

JUNIPER NETWORKS STRM TECHNICAL NOTE

OPEN PORTS USED BY STRM

FEBRUARY 2008

This document provides information about the ports used by and between STRM components.

[Table 1](#) lists the common ports used by STRM components, identifies the signaling direction for that port, and provides the reason for using the port.



Note: *The ports listed in this document are valid only when IPtables is enabled on your STRM system.*

Table 1 List of Common Ports Used by STRM Components

Port	Direction	Reason
TCP 22 - SSH	STRM Console to all other components	<ul style="list-style-type: none">• Remote management access• Adding a remote system as a managed host• Retrieving log files• End-user desktops to the QRadar Console
TCP 25 - SMTP	From all managed hosts to your SMTP gateway	<ul style="list-style-type: none">• E-mail to an SMTP gateway• Error/warning e-mail messages to an administrative e-mail contact
UDP/TCP 37 - Rdate (time)	<ul style="list-style-type: none">• All systems to the STRM Console• STRM Console to the NTP or RDATA server	To keep time synchronized, especially on QFlow Collectors
TCP 80 - Apache/https	<ul style="list-style-type: none">• End users to the STRM Console• End users to the STRM Deployment Editor	<ul style="list-style-type: none">• Administration Console component downloads from the STRM Console to end-user desktops• Deployment Editor component downloads from the STRM Console to end-user desktops

Table 1 List of Common Ports Used by STRM Components (continued)

Port	Direction	Reason
TCP 443 - Apache/https	<ul style="list-style-type: none"> STRM managed hosts connecting to the STRM Console End users connecting to the STRM Console 	<ul style="list-style-type: none"> Configuration downloads to STRM managed hosts from the STRM Console Access to the STRM user interface for end users
UDP 514 - Syslog	External event sources to STRM Event Collectors	Event data feeds from STRM components
TCP 5432 - Postgres	From all remote managed hosts running Event Collector/Event Processor to the STRM Console.	When provisioning managed hosts using the Administration Console
TCP 10000 - Remote Server management (Web-Based System Administration Interface)	End-user desktop to all STRM hosts	Server changes, such as root password and firewalls
TCP 7676, 7677 - Messaging connections (imq)	<ul style="list-style-type: none"> All STRM managed hosts to the STRM Console The STRM Console to all STRM managed hosts 	Configuration data changes are sent back and forth between the STRM Console and managed hosts
TCP 32000-33999 - Data flow (flows, events, flow context)	Bi-directional between STRM components	Data flows, such as events, flows, flow context, and event search queries
UDP 2055, 9995	From the management interface on the flow source (typically a router) to the Flow Collector	NetFlow datagram from components, such as routers

All the ports listed in [Table 1](#) can be tunneled, by encryption, through port 22 over SSH.

Juniper Networks, Inc.
 1194 North Mathilda Avenue
 Sunnyvale, CA 94089 USA

Copyright © 2008 Juniper Networks, Inc. All rights reserved. Juniper Networks and the Juniper Networks logo are registered trademarks of Juniper Networks Inc. in the United States and other countries. All other trademarks, service marks, registered trademarks, or registered service marks in this document are the property of Juniper Networks or their respective owners. All specifications are subject to change without notice. Juniper Networks assumes no responsibility for any inaccuracies in this document or for any obligation to update information in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

Part Number 530-023924-01