TECHNICAL NOTE
STORMSHIELD NETWORK SECURITY

# 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

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.

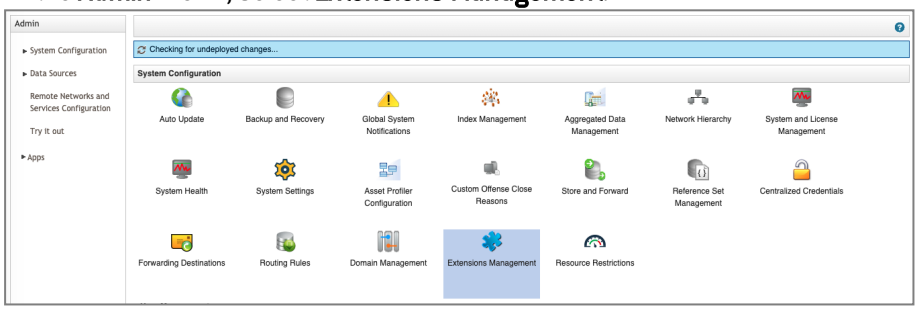
# Installing the SNS extension in IBM QRadar

To install the extension:

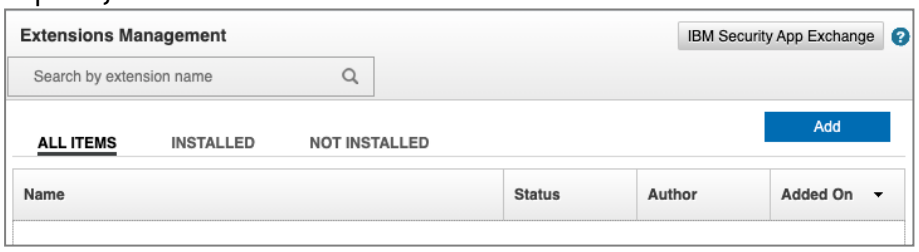
- Download the Stormshield Network Security DSM from the IBM application store,
- Import the DSM into QRadar,
- Configure a log source that accepts and maps syslog messages from the SNS firewall to the DSM.

## Downloading the DSM

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




3. Click on **IBM Security App Exchange**.
   Your browser will open the page https://exchange.xforce.ibmcloud.com/hub/ (IBM ID required).

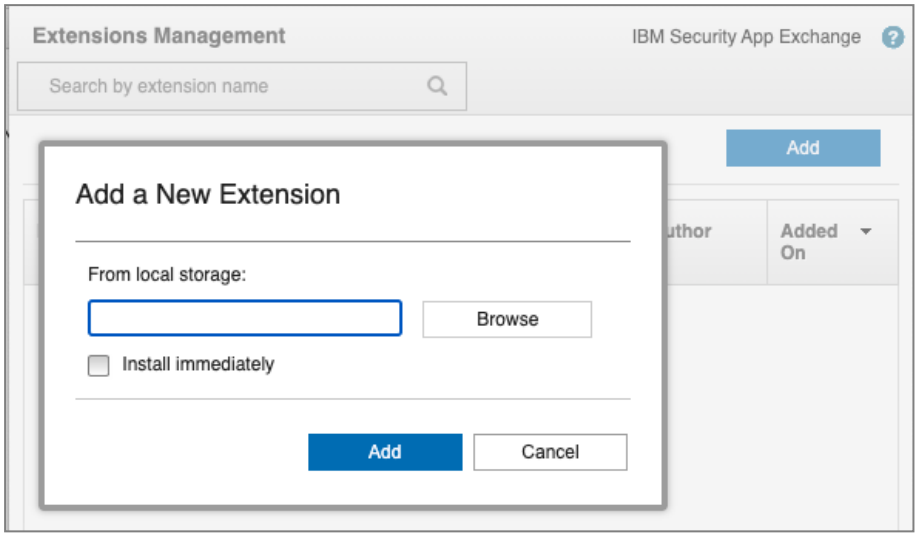



4. Download the "Stormshield Network Security" DSM.

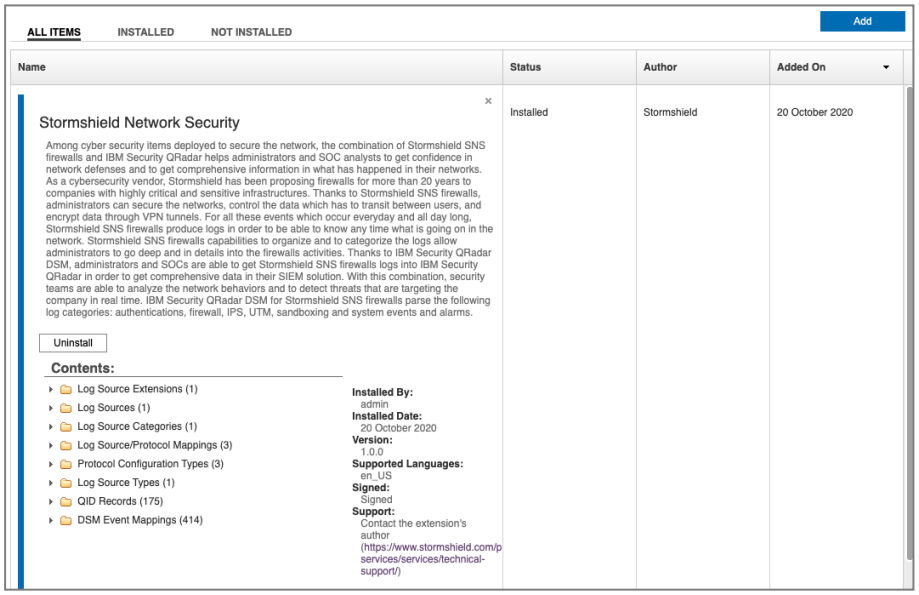
## Importing the DSM into QRadar

In your IBM QRadar console:

1. Go to **Admin** > **Extensions Management.**
2. Click on **Add a New Extension:**




3. Select the zip archive downloaded earlier (Stormshield_Network_Security_DSM_v1.0.0.zip).
4. Click on **Add** to install the extension:



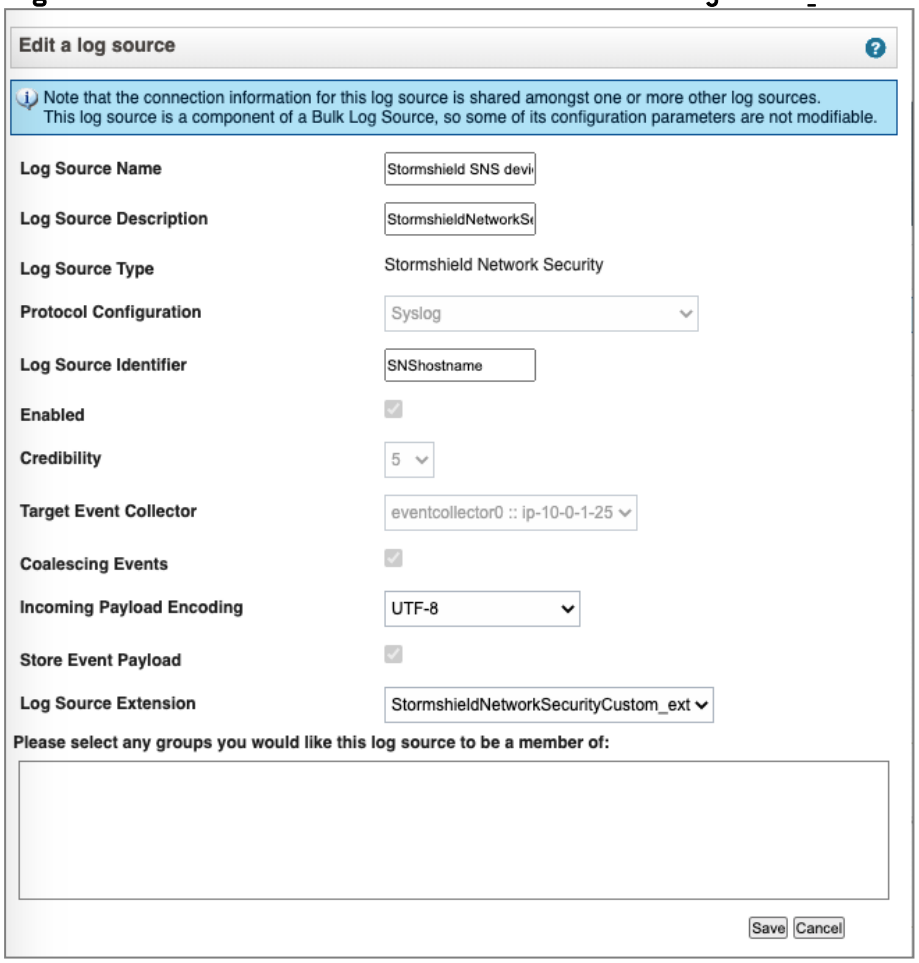

## Configuring the log source

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: select **StormshieldNeworkSecurityCustom_ext.**




5. Click on **Save**.

## Adapting the size of *syslog* UDP messages in QRadar

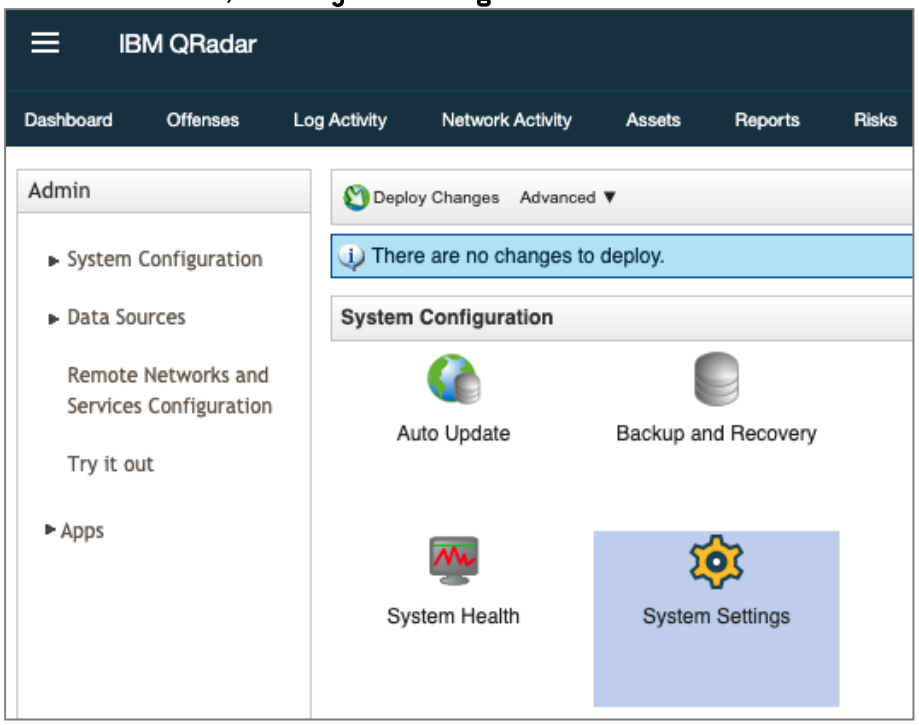
QRadar uses a default payload size of 1024 bytes for syslog UDP messages.
When a message exceeds this size, it will be automatically truncated.

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.

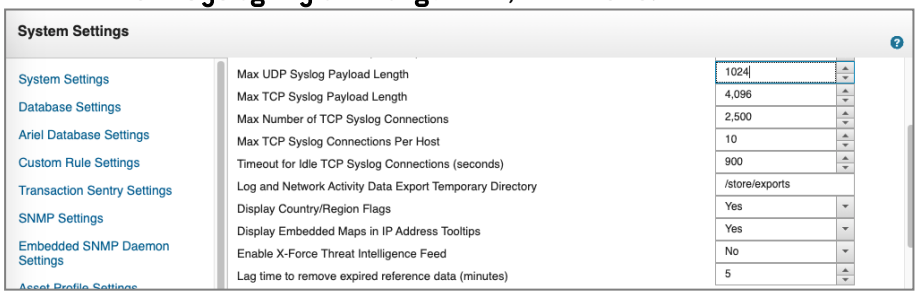
The size of syslog UDP messages that IBM QRadar accepts must therefore be changed. Increasing the limit to 2048 bytes will sufficiently cover all types of messages that the firewall may send.

## 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:**



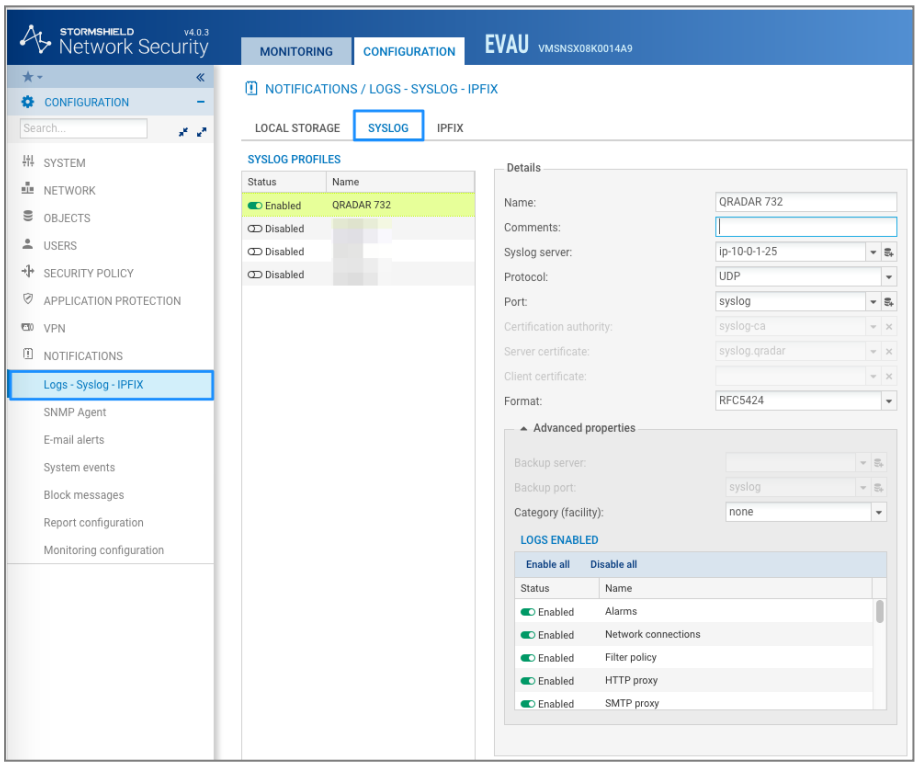

3. Switch the system settings panel from **Basic** to **Advanced** mode.
4. In the **Max UDP Syslog Payload Length** field, enter **2048:**




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.



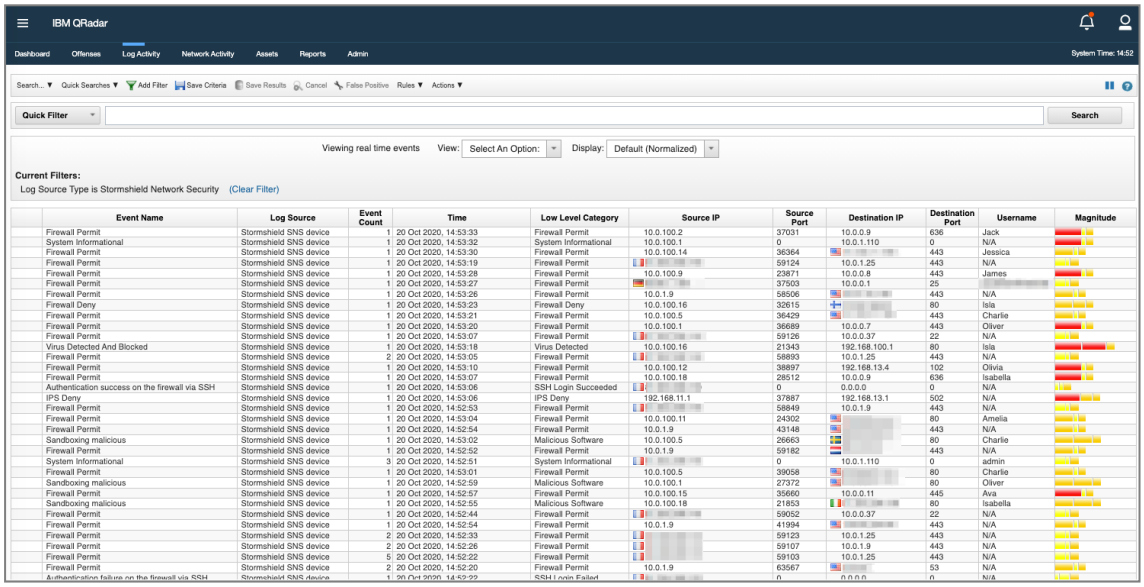

The installation is complete – the SNS firewall's logs will be redirected to the IBM QRadar platform.

# 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.




**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,
- SourceIp,

- SourceMAC,
- SourcePort,
- SourceIpPostNAT,
- 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.

STORMSHIELD

documentation@stormshield.eu