



INTEGRATING SNS LOGS IN IBM QRADAR

Product concerned: SNS 3.7.x and higher, SNS 4.x Document last update: December 23, 2020 Reference: sns-en-integrating_SNS_logs_in_IBM_QRadar_technical_note





Table of contents

Getting started	3
About this document	3
Requirements and compatibility	3
Installing the SNS extension in IBM QRadar	4
Downloading the DSM	4
Importing the DSM into QRadar	4
Configuring the log source	5
Adapting the size of syslog UDP messages in QRadar	6
Changing the payload size of syslog messages in QRadar	7
Configuring the SNS firewall to send logs to IBM QRadar	8
Using QRadar with the SNS DSM	9
Support1	10



Getting started

Of all the cybersecurity components that can be deployed to secure a network, Stormshield's SNS firewalls and IBM's Security QRadar come together to ensure that security operations center (SOC) analysts and administrators can fully trust the defenses that are implemented and obtain relevant information about events occurring on their networks.

As a cybersecurity vendor, Stormshield has protected organizations that host critical and highly sensitive infrastructures for the past 20 years with its firewall range. Thanks to Stormshield firewalls, administrators are able to secure their networks, monitor the nature of data that their users share, and encrypt data through IPSec VPN tunnels. As for all the routine events that take place every day, Stormshield firewalls generate logs that keep administrators informed as soon as events occur on the network. Stormshield SNS firewalls' ability to organize and categorize logs gives administrators a deeper understanding of what their firewalls process.

IBM's Security QRadar Device Support Module (DSM) offers administrators and SOCs the possibility of integrating SNS firewall logs into IBM Security QRadar so that they can obtain relevant information in their security information and event management (SIEM) solution. With this combination, security teams can analyze network behavior in real time and detect threats that target their organization.

The IBM Security Qradar DSM for Stormshield firewalls makes it possible to analyze the following log categories:

- Authentication,
- Firewall,
- Intrusion prevention (IPS),
- Threat management (UTM),
- Sandboxing,
- System events,
- Alarms.

About this document

IBM QRadar is a security information and event management (SIEM) solution that enables the real-time analysis of security alerts generated by network-based applications and solutions.

This document explains how to integrate the Stormshield Network Security DSM into IBM QRadar.

Requirements and compatibility

- SNS DSM version: 1.0.0 (published: October 2020),
- IBM QRadar 7.3.2 and higher,
- SNS 3.7 and higher.



Installing the SNS extension in IBM QRadar

To install the extension:

- Download the Stormshield Network Security DSM from the IBM application store,
- Import the DSM into QRadar,
- Configure a log source that accepts and maps syslog messages from the SNS firewall to the DSM.

Downloading the DSM

- 1. Log in to your IBM QRadar console.
- 2. In the Admin menu, select Extensions Management:

Admin								0
 System Configuration 	Checking for undeploye	ed changes						
 Data Sources 	System Configuration							
Remote Networks and Services Configuration			1	<u>а</u>	C.	a ¹⁰	<u>w</u>	
Try it out	Auto Update	Backup and Recovery	Global System Notifications	Index Management	Aggregated Data Management	Network Hierarchy	System and License Management	
► Apps	M	\$	물모	ul,	2.	(1)	9	
	System Health	System Settings	Asset Profiler Configuration	Custom Offense Close Reasons	Store and Forward	Reference Set Management	Centralized Credentials	
		1		*	6			
	Forwarding Destinations	Routing Rules	Domain Management	Extensions Management	Resource Restrictions			

3. Click on IBM Security App Exchange.

Your browser will open the page https://exchange.xforce.ibmcloud.com/hub/ (IBM ID required).

Extensions Management		IBM Se	curity App Exchange
Search by extension name Q			
ALL ITEMS INSTALLED NOT INSTALLED			Add
Name	Status	Author	Added On 👻

4. Download the "Stormshield Network Security" DSM.

Importing the DSM into QRadar

In your IBM QRadar console:



1. Go to Admin > Extensions Management.

2. Click on Add a New Extension:

Extensions Management Search by extension name Q	IBM Security /	App Exchange
Add a New Extension From local storage:	uthor	Add Added ~ On
Install immediately Add Cancel		

- 3. Select the zip archive downloaded earlier (Stormshield Network Security DSM v1.0.0.zip).
- 4. Click on **Add** to install the extension:

-		Status	Author	Added On
Stormshield Network Security Among cyber security items deployed to secure the network firewalls and IBM Security QPAdat helps administrators and helps of defines and to get competentive information in helps of the security of the security of the security companies with highly citical and sensitive infrastructures. Stormshield SNS firewalls could cogs in order to be abler network. Stormshield SNS firewalls capabilities to organize administrators are done the networks control the data with encrypt data through VPM tunnels. For all these events with stormshield SNS firewalls could cogs in order to be abler network. Stormshield SNS firewalls capabilities to organize diministrators to go deep and in details into the lirewalls and DSM, administrators and SOCs are able to get Stormshield Chadar in order to get comprehensive data in their SIEM st teams are able to analyze the network behaviors and to deil ompany in neal time. IBM Security GRadar DSM for Storm log categories: authentications, firewall, IPS, UTM, sandbox	x t; the combination of Stormshield SNS (SOC analysts to get contributed SNS (SOC analysts to get contributed SNS (SOC analysts of the second that has happend in their networks, that has to transit between users, and the occur everyday and all day long, to show any time what is going on in the and to categorize the logs allow (NIII) (SNS (Timevalls) (SOC Anadar SNS (Travalls) logs into IBM Security ultime. Thanks to IBM Security Unition. With this parse the following theid SNS Tirewalls parse the following inig and system events and alarms.	Installed	Stormshield	20 October 2020
Uninstal Contents: 	Installed By: admin 20 October 2020 Version: 9 Supported Languages: en_US Signed:			

Configuring the log source

SNS firewalls send their logs to IBM QRadar over the syslog protocol.

- 1. Log in to your IBM QRadar console.
- 2. In the Admin menu, select Log Source.
- 3. Click on Add.
- 4. Fill in the form to create the Log Source:
- Log Source Name field: enter a name for your new log source (e.g.: Stormshield SNS device).
- Log Source description field: enter a description of your new log source.
- Protocol Configuration field: select Syslog.



- Log Source Identifier field: enter the host name of your SNS firewall. If no host name has been defined on your firewall, enter its serial number (e.g.: *VMSNSX0000000A1*).
- Log Source Extension field: selectStormshieldNeworkSecurityCustom ext.

og Source Name Stormshield SNS devij og Source Description Stormshield Network Security og Source Type Stormshield Network Security rotocol Configuration Syslog og Source Identifier SNS hostname nabled Image Source Collector redibility 5 < oalescing Events Image Source Type coming Payload Encoding UTF-8 og Source Extension Stormshield Network SecurityCustom_ext		
bg Source Description StormshieldNetworkSe bg Source Type StormshieldNetworkSecurity rotocol Configuration Syslog bg Source Identifier SNShostname nabled Image Source Identifier redibility 5 arget Event Collector Image Source Identifier coming Payload Encoding UTF-8 utore Event Payload StormshieldNetworkSecurityCustom_ext bg Source Extension StormshieldNetworkSecurityCustom_ext	og Source Name	Stormshield SNS devi
og Source Type Stormshield Network Security rotocol Configuration Syslog og Source Identifier SNShostname nabled Image: Support of the security redibility 5 arget Event Collector eventcollector0 :: ip-10-0-1-25 oalescing Events Image: Support of the security Custom of the securit	og Source Description	StormshieldNetworkSt
votocol Configuration Syslog og Source Identifier SNShostname nabled Image: Sinshostname redibility 5 < arget Event Collector eventcollector0 :: ip-10-0-1-25 oalescing Events Image: Sinshostname coming Payload Encoding Image: Image: SinshieldNetworkSecurityCustom_ext og Source Extension StormshieldNetworkSecurityCustom_ext	og Source Type	Stormshield Network Security
og Source Identifier SNShostname nabled Image: SNShostname redibility S arget Event Collector eventcollector0:::ip-10-0-1-25 oalescing Events Image: SNShostname ocoming Payload Encoding UTF-8 tore Event Payload StormshieldNetworkSecurityCustom_ext og Source Extension StormshieldNetworkSecurityCustom_ext	rotocol Configuration	Syslog 🗸
inabled Image: Constrained in the second	og Source Identifier	SNShostname
Stredibility 5 arget Event Collector eventcollector0::: ip-10-0-1-25 coalescing Events I coalescing Events I coalescing Payload Encoding UTF-8 ctore Event Payload I cog Source Extension StormshieldNetworkSecurityCustom_ext ease select any groups you would like this log source to be a member of:	nabled	
arget Event Collector eventcollector0:::ip-10-0-1-25 v coalescing Events Import to the second to the se	redibility	5 🗸
Coalescing Events Image: Coalescing Events Incoming Payload Encoding UTF-8 Store Event Payload Image: Coalescing Events Image: Coalescing Events Image: Coalescing Events Store Event Payload Image: Coalescing Events Image: Coalescing Events StormshieldNetworkSecurityCustom_ext Image: Coalescing Events StormshieldNetworkSecurityCustom_ext Image: Coalescing Events StormshieldNetwork to be a member of:	arget Event Collector	eventcollector0 :: ip-10-0-1-25 🗸
ncoming Payload Encoding UTF-8 Store Event Payload Image: Comparison of the store state sta	oalescing Events	
Store Event Payload Image: Comparison StormshieldNetworkSecurityCustom_ext lease select any groups you would like this log source to be a member of:	coming Payload Encoding	UTF-8 🗸
Log Source Extension StormshieldNetworkSecurityCustom_ext lease select any groups you would like this log source to be a member of:	tore Event Payload	
lease select any groups you would like this log source to be a member of:	og Source Extension	StormshieldNetworkSecurityCustom_ext ~
	ease select any groups you would li	ike this log source to be a member of:

5. Click on Save.

Adapting the size of syslog UDP messages in QRadar

QRadar uses a default payload size of 1024 bytes for syslog UDP messages. When a message exceeds this size, it will be automatically truncated.

Incidentally, some of the events that SNS firewalls send exceed this size. Since the log type is placed at the end of the line, QRadar will not be able to extract the corresponding event category, and treat these messages as unknown.

The size of syslog UDP messages that IBM QRadar accepts must therefore be changed. Increasing the limit to 2048 bytes will sufficiently cover all types of messages that the firewall may send.



Changing the payload size of syslog messages in QRadar

- 1. Log in to your IBM QRadar console.
- 2. In the Admin menu, select System settings:



3. Switch the system settings panel from Basic to Advanced mode.

4. In the Max UDP Syslog Payload Length field, enter 2048:

System Settings		0	
System Settings	Max UDP Syslog Payload Length	1024	
Database Settings	Max TCP Syslog Payload Length	4,096	
Database Settings	Max Number of TCP Syslog Connections	2,500	
Ariel Database Settings	Max TCP Syslog Connections Per Host	10	
Custom Rule Settings	Timeout for Idle TCP Syslog Connections (seconds)	900	
Transaction Sentry Settings	Log and Network Activity Data Export Temporary Directory	/store/exports	
	Display Country/Region Flags	Yes 👻	
SNMP Settings	Display Embedded Maps in IP Address Tooltips	Yes 👻	
Embedded SNMP Daemon	Enable X-Force Threat Intelligence Feed	No 👻	
Accet Profile Settinge	Lag time to remove expired reference data (minutes)	5 🔺	

5. Click on **Save** to save your changes.



Configuring the SNS firewall to send logs to IBM QRadar

- 1. Log in to the web administration interface of your SNS firewall.
- 2. Go to Configuration > Notifications > Logs Syslog IPFIX > SYSLOG tab.
- 3. Edit one of the four available SYSLOG profiles.
- 4. Name field: enter a custom name for this profile.
- 5. Syslog server field: select or create a network object representing the IBM QRadar machine.
- 6. Protocol field: select UDP.
- 7. Port field: select syslog.
- 8. Format field: select RFC5424.
- 9. In Advanced properties > Logs enabled, select the log categories to be sent to IBM QRadar.
- 10. Click on Apply.
- 11. Double-click in a profile's Status cell to enable it.

Network Security	MONITORING CONFIGURAT	ION EVAU VMSNSX08K0014A9	
*- «			
CONFIGURATION -	I NOTIFICATIONS/ LOGS- STSI		
Search 💉 🖉	LOCAL STORAGE SYSLOG	IPFIX	
+种 SYSTEM	SYSLOG PROFILES	Details	
NETWORK	Status Name	D C CANO	
S OR LECTS	C Enabled QRADAR 732	Name:	QRADAR 732
	C Disabled	Comments:	
a USERS	C Disabled	Syslog server:	ip-10-0-1-25 💌 🕏
* SECURITY POLICY	C Disabled	Protocol:	UDP 💌
APPLICATION PROTECTION		Port:	syslog 👻 🕏
CO VPN			syslog-ca 👻 🗙
NOTIFICATIONS			syslog.qradar 👻 🗙
Logs - Syslog - IPFIX			* X
SNMP Agent		Format:	RFC5424 *
E-mail alerts		 Advanced properties 	
Evistem events			v 85
System events			syslog 👻 🛼
Block messages		Category (facility):	none
Report configuration			
Monitoring configuration		Enable all Disable all	
		Status Name	
		Enabled Alarms	
		 Enabled Network connections 	
		Enabled Filter policy	
		Enabled HTTP proxy	
		Enabled SMTP proxy	

The installation is complete - the SNS firewall's logs will be redirected to the IBM QRadar platform.

Using QRadar with the SNS DSM

- 1. Log in to your IBM QRadar console.
- 2. In the Log Activity menu, click on New Search.
- 3. Fill in the various fields of the search form:
- Parameter field: select Log Source Type,
- Operator field: select Equals,
- Value field: select Stormshield Network Security.
- 4. Confirm by clicking on Add Filter.
- 5. Click on **Search**. Stormshield logs will appear in the grid.

E IBM QRadar										¢.
ashboard Offenses Log Activity Network Activi	ty Assets Reports	Admin								System Time: 1-
earch 🔻 Quick Searches 🔻 🍟 Add Filter 🕌 Save Criteria	🕼 Save Results 🔗 Cancel 🤸	False Positive	Rules ¥ Actions ¥							
Quick Filter *										Search
	Viewi	ng real time	events View: Select Ar	Option: * Display: De	fault (Normalized)					
urrent Filters: Log Source Type is Stormshield Network Security	(Clear Filter)									
Event Name	Log Source	Event	Time	Low Level Category	Source IP	Source	Destination IP	Destination	Username	Magnitude
Firewall Permit	Stormshield SNS device	1	20 Oct 2020, 14:53:33	Firewall Permit	10.0.100.2	37031	10.0.0.9	636	Jack	
System Informational	Stormshield SNS device	1	20 Oct 2020, 14:53:32	System Informational	10.0.100.1	0	10.0.1.110	0	N/A	
Firewall Permit	Stormshield SNS device	1	20 Oct 2020, 14:53:30	Firewall Permit	10.0.100.14	36364		443	Jessica	
Firewall Permit	Stormshield SNS device	1	20 Oct 2020, 14:53:19	Firewall Permit		59124	10.0.1.25	443	N/A	
Firewall Permit	Stormshield SNS device	1	20 Oct 2020, 14:53:28	Firewall Permit	10.0.100.9	23871	10.0.0.8	443	James	
Firewall Permit	Stormshield SNS device	1	20 Oct 2020, 14:53:27	Firewall Permit		37503	10.0.0.1	25	and the second second	
Firewall Permit	Stormshield SNS device	1	20 Oct 2020, 14:53:26	Firewall Permit	10.0.1.9	58506		443	N/A	
Firewall Denv	Stormshield SNS device	1	20 Oct 2020 14:53:23	Eirewall Dervy	10.0.100.16	32615	-des	80	Isla	
Eirowall Parmit	Stormshield SNS device		20 Oct 2020, 14:53:21	Eirawall Darmit	10.0.100.5	36429		442	Charlia	
Eiraual Darmit	Stormobiold SNS doulog		20 Oct 2020, 14:53:20	Eirowall Dormit	10.0.100.1	26690	10.0.0.7	440	Oliver	
Firewall Permit	Stormshield SNS device		20 Oct 2020, 14:53:20	Firewall Permit	10.0.100.1	50000	10.0.0.7	993	NI/A	
View Detected And Disclord	Otermakiald CNC device		20 Oct 2020, 14-53-07	Minus Datastad	10.0.100.10	05120	100.0.07	22	IN/A	
Virus Detected And Blocked	Stormshield SNS device		20 Oct 2020, 14:53:16	Virus Detected	10.0.100.16	21343	192.168.100.1	00	ISIB	
Firewall Permit	Stormshield SNS device	2	20 Oct 2020, 14:53:05	Firewall Permit	10.0.100.10	50693	10.0.1.25	443	DVA OF 1	
Firewall Permit	Stormshield SNS device	1	20 Oct 2020, 14:53:10	Firewall Permit	10.0.100.12	38897	192.168.13.4	102	Olivia	
Firewait Permit	Stormshield SNS device	1	20 Oct 2020, 14:53:07	Firewall Permit	10.0.100.18	28512	10.0.0.9	636	Isabella	a la companya da companya d
Authentication success on the firewall via SSH	Stormshield SNS device	1	20 Oct 2020, 14:53:06	SSH Login Succeeded		0	0.0.0.0	0	N/A	
IPS Deny	Stormshield SNS device	1	20 Oct 2020, 14:53:06	IPS Deny	192.168.11.1	37887	192.168.13.1	502	N/A	
Firewall Permit	Stormshield Sivs device		20 Oct 2020, 14:52:53	Firewall Permit	10.0.100.11	50049	10.0.1.9	993	IN/A	
Firewail Permit	Stormshield SNS device	1	20 Oct 2020, 14:53:04	Firewall Permit	10.0.100.11	24302		80	Amelia	
Firewall Permit	Stormshield SNS device	1	20 Oct 2020, 14:52:54	Firewall Permit	10.0.1.9	43148		443	N/A	
Sandboxing malicious	Stormshield SNS device	1	20 Oct 2020, 14:53:02	Malicious Software	10.0.100.5	26663		80	Charlie	
Firewall Permit	Stormshield SNS device	1	20 Oct 2020, 14:52:52	Firewall Permit	10.0.1.9	59182	-	443	N/A	
System Informational	Stormshield SNS device	3	20 Oct 2020, 14:52:51	System Informational		0	10.0.1.110	0	admin	
Firewall Permit	Stormshield SNS device	1	20 Oct 2020, 14:53:01	Firewall Permit	10.0.100.5	39058		80	Charlie	
Sandboxing malicious	Stormshield SNS device	1	20 Oct 2020, 14:52:59	Malicious Software	10.0.100.1	27372		80	Oliver	
Firewall Permit	Stormshield SNS device	1	20 Oct 2020, 14:52:57	Firewall Permit	10.0.100.15	35660	10.0.0.11	445	Ava	
Sandboxing malicious	Stormshield SNS device	1	20 Oct 2020, 14:52:55	Malicious Software	10.0.100.18	21853		80	Isabella	
Firewall Permit	Stormshield SNS device	1	20 Oct 2020, 14:52:44	Firewall Permit		59052	10.0.0.37	22	N/A	
Firewall Permit	Stormshield SNS device	1	20 Oct 2020, 14:52:54	Firewall Permit	10.0.1.9	41994		443	N/A	
Firewall Permit	Stormshield SNS device	2	20 Oct 2020, 14:52:33	Firewall Permit		59123	10.0.1.25	443	N/A	
Firewall Permit	Stormshield SNS device	2	20 Oct 2020, 14:52:26	Firewall Permit		59107	10.0.1.9	443	N/A	
Firewall Permit	Stormshield SNS device	5	20 Oct 2020, 14:52:22	Firewall Permit		59103	10.0.1.25	443	N/A	
	Control do theo	0	00.0.100000.11.50.00	Eireunell Dermit	10.0.1.0	63567		63	NI/A	
Firewall Permit	Stormshield SNS device		20 0012020 14/52/20	P IT IT MARKED P ITT ITTI	112.12.1.77					

🚺 NOTE:

There are two limitations in version 1.0.0 of the SNS DSM:

- IPv6 values are not taken into account.
- Only standard QRadar fields are used; custom properties to filter by vendor-specific values are not available.

The Stormshield DSM provides the values of the following QRadar standard properties:

- DestinationIp,
- DestinationMAC,
- DestinationPort,
- DestinationIpPreNAT,
- DestinationPortPreNAT,
- DeviceTime,
- EventCategory,
- Protocol,
- Sourcelp,

- SourceMAC,
- SourcePort,
- SourcelpPostNAT,
- SourcePortPostNAT,
- UserName.

Following events are categorised by QRadar:

- Connections Pass or Block,
 - Firewall and proxies,
 - Filter policy,
 - Alarms (IPS Permit or Deny),
- Proxies,
 - Virus detection,
 - Sandboxing detection,
- Authentication errors,
- System events.

Support

If you encounter issues while installing or using the Stormshield Network Security DSM on the IBM QRadar platform, feel free to get in touch with **Stormshield technical support**.

documentation@stormshield.eu

All images in this document are for representational purposes only, actual products may differ.

Copyright © Stormshield 2020. All rights reserved. All other company and product names contained in this document are trademarks or registered trademarks of their respective companies.