



STORMSHIELD



NOTE TECHNIQUE

STORMSHIELD NETWORK SECURITY

INTÉGRER LES LOGS SNS DANS IBM QRADAR

Produits concernés : SNS 3.7.x et supérieures, SNS 4.x

Dernière mise à jour du document : 23 décembre 2020

Référence : sns-fr-integrer_logs_SNS_dans_IBM_QRadar_note_technique



Table des matières

Avant de commencer	3
A propos de ce document	3
Prérequis et compatibilité	3
Installer l'extension SNS dans IBM QRadar	4
Télécharger le DSM	4
Importer le DSM dans QRadar	4
Configurer la source de logs	5
Adapter la taille des messages syslog UDP dans QRadar	7
Modifier la taille de la charge utile des messages syslog dans QRadar	7
Configurer le firewall SNS pour l'envoi des logs vers IBM QRadar	8
Utiliser QRadar avec le DSM SNS	9
Support	10
Pour aller plus loin	11



Avant de commencer

Parmi tous les éléments de cybersécurité pouvant être déployés pour sécuriser le réseau, la combinaison des firewalls Stormshield SNS et d'IBM Security QRadar permet aux administrateurs et aux analystes des Security Operations Centers (SOC) d'être pleinement confiants sur les défenses mises en place et d'obtenir des informations pertinentes au sujet des événements survenus au sein de leurs réseaux.

En tant que fournisseur dans le domaine de la cybersécurité, Stormshield propose, depuis plus de 20 ans, des firewalls aux entreprises disposant d'infrastructures critiques et hautement sensibles. Grâce aux firewalls Stormshield, les administrateurs peuvent sécuriser leurs réseaux, contrôler la nature des données qui transitent entre leurs utilisateurs et chiffrer les données au travers de tunnels VPN IPsec. Pour tous les événements qui se produisent en permanence au quotidien, les firewalls Stormshield produisent des logs permettant d'être informé à tout moment des événements survenus sur le réseau. La capacité des firewalls Stormshield SNS à organiser et catégoriser les logs offre aux administrateurs la possibilité d'approfondir leur connaissance de l'activité de leurs firewalls.

Grâce à IBM Security QRadar Device Support Module (DSM), les administrateurs et les SOC ont la capacité d'intégrer les logs des firewalls SNS au sein d'IBM Security QRadar afin de disposer d'informations pertinentes dans leur solution de Gestion de l'Information et des Événements de Sécurité (SIEM - Security Information and Event Management). Avec cette combinaison, les équipes de sécurité peuvent en temps réel analyser les comportements de leurs réseaux et détecter les menaces ciblant leur entreprise.

Le DSM IBM Security QRadar pour les firewalls Stormshield permet d'analyser les catégories de logs suivantes :

- Authentification,
- Firewall,
- Prévention d'intrusion (IPS),
- Gestion des menaces (UTM),
- Sandboxing,
- Événements système,
- Alarmes.

A propos de ce document

IBM QRadar est une solution de Gestion de l'Information et des Événements de Sécurité (SIEM - Security Information and Event Management) permettant l'analyse en temps réel des alertes de sécurité générées par les applications et solutions réseau.

Ce document décrit comment intégrer le DSM Stormshield Network Security à IBM QRadar.

Prérequis et compatibilité

- SNS DSM Version : 1.0.0 (date de publication : octobre 2020),
- IBM QRadar 7.3.2 et supérieur,
- SNS 3.7 et supérieur.



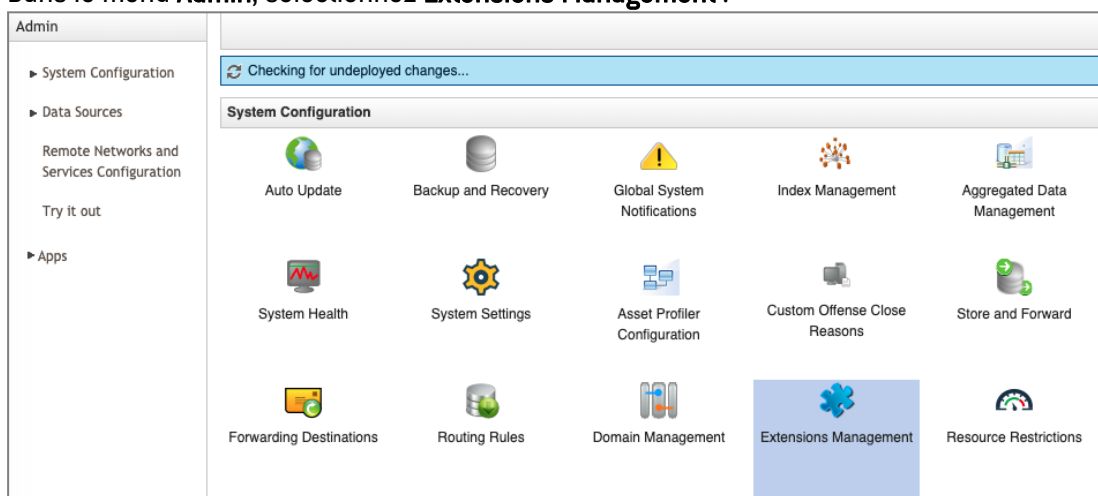
Installer l'extension SNS dans IBM QRadar

Les étapes d'installation de l'extension sont les suivantes :

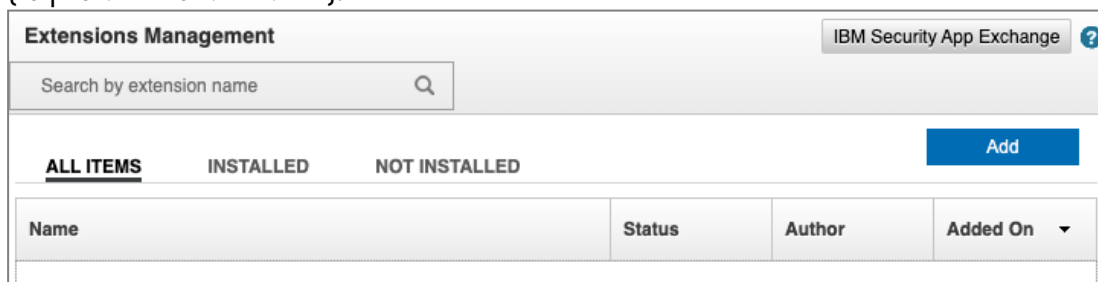
- Télécharger le DSM Stormshield Network Security depuis le [magasin d'applications IBM](#),
- Importer le DSM dans QRadar,
- Configurer une source de log qui accepte et associe les messages syslog provenant du firewall SNS au DSM.

Télécharger le DSM

1. Connectez-vous à votre console IBM QRadar.
2. Dans le menu **Admin**, sélectionnez **Extensions Management** :



3. Cliquez sur **IBM Security App Exchange**.
Votre navigateur Internet ouvre la page <https://exchange.xforce.ibmcloud.com/hub/> [requiert un identifiant IBM].



4. Téléchargez le DSM "Stormshield Network Security".

Importer le DSM dans QRadar

Dans votre console IBM QRadar :



1. Allez dans le menu **Admin > Extensions Management**.
2. Cliquez sur **Add a New Extension** :

Extensions Management IBM Security App Exchange

Search by extension name

Add

Add a New Extension

From local storage:

Browse

☐ Install immediately

Add Cancel

3. Sélectionnez l'archive au format ZIP précédemment téléchargée (Stormshield_Network_Security_DSM_v1.0.0.zip).
4. Cliquez sur **Add** pour installer l'extension :

ALL ITEMS INSTALLED NOT INSTALLED Add			
Name	Status	Author	Added On
Stormshield Network Security Among cyber security items deployed to secure the network, the combination of Stormshield SNS firewalls and IBM Security QRadar helps administrators and SOC analysts to get confidence in network defenses and to get comprehensive information in what has happened in their networks. As a cybersecurity vendor, Stormshield has been proposing firewalls for more than 20 years to companies with highly critical and sensitive infrastructures. Thanks to Stormshield SNS firewalls, administrators can secure the networks, control the data which has to transit between users, and encrypt data through VPN tunnels. For all these events which occur everyday and all day long, Stormshield SNS firewalls produce logs in order to be able to know any time what is going on in the network. Stormshield SNS firewalls capabilities to organize and to categorize the logs allow administrators to go deep and in details into the firewalls activities. Thanks to IBM Security QRadar DSM, administrators and SOCs are able to get Stormshield SNS firewalls logs into IBM Security QRadar in order to get comprehensive data in their SIEM solution. With this combination, security teams are able to analyze the network behaviors and to detect threats that are targeting the company in real time. IBM Security QRadar DSM for Stormshield SNS firewalls parse the following log categories: authentications, firewall, IPS, UTM, sandboxing and system events and alarms. Uninstall Contents: Log Source Extensions (1) Log Sources (1) Log Source Categories (1) Log Source/Protocol Mappings (3) Protocol Configuration Types (3) Log Source Types (1) QID Records (175) DSM Event Mappings (414) Installed By: admin Installed Date: 20 October 2020 Version: 1.0.0 Supported Languages: en_US Signed: Signed Support: Contact the extension's author (https://www.stormshield.com/p/services/services/technical-support/)	Installed	Stormshield	20 October 2020

Configurer la source de logs

Un firewall SNS envoie ses logs à IBM QRadar à l'aide du protocole syslog.

1. Connectez-vous à votre console IBM QRadar.
2. Dans le menu **Admin**, sélectionnez **Log Source**.



3. Cliquez sur **Ajouter**.
4. Complétez le formulaire de création de Log Source :
 - Champ **Log Source Name** : indiquez un nom pour votre nouvelle source de logs (exemple : *Stormshield SNS device*).
 - Champ **Log Source description** : précisez une description pour votre nouvelle source de logs.
 - Champ **Protocol Configuration** : sélectionnez **Syslog**.
 - Champ **Log Source Identifier** : indiquez le nom d'hôte de votre firewall SNS. Si aucun nom d'hôte n'est défini sur votre firewall, indiquez son numéro de série (exemple : *VMSNSX0000000A1*).
 - Champ **Log Source Extension** : sélectionnez **StormshieldNetworkSecurityCustom_ext**.
5. Cliquez sur **Save**.

Edit a log source ?

Note that the connection information for this log source is shared amongst one or more other log sources. This log source is a component of a Bulk Log Source, so some of its configuration parameters are not modifiable.

Log Source Name	Stormshield SNS devi
Log Source Description	StormshieldNetworkSe
Log Source Type	Stormshield Network Security
Protocol Configuration	Syslog ▼
Log Source Identifier	SNShostname
Enabled	☒
Credibility	5 ▼
Target Event Collector	eventcollector0 :: ip-10-0-1-25 ▼
Coalescing Events	☒
Incoming Payload Encoding	UTF-8 ▼
Store Event Payload	☒
Log Source Extension	StormshieldNetworkSecurityCustom_ext ▼

Please select any groups you would like this log source to be a member of:

Save Cancel



Adapter la taille des messages *syslog* UDP dans QRadar

QRadar utilise une taille par défaut de 1024 octets pour les messages syslog UDP (taille de la charge utile ou *payload*).

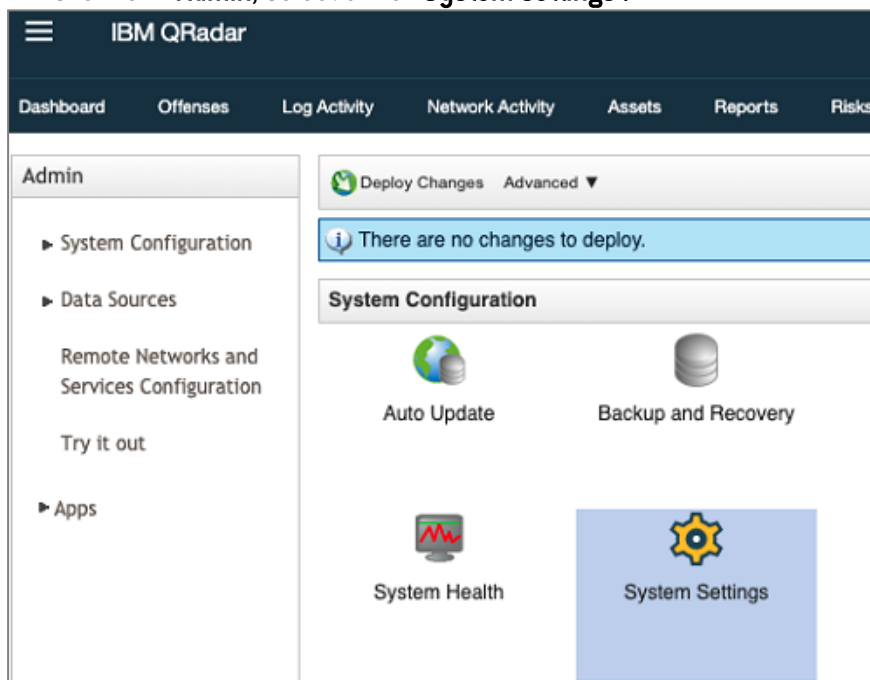
Lorsque un message excède cette taille, il est alors automatiquement tronqué.

Or, certains événements émis par les firewalls SNS excèdent cette taille. Le type de log étant positionné en fin de ligne, la catégorie d'événement correspondante ne pourra donc pas être extraite par QRadar et ces messages seront alors considérés comme inconnus par QRadar.

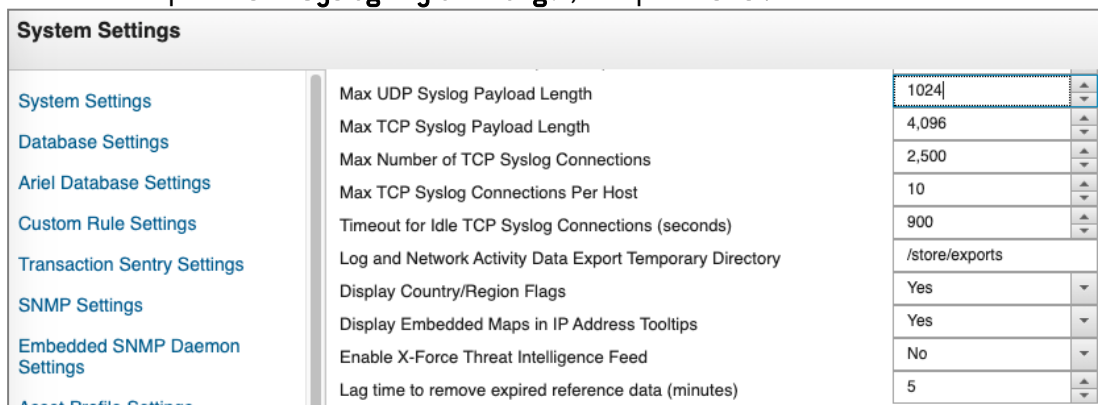
Il est donc nécessaire de modifier la taille des messages syslog UDP acceptés par IBM QRadar. Une taille de 2048 octets est suffisante pour couvrir l'ensemble des types de messages pouvant être émis par le firewall.

Modifier la taille de la charge utile des messages syslog dans QRadar

1. Connectez-vous à votre console IBM QRadar.
2. Dans le menu **Admin**, sélectionnez **System settings** :



3. Passez l'affichage du panneau de réglages système du mode **Basic** au mode **Advanced**.
4. Dans le champ **Max UDP Syslog Payload Length**, indiquez **2048** :



5. Cliquez sur **Save** pour enregistrer vos modifications.



Configurer le firewall SNS pour l'envoi des logs vers IBM QRadar

1. Connectez-vous à l'interface Web d'administration de votre firewall SNS.
2. Placez-vous dans le module **Configuration** > **Notifications** > **Traces - Syslog - IPFIX** > onglet **SYSLOG**.
3. Éditez l'un des quatre profils SYSLOG disponibles.
4. Champ **Nom**, indiquez un nom personnalisé pour ce profil.
5. Champ **Serveur Syslog** : sélectionnez ou créez un objet réseau correspondant à la machine IBM QRadar
6. Champ **Protocole** : sélectionnez **UDP**.
7. Champ **Port** : sélectionnez **syslog**.
8. Champ **Format** : sélectionnez le format **RFC5424**.
9. Dans la partie **Configuration avancée** > **Traces activées**, sélectionnez éventuellement les catégories de logs à envoyer à IBM QRadar.
10. Cliquez sur **Appliquer**.
11. Faites un double clic dans la cellule **État** du profil pour activer celui-ci.

The screenshot shows the Stormshield web interface for configuring Syslog profiles. The left sidebar has a menu with 'CONFIGURATION' at the top, followed by 'SYSTEM', 'NETWORK', 'OBJECTS', 'USERS', 'SECURITY POLICY', 'APPLICATION PROTECTION', 'VPN', and 'NOTIFICATIONS'. Under 'NOTIFICATIONS', 'Logs - Syslog - IPFIX' is selected. The main area is titled 'NOTIFICATIONS / LOGS - SYSLOG - IPFIX' and has tabs for 'LOCAL STORAGE', 'SYSLOG' (which is active), and 'IPFIX'. Under the 'SYSLOG' tab, there is a 'SYSLOG PROFILES' table with columns 'Status' and 'Name'. The first row is 'QRADAR 732' with a green 'Enabled' status. Below this table, there is a 'Details' section for the selected profile. It includes fields for 'Name' (QRADAR 732), 'Comments', 'Syslog server' (ip-10-0-1-25), 'Protocol' (UDP), 'Port' (syslog), 'Certification authority' (syslog-ca), 'Server certificate' (syslog.qradar), 'Client certificate', and 'Format' (RFC5424). There is also an 'Advanced properties' section with 'Backup server', 'Backup port' (syslog), and 'Category (facility)' (none). At the bottom, there is a 'LOGS ENABLED' section with a table showing various log categories (Alarms, Network connections, Filter policy, HTTP proxy, SMTP proxy) all with 'Enabled' status.

Status	Name
Enabled	QRADAR 732
Disabled	
Disabled	
Disabled	

Details

Name: QRADAR 732
Comments:
Syslog server: ip-10-0-1-25
Protocol: UDP
Port: syslog
Certification authority: syslog-ca
Server certificate: syslog.qradar
Client certificate:
Format: RFC5424

Advanced properties

Backup server:
Backup port: syslog
Category (facility): none

LOGS ENABLED

Status	Name
Enabled	Alarms
Enabled	Network connections
Enabled	Filter policy
Enabled	HTTP proxy
Enabled	SMTP proxy

L'installation est terminée : les logs du firewall SNS sont redirigés vers la plate-forme IBM QRadar.



Utiliser QRadar avec le DSM SNS

1. Connectez-vous à votre console IBM QRadar.
 2. Dans le menu **Log Activity**, cliquez sur **New Search**.
 3. Remplissez les différents champs du formulaire de recherche :
 - Champ **Parameter** : sélectionnez **Log Source Type**,
 - Champ **Operator** : sélectionnez **Equals**,
 - Champ **Value** : sélectionnez **Stormshield Network Security**.
 4. Validez en cliquant sur **Add Filter**.
 5. Cliquez sur **Search**.
- Les logs Stormshield s'affichent dans la grille.

Event Name	Log Source	Event Count	Time	Low Level Category	Source IP	Source Port	Destination IP	Destination Port	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	Low
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	Low
Firewall Permit	Stormshield SNS device	1	20 Oct 2020, 14:53:30	Firewall Permit	10.0.100.14	36364	10.0.0.9	443	Jessica	Low
Firewall Permit	Stormshield SNS device	1	20 Oct 2020, 14:53:19	Firewall Permit	10.0.100.9	59124	10.0.1.25	443	N/A	Low
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	Low
Firewall Permit	Stormshield SNS device	1	20 Oct 2020, 14:53:27	Firewall Permit	10.0.100.9	37503	10.0.0.1	25	N/A	Low
Firewall Permit	Stormshield SNS device	1	20 Oct 2020, 14:53:26	Firewall Permit	10.0.1.9	58506	10.0.0.9	443	N/A	Low
Firewall Deny	Stormshield SNS device	1	20 Oct 2020, 14:53:23	Firewall Deny	10.0.100.16	32615	10.0.100.16	80	Isia	Low
Firewall Permit	Stormshield SNS device	1	20 Oct 2020, 14:53:21	Firewall Permit	10.0.100.5	36429	10.0.0.7	443	Charlie	Low
Firewall Permit	Stormshield SNS device	1	20 Oct 2020, 14:53:20	Firewall Permit	10.0.100.1	36689	10.0.0.7	443	Oliver	Low
Firewall Permit	Stormshield SNS device	1	20 Oct 2020, 14:53:07	Firewall Permit	10.0.100.1	59126	10.0.0.37	22	N/A	Low
Virus Detected And Blocked	Stormshield SNS device	1	20 Oct 2020, 14:53:18	Virus Detected	10.0.100.16	21343	192.168.100.1	80	Isia	Low
Firewall Permit	Stormshield SNS device	2	20 Oct 2020, 14:53:05	Firewall Permit	10.0.100.12	58893	10.0.1.25	443	N/A	Low
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	Low
Firewall Permit	Stormshield SNS device	1	20 Oct 2020, 14:53:07	Firewall Permit	10.0.100.18	28512	10.0.0.9	636	Isabella	Low
Authentication success on the firewall via SSH	Stormshield SNS device	1	20 Oct 2020, 14:53:06	SSH Login Succeeded	192.168.11.1	0	0.0.0.0	0	N/A	Low
IP Deny	Stormshield SNS device	1	20 Oct 2020, 14:53:06	IP Deny	10.0.100.1	37887	192.168.13.1	502	N/A	Low
Firewall Permit	Stormshield SNS device	1	20 Oct 2020, 14:52:53	Firewall Permit	10.0.100.1	58849	10.0.1.9	443	N/A	Low
Firewall Permit	Stormshield SNS device	1	20 Oct 2020, 14:53:04	Firewall Permit	10.0.100.11	24302	10.0.1.110	80	Amelia	Low
Firewall Permit	Stormshield SNS device	1	20 Oct 2020, 14:52:54	Firewall Permit	10.0.1.9	43148	10.0.0.9	443	N/A	Low
Sandboxing malicious	Stormshield SNS device	1	20 Oct 2020, 14:53:02	Malicious Software	10.0.100.5	26663	10.0.0.9	80	Charlie	Low
Firewall Permit	Stormshield SNS device	1	20 Oct 2020, 14:52:52	Firewall Permit	10.0.1.9	59182	10.0.0.11	445	N/A	Low
System Informational	Stormshield SNS device	3	20 Oct 2020, 14:52:51	System Informational	10.0.100.5	0	10.0.1.110	0	admin	Low
Firewall Permit	Stormshield SNS device	1	20 Oct 2020, 14:53:01	Firewall Permit	10.0.100.5	39058	10.0.1.110	80	Charlie	Low
Sandboxing malicious	Stormshield SNS device	1	20 Oct 2020, 14:52:59	Malicious Software	10.0.100.1	27372	10.0.0.37	22	N/A	Low
Firewall Permit	Stormshield SNS device	1	20 Oct 2020, 14:52:57	Firewall Permit	10.0.100.15	36660	10.0.0.11	445	Ava	Low
Sandboxing malicious	Stormshield SNS device	1	20 Oct 2020, 14:52:55	Malicious Software	10.0.100.18	21853	10.0.0.37	22	N/A	Low
Firewall Permit	Stormshield SNS device	1	20 Oct 2020, 14:52:44	Firewall Permit	10.0.1.9	59052	10.0.0.37	22	N/A	Low
Firewall Permit	Stormshield SNS device	1	20 Oct 2020, 14:52:54	Firewall Permit	10.0.1.9	41994	10.0.1.25	443	N/A	Low
Firewall Permit	Stormshield SNS device	2	20 Oct 2020, 14:52:33	Firewall Permit	10.0.1.9	59123	10.0.1.25	443	N/A	Low
Firewall Permit	Stormshield SNS device	2	20 Oct 2020, 14:52:26	Firewall Permit	10.0.1.9	59107	10.0.1.25	443	N/A	Low
Firewall Permit	Stormshield SNS device	5	20 Oct 2020, 14:52:22	Firewall Permit	10.0.1.9	59103	10.0.1.25	443	N/A	Low
Firewall Permit	Stormshield SNS device	2	20 Oct 2020, 14:52:20	Firewall Permit	10.0.1.9	63567	10.0.0.0	0	N/A	Low
Authentication failure on the firewall via SSH	Stormshield SNS device	1	20 Oct 2020, 14:52:20	SSH Login Failed	10.0.1.9	0	0.0.0.0	0	N/A	Low

NOTE

La version 1.0.0 du DSM SNS présente deux limitations :

- Les valeurs IPv6 ne sont pas prises en compte.
- Seuls les champs standards QRadar sont utilisés : les propriétés personnalisées destinées à filtrer selon des valeurs spécifiques au constructeur ne sont pas disponibles.

Les propriétés standard QRadar alimentées par le DSM Stormshield sont les suivantes :

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



- Protocol,
- SourceIp,
- SourceMAC,
- SourcePort,
- SourceIpPostNAT,
- SourcePortPostNAT,
- UserName.

Les événements suivants sont catégorisés dans QRadar :

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

Support

Si vous rencontrez des difficultés lors de l'installation ou de l'utilisation du DSM Stormshield Network Security sur la plate-forme IBM QRadar, nous vous invitons à vous rapprocher du [support technique Stormshield](#).



Pour aller plus loin

Des informations complémentaires et réponses à vos éventuelles questions sont disponibles dans [la base de connaissances Stormshield](#) (authentification nécessaire).



STORMSHIELD

documentation@stormshield.eu

Les images de ce document ne sont pas contractuelles, l'aspect des produits présentés peut éventuellement varier.

Copyright © Stormshield 2023. Tous droits réservés. Tous les autres produits et sociétés cités dans ce document sont des marques ou des marques déposées de leur détenteur respectif.