

SNYPR 6.1

Data Source Guide

Juniper Netscreen Remote HVD VPN

Securonix Proprietary Statement

This material constitutes proprietary and trade secret information of Securonix, and shall not be disclosed to any third party, nor used by the recipient except under the terms and conditions prescribed by Securonix.

The trademarks, service marks, and logos of Securonix and others used herein are the property of Securonix or their respective owners.

Securonix Copyright Statement

This material is also protected by Federal Copyright Law and is not to be copied or reproduced in any form, using any medium, without the prior written authorization of Securonix.

However, Securonix allows the printing of the Adobe Acrobat PDF files for the purposes of client training and reference.

Information in this document is subject to change without notice. The software described in this document is furnished under a license agreement or nondisclosure agreement. The software may be used or copied only in accordance with the terms of those agreements. Nothing herein should be construed as constituting an additional warranty. Securonix shall not be liable for technical or editorial errors or omissions contained herein. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or any means electronic or mechanical, including photocopying and recording for any purpose other than the purchaser's internal use without the written permission of Securonix.

Copyright 2018 © Securonix All rights reserved.

Contact Information

Securonix, Inc.

14665 Midway Rd. Ste. 100, Addison, TX 75001

www.securonix.com

855.732.6649

Revision History

Date	Product Version	Description
3/13/2018	6.1	Revision

Copyright © 2018 Securonix, Inc.

Table of Contents

2

Juniper Netscreen Remote HVN VPN **4**

What is Juniper Netscreen Remote HVN VPN? 4

Supported Collection Methods 4

Taxonomy 4

Device Event Field Mapping 4

Device Event Categorization 6

Sample Line Filters 6

References 7

Copyright © 2018 Securonix, Inc.

Juniper Netscreen Remote HVN VPN

This data source guide provides information about how the Juniper Netscreen Remote HVN VPN data source events are parsed, normalized and categorized to SNYPR fields. In particular, it provides the following:

- Device event field mapping
- Device event severity mapping
- Device event categorization

To download the Juniper Netscreen Remote HVN VPN parser from the Securonix Threat Library, search Available Resources Types for Deployment by Vendor name or Functionality. Downloading the resource downloads the parser along with the applicable dashboards, reports, policies and threat models.

What is Juniper Netscreen Remote HVN VPN?

Juniper Netscreen Remote is a product of Juniper Networks. Juniper Netscreen Remote is a remote VPN connections client software for ScreenOS and SRX devices.

Supported Collection Methods

The method of collection is syslog.

Taxonomy

Securonix Open Event Format (OEF) 1.0 is used. OEF is an event interoperability standard/schema. It provides a set of standardized attributes (fields) for consistent representation of logging output from disparate security and non-security devices and applications. For additional information, refer to the Data Dictionary section on the Securonix documentation portal.

Device Event Field Mapping

This section lists the mappings of the device to SNYPR fields.

Juniper Netscreen Remote HVN VPN Field	SNYPR Field
Device ID	additionaldetails1
Severity Level	deviceseverity
Type ID	flowsiemid
duration	customnumber2
Service	transportprotocol
Protocol Number	additionaldetails2
Action	deviceaction

Copyright © 2018 Securonix, Inc.

Juniper Netscreen Remote HVN VPN Field	SNYPR Field
Sent	bytesout
Source IP	sourceaddress
Destination IP	destinationaddress
Source Port	sourceport
Destination Port	destinationport
Session ID	sessionid
Received	bytesin
ICMP Type	customnumber1
Outcome	eventoutcome
End Time	endtime
User	accountname
Context	requestcontext
Server IP	requestcontext
Server IP	deviceaddress
Start Time	DATETIME
Policy ID	baseeventid
Event Category	deviceeventcategory
Src Zone	devicecustomstring4
Dest Zone	devicecustomstring5
Error Type	devicecustomstring2
Reason	devicecustomstring1
Src-xlated IP	additionaldetails3
dst-xlated IP	additionaldetails4

This table maps device severity fields to the SNYPR category severity fields.

Device Severity	SNYPR Category Severity
Very High=0,1;	alert

Copyright © 2018 Securonix, Inc.

Device Severity	SNYPR Category Severity
High=2.3;	critical
Medium=4,5;	warning
low-6,7	info

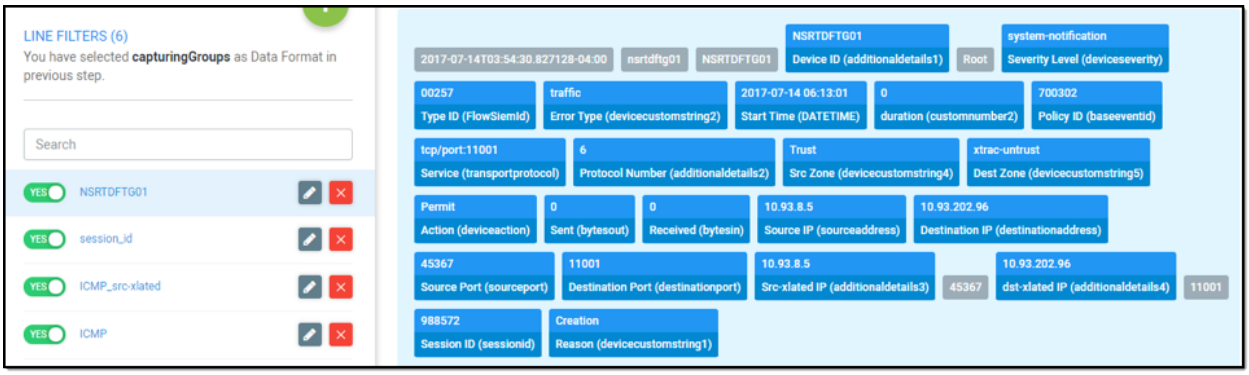
Device Event Categorization

This section contains the rules used to categorize the device events.

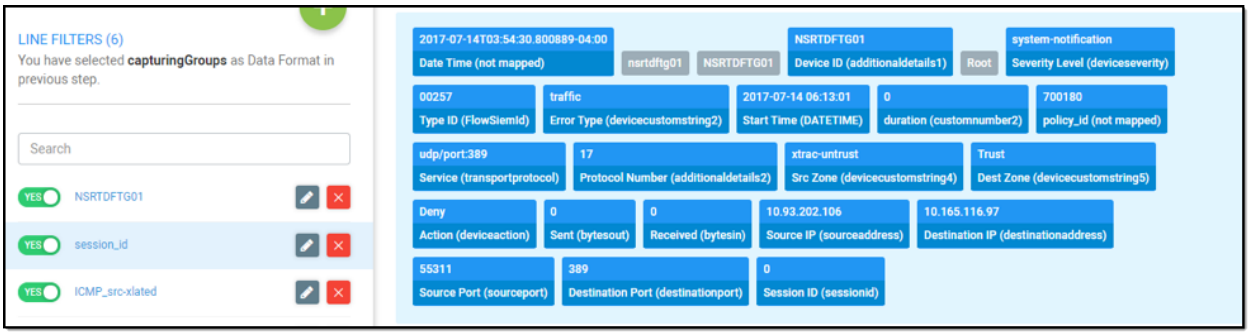
Rule	Category Object	Category Behavior	Category Outcome
Action equal to permit	Device	Authentication	Allow
Action equal to Deny	Device	Authentication	Block

Sample Line Filters

Sample 1

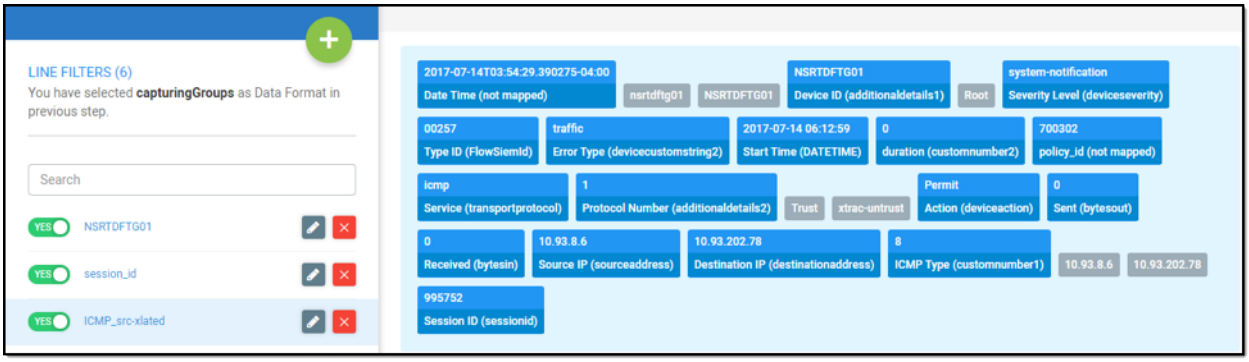


Sample 2



Copyright © 2018 Securonix, Inc.

Sample 3



References

Copyright © 2018 Securonix, Inc.