activated when time expires.

Host Check Policy	Result	Suggested Action
AcmeAVIsRunning	PASS	
AcmePFIsRunning	Acme Personal Firewall is not activated on this host	Please activate Acme Personal Firewall or purchase the latest version of Acme Personal Firewall.

Remind me again in

Configuring Properties for the Sample Host Check Result Portal

The sample Host Check Result portal provided with the SRC software is designed to be used with the IVE integration implementation and the sample data. To use the sample Host Check Result portal, edit the *WEB-INF/hostcheckportal.props* file. This file is in the */webapp/hostcheckPortal.war* file on the SRC application library CD.

To edit the *WEB-INF/hostcheckportal.props* file:

1. Copy the *hostcheckPortal.war* file to a temporary folder, and work in that folder.
2. Extract the *WEB-INF/hostcheckportal.props* file from the *hostcheckPortal.war* file.

jar xvf hostcheckPortal.war WEB-INF/hostcheckportal.props

3. With a text editor, edit the *WEB-INF/hostcheckportal.props* file:
 - Review the basic portal properties listed in “Basic Portal Properties” on page 33, and update fields as needed.
 - Review the entries for the SAE locator listed in “Locator Properties” on page 35, and change them as needed to accommodate your SRC configuration.

- Configure properties in the network information collector (NIC) proxy configuration section of the file. For information about the values to configure for NIC properties, see Overview of NIC Proxy Configuration.
- 4. Replace the *WEB-INF/hostcheckportal.props* file and any other updated files in the *hostcheckPortal.war* file.

jar uvf hostcheckPortal.war WEB-INF/hostcheckportal.props

Basic Portal Properties

The following list describes properties to specify how the portal uses host-checking results received from IVE.

HostChecking.captiveService

- Name of the host-checking service that you use to redirect subscribers to the Host Checker. The Host Check Result portal deactivates this service to protect the IVE system from subscribers who rapidly make Web requests. If you use the “Remind me again in” control on the Web page and the subscriber selects this control, the portal schedules the activation of this service for a later time.
- Value— < service name >
- Default—HostCheck

HostChecking.nonComplianceOption

- Option used when the host violates any Host Checker policy. This property must be set.
- Value
 - Block—Activate the blocking service.
 - Snooze—Allow the subscriber to select a later time for rechecking.
- Default—Block

HostChecking.blockingService

- Name of the blocking service to activate when the Host Checker policy is violated and the HostChecking.nonComplianceOption property is set to Block.
- Value— < service name >
- Guidelines—This service should restrict potentially dangerous users by rate limiting or filtering their traffic, and by policy routing all their Web traffic to the Host Check Result portal to continually remind them that they are not in compliance with the service provider’s policies.
- Default—Block

HostChecking.IVESignInURL

- URL to which the subscriber is redirected to perform the host check when the subscriber clicks the Check Again button.
- Value—https:// < IVE hostname > /check

HostChecking.IVELogoutURL

- URL used to log out the subscriber. Each time a subscriber is directed to the Host Check Result portal by the IVE, the Host Check Result portal will use this URL to log the subscriber out of the IVE so that the IVE will reverify the subscriber the next time the subscriber is directed to the IVE.
- Value—https:// < IVE hostname > /dana-na/auth/logout.cgi

HostChecking.policy.<policyName>.description

- Description to display when the specified Host Checker policy is violated. This description is displayed on the Host Check Result portal.
- Value—Text
- Guidelines—This property can contain HTML tags for formatting or embedding hyperlinks.
- Example—HostChecking.policy.AcmeAVIsRunning.description = Acme AntiVirus is not activated on this host

HostChecking.policy.<policyName>.action

- Suggested action when subscribers violate the specified Host Checker policy. This description is displayed on the Host Check Result portal.
- Value—Text
- Guidelines—This property can contain HTML tags for formatting or embedding hyperlinks.
- Example—HostChecking.policy.AcmeAVIsRunning.action = Please activate Acme AntiVirus or purchase the latest version of < a href = "http://www.juniper.net" target = "newWindow" > Acme AntiVirus. < /a >

HostChecking.record.number

- Maximum number of Host Checker results to be stored for use by the IVE captive portal. When this number is exceeded, the number of old records is removed as specified by the HostChecking.record.removeStep property.
- Value—Number in the range 1–2147483647
- Default—100

HostChecking.record.removeStep

- Number of records to be deleted when the number of records stored reaches the limit specified by the HostChecking.record.number property. The records are removed sequentially, starting with the oldest record, then the next oldest, and so forth.
- Value—Number in the range 1–2147483647
- Guidelines—This number must be less than the value configured for the HostChecking.record.number property.
- Default—10

Locator Properties

The following list describes SAE locator properties that you change to conform to your configuration. Other configuration properties in the *hostcheckportal.props* file are specific to NIC proxy configuration and logging. For information about NIC proxy configuration, see Overview of NIC Proxy Configuration. For information about logging configuration, see To configure logging for the traffic-mirroring application, see Configuring System Logging (SRC CLI) or Configuring a Component to Store Log Messages in a File (SRC CLI).

Factory.locator

- Method that the portal uses to locate the SAE.
- Value
 - `net.juniper.smgmt.idp.portal.LocalFeatureLocator`—Uses the locally configured object reference
 - `net.juniper.smgmt.idp.portal.DistributedFeatureLocator`—Uses NIC configuration
- Guidelines—If you specify `net.juniper.smgmt.idp.portal.LocalFeatureLocator`, configure a value for `LocalFeatureLocator.objectRef`.

LocalFeatureLocator.objectRef

- Location of the SAE server.
- Value—Location in one of the following formats:
 - The IOR file URL in the format `file:// < absolutePath >`
 - The corbaloc URL in the format `corbaloc:: < IP address > : < port > /SAE`
 - `< IP address >` —IP address.
 - `< port >` —Port number, where 8801 is the default port for the SAE.
 - The actual IOR in the format `IOR: < objectReference >`
- Default—`corbaloc::127.0.0.1:8801/SAE`
- Examples
 - `LocalFeatureLocator.objectRef = file:///opt/UMC/sae/var/run/sae.ior`
 - `LocalFeatureLocator.objectRef = corbaloc::10.10.6.171:8801/SAE`

DistributedFeatureLocator.locName

- Namespace for the NIC proxy configuration.
- Value—`< namespace >`
- Default—`/`, which indicates the root namespace
- Example—`DistributedFeatureLocator.locName = /nicProxy` indicates that the NIC proxy configuration is in `/nicProxy`.

Config.java.naming.provider.url

- Location of the LDAP server.

- Value—`ldap:// <IP address> : <port number>`
- Example—`ldap://127.0.0.1:389`

Config.net.juniper.smgmt.des.backup_provider_urls

- Location of a backup LDAP server.
- Value—`ldap:// <IP address> : <port number>` , with more than one URL separated by semicolons

Deploying the Sample Host Check Result Portal

To deploy the updated *hostcheckPortal.war* file:

- Copy the file to the deployment directory for your Web server.

If you are using JBoss, copy the file to the `/opt/UMC/jboss/server/default/deploy` directory. JBoss automatically starts the Web application when a new WAR file is copied into the *deploy* directory.

Accessing the Portal

Access the portal to ensure that you can view the page and to review the page setup. To access the Host Check Result portal, type a URL in the following form in your Web browser, and press Enter:

[http\(s\)://<host>:<port>/hostcheckPortal/checkingResult.jsp](http(s)://<host>:<port>/hostcheckPortal/checkingResult.jsp)

Configuring the Redirect Server to Redirect Traffic to the Captive Portal

You must configure the Redirect Server to redirect Web requests to the IVE sign-in page. For information about configuring the redirect server, see “Overview of the Residential Portal” on page 117.

In the `/opt/UMC/redir/etc/redir.properties` file, specify the URL of the IVE sign-in page for the `redir.url` property. This entry has the form:

`redir.url = http(s):// <IVE hostname> /check`

Configuring Services for Subscribers

You can configure services to control subscriber traffic in response to IVE Host Checker policy compliance by a subscriber’s machine.

To configure services to check hosts for subscribers:

1. Configure a policy to check hosts for a subscriber. For a host-checking policy, specify policy rules for subscribers to redirect the subscriber's HTTP traffic to the IVE Host Checker or to the captive portal.

For a sample policy that slows all subscriber traffic and forces all Web traffic to a redirect server with the specified address, which then redirects the traffic to the IVE Host Checker server, see *policyGroupName = hostcheck*, *ou = hostchecker*, *o = Policies*, *o = umc* in the sample data.

For a sample policy that slows all subscriber traffic and forces all Web traffic to a redirect server with the specified address, which then redirects the traffic to the Host Check Result portal, see *policyGroupName = block*, *ou = hostchecker*, *o = Policies*, *o = umc* in the sample data.

2. Create a scope for the services that define actions to be taken in response to IVE host-checking results.

For a sample scope, see *l = HC-Subscriber*, *o = Scopes*, *o = umc* in the sample data.

3. In the scope you created in Step 2, create a service that defines actions to be taken in response to the IVE host-checking results. Then set the type to normal, and specify the policy group configured in Step 1.

For a sample service that redirects traffic to the IVE Host Checker server, see *serviceName = HostCheck*, *l = HC-Subscriber*, *o = Scopes*, *o = umc* in the sample data.

For a sample service that redirects traffic to the Host Check Result portal, see *serviceName = Block*, *l = HC-Subscriber*, *o = Scopes*, *o = umc* in the sample data.

4. Assign the scope to a subscriber folder to make the service available to the subscribers.

For a retailer, specify any plug-ins that the subscribers in the domain might use, and specify a service that would be applied to subscribers who do not belong to a specific group of subscribers.

For a sample subscription that performs host checking for a retailer, see *retailermame = SP-HC*, *o = Users*, *o = umc* in the sample data.

5. Create service subscriptions for subscribers. To allow all subscribers in the folder to inherit the subscription, create a subscription at the folder level. For a subscriber, create any objects that might apply to the group of subscribers, such as service subscription, service schedule, or subscriber.

For a sample subscription that automatically performs host checking when the subscriber logs in, see *serviceName = HostCheck*, *ou = CheckOnLogin-Subscribers*, *retailermame = SP-HC*, *o = Users*, *o = umc* in the sample data.

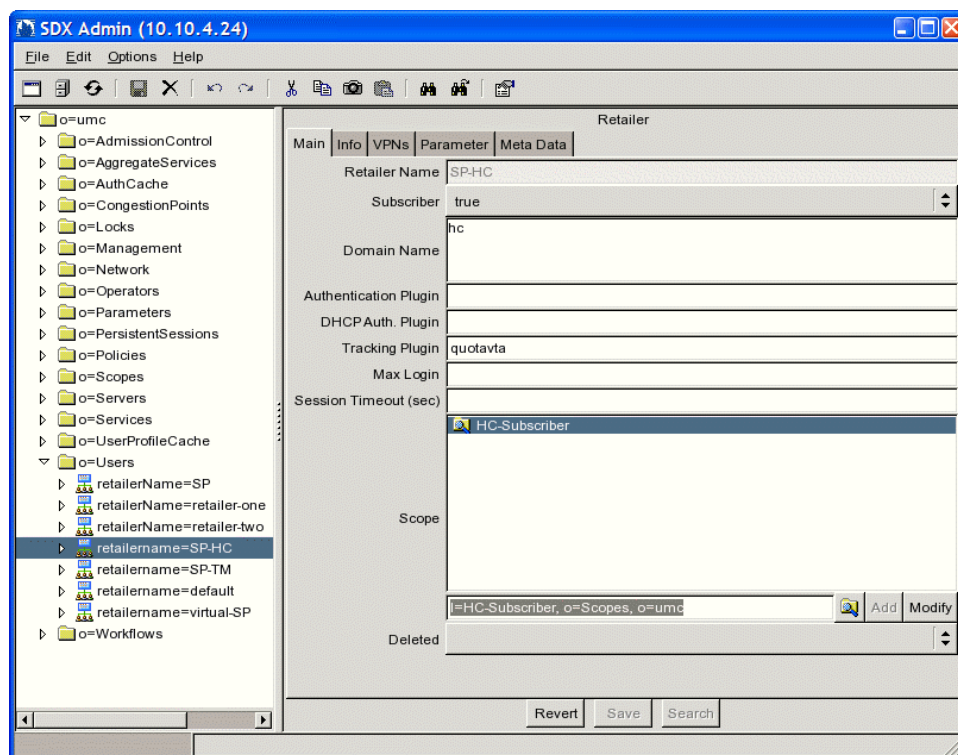
For a sample subscription that performs host checking that is activated according to a service schedule, see *serviceName = HostCheck*, *ou = CheckOnSchedule-Subscribers*, *retailermame = SP-HC*, *o = Users*, *o = umc* in the sample data.

For a sample subscription that performs host checking that is activated according to a Quota VTA plug-in, see *serviceName = HostCheck*, *ou = VTASched-Subscribers*, *retailername = SP-HC*, *o = Users*, *o = umc* in the sample data.

For a sample subscription that redirects all other subscribers for this retailer to the captive portal, see *serviceName = Block*, *retailername = SP-HC*, *o = Users*, *o = umc* in the sample data.

Figure 6 on page 38 shows the SDX Admin navigation pane with the retailer used in the sample data.

Figure 6: Sample Retailer Configuration for Host Checking



Scheduling Subscriber Host Checking

The SRC application library provides a Quota VTA configuration example as sample data for scheduling subscriber host checking. For information about developing Quota VTAs, see Overview of the SRC-VTA.

The HostCheck configuration example configures the Quota VTA to schedule subscriber host checking by setting the account balance as a date and activating a host-checking service based on subscriber login events. In SDX Admin, see *l = HostCheck*, *l = Applications*, *l = VTA*, *ou = staticConfiguration*, *ou = Configuration*, *o = Management*, *o = umc* for more information about this configuration example.

Part 3

Providing Threat Mitigation Services with IDP

- Overview of IDP Integration on page 41
- Configuring Services and Subscriptions to Integrate IDP on page 49
- Sending E-Mail to Subscribers on page 63
- Monitoring Subsets of Subscriber Traffic on page 71
- Defining Actions to Be Taken for Subscriber Traffic on page 81
- Enabling SRC Actions from IDP Manager on page 91

Chapter 4

Overview of IDP Integration

- Overview of IDP Integration on page 41
- Before You Integrate IDP into an SRC Environment on page 42
- Example: Integrating IDP into an SRC Environment on page 42
- Directing Subscriber Traffic to IDP for Monitoring on page 45
- Integrating IDP into an SRC Environment on page 47

Overview of IDP Integration

IDP monitors network traffic to detect potentially detrimental traffic and responds to problem incidents to prevent damage to the network. By integrating IDP into an SRC-managed environment, you can use SRC extensions that support IDP to:

- Monitor subscriber traffic.
- Take actions for subscribers who are sending or receiving traffic that behaves in a detrimental manner on the network by:
 - Redirecting a subscriber's Web requests to a Web page that provides information about the nature of the problem traffic
 - Sending e-mail to a subscriber to provide information about the problem
 - Applying policies to the subscriber interface to manage subscriber traffic, such as applying policies that reduce the amount of bandwidth available to the subscriber to limit traffic sent to and received from the subscriber

You can deploy IDP in a network to monitor all traffic, or you can configure the SRC software to direct subsets of subscriber traffic to IDP for monitoring.

The Surveillance Director is the component that manages the process of selecting subscriber traffic to be monitored and activating SRC services to direct specified traffic to an IDP sensor (IDP hardware appliances that run the IDP sensor software). It divides subscribers into groups, then directs traffic for one group at a time through IDP. This means that IDP monitors different groups of traffic at different times, and that traffic for SRC-managed subscribers is periodically monitored. The Surveillance Director relies on SRC services to policy-route traffic from JUNOSe routers or to mirror traffic from JUNOS routing platforms to the IDP sensor.

Before You Integrate IDP into an SRC Environment

Integrating IDP into an SRC-managed environment requires:

- The UMCidp package installed with your SRC application library software.
- SRC-managed JUNOS routers or SRC-managed JUNOS routers and JUNOS routing platforms in the network.



NOTE: If you want to integrate IDP into an SRC-managed network that manages enterprise subscribers from a JUNOS routing platform as a subscriber access router, contact Juniper Networks Professional Services for assistance.

- Subscriber IP addresses assigned from an IP pool that is defined in the virtual router entry in the directory

Typically, IP addresses are assigned from an IP pool for residential subscribers. For enterprise subscribers or for subscribers who use a static IP address, make sure that the IP addresses are allocated from the IP pool that is defined in the virtual router entry in the directory.

- Working knowledge of aggregate services.
- Working knowledge of the IDP software, including IDP Manager, and familiarity with IDP documentation. See

<http://www.juniper.net/techpubs/software/management/idp/>

Before you extend IDP traffic monitoring to SRC subscriber traffic, you typically:

- Install the IDP sensors. The sensors monitor network traffic to detect suspicious or anomalous traffic and respond as configured.
- We recommend that IDP sensors, or sensor clusters, be one hop from all the routers in the network for which the sensor monitors traffic. (Recommended) Deploy IDP as an active gateway. In instances in which traffic is copied to an IDP sensor, ensure that IDP routes the traffic to a null interface so that the traffic is not forwarded.
- Configure IDP rules for the type of traffic incidents to report.

Example: Integrating IDP into an SRC Environment

The SRC application library provides a robust sample implementation for integrating IDP into an SRC-managed network. It illustrates configurations for a network that contains only JUNOS routers, and for a network that contains JUNOS routers as subscriber access routers with JUNOS routing platforms as core routers.

You can also customize the sample data and applications to integrate IDP into your network, or you can use the samples as a guide to create your own implementation.

For a full configuration example, see the *IDP.xml* file in the SAE folder in SDX Configuration Editor.

Sample Network Topologies

Figure 7 on page 43 shows the network topology that serves as the basis for the configuration in the sample data for a network that contains only JUNOSe routers.

Figure 7: Sample Network Topology with a JUNOSe Router

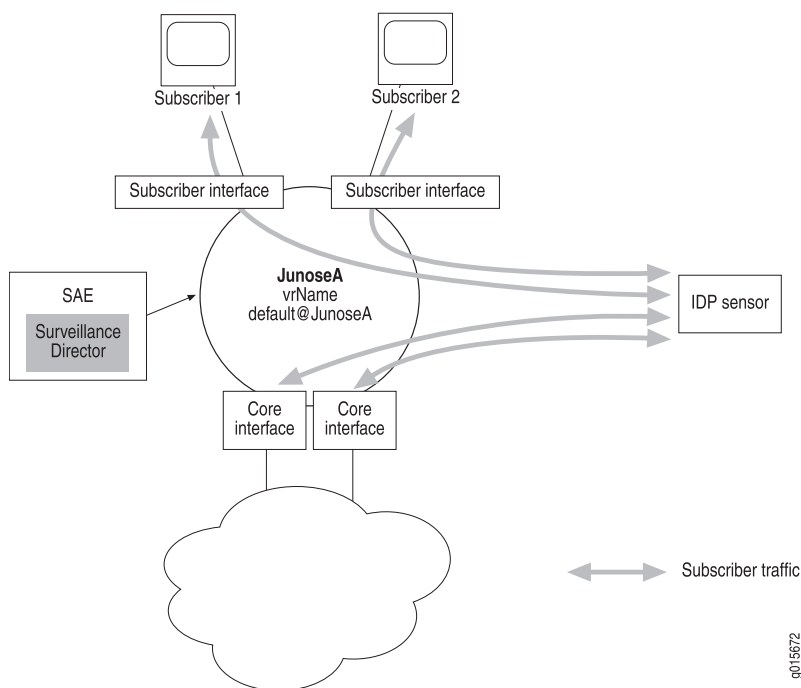
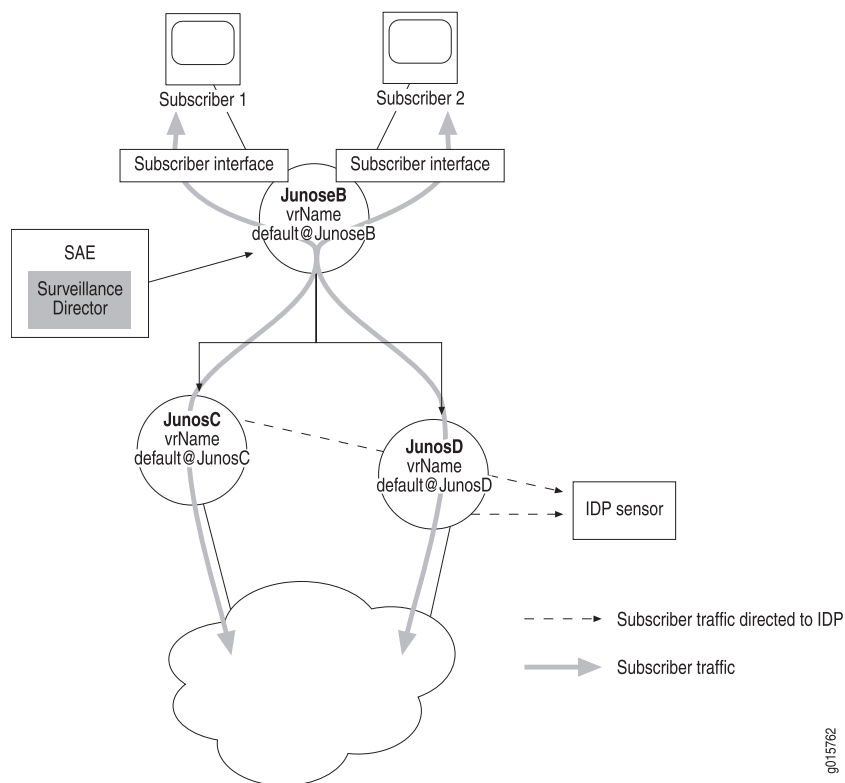


Figure 8 on page 44 shows the network topology that serves as the basis for the configuration in the sample data for a network that contains JUNOSe routers and JUNOS routing platforms.

Figure 8: Sample Network Topology with a JUNOS Router and JUNOS Routing Platforms

Components in Sample Data

The sample implementation includes:

- Policies, services, router definitions, and SAE configurations in the sample data. Sample entries for IDP integration have the prefix IDP

For information about installing sample data, see “Installing the Sample SRC Applications” on page 3.

- IDP captive portal application (a Web page that receives redirected HTTP requests in response to a problem detected by IDP) with policies and services to limit bandwidth and direct Web requests to the sample portal
- IDP E-Mailer application
- Script to enable subscriber actions from IDP Manager

You can use the sample data and applications to create a demonstration implementation. The IDP router definitions, identified as IDP <routername> in the sample data, can be configured to act as simulated routers for a demonstration environment. For information about setting up a simulated router, see Configuring Simulated Router Drivers (SRC CLI).

The sample data uses the following terminology:

- Subscriber-facing router—Subscriber access router
- Core-facing router—Router that transmits subscriber traffic to the network core

Directing Subscriber Traffic to IDP for Monitoring

You can direct all traffic to IDP by placing an IDP sensor in the network paths through which all incoming and outgoing subscriber traffic passes. In this case, you do not need to configure the SRC software to direct subscriber traffic to an IDP sensor.

If you do plan to direct subsets of subscriber traffic to an IDP sensor, how you do so depends on your network configuration. Table 7 on page 45 lists ways in which you route subscriber traffic to an IDP sensor.

Table 7: Network Configuration and Forwarding Method

For This Network Configuration	Use This Method to Forward Subscriber Traffic
JUNOSe routers as subscriber access routers	Policy-based routing from the JUNOSe router
No JUNOS routing platforms as core routers	
JUNOSe routers as subscriber access routers	Mirroring from the JUNOS routing platform
and	
JUNOS routing platforms as core routers	



NOTE: Use mirroring from JUNOS routing platform(s) if you are sure that most, or all, of the subscriber traffic traverses those routers. When you mirror traffic to IDP, IDP monitors only the subscriber traffic that traverses a JUNOS routing platform.

For policy-based routing from JUNOSe routers, a service is activated on subscriber interfaces for each subscriber IP address, and on each core interface. For mirroring on JUNOS routing platforms, a service is activated only one time for a router or for a set of routers. If your configuration includes a JUNOS routing platform, we recommend that you use mirroring to direct subscriber traffic to IDP.

Surveillance Director

The Surveillance Director manages how to direct subscriber traffic to an IDP sensor. It queries the directory for IP pools associated with specified virtual routers and generates classless interdomain routing (CIDR) subnets that include only the set of IP addresses that are assigned to subscribers. You can configure the number of IP addresses to be included in a CIDR subnet. The Surveillance Director uses CIDR subnets because routers can efficiently handle these subnets to match policy rules.

For each CIDR subnet, the Surveillance Director activates a specified aggregate service, and then the aggregate service activates its fragment services to route traffic to an IDP sensor. The configuration for the fragment services determines whether it policy-routes or mirrors traffic.

Table 8 on page 46 describes the types of fragment services to configure in an aggregate service, and shows where the fragment services are activated.

Table 8: Types of Fragment Services in an Aggregate Service

Fragment Services	Policy	Where Fragment Service Is Activated
Policy-Based Routing		
Subscriber-interface fragment	Routes traffic sent by a subscriber to an IDP sensor	JUNOSe routers
Core-interface fragment	Routes traffic destined for a subscriber to an IDP sensor	JUNOSe routers
Mirroring		
Router (forwarding)-interface fragment	Mirrors traffic to an IDP sensor	JUNOS routing platforms that transmit subscriber traffic

Traffic for one group of CIDR subnets at a time is sent to an IDP sensor for monitoring. You can configure the length of the interval during which to monitor traffic from CIDR subnet; all traffic for subscribers with IP addresses within the CIDR subnet is monitored during a specified monitoring interval.

The Surveillance Director provides subscriber IDs in the form of a distinguished name (DN) to locate the subscriber session in which to activate a service. The DN is used to locate the SAE that manages the subscriber session in which the aggregate service is activated.

Router and Interface Subscriber Sessions

In addition to the typical subscriber sessions used to activate services, the services to support IDP integration require special subscriber sessions to host:

- An aggregate service
- Core interface fragment services if traffic is policy-routed to an IDP sensor
- Router fragment services if traffic is mirrored to an IDP sensor

Subscriber Session to Host an Aggregate Service

On a JUNOSe router, a router subscriber session hosts an aggregate service. In these cases, a subscriber profile must have a name in the form `<vrName> @ <routerName>`. The `<vrName>` and `<routerName>` must

correspond to virtual router names and routers names of objects under *o = Networks*, *o = umc* in the directory.

Subscriber Session to Host a Core Interface Fragment Service

On a JUNOS router, a subscriber session is needed to activate a core interface fragment service that policy-routes traffic to the IDP sensor. All core routing interfaces use a single shared subscriber object in the directory.

Subscriber Session to Host a Router Interface Fragment Service

On a JUNOS routing platform, a router subscriber session is used to activate the fragment service that mirrors traffic to the IDP sensor. We recommend that the router subscriber profile have a name in the form `<vrName> @ <routerName>`. The router subscriber session must be associated with the forwarding interface that the SRC software creates.

Integrating IDP into an SRC Environment

How you integrate IDP into your SRC environment depends on whether or not you direct all traffic to an IDP sensor. If you direct all traffic to an IDP sensor by placing an IDP sensor in the network paths through which all incoming and outgoing subscriber traffic passes, you do not need to configure services and subscriptions to director traffic to a sensor, and do not need to monitor subsets of traffic. In this case, you can skip Steps 1 and 2 in the following procedure.

To integrate IDP into an SRC environment:

1. Configure services to direct traffic to IDP.

See “Configuring Services and Subscriptions to Integrate IDP” on page 49.
2. Configure Surveillance Director to monitor groups of subscriber traffic.

See “Monitoring Subsets of Subscriber Traffic” on page 71.
3. Configure actions to be taken for traffic that IDP identifies as malicious.

See “Defining Actions to Be Taken for Subscriber Traffic” on page 81.
4. (Optional) Create an application, such as one to send e-mail notification to a subscriber about problem traffic that have sent or received.

We provide a sample application to send an e-mail notification to a subscriber about the problem. See “Sending E-Mail to Subscribers” on page 63.

5. Create an SRC script for IDP Manager to complete the IDP integration with the SRC software.

See “Enabling SRC Actions from IDP Manager” on page 91 .

Chapter 5

Configuring Services and Subscriptions to Integrate IDP

This chapter describes how to configure services and how to configure user classification and interface classification to redirect subscriber traffic to IDP. Topics include:

- Configuring Services and Subscriptions to Send Traffic to an IDP Sensor on page 49
- Configuring Services to Policy-Route Traffic to IDP on page 50
- Configuring Services to Mirror Traffic to IDP on page 55
- Subscribing to an Aggregate Service from a JUNOS Router on page 59
- Classifying Subscribers for IDP Integration on page 60
- Classifying Interfaces for IDP Integration on page 61

Configuring Services and Subscriptions to Send Traffic to an IDP Sensor

Which tasks you perform to create services and subscriptions depends on whether you are sending traffic to an IDP sensor by policy-based routing or mirroring.

To configure services and subscriptions to integrate IDP into an SRC-managed environment:

1. Configure services.

See “Configuring Services to Policy-Route Traffic to IDP” on page 50 or “Configuring Services to Mirror Traffic to IDP” on page 55.

2. Create a subscription to the aggregate service configured in Step 1.

See “Subscribing to an Aggregate Service from a JUNOS Router” on page 59.

3. Classify subscribers.

See “Classifying Subscribers for IDP Integration” on page 60.

4. Classify interfaces.

See “Classifying Interfaces for IDP Integration” on page 61.

Configuring Services to Policy-Route Traffic to IDP

The tasks to configure services to policy-route traffic to IDP are:

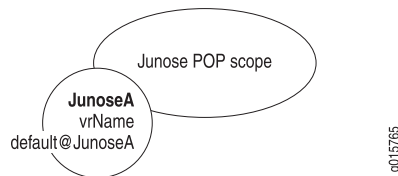
1. (Optional) “Configuring Scopes When You Use Policy-Based Routing” on page 50
2. “Defining Services for Policy-Based Routing on JUNOSe Routers” on page 50

Configuring Scopes When You Use Policy-Based Routing

You configure scopes to define the services to be activated for a specific SRC-managed network. Which scopes you configure depends on how you direct traffic to an IDP sensor.

In a network that contains only JUNOSe routers, you can assign a single scope to one or more JUNOSe routers. Figure 9 on page 50 shows the scope and JUNOSe router configured in the sample data. This scope also contains the aggregate and fragment services.

Figure 9: Scopes to Support Policy-Based Routing of Traffic to an IDP Sensor



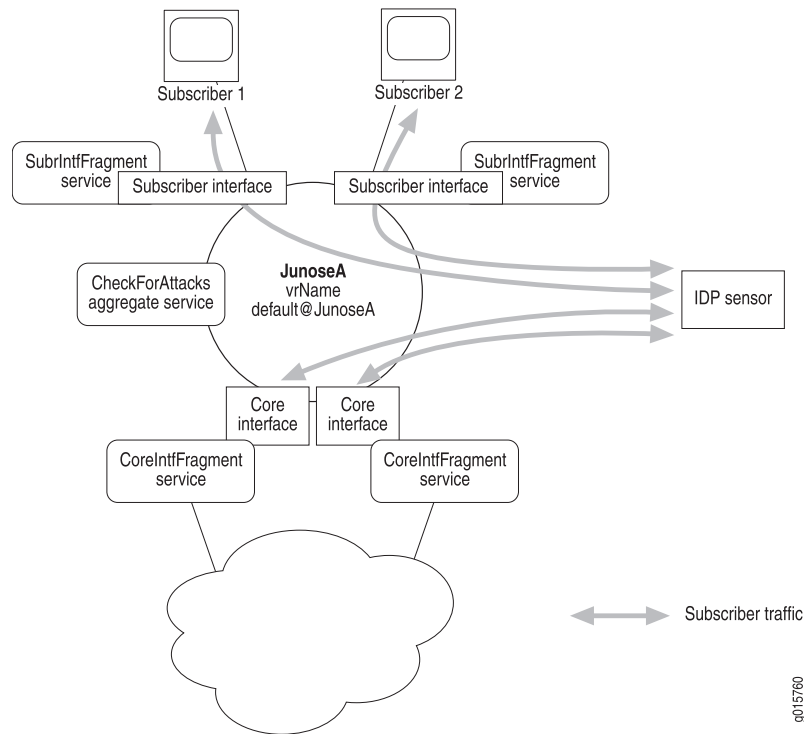
To policy-route traffic from a JUNOSe router to an IDP sensor:

1. Create one JUNOSe point of presence (POP) scope.
2. Assign this scope to all the JUNOSe subscriber access routers that use policy routing. Make sure that these routers appear under *o = Networks*, *o = umc* in the directory. You create the aggregate services in this scope.

For a sample JUNOSe POP scope, see *l = IDP-JunosePop*, *o = Scopes*, *o = umc* in the sample data.

Defining Services for Policy-Based Routing on JUNOSe Routers

Figure 10 on page 51 illustrates the services in the sample data that policy-route incoming and outgoing subscriber traffic to an IDP sensor. In this example this DN for subscriber profiles is routerName = default@JunoseA, < DN of Router Profiles > .

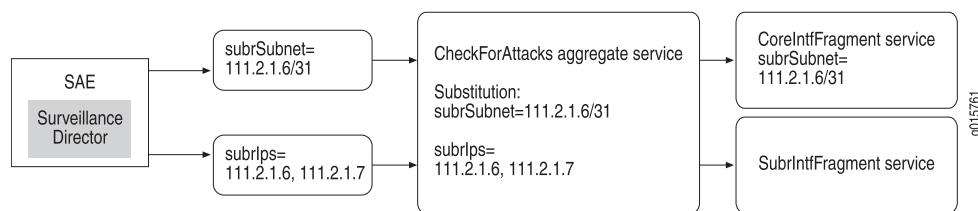
Figure 10: Services to Policy-Route Traffic to an IDP Sensor

The Surveillance Director provides the following information to the services:

- **subrSubnet**—CIDR subnet. Core interface fragments are activated with this parameter.
- **subrIps**—List of addresses. A subscriber interface service fragment is created for each address supplied by the parameter.

The aggregate service passes the value of the **subrSubnet** parameter to each **CoreIntfFragment** service, and uses the value of the **subrIps** parameter when the **SubrIntfFragment** services are created. A **SubrIntfFragment** service is created for each IP address (which is specified as the subscriber ID). A **CoreIntfFragment** service is created for the subscriber ID or IDs specified in the configuration for the aggregate service (**idp@idp** in the sample data).

For example, in Figure 11 on page 52 the Surveillance Director passes the value **111.2.1.6/31** for the CIDR subnet, and the list of addresses **111.2.1.6** and **111.2.1.7** to the aggregate service. The aggregate service passes the value for the CIDR subnet to the **CoreIntfFragment** service, and activates a **SubrIntfFragment** service for each address in the list—in this case for IP addresses **111.2.1.6** and **111.2.1.7**.

Figure 11: Sample Values for SubrSubnet and Subrlps Parameters in Services for Policy-Based Routing of Traffic

To set up policy-based routing to direct subscriber traffic from a JUNOSe router to IDP:

- Configure the following services:
 - A service that applies a policy to route traffic from the subscriber interfaces. The Surveillance Director activates this service once for each subscriber whose IP address is in the CIDR subnet that includes the addresses being monitored.

Configuring a Subscriber Interface Service

Before you configure a subscriber interface service, read the overview of services to be used for policy-based routing. See “Defining Services for Policy-Based Routing on JUNOSe Routers” on page 50 .

To configure the subscriber interface service:

1. Configure a policy to direct subscriber traffic entering a subscriber interface to an IDP sensor.

We recommend that you use a next-hop policy rule to route traffic sent by subscribers to the IP address of the IDP sensor. Depending on your network configuration you can also route traffic to a system interface that then routes traffic to the IDP sensor, or you can specify a substitution to indicate the IP address of the IDP sensor.

For a sample policy group see *policyGroupName = policyRouteSubscriberToIdp*, *ou = idp*, *o = Policies*, *o = umc* in the sample data.

2. In SDX Admin in the JUNOSe scope, create a service, set the type to normal, and specify the policy group configured in Step 1 .

For a sample subscriber interface service, see *serviceName = SubrIntfFragment*, *o = IDP-junosePop*, *o = Scopes*, *o = umc* in the sample data.

Configuring a Core Interface Service

Before you configure a core interface service, read the overview of services to be used for policy-based routing. See “Defining Services for Policy-Based Routing on JUNOSe Routers” on page 50 .

To configure the core interface service:

1. Configure policies to direct the traffic destined for subscribers to an IDP sensor.

We recommend that you use a next-hop policy to route traffic sent to subscribers to the IP address of the IDP sensor. The policy must be applied to each ingress interface that might transmit traffic destined for a subscriber.

A core interface policy requires that the subscriber CIDR subnet be available from a substitution. You can use the `subrSubnet` substitution in policies that are applied to all core interfaces.

For a sample core interface policy, see *policyGroupName = policyRouteSubnetToIdp, ou = idp, o = Policies, o = umc* in the sample data.

2. In SDX Admin in the JUNOSe scope, create a service, set the type to normal, and specify the policy group configured in Step 1.

For a sample core interface service, see *serviceName = CoreIntfFragment, o = IDP-junosePop, o = Scopes, o = umc* in the sample data.

Configuring an Aggregate Service

Before you configure an aggregate service, read the overview of services to be used for policy-based routing. See “Defining Services for Policy-Based Routing on JUNOSe Routers” on page 50 .

You configure an aggregate service to include the subscriber interface service and the core interface service as fragment services.

To configure an aggregate service:

1. In SDX Admin in the JUNOSe scope, create an aggregate service.
2. Add the subscriber interface service as a fragment service, and in the Fragment Service dialog box specify:

- Expression—A subscriber reference expression written in Python to supply a list of IP addresses, such as:

```
address = “ <- substitution.subrIps ->”
```

where `subrIps` is a parameter that provides a list of subscriber IP addresses.

This expression causes one subscriber interface fragment service to be activated for each subscriber whose address appears in the list.

- Service—Name of a subscriber interface service.
- Mandatory—False.

When set to false, the service is activated even if some of the subscribers for some of the addresses are offline. If set to true, the aggregate service is not activated when some of the addresses are not in use.

- Redundancy Group—Name of a group of services that provide redundancy.

We recommend that you configure a redundant service. By configuring a redundancy group, the Surveillance Director can move through the groups of addresses more rapidly. When you configure a group, at least one of the fragments must become active for the aggregate service to become active. If none of the subscribers for the addresses is online when the aggregate service is being activated, activation of the aggregate service fails, and the Surveillance Director skips to the next group of addresses.

- Subscription—False.
- Substitution—idpAddress. Specifies the IP address of an IDP sensor. The sample data defines the value for the idpAddress substitution in the service. You can use this strategy if an IDP sensor or cluster of sensors has a single IP address. If you use more than one IDP sensor that have different IP addresses, define the value of the idpAddress substitution in a scope, one scope for each IDP sensor, and assign the scope for an IDP sensor to the routers that use that sensor.

3. Add the core interface service as a fragment service, and in the Fragment Service dialog box specify:

- Expression—A subscriber reference expression written in Python to supply the virtual router name and the login name used to identify subscriber sessions in which to activate the core fragment service. For example:

```
vr = "<- virtualRouterName ->" , login_name = " idp@idp"
```

The expression specifies a set of core interfaces on the same virtual router as the aggregate service.

The loginName that you use in this expression must be the same as the login name configured in the subscriber classification script for the core interfaces. For information about configuring the login name, see “Classifying Subscribers for IDP Integration” on page 60 .

- Service—Name of a core interface service.
- Mandatory—False.

When set to false, the service is activated even if some of core interfaces are down. If set to true, the aggregate service is not activated when some of the core interfaces are down.

- Redundancy Group—Name of a group of services that provide redundancy.

We recommend that you configure a redundant service. By configuring a redundancy group, the Surveillance Director can move through the groups of addresses more rapidly. When you configure a group, at least one of the fragments must become active for the aggregate service to become active. If none of the core interfaces is up when the aggregate service is being activated, activation of the aggregate service fails, and the Surveillance Director skips to the next group of addresses.

- Subscription—False.
- Substitutions:

- **idpAddress**—Specifies the IP address of the IDP sensor

The sample data defines the value of the **idpAddress** substitution in the service. You can use this strategy if an IDP sensor or cluster of sensors has a single IP address. If you use more than one IDP sensor that have different IP addresses, define the value of the **idpAddress** substitution in a scope, one scope for each IDP sensor, and assign the scope for an IDP sensor to the routers that use that sensor.

- **subrSubnet**—Specifies the addresses provided by the Surveillance Director

The **subrSubnet** parameter specifies a CIDR-specified subnet. The core interface fragment service uses the **subrSubnet** parameter in policies that are applied to each core interface.

For a sample aggregate service, see *serviceName = CheckForAttacks, o = IDP-JunosePop, o = Scopes, o = umc* in the sample data.

Configuring Services to Mirror Traffic to IDP

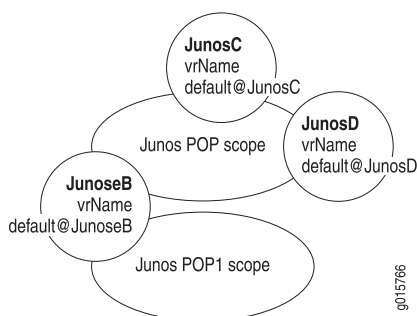
The tasks to configure services to policy-route traffic to IDP are:

1. (Optional) “Configuring Scopes When Mirroring Traffic” on page 55
2. “Defining Services for Mirroring on JUNOS Routing Platforms” on page 56

Configuring Scopes When Mirroring Traffic

You configure scopes to define the services to be activated for a specific SRC-managed network. Which scopes you configure depends on how you direct traffic to an IDP sensor.

In a network that contains both JUNOSe routers and JUNOS routing platforms, you can assign a single scope to all routers, and a second scope to only JUNOS routing platforms. Figure 12 on page 56 shows the scopes and routers configured in the sample data. The Junos POP scope contains the aggregate and fragment services. The Junos POP1 scope defines the list of JUNOS routing platforms that provide the mirroring service for the subscriber access router.

Figure 12: Scopes to Support Mirroring Traffic to an IDP Sensor

To mirror traffic from a JUNOS routing platform to an IDP sensor:

1. Create a general JUNOS POP scope.
2. Assign the scope to the virtual routers on the JUNOSE subscriber access router and the JUNOS routing platforms. Make sure that these routers appear under *o = Networks*, *o = umc* in the directory. You create the aggregate service in this scope.

For a sample scope for JUNOS routing platforms, see *l = IDP-JunosPop*, *o = Scopes*, *o = umc* in the sample data.

3. Create a network-specific JUNOS scope that is associated with the general JUNOS scope for each specific POP.

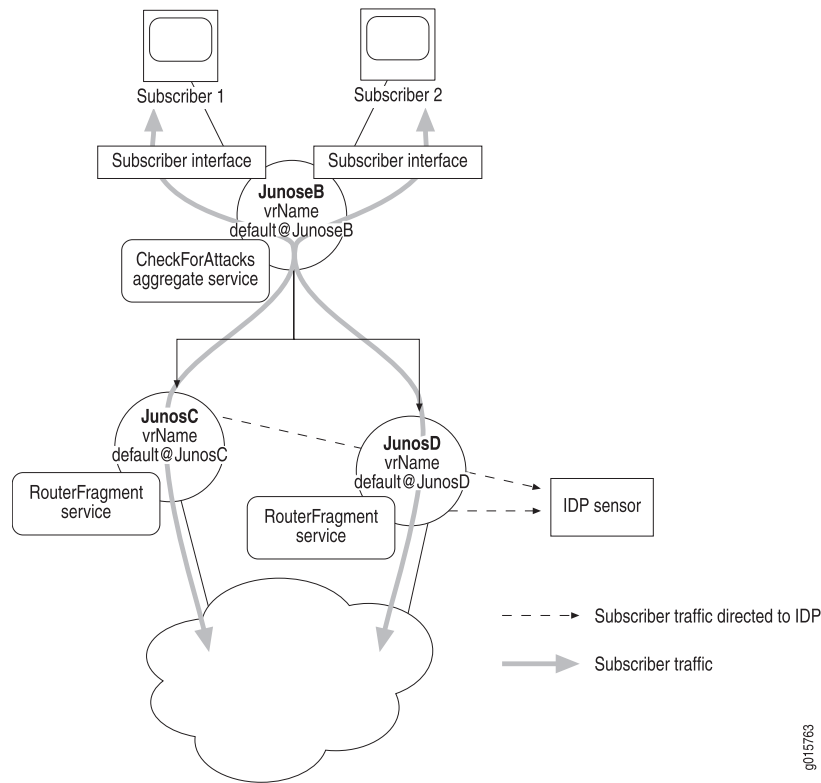
To show the relationship between the two types of JUNOS scopes, we recommend that you incorporate the name of the general JUNOS scope into the name of the network-specific scope. For example, if the name of the general JUNOS scope is *JunosPop*, then the names of network-specific scopes are *JunosPop1*, *JunosPop2*, and so on.

A network-specific scope must contain a parameter that lists the names of the JUNOS routers in the JUNOS POP. By using this list, the SRC software activates the services in the JUNOS scope for each router listed.

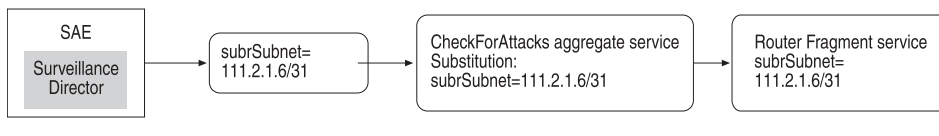
For an example of a network-specific scope, see *l = IDP-JunosPop1*, *o = Scopes*, *o = umc* in the sample data.

Defining Services for Mirroring on JUNOS Routing Platforms

Figure 13 on page 57 illustrates the services in the sample data that mirror subscriber traffic from JUNOS routing platforms to an IDP sensor and shows the routers on which the services are activated. In this example, the DN for subscriber profiles is *routerName = default@JunoseB*, < DN of Router Profiles > .

Figure 13: Services to Mirror Traffic to an IDP Sensor

The Surveillance Director passes the value for the subSubnet parameter to the aggregate service; the aggregate service then passes the value of the parameter to the router fragment services. For example, in Figure 14 on page 57 the Surveillance Director passes value 111.2.1.6/31 for the CIDR subnet, to the aggregate service. The aggregate service passes the value for the CIDR subnet to the router fragment services.

Figure 14: Sample Values for SubSubnet Parameter in Services for Mirroring

Before you configure services to mirror subscriber traffic to an IDP sensor:

- Make sure that the configuration on the JUNOS routing platform:
 - Specifies which ports to use for mirroring
 - Has a forwarding interface configured

SRC service policies specify which traffic to mirror; the router configuration specifies how to implement mirroring on that system. For information about port mirroring on a JUNOS routing platform, see the JUNOS documentation at

<http://www.juniper.net/techpubs/software/junos/junos71/index.html>

- Read the overview of services to be used to mirror traffic to an IDP sensor. See “Defining Services for Mirroring on JUNOS Routing Platforms” on page 56 .

To configure services to mirror subscriber traffic to an IDP sensor:

1. Configure a policy to mirror traffic for a set of subscribers (selected by Surveillance Director) to the IDP sensor. The subSubnet parameter (for a specified CIDR subnet) includes the source IP addresses designated for traffic sent by these subscribers.

For a mirroring policy, you specify policy rules for traffic sent to and received from the subscriber subnet (the value of the subSubnet parameter) that have the action Port Mirror.

For a sample policy that implements mirroring, see *policyGroupName = mirrorToIdp, ou = idp, o = Policies, o = umc* in the sample data.

2. Create a service, which is a router fragment service in this configuration; set the type to normal; and specify the policy group configured in Step 1. This service is activated once for each JUNOS routing platform in a specified POP.

For a sample service, see *servicename = RouterFragment, l = IDP-JunosPop, o = Scopes, o = umc* in the sample data.

3. Create an aggregate service; add the service configured in Step 2 to the aggregate service; and in the Service Fragment dialog box specify:
 - Expression—A subscriber reference expression to specify the vrNames substitution and the interface name used to activate the service. For example:

```
vr = “ <- substitution.vrNames ->” , interfaceName = “
    FORWARDING_INTERFACE”
```

where FORWARDING_INTERFACE is used to activate the fragment service for the forwarding table. The vrNames substitution must be defined in each separate POP-specific scope.

For the configuration shown in Figure 13 on page 57, the substitution would be:

```
vrNames=[“ default@JunosC” , “ default@JunosD” ]
```

as defined in the JUNOS POP1 scope.

- Mandatory—Set the value to false if you want the traffic to be redirected to the IDP sensor even if some of the core routers are down.
- Redundancy Group—Name of a group of services that provide redundancy.

We recommend that you configure a redundant service. By configuring a redundancy group, the Surveillance Director can move through the groups of addresses more rapidly. When you configure a group, at least one of the fragments must become active for the aggregate service to become active. If none of the core routers is up for the subscriber addresses when the

aggregate service is being activated, activation of the aggregate service fails, and the Surveillance Director skips to the next group of addresses.

- Subscription—False.
- Substitution—subrSubnet specifies the list of addresses provided by the Surveillance Director.

For a sample aggregate service, see *serviceName = CheckForAttacks*, *l = IDP-JunosPop*, *o = Scopes*, *o = umc* in the sample data.

Subscribing to an Aggregate Service from a JUNOSe Router

You subscribe to an aggregate service that policy-routes traffic or one that mirrors traffic to an IDP sensor from a JUNOSe router.

To create a subscription to an aggregate service:

1. In SDX Admin, under Users select a retailer, and then create a subscriber folder for router subscribers.
2. In the folder for router subscribers, create a router subscriber for each router.

For sample router subscriptions, see *ou = routers*, *retailername = SP-IDP*, *o = Users*, *o = umc* in the sample data.

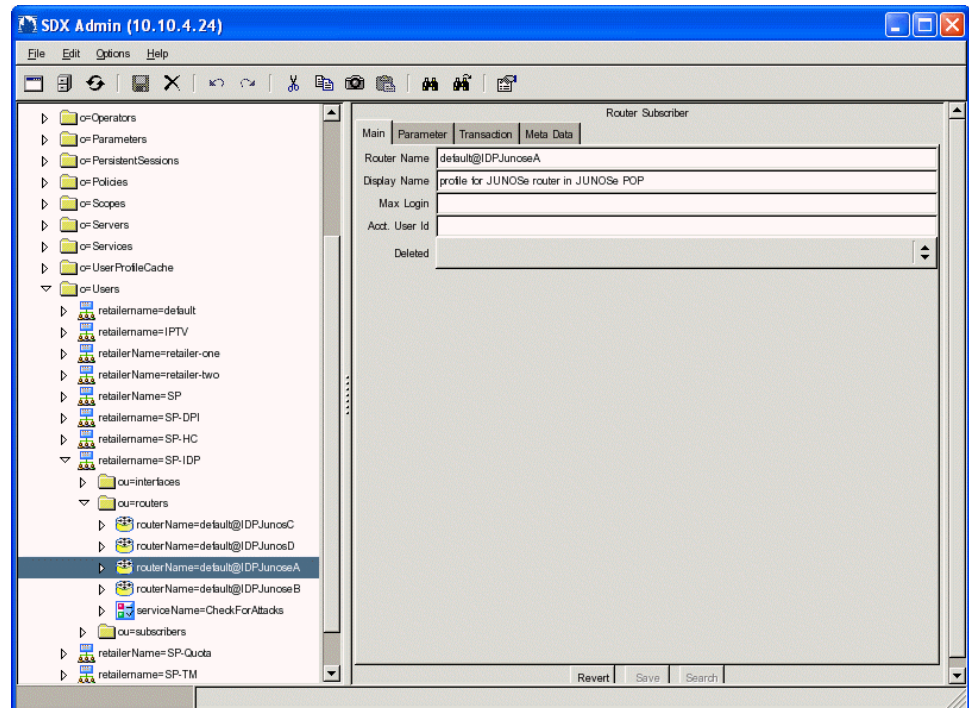
3. Create a subscription to an aggregate service in the folder that includes the router subscribers.

For the sample service *CheckForAttacks*, to which router subscribers subscribe, see *serviceName = CheckForAttacks*, *ou = routers*, *retailername = SP-IDP*, *o = Users*, *o = umc* in the sample data.

4. For policy-based routing to an IDP sensor from a JUNOSe router:
 - a. Under the retailer, create a subscriber folder for the core interfaces.
 - b. In the interfaces folder, create one subscriber that is shared by all JUNOSe interfaces that transmit traffic to the network core.

See *routerName = idp*, *ou = interfaces*, *retailerName = SP-IDP*, *o=Users*, *o = umc* in the sample data.

Figure 15 on page 60 shows the SDX Admin navigation pane with the router and interface subscribers included in the sample data.

Figure 15: Router and Interface Subscriptions for JUNOSe Routers

Classifying Subscribers for IDP Integration

You configure additional entries in the subscriber classification script to support services for IDP integration.

To add entries to a subscriber classification script to support IDP integration:

1. Add an entry to host aggregate service on JUNOSe routers.
2. (Policy-based routing) Add an entry to host a core interface fragment service for policy-based routing traffic on a JUNOSe router.
3. (Mirroring) Add an entry to host a router fragment service for mirroring traffic on a JUNOS routing platform.

To view the sample subscriber classifications referenced in this section, see *l = IDP*, *l = SAE*, *ou = staticConfiguration*, *ou = Configuration*, *o = Management*, *o = umc* in the sample data.

Example: Router Subscriber Session to Host an Aggregate Service

For JUNOSe routers the subscriber classification script must assign a subscriber profile to the router interface. For example:

```
[ou=routers,retailname=SP-IDP,o=Users,o=UMC??sub?(routerName=<-virtualRouterName->)]
# host subscriber for JUNOSe routers
interfaceName=="Router"
```

Example: Interface Subscriber Session to Policy-Route Traffic to IDP

For JUNOSe routers the subscriber classification script must also assign a shared subscriber profile and a login name to a subscriber session when a core interface service is activated. The following example assigns a login name and IP address for the subscriber session to an interface that has core specified as the ifAlias (as configured on the JUNOSe router).

```
[routerName=idp,ou=interfaces,retailname=SP-IDP,o=Users,o=UMC
?loginName=idp@idp]
# core facing interfaces on JUNOSe routers in JUNOSe POPs
ifAlias=="core"
```

The login name specified in this classification must be the same as the value set in the subscriber reference expression for the core interface fragment service in the aggregate service. The interface alias must be the same as the one specified in the interface classification script.

Example: Router Subscriber Session to Mirror Traffic to IDP

For JUNOS routing platforms, the subscriber classification script must assign subscriber profiles for the forwarding interface. For example:

```
[ou=routers,retailname=SP-IDP,o=Users,o=UMC??sub?(routerName=
<-virtualRouterName->)]
# host subscriber for JUNOS routers
interfaceName=="FORWARDING_INTERFACE"
```

For general information about classifying subscribers, see Overview of Classification Scripts .

Classifying Interfaces for IDP Integration

You configure additional entries in the interface classification script to support services for IDP integration.

To add entries to an interface classification script to support IDP integration:

1. For core interfaces on JUNOSe routers, add an entry to host aggregate service on JUNOSe routers. identify which interfaces to assign a core routing fragment service by specifying an alias for the group of interfaces.
2. For the forwarding interface on a JUNOS routing platform, add an entry for the default policy for forwarding interfaces. The policy must forward all traffic; otherwise, only traffic mirrored to IDP is forwarded.

To view the sample interface classifications referenced in this section, see the interface classification for the IDP < routername > routers listed under *o = Network*, *o = umc* in the sample data.

Example: Interface Classification for Core Interfaces on a JUNOS Router

You identify which interfaces to assign a core routing fragment service by specifying an alias for the group of interfaces. For example:

```
# ifAlias=="core" Add a line similar to this one if policy-based routing is being used.
# This alias needs to be the same as the one defined in the subscriber classification
  script.
# Could add some further rules to manage DHCP subscribers.
```

You do not define a classification for the router interface. The SAE automatically creates a router interface and a subscriber session for it when the COPS-PR or COPS XDR router drivers are in use.

Example: Interface Classification for the Forwarding Interface on a JUNOS Routing Platform

For JUNOS routing platforms, the default policy for forwarding interfaces must forward all traffic; otherwise, only traffic mirrored to IDP is forwarded. For example:

```
policyGroupName=forwardIntfDefault,ou=idp,o=Policies,o=UMC
# manage only forwarding interface on JUNOS routers
interfaceName=="FORWARDING_INTERFACE"
```

For general information about classifying interfaces, see Overview of Classification Scripts .

Chapter 6

Sending E-Mail to Subscribers

- Overview of IDP E-Mailer on page 63
- Configuring Deployment Properties for IDP E-Mailer on page 64
- Configuring Application Properties for IDP E-Mailer on page 65
- Deploying IDP E-Mailer on page 70

Overview of IDP E-Mailer

You can also manage subscribers who have sent or received problem traffic by sending them an e-mail message that gives them information about the problem detected. The SRC application library provides a demonstration application, named IDP E-Mailer, that uses the gateway extension feature for Dynamic Service Activator to send e-mail notifications to subscribers. For information about developing gateway clients that use the gateway extension, see Overview of the Web Services Gateway.

The SRC software lets you map an IP address, which IDP identifies to be associated with problem traffic, to a subscriber so that a message can be sent to the subscriber. In the sample application, you specify a domain to append to subscriber names to formulate an e-mail address. In a production implementation, you could integrate information from a customer database to gain access to actual e-mail addresses. You can use the sample IDP E-Mailer as a basis for an application specific to your environment.

The *idpemail.war* file comprises the files for the IDP E-Mailer servlet. You can locate this file on the SRC application library CD in the */webapp* directory. You can deploy the file as it is as a demonstration application, or you can customize the files in the WAR file. The SRC application library supplies complete source code for the IDP E-Mailer servlet in the *WEB-INF/src* directory in the *idpemail.war* file.

How IDP E-Mailer Responds to Incidents Reported by IDP

When an incident activates the IDP E-Mailer application for a subscriber, the following arguments are provided to the application in the following order:

1. Source of the incident
2. Destination of the incident
3. Description of the incident

The application uses this information when it creates the e-mail message.

The demonstration IDP E-Mailer application is a servlet that maps a subscriber's IP address (for addresses identified as the source or destination of detrimental traffic) to an e-mail address and then sends e-mail to the designated subscriber in the following manner:

1. Uses NIC to locate the SAE that manages the specified IP address.
2. Uses the SAE CORBA remote API to obtain the subscriber session for the IP address.
3. If the subscriber session is active, obtains the login name associated with the subscriber session.
4. Creates the e-mail address by appending a domain name that is specified in the IDP E-Mailer configuration to the subscriber login name. For example, for a domain specified as mycompany.com, and a subscriber login of ChrisB, the e-mail address would be ChrisB@mycompany.com.
5. Creates a message that includes the text received from IDP that specifies the IP address of the source of the detrimental traffic received, or the destination of the detrimental traffic being sent, and a description of the incident.
6. Sends the message.

The configuration for IDP E-Mailer specifies:

- Text to appear on the subject line of the e-mail
- Introductory text to appear in the body of an e-mail message for detrimental traffic sent by the subscriber
- Introductory text to appear in the body of an e-mail message for detrimental traffic sent to the subscriber

Configuring Deployment Properties for IDP E-Mailer

The configuration for the application specifies that the directory server resides on the local system. If the directory server resides on another system, edit the *WEB-INF/bootstrap.properties* file.

To customize files and properties for the IDP E-Mailer application:

1. Copy the *idpemail.war* file to a temporary folder, and work in that folder.
2. Extract the *bootstrap.properties* file from the *idpemail.war* file.

jar xvf idpemail.war WEB-INF/bootstrap.properties

3. (Optional) With a text editor, edit the *WEB-INF/bootstrap.properties* file.

The file provides the default local directory location. To change the location of the directory server, edit the *Config.java.naming.provider.url* property.

4. Replace the *WEB-INF/bootstrap.properties* file and any other updated files in the *idpemail.war* file. To replace the *WEB-INF/bootstrap.properties* file, enter:

jar uvf idpemail.war WEB-INF/bootstrap.properties

Configuring Application Properties for IDP E-Mailer

You configure the IDP E-Mailer application as you would other gateway applications, including configuration for Dynamic Service Activator and logging. For information about configuring a gateway client, see Overview of the Web Services Gateway.

The *idpEmailer.xml* file provides the configuration properties for the IDP E-Mailer application. You can use the template file *idpEmailer.conf* to create other configuration files for IDP E-Mailer.

Tasks to configure properties for IDP E-Mailer are:

- “Configuring General Properties for IDP E-Mailer” on page 65.
- “Configuring a NIC Proxy for IDP E-Mailer” on page 66
- “Configuring Logging for IDP E-Mailer” on page 67
- “Configuring E-Mail Properties for IDP E-Mailer” on page 67

Configuring General Properties for IDP E-Mailer

The general properties for IDP E-Mailer specify the configuration namespaces used by parts of the application.


To use SDX Configuration Editor to configure general properties for IDP E-Mailer:


1. In the navigation pane, select the *IdpEmailer.xml* configuration file.
2. Select the **IDP E-Mailer** tab.

The IDP E-Mailer pane appears.

IDP E-Mailer

Logging Subsystem Configuration Namespace

NIC Proxy Configuration Namespace for IP Subscriber 

E-Mail Configuration Namespace for IDP E-Mailer 

3. In the IDP E-Mailer section, edit or accept the default values.

See “IDP E-Mailer Fields” on page 66 .

4. Select **File > Save**.
5. Right-click the configuration file, select **SDX System Configuration > Export to LDAP Directory**.

IDP E-Mailer Fields

In SDX Configuration Editor, you can modify the following fields in the IDP E-Mailer pane in an *IdpEmailer.xml* configuration file.

Logging Subsystem Configuration Namespace

- Namespace that defines the properties for the logging operations.
- Value—Path, relative to the static configuration DN, that defines the object for the namespace
- Default—*/WebApplication*
- Property name—*loggingNamespace*

NIC Proxy Configuration Namespace for IP Subscriber

- Namespace that defines the properties for the NIC proxy operations.
- Value—Path, relative to the static configuration DN, that defines the object for the namespace
- Default—*/WebApplication/IdpEmailer/nicProxyIp*
- Property name—*nicProxyIpNamespace*

E-Mail Configuration Namespace for IDP E-Mailer

- Namespace that defines the properties for the IDP E-Mailer operations.
- Value—Path, relative to the static configuration DN, that defines the object for the namespace
- Default—*/WebApplication/IdpEmailer/email*
- Property name—*emailNamespace*

Configuring a NIC Proxy for IDP E-Mailer

To use SDX Configuration Editor to configure a NIC proxy for IDP E-Mailer:

1. In the navigation pane, select the *IdpEmailer.xml* configuration file.
2. Select the **NIC Proxy Configurations** tab.

The NIC Proxy Configurations pane appears.

3. Configure the NIC proxy for IDP E-Mailer as you would any NIC proxy. For the demonstration application set the following values:
 - Key Type—Subscriber’s IP address
 - Value Type—SAE server ID

For information about configuring NIC proxies, see Overview of NIC Proxy Configuration.

4. Select **File > Save**.
5. Right-click the configuration file, and select **SDX System Configuration > Export to LDAP Directory**.

Configuring Logging for IDP E-Mailer

To configure logging for IDP E-Mailer, modify the configuration in SDX Configuration Editor. You configure logging in the same way as other components.

Configuring E-Mail Properties for IDP E-Mailer

Configure retailer-specific properties for sending e-mail in the E-Mail Configurations pane.

To use SDX Configuration Editor to configure e-mail properties for IDP E-Mailer:

1. In the navigation pane, select the *IdpEmailer.xml* configuration file.
2. Select the **E-Mail Configurations** tab.

The **E-Mail Configurations** pane appears.

E-Mail Configurations

E-Mail Host

E-Mail Domain

E-Mail Sender Address

E-Mail Subject

Introductory Text for Intrusive Traffic Received

Introductory Text for Intrusive Traffic Sent

3. In the E-Mail Configurations section, edit or accept the default values.
See “E-Mailer Configurations Fields” on page 68 .
4. Select **File > Save**.
5. Right-click the configuration file, and select **SDX System Configuration > Export to LDAP Directory**.

E-Mailer Configurations Fields

In SDX Configuration Editor, you can modify the following fields in the E-Mail Configurations pane in an *IdpEmailer.xml* configuration file.

E-Mail Host

- Hostname or IP address of the Simple Mail Transport Protocol (SMTP) server to be used to send e-mail messages to subscribers in response to detection of malicious traffic sent or received by subscribers.
- Value— < hostname > or < IP address >
- Default—No value
- Property name—EmailHostName

E-Mail Domain

- Domain name to be added to a subscriber's login name to form the subscriber's e-mail address.
- Value— < domain name >
- Guidelines—This implementation of IDP E-Mailer identifies a single domain name for all subscribers who are notified by e-mail of incidents.
- Default—No value
- Property name—EmailDomainName

E-Mail Sender Address

- E-mail address from which e-mail messages are sent. These messages provide information about incidents that IDP detected.
- Value— < e-mail address >
- Default—No value
- Property name—EmailSenderName

E-Mail Subject

- Text to appear in the Subject line of each message sent in response to an incident detected by IDP for which e-mail is to be sent.
- Value—Text
- Default—No value
- Property name—EmailSubject

Introductory Text for Intrusive Traffic Received

- Introductory text to appear in the message body for detrimental traffic received by the subscriber. Text received from IDP that describes the incident appears after this introductory text.
- Value—Text
- Default—No value
- Property name—EmailSourceOfIntrusion

Introductory Text for Intrusive Traffic Sent

- Introductory text to appear in the message body for detrimental traffic sent by the subscriber. Text received from IDP that describes the incident appears after this introductory text.
- Value—Text

- Default—No value
- Property name—EmailDestinationOfIntrusion

Deploying IDP E-Mailer

To deploy the updated *idpemail.war* file:

- Copy the file to the deployment directory for your Web server.

If you are using JBoss, copy the file to the */opt/UMC/jboss/server/default/deploy* directory. JBoss automatically starts the Web application when a new WAR file is copied into the *deploy* directory.

Chapter 7

Monitoring Subsets of Subscriber Traffic

- Overview of Surveillance Director on page 71
- Configuring Initial Properties for the Surveillance Director on page 71
- Customizing How to Monitor Subsets of Subscriber Traffic on page 74

Overview of Surveillance Director

The Surveillance Director is the component that manages the process of selecting subscriber traffic to be monitored and activating SRC services to direct specified traffic to an IDP sensor (IDP hardware appliances that run the IDP sensor software). It divides subscribers into groups, then directs traffic for one group at a time through IDP. This means that IDP monitors different groups of traffic at different times, and that traffic for SRC-managed subscribers is periodically monitored. The Surveillance Director relies on SRC services to policy-route traffic from JUNOS routers or to mirror traffic from JUNOS routing platforms to the IDP sensor.

Configuring Initial Properties for the Surveillance Director

To monitor subsets of subscriber traffic by using the Surveillance Director, you configure properties for the Surveillance Director.

To configure bootstrap properties for the Surveillance Director:

1. On the SAE host, log in as root or as an authorized nonroot admin user.
2. Start the local configuration tool from the installation directory for the IDP integration component:

`/opt/UMC/idp/etc/config -l`

The first time that you issue this command, it creates the *default.properties* file and displays the local configuration tool window for the properties.

3. On the Main tab, configure general properties for Surveillance Director.

See “General Properties for Surveillance Director” on page 72 .

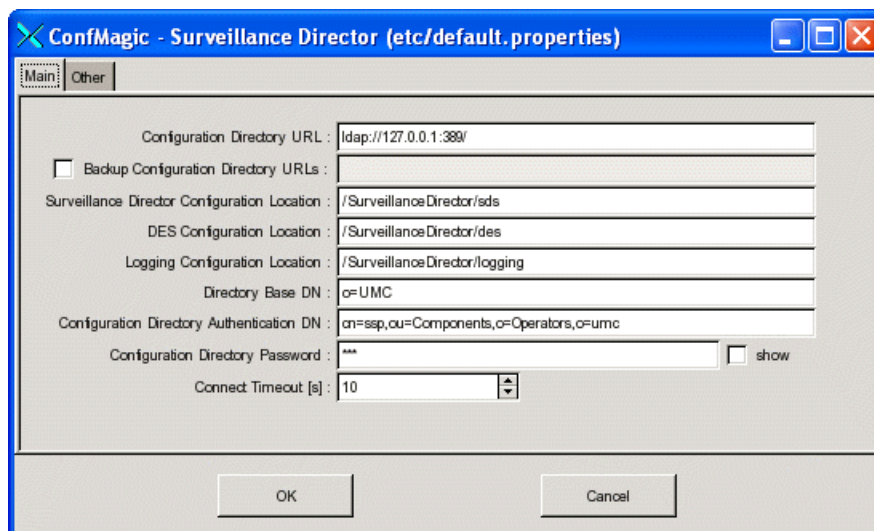
4. On the other tab, configure Java properties for Surveillance Director.

See “Java Properties for Surveillance Director” on page 73 .

5. Click **OK**.

General Properties for Surveillance Director

Use the Main tab to configure general information for the Surveillance Director.



Configuration Directory URL

- URL of the directory server that stores the configuration information for the Surveillance Director.
- Value—URL in the format `ldap:// <host>`
- Default—`ldap://127.0.0.1:389`

Backup Configuration Directory URLs

- URLs of backup directory servers that stores the configuration information for the Surveillance Director.
- Value—URL in the format `ldap:// <URL>`, with more than one URL separated by commas
- Default—No value

Surveillance Director Configuration Location

- Configuration namespace for the Surveillance Director instance definitions.
- Value—Path, relative to the root of the static configuration properties, that defines the object for the namespace in the format `/ <namespace_name>`
- Default—`/surveillanceDriver/sds`

DES Configuration Location

- Configuration namespace for the Surveillance Director's connection to the network directory (the directory that contains `o = Networks`, `o = umc`).
- Value—Path, relative to the root of the static configuration properties, that defines the object for the namespace in the format `/ <namespace_name>`
- Default—`/surveillanceDriver/des`

Logging Configuration Location

- Configuration namespace for logging for the Surveillance Director.
- Value—Path, relative to the root of the static configuration properties, that defines the object for the namespace in the format / < namespace_name >
- Default—/SurveillanceDirector/Logging

Directory base DN

- DN of the root directory for the SAE.
- Value— < DN >
- Guideline—You must set this attribute if you use a directory-naming scheme that differs from the default.
- Default—*o = umc*

Configuration Directory Authentication DN

- DN of the entry in the directory that authenticates the directory bind for the Surveillance Director.
- Value— < DN >
- Default—*cn = conf, o = operators, < base >*

Configuration Directory Password

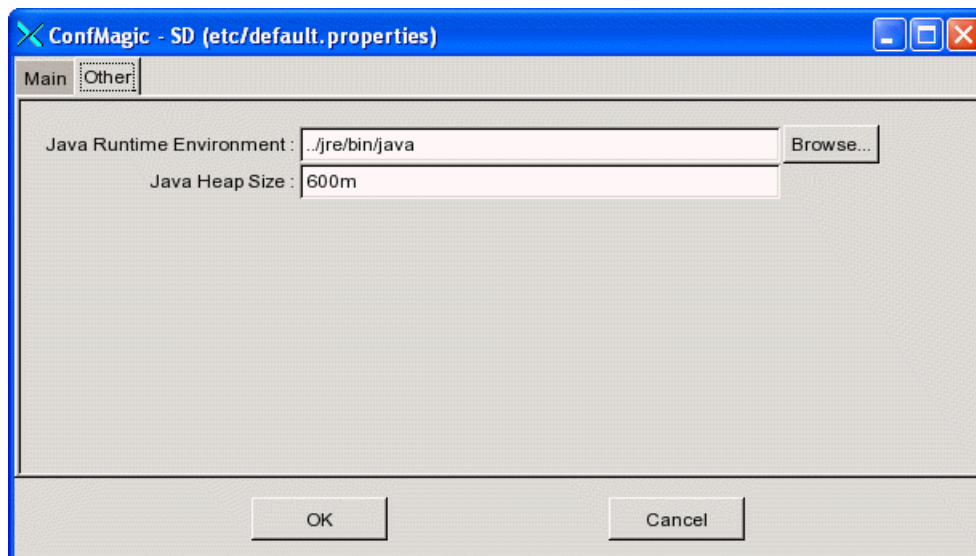
- Authentication password for the directory.
- Value—Text string
- Default—conf

Connect Timeout

- Interval to connect to the directory.
- Value—Number of seconds in the range 0–2147483647
- Default—10

Java Properties for Surveillance Director

Use the Other tab to configure properties for the Java Runtime Environment (JRE).



Java Runtime Environment

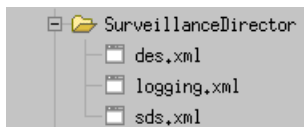
- Path to the JRE.
- Value—Directory path in the format / <pathname >
- Default—../jre/bin/java

Java Heap Size

- Maximum amount of memory available to the JRE.
- Value—Number of megabytes in the format <integer> m
- Guidelines—Change this value if the system has problems caused by insufficient memory. Set the value lower than the available physical memory to avoid low performance caused by disk swapping.
- Default—100m

Customizing How to Monitor Subsets of Subscriber Traffic

You customize the configuration for the Surveillance Director from SDX Configuration Editor. The configuration files in the sample data contain default values for some Surveillance Director properties. Use these files as a starting place for your configuration. After you import the configuration from the directory into SDX Configuration Editor, the following files appear in the SurveillanceDirector folder.



You can edit the files in this location or make copies of the files and then edit them.

For information about how to use SDX Configuration Editor and how to import data from the directory into SDX Configuration Editor, see the *SRC 1.0.x SRC PE Getting Started Guide, Chapter 39, Using SDX Configuration Editor*:

<http://www.juniper.net/techpubs/software/management/src/>

Tasks to configure properties for the Surveillance Director are:

- Configure Directory Properties for the Surveillance Director.
- Configure Logging for the Surveillance Director.
- Configure an Instance of the Surveillance Director.

Configuring Directory Properties for the Surveillance Director

You configure properties specific to the Surveillance Director to access network data in the directory through the directory eventing system (DES). For more information about the DES, see Overview of the Directory Eventing System.

To use SDX Configuration Editor to configure the directory properties for the Surveillance Director:

1. In the navigation pane, select the *des.xml* file under SurveillanceDirector.
2. Select the **LDAP** tab, and expand the **Network** and **DES Client Configurations** sections.

The following pane shows the properties available with the Editing Level for SDX Configuration Editor set to Normal.

LDAP

▼ **Network**

Network Root

DES Client Configuration

URL

Security Principal

Security Credentials

Enable System Management

3. In the Network section, edit or accept the default values for the field.

See “Network Field” on page 76 .

4. In the DES Client Configurations section, edit or accept the default values for the fields.

To complete the entries under DES Client Configuration, see Overview of the Directory Eventing System.

5. Select **File > Save**.
6. Right-click the configuration file, and select **SDX System Configuration > Export to LDAP Directory**.
7. After you complete the configuration changes, stop and then restart the Surveillance Director for the configuration changes to take effect. Use the following commands to stop and then start the Surveillance Director:

```
/opt/UMC/idp/etc/sd stop  
/opt/UMC/idp/etc/sd start
```

Network Field

In SDX Configuration Editor, you can modify the following field in the LDAP pane in a *des.xml* configuration file.

Network Root

- DN of the network object. The network object contains objects for each router that the SRC software manages.
- Value— < DN >
- Default—No value
- Example—*o = Network, o = umc* (value in the sample date)

Configuring Logging for the Surveillance Director

To use SDX Configuration Editor to configure logging for the Surveillance Director:

1. In the navigation pane, select the *logging.xml* configuration file under SurveillanceDirector.

The Logging pane appears.

2. Configure logging properties for the Surveillance Director in the same way that you configure logging for other components.

Configuring an Instance of the Surveillance Director

You configure properties for an instance of the Surveillance Director for a set of virtual routers to be monitored. One virtual router can be monitored by only one instance of the Surveillance Director at a time.

To use SDX Configuration Editor to configure an instance of the Surveillance Director:

1. In the navigation pane, select the *sds.xml* file under SurveillanceDirector.
2. Select the **Surveillance Director** tab, and expand the **Director Instance** and **Surveillance Director** sections.

Surveillance Director

☐ **Director Instances**

Create a New Instance of

▼ **Surveillance Director (sd_1)**

Virtual Router Filter	<input type="text" value=".*@IDPJunose.*"/>	
IDP Service Name	<input type="text" value="CheckForAttacks"/>	
Maximum Number of IP Addresses	<input type="text" value="8"/>	<input type="button" value="Disable"/>
Maximum Number of Subnets	<input type="text" value="4"/>	<input type="button" value="Disable"/>
Maximum Number of IP Addresses per Subnet	<input type="text" value="8"/>	<input type="button" value="Disable"/>
Minimum Number of IP Addresses per Subnet	<input type="text" value="1"/>	<input type="button" value="Disable"/>
Surveillance Time	<input type="text" value="15"/>	<input type="button" value="Disable"/>
Interval Between IDP Service Sessions	<input type="text" value="5"/>	<input type="button" value="Disable"/>
DN of Router Profiles	<input type="text" value="ou=routers, retailername=SP-IDP, o=Users, o=UMC"/>	
Suppress IP Addresses	<input type="text"/>	<input type="button" value="Disable"/>

3. In the Surveillance Director section, edit or accept the default values for the fields.
- See “Surveillance Director Fields” on page 77 .



NOTE: The sample data provides values appropriate for setup and debugging for each of these properties.

4. Select **File > Save**.
5. Right-click the configuration file, and select **SDX System Configuration > Export to LDAP Directory**.

Surveillance Director Fields

In SDX Configuration Editor, you can modify the following fields in the Surveillance Director pane in a *sds.xml* configuration file.

Virtual Router Filter

- Virtual routers to be monitored by this instance of the Surveillance Director.
- Value—A regular expression that matches the virtual routers to be managed.
- Guidelines—For information about regular expressions, see

<http://java.sun.com/j2se/1.4.2/docs/api/java/util/regex/Pattern.html>

Typically, an instance of the Surveillance Director can manage more than one virtual router; however, only one instance of the Surveillance Director manages a virtual router at one time. If more than one instance of the Surveillance Director matches the same virtual router, the first instance of the Surveillance Director that is configured and that matches the virtual router manages it.

If you change the configuration of an instance of the Surveillance Director to stop managing a virtual router, and another instance of the Surveillance Director is already configured to manage that virtual router, then the other instance of the Surveillance Director assumes management of that virtual router.

- Default—No value
- Examples
 - `.*@BRAS.*`—Matches all virtual routers on routers whose names start with BRAS
 - `.*virneo.*@.*`—Matches all virtual routers that contain virneo in the virtual router name, for a router with any name
- Property name—vrFilter

IDP Service Name

- Name of the service to activate in order to direct a subset of subscriber traffic to an IDP sensor.
- Value— < Service name >
- Default—No value
- Property name—idpServiceName

Maximum Number of IP Addresses

- Maximum number of subscriber IP addresses for which the associated traffic should be sent to an IDP sensor or sensor cluster at one time.
- Value—Integer greater than 1
- Guidelines—You must configure a value for this property. This value must be a power of 2. Ensure that the amount of traffic generated by the number of IP addresses identified by this property conforms to the capacity for the IDP system.

For JUNOSe routers, consider system load on the SAE and on the router when you use policy-based routing from JUNOSe routers to an IDP sensor. A fragment service is activated for each IP address.

- Default—8
- Property name—maxIps

Maximum Number of Subnets

- Maximum number of CIDR subnets for which subscriber traffic can be sent to an IDP sensor at one time.
- Value—Integer greater than 1
- Guidelines—Using a large number of CIDR subnets can affect system performance because an aggregate service for IDP is activated once for each CIDR subnet during a specified surveillance time.
- Default—4
- Property name—maxSubnets

Maximum Number of IP Addresses per Subnet

- Maximum number of IP addresses supported in a CIDR subnet.
- Value—Integer greater than 1
- Guidelines—This value must be a power of 2.

If your configuration has a JUNOS routing platform that is being managed from a JUNOS POP, set this value to the value specified for Maximum Number of IP Addresses.

- Default—8
- Property name—maxIpsPerSubnet

Minimum Number of IP Addresses per Subnet

- Minimum number of IP addresses supported in a CIDR subnet.
- Value—Integer greater than 1
- Guidelines—This value must be a power of 2 to efficiently monitor subnets, and must be set to a value less than the value for the Maximum Number of IP Addresses per Subnet.

If the minimum size of a subnet is small and the IP pools do not have large contiguous address ranges, then a surveillance interval can be underused by the number of subscribers. Also with a small minimum size specified, the IP pool can be divided into numerous CIDR subnets to exclude discontinuities in the addresses. In this scenario if the value is a number greater than 1, some addresses may be infrequently or never monitored.

- Default—1
- Property name—minIpsPerSubnet

Surveillance Time

- Length of time to monitor each set of subscribers. This value is also the session timeout for the service specified by the IDP Service Name property.
- Value—Number of seconds greater than 1
- Default—15
- Property name—surveillanceTime

Interval Between IDP Service Sessions

- Length of time between when IDP service sessions time out and when the next IDP service sessions are activated.
- Value—Number of seconds greater than 1
- Guidelines— Typically, services for a specified set of IP addresses time out at approximately the same time; however, the length of time to deactivate the services depends on other factors, such as the number of addresses and subnets for which a service is being deactivated, the software and hardware versions of the routers, and the size of systems running the SAE. Use this property to specify how long the Surveillance Director waits for all services to become inactive before it activates services for the next set of addresses to be monitored.

If the value for this property is too long, IDP is underutilized; if it is too short, the IDP can become overloaded.

- Default—5
- Property name—intraSurveillanceTime

DN of Router Profiles

- DN in the directory of the subscriber folder which contains the subscriber entries that correspond to router entries under the network root. For the Surveillance Director to activate a service configured for IDP integration for `<vrName> @ <routerName>`, it constructs a DN type of subscriber ID in the form `routerName = <vrName> @ <routerName>, <DN of router profiles>`. The Surveillance Director then uses that DN to locate the subscriber session in which to activate the service.
- Value— `<DN>`
- Default—No value
- Example—`ou = routers, retailername = SP-IDP, o = Users, o = umc`
- Property name—routerProfilesDn

Suppress IP Addresses

- Specifies whether the Surveillance Director provides a value for the `subrIps` parameter (a list of all the individual addresses to be monitored during a surveillance interval) when it activates an IDP service. For use when traffic is sent directly from JUNOS routers to an IDP sensor.
- Value—True or false
- Guidelines—Specify false for JUNOS POPs. Specify true for JUNOS POPs.
- Default—False
- Property name—suppressIps

Chapter 8

Defining Actions to Be Taken for Subscriber Traffic

- Actions to Be Taken for Subscriber Traffic on page 81
- Redirecting Web Requests to an IDP Captive Portal on page 81
- Developing and Customizing the Sample IDP Captive Portal on page 84
- Applying Services to Subscribers Associated with Problem Traffic on page 89

Actions to Be Taken for Subscriber Traffic

When IDP processes subscriber traffic that it receives, it identifies malicious traffic as defined by IDP security rules that are configured within IDP. For SRC-managed subscriber traffic, you can configure the SRC software to:

- Redirect subscriber Web requests to an IDP captive portal page that provides information about the problem encountered.
- Activate services to take actions such as limiting the bandwidth available to the subscriber.
- Send e-mail to the subscriber to provide information about a problem encountered by mapping IP addresses to subscriber names.
- Enable in IDP actions that the SRC software takes in response to an incident reported by IDP

Redirecting Web Requests to an IDP Captive Portal

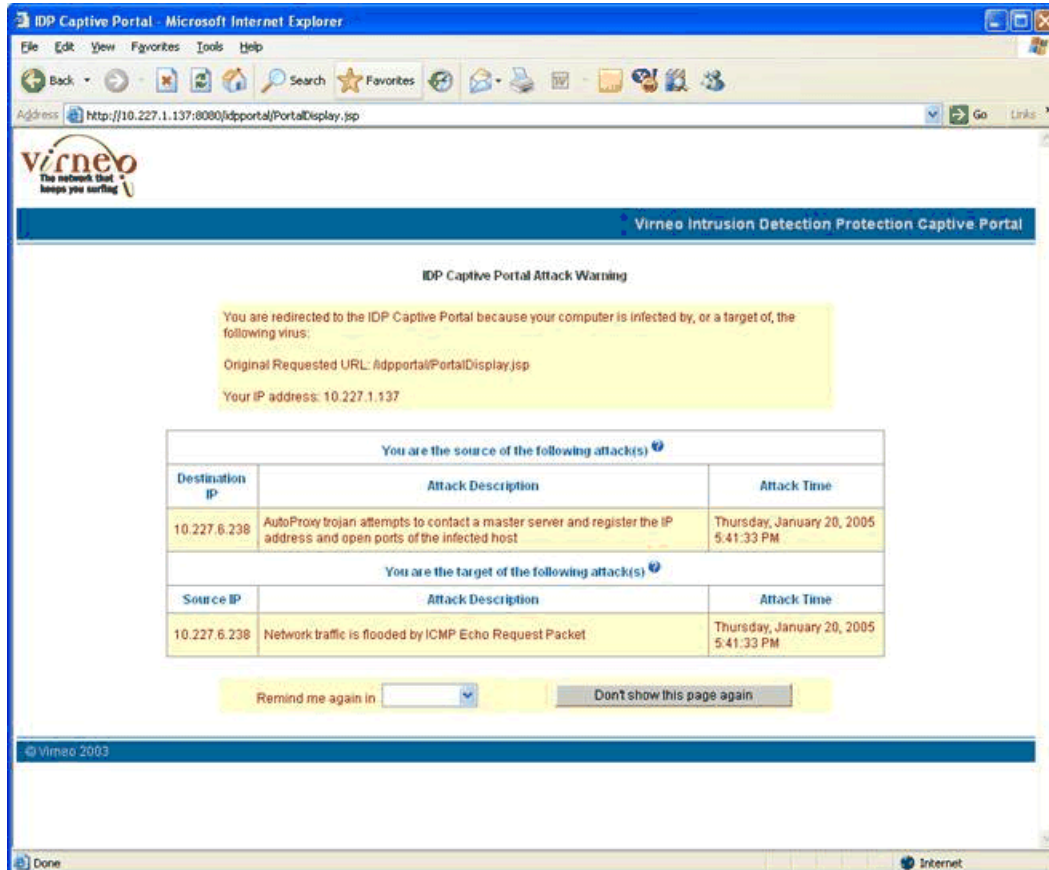
You can configure the SRC software to redirect subscriber Web requests to an IDP captive portal page in response to IDP security rules that detect problem traffic sent by or received by a subscriber. A captive portal is simply a Web page that receives redirected HTTP requests. The SRC application library provides a sample IDP captive portal that is a Java 2 Platform, Enterprise Edition (J2EE) Web application. We provide the application for demonstration purposes. You use an SRC service to redirect Web requests to a captive portal.

You can use the sample IDP captive portal as a basis for a captive portal for your environment, or you can develop a different captive portal based on the sample.

The sample IDP captive portal:

- Provides the source IP address or destination IP address of the problem traffic and provides a description of the incident.

The following page shows a sample IDP captive portal page that identifies incoming as well as outgoing traffic problems that IDP detected. The help buttons provide information about what the subscriber can do in response to the problem. For example, for the incoming traffic the Help could recommend that the subscriber use firewall software.



- Displays general information if the SRC software cannot collect information about the type of traffic that causes a problem; for example, if the IDP management server cannot access the record servlet in the IDP captive portal.
- Lets the subscriber display the Web page that he or she was trying to access when the request was redirected to the captive portal page and be reminded of the error at another time.
- Lets the subscriber prevent display of the IDP captive portal page again for the same incident.

This feature is useful for a subscriber who is addressing a detected problem and who does not want to be redirected to the IDP captive portal page again while addressing the issue. It is not intended that the subscriber simply ignore the problem.

If a new problem occurs, the portal displays a new page.

Sequence for Redirecting Traffic

The sample IDP captive portal takes the following actions in response to incidents detected by IDP:

1. The portal's record servlet records HTTP messages that it receives from the IDP management server. The messages include the source and destination IP addresses of problem traffic and a problem description.
2. The IDP management server activates a service that policy-routes the subscriber's Web traffic to the redirect server.
3. When the subscriber tries to access the Web, the redirect server responds to the subscriber's Web traffic by redirecting the subscriber to the IDP captive portal through an HTTP redirect process.
4. The IDP captive portal then retrieves the subscriber's IP address and the stored messages for this IP address, and displays messages appropriate to the subscriber.

About the Record Servlet

The record servlet receives messages from the **idpsdx.py** script that runs in IDP. It posts messages to a specified URL. The default URL is [http\(s\)://<hostname>:<port>/idpPortal/Record](http(s)://<hostname>:<port>/idpPortal/Record).

The following example shows the type of information that IDP sends to the record servlet. The parameter name in the message appears to the left of the equals sign and the value to the right.

```
fixed.timeGeneratedGMT=2005/01/20 17:41:33
fixed.timeReceivedGMT=2005/01/20 17:41:44
fixed.deviceAddress=10.227.6.116
fixed.devinVIN=A97B-3867-3062-D6E6
fixed.sourceAddress=10.227.6.238
fixed.sourcePort=35170
fixed.destinationAddress=10.227.6.252
fixed.destinationPort=8
fixed.inboundInterface=eth0
fixed.outboundInterface=
fixed.virtualDevice=s0
fixed.attack=ICMP:EXPLOIT:FLOOD
fixed.policy=FirstPolicy
fixed.policyVersion=6
fixed.rulebase=IDS
fixed.ruleNumber=10
fixed.miscellaneous=repeated 3 times
fixed.bytes=0
fixed.packets=0
fixed.elapsed=0
fixed.protocol=ICMP
fixed.category=ATTACK
fixed.subCategory=ICMP_FLOOD
fixed.action=NONE
fixed.severity=MEDIUM
```

`fixed.isAlert=no`

The record servlet maps addresses to messages for the types of incidents to be recorded to:

- `fixed.sourceAddress`—Source IP address
- `fixed.destinationAddress`—Destination IP address

If the servlet receives more than one record for the same source and destination address at the same time (`fixed.timeGeneratedGMT`) with the same ID (`fixed.attack`), the servlet stores the record once and increases the value of a counter by one for each subsequent occurrence.

For information about the **idpsdx.py** script that runs in IDP Manager, see “Enabling SRC Actions from IDP Manager” on page 91.

Developing and Customizing the Sample IDP Captive Portal

The */webapp* directory on the SRC application library CD contains the *idpPortal.war* file. The *idpPortal.war* file provides:

- Complete source code for the IDP captive portal in the *WEB-INF/src* directory
- Documentation for the Java classes used in the sample IDP captive portal in the */javadoc* directory

For information about expanding the *idpPortal.war* file, see “Configuring Properties for the Sample IDP Captive Portal” on page 84.

The IDP captive portal uses the SAE CORBA remote application programming interface (API) to perform actions such as activating, deactivating, or scheduling services. For information about the SAE CORBA remote API, see the SAE CORBA remote API online documentation on the SRC software distribution in the directory *SDK/doc/idl/index.html*.

The tasks to deploy the sample IDP captive portal are:

1. “Configuring Properties for the Sample IDP Captive Portal” on page 84
2. “Deploying the Updated WAR File” on page 88
3. “Accessing the IDP Captive Portal” on page 88
4. “Configuring the Redirect Server to Redirect Traffic to the IDP Captive Portal” on page 88

Configuring Properties for the Sample IDP Captive Portal

The sample IDP captive portal provided with the SRC software is designed to be used with the IDP integration implementation and the sample data. To use the sample IDP captive portal, edit the *WEB-INF/portal.props*. The */opt/UMC/idp/idpPortal.war* file contains the *WEB-INF/portal.props* file.

To edit the *WEB-INF/portal.props* file:

1. Copy the *idpPortal.war* file to a temporary folder, and work in that folder.
2. Extract the *WEB-INF/portal.props* file from the *idpPortal.war* file.

jar xvf idpPortal.war WEB-INF/portal.props

3. With a text editor, edit the *WEB-INF/portal.props* file:
 - Review the basic portal properties, and update as needed.
See “Basic Portal Properties” on page 85.
 - Review the entries for the SAE locator, and change them as needed to accommodate your SRC configuration.
See “Locator Properties” on page 87.
 - Configure properties in the network information collector (NIC) proxy configuration section of the file.
For information about the values to configure for NIC properties, see Overview of NIC Proxy Configuration.
4. Replace the *WEB-INF/portal.props* file and any other updated files in the *idpPortal.war* file.

jar uvf idpPortal.war WEB-INF/portal.props

Basic Portal Properties

In the *WEB-INF/portal.props* file, you can modify the following properties. These properties specify how the portal uses records received from IDP.

Attack.Record.number

- Maximum number of incident records to be stored for use by the IDP captive portal.
- Value—Integer in the range 1–2147483648
- Default—100

Attack.Record.removeStep

- Number of records to be deleted when the number of records stored reaches the limit specified by the *Attack.Record.number* property. The records are sequentially removed, starting with the oldest record, then the next oldest, and so forth.
- Value— < number >
- Guidelines—This number must be less than the value configured for *Attack.Record.number*.
- Default—10

DateTime.Format

- Format in which to display the date and time of an incident.
- Value—yyyy/MM/dd hh:mm:ss, where yyyy represents the year, MM the month, dd the day, hh the hour, mm the minute, and ss the second
- Guidelines—For more information about this property, including its value see <http://java.sun.com/j2se/1.4.2/docs/api/java/text/SimpleDateFormat.html>
- Default—No value

<Incident-name>

- Name of a parameter that indicates the type of security incident encountered, and provides a description of the parameter.
- Value— < parameter > = < description >
- Guidelines—Enter the parameter and description in the section " Attack Name and the corresponding description."

For information about security parameters, see the IDP documentation at

<http://www.juniper.net/techpubs/software/management/idp/>

- Default—No value
- Example

ICMP.EXPLOIT.FLOOD = Network traffic that is flooded by ICMP Echo Request Packet

TROJAN.AUTOPROXY.INFECTED-HOST = AutoProxy trojan attempts to contact a master server and register the IP address and open ports of the infected host

Attack.Captive.service

- Name of the service for the IDP captive portal. The IDP management server activates this service for subscribers who receive or send malicious traffic. If you use a " remind me later" control on the Web page and the subscriber selects this control, the portal deactivates this service and schedules service activation for a later time. If you use a " don't show this page again" control and the subscriber selects this control, the portal deactivates this service.
- Value— < service name >
- Default—Quarantine

Attack.showRemindLater

- Specifies whether the IDP captive portal page provides the Remind me again in field. This field lets subscribers specify a time at which the portal reminds them of the security incident.
- Value—true or false
- Default—true

Attack.showIgnore

- Specifies whether the IDP captive portal page provides the Don't show this page again field. The field lets subscribers stop display of the captive portal page for incidents that have already been detected. The portal displays another page when another incident occurs.
- Value—true or false
- Default—true

Locator Properties

In the *WEB-INF/portal.props* file, you can modify the following properties. Change these properties to conform to your configuration.

Factory.locator

- Method that the portal uses to locate the SAE.
- Value
 - `net.juniper.smgmt.ssp.LocalFeatureLocator`—Uses the locally configured object reference
 - `net.juniper.smgmt.ssp.DistributedFeatureLocator`—Uses NIC configuration
- Guidelines—If you specify `net.juniper.smgmt.ssp.LocalFeatureLocator`, configure a value for `LocalFeatureLocator.objectRef`.

LocalFeatureLocator.objectRef

- Location of the SAE server.
- Value—Location in one of the following formats:
 - Absolute path to the interoperable object reference (IOR) file in the form `file:// <absolutePath>`
 - Corbaloc URL in the format `corbaloc:: <host> : <port> /SAE`
 - `<host>` —IP address or host on which the SAE is installed.
 - `<port>` —Port used by the SAE on the specified host. The default is 8801.
 - The actual IOR in the form `IOR: <objectReference>`
- Default—No value
- Examples
 - Absolute path—`file:///opt/UMC/sae/var/run/sae.ior`
 - corbaloc URL—`corbaloc::10.10.6.171:8801/SAE`
 - Actual IOR—
IOR:00000000000000002438444C3A736D67742E6A756E697...

DistributedFeatureLocator.locName

- Namespace for the NIC proxy configuration.
- Value— < namespace >
- Default—/, which indicates the root namespace
- Example—DistributedFeatureLocator.locName = /nicProxy indicates that the NIC proxy configuration is in /nicProxy.

Config.java.naming.provider.url

- Location of the LDAP server.
- Value—ldap:// < IP address > : < port number >
- Default—No value
- Example—ldap://127.0.0.1:389

Config.net.juniper.smgmt.des.backup_provider_urls

- Location of a backup LDAP server.
- Value—ldap:// < IP address > : < port number > , with more than one URL separated by commas
- Default—No value

Deploying the Updated WAR File

To deploy the updated WAR file for the application:

- Copy the file to the deployment directory for your Web server.

If you are using JBoss, copy the file to the */opt/UMC/jboss/server/default/deploy* directory. JBoss automatically starts the Web application when a new WAR file is copied into the *deploy* directory.

Accessing the IDP Captive Portal

Access the portal to ensure that you can view the page and to review the page setup. To access the IDP captive portal:

- Enter a URL in the following form in your Web browser, and press Enter.

http(s)://<host>:<port>/idpPortal

Configuring the Redirect Server to Redirect Traffic to the IDP Captive Portal

To configure the redirect server to redirect Web requests to the IDP captive portal:

1. Follow the instructions for configuring the redirect server in “Overview of the Residential Portal” on page 117.
2. In the */opt/UMC/redir/etc/redir.properties* file, specify the URL of the IDP captive portal for the *redir.url* property. This entry has the form

redir.url = http(s):// < host > : < port > /idpPortal/PortalDisplay.jsp

Applying Services to Subscribers Associated with Problem Traffic

You can configure services to control subscriber traffic, such as limiting bandwidth available to a subscriber, in response to detection of malicious traffic sent or received by a subscriber. The following procedure describes how to configure policies to decrease the amount of bandwidth available to the subscriber and to redirect subscriber Web requests to an IDP captive portal as implemented in the sample data. You can also create separate services or a service for only one of these actions.

To limit bandwidth and redirect subscriber Web requests to a captive portal:

1. In Policy Editor, create a policy that defines an action to be taken, such as a policy that limits a subscriber's bandwidth and redirects Web requests to a captive portal.

For a sample policy group, see *policyGroupName = Quarantine, ou = idp, o = Policies, o = UMC* in the sample data.

2. (Optional) In SDX Admin, create a scope for the services that define actions to be taken in response to IDP rules configured in IDP.
3. If you created a scope in Step 2:
 - a. In that scope, create a service that defines actions to be taken in response to IDP rules. Then set the type to normal, and specify the policy group configured in Step 1.

For a sample service, see *serviceName = Quarantine, l = IDP-Subscriber, o = Scopes, o = umc* in the sample data.

- b. Assign the scope to a subscriber folder to make the service available to subscribers.
4. Create service subscriptions for subscribers. In the sample data, we create a subscription at the folder level to allow all subscribers in the folder to inherit the subscription.

For a sample implementation, see *serviceName = Quarantine, ou = subscribers, retailerName = SP-IDP, o = Users, o = umc* in the sample data.

Chapter 9

Enabling SRC Actions from IDP Manager

- Overview of How to Enable Actions from IDP Manager on page 91
- Configuring Scripts for IDP on page 91

Overview of How to Enable Actions from IDP Manager

After you complete all the configuration to integrate IDP with the SRC software, you configure the **idpsdx.py** script—a script that implements the messaging to record problem incidents and identifies the action for the SRC software to take: redirect traffic to an IDP captive portal, activate services, and send e-mail.

In a testing environment, you can use the **idpsdx.sh** script to set up and troubleshoot a configuration that integrates IDP into an SRC-managed environment. The **idpsdx.sh** script sets the library paths, redirects debugging output, and executes the **idpsdx.py** script. Do not use the **idpsdx.sh** script in a production environment.

The **idpsdx.py** script requires Python version 2.3 and the following Python libraries installed on the system that runs the IDP management server:

- SOAPpy (0.11.6)
- PyXML (0.8.3)
- fpconst (0.7.0)
- logging (4.8.1)

The SMCpython and UMCpyadd packages in the SRC software distribution contain Python version 2.3 and the libraries listed.

Configuring Scripts for IDP

The **idpsdx.py** script provides documented source code as well as configuration properties to allow you to create customized e-mail messages and implementations. You can locate the scripts in the `/opt/UMC/idp/scripts` directory.

Before You Configure Scripts

Before you configure scripts:

- Complete all other configuration for IDP integration with SRC.

- Verify the location where Python is installed on the system. If you installed Python from the SRC software distribution, the default installation directory is */opt/UMC/python*. If you installed Python to a different directory, update the paths in *idpsdx.py* and in *idpsdx.sh* (if you use this file).
- For a production environment, start the IDP management server in an environment in which the library path includes the Python libraries.

Configuring Scripts

To configure scripts:

1. Edit the *idpsdx.py* file to specify the actions to be taken.

See “Properties in the *idpsdx.py* File” on page 92.

2. Copy the *idpsdx.py* file and the *idpsdx.sh* file (if you use this file) to the appropriate directory for IDP Manager. For the location of this directory, see the IDP documentation at

<http://www.juniper.net/techpubs/software/management/idp/>

Properties in the *idpsdx.py* File

You can modify the following properties in the *idpsdx.py* file.

RECORD URL

- URL of the record interface of the IDP captive portal that stores information received from IDP. The interface records information about detrimental traffic under the source and destination of the traffic. The security rules configured in IDP determine the type of incidents recorded.
- Value—“ <URL> ”
- Guidelines—Enclose the URL in quotation marks because this entry is a Python string. The value “ <http://<IP-address>/idpPortal/Record>” is the default URL specified in the *WEB-INF/web.xml* file for *idpPortal.war*.
- Example—“ <http://192.0.2.25/idpPortal/Record>”

DSA URL

- URL of the Web application server running Dynamic Service Activator and the path to the Web service description of Dynamic Service Activator.
- Value—URL in the form “ [http\(s\)://<user>:<password>@<host>:<port>/dsa/services/DynamicServiceActivation?wsdl](http(s)://<user>:<password>@<host>:<port>/dsa/services/DynamicServiceActivation?wsdl)”
 - <user> —Client ID configured for Dynamic Service Activator
 - <password> —Password associated with the client ID configured for Dynamic Service Activator
 - <host> —Hostname or IP address of the server on which Dynamic Service Activator runs

- `<port>` —Port number used by Dynamic Service Activator on the server
- `wsdl`—Indicates Web Services Description Language
- Guidelines—Enclose the URL in quotation marks because this entry is a Python string.

In the sample implementation, Dynamic Service Activator is used by the **idpsdx.py** integration script to send e-mail and activate the captive portal service.

- Example—“
`http://idp:secret@10.227.6.171:8080/dsa/services/DynamicServiceActivation?wsdl`”

DEBUG

- Specifies whether or not to print diagnostic messages to the screen.
- Value—True or False

RECORD

- Specifies whether or not to send messages to the captive portal to record the details of an incident. The portal stores these messages and provides information about the incidents to a subscriber when Web requests for the subscriber are redirected to the captive portal.
- Value—True or False

CAPTIVE

- Specifies whether or not to activate a captive portal to notify subscribers that IDP detected malicious traffic sent to or received from them.
- Value—True or False

CAPTIVE SERVICE

- Specifies the name of the service that activates a captive portal.

For a subscriber to have Web requests redirected to a captive portal, the subscriber must have or inherit a subscription to the service.
- Value—“ `<service name>` ”
- Guidelines—Enclose the service name in quotation marks because this entry is a Python string.
- Example—“ `Quarantine` ”

EMAIL

- Specifies whether or not to send notification e-mail messages to subscribers that IDP detected malicious traffic sent or received by them.
- Value—True or False

Sample *idpsdx.py* Script

Through Dynamic Service Activator, the sample **idpsdx.py** script activates the service that redirects subscribers to the captive portal. Because Dynamic Service Activator does not support persistent activation, the sample portal activates the service for the captive portal only for users who are logged in to their account.

If you want subscribers to see the IDP captive portal at any time—for example, when they log out of their account, and then log back in to their account but do not try to access the Web—you can write an SAE extension script and invoke it from the `invokeScript` method in Dynamic Service Activator.

Part 4

Integrating IP Address Managers

- Integrating IP Address Managers with the SAE on page 97

Chapter 10

Integrating IP Address Managers with the SAE

- Overview of IP Address Manager Integration on page 97
- Installing Monitoring Agent on page 99
- Configuring Monitoring Agent on page 99
- Managing Monitoring Agent on page 102

Overview of IP Address Manager Integration

You use the Monitoring Agent application with the event notification method of logging in subscribers and creating subscriber sessions. You can use event notification when you integrate devices into the SRC network that do not notify the SAE about subscriber events, such as when a subscriber logs in or when the address assignment is terminated.

For example, you can use monitoring agent in a cable network. When events occur between the IP address manager and the cable modem termination system (CMTS) device or PacketCable Multimedia Specification (PCMM) device driver, Monitoring Agent creates event notifications on the IP address manager that are delivered to the SAE using the event notification application programming interface (API).

For information about event notification in the PCMM network, see *SRC PE Solutions Guide*.

For information about event notification with other third-party network devices, see *SRC PE Getting Started Guide*.

The Monitoring Agent application monitors DHCP or RADIUS messages for DHCP or RADIUS servers running on the same host as Monitoring Agent and generates subscriber events. Monitoring Agent intercepts messages on every available interface unless configured to do otherwise in the property file.

The Monitoring Agent application must run on every server host that can allocate IP addresses to subscribers. Monitoring Agent is stateless and cannot synchronize the current set of subscribers when there is a failure. If events are missed because of a software or network failure, the overall state recovers when DHCP leases are renewed or RADIUS interim updates are sent. For example, missed ipUp events become effective when the affected lease is renewed or the next interim update is sent, and

missed ipDown events time out when the lease expires or after the configured RADIUS time to live.

The Monitoring Agent application can be configured as the pseudo-RADIUS server. In this case, Monitoring Agent acts as a RADIUS accounting server and no longer needs to run on the same host as the RADIUS server. However, your router or RADIUS server should be configured to duplicate accounting packets to Monitoring Agent. When Monitoring Agent is the pseudo-RADIUS server, it handles software failures more robustly. The pseudo-RADIUS server does not acknowledge failed accounting requests and gives the RADIUS client the option to retransmit the accounting packet to a backup Monitoring Agent.

Monitoring DHCP Messages

When Monitoring Agent is intercepting DHCP messages, it captures every UDP packet that is received or sent on UDP port 67 (BOOTP/DHCP server).

Monitoring Agent processes messages for the following DHCP message types:

- DHCPACK—Sent from the server to the client when a lease is acknowledged. The Monitoring Agent application translates the client IP address and IP address lease time into an ipUp event.
- DHCPNAK—Sent from the server to the client when a lease is not renewed or the client configuration is wrong. The Monitoring Agent application translates the client IP address into an ipDown event.
- DHCPRELEASE—Sent from the client to the server when the client cancels the lease. The Monitoring Agent application translates the client IP address into an ipDown event.

All other DHCP messages are ignored.

Monitoring RADIUS Messages

When Monitoring Agent is intercepting RADIUS accounting messages, it captures every UDP packet that is sent to the RADIUS accounting port (1813 is the default port).

Monitoring Agent processes messages for the following RADIUS attributes:

- Acct-Status-Type (RADIUS attribute [40])—Start and interim update events are translated into ipUp events. Stop events are translated into ipDown events.
- Framed-Ip-Address (RADIUS attribute [8])—The IP address identifies the notified interface.
- Acct-Session-Id (RADIUS attribute [44])—The accounting session ID is set as the EA_SESSION_ID attribute of the event notification.
- NAS-Port-Id (RADIUS attribute [87])—If present, the NAS port ID is set as the EA_NAS_PORT_ID attribute of the event notification.

The RADIUS client must send interim update accounting requests with a known frequency because the Monitoring Agent application cannot keep the state of logged

subscriber sessions. To allow for lost messages, you might set the timeout value for ipUp notifications to a value that is larger than the interim update interval. For example, setting the timeout value to twice the interim update interval allows for one lost message.

Installing Monitoring Agent

You must manually install the UMCmagt package on the server host to deploy the Monitoring Agent application.

```
pkgadd -d /cdrom/cdrom0/Demos+Sample_Applications UMCmagt
```

For information about installing Monitoring Agent, see “Installing the Sample SRC Applications” on page 3.

Configuring Monitoring Agent

Tasks to configure Monitoring Agent are:

- “Configuring Properties” on page 99
- “Configuring NIC Proxy” on page 101

Configuring Properties

The properties for Monitoring Agent determine the behavior of the application. The default values allow the Monitoring Agent application to operate, but you can specify different timeout values, device names, or RADIUS ports.

To configure properties for Monitoring Agent:

1. On the server host, log in as root or as an authorized nonroot admin user.
2. Verify that Monitoring Agent is not running. (See “Displaying Monitoring Agent Status” on page 103 and “Stopping Monitoring Agent” on page 102).
3. With a text editor, edit the */opt/UMC/monAgent/etc/ma_default.properties* file.

See “Monitoring Agent Properties” on page 99.

4. Save the file.
5. Start Monitoring Agent for the changes to take effect. (See “Starting Monitoring Agent” on page 102).

Monitoring Agent Properties

With a text editor, you can configure the following properties for Monitoring Agent.

MonAgent.capture.devices

- Space-delimited list of devices where packets are captured. When this list is empty, packets on all available interfaces are captured.
- Value—Text string in the format <interfaceName> <interfaceName>

- <interfaceName> identifies the network interface on the host where the Monitoring Agent application is running.
- Default—Empty
- Example—dmfe0 dmfe1

MonAgent.capture.pool

- Maximum number of concurrent event handlers.
- Value—Integer in the range 0-2147483647
- Default—8

MonAgent.timeout

- Time to keep an event handler alive for reuse.
- Value—Number of seconds in the range 0-2147483647
- Default—300

MonAgent.event.timeout

- Time to wait before discarding failed events.
- Value—Number of seconds in the range 0-2147483647
- Default—300

MonAgent.event.retry_time

- Time to wait before retrying failed events.
- Value—Number of seconds in the range 0-2147483647
- Default—30

MonAgent.dhcp.packet.forward

- Controls the attachment of the whole packet to the notification.
- Value
 - true—Enables the attachment of the packet.
 - false—Disables the attachment of the packet.
- Default—true

MonAgent.dhcp.enable

- Controls the monitoring of DHCP messages.
- Value
 - true—Enables the monitoring of DHCP messages.
 - false—Disables the monitoring of DHCP messages.
- Default—true

MonAgent.radius.enable

- Controls the monitoring of RADIUS messages.
- Value
 - true—Enables the monitoring of RADIUS messages.
 - false—Disables the monitoring of RADIUS messages.
- Default—true

MonAgent.radius.port

- UDP port on which RADIUS accounting messages are expected.
- Value—Integer; valid port number in the range 1–65535
- Default—1813

MonAgent.radius.server

- Controls the monitoring of RADIUS packets by the pseudo-RADIUS server on the RADIUS accounting port. If you enable the pseudo-RADIUS server, you must also set `MonAgent.radius.enable = true`.
- Value
 - true—Enables the pseudo RADIUS server to receive RADIUS packets.
 - false—Disables the pseudo RADIUS server from receiving RADIUS packets.
- Default—false

MonAgent.radius.secret.<IP address>

- Shared secret between the RADIUS server and trusted RADIUS client. This value is ignored if `MonAgent.radius.server` is false.
- Value—IP address and shared secret pair in the format `MonAgent.radius.secret. < ip address > = < shared secret >`

 For example, a RADIUS client with an IP address of 10.227.7.47 that has a shared secret of secret with the pseudo-RADIUS server would be specified as `MonAgent.radius.secret.10.227.7.47 = secret`.
- Default—`MonAgent.radius.secret.127.0.0.1 = secret`

MonAgent.ttl

- Time to wait for a detected IP address.
- Value—Number of seconds in the range 0-2147483647
- Guidelines—This timeout value should be larger than the interim update interval; we recommend twice the value.
- Default—1800

Configuring NIC Proxy

To configure a NIC proxy for the Monitoring Agent application, see Overview of NIC Proxy Configuration.

Managing Monitoring Agent

The Monitoring Agent application must be running on the same host as each DHCP server or RADIUS server that can allocate IP addresses to subscribers.

Tasks to manage Monitoring Agent are:

- “Starting Monitoring Agent” on page 102
- “Stopping Monitoring Agent” on page 102
- “Displaying Monitoring Agent Status” on page 103
- “Cleaning Monitoring Agent Logs” on page 103

Starting Monitoring Agent

Before you start Monitoring Agent, you must do the following:

1. Install Monitoring Agent as described in “Installing Monitoring Agent” on page 99.
2. Configure Monitoring Agent as described in “Configuring Monitoring Agent” on page 99.

To start Monitoring Agent:

1. On the Monitoring Agent host, log in as root.
2. Start Monitoring Agent from its installation directory.

`/opt/UMC/monAgent/etc/monAgent start`

The system responds with a start message. If Monitoring Agent is already running, the system responds with a warning message.

Stopping Monitoring Agent

Before you reconfigure Monitoring Agent, you must manually stop it.

To stop Monitoring Agent:

1. On the Monitoring Agent host, log in as root.
2. Stop Monitoring Agent from its installation directory.

`/opt/UMC/monAgent/etc/monAgent stop`

The system responds with a stop message. If Monitoring Agent is not running when you issue the command, the system responds with a warning message.

Displaying Monitoring Agent Status

To display the Monitoring Agent status:

1. On the Monitoring Agent host, log in as root.
2. Display the status from the Monitoring Agent installation directory.

`/opt/UMC/monAgent/etc/monAgent status`

The system responds with a status message.

Cleaning Monitoring Agent Logs

To delete the log files for Monitoring Agent:

1. On the Monitoring Agent host, log in as root.
2. Delete the log files from the Monitoring Agent installation directory.

`/opt/UMC/monAgent/etc/monAgent clean`

By using the **`stdout`** and **`stderr`** options, you can clean the log files for the Monitoring Agent application and delete the persistent data that the agent writes to files or devices.

Part 5

Integrating Prepaid Service Applications

- Providing Prepaid Services on page 107

Chapter 11

Providing Prepaid Services

- Overview of Prepaid Services Demo on page 107
- Installing and Configuring the Prepaid Services Demo on page 109
- Managing Prepaid Accounts on page 113

Overview of Prepaid Services Demo

Prepaid service applications assume that users (subscribers) are registered with a subscriber management system, so that they can log in to the network and be authenticated. By default a subscriber has no access to the network. All attempts to access the Internet are intercepted and captured by the Service Selection Portal.

Subscribers pay for the service in advance of use by purchasing an access card that has a valid account number and expiration date. The subscriber then can activate the prepaid service, which might be, for example, access to the Internet or access to a gaming server. At activation, the portal prompts the subscriber for the account number and validates the access. The portal grants access if appropriate, and charging starts as soon as the portal grants access.

To integrate prepaid service applications, the prepaid services demo consists of the following two components:

- The prepaid account server is a Solaris package, `UMCpddemo`, located in the *solaris* directory on the SRC application library CD.
- The Prepaid Account Administration application is a standard Web application archive (WAR file) located on the SRC application library CD, */webapp/accountAdmin.war*. You must install this component in your application server, such as JBoss, and configure the object reference for the account server.

The prepaid services demo supports two types of prepaid service applications, time based and volume based. Both types are limited in the demo to a single service being concurrently active per prepaid account. The account server maintains the accounts.

Account Server

The account server is the central data repository for the prepaid services demo. It maintains the different accounts and provides access for the other SRC components. The account server is a CORBA server with a data storage backend. In the prepaid services demo, data is stored on the local file system; in a real application you should use a relational database management system (RDBMS) for data storage.

The account server employs the SAE plug-in interface. The server publishes an object reference to a standard COS naming service or to a file in the local file system. It uses the managed accounts to authorize access to prepaid services and updates the accounts based on actual usage.

The model assumes that subscribers can log in and be authenticated. By default, all attempts to access the Internet are intercepted and captured by the portal. Subscribers pay for the service in advance of use by purchasing a valid access card. The subscriber then can activate the prepaid service. At activation, the portal prompts the subscriber for the account number and validates the access. The portal grants access if the account exists, has not expired, is not locked, and has a remaining balance (time or volume) greater than 0. When it grants access in response to a request, the account server locks the account against concurrent access. Charging starts as soon as the portal grants access.

Time-Based Services

Time-based services are sold by access time. These services have no limits placed on the data transmitted. For example, voice long distance service accounts are measured in connection time.

When it authorizes a time-based prepaid account, the account server sets the session timeout based on the current balance of the account. The account server locks the account when the session start is signaled. When the session stop is signaled, the account server updates the account based on the session time and unlocks it.

When the service stops (because the subscriber stops service on the portal, the subscriber logs out, or the session timeout expires), the account is unlocked, and its time balance is decreased by the session time.

Volume-Based Services

Volume-based services are sold based on upload or download data volume. For the demo application, volume is defined as the sum of the upload and download volumes. A real implementation might distinguish between the two for accounting purposes.

When it authorizes a volume-based prepaid service, the account server sets an interim update interval according to the following formula:

$$\text{interim update interval} = \frac{\text{remaining volume in account}}{\text{maximum bandwidth available to subscriber}}$$

The maximum bandwidth is the greater of the two plug-in attributes `upstreamBandwidth` and `downstreamBandwidth`. If you do not specify values for these attributes, then the maximum bandwidth defaults to 1 Mbps.

When the session start is signaled, the account server locks the account.

When an interim update is signaled, the account server updates the interim update interval based on the account balance and the current consumption. It compares the

volume used so far in the session with the remaining volume. If the session volume is greater than the remaining volume, the account server sets the session timeout to zero to stop the session.

If the session volume is less than the remaining volume, the interim update interval is recalculated, and no further action takes place until the end of that interval.

The interim update interval must be larger than a specified minimum value; the demo application employs a minimum of 5 minutes. This feature enables accounts to be overdrawn by an amount equal to the maximum bandwidth times the minimum time.

When the session stop is signaled, the account server updates the account based on the volume counters and unlocks it.

Installing and Configuring the Prepaid Services Demo

You must install and configure both the account server and the Prepaid Account Administration application. Additionally, you must configure the prepaid plug-in on the SAE and create and configure the service(s) that will use the prepaid accounts.

Installing the Account Server

You must manually install the UMCppdemo package to deploy the account server.

```
pkgadd -d /cdrom/cdrom0/Demos+Sample_Applications UMCppdemo
```



NOTE: The prepaid services demo is provided on the SRC application library CD.

For information about installing the prepaid services demo, see “Installing the Sample SRC Applications” on page 3.

Configuring the Account Server

Before you start the account server for the first time, you must run a script to configure it. To configure the account server:

1. On the SAE host, log in as root or as an authorized nonroot admin user.
2. Launch the configuration script from the prepaid services demo installation directory.

```
/opt/UMC/prepaid/etc/config
```

3. The configuration script prompts you for input and confirms your choices, as in the following example:

```
Which naming prefix shall be used for publishing the objects?
[demo/accountServer] [?,q]
demo/accountServer
Which naming server do you want to use? [] [?,q]
```

corbaname::localhost

Which file name prefix shall be used for publishing the objects? [] [?,q]

/var/tmp/accountServer

Which user-id shall be running the account server? [nobody] [?,q]

nobody

COSName: "demo/accountServer"

NameServer: "corbaname::localhost"

IORFile: "/var/tmp/accountServer"

USERID: "nobody"

Is this correct? **y**

4. The script configures the account server according to your responses.

Publishing the Object References

The sample configuration presented above configures the account server to publish the object references to a COS naming service and to a local file. Depending on your needs, you might want to choose only one or the other method.



NOTE: The account server and the Prepaid Account Administration application must run on the same host for the local file feature to work. If you install these components on multiple hosts, you must configure the account server to publish the object references to a COS naming service.

When you publish the objects to a COS naming service, you specify the prefix of the published name, such as `demo/accountServer`, and the URL of the name server, such as `corbaname::localhost`. In this case the account server publishes the object reference of the plug-in to the URL `corbaname::localhost#demo/accountServer.plugin`. The account server publishes the object reference of the account manager to the URL `corbaname::localhost#demo/accountServer.acctMgr`.

The local file is specified by the path and prefix of the filename, `/var/tmp/accountServer`. In this case the account server publishes the object reference of the account manager to `/var/tmp/accountServer.acctMgr` and the object reference of the prepaid plug-in to `/var/tmp/accountServer.plugin`.

Manual Configuration

Although the configuration script is sufficient to configure the account server for most purposes, you can also configure the server by using the command line.

- To publish the object references into a local file, specify the path and prefix of the filename:

```
#accountServer -f <fileNamePrefix>
```

- To publish the object references to a COS naming service, specify the prefix of the published name:

```
#accountServer -c <namePrefix>
```

- The COS naming server is taken from the initial references. You can do one of the following:

- Globally configure omniORB in the file */etc/omniORB.cfg*
- Specify the following option when you configure the account server:

```
-ORBInitRef NameService=corbaname::nameServerHostname
```

For example, to publish the object references to a COS naming server running on server ns.domain.com, configure the account server as follows:

```
#accountServer -ORBInitRef NameService=corbaname::ns.domain.com -c
demo/accountServer
```

- If you start the account server as a root user, the account server switches the user ID to an unprivileged user after initialization. The default user ID is nobody. To override the default value, specify a different user:

```
#accountServer -f /var/tmp/accountServer -u <username>
```

Starting the Account Server

To start the account server:

1. On the account server host, log in as root or as an authorized nonroot admin user.
2. Start the account server from the root directory.

```
/etc/init.d/accountServer start
```

The system responds with a start message.

Stopping the Account Server

To stop the account server:

1. On the account server host, log in as root or as an authorized nonroot admin user.
2. Stop the account server from the root directory.

```
/etc/init.d/accountServer stop
```

The system responds with a stop message.

Configuring the SAE for the Prepaid Plug-In

You configure the prepaid plug-in in the same way that you configure other SAE external plug-ins. For information about configuring SAE plug-ins, see *SRC PE Subscribers and Subscriptions Guide*

The properties for this plug-in are as follows.

Plugin.prepaid.objectref

- Specifies the reference of the plug-in object implemented by the account server.
- Value—Depends on the host and the configuration of the account server; that is, whether the object reference is published to a COS naming service or a local file
- Examples

In the following example, the object reference has been published to a COS naming service running on the host ns.domain.com:

```
Plugin.prepaid.objectref =
corbaname::ns.domain.com#demo/accountServer.plugin
```

In the following example, the object reference has been published to a local file on the host:

```
Plugin.prepaid.objectref = file:/var/tmp/accountServer.plugin
```

Plugin.prepaid.attr

- Defines the attributes used by the plug-in.
- Value—Use only the following value:
 Plugin.prepaid.attr = PA_UID,PA_AUTH_USER_ID, PA_SESSION_TIME,
 PA_DOWNSTREAM_BANDWIDTH, PA_UPSTREAM_BANDWIDTH

Configuring the Prepaid Services

Each defined service that uses prepaid accounts must be configured to use the prepaid plug-in as its authorization and tracking plug-in. For example, suppose you have a GameMaster premium gaming service for which you want to use prepaid accounts. You must create this service with SDX Admin and enter the value “prepaid” into the Authorization Plugin and Tracking Plugin fields.

Deploying the Prepaid Account Administration Application

You must deploy the WAR file for the Prepaid Account Administration application in the Web application server. You can find this file, *accountAdmin.war*, in the folder *webapp* on the SRC application library CD. Refer to the documentation for your Web application server for information about deploying applications.

For example, to deploy the Prepaid Account Administration application inside JBoss, copy the file to the JBoss */server/default/deploy* directory.

```
cp /cdrom/cdrom0/Demos+Sample_Applications/webapp/accountAdmin.war
/opt/UMC/jboss/server/default/deploy
```

JBoss automatically starts the application when a new WAR file is copied into the deploy directory.

Configuring the Prepaid Account Administration Application

You must configure the Prepaid Account Administration application with the object reference of the account manager. Configure the object reference as a `<context-param>` in the `WEB-INF/web.xml` file from the `accountAdmin.war` file. The parameter name is `acctMgr`, and the value is a CORBA URL of the account manager object reference, as in the following example:

```
<context-param>
  <param-name>acctMgr</param-name>
  <param-value>corbaname::ns.domain.com#demo/accountServer.acctMgr
</param-value>
</context-param>
```

Managing Prepaid Accounts

Use the Prepaid Account Administration application to manage prepaid accounts.

Accessing the Prepaid Account Administration Application

To access the Prepaid Account Administration application, enter the following in your Web browser:

`http://<host>:8080/accountAdmin`

where `<host>` is the name or IP address of the workstation on which you installed the Prepaid Account Administration application.

The Prepaid Account Home page appears.

Administering Accounts

On the Prepaid Account Home page, you can select to list, create, update, or clear accounts.

- Listing an Account—You can display summary information for accounts. You can also display the state of an account selected by its account number.
- Creating an Account—On the Create Accounts page, you can create multiple similar accounts simultaneously, but all must have the same type (time or volume), balance, and expiration (expiry) date.

Specify the expiration date in the format `YYYYMMDD`. You can optionally specify an expiration time after the date in the format `HHmm`. If you do not specify a time, the account expires at midnight on the specified date. For example, to set the expiration for July 21, 2004 at 08:35 a.m., specify the following in the Expiry Date field:

200407210835

After completing the account fields, click OK to create the account(s).

- Updating an Account—On the Update Accounts page, you can manually credit an account, extend its expiration date, or unlock it.
- Clearing an Account—On the Clear Accounts page, you can delete expired accounts.

Part 6

Managing Access Portals for Residential Subscribers

- Overview of the Residential Portal on page 117
- Installing and Configuring the Sample Residential Portal on page 121
- How Subscribers Use the Sample Residential Portal on page 133
- Developing a Residential Portal on page 153

Chapter 12

Overview of the Residential Portal

- How Subscribers Use a Residential Portal on page 117
- Overview of a Residential Portal on page 118
- Subscriptions to Services on page 118
- Service Schedules in a Residential Portal on page 119
- Equipment Registration for DHCP Login on page 119
- Overview of the Sample Residential Portal on page 119

How Subscribers Use a Residential Portal

A residential portal is a Web application designed for use by individual subscribers who use their own computer to connect to the network, or households composed of multiple subscribers who use one or more computers and share the same network connection. The portal can be the single access point for subscribers to log in to the Internet. In addition to Internet access, a residential portal lets users manage subscriptions to services that supplement their basic Internet access package.

Residential portals can be used in wire-line, wireless, and roaming wireless environments:

- Fixed access environment—Subscribers can connect to a wholesaler or retailer using PPP, static IP, or DHCP through media such as cable, DSL, or telephone wire-line connections.

For DHCP connections that do not use equipment registration, PPP connections, or static IP connections, subscribers establish connections to a specific provider. If they want to connect to a different provider, subscribers log out of the current connection, and then log in to another one.

- Local wireless environment—Subscribers registered with the local wireless operator can connect to the location, typically by using DHCP.
- Roaming wireless environment—Subscribers can log in at a variety of wireless locations owned by service providers that participate in a roaming network agreement. Typically the connections use DHCP.

In each of these scenarios, the subscriber's experience is similar:

1. The subscriber connects to and logs in to an access point.
2. Based on the login, the subscriber's user profile is retrieved, and services are started on the router.
3. The subscriber's Web browser is redirected to a home or start page for the residential portal.
4. After logging in to the portal, subscribers can manage the services available from the provider.

Overview of a Residential Portal

Typically a residential portal is composed of dynamic Web pages that reference classes and methods from the Java packages and the Common Object Request Broker (CORBA) remote application programming interface (API) to:

- Authenticate subscribers, and log subscribers in to and out of the portal.
- Specify which services are to be available to subscribers.
 - Specify whether scheduling is available to subscribers and, if so, which scheduling features are available.
 - Specify whether the services start automatically at portal login or whether these services are to be started manually by the subscriber.
- Show subscribers accounting statistics for services that are active.
- Allow the subscribers to register their client devices to automatically obtain an authenticated IP address when they log in to the portal.

To use the SRC software to handle unauthorized requests to Web services and Web content sites, you install and configure the captive portal system, see “Redirecting Traffic to a Captive Portal Web Page” on page 154.

Subscriptions to Services

A residential portal lets subscribers manage subscriptions to additional services that a service provider makes available to subscribers. These services could provide additional bandwidth, access to specified content providers, or other services configured in the SAE.

Using a residential portal simplifies how service providers deliver services and how subscribers gain access to these services. The service provider can make services available to subscribers without directly contacting them, and subscribers can start and stop available services without contacting the service provider. Service providers can also charge for any service that a subscriber uses, based on the type of service and how long the subscriber uses the service. Through a residential portal, the service provider can provide information to subscribers about the cost and use of these services.

Service Schedules in a Residential Portal

A residential portal can allow users to subscribe to a service at scheduled times. For example, if a subscriber regularly views video every morning, the subscriber can set up a schedule to turn on a video-on-demand gold service (that is available from the service provider) every weekday morning at 9 a.m., and turn it off on the same day at 10:30 a.m. This way the subscriber has access to additional bandwidth only for the interval needed and pays for this service accordingly.

Equipment Registration for DHCP Login

The residential portal provides support for equipment registration for DHCP connections. Registration lets a subscriber automatically obtain an authenticated IP address when logging in to the portal. The equipment can be a device other than a PC, such as an IP phone or a set-top box. If a subscriber uses equipment registration and enables persistent login, the subscriber's authentication remains valid until the subscriber logs out of the system.

Overview of the Sample Residential Portal

The sample residential portal is a demonstration portal that shows how to use some of the features available in the Common Object Request Broker Architecture (CORBA) remote application programming interface (API) to create a Web application. You can customize the sample residential portal for your environment, or create a new Web application using the SAE CORBA remote API.

Web Application Architecture

The sample residential portal uses the Jakarta Struts Web application framework. Although Struts provides an easy and extensible framework for building Web applications, it is not required for building portals that use the CORBA remote API.

Jakarta Struts supports the model-view-control design paradigm, which separates an application into three sets of components:

- Model—Contains the data and business logic.
- View—Contains the presentation to the subscriber.
- Control—Contains the interface procedures.

The strict separation of the three layers promotes reuse of the components and allows easy adaptation of the application to different requirements.

Model Components

The model provides an abstraction layer of the CORBA remote API and contains the business logic, which determines how the sample portal behaves. The sample residential portal includes several implementations of the model (which we call

behaviors) to demonstrate some typical usage scenarios. See “Behaviors for the Sample Residential Portal” on page 120 for more information.

View Components

The view components of the Web application provide the HTML code sent to the subscriber’s browser. The view is implemented by means of JavaServer Pages (JSP) and several tag libraries provided as part of Jakarta Struts.

The tiles tag library provides a template mechanism to build Web pages based on reusable partial pages. The general layout of all pages of the portal application is defined in a single JSP page.

Control Components

The control components provide the interactions between the subscriber and the mode through the Action and ActionForm classes.

Action classes implement the functionality for a single operation, such as “ list the subscriptions of a particular service category,” or “ activate a service.”

ActionForm classes encapsulate data provided by the subscriber on an input form. The Struts framework initializes these classes with data entered in an HTML form and passes them to the appropriate action. The ActionForms are then passed to a view component that uses the data to initialize the content of fields in an input form.

Behaviors for the Sample Residential Portal

The sample residential portal provides the following user behaviors (scenarios):

- Equipment registration

Used by subscribers who use Dynamic Host Configuration Protocol (DHCP) connections to register their devices to receive an authenticated IP address.

- Internet Service Provider (ISP) service

Used by subscribers who use Point-to-Point Protocol (PPP), static IP, or unauthenticated DHCP connections to log in to the portal and receive an unauthenticated IP address.

- Cable

Used by subscribers who have assigned IP addresses in a PacketCable Multimedia (PCMM) environment.

Chapter 13

Installing and Configuring the Sample Residential Portal

- Before You Install and Configure the Sample Residential Portal on page 121
- Overview of Configuration Files for the Sample Residential Portal on page 123
- Installing the Sample Residential Portal on page 129
- Removing Access to the Sample Residential Portal on page 131

Before You Install and Configure the Sample Residential Portal

Before you install and configure the sample residential portal:

- Decide which behavior model the portal will use:
 - Equipment registration behavior—The equipment registration example demonstrates an application that provides an association between a subscriber and the equipment being used to make the DHCP connection. This type of association is used in many cable environments.
 - ISP service behavior—The ISP service example demonstrates an application that provides a means for subscribers to directly log in to a subscriber session for their ISP. The ISP service behavior is well suited for any environment in which subscribers connect directly to their ISP.
 - Cable behavior—The cable behavior is provided for a PCMM environment in which an application creates a subscriber session.
- (Optional) Set up subscriber authentication through RADIUS at portal login.
- (Optional) Customize how the sample residential portal handles unrecognized IP subscribers.

Configuring Equipment Registration and ISP Service Behaviors

The equipment registration and ISP portal behaviors use a RADIUS server for authentication and authorization. The Juniper Networks database and the add-on packages for other supported directories include sample data to authenticate portal logins. RADIUS servers can be configured to use these directories.

The version of Steel-Belted RADIUS in the SRC software distribution is preconfigured to use the SRC sample data to authenticate the domains for the sample residential

portal. In the Steel-Belted RADIUS configuration, identify the host on which the directory is running if the host (if it is not localhost).

Configuring Cable Behavior

For a PCMM environment, you can create an application to create a subscriber session by either:

- Using the event API to integrate an IP address manager such as a DHCP server or a RADIUS server.
- Having the application provide the IP address, the associated interface name, and virtual router name for the subscriber making the request. Typically, the IP address is used to identify the associated virtual router.

If the application provides the subscriber IP address and associated information, you can configure the portal application to locate the SAE that manages the subscriber session by configuring one of the following:

- Network information collector (NIC)
 - NIC host that resolves a subscriber IP address to name of the virtual router managing the IP address and an SAE interoperable object reference (IOR)
 - NIC proxy for the application to communicate with the NIC host
- A local feature locator in the properties for the residential portal. See “WEB-INF/portalBehavior.properties” on page 123 .

Authenticating Subscribers Through RADIUS

If you use RADIUS to manage subscriber data, you can use RADIUS to authentication subscribers when they log in to a residential portal. You configure RADIUS authentication plug-ins to provide RADIUS authentication or authorization. In the configuration for the plug-in, you specify how the SAE handles RADIUS attributes received from the RADIUS server.

Because the SAE rather than a JUNOS router receives the authentication response, you can specify that the response include attributes other than serviceBundle and class, and you can specify more than value for the RADIUS class attribute.

To authenticate subscribers through RADIUS at portal login:

1. Create a RADIUS authorization plug-in to authenticate subscriber sessions.
2. Configure the RADIUS authorization plug-in to specify:
 - The RADIUS attributes to be set in an authorization response
 - The action to be taken in response to the attribute values received

For example, you could create a RADIUS authorization plug-in to:

- Authenticate a PPP subscriber session on a JUNOS router
- Specify the setLoadServices value for the serviceBundle attribute

By default, the flexible RADIUS authentication plug-in defines this attribute as:

```
RadiusPacket.stdAuth.userresp.vendor-specific.Juniper.Service-Bundle =
    setLoadServices
```

For more information about RADIUS authentication plug-ins, see *SRC PE Subscribers and Subscriptions Guide*.

Customizing How the Sample Residential Portal Handles Unrecognized IP Subscribers

By default, the sample residential portal sends unrecognized IP subscribers to a login page rather than to an error page.

To customize how unrecognized IP subscribers are handled:

- Edit the *struts-config.xml* file.

Overview of Configuration Files for the Sample Residential Portal

The *ssportal.war* file contains the following configuration files in the *WEB-INF* directory:

- *portalBehavior.properties*—Specifies properties to configure the *portalBehavior* servlet that determines the behavior of the sample residential portal.

Modify this file to run the sample residential portal. See “WEB-INF/portalBehavior.properties” on page 123 .

- *web.xml*—Specifies the deployment descriptor for the sample residential portal. It describes the servlets, other components, and initialization parameters.



NOTE: We recommend that you do not change the deployment descriptor.

- *jboss-web.xml*—Contains one configuration property that defines the Web context of the sample residential portal as the root context.

Modify this file to run the sample residential portal in a context other than root. The *WEB-INF/jboss-web.xml* file is proprietary to the JBoss application server.

- *struts-config.xml*—Contains the configuration for the struts action servlet. See WEB-INF/struts-config.xml on page 125 .
- *tiles-defs.xml*—Contains the definitions of the tiles template system. The definitions describe the general layout of every Web page used in the sample residential portal. See WEB-INF/tiles-defs.xml on page 128 .

WEB-INF/portalBehavior.properties

Set the following properties to configure the *portalBehavior* servlet to determine the behavior of the sample residential portal, and to connect to the LDAP server.

In addition, configure the other properties listed in the file for the network information collector (NIC) proxy configuration. For information about the values to configure for NIC properties, see *SRC PE Network Guide* .

Factory.behavior

- Model for handling subscribers who connect using DHCP.
- Value
 - `net.juniper.smgmt.ssp.model.EquipmentRegistrationBehavior`
 - `net.juniper.smgmt.ssp.model.ISPServiceBehavior`
 - `net.juniper.smgmt.ssp.model.CableBehavior`
- Guidelines—For information about the behaviors, see “Installing the Sample Residential Portal” on page 129 .

Factory.locator

- Method that the portal uses to locate the SAE that is managing the subscriber who tries to access the application.
- Value
 - `net.juniper.smgmt.ssp.LocalFeatureLocator`—Uses the locally configured object reference

If you specify `net.juniper.smgmt.ssp.LocalFeatureLocator`, configure a value for `LocalFeatureLocator.objectRef`.
 - `net.juniper.smgmt.ssp.DistributedFeatureLocator`—Uses NIC configuration

LocalFeatureLocator.objectRef

- CORBA object reference for the single SAE whose address is resolved by the locator. Specify the object reference if you set `net.juniper.smgmt.ssp.LocalFeatureLocator` for `Factory.locator`.
- Value—A reference to the CORBA object in one of the following formats:
 - The absolute path to the IOR file in the form `file:// <absolutePath>`
 - The corbaloc URL in the format:

`corbaloc:: <host> : <port> /SAE`

 - `<host>` — IP address or host on which the SAE is installed.
 - `<port>` —TCP/IP port number for the SAE. The default is 8801.
 - COS naming service in the format:

`corbaname:: <host> [: <port>][/NameService]# <key>`

where `<key>` is provided by the publisher of the IOR to the COSnaming service.
 - The actual IOR in the form `IOR: <objectReference>`

- Guidelines—Configure this property to use the portal as a demonstration application in a small environment that does not use NIC.

By default, the SAE does not publish its IOR to a COSNaming service.

- Example
 - Absolute path—file:///opt/UMC/sae/var/run/sae.ior
 - corbaloc URL—corbaloc::10.10.6.171:8801/SAE
 - Actual IOR—
IOR:0000000000000002438444C3A736D67742E6A756E697...

LocalFeatureLocator.vrName

- Virtual router to use in a Packet Cable Multimedia (PCMM) environment as the virtual router on the local machine.
- Value—Name of virtual router
- Guidelines—Configure this property only if you configured a value for LocalFeatureLocator.objectRef.
- Default—default@simJunos

DistributedFeatureLocator.locName

- Namespace for the NIC proxy configuration.
- Value— < namespace >
- Guidelines—For the cable behavior to create an assigned IP subscriber, the NIC must resolve an IP address to both the SAE IOR and the name of the virtual router that manages the IP address.
- Default—/ which indicates the root namespace
- Example—DistributedFeatureLocator.locName = /nicProxy indicates that the NIC proxy configuration is in /nicProxy.

Config.java.naming.provider.url

- Location of the LDAP server.
- Value—ldap:// < IP address > : < port number >
- Example—ldap://127.0.0.1:389 (default location if you are using the default OpenLDAP installation from the SRC installation).

Config.net.juniper.smgmt.des.backup_provider_urls

- Location of a backup LDAP server.
- Value—ldap:// < IP address > : < port number >

WEB-INF/struts-config.xml

The *WEB-INF/struts-config.xml* file contains the following settings. The file has multiple sections.

data-sources

- Not used by the sample residential portal.

form-beans

- Holds data entered in an HTML form and makes it available to the associated action.

global-exceptions

- Specifies that the sample residential portal declare one global exception handler, which is invoked for any exception raised during action processing.

global-forwards

- Global forwards for handling error situations. The sample residential portal declares a number of global forwards.
- Value
 - `unknownUser`—Used when an action is processed for a subscriber who is not known by the system. The possible pages are either *.error.unknownUser.page*, which displays an error message, or *.login.page*, which asks the user to log in.
 - `nonUniqueUser`—Used when a request cannot be mapped to a single subscriber session.

The sample residential portal uses the IP address of the subscriber, preventing this error.

- `unknownService`—Used when a request refers to a service that is not loaded by the SAE. This can happen if services are modified while subscribers are connected to the portal.
- `unknownSubscription`—Used when a request refers to a service to which the current subscriber is not subscribed.
- `serviceAuthError`—Used if authorization for a service is denied; for example, because mutex group restrictions are violated or a plug-in has denied authorization.
- `loginError`—Used if login was unsuccessful.
- `saeError`—Used for SAE internal errors.
- `error`—Used for any other problem.

action-mappings

- Actions that each correspond to an interaction of the subscriber with the portal page. The sample residential portal declares a number of actions.
- Value

- `/index`—Displays the main page of the portal; collects information about the subscriber requesting the page and forwards it to the `.index.page`.
- `/services`—Gets information about the subscribed services and forwards to the `.services.page`.
- `/activate`—Checks whether authentication is required and forwards the request either to the `.service.auth.page` or back to the `.services.page`.

Called when the subscriber wants to activate a service.

- `/deactivate`—Forwards the request back to the `.services.page`.

Called when the subscriber wants to deactivate an active service.

- `/schedules`—Gets information about the service schedule. Allows the subscriber to view and change service schedules. The action forwards the request to the `.schedules.page`.
- `/scheduleOperation`—Forwards the request back to the `.schedules.page`.

Called when the subscriber wants to change the service schedule.

- `/usage`—Collects statistics for currently active services and forwards them to the `.usage.page`.
- `/account`—Allows modification of the `activationTrigger` property of currently subscribed services. After a change of the `activationTrigger` property has been processed, the action forwards subscribers to the `.account.page`.
- `/subscribe`—Allows the subscriber to subscribe to and unsubscribe from services. After processing the subscription change, the action forwards subscribers to the `.subscribe.page`.
- `/register`—Allows subscribers to register MAC addresses for authenticated DHCP addresses. The action checks whether the subscriber has provided a username and password and forwards the request to the `.register.auth.page` to enter the username and password or to the `.register.page` displaying the currently registered equipment.
- `/unregister`—Allows subscribers to remove MAC addresses that are registered for DHCP addresses. The action checks whether the subscriber provided a username and password and forwards the request to the `.unregister.auth.page` to enter the username and password or to the `.unregister.page` displaying the currently registered equipment.
- `/login`—Allows the subscriber to log in to the system. If the login causes a switch of the DHCP IP address, the request is forwarded to the `.wait.page`. If the DHCP IP address remains the same after the login, the request is forwarded to the `.index.page`.
- `/logout`—Allows the subscriber to log out of the system. If the logout causes a switch of the DHCP IP address, the request is forwarded to the `.wait.page`. If the DHCP IP address remains the same after the login, the request is forwarded to the `.index.page`.

- `/wait`—Checks whether the IP address of the current subscriber is authenticated or unauthenticated. If the address is of the wrong type, the request is forwarded to the `.wait.page`, which will renew itself automatically. If the address is of the expected type, the request is forwarded to `.index.page`.
- `/accessDenied`—Processes a captive portal request. The request is forwarded only to the `.error.accessDenied.page`.

controller

- Ensures generation of the correct headers for disabling caching of the generated pages.
- Value—`nocache`

message-resources

- Base name of the resource bundle. The resource bundle contains message strings in different languages.
- Value
 - `WEB-INF/classes/net/juniper/smgmt/ssp/ApplicationResources.properties`
 The location of the resource file containing messages in English that is shipped with the sample residential portal.
 - `WEB-INF/classes/net/juniper/smgmt/ssp/ApplicationResources_xx.properties`
 where `xx` is the two-letter ISO language code, optionally followed by an underline and the two-letter country code; for example, `en_CA` for English/Canada or `zh_TW` for Chinese/Taiwan.

 To create a sample residential portal that supports other languages, translate the messages and store the translated file in the above location.

plug-in

- Processes templates.

WEB-INF/tiles-defs.xml

The `WEB-INF/tiles-defs.xml` file contains the following settings.

site.layout

- Main definition that specifies the general structure of all pages. The layout is based on a common template file, `/layouts/common.jsp`. The definition contains values for template variables shared by all page definitions.
- Value
 - `title`—Common title of all pages.
 - `header`—Page fragment displaying the header section of the pages.
 - `menu`—Page fragment displaying the menu bar.

- footer—Page fragment displaying the footer section of the pages.
- body—Page fragment displaying the content of the pages. The default setting is empty and should be overwritten by individual page definitions.
- color—Color scheme used the by pages. A color scheme consists of a style sheet (*style_sheets/color.css*) and a set of images (stored in *images/color*). The predefined color schemes are blue and green.
- menuTag—Action name of the current page. The menu bar code uses this tag to highlight the action associated with the current page.

site.layout.nomenu

- Provides an extension of the main layout that defines a version of the page without a menu bar.

.*.page

- Provides the definition of portal pages. These pages are used for forwards in the action-mappings section of the *struts-config.xml* file. The page definitions extend one of the common layouts and define the value of the body variable as appropriate.

Installing the Sample Residential Portal

The sample residential portal is a Web application. The application is packaged as a standard Web application archive (WAR file) in the *webapp* subdirectory in the SRC software distribution.

Before you install the sample residential portal:

- Install a Web application server on the machine on which you want to install the sample residential portal.
- Install the sample data from the SRC software distribution. See Loading Sample Data in to a Juniper Networks Database (SRC CLI).
- Set up the RADIUS *authfile* for the user scenario you want to demonstrate. See “Installing the Sample Residential Portal” on page 129 .

Tasks to install the sample residential portal are:

1. “Preparing the Application for Customization” on page 130
2. “Configuring the Sample Residential Portal” on page 130
3. “Deploying the Updated WAR File” on page 130



NOTE: The sample residential portal can be installed by root or authorized nonroot users.

Preparing the Application for Customization

When you customize the sample residential portal, copy the WAR file to a temporary folder and work in that folder. To do so:

1. Login as root or another authorized user.
2. Create a temporary folder in which you will work on the WAR file.

```
mkdir ssportal
```

3. Access the temporary folder.

```
cd ssportal
```

4. Copy the WAR file to the temporary folder.

```
cp /cdrom/cdrom0/Demos+Sample_Applications/webapp/ssportal.war.
```

Configuring the Sample Residential Portal

To configure the sample residential portal:

1. Access the temporary folder to which you copied the WAR file.

```
cd ssportal
```

2. Extract the files from the WAR file.

```
unzip -quo ssportal.war
```

3. With a text editor, edit the *portalBehavior.properties* file and other files in the *WEB-INF* directory as needed. See “Overview of Configuration Files for the Sample Residential Portal” on page 123 .

Use “WEB-INF/portalBehavior.properties” on page 123 as a guideline for editing the *portalBehavior.properties* file to use properties specific to your environment.

4. Replace the *portalBehavior.properties* and any other updated files in the WAR file.

```
zip -u ssportal.war
```

Deploying the Updated WAR File

To deploy the updated WAR file:

- Copy the WAR file to the deployment directory for your Web server.

If you are using JBoss, copy the file to `/opt/UMC/jboss/server/default/deploy` directory. JBoss automatically starts the Web application when a new WAR file is copied into the deployment directory.

By default the sample residential portal is deployed into the root context (“/”). You can access the portal through `http://server:8080`. If you want to deploy the sample residential portal into something other than the root context, modify the `WEB-INF/jboss-web.xml` configuration file.

Testing a Portal Application

Simulated router drivers allow you to create subscriber sessions without connecting to a router. You can use a simulated router drive when you want to test your portal application. See *SRC PE Monitoring and Troubleshooting Guide*.

Removing Access to the Sample Residential Portal

To remove access to the sample residential portal:

- Remove the `ssportal.war` file from the deployment directory.

Chapter 14

How Subscribers Use the Sample Residential Portal

- Overview of the Sample Residential Portal on page 133
- Before You Use the Sample Residential Portal on page 133
- Logging In to the Sample Residential Portal Using a Simulated User Profile on page 133
- Managing Services from the Sample Residential Portal on page 136
- Logging Out of the Sample Residential Portal on page 149
- Using the Sample Residential Portal from PDAs on page 150

Overview of the Sample Residential Portal

The sample residential portal allows subscribers to manage subscriptions to services that supplement their basic Internet services. The sample residential portal shows how subscribers could log in to a portal, start and stop supplementary services, and manage subscriptions for their special services. The services available in the sample residential portal are configured in the sample data.

If you are a portal developer and want to view the Javadoc documentation for the sample portal, you can access the documentation from the Welcome page of the sample residential portal after you log in to the portal.

Before You Use the Sample Residential Portal

Before you can log in to the sample residential portal, the portal must be configured for use in your environment. For information about installing and configuring the sample residential portal, see “Installing and Configuring the Sample Residential Portal” on page 121.

Logging In to the Sample Residential Portal Using a Simulated User Profile

Logging in to the sample residential portal requires that you enter the username and password for a subscriber. You can log in to the sample residential portal by using a simulated user profile in a test environment, or you can log in as a subscriber in an environment that includes a JUNOS router or a JUNOS routing platform. If you

add a subscriber to the directory, do so under a retailer below the folder *o = Users*, *o = umc*.

If you want to use a simulated user profile to log in to the sample residential portal, you can use one of the subscribers in the sample data, or a subscriber that you create. Before you can log in to the sample residential portal, you log the subscriber in to a simulated user session from the SRC CLI. For information about using a simulated user profile. See *SRC PE Monitoring and Troubleshooting Guide*.

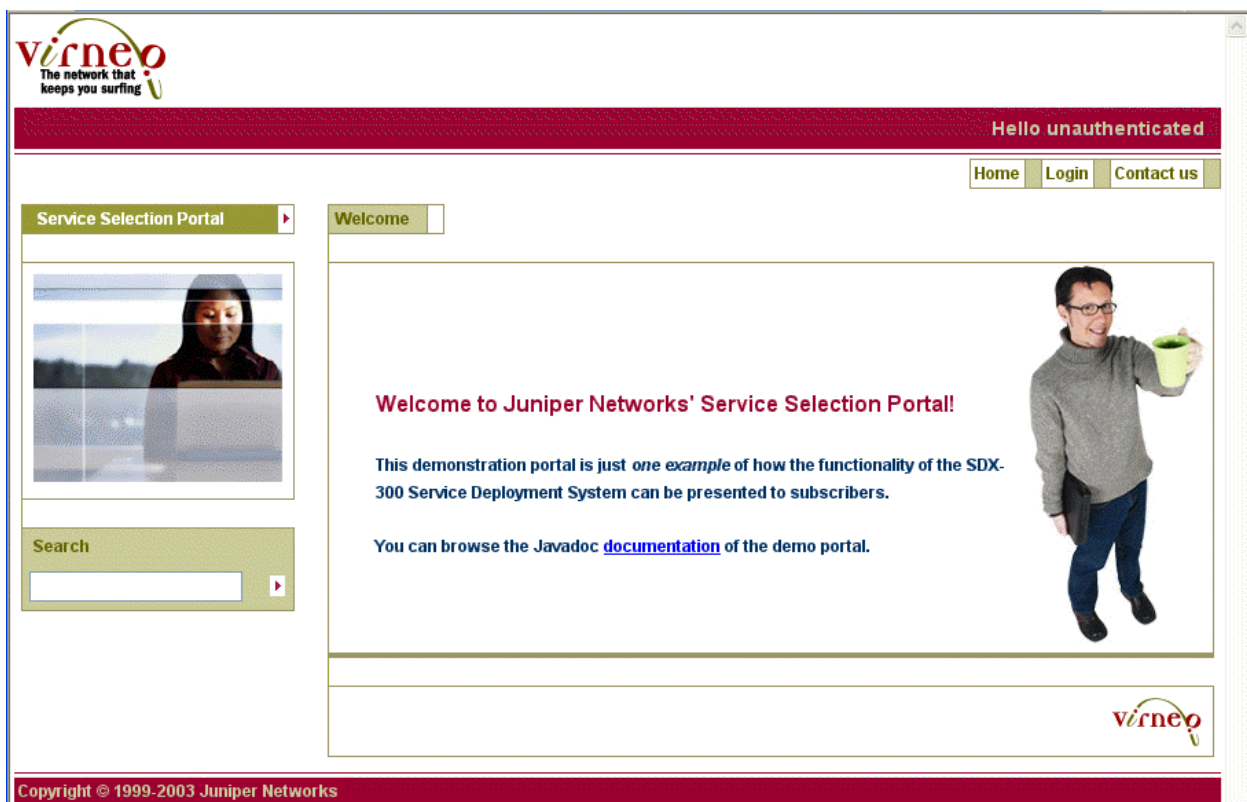
Logging In to the Sample Residential Portal

To log in to the sample residential portal:

1. Connect to the sample residential portal from a Web browser.

The default URL for the sample residential portal is `http://< IP address of Web server > :8080`.

The Welcome page appears.



2. Click **Login**.

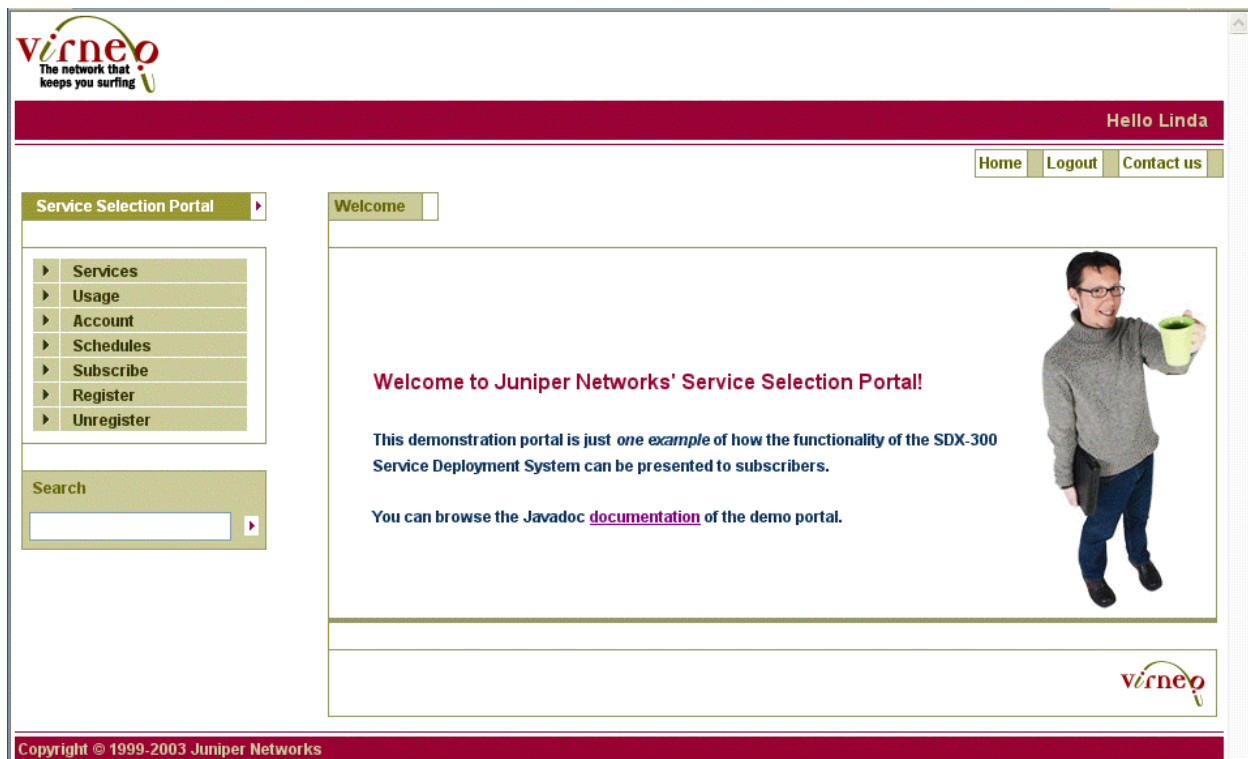
The Login page appears.



NOTE: The Sign up, Click here, and Search links are not operational in the sample portal.

3. Enter your username and password; then click **Login**.

Your personalized Welcome page appears.



Managing Services from the Sample Residential Portal

After you log in to the portal, you can use the portal in the same way that a subscriber would use it. This section describes how to use the sample residential portal from a subscriber's viewpoint.

Use the navigation pane on the left side of the page to move from one page to another.

You can set up, activate, and schedule additional services. These services supplement your basic Internet services, and may carry additional fees.

If you use DHCP to receive an IP address, you can also manage equipment registration.

Table 9 on page 136 describes the tasks that you can perform in the sample residential portal and shows which item to select in the navigation pane to display the page that lets you perform the task.

Table 9: Navigation Pane for the Sample Residential Portal

To Do This	Select This Item in the Navigation Pane
Start and stop supplementary services.	Services
View the price of a supplementary service.	

Table 9: Navigation Pane for the Sample Residential Portal *(continued)*

To Do This	Select This Item in the Navigation Pane
View service statistics for traffic sent and received during your login session.	Usage
View the list of services made available to you by the Internet service provider. The list shows whether a service is automatically activated at login or whether you need to activate the service from the portal.	Account
Change the type of service activation from this page.	
Specify a schedule that indicates when a specified service should be activated and/or deactivated.	Schedules
View and change the services to which you subscribe.	Subscribe
If you are a DHCP user, register your DHCP equipment to always obtain an authenticated IP address.	Register
If you have equipment registration enabled, disable it.	Unregister

Starting and Stopping Services

You can start and stop services to which you have a subscription. You can view which supplementary services the Internet service provider makes available to you in the Subscribe page, and subscribe to services there. After you subscribe to a service, the Services page lists the service. See “Subscribing to Services” on page 145 .

To start or stop services:

1. In the navigation page, click **Services**.

The Services page appears.

Virneo
The network that keeps you surfing

Hello Linda

Home Logout Contact us

Service Selection Portal

- Services
- Usage
- Account
- Schedules
- Subscribe
- Register
- Unregister

Search

Services

You can start or stop a service by clicking on the circle in the "Status" column. A green circle (🟢) means the service is currently on. A red circle (🔴) means the service is currently off.

You can persistently activate a service by clicking on the check box in the "Persistent" column. Persistently activated services are automatically activated when you login to the portal.

Audio Internet News Video

Service Description	Status	Password required	Persistent	Price
Example for content provider allowing gold audio access	🔴		<input type="checkbox"/>	N/A

Virneo

Copyright © 1999-2003 Juniper Networks

2. Click the tab that specifies the type of service to start or stop.
3. In the page that lists the service:
 - To start a service, click the red circle under Status.
 - To stop a service, click the green check mark under Status.
4. If a password is required to start a service, enter your password at the prompt.
5. To have a service become active when you log in to the portal again, click **Persistent** before you start the service.

If you specify a schedule for a service, that service is active as defined in the schedule and may remain active after you log out of the portal. See "Setting Up Service Schedules" on page 140 .

Getting Usage Information

From the portal, you can view information about how long a service has been active and can view traffic statistics for your current login session. Internet service providers could use this type of information to generate accounting data for specified services, such as a video gold service that would support video on demand.

To get usage information for your current login session:

1. In the navigation pane, click **Usage**.

The Usage page appears.

virneo
The network that keeps you surfing

Hello Linda

Home Logout Contact us

Service Selection Portal Usage

Services
Usage
Account
Schedules
Subscribe
Register
Unregister

Search

Accounting data for each of your subscribed services is listed below.

This information describes your *most recent* use of each service during your *current* login session. The status column shows a green circle for an active service or a red circle for a non active service. The time column shows the time at which the data was collected from the network.

Audio Internet News Video

Service description	Status	Been active for	Time	Bytes out	Bytes in	Packets out	Packets in
Example for content provider allowing gold audio access	●	0 sec	Never				

virneo

Copyright © 1999-2003 Juniper Networks

2. Click the tab that specifies the type of service for which you want usage information for your current login session.

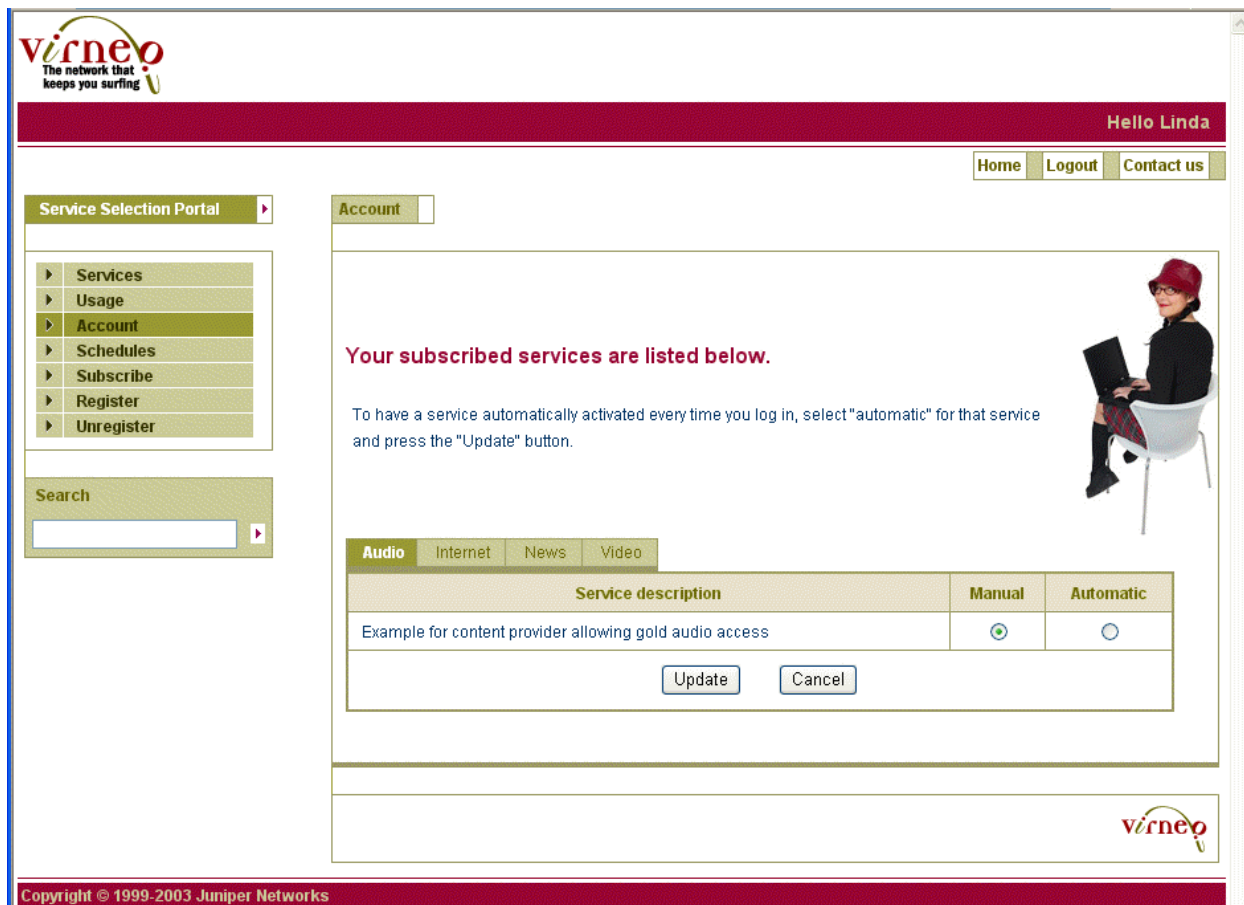
Setting Up the Type of Service Activation

You can have a service activated every time you log in to the portal, or you can activate it from the Services page when needed.

To view information about service activation and change how a service is activated:

1. In the navigation pane, click **Account**.

The Account page appears.



2. Click the tab that specifies the type of service that you want to view or for which you want to change the type of activation:
 - To start a specified service when you connect to your Internet service provider, click **Automatic**.
 - To start a specified service only when you want it to become active, click **Manual**.
3. Click **Update**.

Setting Up Service Schedules

You can set up schedules to activate specified services and deactivate specified services at fixed times. The schedules operate independently of whether you are logged in to the portal. For example, you could set up a schedule that activates a video gold service at 12 noon on every Saturday and deactivates the service at 12 midnight on the same day.

To create a service schedule:

1. In the navigation pane, click **Schedules**.

The Schedules page appears.

Virneo
The network that keeps you surfing

Hello Linda

Home Logout Contact us

Service Selection Portal

- Services
- Usage
- Account
- Schedules**
- Subscribe
- Register
- Unregister

Search

Schedules

Your current schedule is shown below.

You can add new events to your schedule, or delete scheduled events. You can also view the detail information about each of your scheduled events.

ThisMonth EventList

Schedule Name	Action
You have no schedules events for the given period.	

Main

Name:

Schedule Cancel

Schedule

	Year	Month	Day	DOW	TZ
from	2004	9	23	*	*
	Hour: *	Minute: 0,30			
to	Year: *	Month: *	Day: *	DOW: *	TZ: *
	Hour: *	Minute: *			

Actions

Order	Operation	Service
0	Please Select	Please Select

2. In the Name field, specify a name for the schedule.
3. Under Schedule, specify the time to start the service under *from*, and the time to stop the service under *to*.

For information about the type of information to enter in these fields, see “Specifying Values for Times” on page 142 and “Setting Times” on page 142 .

4. Under Actions, specify the operation to be performed for the service that you select under **Service**.

For information about the type of information to enter in these fields, see “Setting Actions” on page 144 .

5. After you finish making all schedule entries, click **Schedule**.

The schedule appears under EventList, and the schedule of actions for this month appears under ThisMonth.

Specifying Values for Times

When you create or change schedules, you can use the values in the following list to make entries in the from and to sections in the Schedules page. See “Setting Times” on page 142 for a description of each entry field under the Schedule area of the page.

- Asterisks (*) are interpreted differently depending on the field in which you enter one as a value. The following list describes how the SRC software interprets an * as a value for the various fields:
 - Minutes and hours—0 (zero)
 - Time zones—Local SAE time zone
 - All other fields—First through last
 - For fields in the To section of the schedule area, * for the end time is equivalent to “ deny service activation after this start date.”
 - For dates in the From section of the schedule area, * is equivalent to “ deny service activation anytime before this end date.”
- Range of numbers or letters separated by a hyphen—The range is inclusive; for example, 1-5 for the hour specifies hours 1, 2, 3, 4, and 5. A range of mon-wed specifies Monday, Tuesday, and Wednesday.
- List of numbers, letters, or ranges separated by commas—For example, 1,2,5,9 or 0-4,8-12 or mon-wed,fri-sat.
- Skip values in ranges.
 - Skip a number’s value through the range, follow a range with / < number > . For example, 0-23/2 used in the hours field specifies that the event occurs every other hour.
 - Skip values with *. If you want to specify every two hours, use */2.



NOTE: If you set both a day of the month and a day of the week, the day of the month is used.

Setting Times

Use the following field definitions when you make entries in the from and to sections in the Schedules page. For information about general guidelines that apply to these entry fields, see “Specifying Values for Times” on page 142 .

Year

- Year in which to schedule an action.
- Value—Four integers that indicate the year
- Default— *

Month

- Month of the year in which to schedule an action.
- Value
 - 1–12
 - First three letters of the name of the month
- Default— *
- Example—For January, specify one of the following:
 - jan
 - 1

Day

- Day of the month in which to schedule an action.
- Value—1–31
- Default— *

Hour

- Hour of the day in the indicated month in which to schedule an action.
- Value—0–23
- Default— *

Minute

- Number of minutes past the indicated hour in which to schedule an action.
- Value—0–59
- Default— *

DOW

- Day of the week in which to schedule an action.
- Value
 - 0–6, with 0 representing Sunday, and each subsequent number representing the next day of the week.
 - First three letters of the name of the day
- Default— *
- Example—For Saturday and Sunday, specify one of the following:
 - sat, sun

- 6, 0

TZ

- Time zone to use in the schedule.
- Value
 - * —Local time zone of the SAE.
 - An offset to Greenwich Mean Time (GMT) in the format:
 GMT (+ | -) (hh:mm | hh mm | hh)
 hh— < hour >
 mm— < minute >
- Default—Time zone specified by the Internet service provider
- Example
 - Canada/Eastern or America/New York
 - GMT + 5 sets the time zone to 5 hours behind GMT.

Setting Actions

In the Actions area, specify the type of action to be taken for a specified service.

Operation

- Type of action to be taken at the indicated time.
- Value—Menu of actions to be taken
 - deactivate—Deactivates the specified service at the indicated time.
 - activate—Activates the specified service at the indicated time.
 - deny—Does not allow activation of the specified service at the indicated time.
 - deny and deactivate—Deactivates the service if it is currently active and does not allow activation of the indicated service at the specified time.
- Guidelines—For deactivate and activate, specify times only in the from fields; any entries in the to fields are ignored.

Service

- Service for the schedule.
- Value—Menu of services to which you have a subscription

Subscribing to Services

After you subscribe to a service, you can activate the service to use it. Your Internet service provider decides which services are available to you for subscription. For information about activating a service, see “Starting and Stopping Services” on page 137.

To manage subscriptions to services:

1. In the navigation pane, click **Subscribe**.

The Subscribe page appears.

virneo
The network that keeps you surfing

Hello Linda

Home Logout Contact us

Service Selection Portal

- Services
- Usage
- Account
- Schedules
- Subscribe**
- Register
- Unregister

Search

Subscribe

All available services are listed below.

It may take a minute for your new subscriptions to take effect.

Audio **Video** Internet News

Service Name	Service description	Subscribed	Unsubscribed
Video-Bronze	Example for content provider allowing bronze video access	<input type="radio"/>	<input checked="" type="radio"/>
Video-Gold	Example for content provider allowing high speed access	<input checked="" type="radio"/>	<input type="radio"/>
Video-Silver	Example for content provider allowing silver video access	<input type="radio"/>	<input checked="" type="radio"/>

OK Cancel

virneo

Copyright © 1999-2003 Juniper Networks

2. Click the tab that specifies the type of service to which you want to subscribe or unsubscribe.
 - To subscribe to a specified service, click **Subscribed**.
 - To stop a subscription to a specified service, click **Unsubscribed**.
3. After you finish making all schedule entries, click **OK**.

Registering Equipment for DHCP Login

If your Internet service provider assigns an IP address by using DHCP, you can register your equipment to automatically obtain an authenticated IP address when you log in to the portal. Your equipment can be a device other than a PC, such as an IP phone or a set-top box.

To register your equipment:

1. In the navigation pane, click **Register**.

The Register page appears.

virneo
The network that keeps you surfing

Hello Linda

Home Logout Contact us

Service Selection Portal

- Services
- Usage
- Account
- Schedules
- Subscribe
- Register**
- Unregister

Search

Register

You may register your DHCP equipment so that it always obtains a public IP address. The first step is to supply the credentials that will authorize your equipment to receive a public IP address.

Equipment Credentials

Please enter your username and password for the Equipment Registration:

Username:

Password:

Continue

virneo

Copyright © 1999-2003 Juniper Networks

2. Specify the username and password to use for equipment registration, and click **Continue**.
3. In the page that appears, specify the media access control (MAC) address of the equipment to be registered, provide a brief description of this equipment, and click **Register**.



The screenshot shows the Virneo Sample Residential Portal. At the top left is the Virneo logo with the tagline "The network that keeps you surfing". A red banner at the top right says "Hello Linda". Below this are links for "Home", "Logout", and "Contact us". On the left is a "Service Selection Portal" with a dropdown menu showing options: Services, Usage, Account, Schedules, Subscribe, Register (highlighted), and Unregister. Below the menu is a search box. The main content area is titled "New Equipment Registration" and contains the instruction: "Please enter the MAC address (e.g. 03:3A:FE:98:3C:CB) and a brief description of the device you want to register." There are two input fields labeled "MAC address:" and "Description:". Below these are "Register" and "Cancel" buttons. To the right of the form is an illustration of a computer monitor, keyboard, mouse, and a golf bag. The Virneo logo is in the bottom right corner of the main content area. A red banner at the very bottom contains the copyright notice: "Copyright © 1999-2003 Juniper Networks".

The page displays the registration information.

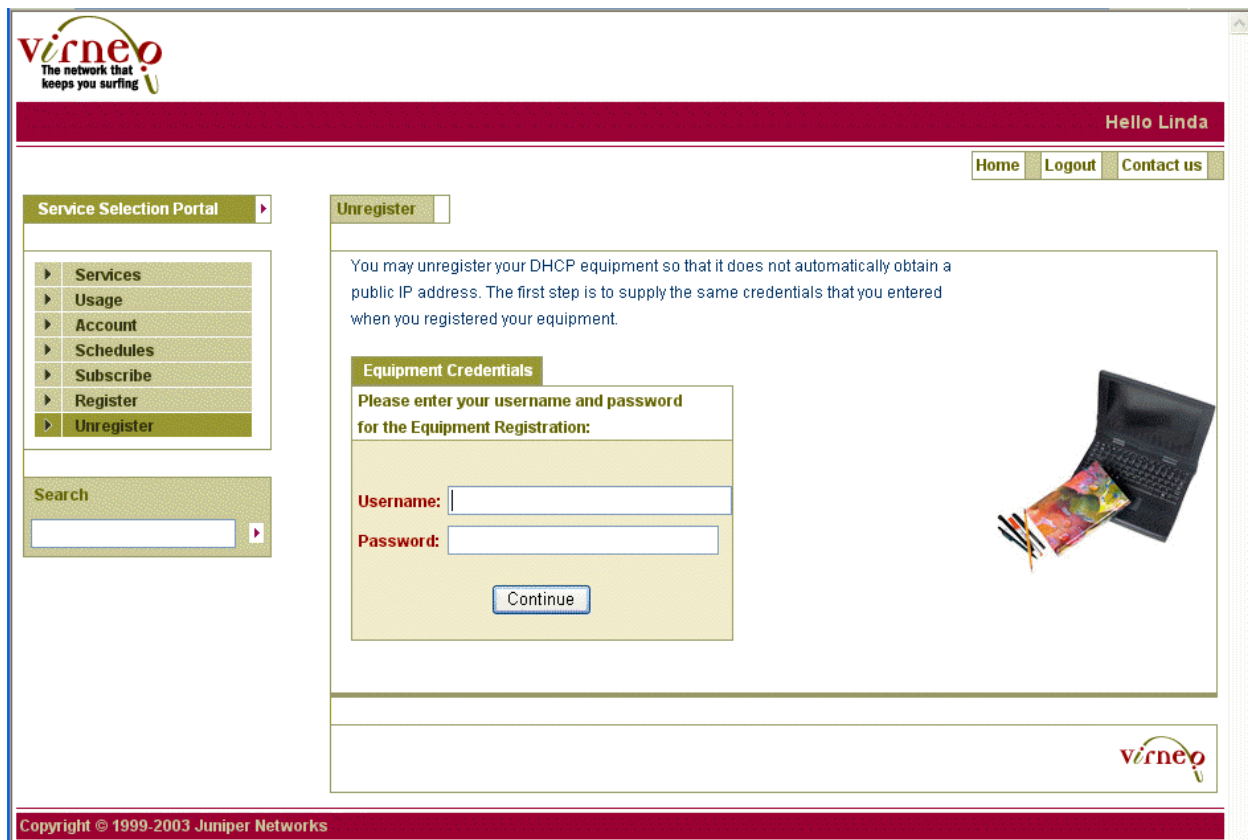
Disabling Equipment Registration

If you previously registered your equipment to obtain an authenticated IP address, you can change your configuration to disable equipment registration.

To disable registration of your equipment:

1. In the navigation pane, click **Unregister**.

The Unregister page appears.



The screenshot shows the Virneo web portal interface. At the top left is the Virneo logo with the tagline "The network that keeps you surfing". A maroon banner at the top right says "Hello Linda". Below the banner are links for "Home", "Logout", and "Contact us". On the left is a "Service Selection Portal" with a list of services: Services, Usage, Account, Schedules, Subscribe, Register, and Unregister. Below this is a search box. The main content area is titled "Unregister" and contains a paragraph explaining that users can unregister their DHCP equipment. Below this is a section titled "Equipment Credentials" with a prompt to enter a username and password for registration. There are input fields for "Username:" and "Password:", and a "Continue" button. To the right of the input fields is an image of a laptop with a colorful screen. The footer of the page contains the copyright notice "Copyright © 1999-2003 Juniper Networks" and the Virneo logo.

virneo
The network that keeps you surfing

Hello Linda

Home Logout Contact us

Service Selection Portal

- Services
- Usage
- Account
- Schedules
- Subscribe
- Register
- Unregister

Search

Unregister

You may unregister your DHCP equipment so that it does not automatically obtain a public IP address. The first step is to supply the same credentials that you entered when you registered your equipment.

Equipment Credentials

Please enter your username and password for the Equipment Registration:

Username:

Password:

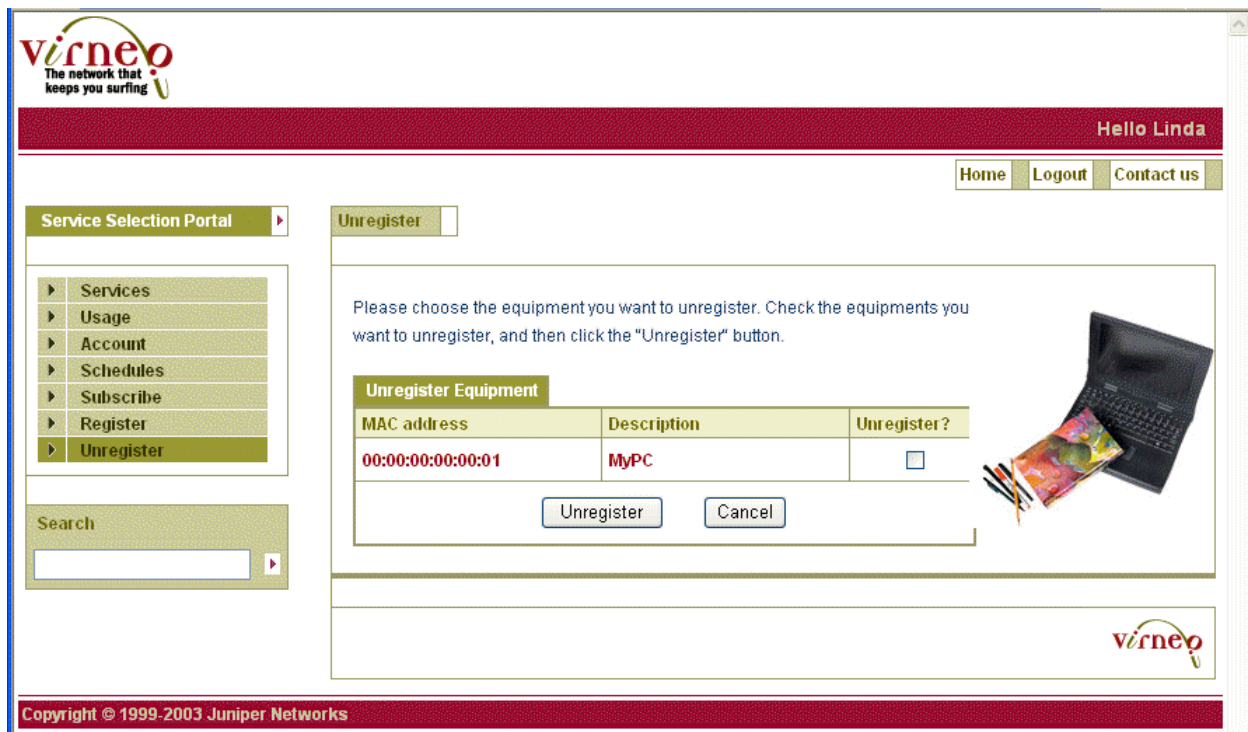
Continue

virneo

Copyright © 1999-2003 Juniper Networks

2. Enter your username and password, and click **Continue**.

A page appears that shows the equipment that you have registered.



3. Select the Unregister check box, and click **Unregister**.

The Welcome page for the portal appears.

You can also disable equipment registration when you log out of the portal; see "Logging Out of the Sample Residential Portal" on page 149 .

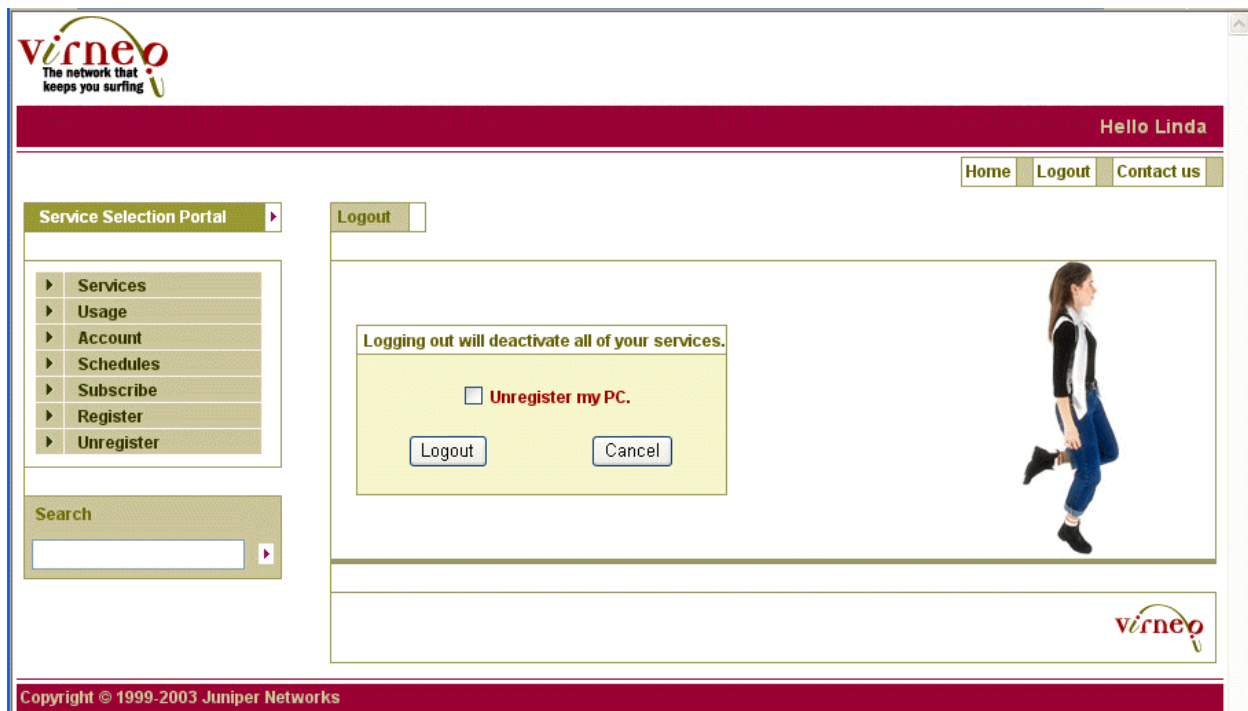
Logging Out of the Sample Residential Portal

When you finish using subscriptions to services, log out of the sample residential portal.

To log out of the sample residential portal:

1. On any portal page, click **Logout**.

The Logout page appears.



2. If you want to disable equipment registration, select **Unregister my PC**.
3. Click **Logout**.

The Welcome page appears again.

Using the Sample Residential Portal from PDAs

You can also access the sample residential portal from a personal digital assistant (PDA).

To use the sample residential portal from a PDA:

1. Start the sample residential portal from a PDA in the same way that you start the portal from a Web browser running on your PC. See “Logging In to the Sample Residential Portal Using a Simulated User Profile” on page 133 .

The Welcome page appears.



2. Click **Login**.

The login page appears.

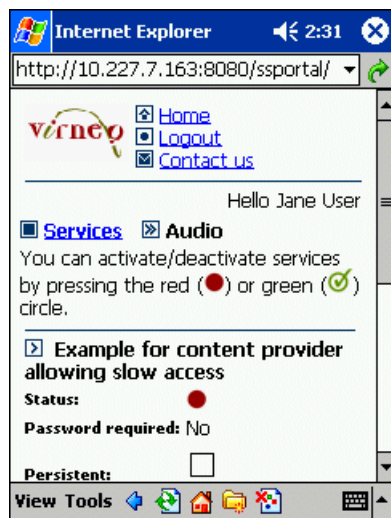


3. Enter your username and password.

After you log in, you can view the available services.



4. Navigate through the menus to activate and deactivate services.



Chapter 15

Developing a Residential Portal

- Before You Develop a Residential Portal on page 153
- Development Tools to Create a Residential Portal on page 153
- Virtual IP Address for Policies on page 154
- Redirecting Traffic to a Captive Portal Web Page on page 154
- Managing Security for Public Wireless LAN Applications on page 156
- Developing a Portal Based on the Sample Residential Portal on page 156

Before You Develop a Residential Portal

You can develop a residential portal based on the sample residential portal that accompanies the SRC software, or you can create a new one. Before you set up a residential portal, the SAE configuration for the retailers, services, subscribers, and basic subscriber services should already be in place.

Before you start to develop a portal, make sure that you understand the SAE configuration and how subscribers are expected to log in to the portal. See the following sources for information about the SAE and its configuration:

- *SRC PE Network Guide*
- *SRC PE Subscribers and Subscriptions Guide*

When you are planning an SRC network that uses residential portals, consider how many instances of the portals you need. For example, if your network includes a number of different retailers, you could create different portals for different retailers. Residential portals use CORBA to connect to the SAEs, allowing you to create distributed Web applications. These applications can be deployed in clusters for load sharing.

Development Tools to Create a Residential Portal

The SRC software provides the following tools for service providers to make residential portals available to residential customers:

- CORBA remote API—Provides remote access to the SAE core API

The CORBA remote API is the preferred interface to use between external applications and the SRC software. See the following sources for more information:

- *SRC PE Network Guide*.
- SAE CORBA remote API documentation in the SRC software distribution in the folder *SDK/doc/idl* or on the Juniper Networks Web site at

<http://www.juniper.net/techpubs/software/management/src/api-index.html>

- Javadoc documentation for the sample residential portal—Provides information about the Java interface

You can access the Javadoc documentation for the sample portal from the Welcome page of the sample portal after you log in to the portal. See “How Subscribers Use the Sample Residential Portal” on page 133.

- Sample residential portal

You can customize and extend the sample residential portal included with this release or create your own portal based on the sample. For information about the sample residential portal, see “Installing and Configuring the Sample Residential Portal” on page 121 and “How Subscribers Use the Sample Residential Portal” on page 133.

Virtual IP Address for Policies

You can configure a virtual IP address to specify an IP address that policies use as a substitution to send traffic to a captive portal.

For information about how to configure a virtual IP address from the SRC CLI, see the documentation for the following statement in the *SRC PE CLI Command Reference*:

```
shared sae configuration driver {
    virtual-portal-address virtual-portal-address ;
}
```

Redirecting Traffic to a Captive Portal Web Page

A captive portal Web page is a page that receives redirected HTTP requests. You can use a captive portal page as the initial page a subscriber sees after logging in to a subscriber session and as a page used to receive and manage HTTP requests to unauthorized Web resources.

The type of information available from a captive portal page depends on the portal design. The page can provide informational messages or can let subscribers perform actions such as activating a service to which they have a subscription. For example, if a subscriber requests access to a service that the subscriber has not activated, the portal could display a captive portal page that tells the subscriber that the service is not available, or the page could prompt the subscriber to activate the requested service.

Implementing a captive portal requires the following:

- An instance of the redirect server installed on a host in the same network as a JUNOSe router. The redirect server redirects HTTP requests received from IP Filter to a captive portal page.
- When the SRC software is installed on a Solaris platform, the IP Filter tool installed and configured on the same host as the redirect server. This tool redirects incoming HTTP requests to the redirect server.
- Default policies installed on the JUNOSe router. The default policies on the JUNOSe router must include a forwarding or rate-limiting policy that permits access to the portal server and a next-hop rule to intercept the unauthorized access request packets. The target of the next-hop rule is the host on which the redirect server resides.
- A portal server for serving the captive portal pages.

For a sample captive portal, see the sample residential portal.

For information about configuring the redirect server, see *Configuring the Redirect Server* (SRC CLI).

Sequence for Redirecting Traffic

The following list describes the sequence of events that occurs when a subscriber tries to access a restricted service:

1. A subscriber opens a Web browser and attempts to access a restricted server; for example, `http://a.com`.
2. A next-hop policy on the JUNOSe router sends this request to the redirect server instead of to the requested server.

The policy does not affect the destination address (resolved from `a.com`) in the IP packets.

3. For environments that have the SRC software installed on a Solaris platform, the IP Filter process running on the same host as the redirect server filters traffic and redirects traffic arriving on port 80 on the host's incoming interface.
4. The captured request is redirected to an address and a port where the redirect server listens.
5. The redirect server opens a TCP port (8800 by default) and sends the type of response configured—an HTTP 200 (OK) or a small HTML document that encodes a refresh in the meta header of the of the file—to the subscriber's browser for the requests.
6. The subscriber browser follows the redirect request and opens the captive portal page on the portal server.

Configuring the SRC Software in a Multihop Environment

The captive portal system implemented by the HTTP redirect server requires a single-hop connection; that is, the router accessed by the subscriber cannot be more

than one hop away from the redirect server. However, some networking environments will require a multihop connection—through more than one router—to the redirect server.

You can use any of several methods to get around the intermediate, next-hop routers, such as IP-in-IP tunneling, deployment of a NAT device, and dynamic DNS. Contact Juniper Networks Professional Services for assistance with these methods.

Managing Security for Public Wireless LAN Applications

You can include in a residential portal a Web page that automatically refreshes itself and provides a keepalive application that verifies the HTTP session. If the keepalive application cannot verify the HTTP session, the portal terminates the subscriber session. This feature improves security for public wireless LAN applications.

If you include this Web page in a residential portal, the following sequence of events occurs:

1. When a subscriber logs in through the portal, the SRC software starts the keepalive application.
2. The keepalive application creates a session key and sends it to the residential portal.
3. The residential portal stores the session key in its corresponding HTTP session.
4. The keepalive application sets the timeout for the subscriber session to a value greater than the refresh time.
5. When the Web page refreshes itself, the keepalive application sends the session key to the residential portal.
6. The portal responds as follows:
 - If the session key matches the value in the portal's HTTP session, the portal updates the timeout for the subscriber session, creates a new session key, and sends the new key to the keepalive page.
 - If the session key does not match the value in the portal's HTTP session, the portal terminates the subscriber session.
7. If the Web page does not refresh itself before the timeout expires (for example, if the subscriber closes the Web browser or turns off the PC without logging out), the portal terminates the subscriber session.

Developing a Portal Based on the Sample Residential Portal

The source code is included with the sample residential portal. To modify the behavior of the portal beyond a simple configuration, install a Java development environment. You can find the source code of the sample residential portal in the directory *WEB-INF/src*. The portal pages are stored in the layout and tiles directories.

The sample residential portal does not require any specific environment, but the procedures below assume that you use the Eclipse platform. A servlet container is

required to run the portals during development. We recommend that you use Tomcat and its Eclipse plug-in.

For information about your development environment, see the documentation for the product you are using.

Preparing to Develop a Portal Based on the Sample Residential Portal

The following instructions describe how to set up a development environment that uses Eclipse and Tomcat on a Solaris platform. If you want to use Eclipse and Tomcat on a different operating system, see the following Web sites:

- For Eclipse:

<http://www.eclipse.org>

- For Tomcat:

<http://jakarta.apache.org/tomcat>

To get ready to develop a portal based on the sample residential portal:

1. Download and install Eclipse from

<http://www.eclipse.org>

2. Download the Tomcat plug-in for Eclipse from

<http://www.sysdeo.com/eclipse/tomcatPlugin.html>

3. Unzip the plug-in into the Eclipse installation directory.
4. Download Tomcat from

<http://jakarta.apache.org/tomcat>

5. Install Tomcat:

```
mkdir $HOME/eclipse
cd $HOME/eclipse
unzip /tmp/eclipse-SDK-2.0.2-solaris-motif.zip
unzip /tmp/tomcatPluginV201.zip
cd $HOME
gzip -dc /tmp/tomcat-4.1.18.tar.gz | tar xvf -
```

6. Start Eclipse.
7. Configure the Tomcat plug-in.

Select **Window > Preferences > Tomcat**, and configure the Tomcat version and the path where you installed Tomcat.

Creating a Portal Project

To create a new Tomcat project inside Eclipse:

1. Select **File > New > Project > Java > Tomcat Project**, enter the name of the project, and click **Finish**.
2. Select **File > Import... > Zip File**, enter the path for *ssportal.war*; and click **Finish**.
3. Select **File > Properties > Java Build Path > Libraries > Add Jars**, open the sample project, navigate to *WEB-INF/lib*, and select all JAR files in the *WEB-INF/lib* directory.
4. Select **File > Properties > Tomcat**, and click **Can update server.xml file**.

Building the Portal

Eclipse automatically rebuilds the project when you save a modified source file.

To test or debug the project, run the code inside Tomcat.

To start Tomcat:

- Select **Tomcat > Start Tomcat**.

You can set break points in your code to debug the code.

Deploying the Portal

To create a new Web application, set the name of the target WAR file.

1. Select **File > Properties > Tomcat**.
2. Enter the path of the target WAR file in the field WAR file for export.
3. Right-click the portal project, and select **Tomcat Project > Export to the WAR file set** in project properties.
4. Copy the WAR file to the final deployment location; for example, */opt/UMC/jboss/server/default/deploy* on your portal server.

Testing a Portal Application

Simulated router drivers allow you to create subscriber sessions without connecting to a router. You can use a simulated router drive when you want to test your portal application. See Configuring Simulated Router Drivers (SRC CLI).

Part 7

Designing Services for Enterprise Manager Portal

- Reviewing and Configuring Policies and Services for Enterprise Manager Portal on page 161

Chapter 16

Reviewing and Configuring Policies and Services for Enterprise Manager Portal

- Overview of Services for Enterprise Manager Portal on page 161
- Before You Configure Services for Enterprise Manager Portal on page 162
- Configuring Firewall Policies and Services for Enterprise Manager Portal on page 163
- Configuring NAT Policies and Services for Enterprise Manager Portal on page 172
- Configuring Bandwidth Policies and Services for Enterprise Manager Portal on page 174
- Enabling Schedules for Subscriptions for Enterprise Manager Portal on page 182
- Configuring VPNs for Enterprise Manager Portal on page 182
- Billing Subscribers Through SCU/DCU for JUNOS Routing Platforms on page 184

Overview of Services for Enterprise Manager Portal

Enterprise Manager Portal is an application that lets service providers provision services for enterprise subscribers.

Enterprise Manager Portal can apply the types of services listed in Table 10 on page 161 to enterprise traffic as specified on JUNOS routing platforms or JUNOSe routers.

Table 10: Services Available from Enterprise Manager Portal

Types of Service	Types of Router
Firewalls—stateful or stateless	JUNOS routing platforms
Network Address Translation (NAT)	JUNOS routing platforms
Bandwidth on demand (BoD)	JUNOS routing platforms or JUNOSe routers
BoD for traffic routed to specified layer 3 VPNs	JUNOS routing platforms

The service provider uses services and policies in the SRC directory to manage traffic on a JUNOS routing platform or on a JUNOSe router. IT managers in enterprises that are customers of the service provider subscribe to these services through Enterprise Manager Portal.

Some of the services and policies are defined in the sample data and require little or no customization. You can, however, create some new services and policies, such as those for BoD.

Directory Structure

Use the directory structure in the sample data to organize services and policies. The following list shows the location of the policies and services in the directory:

- Services—*l = entJunos, o = Scopes, o = umc*
- Policies—*ou = entJunos, o = Policies, o = umc*

Although the scope that includes services for Enterprise Manager Portal is named *entJunos*, the policies for the BoD services have policy rules for both JUNOSe routers as well as JUNOS routing platforms.

Priorities for Subscriptions

Each subscription to a service has a priority that is identified by a service parameter named *priority*. A subscription with a lower priority setting takes precedence over a subscription with a higher priority setting. The SAE uses the priorities to determine the order in which it applies subscriptions to a particular type of service to traffic. For example, if the same traffic is affected by subscriptions to several firewall services on a JUNOS routing platform, the SAE applies those subscriptions in a prioritized order. Priorities of different types of service are independent of each other; for example, for JUNOS routing platforms, priorities of NAT services are independent of priorities for BoD services.

Depending on the type of service, you must specify either an explicit priority or a range of priorities in the service or the policy rules. When you specify a range of priorities, the IT manager selects an explicit priority in this range through Enterprise Manager Portal. The sample data includes definitions of priorities for each type of service; however, you can modify the priorities if you want to provide different ranges of priorities.

A substitution in a subscription provides the value for the service parameter named *priority*. This parameter is in the precedence policy rule field to control the ordering of policies when a subscription is activated.

Before You Configure Services for Enterprise Manager Portal

Before you configure services for use by Enterprise Manager Portal:

1. Configure the SAE.
2. If you are managing services on JUNOS routing platforms, configure the JUNOS routing platform, and enable it to interact with the SRC software.

See the JUNOS documentation and Locating Subscriber Management Information.

3. If you are managing services on JUNOSe routers, configure the JUNOSe router, and enable it to interact with the SRC software).

See the JUNOSe documentation and Adding JUNOSe Routers and Virtual Routers with the CLI.

4. For prerequisites to using policy rules on JUNOS routing platforms and JUNOSe routers, see Before You Configure SRC Policies.
5. For general information about configuring services, see Policy Management Overview.

Configuring Firewall Policies and Services for Enterprise Manager Portal

Before you configure firewall policies and services in Enterprise Manager Portal, you review and update the configuration from the Policies, Services, and Subscribers CLI or the Policies, Services, and Subscribers subtasks in the C-Web interface. Topics in this section include:

- Types of Firewall Services on page 163
- Overview of Basic Firewall Services and Policies on page 164
- Tasks to Configure Firewall Policies and Services on page 165
- Configuring Basic Firewall Policies on page 165
- Configuring Basic Firewall Services on page 166
- Reviewing the fwrule Policy Group for Exceptions to Stateful Firewalls on page 166
- Reviewing the Firewall Rule Service for Exceptions to Stateful Firewalls on page 166
- Reviewing Services for Exceptions to Stateless Firewalls on page 167
- Parameter Values Used by Services for Exceptions to Stateless Firewalls on page 168
- Planning Services for Custom Firewall Exceptions on page 169
- Configuring Policies for Custom Firewall Exceptions on page 169
- Configuring Services for Custom Firewall Exceptions on page 170
- Configuring Priorities for Stateless or Stateful Firewall Services on page 170

Types of Firewall Services

The SRC software represents a JUNOS firewall as two types of SRC services:

- Basic firewall service—Defines the action that the firewall takes and specifies the types of traffic that the firewall affects.
- Services to provide firewall exceptions—Defines exception rules to block traffic that otherwise would be permitted to traverse the firewall, or to admit traffic that would otherwise be blocked. Exceptions specify criteria against which packets and application flows are inspected.

For example, to configure an access only to accept e-mail from a specific IP address, you can use a basic firewall service that blocks all incoming and outgoing traffic; then you can use a firewall exception that allows incoming e-mail traffic from that IP address.

The SRC software supports the following types of firewalls on JUNOS routing platforms:

- Stateless firewalls—Inspect each packet in isolation; do not evaluate the traffic flow.
- Stateful firewalls—Inspect track traffic flows and conversations between applications, and evaluate this information when applying exception rules to the traffic.

An application is typically associated with a stateful firewall rule. After a flow or conversation meets firewall criteria, packets in that flow can pass through the firewall. For example, when an FTP control connection requests a file download, the stateful firewall knows to expect and allows a TCP data connection to start.

The same criteria may not be applied to each packet. For example for a TCP application, the criteria changes when a new TCP session is initiated to allow subsequent packets in the flow.

You can make either stateless firewalls or stateful firewalls available from Enterprise Manager Portal.

Overview of Basic Firewall Services and Policies

You can create as many basic firewall services in the directory as you want. Table 11 on page 164 shows the names of the services and policies associated with the basic firewall services in the sample data.

Table 11: Basic Firewall Services and Policies

Name of Service	Name of Policy Group	Function of Firewall
BrickWall	brickwall	Blocks all incoming and outgoing traffic
EmailAndWeb	emailweb	Blocks all incoming traffic and allows only outgoing e-mail and HTTP traffic
Multiservice	multiservice	Blocks all incoming traffic and allows outgoing e-mail, HTTP, FTP, telnet, and Real-Time Streaming Protocol (RTSP) traffic

The services are located under *l = entJunos*, *o = Scopes*, *o = umc* in the sample data.

The policies are located under *ou = entJunos*, *o = Policies*, *o = umc* in the sample data.

You can use these services and their associated policies as a starting point for developing your own basic firewall services.

Tasks to Configure Firewall Policies and Services

The tasks to configure policies and services for firewalls are:

1. “Configuring Basic Firewall Policies” on page 165
2. “Configuring Basic Firewall Services” on page 166
3. For stateful firewalls:
 - a. “Reviewing the fwrule Policy Group for Exceptions to Stateful Firewalls” on page 166
 - b. “Reviewing Services for Exceptions to Stateless Firewalls” on page 167
4. For stateless firewalls:
 - a. “Reviewing Services for Exceptions to Stateless Firewalls” on page 167
 - b. “Parameter Values Used by Services for Exceptions to Stateless Firewalls” on page 168
 - c. “Planning Services for Custom Firewall Exceptions” on page 169
 - d. “Configuring Policies for Custom Firewall Exceptions” on page 169
 - e. “Configuring Services for Custom Firewall Exceptions” on page 170

Configuring Basic Firewall Policies

You can create policies with the Policies, Services, and Subscribers CLI or the Policies, Services, and Subscribers subtasks in the C-Web interface.

To create a basic firewall policy:

1. Create a policy group and associated policy rules in *ou = entjunos, o = Policies, o = umc*.
2. Specify a precedence for the policy rules.

All basic firewall services should have a similar value that is higher than the range of precedences you configure for firewall exceptions. In the sample data, we use precedences of 600 and 601 for basic firewall policies.

Ensure that the precedence for basic firewall policies integrate with other policies that affect the same traffic. See “Configuring Priorities for Stateless or Stateful Firewall Services” on page 170.

For a sample basic firewall policy, see *policyGroupName = brickwall, ou = entjunos, o = Policies, o = umc* in the sample data.

Configuring Basic Firewall Services

You can create services with the Policies, Services, and Subscribers CLI or the Policies, Services, and Subscribers subtasks in the C-Web interface.

To create a basic firewall service:

1. Create a service.
2. Specify the following values for the service:
 - Category—Text string `basicFirewall` (service's LDAP attribute `sspCategory`)
 - Description—Summary of what the firewall service does (service's LDAP attribute `description`)

This description will appear on the portal, and subscribers will use the description to select a firewall service. Although there is no upper limit for the length of this attribute, the portal will display the text in one paragraph.

- Policy Group—Policy group configured for use with this service

For a sample firewall service, see `serviceName = BrickWall`, `l = entJunos`, `o = Scopes`, `o = umc` in the sample data.

Reviewing the `fwrule` Policy Group for Exceptions to Stateful Firewalls

The policy group `policyGroupName = fwrule`, `ou = entJunos`, `o = Policies`, `o = umc` is predefined in the sample data. Do not modify any settings or substitutions for this service.

Reviewing the Firewall Rule Service for Exceptions to Stateful Firewalls

The SRC sample data provides one service for firewall exceptions, `serviceName = FirewallRule`, `l = entJunos`, `o = Scopes`, `o = umc`, that is designed to work with Enterprise Manager Portal. Do not modify the definition for this service or its associated policy.

You can modify the allowed priority ranges for the service. See “Configuring Priorities for Stateless or Stateful Firewall Services” on page 170.

Each subscription to this service adds a rule to the stateful firewall. The `FirewallRule` service and its associated policy are general and contain many parameters, such as the priority of the firewall exception and the action that the firewall should take. IT managers supply actual values for these parameters through Enterprise Manager Portal.

You can modify the priority ranges for this policy group if necessary; do not modify any other settings. The values for these parameters must be lower than the precedence settings for the policy rules in the basic firewall policy groups. This distinction allows the firewall exception to take priority over the basic firewalls. In the sample data, the `FirewallRule` service has priorities in the range 500–579.

Reviewing Services for Exceptions to Stateless Firewalls

Review the services that Enterprise Manager Portal requires to ensure that configuration of these services works in your environment. These services are firewall exceptions—services that define the types of traffic that a firewall admits or blocks.

Enterprise Manager Portal requires that specific services be configured to cover each of the following traffic actions:

- Allow
- Reject
- Discard

These actions are required for each traffic direction; that is, traffic:

- Entering the network
- Exiting the network
- Entering and exiting the network

Table 12 on page 167 lists the names of services required by Enterprise Manager Portal. The naming convention for the services specifies both action and direction; for example, for the FWR_Fwd_Out service:

- Action—allow (forward)
- Direction—Outgoing (from the enterprise)

Services configured to reject traffic return a “network-unreachable” ICMP message.

Table 12: Stateless Firewall Services in Sample Data

	Traffic Entering the Enterprise	Traffic Exiting from the Enterprise	Traffic Entering and Exiting the Enterprise
Traffic Allowed	FWR_Fwd_In	FWR_Fwd_Out	FWR_Fwd_Both
Traffic to Be Discarded	FWR_Filter_In	FWR_Filter_Out	FWR_Filter_Both
Traffic Rejected	FWR_Rej_In	FWR_Rej_Out	FWR_Rej_Both

The services are located under *l = entJunosStatelessFW*, *o = Scopes*, *o = umc* in the sample data. These services and the associated policies configured in the sample data are designed for a subscriber-facing interface on a provider edge device.

In most cases you can use the services as configured. If needed—for example, for a service provider-facing interface in a customer edge device—you can customize the services listed in Table 12 on page 167, but do not change the names.

To customize services for an enterprise-facing interface, change the configuration for:

- Source IP addresses and ports
- Destination IP addresses and ports

You can also create services that provide custom exceptions to a firewall. Portal users can select custom exceptions under Firewall actions on the Firewall page in Enterprise Manager Portal.

Parameter Values Used by Services for Exceptions to Stateless Firewalls

Table 13 on page 168 lists the parameters for which Enterprise Manager Portal provides values. The parameter names start with “fw” (service’s LDAP attribute parameterSubstitution). The services listed in “Before You Configure Services for Enterprise Manager Portal” on page 162 use these parameters.

Table 13: Parameters for Stateless Firewall Services for Enterprise Manager Portal

To Specify this Value	Use This Parameter
Protocol	fwProtocol
Source network	fwSrcIp
Source port	fwSrcPort
Destination network	fwDestIp
Destination port	fwDestPort
TOS byte	fwTosByte
TOS byte mask	fwTosByteMask
TCP flags	fwTcpFlags
TCP flags mask	fwTcpFlagsMask
IP flags	fwIpFlags
IP flags mask	fwIpFlagsMask
Fragmentation offset	fwIpFragOffset
ICMP type	fwIcmpType
ICMP code	fwIcmpCode
Packet length	fwPacketLength

Planning Services for Custom Firewall Exceptions

Typically, you use custom exceptions to provide bandwidth management as well as firewall exceptions. Using custom exceptions that do both simplifies the way you integrate BoD and firewall services. For example, you can create custom exceptions to police traffic or to assign a traffic class to the traffic and to specify firewall behavior.

See examples of services for custom exceptions in the sample data:

- *l = Limit1Mbs, l = entJunosStatelessFW, o = Scopes, o = umc*
- *l = Limit2Mbs, l = entJunosStatelessFW, o = Scopes, o = umc*
- *l = Limit5kbs, l = entJunosStatelessFW, o = Scopes, o = umc*

The sample services and the associated policies are designed for a subscriber-facing interface on a provider edge device. When you create policies, policy direction (input or output) can map to incoming or outgoing traffic depending on whether the SRC-managed interface is a subscriber-facing interface on a service provider edge device, or a service-provider facing interface on the customer edge device in an enterprise. When you configure policies for services designed for use through the Enterprise Management Portal, you typically assume that:

- Source IP addresses and ports are inside an enterprise
- Destination IP addresses and ports are outside an enterprise

Configuring Policies for Custom Firewall Exceptions

You can create policies with the Policies, Services, and Subscribers CLI or the Policies, Services, and Subscribers subtasks in the C-Web interface.

To configure a policy for a custom firewall exception:

1. Create a stateless firewall policy group and associated policy rules.
2. Specify parameters for the following properties for each policy rule:
 - IP protocol
 - TOS byte in the IP header
 - Source IP addresses
 - Source TCP/UDP ports
 - Destination IP addresses
 - Destination TCP/UDP ports
 - TCP flags
 - IP flags (fragmentation flags)
 - Fragmentation offset
 - Packet length

- ICMP type
- ICMP code

For a sample policy, see *policyGroupName = custom_policer*, *ou = entjunos_statelessfw*, *o = Policies*, *o = umc* in the sample data.

Configuring Services for Custom Firewall Exceptions

You can create services with the Policies, Services, and Subscribers CLI or the Policies, Services, and Subscribers subtasks in the C-Web interface. You can create services that take actions such as those listed in Table 12 on page 167.

To configure a service for a custom firewall exception:

1. Create a service for each traffic action listed in Table 12 on page 167. Specify a name that provides meaningful information to a user, including information about the forwarding treatment for traffic. The name appears in the Firewall Action field on the Firewall tab in Enterprise Manager Portal.
2. Specify the following values for the service:
 - Category—customFWRule (the service's LDAP attribute sspCategory)
 - Policy Group—Policy group that supports custom firewall exceptions
3. Specify substitutions for the service.

Configuring Priorities for Stateless or Stateful Firewall Services

If you design services to be accessed from Enterprise Manager Portal, you can configure ranges of priority values that are enterprise specific and ranges that are available to a number of enterprises. Setting the two ranges makes it possible for a service provider to specify firewall exceptions that an IT manager in an enterprise cannot override.

Configuring Priorities to Have Enterprise Services Work Together

You can configure the parameters in the following list as global parameters that apply to all subscribers, and as subscriber-specific parameters. If you configure both, the global range takes precedence over a subscriber-specific limit.

- fwMinPriority—Specifies the lower limit of the range of precedences available for subscriptions to firewall exceptions.
- fwMaxPriority—Specifies the upper limit of the range of precedences available for subscriptions to firewall exceptions.
- fwEnterpriseMinPriority—Specifies the lower limit of the range of precedences that an enterprise-specific manager can make available for subscriptions to firewall exceptions.
- fwEnterpriseMaxPriority—Specifies the upper limit of the range of precedences that an enterprise-specific manager can make available for subscriptions to firewall exceptions.

Ensure that:

- fwMaxPriority is greater than or equal to fwEnterpriseMaxPriority
- fwEnterpriseMaxPriority is greater than fwEnterpriseMinPriority
- fwEnterpriseMinPriority is greater than or equal to fwMinPriority

Configuring Priorities for Individual Scopes by Defining Them in Services

You can use parameters to limit priority ranges for services within a scope. For stateful firewall services, you set parameters to limit priority ranges in the FirewallRule service. For stateless firewall services, you set parameters to limit priority ranges in the FRW_Filter_Both service.

You can use parameters to limit priority ranges for services within a scope in addition to using global ranges. For example, you can define a global range, and then define a different range that overrides the global range for specified subscribers.

To allow priority values for services in one scope to override the priority values for services in another scope:

1. In a service that resides in a service scope that has a low precedence (indicated by a higher number), define default values for parameters that limits a priority range.
2. Attach this scope to an entry at a high level in the subscriber folder; for example, to a retailer.
3. Create a second scope that has a higher precedence.
4. Create a service that uses parameters to limit priority ranges in the second scope.
5. Attach the second scope (which has a higher precedence) to the enterprise.

The services with the higher precedence override the services with a lower precedence.

Using Stateless Firewall and BoD Applications Together

In most cases, you can use the services listed in Table 12 on page 167 to provide bandwidth management and firewall support. However, if you want to design special services to have firewalls work with BoD services, use the following guidelines to design your services:

- Specify a higher priority in the BoD policies.
- Specify next-rule actions for the BoD policies.

After all the BoD policy rules are applied, the stateless firewall policy rules are applied. Packets are forwarded or dropped as appropriate.

Configuring NAT Policies and Services for Enterprise Manager Portal

Before you configure NAT addressing in Enterprise Manager Portal, review and update the configuration from the SRC CLI or the C-Web interface. Topics in this section include:

- NAT Policies and Services in the SRC Sample Data on page 172
- Configuring the dynsrcnat Policy Group on page 172
- Reviewing the DynSrcNat Service on page 173
- Configuring the staticdstnat Policy Group on page 173
- Configuring the StaticDstNat Service on page 173
- Configuring the staticsrcnat Policy Group on page 173
- Configuring the StaticSrcNat Service on page 174

NAT Policies and Services in the SRC Sample Data

The NAT policy groups and services provided in the sample data are designed to work with Enterprise Manager Portal and require little configuration. Table 14 on page 172 shows the names of the policy groups and services associated with each type of NAT that the SRC software supports.

Table 14: NAT Services and Policies

Type of NAT	Name of Policy Group	Name of Service
Dynamic source NAT	dynsrcnat	DynSrcNat
Static destination NAT	staticdstnat	StaticDstNat
Static source NAT	staticsrcnat	StaticSrcNat

The services are located under *l = entJunos, o = Scopes, o = umc* in the sample data.

The policies are located under *ou = entJunos, o = Policies, o = umc* in the sample data.

For information about creating NAT policies, including prerequisites on the JUNOS routing platform, see the *SRC PE Services and Policies Guide*.

Configuring the dynsrcnat Policy Group

You can modify the precedence settings in the policy rules for the dynsrcnat policy group. Use the following guidelines if you make changes to the precedence settings:

- The precedence settings for the policy rules in the dynsrcnat policy group must be higher than the precedence settings for the policy rules in the staticsrcnat policy group. This distinction allows static source NAT rules to take priority over dynamic source NAT rules.

- The value for this setting must be higher than the precedence of any firewall exception. This distinction ensures that the SAE activates the artificial firewall rule first.

Reviewing the DynSrcNat Service

The DynSrcNat service is predefined in the sample data. Do not modify any settings or substitutions for this service.

Configuring the staticdstnat Policy Group

This policy group contains two policy rules:

- SFWR —Acts as an artificial firewall rule that ensures that the SAE activates a basic firewall service for the access before activating a NAT service; the JUNOS software requires that a firewall be active before you implement a NAT rule.
- PR—Defines the policy for the static destination NAT service.

The only setting you can modify for this policy group is the precedence setting for the SFWR policy rule. The value for this setting should be higher than the precedence of any other firewall exception. This distinction ensures that the SAE activates the artificial firewall rule first.

Configuring the StaticDstNat Service

You can modify the following substitutions for the StaticDstNat service; do not modify any other settings for this service.

- staticDestNatMinPriority—Lower limit of the range of precedences available for subscriptions to static destination NAT rules
- staticDestNatMaxPriority—Upper limit of the range of precedences available for subscriptions to static destination NAT rules

Configuring the staticsrcnat Policy Group

This policy group contains two policy rules:

- SFWR—Acts as an artificial firewall rule that ensures that the SAE activates a basic firewall service for the access before activating a NAT service; the JUNOS software requires that a firewall be active before you implement a NAT rule.
- PR—Defines the policy for the static source NAT service.

The only setting you can modify for this policy group is the precedence setting for the SFWR policy rule. The value for this setting should be higher than the precedence of any other firewall exception. This distinction ensures that the SAE activates the artificial firewall rule first.

Configuring the StaticSrcNat Service

You can modify the following substitutions for the StaticSrcNat service; do not modify any other settings or substitutions for this service.

- staticSrcNatMinPriority—Lower limit of the range of precedences available for subscriptions to static source NAT rules
- staticSrcNatMaxPriority—Upper limit of the range of precedences available for subscriptions to static source NAT rules

The values for these parameters must be lower than the precedence settings for the policy rules in the dynsrcnat policy group. This distinction allows static source NAT rules to take priority over dynamic source NAT rules.

Configuring Bandwidth Policies and Services for Enterprise Manager Portal

You configure bandwidth-on-demand services to make them available through the Enterprise Manager Portal. Topics in this section include:

- Bandwidth-on-Demand Services for Enterprise Manager Portal on page 174
- Parameter Values Used by BoD Services on page 175
- Bandwidth Policies for Different Routing Platforms on page 176
- Configuring Basic BoD Policies on page 176
- Configuring Basic BoD Services on page 177
- Configuring BoD Policies on page 178
- Configuring BoD Services on page 179
- Using BoD Services to Assign Traffic to Bandwidth Categories on page 179
- Using BoD and Basic BoD Services Together to Supply Class of Service on page 180
- Examples: Setting Up Forwarding Preferences on page 180

Bandwidth-on-Demand Services for Enterprise Manager Portal

You can make bandwidth available on demand to IT managers by creating the following types of services:

- Basic BoD service—Specifies the bandwidth level available to an access link.
- BoD service—Classifies traffic and assigns a service level that specifies the forwarding treatment for the traffic class.

BoD and basic BoD services allow billing for subscriptions to supplementary services.

You can create services to provide JUNOS class of service (CoS) or JUNOSe quality of service (QoS) by configuring BoD and basic BoD services that interact with each other. You can provide different service levels to different traffic by specifying traffic classification criteria.

You can create any number of basic BoD services and any number of BoD services. Only one basic BoD service, but numerous BoD services can be assigned to an access link.

BoD services can be configured to provision bandwidth provided by basic BoD services for a link. For example, you could provide a basic BoD service that provides 1 Mbps to the access link, and two video services as BoD services, each with different characteristics.

When you configure BoD and basic BoD services, they are available to IT managers through Enterprise Manager Portal

- Related Topics**
- Overview of Bandwidth-on-Demand Services on page 229
 - Configuring Basic BoD Policies on page 176
 - Configuring Basic BoD Services on page 177
 - Configuring BoD Policies on page 178
 - Configuring BoD Services on page 179
 - Using BoD Services to Assign Traffic to Bandwidth Categories on page 179

Parameter Values Used by BoD Services

Table 15 on page 175 lists the parameters for which Enterprise Manager Portal provides values. The parameter names start with “bod” (service’s LDAP attribute parameterSubstitution).

Table 15: Parameters for BoD Services for Enterprise Manager Portal

To Specify This Value	Use This Parameter
Protocol	bodProtocol
TOS byte	bodTosByte
TOS byte mask	bodTosByteMask
Source network	bodSrcIp
Source port	bodSrcPort
Destination network	bodDestIp
Destination port	bodDestPort
TCP flags	bodTcpFlags
TCP flags mask	bodTcpFlagsMask
IP flags	bodIpFlags
IP flags mask	bodIpFlagsMask

Table 15: Parameters for BoD Services for Enterprise Manager Portal *(continued)*

To Specify This Value	Use This Parameter
Fragmentation offset	bodIpFragOffset
Packet length	bodPacketLength
ICMP type	bodIcmpType
ICMP code	bodIcmpCode

Bandwidth Policies for Different Routing Platforms

If you support environments that include both JUNOS routers and JUNOS routing platforms, you can configure policies to have policy rules for JUNOS filters and JUNOS filters. This way, if the service is activated on a JUNOS router, the JUNOS rule is used, and if the service is activated on a JUNOS routing platform, the JUNOS policies are used.

When Enterprise Manager Portal has JUNOS compatibility enabled, the portal allows:

- Single subnets for source and destination addresses
- Single ports or single port ranges for source and destination ports

In addition, with JUNOS compatibility enabled, Enterprise Manager Portal does not show the following configuration fields for BoD services:

- TCP flags
- IP flags
- Fragment offset
- Packet length
- ICMP type
- ICMP code

You should be familiar with the types of bandwidth management policies available for the type of router for which you are configuring policies. See Policy Management Overview.

Configuring Basic BoD Policies

You can create policies with the Policies, Services, and Subscribers CLI or the Policies, Services, and Subscribers subtasks in the C-Web interface.

To configure a basic BoD policy:

1. Create a policy group and associated policy rules.

Typically the policy rules include JUNOS schedulers, JUNOS policers, JUNOS filters, or JUNOS filters that specify a traffic classification, and basic rules that define best-effort forwarding and drop behavior.

2. Include parameters in the classify-traffic conditions of the policer. Use parameter names from Table 15 on page 175.
3. Specify a precedence for the policy rules.

Structure the precedence for policies to ensure that policy rules for JUNOS schedulers and JUNOS policers have a higher precedence, and therefore a lower number, than default policy rules. If the configuration includes BoD services, the policies to support BoD services should have a higher precedence, indicated by a lower number.

For a sample basic BoD policy, see *policyGroupName = basicBod, ou = entjunos, o = Policies, o = umc* in the sample data.

Configuring Basic BoD Services

You can create services with the Policies, Services, and Subscribers CLI or the Policies, Services, and Subscribers subtasks in the C-Web interface.

Basic BoD services do not have service parameters.

To configure a service that uses basic BoD:

1. Create a service.
2. Specify the following values for the service:
 - Category—basicBod (service's LDAP attribute sspCategory)
 - Description—Description of the bandwidth provided by the service

If you plan to integrate a basic BoD service with a BoD service, the description for each basic BoD service should explain the bandwidth provided, and the relationship between this bandwidth level and the BoD service. The description should also explain the relationship between the service name, which is shown on the portal in the Bandwidth Level list, and the bandwidth provided. For example, for a service named 1 Mbps, the bandwidth provided could be 1 Mbps downstream and 500 Kbps upstream.

This description will appear in the online help for Bandwidth Level in Enterprise Manager Portal. Although there is no limit for the length of the text entered, the portal displays the text in one paragraph.

- Policy Group—Policy group that supports basic BoD services

For a sample BoD service, see *serviceName = 1.0 Mbps, l = EntJunos, o = Scopes, o = umc* in the sample data.

Configuring BoD Policies

When configuring BoD policies, you create rules that classify traffic. Make sure that the source and destination policy rules correspond to location of the enterprise relative to the subscriber interface that the SRC software manages. When configuring Enterprise Manager Portal, you follow the same rules for defining source and destination fields. See Policy Components.

You can create policies with the Policies, Services, and Subscribers CLI or the Policies, Services, and Subscribers subtasks in the C-Web interface.

To configure a BoD policy:

1. Create a BoD policy group and associated policy rules.

You can create some policy rules as JUNOS filters and others as JUNOSe filters.

Specify values or parameters for the following for each policy rule for the BoD service:

- TOS byte in the IP header
- Mask used for the ToS byte
- Source TCP/UDP port
- Destination TCP/UDP port
- IP address of source
- IP address of destination
- TCP flags
- Fragmentation flags
- Fragmentation offset
- ICMP type
- ICMP code

2. Specify a precedence for the policy rules.

If the configuration includes basic BoD services, the policies to support basic BoD services should have a lower precedence, indicated by a higher number.

For information about policy rules and precedences, see Policy Information Model.

For a sample BoD policy, see *policyGroupName = bod, ou = entjunos, o = Policies, o = umc* in the sample data. In the sample BoD policies, substitutions in services rename policy parameters to names required by Enterprise Manager Portal.

The sample data is based on a scenario that has the SRC managed interface on a device with egress to the access link that leads to the enterprise.

Configuring BoD Services

You can create services with the Policies, Services, and Subscribers CLI or the Policies, Services, and Subscribers subtasks in the C-Web interface.



NOTE: If you configure BoD services that use forwarding classes, take into consideration the number of forwarding classes supported on the router.

To configure a service for BoD:

1. Create a service.
2. Specify the following values for the service:
 - Category—bod (service's LDAP attribute sspCategory).
 - Description—Description of how this service will affect traffic.

If you plan to integrate a basic BoD service with a BoD service, the description for each BoD service should take into consideration how the BoD service interacts with any basic BoD service selected. The description should also provide information about the forwarding treatment for traffic.

This description will appear in the online help for BoD services in Enterprise Manager Portal. Although there is no upper limit for the length of this attribute, the portal will display the text in one paragraph.

- Substitutions—Substitutions for the parameter names; these names start with “ bod” (service's LDAP attribute parameterSubstitution).

Note that the actual parameter names are required to be the service parameter names for Enterprise Manager Portal.

- Policy Group—Policy group that supports BoD services.

For a sample BoD service, see *serviceName = Gold, l = entJunos, o = Scopes, o = umc* in the sample data.

Using BoD Services to Assign Traffic to Bandwidth Categories

You can use BoD services to assign different classes of traffic to different bandwidth categories, with each category identified by a specified quantity of bandwidth.

For example, a configuration could provide two services:

- Silver—Bandwidth of 500,000 Mbps
- Gold— Bandwidth of 1,000,000 Mbps

Each service has the specified bandwidth available to specified traffic flows, based on the policy rules for traffic classification and policing.

Using BoD and Basic BoD Services Together to Supply Class of Service

You can use BoD and basic BoD services together to provide more sophisticated bandwidth level management to IT managers. For example, you can integrate these types of services to take advantage of the CoS features available on JUNOS routing platforms.

On the JUNOS routing platform, policers are applied before schedulers. The type of service defined by these settings is applied to traffic exiting from the JUNOS routing platform. For information about policing, scheduling, and queuing traffic on the JUNOS routing platform, see *JUNOS Network Interfaces and Class of Service Configuration Guide*.

If you want to integrate basic BoD services and BoD services, you can base your configuration on the implementation in the sample data. The sample services and data are designed to work with Enterprise Manager Portal and require little configuration.

You can also create a configuration to meet requirements specific to your environment. If you want to create a configuration that has both basic BoD and BoD services, carefully plan services and associated policies. Ensure that the bandwidth requirements for BoD services are in proportion to the bandwidth provided by the basic BoD services. for another way to provide BoD to IT managers.



NOTE: When configuring services to use JUNOS CoS, take into consideration which interfaces on the router support CoS.

Examples: Setting Up Forwarding Preferences

We provide two examples for setting up forwarding preferences.

Setting Up Forwarding Preferences by Using CoS on JUNOS Routing Platforms

The sample data provides an implementation that supports CoS features on the JUNOS routing platform. This implementation provides:

- Basic BoD services to apply a JUNOS policer only to best-effort traffic
- BoD services to assign traffic to forwarding classes other than best-effort
- Policing for best-effort traffic

Table 16 on page 181 lists the services and policies in the sample data. You can locate the services in *l=entjunos*, *o=Scopes*, *o=umc*. You can customize the policies and services as needed. For general information about configuring policies and services, see “Configuring Basic BoD Policies” on page 176 and “Configuring BoD Policies” on page 178 .

Table 16: Integrated BoD and Basic BoD Services in Sample Data

Name of Service	Category of Service	Name of Policy Group	Description of Service
1.0 Mbps	basic BoD	basic BoD	Specifies that a bandwidth of 1.0 Mbps be available to a specified access link for best-effort traffic.
3.0 Mbps	basic BoD	basic BoD	Specifies that a bandwidth of 3.0 Mbps be available to a specified access link for best-effort traffic.
5.0 Mbps	basic BoD	basic BoD	Specifies that a bandwidth of 5.0 Mbps be available to a specified access link for best-effort traffic.
Silver	BoD	BoD	Marks associated traffic as belonging to an assured forwarding class.
Gold	BoD	BoD	Marks associated traffic as belonging to an expedited forwarding class.

Billing can be established for traffic in the assured forwarding class and in the expedited forwarding class because the SRC software can account for traffic in each of these forwarding classes separately from other forwarding classes. Traffic in the assured forwarding class and in the expedited forwarding class is not included in the accounting data for the currently selected basic BoD service.

Setting Up Forwarding Preferences by Allocating a Percentage of a Link's Bandwidth to a Service

The following example shows another way to use BoD and basic BoD services to provide BoD services. In this example, a percentage of an access link's bandwidth is allocated to a specified service.

This configuration provides:

- Three bandwidth levels available to access links: 1.0 Mbps, 1.5 Mbps, and 2.0 Mbps.
- Three service levels defined to use a specified percentage of the bandwidth set for the access link: best effort 20 %, Silver 30 %, and Gold 50 %.

Each traffic class uses only the bandwidth assigned to it and does not share bandwidth with other traffic classes.

For an SRC configuration to support this scenario, you could create policies such as the following and assign these policies to services:

- Policies that provide a local policy parameter, *bw*, whose value is set by the service that references the policy:

For policy 1.0 Mb, *bw* = 1000000

For policy 1.5 Mb, bw = 1500000

For policy 2.0 Mb, bw = 2000000

- The transmission rate, bandwidth allocation, and priority scheduling for specified forwarding classes as shown in Table 17 on page 182.

Table 17: Policies to Specify Forwarding Treatment for Specified Traffic Classes

Forwarding Class	Transmission Rate	Exact	Priority Scheduling
Best effort	bw*0.2 bps	true	Low
Silver (assured forwarding)	bw*0.3 bps	true	Medium
Gold (expedited forwarding)	bw*0.5 bps	true	High

By setting exact to true, you can ensure that the sum of the transmission rates is less than the bandwidth allocated to the access link.

Enabling Schedules for Subscriptions for Enterprise Manager Portal

You can add schedules to subscriptions from Enterprise Manager Portal for subscriptions to BoD and firewall services that have scheduling enabled.

To enable scheduling:

1. In the SRC CLI or the C-Web interface, navigate to the service to be scheduling-enabled.
2. For service parameters, add the Substitution **isSchedulable = 1**.

This substitution lets enterprise subscribers configure schedules for subscribers to this service.

Configuring VPNs for Enterprise Manager Portal

You configure VPNs, then manage them through the Enterprise Manager Portal. Topics in this section include:

- Overview of VPN Management Through Enterprise Manager Portal on page 183
- Before You Configure VPN Policies and Services on page 183
- Configuring Policies for BoD Traffic Destined for VPNs on page 183
- Configuring Services for BoD Traffic Destined for VPNs on page 184

Overview of VPN Management Through Enterprise Manager Portal

You can use the SRC software to allow IT managers to manage layer 3 VPNs on JUNOS routing platforms. This type of VPN supports membership based on filter-based forwarding policies.

You can configure Enterprise Manager Portal to display VPN features. IT managers can modify VPNs and send traffic associated with BoD subscriptions to specific VPNs. In addition, if you configure Enterprise Manager Portal to display extranet features, IT managers with privileges to configure VPNs can create extranets for other enterprises and retailers by exporting those VPNs. Enterprises and retailers who share VPNs that other subscribers own are called *extranet clients*.

To provide VPN services from Enterprise Manager Portal, you create corresponding VPN versions of the BoD services and their associated policies.

Before You Configure VPN Policies and Services

When you configure the SRC software to manage VPNs, complete the following tasks specific to the VPN configuration:

1. Configure the VPNs on the JUNOS routing platform.

See *JUNOS VPNs Configuration Guide*.

All routing instances that implement a specific VPN must have the same name.

2. Add the VPNs to the directory.

The identifier for a VPN in the directory must match the name of the routing instance configured on the JUNOS routing platform.

3. If you want to send traffic associated with BoD services to specific VPNs, configure policies and services for BoD traffic destined for VPNs.

See “Configuring Policies for BoD Traffic Destined for VPNs” on page 183 and “Configuring Services for BoD Traffic Destined for VPNs” on page 184.

4. Implement an addressing scheme for VPNs that allows extranet clients to access the VPNs.

- Related Topics**
- Before You Configure Services for Enterprise Manager Portal on page 162
 - Before You Add a JUNOS VPN to the SRC Configuration
 - Adding VPNs for Retailers and Enterprises

Configuring Policies for BoD Traffic Destined for VPNs

You can manage policies with the Policies, Services, and Subscribers CLI or the Policies, Services, and Subscribers subtasks in the C-Web interface.

To configure a policy for a BoD service associated with a VPN (a VPN policy):

1. Copy the policy for the BoD service in the directory.
2. Rename the policy you copied to a similar name that indicates this policy is the VPN version; for example, you can use `< bodPolicy > Vpn`, where `< bodPolicy >` is the name of the BoD policy.

For example, if the name of the original policy is `bod`, rename the service you copied to `bodVpn`.

3. Add a new local parameter (the name is arbitrary, for example `vpnName`) of type `Routing Instance` to the VPN policy.
4. Add a new action of type `RoutingInstanceAction` to the input policy rule, and specify a `Routing Instance` of `vpnName` for this action.
5. Save the VPN policy.

For a sample VPN policy, see *policyGroupName = bodVpn, ou = entjunos, o = Policies, o = umc* in the sample data. In the sample BoD policies, substitutions in services rename policy parameters to names required by Enterprise Manager Portal.

Configuring Services for BoD Traffic Destined for VPNs

You can manage services with the Policies, Services, and Subscribers CLI or the Policies, Services, and Subscribers subtasks in the C-Web interface.

To configure a BoD service that will be associated with a VPN (a VPN service):

1. Copy the BoD service in the directory.
2. Rename the service you copied to `< bodService > _VPN`, where `< bodService >` is the name of the original BoD service.

For example, if the name of the original BoD service is called `Gold`, rename the service you copied to `Gold_VPN`.

3. Add to the VPN service a parameter with a name that matches the parameter of type `Routing Instance` that you defined in the policy.

See “Configuring Policies for BoD Traffic Destined for VPNs” on page 183.

```
!vpnName=bodVpnName
```

4. Modify the VPN service to use the corresponding VPN policy that you created.
5. Save the service.

For a sample VPN service, see *serviceName = Gold_VPN, l = entjunos, o = Scopes, o = umc* in the sample data.

Billing Subscribers Through SCU/DCU for JUNOS Routing Platforms

All services that you configure for JUNOS routing platforms support billing that uses the source class usage (SCU) and destination class usage (DCU) features for egress traffic on the JUNOS routing platform. The SRC software supports this feature through

the SAE and policy engine, which match source and destination classes in JUNOS policy rules. To enable SCU/DCU-based billing:

1. Configure the JUNOS routing platforms in the network to support SCU/DCU accounting, ensuring that all traffic is tagged with the appropriate classes.

The classes depend on the routes that the routers use to forward the traffic. For information about configuring SCU/DCU accounting with the JUNOS software, see the JUNOS documentation set.

2. Configure policies that match the source and destination classes you defined and that contain accounting rules.
3. Configure the services to which enterprises subscribe to use these policies.

For example, a service provider may want to bill local and long-distance traffic at different rates. The service provider could achieve this goal as follows:

1. Configure the JUNOS routing platform to tag traffic that exits the SRC network with the class `netout` and traffic that stays within the network with the class `netin`.
2. Define a service called `LocalBestEffortData`, and associate with this service a policy that matches the destination class `netin` at output.
3. Define a service called `LongDistanceBestEffortData`, and associate with this service a policy that matches the destination class `netout` at input and output.

The service provider can monitor the use of each service and whether the traffic remains within the network. With this information, the service provider can bill the enterprise accordingly. An IT manager in the enterprise can subscribe to both services and can monitor the enterprise's use of each service through the portal.

Part 8

Managing Access Portals for Enterprise Subscribers

- Overview of Enterprise Service Portals on page 189
- Planning Deployment for Enterprise Service Portals on page 199
- Installing and Configuring Enterprise Service Portals on page 205
- Managing Services with Enterprise Manager Portal on page 219
- Managing Enterprise Service Portals on page 285
- Using NAT Address Management Portal on page 291
- Using the Sample Enterprise Service Portal on page 295
- Developing an Enterprise Service Portal on page 305

Chapter 17

Overview of Enterprise Service Portals

- Function of Enterprise Service Portals on page 189
- Enterprise Service Portals Provided with the SRC Software on page 191
- Enterprise Service Portal Audit Plug-In on page 193
- Network Information Collector with Enterprise Service Portals on page 193
- Service Parameters on page 193
- Substitutions and the Parameter Acquisition Path on page 194
- Managing Subscriptions to Aggregate Services on page 196
- Configuring Your Web Browser to Use an Enterprise Service Portal on page 196
- Accessing Enterprise Service Portals on page 196

Function of Enterprise Service Portals

The SRC software enables service providers to use enterprise service portals to provision services to enterprise subscribers who connect to the SRC network by means of a JUNOSe router or a JUNOS routing platform. An enterprise service portal is a standalone Web application that runs in a Java 2 Platform, Enterprise Edition (J2EE)-compliant Web application server. An enterprise service portal must have a corresponding configuration in the directory. Typically, a service provider provisions the router and configures the initial directory structure.

IT managers in an enterprise log in to the SRC network through an enterprise service portal. The managers can then activate services and perform some administrative tasks associated with their enterprises. When an IT manager requests an action through an enterprise service portal, the enterprise service portal uses the SRC software's enterprise service portal application programming interface (API) to interact with the SAE and to update data in the directory.

More specifically, the enterprise service portal calls methods in this API to:

- Authenticate IT managers in an enterprise.
- Create, delete, and modify accounts for IT managers.
- Navigate among retailers, enterprises, sites, and accesses.
- Create, delete, activate, and deactivate subscriptions to services.
- Get feedback from the sessions that a subscription generates. This feedback, which comes directly from the SAE managing the session, indicates whether the

session is active in the network and provides the values used for the service parameters.

- Get feedback about the use of resources, such as the number of bytes and packets the SAE has sent or received for a particular service.
- Configure values for service parameters .

Consistency of Data in the Directory

Enterprise service portals can monitor the consistency of data as you enter it through the portal; for example, an enterprise service portal can prevent you from deleting a subscription if that subscription depends on other data in the directory. Enterprise service portals do not constantly monitor the consistency of existing data in the directory for all subscribers, however, because doing so would consume significant network resources. Consequently, if you use an LDAP browser to modify data in the directory that was entered through a portal, you must be sure that the data in the directory is consistent.

Privileges of IT Managers

The enterprise service portal API controls the privileges that determine how IT managers can manipulate subscribers, subscriptions, and services associated with a retailer or enterprise. All IT managers in an enterprise share the same connections to the directory.

Developing and Customizing Enterprise Service Portals

You can customize enterprise service portals to provide customer-specific Web pages and supply specified services. By modifying JavaServer pages (JSP), which use a set of customized tags to call methods in the enterprise service portal API, you can customize an enterprise service portal to suit a customer's environment.

For information about the JSP tags that you can use to customize an enterprise service portal, see the documentation for the enterprise tag library on the Juniper Networks Web site at <http://www.juniper.net/techpubs/software/management/src/api-index.html>

Identifying the SAE

An enterprise service portal handles a request from an IT manager by communicating with the SAE that manages the subscriber affected by the IT manager's request. You can use the following methods to allow the enterprise service portal to identify which SAE manages a subscriber:

- For SRC implementations that use more than five SAEs, configure a network information collector (NIC) that takes the distinguished name (DN) of an access as the key and returns the corresponding SAE as the value.
- For SRC implementations that use five or fewer SAEs, you can use directory eventing to identify the SAEs. If you configure this option, SAEs update the addresses of their external interfaces in the directory at a specified time interval. Each update triggers an event that is sent to the enterprise service portal to confirm that the corresponding SAE is available. If the enterprise service portal

does not receive the update event within a certain time, the enterprise service portal assumes that the SAE is not available and subsequently does not send any service activation or feedback requests to that SAE. When the SAE becomes available and starts to manage subscribers again, the enterprise service portal sends new requests to that SAE.

Enterprise Service Portals Provided with the SRC Software

We provide several enterprise service portals in the in the SDK+AppSupport+Demos+Samples.tar.gz file on the Juniper Networks Web site at: <https://www.juniper.net/support/csc/swdist-erx/src.html> Some of the enterprise service portals we provide are intended for demonstration purposes or as a basis for developing a customized enterprise service portal for your SRC implementation. Other enterprise service portals are intended to serve a specific purpose and require little customization. The WAR files for the enterprise service portals contain all required libraries and Web contents.

The following enterprise service portals are available:

- Sample enterprise service portal
- Enterprise Manager Portal
- NAT Address Management Portal

Sample Enterprise Service Portal

The sample enterprise service portal incorporates many of the features that the enterprise service portal API offers. You can use the sample enterprise service portal to demonstrate the functionality available, and you can customize the sample enterprise service portal to create a portal for your own SRC implementation. The source code for the sample enterprise service portal is in its JSP pages; the code was created with the tags in the enterprise portal tag library.

For information about the JSP tags that you can use to customize an enterprise service portal, see the documentation for the enterprise tag library on the Juniper Networks Web site at <http://www.juniper.net/techpubs/software/management/src/api-index.html>

Enterprise Manager Portal

Service providers can deploy Enterprise Manager Portal to provision services for enterprise subscribers. IT managers can access the SRC network through this portal and select the services they require. Enterprise Manager Portal is a complete application for which you need to customize only style sheets and icons.

NAT Address Management Portal

Service providers can deploy this enterprise service portal to manage public IP addresses for use with NAT services on JUNOS routing platforms. IT managers make requests about public IP addresses through Enterprise Manager Portal. The service provider responds to these requests through NAT Address Management Portal. This

enterprise service portal is a complete application for which you need to customize only style sheets and icons.

When an IT manager makes a request about public IP addresses through Enterprise Manager Portal, Enterprise Manager Portal sends an e-mail to a human administrator or a machine. For small installations or demonstration purposes, a human administrator can manage the public IP addresses; however, for large installations, public IP addresses are managed by machines. NAT Address Manager handles two operations: the supply of new IP addresses and the return of unwanted public IP addresses.

If a human administrator provides the IP addresses, the administrator can access the Address Manager portal by clicking the portal address that is included in the e-mail from Enterprise Manager Portal. The administrator can then use NAT Address Management Portal to make a change to the IT manager's public IP addresses in the directory. The IT manager can view the changes through Enterprise Manager Portal and can use the assigned IP addresses in subscriptions to NAT services.

If you use a machine to manage public IP addresses, you must write an application that allows the machine to handle the e-mails that Enterprise Manager Portal sends. The e-mails contain XML code that NAT Address Management Portal and the machine must interpret. The following sequence of events describes how the machine interacts with the portals.

1. The IT manager requests one or more IP addresses through Enterprise Manager Portal.
2. Enterprise Manager Portal sends an e-mail to the machine that administers IP addresses.

The subject line of the e-mail contains the URL of NAT Address Management Portal. The body of the e-mail contains an SDXNATStatusRequest message—XML code that contains a request for information about the status of a particular access.

3. The machine forwards the e-mail to the URL in the subject line of the e-mail.
4. The machine extracts the SDXNATStatusRequest message from the e-mail and sends it by means of HTTP to NAT Address Management Portal.
5. NAT Address Management Portal analyzes the SDXNATStatusRequest message and returns an SDXNATStatusResponse message to the machine.
6. The machine analyzes the response and determines the next action, such as providing an IP address for the enterprise.
7. The machine sends the appropriate information in an SDXNATOperationRequest message to NAT Address Management Portal.
8. NAT Address Management Portal updates the directory and returns an SDXNATOperationResponse message to the machine.

When NAT Address Management Portal updates the directory, the IT manager can view the new status in Enterprise Manager Portal and can use the assigned IP addresses in subscriptions to NAT services.

The XML messages described above contain subordinate elements that depend on whether the IT manager's request is to obtain or return IP addresses. The document type definition (DTD) for the XML messages describes these subordinate elements. You can find the DTD in the in the **SDK+AppSupport+Demos+Samples.tar.gz** file on the Juniper Networks Web site at: <https://www.juniper.net/support/csc/swdist-erx/src.html>. The file is located in the folder **SDK/dtd**.

Enterprise Service Portal Audit Plug-In

The Enterprise Service Portal audit plug-in, also referred to as the enterprise service portal IT Manager audit plug-in or Enterprise Service audit plug-in, defines a callback interface, `net.juniper.sgmt.ent.plugin.AuditPluginEventListener`, which receives events when IT managers complete specified operations, such as subscribing to a service or changing the parameter substitutions of a subscription. The events report the type of operation, the identity of the IT manager, and other attributes.

You can write audit plug-in event listeners by implementing the callback interface. A listener performs tasks such as processing received events and then publishing the events to one or more event handlers, such as a log file, system log, or database. Events are sent after the corresponding operations have been completed. The plug-in processes events, which are sent synchronously, and then returns control to the enterprise service portal. Future events are blocked from being processed until the listener returns the thread.

Network Information Collector with Enterprise Service Portals

You can improve the performance of service activation for an enterprise service portal by implementing the NIC in your network. In this case, the enterprise service portal uses the NIC to locate the SAE managing a particular session. If you do not configure a NIC for your network, the enterprise service portal locates the managing SAE by polling all the SAEs in the network.

Related Topics ■ Locating Subscriber Management Information

Service Parameters

Subscribing to and activating services are only part of the functionality available through the enterprise service portal API. An enterprise service portal can also expose the power of service parameters.

An enterprise service is, at its core, a set of policies that affect network traffic when they are applied to the router interfaces associated with some subset of an enterprise's accesses. When these service policies are defined by the service provider, they can contain parameters. For example, a service that provides protection against denial-of-service attacks may limit the traffic on a specific port to a specific percentage of the bandwidth available on a router interface. Both the port and the percentage can be expressed as parameters in the service's network policies.

Service parameters allow for some very powerful functionality. For example, they allow the service provider to define a generic service that can be customized for specific enterprises or for specific sites or accesses within an enterprise. The enterprise

customer can perform this customization at any time (even while the service is active) through an enterprise service portal. The enterprise service portal must invoke a method in the enterprise API to provide the value for each parameter.

For an enterprise service portal to detect service parameters configured for fragment services for an aggregate service, the parameters must be defined in the configuration for the aggregate service.

Substitutions and the Parameter Acquisition Path

Each parameter in a service policy requires that a value be obtained. In the example above, the denial-of-service protection policies have two parameters: port number and bandwidth percentage. Each of those parameters in a service's network policies results in the creation of a variable. Policy configuration specifies the name of a variable.

Each of these variables must have a value assigned to it (unless it already has a default value). The enterprise service portal can obtain that value from the enterprise customer. The enterprise service portal must then call a method in the API to assign that value to the variable. The API will record this value by writing a substitution into an LDAP entry. A substitution is an LDAP entry attribute that, at its simplest, just assigns a value to a variable.

More than one substitution can exist for a given variable. Substitutions for a given variable can exist in any LDAP entry on the acquisition path. The acquisition path is a path through a sequence of LDAP entries. It begins with a most specific entry and ends with a most general entry. When the value for a given variable is specified through substitution attributes in multiple LDAP entries on this path, only the most specific entry's substitution is actually used.

The ordering of the LDAP entries in the acquisition path is always the same. Starting from the most specific, they are the:

1. SSP subscription entry under the access entry (if one exists for the service in question)
2. Access entry
3. SSP subscription entry under the site entry (if one exists for the service in question)
4. Site entry
5. SSP subscription entry under the enterprise entry (if one exists for the service in question)
6. Enterprise entry
7. Relevant localized version of the SSP service entry (if one exists)
8. SSP service entry

The acquisition path allows values assigned to variables at a more general place in the acquisition path to be overridden by values assigned at a more specific place in the acquisition path. This method enables an enterprise to subscribe to a given service, to specify values for that service's parameters at a more general place in the

acquisition path, and then to override those values at a more specific level according to the needs of local enterprise IT managers who control a given site or access.



NOTE: Each session of a subscription uses a different acquisition path (because each is associated with a different access). This means that each session of a subscription may end up with different values for a given service parameter. For each session, the enterprise API exposes detailed information about the actual values used for every service parameter.

Power of Substitutions

In addition to assigning values to the variables that are used as service parameters, a substitution can declare that the value it assigns is fixed. When a fixed value is declared, substitutions for the same variable that exist in more specific places in the acquisition path are ignored (that is, the fixed value cannot be overridden). More important, a substitution can specify the value for a variable as an expression that includes other variables. A substitution can also introduce new variables. The new variables are then available for use in other substitutions at any more specific point on the acquisition path. Enterprise service portals that expose these features allow enterprises to define their own way of presenting and managing service parameters. For more detail on service parameters, the acquisition path, and the uses of substitutions, see *Parameters and Substitutions* and *Value Acquisition for Single Subscriptions*.

Substituting Values for Policy Parameters

The value substitution feature of an enterprise service portal gives the enterprise IT manager the ability to customize subscribed services in his or her sphere of control. The enterprise IT manager can be required to provide a set of substitutions that define the values for the parameters of the underlying service policies everywhere the policies are applied. Sample parameter types that might require value substitution include:

- Network—Address/prefix length pairs that denote networks
- Interface—Router interface specifications
- Protocol—Eight-bit unsigned integers enumerating protocols such as IP, TCP, and UDP
- Rate—32-bit unsigned integers used for rate-limit and burst-size calculations

For example, the service provider could offer a service to the enterprise that applies a firewall policy. The firewall policy could screen ingress traffic from a source network and redirect the screened traffic to a specific destination. The enterprise IT manager might want to specify at the time of subscription or subscription activation which source networks are involved. The service provider establishes a general policy template, in this case configuring the destination. The enterprise IT manager modifies the template by means of value substitution for the particular needs of the enterprise, such as providing a range of IP addresses for one or more source networks.

A different service might have an egress rate-limit policy with policy rules to screen egress traffic from the source network, by protocol, or according to a traffic rate limit. Value substitution for the parameters defined in the generic policy template enables the manager to define the policy to match the needs of the enterprise.

Note that parameter names provided to one customer can be renamed by the service provider to suit the needs of another customer. For example, one customer might prefer a parameter named “ department” to one named “ network” because that name better fits the enterprise hierarchy.

The service provider can specify whether all parameters or only certain ones can be modified in the enterprise service portal by the enterprise IT manager by means of value substitution. Likewise, an IT manager can determine whether subordinate managers have the ability to modify a given service parameter. Parameters for which values cannot be substituted at a given level are said to be fixed at some higher level. For example, in the sample portal, the enterprise service portal populates drop-down lists from which the manager at that level can select values to substitute. If a parameter substitution is fixed at a higher management level, lower-level managers will not see options for substituting for that parameter in the drop-down lists on their instance of the enterprise service portal.

- Related Topics**
- Parameters and Substitutions
 - Value Acquisition for Multiple Subscriptions

Managing Subscriptions to Aggregate Services

If an enterprise service portal manages subscriptions to aggregate services, ensure that each parameter defined for a fragment service is also defined in the aggregate service.

- Related Topics** *SRC PE Services and Policies Guide.*

Configuring Your Web Browser to Use an Enterprise Service Portal

Before you can use an enterprise service portal, you must enable your Web browser to:

- Allow cookies from the enterprise service portal.
- (Enterprise Manager Portal and NAT Address Management Portal only) Use JavaScript.

Accessing Enterprise Service Portals

When viewing the enterprise service portals, take care to open only one browser window yourself. The portals automatically open pop-up windows for various operations. If you open more than one browser window yourself, the information in the original window may not be updated correctly when you complete an operation in a pop-up window.

To access an enterprise service portal:

1. Enter the URL of the portal in your Web browser, and press Enter. For example, to access Enterprise Manager Portal, type:

http://192.0.2.1:8080/entmgr

The enterprise service portal displays the login page.

2. Select your service provider from the Retailer menu.
3. Enter your username in the Login ID field and your password in the Password field.

The enterprise service portal displays your Welcome page. On the left of the page is a navigation pane for the objects in the service provider's directory over which you have control. Your login identity is the root of this navigation pane.

Chapter 18

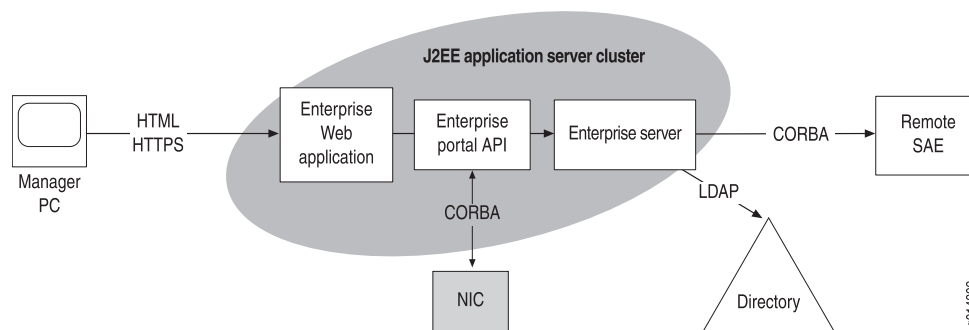
Planning Deployment for Enterprise Service Portals

- Architecture of Enterprise Service Portals on page 199
- Deployment Scenario for an Enterprise Service Portal on page 200
- Deciding Which Enterprise Service Portal to Use on page 201
- Planning Number of Instances of an Enterprise Service Portal on page 202
- Planning Namespace Hierarchy for an Enterprise Service Portal on page 202

Architecture of Enterprise Service Portals

Figure 16 on page 199 shows the basic elements and communication protocols of an enterprise service portal.

Figure 16: Elements and Communication Protocols for an Enterprise Service Portal



Elements for an Enterprise Service Portal

An enterprise service portal consists of a server cluster that communicates with the following network elements:

- Directory system—A distributed set of directories with information shadowing and chaining agreements between master and slave servers
- (Optional) Network information collector

For SRC implementations that use more than five SAEs, an enterprise service portal requires a NIC to identify which SAE is managing a subscriber. This NIC

takes the distinguished name (DN) of an access as the key and returns the corresponding SAE as the value. For SRC implementations that use five or fewer SAEs, you can use directory eventing to identify the SAEs.

- Remote SAE
- Manager PC—A client PC on which a person managing an enterprise runs a Web browser to communicate with an enterprise service portal

Internally, an enterprise service portal consists of a J2EE application server cluster that implements an Enterprise API or Enterprise Tags Library, an enterprise Web application that uses one of these interfaces, and an enterprise server. The enterprise server requires persistent sessions in the cluster. That is, the cluster member that receives the first manager session request must receive all subsequent requests for the same session.

Communication Protocols

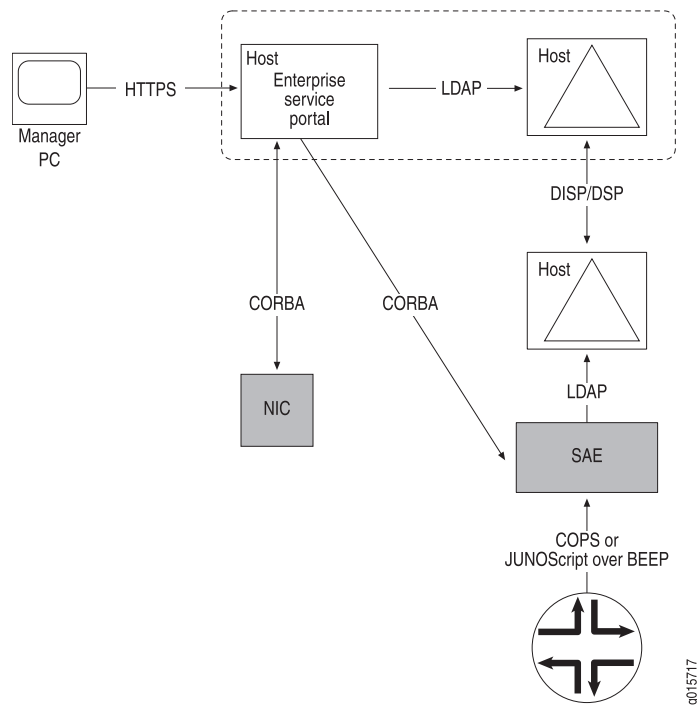
Table 18 on page 200 describes the communication protocols that are used between elements in the enterprise service portal network.

Table 18: Communication Protocols for an Enterprise Service Portal

Protocol	Used for Communication Between
HTML/HTTPS (HyperText Markup Language over Secure HyperText Transmission Protocol)	Enterprise manager's Web browser and the enterprise portal Web application running in the enterprise service portal
Enterprise Portal API	Enterprise Web application and the enterprise server
CORBA	Enterprise server and remote SAEs running in a different Web application server than the enterprise server
LDAP	Enterprise server and SRC directories

Deployment Scenario for an Enterprise Service Portal

Figure 17 on page 201 shows component interactions for a sample deployment of an enterprise service portal.

Figure 17: Deployment for an Enterprise Service Portal

The directory servers are synchronized by means of server-to-server protocols, such as DISP and DSP in the case of X.500 directories, and DirX and equivalent protocols in the case of native LDAP directories, such as Sun ONE Directory Server.

In this configuration, bulk service session requests and implicit subscription reactivation caused by substitution changes are made through replication of directory information. The enterprise service portal writes new information to its local directory, and the server-to-server protocols transfer the information to the SAE's local directory. Then the SRC directory eventing system notifies the SAE of the new information, and the SAE reacts by activating and deactivating subscriptions.

The enterprise service portal receives feedback on the session state and parameter values of a session using remote procedure calls through the CORBA connection directly to the SAE managing the session.

Deciding Which Enterprise Service Portal to Use

Table 19 on page 201 describes which application to use in your organization.

Table 19: Enterprise Service Applications

To Perform This Task	Use This Application
Provide services to a number of enterprises, and let IT managers at the enterprises manage services for their enterprise	Enterprise Manager Portal

Table 19: Enterprise Service Applications *(continued)*

To Perform This Task	Use This Application
Manage address allocation	NAT Address Management Portal with Enterprise Manager Portal
Provide custom management functions through an enterprise service portal	Customized version of the sample Enterprise Service Portal

Planning Number of Instances of an Enterprise Service Portal

When you are planning an SRC network that uses enterprise service portals, consider how many instances of the enterprise service portal you need. For example, if your network has multiple points of presence (POPs), you may want to install an enterprise service portal in each POP.

Planning Namespace Hierarchy for an Enterprise Service Portal

Each enterprise service portal that you install must have a namespace that defines the location of its configuration in the directory. The namespaces form a hierarchy of LDAP entries, and a namespace inherits all the properties defined in its parent namespaces. Properties defined in subordinate namespaces override properties of the same name inherited from parent namespaces. Multiple enterprise service portals can use the same namespace if all the properties in the configurations are identical.

For example, in the sample data, the namespaces for Enterprise Manager Portal and NAT Address Management Portal are subordinate to the namespace for the sample Enterprise Service Portal (see Table 20 on page 202). Consequently, the subordinate configurations inherit property definitions from the sample Enterprise Service Portal configuration, unless specific settings in the subordinate configurations override those in the sample Enterprise Service Portal configuration.

Table 20: Namespaces for Enterprise Service Portals

Name of Enterprise Service Portal	Namespace
Sample Enterprise Service Portal	<i>l = EASP, ou = staticConfiguration, ou = Configuration, o = Management, o = umc</i>
Enterprise Manager Portal	<i>l = ENT-MGR, l = EASP, ou = staticConfiguration, ou = Configuration, o = Management, o = umc</i>
NAT Address Management Portal	<i>l = ADDR-MGR, l = EASP, ou = staticConfiguration, ou = Configuration, o = Management, o = umc</i>

You can use the hierarchy of namespaces to minimize the number of properties you configure for a particular instance of an enterprise service portal. For example, suppose you want to deploy two instances of Enterprise Manager Portal in different

POPs—Ottawa and Montreal. The POPs use the same directory for services; however, each POP uses its own directory for subscribers.

To minimize the number of properties you configure for the enterprise service portal, you can:

1. Create the following two namespaces subordinate to *l = ENT-MGR*, *l = EASP*, *ou = staticConfiguration*, *ou = Configuration*, *o = Management*, *o = umc*:
 - *l = ENT-MGR-Ottawa*
 - *l = ENT-MGR-Montreal*
2. Configure information about the service directory in *l = ENT-MGR*, *l = EASP*, *ou = staticConfiguration*, *ou = Configuration*, *o = Management*, *o = umc*.
3. Configure information about the respective subscriber directories in *l = ENT-MGR-Ottawa* and *l = ENT-MGR-Montreal*.

Chapter 19

Installing and Configuring Enterprise Service Portals

- Before You Install an Enterprise Service Portal on page 205
- Setting Up Enterprise Service Portals on page 206
- Preparing the Web Applications for Customization on page 206
- Configuring Connections to the Directory on page 207
- Configuring Deployment Settings for Enterprise Manager Portal on page 209
- Configuring the URL for an Enterprise Service Portal on page 215
- Writing an Application to Allow a Machine to Provide Public IP Addresses for NAT on page 215
- Configuring an Enterprise Service Portal Audit Plug-In on page 216

Before You Install an Enterprise Service Portal

Before you install the enterprise service portal:

- Identify the machine on which you want to install the application.

If you plan to use Enterprise Manager Portal and NAT Address Management Portal, which work together but serve different purposes, you must install both portals. You can install these portals on the same or different machines.
- Install a Web application server on the machine on which you want to install the enterprise service portal.
- If you use JBoss or another Web application server that performs load balancing, you must configure the Web application server to use *sticky sessions* to process requests to the enterprise service portal.

Sticky sessions are sessions between a server and client in which information is preserved between different transactions in an activity. When a server establishes a session for an activity with a particular client, the Web application server preserves session information by sending subsequent requests from the client to the same server. For enterprise service portals, use of sticky sessions ensures that the Web application server always routes requests from IT managers to the same instance of the enterprise service portal that they logged into.

For information about configuring sticky sessions for the Web application server, see the documentation for your Web application server.

- Determine how you will identify the SAE that manages a subscriber who connects to the SRC network through an enterprise service portal. . If you will use a network information collector (NIC) for this purpose, configure a NIC that takes the distinguished name (DN) of an access and returns the corresponding SAE reference (for more information about the NIC, see Locating Subscriber Management Information).
- In the directory, create any new namespaces for the enterprise service portals you will install. . To create a namespace, you can copy one of the enterprise service portal configurations included with the same data to another location in the directory.

Setting Up Enterprise Service Portals

Tasks to install an enterprise service portal are:

1. “Preparing the Web Applications for Customization” on page 206
2. “Configuring Connections to the Directory” on page 207
3. (Enterprise Manager Portal only) “Configuring Deployment Settings for Enterprise Manager Portal” on page 209
4. “Configuring the URL for an Enterprise Service Portal” on page 215

After you install an enterprise service portal:

- If you use a machine to administer public IP addresses in conjunction with NAT Address Management Portal, write an application to handle the interaction between the machine and this portal. See “Writing an Application to Allow a Machine to Provide Public IP Addresses for NAT” on page 215.
- If you use Enterprise Manager Portal, NAT Address Management Portal, or an application that uses a configuration file based on the `easp_conf` template, see “Configuring an Enterprise Service Portal Audit Plug-In” on page 216.

Preparing the Web Applications for Customization

When customizing the Web applications, copy the WAR files to a temporary folder and work in that folder.

To copy the WAR file to a temporary folder:

1. Login as root or another authorized user.
2. Create a temporary folder in which you will work on the WAR file. For example:

```
mkdir tempWar
```

3. Access the temporary folder. For example:

```
cd tempWar
```

4. Copy the WAR file to the temporary folder.

```
cp /cdrom/cdrom0/webapp/<filename>
```

< filename > —Name of the WAR file; for example, *entmgr.war*

Configuring Connections to the Directory

To configure a connection between the Web application and the directory that contains the configuration for the enterprise service portal:

1. Access the temporary folder to which you copied the WAR file.

```
cd tempWar
```

2. Extract the *boot.props* file from the WAR file.

```
jar xvf <filename> WEB-INF/boot.props
```

< filename > —Name of the WAR file; for example, *entmgr.war*

3. Edit the *boot.props* file with any text editor.

See “Initialization Properties for Enterprise Service Portals” on page 207.

4. Replace the *boot.props* file in the WAR file.

```
jar uvf <filename> WEB-INF/boot.props
```

Initialization Properties for Enterprise Service Portals

In the boot properties file for an enterprise service portal, you can modify the following fields.

Config.java.naming.provider.url

- URL of the primary directory in URL string format.
- Value—`ldap:// <host> : <portNumber> /`
 - < host > —IP address or name of the host that supports the directory
 - < portNumber > —Number of the TCP port
- Default—`ldap://127.0.0.1:389/`

Config.java.naming.security.credentials

- Password that the Web application server uses to authenticate and authorize access to the directory.
- Value— < password >
- Guidelines—The password can be encoded in base64 and not visible in plain text. To use an encoded value, use the format {BASE64} < encoded-value > .
- Default—ent

Config.java.naming.security.principal

- DN that contains the username that the Web application server uses to authenticate and authorize access to the directory.
- Value—DN of the object that contains the username
- Default—*cn = ent-admin, o = operators, o = umc*

Config.net.juniper.smgmt.des.backup_provider_urls

- Redundant directories that store configuration information.
- Value—List of URLs in URL string format separated by semicolons (see description for the property).
- Default—*ldap://127.0.0.1:389/; ldap://127.0.0.1:389/*

Config.net.juniper.smgmt.des.<propertySuffix>

- Set of properties that specify how the Web application interacts with the directory.

See *SRC 2.0.x Getting Started Guide*.

See *SRC 2.0.x Getting Started Guide*.

Config.net.juniper.smgmt.lib.config.staticConfigDN

- Root of the static configuration properties.
- Value—DN of the object that contains the username
- Default—*ou = staticConfiguration, ou = configuration, o = Management, o = umc*

Config.EASP.namespace

- Location of the enterprise service portal's configuration in the directory.
- Value—Path, relative to the root of the static configuration properties, that defines the location
- Guidelines—If you are using the enterprise service portals we provide, use the defaults, which match the locations of the configurations in the sample data.
- Default—Depends on the enterprise service portal:
 - Sample Enterprise Service Portal—/EASP

- Enterprise Manager Portal—/EASP/ENT-MGR
- NAT Address Management Portal—/EASP/NAT-ADDR

Configuring Deployment Settings for Enterprise Manager Portal

You configure deployment settings for Enterprise Manager Portal. You do not need to configure deployment settings for the sample Enterprise Service Portal or NAT Address Management Portal.

To configure deployment settings for Enterprise Manager Portal:

1. Access the temporary folder to which you copied the WAR file.

```
cd tempWar
```

2. Extract the *web.xml* file from the WAR file.

```
jar xvf entmgr.war WEB-INF/web.xml
```

3. Edit the *web.xml* file in the *entmgr.war* file with any text editor.

See “Deployment Properties for Enterprise Manager Portal” on page 209.

4. Replace the *web.xml* file in the WAR files.

```
jar uvf entmgr.war WEB-INF/web.xml
```

Deployment Properties for Enterprise Manager Portal

The *web.xml* file contains deployment properties for Enterprise Manager Portal. This file specifies which applications Enterprise Manager Portal displays and specifies how to generate e-mails when IT managers request public IP addresses through this enterprise service portal. You can modify the following fields.

showBasicBandwidthOnDemand

- Whether or not the enterprise service portal displays basic bandwidth-on-demand (BoD) features.
- Value
 - True—Displays the basic BoD features

- False—Hides the basic BoD features
- Guidelines—Specify True if you want to provision basic BoD with a JUNOS routing platform. When enabled, service providers can offer basic BoD services to IT managers as service options that affect all traffic on an access link, including customizing the amount of bandwidth provided to meet their traffic requirements.

To make class of service (CoS) services available, BoD services and basic BoD services must be enabled. If both are enabled, IT managers must select a basic BoD service before they can subscribe to BoD services.

- Default—True

showBandwidthOnDemand

- Whether or not the enterprise service portal displays BoD features.
- Value
 - True—Displays the BoD features
 - False—Hides the BoD features
- Guidelines—Specify True if you want to provision BoD with a JUNOS routing platform. To make CoS services available, BoD services and basic BoD services must be enabled. If both are enabled, IT managers must select a basic BoD service before they can subscribe to BoD services.
- Default—True

showFirewall

- Whether or not the enterprise service portal displays firewall features.
 - Value
 - True—Displays the firewall features
 - False—Hides the firewall features
 - Guidelines—Specify True if you want to provision firewall services with a JUNOS routing platform.
- If you set showFirewall to True and statelessFirewall to False, the portal provides support for stateful firewalls on JUNOS routing platforms.
- Default—True

statelessFirewall

- Whether or not the enterprise service portal displays stateless firewall features.
- Value
 - True—Displays the stateless firewall features

- False—Hides the stateless firewall features
- Guidelines—Specify True if you want to provision firewall services on a JUNOS routing platform. The showFirewall field must also be set to True.

When you set statelessFirewall to True, the Firewall tab but not the Application tab appears in Enterprise Manager Portal.

You can configure either stateless firewalls or stateful firewalls from Enterprise Manager Portal. If you set showFirewall to True and statelessFirewall to False, the portal provides support for stateful firewalls on JUNOS routing platforms.

- Default—True

showNat

- Whether or not the enterprise service portal displays NAT features.
- Value
 - True—Displays the NAT features
 - False—Hides the NAT features
- Guidelines—Specify True if you want to provision NAT services with a JUNOS routing platform. If this property is set to True, the enterprise service portal always displays the firewall features, regardless of the value of the showFirewall property.
- Default—True

showSchedule

- Whether or not the enterprise service portal displays scheduling features for services.
- Value
 - True—Displays the scheduling features
 - False—Hides the scheduling features
- Default—True

showVpn

- Whether or not the enterprise service portal displays VPN features.
- Value
 - True—Displays the VPN features

- False—Hides the VPN features
- Guidelines—Specify True if you want to provision VPNs with a JUNOS routing platform. If you set this property to True, you must also set the showBandwidthOnDemand property to True.
- Default—True

showExtranet

- Whether or not the enterprise service portal displays VPN extranet features.
- Value
 - True—Displays the VPN extranet features
 - False—Hides the VPN extranet features
- Guidelines—Specify True if you want to provision VPN extranets with a JUNOS routing platform. If you set this property to True, you must also set the showVPN property to true.
- Default—True

junoseCompatibleBoD

- Whether or not the enterprise service portal can be used to configure BoD services on JUNOSe routers.
- Value
 - True—Provides configuration for BoD services on JUNOSe routers
 - False—Does not provide configuration for BoD services on JUNOSe routers
- Guidelines—If set to true, this field allows BoD services to be configured for JUNOSe routers as well as JUNOS routing platforms. This setting limits the configuration for IP protocol, source IP address, source port or port range, destination IP address, and destination port or port range for a BoD rule to one each for JUNOS routing platforms as well as JUNOSe routers. The online help indicates that users can specify one value for these fields if **junoseCompatibleBoD** is set to True, and that users can specify more than one value for these fields if **junoseCompatibleBoD** is set to False.

Consider that if both JUNOS routing platforms and JUNOSe routers exist in an enterprise's network, IT managers who are using the enterprise service portal to configure their SRC-managed environment do not know which routers are JUNOSe routers and which are JUNOS routing platforms.

- Default—False

machineReadableNotifications

- Format of the e-mails that indicate that public addresses have been requested or released for a particular access link.
- Value

- True—E-mails contain XML code and will be handled by a machine.
- False—E-mails contain ordinary text and will be handled by a human administrator.
- Default—False

renotificationInterval

- Minimum time between e-mails that notify the service provider about outstanding requests for IP addresses.
- Value—Number of seconds in the range 1–2147483647
- Guidelines—For actual SRC implementations that use a human administrator, we recommend a value of 86400 seconds (1 day). For demonstrations of the SRC software that use a human administrator, we recommend a value of 240 seconds. For actual SRC implementations that use machines, the value depends on how you design an application to handle the e-mails; a value of 600 seconds (10 minutes) may be a good starting point.
- Default—120
- Example—200

addressManagerUrl

- URL of NAT Address Management Portal that the service provider uses to manage public IP addresses for enterprises. This value is included in the e-mails about IP addresses.
- Value—URL in the format

http://<host>:<port><path>

- <host> —Name or IP address of the machine on which you install the Web application for NAT Address Management Portal
 - <port> —TCP/UDP port for HTTP traffic
 - <path> —Path to location of the Web application
- Default—http://example.com:8080/nataddr/AddressManager

mail.smtp.host

- SMTP mail server that Enterprise Manager Portal uses to send e-mails about requests for or release of public IP addresses.
- Value—Name or IP address of the mail server
- Default—mailhost

notificationFrom

- Sender's address in e-mails that Enterprise Manager Portal sends about public IP addresses.
- Value—Text string that specifies the sender's name and e-mail address in XML format
- Guidelines—Be sure to use the correct XML escape sequences for any special characters in the value.
- Default—"Enterprise Portal" <entMgrPortal@example.com >

notificationTo

- Human administrator or machine to which Enterprise Manager Portal should send e-mails about requests for or release of public IP addresses.
- Value—Text string that specifies the name and e-mail address of the human administrator or machine in XML format
- Guidelines—Be sure to use the correct XML escape sequences for any special characters in the value.
- Default—"Public IP Address Manager" <ipManager@example.com >

notificationSubject

- Text used for the subject of e-mails about requests for or release of public IP addresses.
- Value—Text string that specifies the subject of the e-mail in XML format
- Guidelines—This value is not used if you configure e-mails to be machine-readable notifications. Be sure to use the correct XML escape sequences for any special characters in the value.
- Default—An IP request or release needs your attention.

renotificationSubject

- Text used for the subject of reminders to administrators about requests for or release of public IP addresses.
- Value—Text string that specifies the subject of the e-mail in XML format
- Guidelines—This value is ignored if you configure e-mails to be machine-readable notifications. Be sure to use the correct XML escape sequences for any special characters in the value.
- Default—REMINDER: An IP request or release still needs your attention.

notificationText

- Text that appears in the body of the e-mail.
- Value—Text string in XML format that specifies the body of the e-mail message

- Guidelines—This text and the URL appear in the body of the message if you specify that the e-mails are not machine-readable notifications. Otherwise, the URL appears in the subject, and the body is an XML document indicating which access needs attention. Be sure to use the correct XML escape sequences for any special characters in the value.
- Default—Please click on the link in this e-mail to go to a Web page where you will be able to fulfill a customer's request for public IP addresses, or acknowledge a customer's release of public IP addresses.

maxIpPoolSize

- Maximum number of public IP addresses that you can include in the pool that is used for the dynamic source NAT service.
- Value—Integer in the range 0–2147483647
- Guidelines—Configure this property if you want to provide NAT addresses through NAT Address Management Portal. Consult the JUNOS documentation for information about the maximum for each JUNOS routing platform.
- Default—32

Configuring the URL for an Enterprise Service Portal

The way you deploy the enterprise service portals depends on your Web application server. See the documentation for your Web application server for information about the deployment.

By default, the name of the WAR file determines the URL that you use to access the enterprise service portal. For example, if the name of the WAR files is *entmgr.war*, the URL for the enterprise service portal is `http:// <host> : <port> /entmgr`.

- `<host>` —Name or IP address of the machine on which you install the enterprise service portal
- `<port>` —TCP/UDP port for HTTP traffic

If you want use a different URL, you must modify the relevant configuration file for your Web application server. For information about this task, see the documentation for your Web application server.

Writing an Application to Allow a Machine to Provide Public IP Addresses for NAT

If you use Enterprise Manager Portal and NAT Address Management Portal, and you use a machine to administer public IP addresses that you provide to enterprises.

To use a machine to administer public IP addresses:

1. Write an application that handles:
 - E-mails from Enterprise Manager Portal

- XML messages that NAT Address Management Portal uses to communicate with the software that manages the IP addresses
2. Install the application that you created in the preceding step on a machine that contains the software for managing IP addresses.

Configuring an Enterprise Service Portal Audit Plug-In

The SRC software provides a sample event listener, `DefaultAuditEventListener`. You can use the sample listener, customize it, or use the information in the sample to create another audit plug-in. The sample event listener and its documentation is in the `SDK+AppSupport+Demos+Samples.tar.gz` file on the Juniper Networks Web site at: <https://www.juniper.net/support/csc/swdist-erx/src.html>. You can locate the application in the directory `/SDX/doc/ent/plugin/doc/net/juniper/smg/ent/plugin`. The sample listener sends output to a log file. The documentation for the plug-in is also in the `SDK+AppSupport+Demos+Samples.tar.gz` file in the folder `/SDX/doc/ent/plugin/doc`. You can also find the documentation on the Juniper Networks Web site at <http://www.juniper.net/techpubs/software/management/src/api-index.html>.

If you create an audit plug-in, you add the plug-in class to the WAR file for the enterprise service portal.

Table 21 on page 216 shows the common information that is provided by every enterprise service portal audit plug-in event.

Table 21: Common Audit Plug-In Information

Information	Description
Manager DN	Distinguished name that identifies the manager's profile in the directory; for example: <i>cn = unimgr, enterprisename = jnpr, ou = local, retailername = default, o = users, o = umc</i>
Manager principle	Manager's fully qualified log-in principle for logging in to the enterprise portal. For example, the equivalent principle for the Manager DN above is: <i>unimgr@jnpr.local/default</i>
Operation time	Time when the corresponding operation was successfully completed.

Table 22 on page 216 describes the events that an audit plug-in listener can listen for and the information reported in those events.

Table 22: Events Reportable to the Audit Plug-In

Event	IT Manager Action That Initiates Event	Information Reported
ManagerLoginEvent	Logs in to an enterprise service portal.	Common information only.

Table 22: Events Reportable to the Audit Plug-In (continued)

Event	IT Manager Action That Initiates Event	Information Reported
ManagerLogoutEvent	Logs out of an enterprise service portal.	Common information only.
SubscribeAuditEvent	Subscribes to a service.	Common information plus: <ul style="list-style-type: none"> ■ DN of the new subscription object in the directory. ■ Attributes of the new subscription, including sspState, sspAction, and parameterSubstitution.
UnsubscribeAuditEvent	Unsubscribes from a service.	Common information plus: <ul style="list-style-type: none"> ■ DN of the subscription object removed from the directory. ■ Attributes of the removed subscription, including sspState, sspAction, and parameterSubstitution.
SubscriberUpdateAuditEvent	Changes the parameterSubstitution attribute of a subscriber object, such as adding or removing a substitution from the IT manager's enterprise object.	Common information plus: <ul style="list-style-type: none"> ■ DN of the subscriber object that is changed. ■ Attributes changed in the operation, including the old values and new values of the attributes.
SubscriptionUpdateAuditEvent	Changes the parameterSubstitution attribute of a subscription object; suspends, resumes, activates, or deactivates a subscription.	Common information plus: <ul style="list-style-type: none"> ■ DN of the subscription object that is changed. ■ Old and new values of the changed attributes: ■ parameterSubstitution attribute when subscriber object is changed. ■ sspState attribute when subscription is suspended or resumed. ■ sspAction attribute when subscription is activated or deactivated.

Table 22: Events Reportable to the Audit Plug-In (continued)

Event	IT Manager Action That Initiates Event	Information Reported
ServiceOpStateAuditEvent	<p>Changes the operational state of a session.</p> <p>NOTE: Because changing the operational state of the session—such as dynamically activating or deactivating a subscription session—does not change the directory entry, the change is not persistent, and the subscription session returns to its administrative state after the subscriber's interface is restarted. Changes to the administrative state of a subscription are reported with the SubscriptionUpdateAuditEvent.</p>	<p>Common information plus:</p> <ul style="list-style-type: none"> ■ DN of the subscriber that owns the subscription session. The subscriber must be a leaf in the subscriber tree in the enterprise scenario. ■ DN of the subscription object where the subscription session comes from. ■ Operational state of the session after the IT manager's action.
ExportAuditEvent	Exports a VPN.	<p>Common information plus:</p> <ul style="list-style-type: none"> ■ DN of VPN that is exported. ■ DN of the subscriber to which the VPN is exported.
UnexportAuditEvent	Cancels the export of a VPN.	<p>Common information plus:</p> <ul style="list-style-type: none"> ■ DN of VPN for which export is canceled. ■ DN of the subscriber for which export of the VPN was canceled.

Chapter 20

Managing Services with Enterprise Manager Portal

- Overview of Enterprise Manager Portal on page 219
- Getting Help on Enterprise Manager Portal on page 220
- Setting the Configuration Level for Enterprise Manager Portal on page 220
- Managing Schedules on page 221
- Managing Subscriptions to Bandwidth-on-Demand Services on page 228
- Integrating VPNs into an SRC Network Through Enterprise Manager Portal on page 244
- Classifying Traffic for Stateful Firewall Exceptions and NAT Rules on page 248
- Subscribing to Firewall Services Through Enterprise Manager Portal on page 254
- Working with IP Addressing and NAT Services on page 272
- Monitoring the Status of Subscriptions on page 280
- Troubleshooting Subscriptions That Are Not Functioning Correctly on page 283
- Troubleshooting Subscriptions of Unknown Status on page 285

Overview of Enterprise Manager Portal

IT managers who connect to the SRC network through a JUNOS routing platform or JUNOSe router can use Enterprise Manager Portal to activate services, subscribers, and subscriptions for that enterprise. The services that IT managers can use depend on those that the service provider offers. In SRC-managed environments that include both JUNOS routing platforms and JUNOSe routers, the router type determines which types of services can be configured on a system. The portal does not indicate whether a router is a JUNOS routing platform or a JUNOSe router. Table 23 on page 219 lists the types of services that can be configured from Enterprise Manager Portal for JUNOSe routers and JUNOS routing platforms.

Table 23: Portal Configuration Support for Services on Routers

Type of Service	JUNOSe Router	JUNOS Routing Platform
BoD services	Yes	Yes
VPNs	No	Yes

Table 23: Portal Configuration Support for Services on Routers *(continued)*

Type of Service	JUNOSe Router	JUNOS Routing Platform
Applications	No	Yes
Firewall services	No	Yes
NAT services	No	Yes

If you offer Network Address Translation (NAT) services, IT managers can also use the portal to request public IP addresses for use with NAT services on an access.

Getting Help on Enterprise Manager Portal

Most fields in the portal offer tool tips. To view tool tips for a field in the portal, hold the cursor over that field in the portal.

Some fields and pages in the portal offer more extensive online help. To view this help, click the help icon .

Setting the Configuration Level for Enterprise Manager Portal

The default setting for the configuration level is Normal. With this setting you can configure most services on a JUNOS routing platform. If you want to configure more advanced features, such as static source NAT rules, you must change the configuration level of the portal. To do so:

1. Click the operator icon in the navigation pane.

The operator's Welcome page appears.



Virneo Enterprise Portal

[Log out](#)

Navigation

- ent-admin
- default
- retailer-one
- retailer-two
- SP
- virtual-SP

Refresh

Welcome ent-admin

Please click on the tree to the left to view or modify the enterprises, sites, accesses, services, and managers under your control.

You are currently logged in as:
ent-admin

Your scope of control is:

Retailer:	all
Retailer Folders:	all
Enterprise:	all
Enterprise Folders:	all
Site:	all
Site Folders:	all
Access:	all

You have the following privileges:

Administrator:	true
Activate subscriptions:	false
Modify subscriptions:	false
Modify substitutions:	false

Portal mode:
Normal

© Virneo 2004

2. Select **Advanced** from the Portal mode drop-down list.

Managing Schedules

You can establish schedules for specified services through the Enterprise Manager Portal. Topics include:

- Schedules in Enterprise Manager Portal on page 221
- Enabling Scheduling for the Enterprise Manager Portal on page 222
- Using Schedules in Enterprise Manager Portal on page 222
- Disabling a Schedule for a Service in Enterprise Manager Portal on page 227
- Changing Schedules in Enterprise Manager Portal on page 228

Schedules in Enterprise Manager Portal

An IT manager can configure schedules to be applied to BoD or firewall services for a specified enterprise subscriber. From Enterprise Manager Portal, you can establish schedules that identify the times when a specified BoD or firewall service can be activated or deactivated. Schedules are configured on a per-subscriber basis; they cannot be shared with other subscribers. Schedules are, however, inherited by subscribers subordinate to the subscriber for which the schedule is configured.



NOTE: NAT services cannot be scheduled.

Whether or not scheduling is available depends on the configuration for Enterprise Manager Portal and for the service.

Enabling Scheduling for the Enterprise Manager Portal

To enable scheduling:

1. Edit the *web.xml* file for the portal to enable scheduling.

When scheduling is enabled for the portal, a Schedules tab appears on Enterprise Manager Portal page.

2. Enable scheduling for the BoD or firewall service to be scheduled from Enterprise Manager Portal.

If you plan to schedule BoD or firewall service subscriptions, you can configure the schedules first so that you can assign schedules at the time that you configure the subscription. If the subscriptions are already configured, you can edit the service definition to assign a schedule. The Schedules page lets you create new schedule definitions and view and change existing ones.

Each subscription, whether to the same service or to another one, can have its own schedule.

Using Schedules in Enterprise Manager Portal

Tasks to use a schedule are:

1. Creating a Schedule in Enterprise Manager Portal on page 222
2. Applying a Schedule to a Service in Enterprise Manager Portal on page 226

Creating a Schedule in Enterprise Manager Portal

To create a schedule:

1. Click the **Schedules** tab.

The Schedules page appears.

default	>	local	>	Acme	>	Boca	>	Primary	>												
<div> Bandwidth & VPNs Applications Firewall Addresses NAT Schedules Managers </div> <table> <thead> <tr> <th>Schedule Name</th> <th>Definition</th> <th></th> </tr> </thead> <tbody> <tr> <td>Promotional</td> <td>Occurs on 02/07/2005 from 00:00 for 1 week(s)</td> <td> <div>Edit</div> <div>Delete</div> </td> </tr> <tr> <td>GoldVideo</td> <td>Occurs every Sunday,Saturday effective 02/01/2005 until 06/01/2005 from 00:01 for 23 hour(s)</td> <td> <div>Edit</div> <div>Delete</div> </td> </tr> <tr> <td colspan="3"> <div>Create</div> </td> </tr> </tbody> </table>										Schedule Name	Definition		Promotional	Occurs on 02/07/2005 from 00:00 for 1 week(s)	<div>Edit</div> <div>Delete</div>	GoldVideo	Occurs every Sunday,Saturday effective 02/01/2005 until 06/01/2005 from 00:01 for 23 hour(s)	<div>Edit</div> <div>Delete</div>	<div>Create</div>		
Schedule Name	Definition																				
Promotional	Occurs on 02/07/2005 from 00:00 for 1 week(s)	<div>Edit</div> <div>Delete</div>																			
GoldVideo	Occurs every Sunday,Saturday effective 02/01/2005 until 06/01/2005 from 00:01 for 23 hour(s)	<div>Edit</div> <div>Delete</div>																			
<div>Create</div>																					

2. In the Schedules page, click **Create**.

The Schedule Definition Page appears.

3. Enter field values to define a schedule, and click **Save**.

See “Schedule Fields in Enterprise Manager Portal” on page 224.

A description of the schedule appears in the Schedules page.



NOTE: The system generates the description of the service. If you want a page to display a different description, you can edit the JSP page and change and compile the Java classes found in the WAR file. If you need assistance to make these changes, contact Juniper Professional Services.

Schedule Fields in Enterprise Manager Portal

Use the fields in this topic to define a service schedule.

Schedule Name

- Name of the schedule.
- Value—Text string
- Default—No value

Subscription is

- Whether or not the subscription can be activated during or outside the scheduled time.
- Value
 - Enabled during schedule—Service can be activated during the scheduled time.
 - Enabled outside schedule—Service can be activated outside the scheduled time.
- Default—No value

Start Time

- Time that a scheduled activity is to start.
- Value—Time of day in the format hh:mm, where hh indicates the hour and mm indicates the minute. The range is 00:00 to 23:59.
- Default—No value
- Example—13:15

Time Zone

- Time zone for which the schedule is defined.
- Value—Name of time zone
- Default—Local time zone

Duration

- Length of time after the start time that a scheduled activity is allowed.
- Value—Length of time in minutes, hours, days, or weeks
- Guidelines—The length of time should be more than 15 minutes; using a shorter time could adversely affect system performance. Table 24 on page 225 shows the maximum duration for specified recurrence patterns.

Table 24: Maximum Duration for Recurrence Patterns

For This Recurrence Pattern	Duration Must Be Less Than
Daily	24 hours
Weekly	24 hours
Monthly	28th day of the month
Yearly	365 days

- Default—No value
- Example—2 hours

During the interval from the start time to 2 hours after the start time, the action (defined on the Schedule Definition Page under the *During schedule subscription* is field) is available.

Once

- Date on which the scheduled activity is to occur.
- Value—Date in the format mm/dd/yyyy, where mm indicates the month, dd indicates the day, and yyyy indicates the year
- Default—No value
- Example—12/10/2005

Daily

- Whether or not the scheduled activity is to occur every day of the week or every weekday.
- Value
 - day—Scheduled activity is to occur on every day of the week
 - weekday—Scheduled activity is to occur on each day Monday through Friday
- Default—No value

Weekly

- Scheduled activity occurs on a specified day or days during a week.
- Value—Name of day(s) of the week
- Default—No value

Monthly

- Scheduled activity occurs on the indicated day every month
- Value—Day of the month
- Default—No value

Yearly

- Scheduled activity occurs on a specified day each year
- Value—Month and day
- Default—No value

Range of recurrence Start by

- Date on which a schedule starts for a recurring action.
- Value—Date in the format mm/dd/yyyy, where mm indicates the month, dd indicates the day, and yyyy indicates the year
- Default—No value

The default indicates that the recurring schedule starts immediately—the next time the recurrence pattern applies.

- Example—12/10/2005

Range of recurrence End by

- Date on which a schedule ends for a recurring action.
- Value—Date in the format mm/dd/yyyy, where mm indicates the month, dd indicates the day, and yyyy indicates the year
- Default—No value

The default indicates that the schedule has no end date and remains in place indefinitely.

- Example—12/10/2005

Applying a Schedule to a Service in Enterprise Manager Portal

Before you can schedule a subscription, you must define a schedule..

To apply a schedule to a service that was configured earlier:

1. In the navigation pane of Enterprise Manager Portal, click the subscriber for which you want to schedule a service.
2. Click the tab for the type of service to be scheduled:
 - Bandwidth or Bandwidth & VPNs
 - Firewall



NOTE: If VPN features are not configured, the tab is named Bandwidth.

3. On the same line as the service to be assigned to a schedule, select the name of a schedule under Schedule, and click **Apply**.

The service provider controls which services can be scheduled. Text on the page indicates which services cannot be scheduled.

default ▶ local ▶ Acme ▶ Boca ▶ **Primary** ▶

Bandwidth & VPNs Applications Firewall Addresses NAT Schedules Managers

Bandwidth Level ?

1.0 Mbps ▼ Apply

Inherited from site "Boca"

Status... Usage data...

Name	Affected Traffic	BoD Service ?	Destination VPN ?	Schedule ?	Enabled	
Rule1	Source IPs: 192.0.2.1/22 Destination IPs: 192.0.2.22/22 Edit	Gold ▼	None ▼	GoldVideo ▼	<input type="checkbox"/>	Delete
				Apply		Status... Usage data...
Rule2	Source IPs: 10.10.10.168/24 Destination IPs: 10.10.10.100/24 Edit	Silver ▼	None ▼	No schedule ▼	<input type="checkbox"/>	Delete
				Apply		Status... Usage data...
Create Subscription						

Disabling a Schedule for a Service in Enterprise Manager Portal

When you disable a schedule for a subscription, the service remains in the same state as when the schedule was disabled. For example, if the service is inactive at the time the schedule is removed, the service remains inactive. This state can be different from the one indicated by the Enabled check box. After disabling a schedule for a service, ensure that the status of the service is the same as indicated by the Enabled check box.

To disable a schedule for a service:

1. In the navigation pane of Enterprise Manager Portal, click the subscriber for whom you want to remove a schedule that is assigned to a service, and then click the **Bandwidth & VPNs** (or **Bandwidth**) or **Firewall** tab.
2. On the line for the service select **No Schedule**, and then in the last column click the **Status** link.
3. On the Subscription Status page, check the status of the sessions listed. If a session status is different from what it should be—for example if it is inactive instead of active—click **Fix Problems** to activate or deactivate the session.

See “Monitoring the Status of Subscriptions” on page 280 .

Changing Schedules in Enterprise Manager Portal

You can change a schedule at any time. Before you delete a service schedule, however, you must make sure that the schedule is not being used by any service.

To modify a schedule:

1. Click the **Schedules** tab; then on the line that describes the schedule that you want to change, click **Edit**.
2. On the Schedule Edit page, change values. , and click **Apply**.

To delete a schedule:

1. Before you delete a schedule, make sure that none of the services reference this schedule:
 - Go to the Bandwidth (or Bandwidth & VPNs) page and review the names of schedules listed under Schedule. If the name of the service to be changed is listed, change the schedule to another one or to Any.
 - Go to the Firewall page and review the names of schedules listed under Schedule. If the name of the service to be changed is listed, change the schedule to another one or to Any.
2. Click the **Schedules** tab; then on the line that describes the schedule that you want to delete, click **Delete**.

The Schedules page no longer lists the schedule.

Managing Subscriptions to Bandwidth-on-Demand Services

You can configure and manage bandwidth-on-demand services in Enterprise Manager Portal. Topics include:

- Overview of Bandwidth-on-Demand Services on page 229
- Planning Subscriptions to BoD Services on page 229
- Creating a Subscription to BoD Services on page 230
- Modifying Rules for a Subscription to a BoD Service on page 242

- Modifying the Bandwidth Level on page 242
- Moving the Bandwidth Level on page 242
- Deleting a Subscription for a BoD Service on page 242
- Deleting the Bandwidth Level on page 243
- Monitoring Use of Subscriptions to BoD Services on page 243

Overview of Bandwidth-on-Demand Services

The service provider makes bandwidth services available to enterprises. IT managers can use these services to provision bandwidth within an enterprise to meet the forwarding requirements for subscriber traffic. The service provider can make the following types of bandwidth services available:

- Bandwidth-level allocation for an Internet access link

Only one subscription to one bandwidth level is supported for an access link.
- BoD services that classify traffic and assign different classes of traffic to different BoD services

You can classify traffic by source IP address, destination IP address, source Transmission Control Protocol (TCP) or User Datagram Protocol (UDP) port, destination TCP or UDP port, or type-of-service (ToS) byte, and assign that traffic to a service level.



NOTE: Enterprise Manager Portal supports only services that have policies configured.

When both of these services are available, you can provide subscribers with class of service (CoS)—the method of classifying traffic on a packet-by-packet basis with information in the ToS byte to provide different service levels to different traffic.

Whether bandwidth level (a basic BoD service), BoD services, or both are available depends on the configuration for the portal.

Planning Subscriptions to BoD Services

When planning subscriptions, consider the following factors:

- In a configuration that includes both a subscription to a bandwidth level and subscriptions to BoD services, the bandwidth level must be set before BoD services can be configured.

If a subscription to a bandwidth level needs to be deleted or moved, all subscriptions to BoD services for subscribers in the same container must be disabled or deleted first.
- BoD services are inherited by subscribers who are subordinate in the navigation pane.

- A rule for a BoD service specifies which fields in the IP header to match—protocol, source IP address, destination IP address, source TCP or UDP port, destination TCP or UDP port, or ToS byte—and the BoD service to assign to packets that match the conditions. If configured, a destination VPN can also be assigned.

If a packet matches more than one rule for BoD services, which rule is applied is unpredictable. For example, if the destination IP address matches a rule for a Gold BoD service, but the destination port matches the source TCP port for a Silver BoD service, and the rules have no other conditions, which rule is applied is uncertain.

Plan rules for BoD services so that a packet matches all the following conditions—protocol, source IP address, destination IP address, source TCP or UDP port, destination TCP or UDP port, or ToS byte—for only one BoD service.

Creating a Subscription to BoD Services

When you create a subscription to a BoD service, you initially set a bandwidth level if available and not previously set. Tasks to create a subscription are:

1. Setting a Bandwidth Level on page 230
2. Adding Subscriptions to BoD Services on page 231

Setting a Bandwidth Level

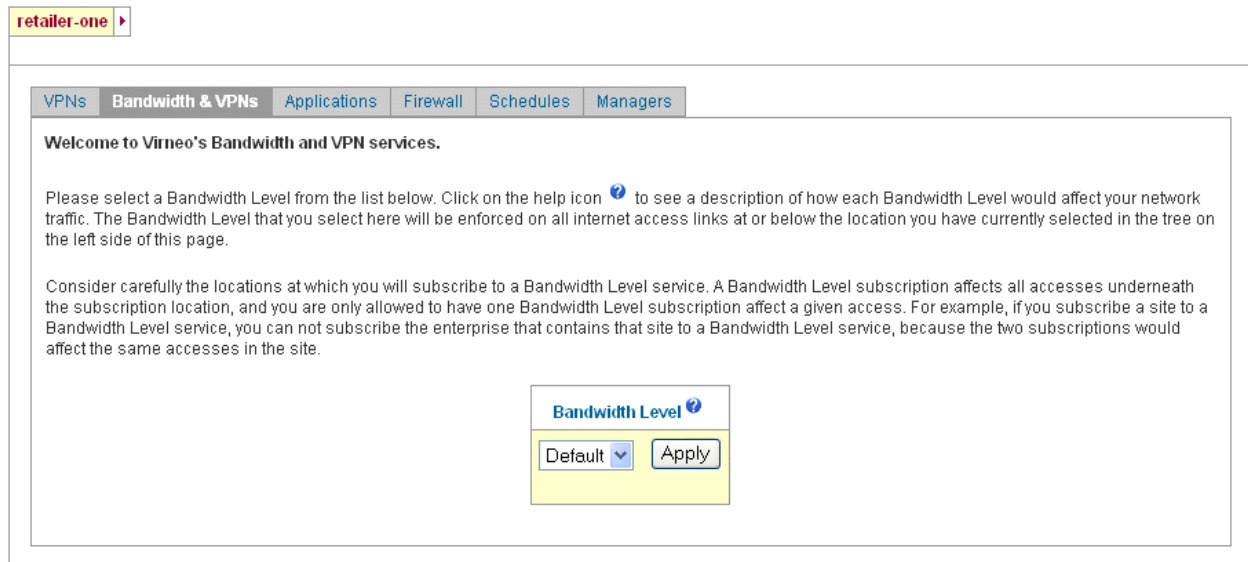
To create a subscription to a bandwidth level:

1. In the navigation pane of Enterprise Manager Portal, click the subscriber for whom you want to provision bandwidth.
2. Click the **Bandwidth & VPNs** tab.



NOTE: If VPN features are not configured, the tab is named Bandwidth.

The Bandwidth & VPNs page appears.

Figure 18: Bandwidth & VPNs Page

- Using the field description below, select a bandwidth level, and click **Apply**.

The bandwidth level becomes available, and the fields for setting BoD services appear on the Bandwidth page.

Bandwidth Level Fields in Enterprise Manager Portal

Use the field in this topic to define the bandwidth level.

Bandwidth Level

- Bandwidth assigned to an access link (the basic BoD service in the directory). The bandwidth level governs the overall bandwidth available on the link.
- Value—Menu of bandwidth levels in the directory available for this subscriber. See the online help for information about the menu entries.
- Guidelines—A subscriber can be assigned to up to one bandwidth level on an access link.

In the navigation pane, a subscriber subordinate to the one who has the bandwidth level subscription inherits the subscription. A subordinate subscriber cannot subscribe to another bandwidth level.

If you select default for the value, all traffic is treated the same.

- Default—Bandwidth level specified as the default by the service provider.

Adding Subscriptions to BoD Services

To add a subscription to a BoD service:

1. In the navigation pane of Enterprise Manager Portal, click the subscriber to assign to a BoD service.
2. Click the **Bandwidth & VPNs** tab.
3. If a bandwidth level has not been set, specify a bandwidth level.

The bandwidth level becomes available, and the fields for setting BoD services appear on the Bandwidth & VPNs page.

Figure 19: Bandwidth & VPNs Page with a Bandwidth Level Set

default ▶ local ▶ Acme ▶ Boca ▶ **Primary** ▶

Bandwidth & VPNs
Applications
Firewall
Addresses
NAT
Schedules
Managers

Bandwidth Level ?

1.0 Mbps ▼ Apply

Inherited from enterprise "Acme"

Status...

Usage data...

Name	Affected Traffic	BoD Service ?	Destination VPN ?	Schedule ?	Enabled	
Rule1	IP Protocol tcp Source Address 192.0.2.0/24 Destination Address 192.0.2.0/24	Gold ▼	None ▼	No schedule ▼	<input type="checkbox"/>	Delete Status... Usage data...
<div>Create Bandwidth Rule</div>						

4. Click **Create Bandwidth Rule**.

The Create Rule dialog box appears.

Create Rule	
Rule Name	<input type="text"/>
IP Protocols	<input type="text"/>
ToS Byte	<input type="radio"/> DiffServ <input type="text"/> <input type="radio"/> Precedence <input type="text"/> <input type="radio"/> Free Format (e.g. 110101xx) <input type="text"/>
Source IP Addresses	<input type="text"/>
Source Ports	<input type="text"/>
Destination IP Addresses	<input type="text"/>
Destination Ports	<input type="text"/>
TCP Flags	<input type="text"/>
Fragmentation Flags	<input type="text"/>
Fragment Offset	<input type="text"/>
Packet Length	<input type="text"/>
ICMP Type	<input type="text"/>
ICMP Code	<input type="text"/>
BoD Service	Gold <input type="button" value="v"/>
Destination VPN	None <input type="button" value="v"/>
Enabled	<input type="checkbox"/>
<input type="button" value="Create"/> <input type="button" value="Cancel"/> <input type="button" value="Reset"/>	

- Using field values to configure subscriptions for BoD services.

See “BoD Service Fields in Enterprise Manager Portal” on page 234

You can configure any number of subscriptions by assigning different traffic flows, identified by rules under Affected Traffic on the Bandwidth & VPNs page, to different BoD services.

6. Click Create.

The subscription appears in the Bandwidth & VPNs page.

BoD Service Fields in Enterprise Manager Portal

Use the fields in this topic to configure subscriptions for BoD services.

Rule Name

- Name of the BoD rule.
- Value—Alphanumeric characters without spaces
- Default—No value
- Example—SalesVideoConference

IP Protocols

- IP protocol associated with traffic affected by this bandwidth rule.
- Value—One of the following:
 - ah—authentication header
 - egp—exterior gateway protocol
 - esp—Encapsulating Security Payload
 - gre—generic routing encapsulation
 - icmp—Internet Control Message Protocol
 - igmp—Internet Group Management Protocol
 - ipip—IP over IP
 - ospf—Open Shortest Path First
 - pim—Protocol Independent Multicast
 - rsvp—Resource Reservation Protocol
 - sctp—Stream Control Transmission Protocol
 - tcp—Transmission Control Protocol

- udp—User Datagram Protocol
- < ipProtocolNumber >
- Guidelines—Specify an IP protocol or its corresponding number if you want to enable BoD for a certain type of traffic. If you want to enable BoD for all IP protocols, leave this field empty. If you specify an IP protocol other than TCP or UDP, the port fields will dim, and you will not be able to specify port numbers for this subscription.
- Default—No value
- Example—tcp

ToS Byte

- ToS byte in the header of the IP datagram associated with traffic affected by this bandwidth rule.
- Value
 - DiffServ—DiffServ is used to classify packets by the selected value.
 - Precedence—Value of the drop precedence.
 - Free Format—ToS byte in binary format.

Use an x to indicate a bit to be ignored.

- Guidelines—You can configure the ToS byte only if the configuration level is set to Advanced (see “Setting the Configuration Level for Enterprise Manager Portal” on page 220).

Specify the ToS byte in this field if you want to enable BoD for a specific type of service. If you want to enable BoD for all types of service, leave this field empty.

- Default—No value
- Example—Free Format 000010xx

Source IP Addresses

- Source IP address(es) (contained in the IP packets) of traffic affected by this bandwidth rule.
- Value—[not] < networkAddress > / < networkMask >
 - not—Address, or set of IP addresses as expressed by the netmask, for which the BoD service is not available
 - < networkAddress > —IP address of the network

- `< networkMask >` —Netmask expressed as an integer 0–32, which specifies how many of the first bits in the address specify the network
- Guidelines—To specify traffic not from a source IP address or not from a set of IP addresses as expressed by the netmask, precede the IP address with the keyword **not**. To specify traffic with any source IP address, leave the field empty.

The order in which you list prefixes, identified by the IP address–netmask pair, is not significant. They are all evaluated to determine whether a match occurs. If prefixes overlap, longest-match rules are used to determine whether a match occurs. For an address to be considered a match, it must match one of the rules in the list.

For information about how JUNOS routing platforms evaluate prefixes, see the *JUNOS Policy Framework Configuration Guide*.

- Default—No value
- Example—In this example for a JUNOS routing platform, all IP addresses on the subnet 172.16.0.0/10 are specified, except for those on the subnet 172.16.2.0/16.

172.16.0.0/10, not 172.16.2.0/16

Source Ports

- Source TCP/UDP port(s) (contained in the IP packets) of traffic affected by this bandwidth rule.
- Values
 - Port number
 - Comma-separated list of port numbers and ranges of port numbers (JUNOS routing platforms)
 - Ranges of port numbers separated by two dots (..)
- Guidelines— To specify all ports, leave this field empty. If you specify an IP protocol other than TCP or UDP for this subscription, the port field will dim, and you will not be able to specify port numbers in this field.
- Default—No value
- Example
 - 2
 - 2, 3, 45..55

Destination IP Addresses

- Destination IP addresse(s) (contained in the IP packets) of traffic affected by this bandwidth rule.
- Value—[not] `< networkAddress > / < networkMask >`

- not—Address, or set of IP addresses as expressed by the netmask, for which the BoD service is not available
- < networkAddress > —IP address of the network
- < networkMask > —Netmask expressed as an integer 0–32, which specifies how many of the first bits in the address specify the network
- Guidelines—To specify traffic not to a destination IP address or not to a set of IP addresses as expressed by the netmask, precede the IP address with the keyword **not**.

The order in which you list prefixes, identified by the IP address–netmask pair, is not significant. They are all evaluated to determine whether a match occurs. If prefixes overlap, longest-match rules are used to determine whether a match occurs. For an address to be considered a match, it must match one of the rules in the list.

For information about how JUNOS routing platforms evaluate prefixes, see the *JUNOS Policy Framework Configuration Guide*.

- Default—No value
- Example—192.0.2.0/24

Destination Ports

- Destination TCP/UDP port(s) (contained in the IP packets) of traffic affected by this bandwidth rule.
- Value
 - Port number
 - Comma-separated list of port numbers and ranges of port numbers (JUNOS routing platforms)
 - Ranges of port numbers separated by two dots (..)
- Guidelines—To specify all ports, leave this field empty. If you specify an IP protocol other than TCP or UDP for this subscription, the port field will dim, and you will not be able to specify port numbers in this field.
- Default—No value
- Example
 - 2
 - 2, 3, 45..55

TCP Flags

- Conditions in the TCP flags in the TCP message header. This field is enabled when the TCP protocol is selected.
- Value—Expression or text synonym that identifies the TCP flags
- Guidelines—You can enter a value for TCP flags only if you select TCP as the IP protocol.

You can enter a logical expression that contains the symbols for the six TCP flags: urgent, ack, push, rst, syn, and fin. You can use the following logical operators in the list of flags:

- &—And. Separates flag settings in the list.
- !—Not. Flags preceded by ! are cleared; flags not preceded by ! are set.

You can use the following expression instead of the entire expression:

- tcp-initial—syn & !ack

The interface displays text synonyms for expressions if stored data matches the expression.

This field appears enabled only if the configuration level is set to Advanced. Although the value can be changed when the configuration level is set to Normal, we recommend that the value of this field not be changed if the field appears disabled.

- Default—No value
- Example
 - syn
 - tcp-initial

Fragmentation Flags

- Logical expression using the dont-fragment, more-fragments, and reserved IP fragmentation flags.
- Value—Flags expression
- Guidelines—The expression can also contain the following logical operators:
 - &—And. Separates flag settings in the list.
 - !—Not. Flags preceded by ! are cleared; flags not preceded by ! are set.
- Default—No value
- Example
 - more-fragments

- ! dont-fragment

Fragment Offset

- IP fragment offset—a value that defines the order in which to assemble fragments for an IP datagram.
- Value—One of the following:
 - Number in the range 0–8191
 - Range of numbers separated by two dots (..) within the range 0–8191
- Default—No value
- Example
 - 50
 - 50 .. 76

Packet Length

- Length of packets.
- Value—One of the following:
 - Number in the range 0–65536
 - Range of numbers separated by two dots (..) within the range 0–65536
- Default—No value
- Example
 - 15000
 - 15000 .. 30000

ICMP Type

- Type of message for Internet Control Management Protocol (ICMP).
- Value—Type of ICMP message in the following formats:
 - Number of the ICMP message type in the range 0–255
 - Symbolic name for an ICMP message type
 - Comma-separated list of ICMP types and ranges of ICMP types

- Ranges of ICMP types separated by two dots (..) within the range 0–255
- Blank—Any ICMP type
- Guidelines—You can enter a value for this field only if you select the icmp protocol (protocol number 1).

The following list shows the symbolic name and associated numbers for ICMP types. The ICMP types are the same as those on JUNOS routing platforms with the addition of traceroute.

- 0—echo-reply
- 8—echo-request
- 16—info-reply
- 15—info-request
- 18—mask-reply
- 17—mask-request
- 12—parameter-problem
- 5—redirect
- 9—router-advertisement
- 10—router-solicit
- 4—source-quench
- 11—time-exceeded
- 13—timestamp
- 14—timestamp-reply
- 30—traceroute
- 3—unreachable

This field appears enabled only if the configuration level is set to Advanced. Although the value can be changed when the configuration level is set to Normal, we recommend that the value of this field not be changed if the field appears disabled.

- Default—Any
- Example—10 .. 25, 27

ICMP Code

- Code for ICMP.
- Value—Type of ICMP code in the following formats:
 - Number of ICMP code in the range 0–255
 - Comma-separated list of code numbers and ranges of code numbers

- Ranges of code numbers separated by two dots (..) within the range 0–255
- Blank—Any ICMP code
- Guidelines—You can enter a value for this field only if you select particular protocols.

This field appears enabled only if the configuration level is set to Advanced. Although the value can be changed when the configuration level is set to Normal, we recommend that the value of this field not be changed if the field appears disabled.

- Default—Any
- Example—75

BoD Service

- Name of the BoD service in the directory that will be applied to the subscription.
- Value—Menu of BoD services available for this subscriber. See the online help for information about the menu entries.
- Guidelines—How BoD services define bandwidth allocation depends on whether or not a bandwidth level is set:
 - On a link that has a bandwidth level set, the BoD service defines the transmission service and the forwarding priority of the traffic for the subscription—for example, expedited or best-effort.
 - On a link that does not have bandwidth allocated, the BoD service typically specifies the fixed bandwidth level available to the traffic type for the subscription.
- Default—BoD service with lowest alphanumeric name in the directory
- Example—Gold

Destination VPN

- Configured VPN to use.
- Value—Name of VPN
- Guidelines—This field appears if configuration for VPNs is enabled for the portal. For more information about VPNs, see “Modifying Subscriber VPN Configuration” on page 244.
- Default—No value

Enabled

- Status of the subscription.
- Value

- Gray box—Subscription is inherited from a parent subscriber
- White box—Subscription is configured for this subscriber
- Box with check mark—Subscription is enabled
- Empty box—Subscription is disabled
- Guidelines—Click box to enable or disable a subscription.
- Default—Subscription is disabled

Modifying Rules for a Subscription to a BoD Service

To modify rules for a subscription to a BoD service:

1. Start at the subscriber's Bandwidth page.
2. Change the values in the fields for this rule.
3. Click **Apply** for the subscription.

Modifying the Bandwidth Level

To modify a bandwidth level:

1. Start at the subscriber's Bandwidth page.
2. Disable all BoD services that this subscriber inherits from parent subscribers.
3. Disable all BoD services defined for this subscriber's subordinate subscribers.
4. Select a new value from the Bandwidth Level menu.
5. Click **Apply**.
6. If needed, enable BoD services that this subscriber inherits from parent subscribers.
7. If needed, enable BoD services defined for this subscriber's subordinate subscribers.

Moving the Bandwidth Level

To move the bandwidth level to another subscriber:

1. Delete the bandwidth level. See "Deleting the Bandwidth Level" on page 243.
2. Set a bandwidth level for another subscriber. See "Creating a Subscription to BoD Services" on page 230.
3. Create BoD services. See "Creating a Subscription to BoD Services" on page 230.

Deleting a Subscription for a BoD Service

To delete a subscription to a BoD service:

1. Start at the subscriber's Bandwidth page.
2. Click **Delete** for the subscription.

Deleting the Bandwidth Level

To delete the bandwidth level:

1. Start at the subscriber's Bandwidth page.
2. Disable all BoD services that this subscriber inherits from parent subscribers.
3. Disable all BoD services defined for this subscriber's subordinate subscribers.
4. Select **Default** from the Bandwidth Level menu.
5. Click **Apply**.

Monitoring Use of Subscriptions to BoD Services

Purpose Monitor the use of a bandwidth subscription.

- Action**
1. Start at the subscriber's Bandwidth page.
 2. Click **Usage Data** for the bandwidth level or subscription.

The Service Usage page appears.



Service Usage

Service Usage Data

This data is for the subscription **Rule1** to service **Gold**.

Access Link	Usage Data					
	For Period From	For Period To	Incoming Bytes	Outgoing Bytes	Incoming Packets	Outgoing Packets
primary.boca.acme.local/default	Unknown	Unknown	Unknown	Unknown	Unknown	Unknown
Refresh						

The table above shows usage data for the service. The usage data covers the period starting when the service was most recently activated on the access link, and ending when the usage data was most recently collected from the network infrastructure. Usage data is collected periodically (e.g. once an hour). No usage data is available for subscriptions that are not active on the access link.

Usage data may be shown as "Unknown". Usage data may be unknown because no data has yet been collected for the access link, or because the access link is currently down, or because the usage data collection mechanism is temporarily unavailable.

Integrating VPNs into an SRC Network Through Enterprise Manager Portal

You can integrate VPNs into your SRC network through the Enterprise manager portal. Topics include:

- Overview of VPNs in an SRC Network on page 244
- Modifying Subscriber VPN Configuration on page 244
- Creating Extranets Through Enterprise Manager Portal on page 246
- Deleting Extranets Through Enterprise Manager Portal on page 247
- Sending Traffic to a VPN on page 247
- Modifying the VPN to Which the Router Sends Traffic on page 247
- Stopping the Router from Sending Traffic to VPNs on page 248

Overview of VPNs in an SRC Network

The service provider creates VPNs in the directory for specific subscribers. If the service provider configures the portal to display VPN features, IT managers with privileges to configure VPNs can make modifications to VPNs that a subscriber owns.

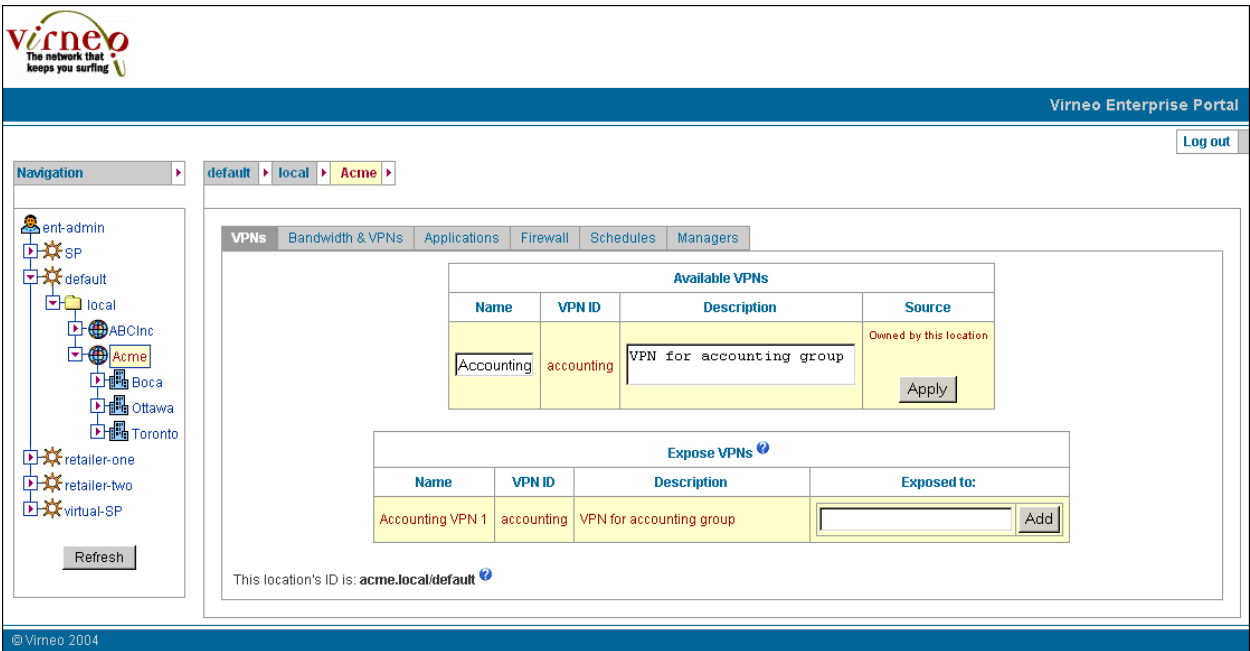
Modifying Subscriber VPN Configuration

To modify a VPN:

1. In the navigation pane of Enterprise Manager Portal, click the subscriber who owns the VPN that you want to modify.
2. Click the **VPNs** tab.

The VPNs page appears and displays the Available VPNs area. If the service provider configures the portal to display extranet features, this page also displays the Expose VPNs area.

Figure 20: VPNs Page



3. Using the field descriptions below, modify the VPN.
4. Click **Apply**.

VPN Fields in Enterprise Manager Portal

Use the fields in this topic to modify a VPN configuration through Enterprise manager Portal.

Name

- Name of the VPN that appears in other pages of Enterprise Manager Portal.
- Value—Text string
- Guidelines—Enter a name that summarizes the application of this VPN.
- Default—Value of the VPN ID field
- Example—Accounting VPN

VPN ID

- Unique identifier for the VPN.
- Value—Text string
- Guidelines—You cannot modify this value.
- Default—Specified by the service provider
- Example—Accounting

Description

- Description of the VPN.
- Value—Text string
- Default—Specified by the service provider
- Example—VPN for accounting in Boca

Source

- Whether or not the subscriber owns, imports, or inherits the VPN.
- Value—Text string
- Guidelines—You cannot modify this value.
- Default—Determined by the configuration of this VPN
- Example—Owned by this location

Creating Extranets Through Enterprise Manager Portal

If the service provider configures the portal to display extranet features, IT managers with privileges to configure VPNs in their scope of control can create extranets for other enterprises and retailers by exporting those VPNs. Enterprises and retailers who share VPNs that other subscribers own are called *extranet clients*.

To create an extranet:

1. Obtain a location identifier from the extranet client.

When you click an enterprise or retailer in the navigation pane of Enterprise Manager Portal, the location identifier for that subscriber appears at the bottom of the VPNs page). The default format of the location identifier is:

[< enterpriseName > . < subscriberFolderName > /] < retailerName >

- enterpriseName—Name of the enterprise in the directory
- subscriberFolderName—Name of the subscriber folder that contains the directory

- retailerName—Name of the retailer in the directory
- 2. Start at the VPN page for the subscriber who owns the VPN.
- 3. In the field called Exposed to in the Expose VPNs area, enter the location identifier for the extranet client.
- 4. Click **Add**.

The VPN page for the subscriber who owns the VPN displays the updated status of the VPN, and the extranet client now has access to the VPN.

Deleting Extranets Through Enterprise Manager Portal

You can delete an extranet by canceling the export of a VPN. To do so:

1. Start at the VPN page for the subscriber who owns the VPN.
2. In the Expose VPNs area, identify the VPN and the extranet client for whom you want to delete the extranet.
3. Click **Delete** for the extranet client in the field Exposed to.

This action will deactivate all subscriptions to this VPN for the extranet client, and the extranet client will not be able to reactivate subscriptions to the VPN.

Sending Traffic to a VPN

If the service provider makes VPN features visible to subscribers, the name of the Bandwidth tab in the portal changes to Bandwidths & VPNs, and you can send traffic associated with BoD services to VPNs. To do so:

1. In the navigation pane of Enterprise Manager Portal, click the subscriber for whom you want to send traffic to a VPN.
2. Click the **Bandwidth and VPNs** tab.
3. Configure a BoD service.
4. From the menu in the Destination VPN field for that subscription, select the VPN to which you want to send the traffic.
5. Click **Create** for the subscription.

Modifying the VPN to Which the Router Sends Traffic

To modify the VPN to which the router sends traffic:

1. Start at the subscriber's Bandwidth & VPN page.
2. From the menu in the Destination VPN field for the subscription, select a different VPN from the menu.
3. Click **Apply** for the subscription.

Stopping the Router from Sending Traffic to VPNs

To stop a router from sending traffic to a VPN:

1. Start at the subscriber's Bandwidth & VPNs page.
2. From the menu in the Destination VPN field for the subscription, select **None**.
3. Click **Apply** for the subscription.

Classifying Traffic for Stateful Firewall Exceptions and NAT Rules

You can classify traffic affected by a firewall exception to a stateful firewall or by a NAT rule. Topics include:

- Overview of Traffic Classification for Firewall Exceptions and NAT Rules on page 248
- Classifying Traffic on page 249
- Modifying Values for Traffic Classifications on page 253
- Deleting Traffic Classifications on page 254

Overview of Traffic Classification for Firewall Exceptions and NAT Rules

You can create for a subscriber a list of application objects that can be used to classify the traffic affected by a firewall exception to a stateful firewall or by a NAT rule. These application objects are based on application protocols—protocols that are categorized in the application layer of the TCP/IP reference model—or IP protocols that the JUNOS routing platform supports. Subordinate subscribers inherit application objects configured for parent subscribers.

An application protocol defines how a client and a server communicate during a *conversation*—a particular activity between the client and the server, such as an FTP session. A conversation in the application layer consists of multiple *flows*. A flow is one element of the conversation; for example, in an FTP session, the initial TCP control connection or a subsequent UDP traffic connection. You can apply a NAT rule or a firewall exception to the initial flow in a conversation by defining an application object. The NAT rule or firewall exception then applies to all subsequent flows in that conversation.

In the FTP example, the client may create a TCP connection to the server and send the server a UDP port number in the initial flow. The server may then start sending UDP traffic to the UDP port specified in the initial flow. If the initial flow matches a defined application object that a firewall allows, the firewall will allow the UDP traffic in the second flow and in all subsequent flows in the conversation.

Certain application protocols, such as FTP, are supported explicitly, and you can select them for your application object. These application protocols usually have an associated IP protocol that the portal selects automatically. If you want to create an application object for an application protocol that is not explicitly supported, such as HTTP, you can create an application object based on an IP protocol only. For example, you could create an application object called HTTP, specify no application

protocol, and select TCP as the IP protocol. You can then specify 8080 for the source and destination ports in the application protocol to identify the HTTP traffic.

Classifying Traffic

To create an application protocol:

1. In the navigation pane of Enterprise Manager Portal, click the subscriber to whom you want to assign the application object.
2. Click the **Applications** tab.

The Applications page appears. This page displays the application protocols that the subscriber inherits from parent subscribers and application protocols configured explicitly for the subscriber.

Figure 21: Applications Page

default ▶ local ▶ Acme ▶ Boca ▶ Primary ▶

Bandwidth & VPNsApplicationsFirewallAddressesNATSchedulesManagers

Name	Application Protocol	IP Protocol	Details	
bootp_boca_primary	bootp	udp	Inactivity timeout: 25 Destination port: 8067	<div>EditDelete</div>
ftp_boca_primary	ftp	tcp	Inactivity timeout: 30 Destination port: 8098	<div>EditDelete</div>
<div>Create Application</div>				

3. Click **Create Application**.

The Create Application page appears.

Create Application

Application Name: (Must be unique.)

Application Protocol:

IP Protocol:

Source Port:

Destination Port:

SNMP Command:

ICMP Type:

ICMP Code:

TTL Threshold:

RPC Program Number:

UUID:

Inactivity Timeout:

4. Using the following field descriptions, specify details for the application protocol.

Some fields are available only for certain applications. When a field is unavailable, the box in which you enter information is dimmed, and you cannot enter information in it.

5. Click **Apply**.

Traffic Classification Fields in Enterprise Manager Portal

Use the fields in this topic to classify traffic for firewall exceptions and NAT rules.

Application Name

- Name for this application protocol.
- Value—Text string
- Default—No value
- Example—bootp-boston

Application Protocol

- Application protocol.
- Value—Type of application protocol or None
- Guidelines—Select a protocol from the menu to specify that the application uses a particular application protocol. Depending on the application protocol you choose, some fields in the application object are irrelevant (and disabled) or restricted to specific values. If the application protocol you want is not available, you can select the option **None** and base the application object on an IP protocol. If you select this option, the NAT rule or firewall exception affects only the first flow in a conversation. Consequently, you can deny or discard a conversation, but you cannot allow a complete conversation.
- Default—Any
- Example—bootp

IP Protocol

- IP protocol.
- Value—Type of IP protocol or number of IP protocol in the range 0–255
- Guidelines—The names of the allowed IP protocols are shown in the tool tips for this field. The portal automatically selects an IP protocol for certain application protocols.
- Default—No value
- Example—tcp

Source Port

- Source TCP/UDP ports (as contained in the IP packets) of traffic for this application object.
- Value—Integer in the range 0–65535
- Guidelines—Enter either a single port number or a range of port numbers separated by two dots (..). To specify all ports, leave this field empty.
- Default—No value
- Example—25..35

Destination Port

- Destination TCP/UDP ports (as contained in the IP packets) of traffic for this application object.
- Value—Integer in the range 0–65535
- Guidelines—Enter either a single port number or a range of port numbers separated by two dots (..). To specify all ports, leave this field empty.
- Default—No value
- Example—25..35

SNMP Command

- Type of command for Simple Network Management Protocol (SNMP).
- Value—Type of SNMP command
- Guidelines—Select a type of command from the menu.
- Default—Any
- Example—get-next

ICMP Type

- Type of message for Internet Control Management Protocol (ICMP).
- Value—Type of ICMP message
- Guidelines—Select a type of message from the menu.
- Default—Any
- Example—info-reply

ICMP Code

- Code for ICMP.
- Value—Type of ICMP code
- Guidelines—Select a type of code from the menu.
- Default—Any
- Example—host-precedence-violation

TTL Threshold

- Depth of network penetration for the traceroute application protocol.
- Value—Integer in the range 0–255 or unspecified

- Unspecified—Allows traceroutes up to a depth of 255.
- Default—Unspecified
- Example—5

RPC Program Number

- Program number for the remote procedure call (RPC) application protocol.
- Value—A single program number or range of program numbers separated by two dots (.). Program numbers are integers in the range 100000–400000.
- Guidelines—Specify the RPC program numbers to which the NAT rule or firewall exception applies. To specify all RPC program numbers, leave this field empty.
- Default—No value
- Example—7..12

UUID

- Universal unique identifier (UUID) for the Distributed Computing Environment (DCE) RPC application protocol.
- Value—Hexadecimal number in the format
xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx
- Guidelines—Specify a number of a specific DCE RPC object to which the NAT rule or firewall exception applies. To specify all DCE RPC objects, leave this field empty.
- Default—No value
- Example—1f356a25-ce67-73ad-2187-631ec8ae1bd6

Inactivity Timeout

- Time for which a conversation associated with the identified application protocol can be inactive before the JUNOS routing platform terminates the conversation.
- Value—Number of seconds in the range 0–2147483647
- Guidelines—Specify a time, or leave this field empty to use the default setting.
- Default—30 seconds
- Example—45

Modifying Values for Traffic Classifications

To modify values for an application object:

1. Start at the Applications page.
2. Click **Edit** for the application object.

The Edit Application page appears.

3. Change the values in the fields for this application object.
4. Click **Apply**.

Deleting Traffic Classifications

To delete an application protocol:

1. Start at the Applications page.
2. Click **Delete** for the application protocol.

Subscribing to Firewall Services Through Enterprise Manager Portal

You can configure subscriptions to firewall services through Enterprise manager Portal. Topics include:

- Overview of Firewall Services in Enterprise Manager Portal on page 254
- Before You Configure Firewall Exception Rules on page 255
- Creating Subscriptions to Firewall Services on page 255
- Creating Firewall Exceptions for Stateless Firewalls on page 256
- Creating Firewall Exceptions for Stateful Firewalls on page 267
- Adding a Schedule to a Firewall Exception on page 270
- Modifying Firewall Exceptions on page 271
- Deleting Firewall Exceptions on page 271
- Deleting Basic Firewalls on page 271
- Monitoring the Use of Subscriptions to Firewall Services on page 272

Overview of Firewall Services in Enterprise Manager Portal

The basic firewall that you configure will be enforced on all Internet access links subordinate to the subscriber you select in the navigation pane. When you have configured a basic firewall, you can create firewall exceptions—variances from the basic firewall—for specific categories of traffic.

Firewall exception rules block traffic that otherwise would be permitted to traverse the firewall, or to admit traffic that would otherwise be blocked. Exceptions specify criteria against which each packet is inspected.

How you configure firewall exceptions depends on which type of firewall service the ISP enabled. Enterprise Manager Portal can support one of the following:

- Stateless firewalls—Inspect each packet in isolation; they do not evaluate the traffic flow.

With stateless firewalls, you can configure exceptions to take customized actions, such as policing specified traffic at a specified rate, or setting the ToS byte. By using customized actions, you can allow traffic from a specified IP address or for a specified IP protocol to traverse the firewall. In addition, you can specify quality of service (QoS) properties such as values for the type of service (ToS) byte.

- Stateful firewalls—Track traffic flows and conversations between applications and evaluate this information when applying exception rules.

An application is typically associated with a stateful firewall rule. After a flow or conversation meets firewall criteria, packets in that flow can pass through the firewall. For example for an FTP connection, when an FTP control connection requests a file download, the stateful firewall knows to expect and allows a TCP data connection to start. You can also create firewall exceptions for traffic associated with a particular application protocol, such as FTP, that originates at a particular address in the enterprise.

Before You Configure Firewall Exception Rules

Before you configure firewall exception rules, make sure that you understand which types of packets you want to pass through a firewall.

Enterprise Manager Portal must be set to Advanced configuration mode to configure some of the properties for a firewall. If the portal is not in Advanced mode, some of the settings appear as read-only fields. For information about setting the portal mode, see “Setting the Configuration Level for Enterprise Manager Portal” on page 220.

Creating Subscriptions to Firewall Services

To create a subscription to a basic firewall service:


1. In the navigation pane of Enterprise Manager Portal, click the subscriber for whom you want to create a subscription to a basic firewall service.
2. Click the **Firewall** tab.

The Firewall page appears.

default > local > Acme > Boca > Primary >


Bandwidth & VPNs Applications **Firewall** Addresses NAT Schedules Managers


Welcome to Virneo's Firewall Services.

Please select one firewall from the list below. Click on the help icon  to see a description of how each firewall would affect your network traffic. The firewall that you select will be enforced on all internet access links at or below the location you have currently selected in the tree on the left side of this page.

Consider carefully the locations at which you will subscribe to a firewall service. A firewall affects all accesses underneath the subscription location, and you are only allowed to have one firewall affect a given access. For example, if you subscribe a site to a firewall service, you can not subscribe the enterprise that contains that site to a firewall service, because the two firewall subscriptions would affect the accesses in the site.

After selecting a firewall, you will be able to specify exceptions to the firewall's normal behaviour. For example, you could open a hole in the firewall for specific traffic at a specific site.

Firewall Service 

No firewall  Apply

3. Click the help icon above the firewall service to review information about the available firewalls.

See “Firewall Service Field in Enterprise Manager Portal” on page 256.

4. Select a firewall service from the menu, and click **Apply**.

The Firewall page changes to allow you to create firewall exceptions.

Firewall Service Field in Enterprise Manager Portal

Use the field in this topic to specify a firewall service in Enterprise manager Portal.

Firewall Service

- Name of the firewall service.
- Value—Menu of firewall services in the directory available for this subscriber
- Default—No Firewall
- Example—BasicFW1

Creating Firewall Exceptions for Stateless Firewalls

To create a firewall exception for a subscriber:

1. Access the subscriber's Firewall page.
2. In the Firewall page, click **Create Firewall Exception**.

The Create Exception dialog box appears. Figure 22 on page 257 shows the appearance of the dialog box when Enterprise Manager Portal is set to Advanced mode.

Figure 22: Create Exception Dialog Box for Stateless Firewalls

The screenshot shows a web browser window titled "Create Exception - Microsoft Internet Explorer". Inside the browser is a form titled "Create Exception". The form has the following fields and controls:

- Rule Name:** A text input field.
- IP Protocols:** A text input field.
- ToS Byte:** Three radio buttons: "DiffServ" (selected), "Precedence", and "Free Format (e.g. 110101xx)". There is a dropdown menu next to "DiffServ" and a text input field next to "Precedence".
- Source IP Addresses:** A list box with up/down arrows.
- Source Ports:** A text input field.
- Destination IP Addresses:** A list box with up/down arrows.
- Destination Ports:** A text input field.
- TCP Flags:** A text input field.
- Fragmentation Flags:** A text input field.
- Fragment Offset:** A text input field.
- Packet Length:** A text input field.
- ICMP Type:** A text input field.
- ICMP Code:** A text input field.
- Priority:** A text input field with the value "0".
- Direction:** A dropdown menu with "Incoming" selected.
- Action:** A dropdown menu with "Allow" selected.
- Enabled:** A checkbox.

At the bottom of the form are three buttons: "Create", "Cancel", and "Reset".

3. Enter field values to configure the values for the firewall exception.

See “Fields for Exceptions to Stateless Firewalls in Enterprise Manager Portal” on page 259.

Which protocols you select determines which associated protocol fields are available for editing.



NOTE: If a user changes the value for a protocol when the configuration level for the portal is set to Normal mode, values for the following fields may be deleted: TCP Flags, Fragmentation Flags, Fragmentation Offset, Packet Length, ICMP Type, and ICMP Code.

If the value of a protocol is changed to the original setting, the portal restores the associated field values that were previously removed.

4. Click **Create**.

The Firewall page shows the exception configured. Figure 23 on page 258 shows three exceptions configured for a brickwall firewall service. The exceptions appear in priority order.

Figure 23: Firewall Page with Firewall Service Applied and Exceptions Configured

Exceptions to Firewall Service							
Name	Affected Traffic	Priority	Direction	Firewall Action	Schedule	Enabled	
tcpProto1	IP Protocol: tcp ToS Byte: precedence: internet_control Source Address: 10.10.10.0/24 Destination Address: 10.11.12.0/24 Destination Port: 6789 TCP Flags: tcp-initial Fragmentation Flags: dont-fragment Fragment Offset: 100..170 Packet Length: 60..70	4	Incoming	Allow	No schedule	<input checked="" type="checkbox"/>	Delete Status... Usage data...
tcprule2	All Traffic	7	Incoming	Allow	No schedule	<input type="checkbox"/>	Delete Status... Usage data...
icmpRule	IP Protocol: icmp Source Address: 1.1.1.0/24 Destination Address: 2.2.2.0/24 Fragmentation Flags: reserved Fragment Offset: 5000 Packet Length: 65535 ICMP Type: info-reply ICMP Code: 50..100	10	Outgoing	Discard	No schedule	<input type="checkbox"/>	Delete Status... Usage data...
tcpProtocol	IP Protocol: tcp ToS Byte: precedence: immediate Source Address: 10.10.10.0/24 Source Port: 23456 Destination Address: 10.11.12.0/24 Destination Port: 6789 TCP Flags: fin & tsyn & rst & lpush & ack & urgent Fragmentation Flags: dont-fragment Fragment Offset: 100..170 Packet Length: 60..70	45	Incoming	Allow	No schedule	<input checked="" type="checkbox"/>	Delete Status... Usage data...

Create Firewall Exception

Fields for Exceptions to Stateless Firewalls in Enterprise Manager Portal

Use the fields in this topic to configure rules for exceptions to stateless firewalls.

Rule Name

- Name of the subscription to the firewall service.
- Value—Alphanumeric string
- Guidelines—You must specify a name for the rule. Do not use spaces, dots, or punctuation characters in the name.
- Default—No value
- Example—WebAccess

IP Protocols

- IP protocol associated with this rule.
- Value—Type of IP protocols separated by commas, with the protocol specified by:
 - Number of IP protocol in the range 0–255
 - The following abbreviations:
 - ah—authentication header
 - egp—exterior gateway protocol
 - esp—Encapsulating Security Payload
 - gre—generic routing encapsulation
 - icmp—Internet Control Message Protocol
 - igmp—Internet Group Management Protocol
 - ipip—IP over IP
 - ospf—Open Shortest Path First
 - pim—Protocol Independent Multicast
 - rsvp—Resource Reservation Protocol
 - sctp—Stream Control Transmission Protocol
 - tcp—Transmission Control Protocol

- udp—User Datagram Protocol
- Blank—Any IP protocol
- Default—No value
- Example—tcp

ToS Byte

- ToS byte in the header of the IP datagram associated with traffic affected by this rule.
- Value
 - DiffServ—DiffServ is used to classify packets by the selected value.
 - Precedence—Value for the drop precedence.
 - Free Format—ToS byte in binary format.

Use an x to indicate a bit to be ignored.

- Guidelines—You can configure the ToS byte only if the configuration level is set to Advanced.

Specify the ToS byte in this field if you want to specify a specific type of service. If you want to specify all types of service, leave this field empty.

- Default—No value
- Example—Free Format 000010xx

Source IP Addresses

- IP addresses (as contained in the IP packets) of traffic to which the rule applies.
- Value—[not] < networkAddress > / < networkMask >
 - not—All addresses except the listed addresses
 - < networkAddress > —IP address of the network
 - < networkMask > —Subnet mask
- Guidelines—To specify traffic with a particular source IP address, enter an IP address. To specify all traffic except that with a particular source IP address, precede the IP address with the keyword **not**. To specify traffic with any source IP address, leave the field empty. To specify multiple source IP addresses, enter multiple addresses on different lines. You can specify multiple source IP addresses only if the configuration level is set to Advanced.
- Default—No value
- Example—192.0.2.0/24

Source Ports

- Source TCP/UDP port(s) (contained in the IP packets) of traffic affected by this rule.
- Values
 - Port number
 - Comma-separated list of port numbers and ranges of port numbers (JUNOS routing platforms)
 - Ranges of port numbers separated by two dots (..)
- Guidelines— To specify all ports, leave this field empty. If you specify an IP protocol other than TCP or UDP for this subscription, the port field will dim, and you will not be able to specify port numbers in this field.
- Default—No value
- Example
 - 2
 - 2, 3, 45..55

Destination IP Addresses

- Destination IP addresse(es) (contained in the IP packets) of traffic affected by this rule.
- Value—[not] < networkAddress > / < networkMask >
 - not—Address, or set of IP addresses as expressed by the netmask, for which the firewall service is not available
 - < networkAddress > —IP address of the network
 - < networkMask > —Netmask expressed as an integer 0–32, which specifies how many of the first bits in the address specify the network
- Guidelines—To specify a netmask for a destination IP address or a set of IP addresses that should not be included, precede the IP address with the keyword **not**. The order in which you list prefixes, identified by the IP address–netmask pair, is not significant. They are all evaluated to determine whether a match occurs. If prefixes overlap, longest-match rules are used to determine whether a match occurs. For an address to be considered a match, it must match one of the rules in the list.

For information about how JUNOS routing platforms evaluate prefixes, see the *JUNOS Policy Framework Configuration Guide*.

- Default—No value
- Example—192.0.2.0/24

Destination Ports

- Destination TCP/UDP port(s) (contained in the IP packets) of traffic affected by this rule.
- Value
 - Port number
 - Comma-separated list of port numbers and ranges of port numbers (JUNOS routing platforms)
 - Ranges of port numbers separated by two dots (..)
- Guidelines—To specify all ports, leave this field empty. If you specify an IP protocol other than TCP or UDP for this subscription, the port field will dim, and you will not be able to specify port numbers in this field.
- Default—No value
- Example
 - 2
 - 2, 3, 45..55

TCP Flags

- Conditions in the TCP flags in the TCP message header. This field is enabled when the TCP protocol is selected.
- Value—Expression or text synonym that identifies the TCP flags
- Guidelines—You can enter a value for TCP flags only if you select TCP as the IP protocol.

You can enter a logical expression that contains the symbols for the six TCP flags: urgent, ack, push, rst, syn, and fin. You can use the following logical operators in the list of flags:

- &—And. Separates flag settings in the list.
- !—Not. Flags preceded by ! are cleared; flags not preceded by ! are set.

You can use the following expression instead of the entire expression:

- tcp-initial—syn & !ack

The interface displays text synonyms for expressions if stored data matches the expression.

This field appears enabled only if the configuration level is set to Advanced. Although the value can be changed when the configuration level is set to Normal,

we recommend that the value of this field not be changed if the field appears disabled.

- Default—No value
- Example
 - syn
 - tcp-initial

Fragmentation Flags

- Logical expression using the dont-fragment, more-fragments, and reserved IP fragmentation flags.
- Value—Flags expression
- Guidelines—The expression can also contain the following logical operators:
 - &—And. Separates flag settings in the list.
 - !—Not. Flags preceded by ! are cleared; flags not preceded by ! are set.
- Default—No value
- Example
 - more-fragments
 - ! dont-fragment

Fragment Offset

- IP fragment offset—a value that defines the order in which to assemble fragments for an IP datagram.
- Value—One of the following:
 - Number in the range 0–8191
 - Range of numbers separated by two dots (..) within the range 0–8191
- Default—No value
- Example
 - 50
 - 50 .. 76

Packet Length

- Length of packets.
- Value—One of the following:
 - Number in the range 0–65536

- Range of numbers separated by two dots (..) within the range 0–65536
- Default—No value
- Example
 - 15000
 - 15000 .. 30000

ICMP Type

- Type of message for Internet Control Management Protocol (ICMP).
- Value—Type of ICMP message in the following formats:
 - Number of the ICMP message type in the range 0–255
 - Symbolic name for an ICMP message type
 - Comma-separated list of ICMP types and ranges of ICMP types
 - Ranges of ICMP types separated by two dots (..) within the range 0–255
 - Blank—Any ICMP type
- Guidelines—You can enter a value for this field only if you select the icmp protocol (protocol number 1).

The following list shows the symbolic name and associated numbers for ICMP types. The ICMP types are the same as those on JUNOS routing platforms with the addition of traceroute.

- 0—echo-reply
- 8—echo-request
- 16—info-reply
- 15—info-request
- 18—mask-reply
- 17—mask-request
- 12—parameter-problem
- 5—redirect
- 9—router-advertisement
- 10—router-solicit
- 4—source-quench
- 11—time-exceeded
- 13—timestamp
- 14—timestamp-reply

- 30—traceroute
- 3—unreachable

This field appears enabled only if the configuration level is set to Advanced. Although the value can be changed when the configuration level is set to Normal, we recommend that the value of this field not be changed if the field appears disabled.

- Default—Any
- Example—10 .. 25, 27

ICMP Code

- Code for ICMP.
- Value—Type of ICMP code in the following formats:
 - Number of ICMP code in the range 0–255
 - Comma-separated list of code numbers and ranges of code numbers
 - Ranges of code numbers separated by two dots (..) within the range 0–255
 - Blank—Any ICMP code
- Guidelines—You can enter a value for this field only if you select particular protocols.

This field appears enabled only if the configuration level is set to Advanced. Although the value can be changed when the configuration level is set to Normal, we recommend that the value of this field not be changed if the field appears disabled.

- Default—Any
- Example—75

Priority

- Numeric value that indicates which firewall exception takes precedence if a subscriber has multiple exceptions for a firewall service.
- Value—Integer in the range specified by the online help for this field
- Guidelines—You must specify a priority for the firewall exception. A lower number indicates a higher priority. Use a unique priority for each firewall exception that relates to the same traffic. If two rules have the same priority, they will be applied to traffic in an unpredictable order.
- Default—No value
- Example—5

Direction

- Direction, with respect to the enterprise, of the traffic.
- Value
 - Incoming—Applies to traffic that starts outside the enterprise
 - Outgoing—Applies to traffic that starts inside the enterprise
 - Both—Applies to traffic flows that start inside or outside the enterprise
 - Guidelines—If you select a custom firewall rule, you cannot specify a direction. Custom firewall rules should have names that reflect what the rule does.
- Default—Incoming
- Example—Both

Action

- Way in which the firewall should handle the incoming or outgoing traffic.
- Value
 - Allow—Let the traffic through the firewall.
 - Reject—Send an ICMP reply that explains why the firewall blocked the traffic.
 - Discard—Drop the traffic without sending any reply.
 - A custom value configured by the service provider.
- Guidelines—Other actions may be available—one for each custom firewall rule.
- Default—Allow
- Example—Discard

Enabled

- Status of the rule.
- Value
 - Gray box—Rule is inherited from a parent subscriber or the rule is scheduled
 - White box—Rule is configured for this subscriber

- Box with check mark—Rule is enabled
- Empty box—Rule is disabled
- Guidelines—Click box to enable or disable a rule.
- Default—Rule is disabled

Creating Firewall Exceptions for Stateful Firewalls

- To create a firewall exception for a subscriber:
1. If you want to create a firewall exception for a particular application object, first create that object.
 2. Access the subscriber’s Firewall page.

Figure 24: Firewall Page with Firewall Service Applied

default ▶ local ▶ Acme ▶ Boca ▶ Primary ▶

Bandwidth & VPNsApplicationsFirewallAddressesNATSchedulesManagers

Firewall Service ⓘ

EmailAndWeb ▼Apply

Status...

Exceptions to Firewall Service

Priority	Name	Affected Traffic				Firewall Action	Schedule ⓘ	Enabled	
		Direction	Source IPs	Destination IPs	Application				
<input type="text"/>	<input type="text"/>	Incoming ▼	<input type="text"/>	<input type="text"/>	Any ▼	Allow ▼		<input type="checkbox"/>	Create

3. Enter field values to configure the values for the firewall exception.

See “Fields for Exceptions to Stateful Firewalls in Enterprise Manager Portal” on page 267.
4. Click **Create**.

Fields for Exceptions to Stateful Firewalls in Enterprise Manager Portal

Use the fields in this topic to specify exceptions to stateful firewalls.

Priority

- Numeric value to indicate which firewall exception takes precedence if a subscriber has multiple exceptions for a firewall service.
- Value—Integer in the range specified by the online help for this field
- Guidelines—You must specify a priority for the firewall exception. A lower number indicates a higher priority. Use a unique priority for each firewall exception that relates to the same traffic. If two rules have the same priority, they will be applied to traffic in an unpredictable order.
- Default—No value
- Example—5

Name

- Name of the subscription to the firewall service.
- Value—Text string
- Guidelines—You must specify a name for the firewall exception.
- Default—No value
- Example—videoConference

Direction

- Direction, with respect to the enterprise, of the initial traffic flow in a conversation.
- Value
 - Incoming—Applies to an initial traffic flow that starts outside the enterprise
 - Outgoing—Applies to an initial traffic flow that starts inside the enterprise
 - Both—Applies to initial traffic flows that start inside or outside the enterprise
- Default—Incoming
- Example—Both

Source IPs

- Source IP addresses (as contained in the IP packets) of traffic to which the firewall exception applies.
- Value—[not] < networkAddress > / < networkMask >
 - not—All addresses except the listed addresses
 - < networkAddress > —IP address of the network

- < networkMask > —Subnet mask
- Guidelines—To specify traffic with a particular source IP address, enter an IP address. To specify all traffic except that with a particular source IP address, precede the IP address with the keyword **not**. To specify traffic with any source IP address, leave the field empty. To specify multiple source IP addresses, set the configuration level of the portal to Advanced (see “Setting the Configuration Level for Enterprise Manager Portal” on page 220), and enter multiple addresses on different lines.
- Default—No value
- Example—192.0.2.0/24

Destination IPs

- Destination TCP/UDP ports (as contained in the IP packets) of traffic to which this firewall exception applies.
- Value—[not] < networkAddress > / < networkMask >
 - not—All addresses except the listed addresses
 - < networkAddress > —IP address of the network
 - < networkMask > —Subnet mask
- Guidelines—To specify traffic with a particular destination IP address, enter an IP address. To specify all traffic except that with a particular destination IP address, precede the IP address with the keyword **not**. To specify multiple destination IP addresses, set the configuration level of the portal to Advanced (see “Setting the Configuration Level for Enterprise Manager Portal” on page 220), and enter multiple addresses on different lines.
- Default—No value
- Example—192.0.2.0/24

Application

- Application object to which the firewall applies.
- Value—Application object you defined
- Guidelines—Select an application object from the menu.
- Default—Any
- Example—ftp

Firewall Action

- The way in which the firewall should handle the incoming or outgoing traffic.
- Value
 - Allow—Let the traffic through the firewall

- Reject—Send an ICMP reply that explains why the firewall blocked the traffic
- Discard—Drop the traffic without sending any reply
- Default—Allow
- Example—Discard

Schedule

- Configured schedule to use.
- Name of the schedule
- Guidelines—This field appears if scheduling is enabled for the portal. .
- Default—No value

Enabled

- Status of the firewall exception.
- Value
 - Gray box—Firewall exception is inherited from a parent subscriber
 - White box—Firewall exception is configured for this subscriber
 - Box with check mark—Firewall exception is enabled
 - Empty box—Firewall exception is disabled
- Guidelines—Click box to enable or disable a firewall exception.
- Default—Firewall exception is disabled

Adding a Schedule to a Firewall Exception

A schedule must be configured before you can apply one to a firewall exception.

To add a schedule to a firewall exception:

1. Access the subscriber's Firewall page.
2. In the Firewall page, select a schedule from the Schedule menu for the exception. See the following field description for details.

Schedule Field for a Firewall Exception

Schedule

- Configured schedule to use.
- Name of the schedule
- Guidelines—This field appears if scheduling is enabled for the portal.
- Default—No value

Modifying Firewall Exceptions

To modify a firewall exception:

1. Start at the Firewall page for the subscriber.
2. Change the values in the fields for this firewall exception.
3. For stateless firewalls, to change the values for affected traffic, click Edit under Affected Traffic, make changes in the Edit Exception dialog box, and click **Apply**.

or

For stateful firewalls, click **Apply** for the application protocol.

Deleting Firewall Exceptions

To delete a firewall exception:

1. Start at the Firewall page for the subscriber.
2. Click **Delete** for the firewall exception.

Deleting Basic Firewalls

To delete a basic firewall:

1. Disable all firewall exceptions and NAT rules configured for this subscriber.

For information about disabling these values, see the field descriptions in “Creating Firewall Exceptions for Stateful Firewalls” on page 267 and “Applying NAT Rules to Traffic” on page 275.

2. Disable all firewall exceptions and NAT rules that this subscriber inherits from parent subscribers.
3. Disable all firewall exceptions and NAT rules defined for this subscriber’s subordinate subscribers.
4. Access the Firewall page for the subscriber for which you configured the firewall.
5. Select **No Firewall** from the Firewall Service menu.
6. Click **Apply**.

Monitoring the Use of Subscriptions to Firewall Services

Purpose Monitor the use of firewall subscriptions.

- Action**
1. Access the subscriber's Firewall page.
 2. In the Firewall page, click the **Usage Data** link in the last column.

or

Click the **Usage Data** link under Firewall Service.

The Service Usage Data page appears.

Service Usage

Service Usage Data

This data is for the subscription **tcpProtocol** to service **Firewall Exception**.

Access Link	Usage Data					
	For Period From	For Period To	Incoming Bytes	Outgoing Bytes	Incoming Packets	Outgoing Packets
primary.toronto.acme.local/default	Wednesday, October 26, 2005 1:46:56 PM	Wednesday, October 26, 2005 1:56:28 PM	0	0	0	0

[Refresh](#)

The table above shows usage data for the service. The usage data covers the period starting when the service was most recently activated on the access link, and ending when the usage data was most recently collected from the network infrastructure. Usage data is collected periodically (e.g. once an hour). No usage data is available for subscriptions that are not active on the access link.

Usage data may be shown as "Unknown". Usage data may be unknown because no data has yet been collected for the access link, or because the access link is currently down, or because the usage data collection mechanism is temporarily unavailable.

Copyright © 1998-2005, Juniper Networks, Inc. ENT.B 6.2.1.002

Working with IP Addressing and NAT Services

You can configure NAT addressing and services from Enterprise Manager Portal. Topics include:

- Requesting Public IP Addresses for NAT Services on page 273
- Canceling Requests for Public IP Addresses on page 274
- Returning Public IP Addresses to Service Providers on page 275
- Applying NAT Rules to Traffic on page 275
- Configuring Public IP Addresses for Outgoing Traffic on page 277

- Configuring Public IP Addresses for Incoming Traffic on page 278
- Configuring Fixed Public Addresses for Outgoing Traffic on page 279
- Modifying NAT Rules on page 280
- Deleting NAT Rules on page 280

Requesting Public IP Addresses for NAT Services

To request one or more IP addresses:

1. In the navigation pane of Enterprise Manager Portal, click the access to which you want to request an IP address.
2. Click the **Addresses** tab.

The Addresses page appears.

Figure 25: Addresses Page Before Requesting Addresses

default > local > Acme > Boca > Primary

Bandwidth & VPNs Applications Firewall **Addresses** NAT Schedules Managers

Public IP Addresses

No public IP addresses have been assigned to this access link.

Request More Public IP Addresses

Number of Addresses	Contiguous	
1	<input type="checkbox"/>	Request

Outstanding Requests for Public IP Addresses

No outstanding requests for public IP addresses exist.

3. In the Number of Addresses field, enter the number of addresses that you want.
- See “Address Fields for NAT Addressing in Enterprise Manager Portal” on page 274.
4. (Optional) If you specify multiple IP addresses and you want the addresses to be sequential, select **Contiguous**.
5. Click **Request**.

Enterprise Manager Portal sends a request to the service provider for the IP addresses and displays the number of outstanding requests. When the service provider allocates the IP addresses, Enterprise Manager Portal displays the public IP addresses assigned to this access and makes the addresses visible in the menus on the NAT page for that access, as shown in Figure 26 on page 274. If a request for an IP address is outstanding for a certain period of time, Enterprise Manager Portal automatically sends a reminder to the service provider.

Figure 26: Addresses Page After Requesting Addresses

Acme ▸ Boca ▸ Primary ▸

Bandwidth & VPNs Applications Firewall **Addresses** NAT Schedules Managers

Public IP Addresses		
Address	Used By	
165.165.165.165		<input type="checkbox"/>
165.165.165.166		<input type="checkbox"/>
165.165.165.167		<input type="checkbox"/>
165.165.165.168		<input type="checkbox"/>
165.165.165.169		<input type="checkbox"/>
165.165.165.170		<input type="checkbox"/>
Release selected public IPs:		<input type="button" value="Release"/>

Request More Public IP Addresses		
Number of Addresses	Contiguous	
<input type="text" value="1"/>	<input type="checkbox"/>	<input type="button" value="Request"/>

Outstanding Requests for Public IP Addresses

No outstanding requests for public IP addresses exist.

Address Fields for NAT Addressing in Enterprise Manager Portal

Use the fields in this topic to specify address range(s).

Number of Addresses

- Number of IP addresses that you want the service provider to supply.
- Value—Integer in the range 1–2147483647
- Default—1

Contiguous

- Whether or not requested multiple IP addresses should be sequential.
- Value
 - Checked box—IP addresses must be contiguous
 - Empty box—IP address need not be contiguous
- Default—IP address need not be contiguous

Canceling Requests for Public IP Addresses

To cancel a request:

- Click **Cancel** for that request in the Outstanding Requests for IP Addresses table.

default ▶ local ▶ Acme ▶ Boca ▶ **Primary** ▶

Public IP Addresses

No public IP addresses have been assigned to this access link.

Request More Public IP Addresses

Number of Addresses	Contiguous	
1	<input type="checkbox"/>	Request

Outstanding Requests for Public IP Addresses

Request Time	Number of Addresses	Contiguous	
Tue Jul 19 09:47:51 EDT 2005	1	No	Cancel

Returning Public IP Addresses to Service Providers

To return one or more IP addresses to the service provider:

1. Start at the Addresses page for the subscriber.
2. In the Public IP Addresses table, click in the small box in the last column for each address that you want to return.

If an enabled NAT rule is using an address, the box for that address is dimmed, and you cannot release that address until you disable or delete the NAT rule listed in the Used By field.

3. Click **Release**.

Applying NAT Rules to Traffic

After you protect an access with a firewall and have obtained one or more public IP addresses for the access, you can apply the following types of NAT rules to traffic on the access.

- Public addresses for outgoing traffic

Also known as *dynamic source NAT*, this type of NAT allows computers with private IP addresses in a private network to share a small set of public IP addresses for outgoing connections. For example, employees in an enterprise can use these public IP address for browsing the Web. You can specify the source IP addresses and, optionally, the ports that the outgoing traffic will use.

- Public addresses for incoming traffic

Also known as *static destination NAT*, this type of NAT allows you to expose to the world a server, such as a Web server, that has a private IP address in your

private network. You specify a public IP address, and incoming connections destined for that public IP address will be received by your server at its private IP address.

- Fixed public addresses for outgoing traffic

Also known as *static source NAT*, this type of NAT allows you to specify the public source IP to be used for specific outgoing traffic. To specify this type of NAT you must set the configuration level of the portal to Advanced (see “Setting the Configuration Level for Enterprise Manager Portal” on page 220).

Enterprise Manager Portal ensures that the SAE activates a basic firewall service before it activates a NAT service.

To apply NAT rules to traffic on JUNOS routing platforms:

1. In the navigation pane of Enterprise Manager Portal, click the access that connects to the router.
2. Click the **NAT** tab.

The NAT page appears.

Figure 27: NAT Page

Virneo Enterprise Portal

Log out

Navigation

default local Acme Boca Backup

ent-admin

default

local

ABCInc

Acme

Boca

Backup

Ottawa

Toronto

Primary

retailer-one

retailer-two

SP

virtual-SP

Refresh

Bandwidth & VPNs Applications Firewall Addresses NAT Schedules Managers

Public Addresses for Outgoing Traffic

Address Range	Port Range	Enabled	
From: 192.0.2.22	From:	<input type="checkbox"/>	Create
To: 192.0.2.22	To:		

Public Addresses for Incoming Traffic

Priority	Name	Public IP	Private IP	Application	Enabled	
		192.0.2.22		Any	<input type="checkbox"/>	Create

Fixed Public Addresses for Outgoing Traffic

Priority	Name	Private IP	Public IP	Application	Enabled	
			192.0.2.22	Any	<input type="checkbox"/>	Create

© Virneo 2004

3. Configure NAT for incoming and outgoing interfaces on the router.

Related Topics

- Configuring Public IP Addresses for Outgoing Traffic on page 277
- Configuring Public IP Addresses for Incoming Traffic on page 278

Configuring Public IP Addresses for Outgoing Traffic

To configure public IP addresses for outgoing traffic:

1. Locate the area called Public Addresses for Outgoing Traffic in the NAT page.
2. Enter field values to specify how the router will apply the NAT rule to outgoing traffic.

See “Outgoing Traffic Fields for NAT Addressing in Enterprise Manager Portal” on page 277.

3. Select **Enabled**.
4. Click **Create**.

Outgoing Traffic Fields for NAT Addressing in Enterprise Manager Portal

Use fields in this topic to configure NAT addressing for outgoing traffic.

Address Range

- Contiguous range of public IP addresses to which the source addresses of clients in the enterprise are translated.
- Value—Public IP addresses
- Guidelines—Select the starting and ending IP addresses in the From and To menus. For one IP address, select the same address in the From and To menus.
- Default—No value

Port Range

- Range of ports that are used as the source ports in outgoing IP packets after the NAT translation.
- Value—Integers in the range 0–65535
- Guidelines—Specify the starting and ending port numbers in the From and To fields. Be sure to use a port range big enough to allow all the private addresses to share the limited set of public addresses. To specify all ports in the range 1024–65535, leave these fields empty.
- Default—No value

Enabled

- Whether or not the router applies NAT to outgoing traffic on this access.
- Value
 - Enabled—Checked box

- Disabled—White box
- Default—Disabled

Configuring Public IP Addresses for Incoming Traffic

To configure public IP addresses for incoming traffic:

1. Locate the area called Public Addresses for Incoming Traffic in the NAT page.
2. Using the field descriptions below, specify how the router will apply the NAT rule to incoming traffic.
3. Click Create.

Incoming Traffic Fields for NAT Addressing in Enterprise Manager Portal

Use fields in this topic to configure NAT addressing for incoming traffic.

Priority

- Numeric value that indicates which NAT rule takes precedence if you specify more than one NAT rule for an IP address.
- Value—Integer in the range specified by the online help for this field
- Guidelines—You must specify a priority for the NAT rule. A lower number indicates a higher priority. Use a unique priority for each NAT rule that relates to the same traffic. If two rules have the same priority, they will be applied to traffic in an unpredictable order.
- Default—No value
- Example—5

Name

- Name of the NAT rule
- Value—Text string
- Default—No value
- Example—rule1

Public IP

- Public IP address that the router translates to a private address in the enterprise.
- Value—IP address
- Guidelines—Select the public destination address that is to be translated into a private destination address inside the enterprise.
- Default—No value

Private IP

- Private IP address to which the router translates the public IP address.
- Value—IP address
- Guidelines—Enter the private address of the host you wish to make available outside the enterprise.
- Default—No value

Application

- Application object to which the router will apply NAT.
- Value
 - < application > —An application object that you created.
 - Any—Any application
- Guidelines—Select a value from the menu.
- Default—Any
- Example—myVideoConference

Enabled

- Whether or not the router applies NAT to incoming traffic on this access.
- Value
 - Enabled—Checked box
 - Disabled—White box
- Default—Disabled

Configuring Fixed Public Addresses for Outgoing Traffic

To configure fixed public IP addresses for outgoing traffic:

1. Set the portal configuration level to Advanced (see “Setting the Configuration Level for Enterprise Manager Portal” on page 220).
2. Locate the area called Fixed Public Addresses for Outgoing Traffic in the NAT page (see Figure 27 on page 276).

3. Click **Create**.

Modifying NAT Rules

To modify a NAT rule:

1. Modify the entry in the appropriate table.
2. Click **Apply**.

Deleting NAT Rules

To delete a public IP address for outgoing traffic, click delete for the address range in the Public Addresses for Outgoing Traffic table.

Monitoring the Status of Subscriptions

Purpose Monitor the status of a subscription.

- Action**
1. Start at the page that lists information about the subscription.
For an example, a page that shows BoD subscriptions.
 2. In the last cell of the row of data for the subscription, click **Status**.

The Subscription Status page appears.

The Subscription Status page displays the status of this subscription for all accesses subordinate to this subscriber. The page appearance varies depending on whether the subscription is scheduled. You can click the **Refresh** button to update status information.

The following Subscription Status page shows the status for an unscheduled subscription.

Subscription Status - Microsoft Internet Explorer

Subscription Status

Subscription Status

The status of the **enabled** subscription to service **1.0 Mbps**.

Access Link	As Of	Status
backup.boca.acme.local/default	Thu Jan 06 10:11:13 EST 2005	Unknown
primary.boca.acme.local/default	Thu Jan 06 10:11:13 EST 2005	Unknown
primary.ottawa.acme.local/default	Thu Jan 06 10:11:14 EST 2005	Inactive (should be active)
backup.toronto.acme.local/default	Thu Jan 06 10:12:32 EST 2005	Unknown
primary.toronto.acme.local/default	Thu Jan 06 10:12:32 EST 2005	Unknown

Refresh Fix Problems

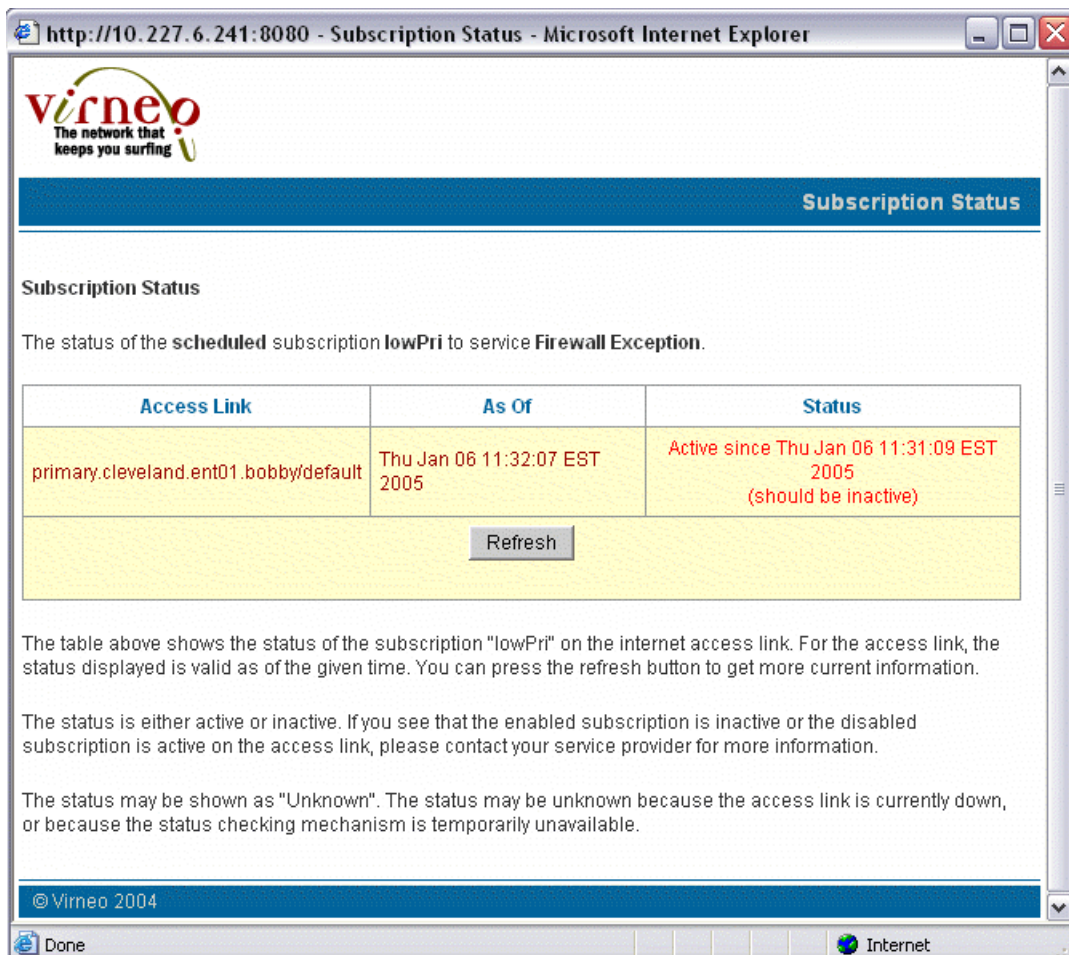
Each row in the table above shows the status of the subscription on one internet access link. For each access link, the status displayed is valid as of the given time. You can press the refresh button to get more current information.

The status is either active or inactive. If you see that an enabled subscription is inactive or a disabled subscription is active on some access links, you will also see a button which you can press to fix these problems. If the system is unable to automatically fix the problems, you will be provided with further information that you or your service provider can use to fix the problems.

The status may be shown as "Unknown". The status may be unknown because the access link is currently down, or because the status checking mechanism is temporarily unavailable.

© Virneo 2004

The following Subscription Status page shows the status for a scheduled subscription.



Meaning Table 25 on page 282 shows the possible status for subscriptions.

Table 25: Possible Subscription Status

Status	Meaning	Category
Active	Subscription is enabled and is operative.	Subscription is functioning correctly.
Inactive	Subscription is disabled.	Subscription is functioning correctly.
Active (should be inactive)	Subscription is disabled but is operative.	Subscription is not functioning correctly.
Inactive (should be active)	Subscription is enabled but is inoperative.	Subscription is not functioning correctly.
Unknown	Enterprise manager Portal cannot currently communicate with the SAE, typically because the access is not functioning correctly or the checking mechanism is temporarily unavailable.	Subscription may be functioning correctly, but another problem exists.

Troubleshooting Subscriptions That Are Not Functioning Correctly

Problem One or more subscriptions are not functioning correctly.

Solution The Fix Problems link appears in the Subscription Status page. To troubleshoot the problems with the nonfunctioning subscriptions, click **Fix Problems**. This action causes Enterprise Manager Portal to attempt to resolve the problems with the subscriptions.

If Enterprise Manager Portal succeeds in resolving the problems, the Subscription Status page displays the new settings. Otherwise, the Subscription Status page displays more information about the problems.

Troubleshooting Subscriptions of Unknown Status

Problem Subscriptions of unknown status and subscriptions are not functioning correctly exist. The software will also attempt to update the unknown subscriptions when you click **Fix Problems**. If Enterprise Manager Portal cannot resolve the status, it will remain unknown.

Solution If you have subscriptions of unknown status and either the Fix Problems link is not available or using the link does not resolve the status, click **Subscription Status** page. If this action does not solve the problem, check the status of the subscription later.

Chapter 21

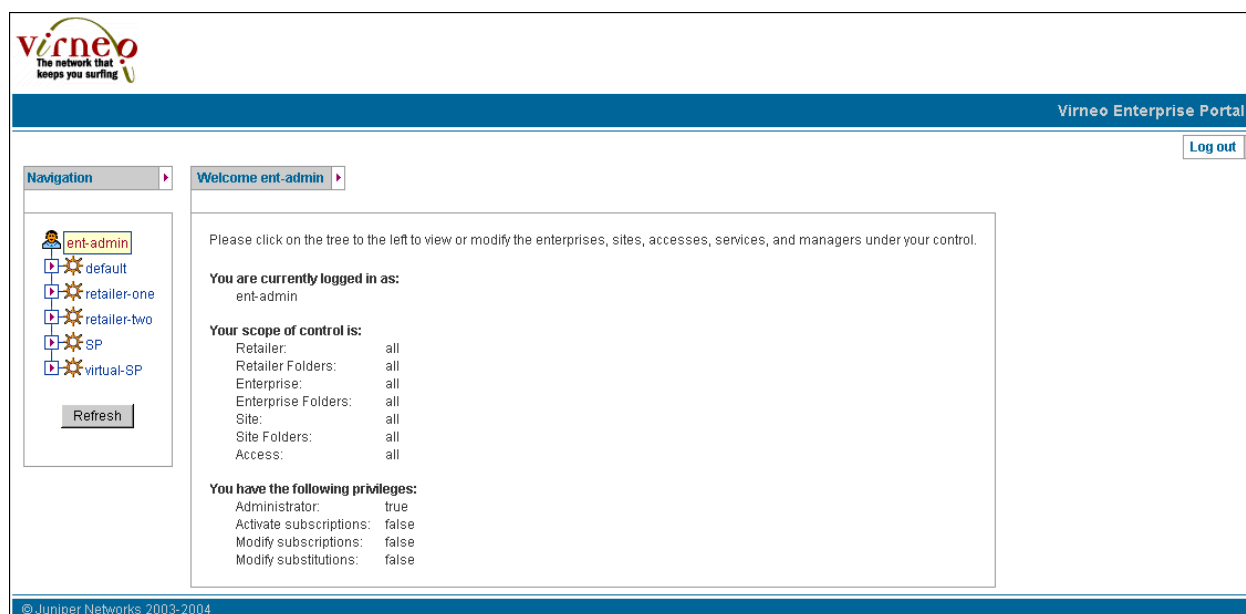
Managing Enterprise Service Portals

- Displaying Information About Your Control in the Enterprise Through the Enterprise Service Portal on page 285
- Updating Data That the Enterprise Service Portal Displays on page 286
- Managing Operators Through the Enterprise Service Portal on page 286
- Creating Managers Through the Enterprise Service Portal on page 286
- Modifying Managers Through the Enterprise Service Portal on page 289
- Deleting Managers Through the Enterprise Service Portal on page 289

Displaying Information About Your Control in the Enterprise Through the Enterprise Service Portal

Purpose Display information about your scope of control and permissions in the enterprise.

Action Click the icon for the manager at the root of the navigation pane. The portal displays your Welcome page.



Updating Data That the Enterprise Service Portal Displays

To update the data that the enterprise service portal displays, click Refresh in the navigation pane. This action deletes data from the enterprise service portal cache and causes the enterprise service portal to display new data from the directory. If you refresh a Web page in the portal with the Web browser's refresh utility, the Web browser displays data from the cache, and you may not see the latest data.

Managing Operators Through the Enterprise Service Portal

Typically, a service provider uses the SRC CLI, the C-Web interface, or an LDAP client to create one operator for each enterprise. This operator, or manager, represents the primary IT manager for the enterprise.

The primary IT manager uses the enterprise service portal to create and manage other managers in the directory and gives those managers privileges to manage specific sites and accesses.

- Related Topics**
- Creating Managers Through the Enterprise Service Portal on page 286
 - Modifying Managers Through the Enterprise Service Portal on page 289
 - Deleting Managers Through the Enterprise Service Portal on page 289

Creating Managers Through the Enterprise Service Portal

To create managers through the enterprise service portal:

1. In the navigation pane of the enterprise service portal, click the object that you want the manager to control.
2. Click the **Managers** tab in the portal.

The portal displays the Manager's page for the object.

Figure 28: Manager's Page

Virneo Enterprise Portal

Log out

Navigation

ent-admin

- SP
- default
- retailer-one
- retailer-two
- virtual-SP

Refresh

default

VPNs	Bandwidth & VPNs	Applications	Firewall	Schedules	Managers		
Login ID	Admin.	Modify sub.	Modify params.	Activate sub.	Modify VPNs	Password	
<input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text"/>	Create

© Virneo 2004

3. Complete the fields in a new line of the table.

See “Managers Fields in the Enterprise Service Portal” on page 287.

4. Click **Create**.

The portal adds the new manager to the table.

Managers Fields in the Enterprise Service Portal

In the Managers tab of an enterprise service portal, you can modify the following fields to control privileges for managers.

Login ID

- Name that this manager uses to access the enterprise portal.
- Value—Text string
- Guidelines—Login IDs for enterprises must be unique within the whole enterprise; retailer-level login IDs must be unique to the retailer.
- Default—No value
- Example—Operator1

Admin.

- Whether or not the manager has complete control over managers, subscribers, subscriptions, substitutions, subscription sessions, and virtual private networks (VPNs) for this object and its subordinate objects.
- Value
 - Enabled—Checked box

- Disabled—White box
- Default—Disabled

Modify sub.

- Whether or not the manager has complete control over subscriptions and subscription sessions for this object and its subordinate objects.
- Value
 - Enabled—Checked box
 - Disabled—White box
- Default—Disabled

Modify params.

- Whether or not the manager can configure substitutions in subscribers and subscriptions for this object and its subordinate objects.
- Value
 - Enabled—Checked box
 - Disabled—White box
- Default—Disabled

Activate sub.

- Whether or not the manager can configure automatic activation of subscriptions and manually activate and deactivate subscription sessions for this object and its subordinate objects.
- Value
 - Enabled—Checked box
 - Disabled—White box
- Default—Disabled

Modify VPNs

- Whether or not the manager can modify, export, and cancel the export of VPNs in the enterprise.
- Value
 - Enabled—Checked box

- Disabled—White box
- Guidelines—This field appears only if the service provider configures the portal to display the VPN features.
- Default—Disabled

Password

- Password that this manager uses to access the enterprise portal.
- Value—Text string
- Default—No value
- Example—Secret

Modifying Managers Through the Enterprise Service Portal

To modify a manager's privileges:

1. Start at the Manager's page.
2. Change the values in the fields for this manager.
3. If you want to revert to the original values, click **Reset**.
4. Click **Apply**.

Deleting Managers Through the Enterprise Service Portal

To delete a manager:

1. Start at the Manager's page.
2. Click **Delete** for the manager.

Chapter 22

Using NAT Address Management Portal

- Overview of NAT Address Management Portal on page 291
- Assigning IP Addresses on page 291
- Acknowledging the Release of IP Addresses on page 292

Overview of NAT Address Management Portal

Service providers use NAT Address Management Portal to manage requests about public IP addresses from IT managers. When an IT manager sends a request about IP addresses through Enterprise Manager Portal, the portal sends an e-mail to the service provider that contains a link to NAT Address Management Portal.

For demonstration purposes or for small service providers, a human administrator can deal with this e-mail manually. In a large production environment, however, the e-mail will be sent to a machine that automatically assigns addresses to accesses.

Assigning IP Addresses

To assign IP addresses to accesses manually:

1. Click the link to NAT Address Management Portal in the e-mail.

NAT Address Management Portal appears and displays the status of IP addresses for this link.

NAT Address Management

default ▶ local ▶ Acme ▶ Boca ▶ Primary ▶

Assigned IP Addresses

No public IP addresses have been assigned to this access link

Released IP Addresses

No public IP addresses have been released by this access link

Outstanding Requests for Public IP Addresses

Request Time	Number of Addresses	Must be Contiguous	
Jun 30, 2004 4:03 PM	1	false	Assign IPs

Copyright Juniper Networks 2004

2. Click **Assign IPs**.

The Assign Public IP Addresses window appears.

Assign Public IP Addresses (Contiguous)

	IP Address
1	<input type="text"/>
2	<input type="text"/>
3	<input type="text"/>

Assign


3. Enter an IP address in each line of this window.
4. Click **Assign**.

Acknowledging the Release of IP Addresses

When an IT manager returns an IP address through Enterprise Manager Portal, NAT Address Management Portal displays the returned IP address. You must acknowledge release of the IP Address to the IT manager.

To acknowledge release of IP addresses:

- Click **Acknowledge** in the Released IP Addresses table.



NAT Address Management

default ▸ local ▸ Acme ▸ Boca ▸ Primary ▸

Assigned IP Addresses

No public IP addresses have been assigned to this access link

Released IP Addresses

Release Time	Released IPs
Jul 19, 2004 6:40 PM	192.0.2.22

Acknowledge

Outstanding Requests for Public IP Addresses

Request Time	Number of Addresses	Must be Contiguous	
Jul 18, 2004 2:55 PM	1	false	Assign IPs

Copyright Juniper Networks 2004

Chapter 23

Using the Sample Enterprise Service Portal

- Overview of the Sample Enterprise Service Portal on page 295
- Starting the Sample Enterprise Service Portal on page 295
- Subscribing to Services on page 296
- Activating Subscriptions on page 297
- Deactivating Subscriptions on page 298
- Suspending Subscriptions on page 298
- Canceling Suspensions of Subscriptions on page 299
- Monitoring Use of Subscriptions on page 299
- Specifying Values for Service Parameters in Subscriptions on page 299
- Restoring Default Values for Service Parameters In Subscriptions on page 300
- Deleting Subscriptions on page 300
- Monitoring Service Sessions for a Subscription on page 300
- Defining Networks for Departments in an Enterprise on page 301
- Modifying Network Definitions for Departments in an Enterprise on page 302
- Deleting Network Definitions for Departments in an Enterprise on page 303

Overview of the Sample Enterprise Service Portal

The sample Enterprise Service Portal illustrates how service providers can make their services available to IT managers in an enterprise and that provides developers with a starting point from which they can create their own service portal.

Starting the Sample Enterprise Service Portal

The WAR file for the sample Enterprise Service Portal is *tagsEntDemo.war*. You can locate the WAR file in the `SDK+AppSupport+Demos+Samples.tar.gz` file on the Juniper Networks Web site at: <https://www.juniper.net/support/csc/swdist-erx/src.html>. You deploy this file to an application server, such as JBoss.

When you view the sample portal, take care to open only one browser window yourself. The portal automatically opens pop-up windows for various operations. If

you open more than one browser window yourself, the information in the original window may not be updated correctly when you complete an operation in a pop-up window.

To start the sample Enterprise Service Portal:

1. Enter the URL of the portal in your Web browser, and press Enter. For example:

http://192.0.2.1:8080/tageEntDemo

The login page appears.

2. Select a retailer, or leave the entry blank to view all retailers.
3. Enter your username in the Login ID field and your password in the Password field.

The Welcome page appears. On the left of the page is a navigation pane for the objects in the service provider's directory over which you have control. Your login identity is the root of this navigation pane.

Subscribing to Services

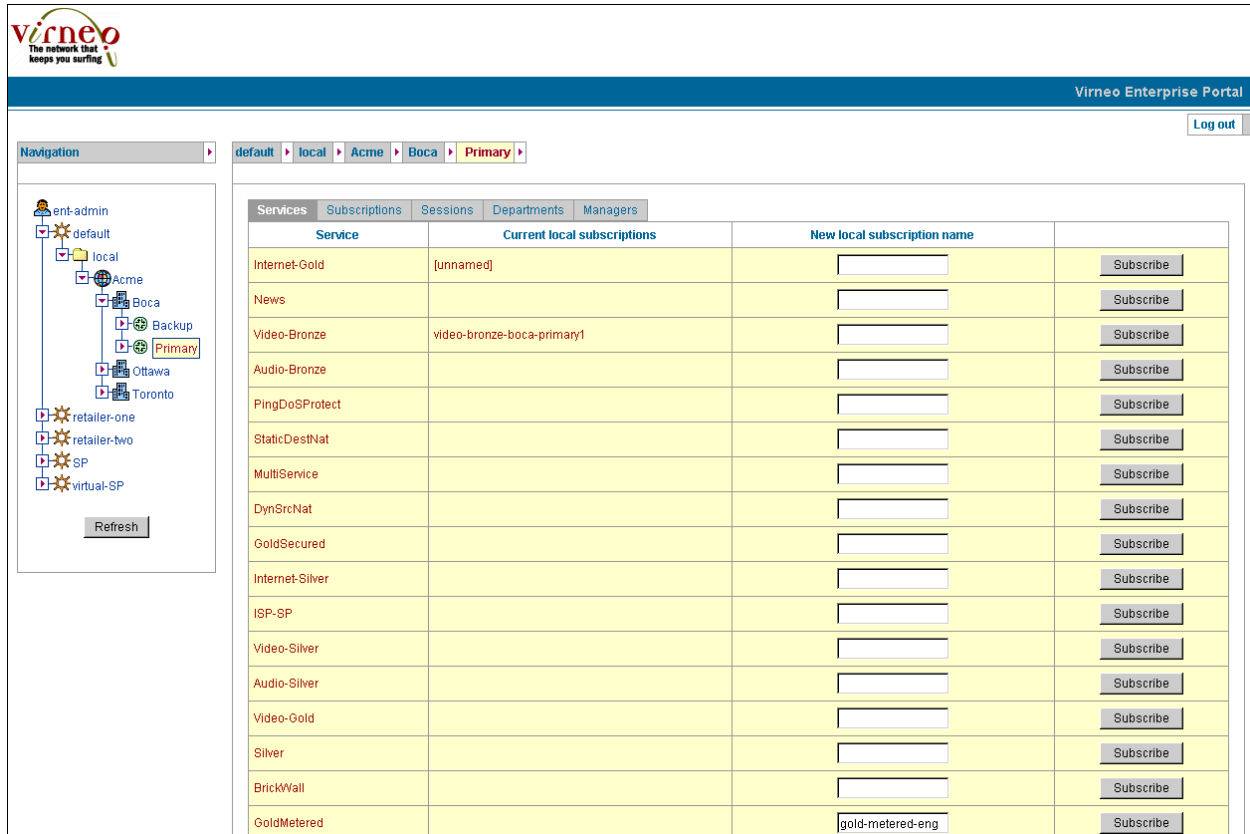
To subscribe to a service:

1. In the navigation pane of the sample Enterprise Service Portal, click the subscriber for whom you want to create a subscription to a service.

The portal displays the information for that subscriber.

2. Click the **Services** tab.

The Services page appears and displays the list of services available to this subscriber and the subscriber's current subscriptions.



The screenshot shows the Virneo Enterprise Portal interface. The navigation pane on the left displays a tree structure with the following nodes: ent-admin, default, local, Acme, Boca, Backup, Primary, Ottawa, and Toronto. The main content area shows a table of services and their current local subscriptions. The 'New local subscription name' field is highlighted for the 'Internet-Gold' service.

Service	Current local subscriptions	New local subscription name	Subscribe
Internet-Gold	[unnamed]		Subscribe
News			Subscribe
Video-Bronze	video-bronze-boca-primary1		Subscribe
Audio-Bronze			Subscribe
PingDoSProtect			Subscribe
StaticDestNat			Subscribe
MultiService			Subscribe
DynSrcNat			Subscribe
GoldSecured			Subscribe
Internet-Silver			Subscribe
ISP-SP			Subscribe
Video-Silver			Subscribe
Audio-Silver			Subscribe
Video-Gold			Subscribe
Silver			Subscribe
BrickWall			Subscribe
GoldMetered		gold-metered-eng	Subscribe

3. In the New local subscription name field, enter a name for the subscription to the service.

You can have one unnamed subscription to a service; if you have multiple subscriptions to a service, only one can be unnamed.

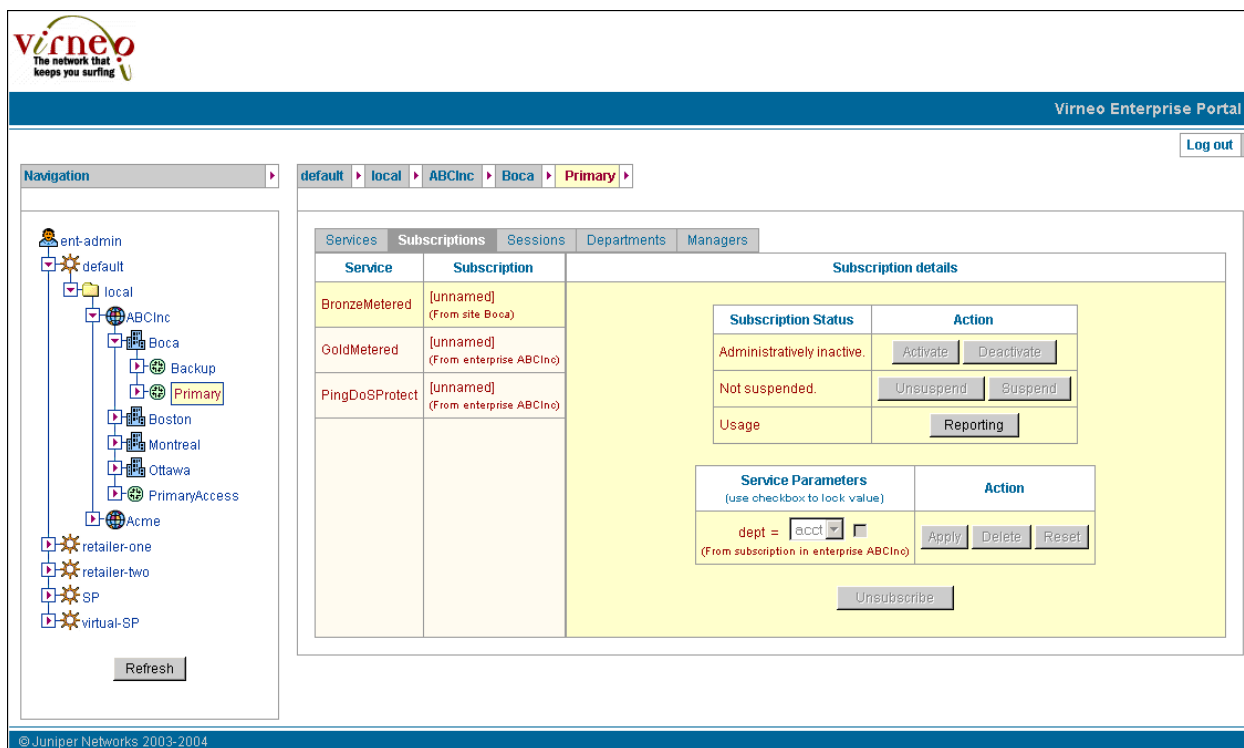
4. Click **Subscribe**.

Activating Subscriptions

To activate a subscription:

1. In the navigation pane of the sample Enterprise Service Portal, click the subscriber for whom the subscription is configured.
2. Click the **Subscriptions** tab.

The Subscriptions page appears. Note that inherited subscriptions cannot be modified.

Figure 29: Subscriptions Page

3. In the Subscription column, click the subscription that you want to activate.
4. In the Subscription details area, click **Activate**.

Deactivating Subscriptions

To deactivate a subscription:

1. Start at the subscriber's Subscriptions page.
2. In the Subscription column, click the subscription you want to deactivate.
3. Click **Deactivate**.

Suspending Subscriptions

You can prevent a subscriber from inheriting a subscription by suspending that subscription. To do so:

1. Start at the subscriber's Subscriptions page.
2. In the Subscription column, click the subscription you want to suspend.
3. Click **Suspend**.

Canceling Suspensions of Subscriptions

If you suspend a subscription for a subscriber, you can restore the inherited subscription for that subscriber. You can also maintain the suspension for that subscriber and restore the inherited subscription for that subscriber's subordinate subscribers. To do so:

1. Start at the Subscriptions page for the subscriber for which you want to restore the inherited subscription.
2. In the Subscription column, click the subscription you want to allow.
3. Click **Unsuspend**.

Monitoring Use of Subscriptions

Purpose Monitor the use of a subscription.

- Action**
1. Start at the subscriber's Subscriptions page.
 2. In the Subscription column, click the subscription you want to view.
 3. Click **Reporting**.

The Usage Reporting page appears. If the enterprise service portal cannot contact the relevant SAE to obtain data for this subscriber, the page displays the statistics as Unknown.

EmailAndWeb%EmailAndWeb1 Service Session under	Usage Information					
	In Bytes	Out Bytes	In Packets	Out Packets	Update Time	Start Time
Primary.Boca.Acme.local/default	Unknown	Unknown	Unknown	Unknown	Unknown	Unknown
<div>Reload</div>						

To update the data on this page, click Reload.

Specifying Values for Service Parameters in Subscriptions

On the Subscriptions page, the Service Parameters column lists the parameters you can specify for this subscription. Subscriptions inherit values for service parameters from subscriptions of parent subscribers. If the parameter is locked by the parent subscriber, the value appears dimmed in the portal, and you cannot modify the value. If the parameter is not locked by a parent subscriber, you can modify the value.

To specify a value for a parameter:

1. Start at the subscriber's Subscriptions page.
2. Locate the parameter in the Service Parameters column.
3. Provide a value for this parameter.

- 4. (Optional) Select **Locked** to prevent managers of subordinate subscribers from changing this value.
- 5. If you want to revert to the original values, click **Reset**.
- 6. Click **Apply**.

Restoring Default Values for Service Parameters In Subscriptions

To restore the default value for a service parameter:

- 1. Start at the subscriber's Subscriptions page.
- 2. Locate the parameter in the Service Parameters column.
- 3. Click **Delete**.

Some services may have parameters without a default value. If you do not supply values for these parameters, the SAE cannot perform the substitutions when it tries to activate a service, and the activation will fail.

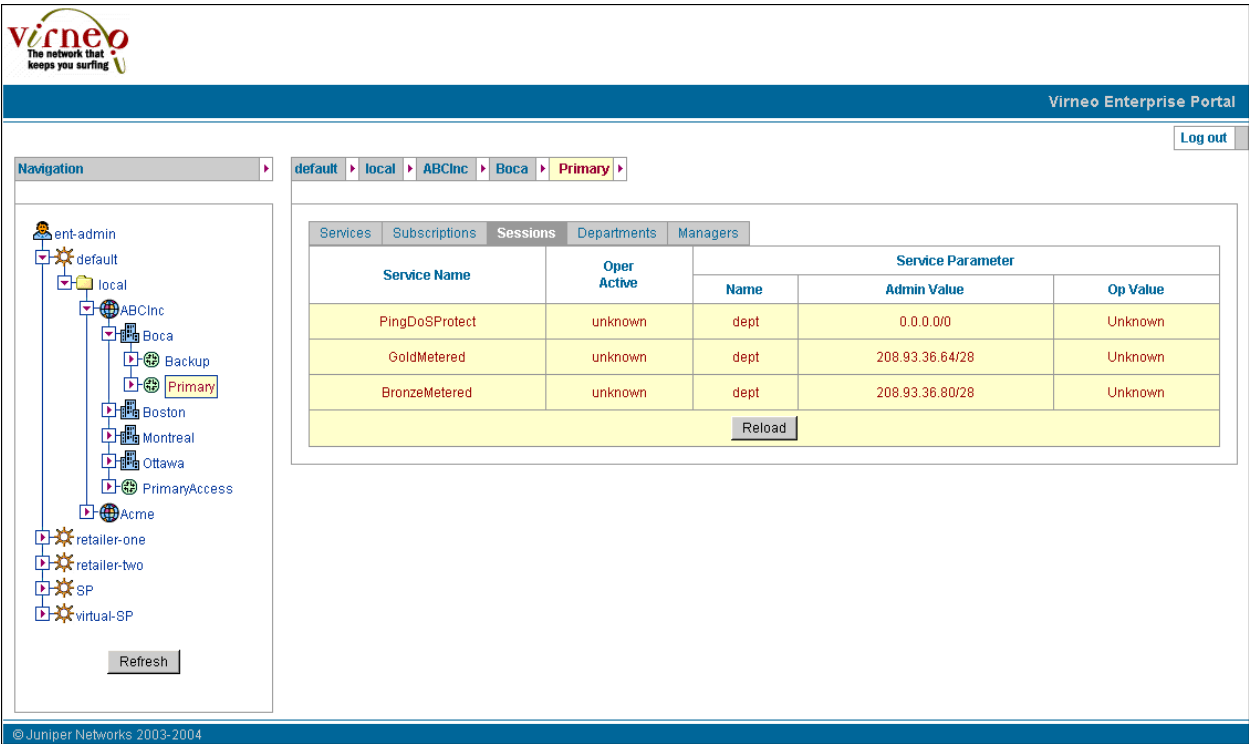
Deleting Subscriptions

To delete a subscription:

- 1. Start at the subscriber's Subscriptions page.
- 2. Click the subscription you want to delete.
- 3. Click **Unsubscribe**.

Monitoring Service Sessions for a Subscription

Purpose	Monitor the service sessions for a subscription.
Action	<div><div>1. In the navigation pane of the sample Enterprise Service Portal, click the subscriber for which you want to monitor the sessions.</div><div>The portal displays the information for that subscriber.</div><div>2. Click the Sessions tab.</div><div>The portal displays the status of each subscription and the parameters associated with each subscription.</div></div>



To update the data on this page, click **Reload**.

Defining Networks for Departments in an Enterprise

To define the networks for departments in an enterprise:

1. In the navigation pane of the sample Enterprise Service Portal, click the subscriber for whom you want to define the department.

The portal displays the information for that subscriber.

2. Click the **Departments** tab.

The Departments page appears.

Figure 30: Departments Page

Virneo Enterprise Portal

Navigation: default local Acme Boca Primary

ent-admin
 default
 local
 Acme
 Boca
 Backup
 Primary
 Ottawa
 Toronto
 retailer-one
 retailer-two
 SP
 virtual-SP
 Refresh

Department	Department network	Locked	
eng	192.0.2.22/2	<input checked="" type="checkbox"/>	Apply Delete Reset
acct	192.0.2.22/3	<input type="checkbox"/>	Apply Delete Reset
		<input type="checkbox"/>	Create

© Juniper Networks 2003-2004

3. In the Department field, enter the name of the department.
4. In the Department network field, enter the network that this department uses, or leave this field empty to use the department name.
5. (Optional) Select **Locked** to prevent managers of subordinate subscribers from changing this value.
6. Click **Create**.

This feature illustrates how service providers can use parameters and substitutions in the portal. The fields called Department and Department network are a name and value for a substitution, respectively. These parameters are also defined in SRC objects such as services and policies. The IT manager provides actual values for the parameters through the portal. Service providers could use these parameters to track and charge each department for the volume of bandwidth. For more information about parameters and substitutions, see [Parameters and Substitutions](#).

Modifying Network Definitions for Departments in an Enterprise

To modify a network definition for a department:

1. Start at the subscriber's Departments page.
2. Modify values for the department.
3. If you want to revert to the original values, click **Reset**.
4. Click **Apply**.

Deleting Network Definitions for Departments in an Enterprise

To delete a network definition for a department:

1. Start at the subscriber's Departments page.
2. Click **Delete** for the department.

Chapter 24

Developing an Enterprise Service Portal

- Developing a Portal Based on the Sample Enterprise Service Portal on page 305
- Preparing to Develop a Sample-Based Enterprise Service Portal on page 305
- Creating a Portal Project for a Sample-Based Enterprise Service Portal on page 306
- Building a Sample-Based Enterprise Service Portal on page 306
- Deploying a Sample-Based Enterprise Service Portal on page 307
- Testing a Sample-Based Enterprise Service Portal on page 307
- Using a Virtual Address for the Portal on page 307

Developing a Portal Based on the Sample Enterprise Service Portal

The source code is included with the sample Enterprise Service Portal. To make complex changes to the portal, we recommend that you install a Java development environment.

The sample Enterprise Service Portal does not require any specific environment, but the procedures to develop a portal assume that you use the Eclipse platform. A servlet container is required to run the portals during development. We recommend that you use Tomcat and its Eclipse plug-in.

For information about your development environment, see the documentation for the product you are using.

Preparing to Develop a Sample-Based Enterprise Service Portal

The following instructions describe how to set up a development environment that uses Eclipse and Tomcat on a Solaris platform. If you want to use Eclipse and Tomcat on a different operating system, see the following Web sites:

- For Eclipse <http://www.eclipse.org>
- For Tomcat <http://jakarta.apache.org/tomcat>

To get ready to develop a portal based on the sample Enterprise Service Portal:

1. Download and install Eclipse from <http://www.eclipse.org>
2. Download the Tomcat plug-in for Eclipse from <http://www.sysdeo.com/eclipse/tomcatPlugin.html>

3. Unzip the plug-in into the Eclipse installation directory.
4. Download Tomcat from <http://jakarta.apache.org/tomcat>
5. Install Tomcat:

```
mkdir $HOME/eclipse
cd $HOME/eclipse
unzip /tmp/eclipse-SDK-2.0.2-solaris-motif.zip
unzip /tmp/tomcatPluginV201.zip
cd $HOME
gzip -dc /tmp/tomcat-4.1.18.tar.gz | tar xvf -
```

6. Start Eclipse.
7. Configure the Tomcat plug-in.

Select **Window > Preferences > Tomcat**, and configure the Tomcat version and the path where you installed Tomcat.

Creating a Portal Project for a Sample-Based Enterprise Service Portal

To create a new Tomcat project inside Eclipse:

1. Select **File > New > Project > Java > Tomcat Project**, enter the name of the project, and click **Finish**.
2. Select **File > Import... > Zip File**, enter the path for *entmgr.war*, and click **Finish**.
3. Select **File > Properties > Java Build Path > Libraries > Add Jars**, open the sample Enterprise Service Portal portal project, and navigate to *WEB-INF/lib*. Select all JAR files in the *WEB-INF/lib* directory.
4. Select **File > Properties > Tomcat**, and click **Can update server.xml file**.

You can find the source code of the sample Enterprise Service Portal in the directory *WEB-INF/src*. The JSP pages are stored in the *layout* and *tiles* directories.

Building a Sample-Based Enterprise Service Portal

Eclipse automatically rebuilds the project when you save a modified source file.

To test or debug the project, you must run the code inside Tomcat.

To start Tomcat:

- Select **Tomcat > Start Tomcat**.

You can set break points in your code to debug the code.

Deploying a Sample-Based Enterprise Service Portal

To create a new Web application, set the name of the target WAR file.

1. Select **File > Properties > Tomcat**.
2. Enter the path of the target WAR file in the field WAR file for export.
3. Right-click the portal project, and select **Tomcat Project > Export to the WAR file set** in project properties.
4. Copy the WAR file to the final deployment location; for example, */opt/UMC/jboss/server/default/deploy* on your portal server.

Testing a Sample-Based Enterprise Service Portal

Purpose	Test a sample-based Enterprise Service Portal.
Action	<ol style="list-style-type: none">1. Use a virtual address for the portal See “Using a Virtual Address for the Portal” on page 307.2. Test the portal. See Configuring Simulated Router Drivers (SRC CLI).
Related Topics	■ Building a Sample-Based Enterprise Service Portal on page 306

Using a Virtual Address for the Portal

You can configure a virtual address for the portal under a common name in the Domain Name System (DNS) to specify the address through which client applications access the portal.

Part 9

Index

- Index on page 311

Index

A

account administration, Prepaid Account	
Administration application.....	113
account server, prepaid services demo.....	107
manual configuration.....	109
publishing object references.....	109
script configuration.....	109
starting.....	109
stopping.....	109
action classes in the sample residential portal.....	119
administration portal, traffic mirroring.....	19
admintool command.....	6
application protocols, managing.....	248
applications	
IDP E-Mailer.....	63
architecture	
enterprise service portal.....	199

B

bandwidth on demand. <i>See</i> BoD	
BoD (bandwidth on demand)	
services.....	161
subscriptions.....	229

C

callback interface.....	193
captive portal	
implementing.....	154
preventing access to resources.....	154
configuration level in Enterprise Manager Portal.....	220
conventions	
notice icons.....	xxv
text.....	xxv
CORBA (Common Object Request Broker Architecture)	
plug-in interface	
enterprise service portal.....	200
remote API.....	153
customer support.....	xxviii
contacting JTAC.....	xxviii

D

DCU (destination class usage).....	184
demonstration application, prepaid services.....	107
demonstration applications.....	3
deploying	
Host Check Result portal.....	36
IDP captive portal.....	84, 88
IDP E-Mailer.....	64, 70
Prepaid Account Administration application.....	109
deployment scenarios	
enterprise service portal.....	200
destination class usage.....	184
directory server	
deployment with remote SAE.....	201
DirX directory server	
deployment with remote SAE.....	201
documentation	
comments on.....	xxvii
Dynamic Service Activator, gateway extension	
example.....	63

E

enterprise	
service parameters.....	193
Enterprise Manager Portal	
application protocols, managing.....	249
BoD subscriptions.....	229
configuration level.....	220
deployment settings.....	209
firewall exception rules	
stateful firewalls.....	267
stateless firewalls.....	256
firewall subscriptions.....	254
fixed addresses for outgoing traffic.....	279
help.....	219
NAT	
IP address.....	273, 274, 275
rules for traffic.....	275
NAT Address Management Portal.....	215
NAT rules.....	275, 280
overview.....	191, 219
policies.....	161

public IP addresses, configuring	
incoming traffic.....	278
outgoing traffic.....	277
schedules.....	221, 228
services.....	161
Enterprise Service Portal audit plug-in.....	216
enterprise service portals.....	189
accessing.....	196
architecture.....	199
configuring directory connections.....	207
data, displaying.....	285
deploying.....	215
improving performance.....	193
installing.....	206
managers.....	286, 289
operators, managing.....	289
overview.....	189
performance.....	193
planning.....	202
prerequisites.....	196, 205
server description.....	199
value substitution.....	195
value substitution for policy parameters.....	195
<i>See also</i> Enterprise Manager Portal	
enterprise tag library.....	189, 191
equipment registration.....	145
description.....	119
<i>See also</i> sample residential portal	
event notification	
DHCP server.....	97
IP address manager.....	97
PCMM network.....	97
RADIUS server.....	97
events, IT manager audit.....	216
example-simple.....	180

F

files	
WEB-INF/jboss-web.xml.....	123
WEB-INF/portalBehavior.properties.....	123
WEB-INF/struts-config.xml.....	123, 125
WEB-INF/tiles-defs.xml.....	123, 128
WEB-INF/web.xml.....	123
firewall ports for sample SRC-applications.....	8
firewall services	
configuring.....	163, 166
description.....	254
managing in Enterprise Manager Portal.....	254
policies for.....	165
router support.....	161
folders for installed software.....	4
forwarding preferences.....	180, 181

H

Host Check Result portal	
deploying.....	36
example.....	36
overview.....	30
properties.....	32
HostCheckServlet for Host Check Result portal.....	30

I

IDP (Intrusion Detection and Prevention)	
integration.....	63
idpsdx.py script.....	81, 91, 92
idpsdx.sh script.....	91
integration tasks.....	49
mirroring traffic to IDP	
overview.....	45, 46
scopes.....	56
subscriber sessions.....	45, 60
policy-routing traffic to IDP	
overview.....	45, 46
scopes.....	50
services.....	52
subscriber sessions.....	45, 60
prerequisites.....	42
RecordServlet.....	81
sample implementation.....	42
services in response to incidents.....	89
Surveillance Director	
configuration.....	71
overview.....	45
<i>See also</i> IDP E-Mailer application	
IDP captive portal.....	84, 88
IDP E-Mailer application.....	63
installing	
Solaris packages.....	5
Web applications.....	6
installing software	
enterprise service portals.....	206
Instant Virtual Extranet. <i>See</i> IVE	
interfaces	
callback.....	193
interim update interval.....	108
IP address managers, event notification.....	97
IP addresses	
acknowledging release.....	292
assigning in NAT Address Management	
Portal.....	291
NAT services.....	273, 274, 275
IP Filter.....	155
IP-in-IP tunneling.....	155
ISP service in sample residential portal.....	120
IT manager	
audit plug-in	
events.....	216
operators, managing.....	286, 289

IVE (Instant Virtual Extranet) integration.....	30
HostCheckServlet.....	30
prerequisites.....	27
properties.....	32
sample implementation.....	29
services in response to compliance.....	36
<i>See also</i> Host Check Result portal	

J

Jakarta Struts Web application framework.....	119
Java development environment, Tomcat.....	156, 305
Javadoc documentation for sample residential portal.....	153
JBoss	
installing Web applications inside.....	6
removing Web applications from.....	7
JSP tag library. <i>See</i> enterprise tag library	
JUNOS routing platforms	
forwarding preferences.....	181
managing traffic.....	161
policies	
basic BoD.....	176
BOD.....	178
BoD and VPNs.....	183
firewall.....	163
NAT.....	172
provisioning services	
prerequisites	162
routing preferences.....	180
services.....	184
basic BoD.....	177
BoD.....	179
BoD and VPNs.....	184
firewall.....	163
NAT.....	172
JUNOSe routers	
policies	
basic BoD.....	176
BOD.....	178
services	
basic BoD.....	177
BoD.....	179

L

listeners, defining.....	193
--------------------------	-----

M

manuals	
comments on.....	xxvii

Monitoring Agent	
acting as pseudo RADIUS server.....	97
configuring	
properties.....	99
pseudo RADIUS agent.....	99
installing.....	99
intercepting DHCP messages.....	97
intercepting RADIUS accounting messages.....	97
monitoring.....	103
overview.....	97
stopping.....	102
multihop environment.....	155

N

NAT (Network Address Translation).....	291
rules.....	280
services for Enterprise Manager Portal.....	172
services, IP address.....	273, 275, 291
types.....	275
<i>See also</i> NAT Address Management Portal	
NAT Address Management Portal	
acknowledging IP address release.....	292
assigning IP addresses.....	291
deployment settings.....	209
Enterprise Manager Portal.....	215
overview.....	291
Network Address Translation. <i>See</i> NAT	
NIC (network information collector)	
enterprise service portals. with.....	193
notice icons.....	xxv

O

object references, publishing.....	109
------------------------------------	-----

P

packages, Solaris. <i>See</i> Solaris packages	
parameters	
acquisition path and substitutions.....	194
sample enterprise service portal.....	302
patches for Solaris.....	4
performance	
enterprise service portals.....	193
plug-ins.....	216
listeners.....	193
<i>See also</i> Enterprise Service Portal audit plug-in	
plug-ins, prepaid	109
policies	
basic BoD.....	176
BoD.....	178
BoD and VPNs.....	183
NAT.....	172
parameters.....	195
port mirroring. <i>See</i> traffic mirroring	

portals	
Host Check Result portal.....	30
IDP captive portal.....	81
Traffic Mirroring Administration.....	19
ports for sample SRC-applications.....	8
precedence	
subscriptions.....	161
Prepaid Account Administration application	
accessing.....	113
administering accounts.....	113
configuring.....	109
deploying WAR file.....	109
overview.....	107
prepaid plug-in configuration.....	109
prepaid services demonstration application	
account server.....	107
components.....	107
configuring.....	109
configuring prepaid services.....	109
installing.....	109
interim update interval.....	108
overview.....	107
SAE configuration.....	109
time-based prepaid services.....	107
volume-based prepaid services.....	108
prevention, use of unauthorized resources.....	154
privileges	
IT managers.....	189
properties for sample residential portal.....	123
proxy request management.....	155
public wireless LAN applications.....	156

R

RecordServlet for IDP captive portal.....	81
removing	
Solaris packages.....	6
Web applications.....	7
residential portal.....	117
developing.....	118
overview.....	117, 153
prerequisites for development.....	153
RADIUS authentication for login.....	122
security.....	156
routing instances.....	183
rules, NAT.....	280

S

SAE (service activation engine)	
identifying.....	190
sample applications.....	3
sample enterprise service portal	
configuring connection to directory	207
customizing.....	206
privileges.....	189

data, displaying.....	286
managing services.....	296
monitoring	
service sessions.....	300
subscriptions.....	299
networks for departments.....	301, 302, 303
overview.....	191
service parameters.....	299, 300
sample residential portal	
action classes.....	119
behaviors.....	120
customizing.....	130
developing portal based on the sample.....	156, 305
development tools.....	153
equipment registration.....	120, 145
installing.....	129
login.....	133
model components.....	119
overview.....	133, 153
personal digital assistant (PDA).....	150
prerequisites.....	129
schedules.....	140
service activation.....	137
services	
management.....	136
schedules.....	140
subscriptions.....	145
usage	
information.....	137
view components.....	119
Web application framework.....	119
scripts	
idpsdx.py.....	81, 91, 92
idpsdx.sh.....	91
sending traffic to VPNs.....	247
service activation.....	193
service parameters, enterprise.....	193
service schedules	
Enterprise Manager Portal, in.....	221
service schedules, sample residential portal.....	142
services.....	254
basic BoD.....	177
BoD.....	179, 229
configuring prepaid.....	109
JUNOS routing platforms.....	184
BoD and VPNs.....	184
NAT.....	172
sample enterprise service portal, managing.....	296
time-based.....	107
volume-based.....	108
<i>See also</i> firewall services	
single-hop environment.....	155
Solaris packages	
installing.....	4, 5
removing.....	6
UMCpdemo.....	107

Solaris patches.....4
 source class usage (SCU).....184
 SRC single-hop requirement.....155
 subscribers
 billing.....184
 subscriptions
 enterprise hierarchy.....196
 priority.....161
 sample enterprise service portal, creating.....296
 substitutions
 parameter acquisition path.....194
 use.....195
 support, technical *See* technical support
 Surveillance Director configuration.....80
 swmtool command.....6

T

technical support
 contacting JTAC.....xxviii
 text conventions defined.....xxv
 Tomcat, as Java development environment.....156, 305
 traffic mirroring
 administration portal.....19
 mirroring tasks
 managing.....19
 starting.....19

U

UMCppdemo Solaris package.....107
 uninstalling. *See* removing

V

value substitution.....195
 virtual portal address.....154
 virtual private networks. *See* VPNs
 VPNs (virtual private networks)
 directory.....244
 identifiers.....183
 modifying.....244
 VPN to which router sends traffic.....247
 sending traffic.....247
 stopping router from sending traffic.....248

W

WAR files.....7
 Web Admin applications.....107
 Web applications
 installing.....6
 removing.....7
 WEB-INF/jboss-web.xml.....123
 WEB-INF/portalBehavior.properties.....123
 WEB-INF/struts-config.xml.....123, 125

WEB-INF/tiles-defs.xml.....123, 128
 WEB-INF/web.xml.....123

