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_les_logs_SNS_dans_IBM_QRadar_note_technique

Table des matières

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.

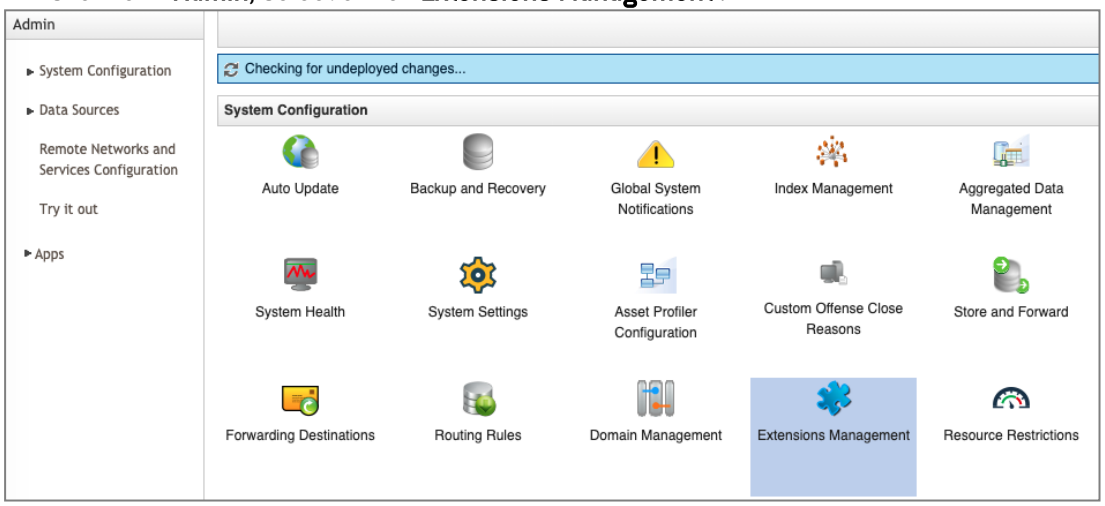
Installer l'extension SNS dans IBM QRadar

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

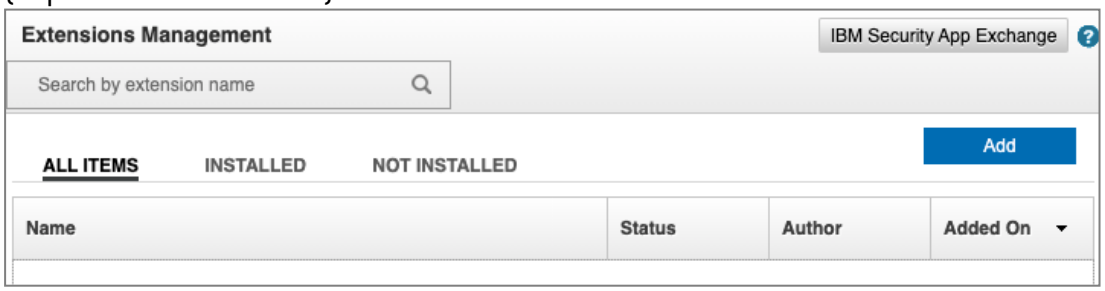
- Télécharger le DSM Stormshield Network Security depuis le magasin d'applications IBM,
- Importer le DSM dans QRadar,
- Configurer une source de log qui accepte et associe les messages syslog provenant du firewall SNS au DSM.

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).

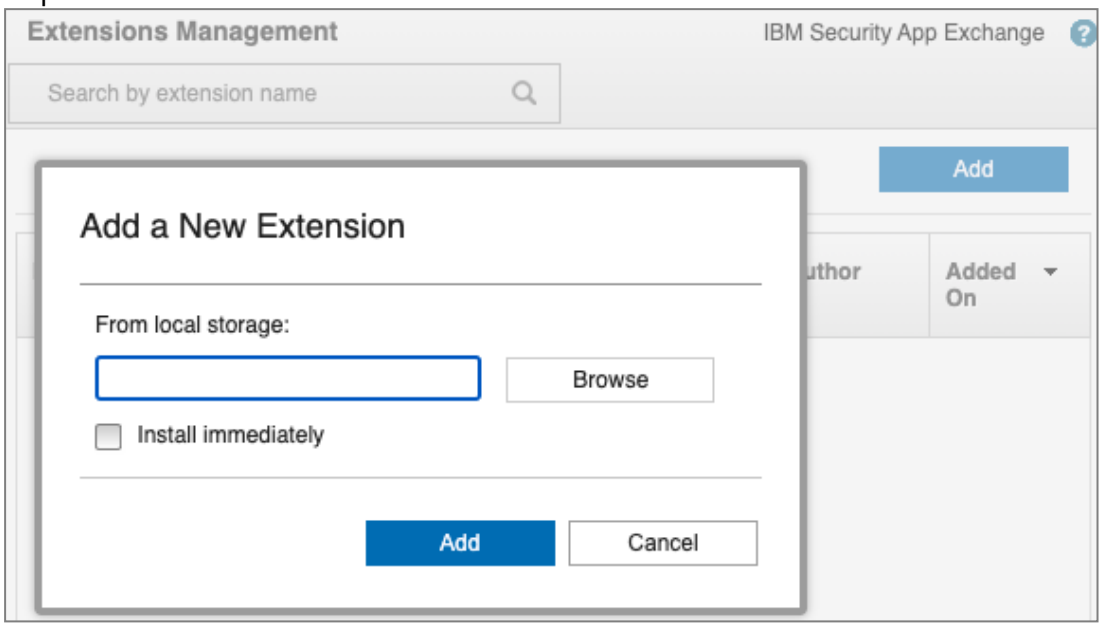


4. Téléchargez le DSM "Stormshield Network Security".

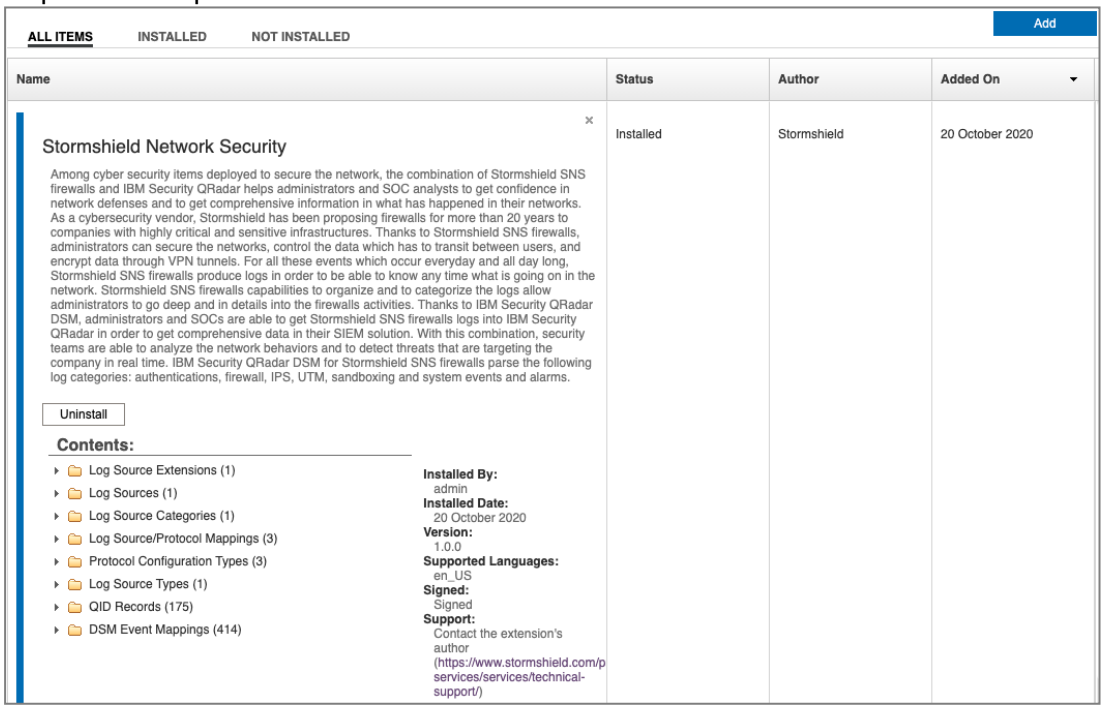
Importer le DSM dans QRadar

Dans votre console IBM QRadar :

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



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 :

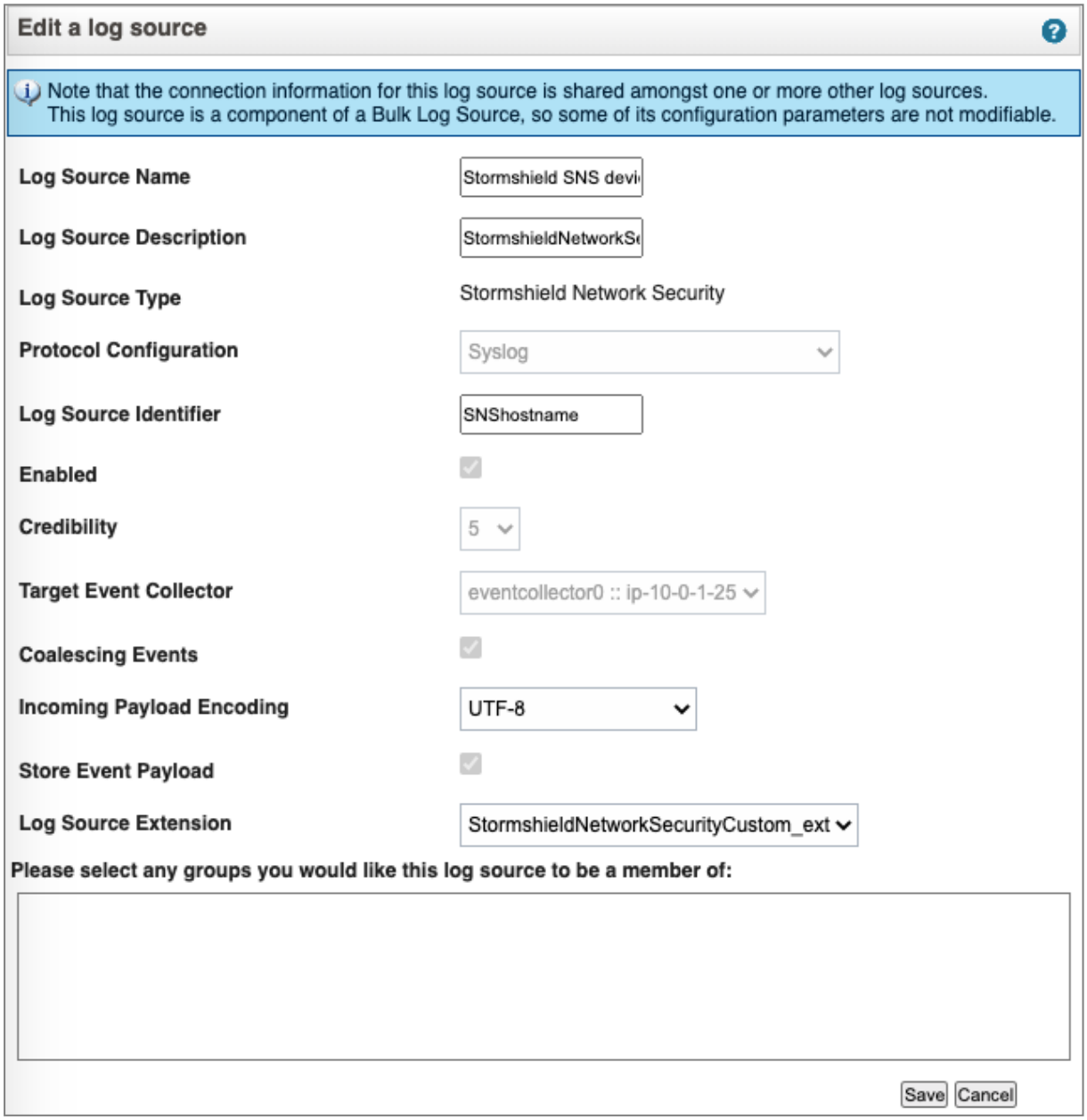


Configurer la source de logs

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 **StormshieldNeworkSecurityCustom_ext.**
5. Cliquez sur **Save**.



Adapter la taille des messages *syslog* UDP dans QRadar

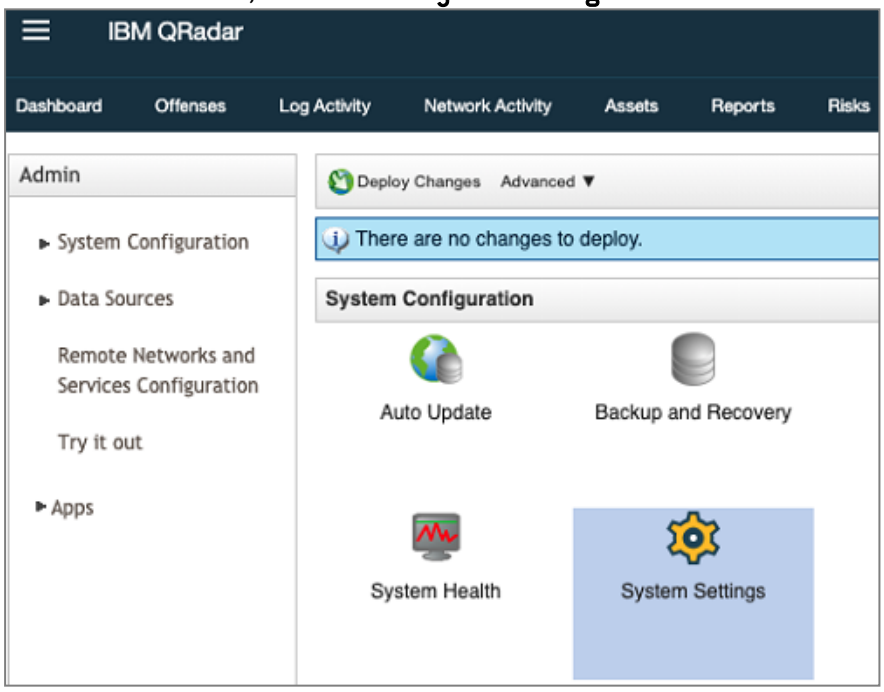
QRadar utilise une taille par défaut de 1024 octets pour les messages syslog UDP (taille de la charge utile ou *payload*).
Lorsque un message excède cette taille, il est alors automatiquement tronqué.

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.

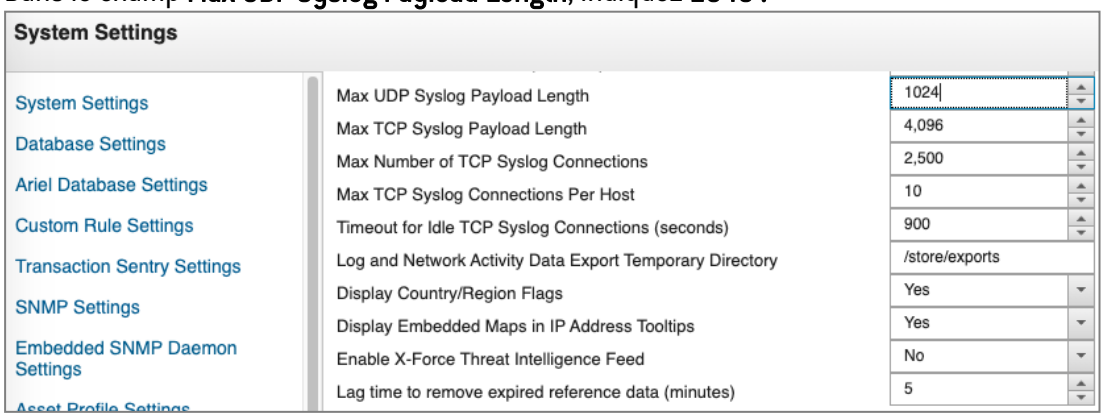
Il est donc nécessaire de modifier la taille des messages syslog UDP acceptés par IBM Qradar. Une taille de 2048 octets est suffisante pour couvrir l'ensemble des types de messages pouvant être émis par le firewall.

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 :**



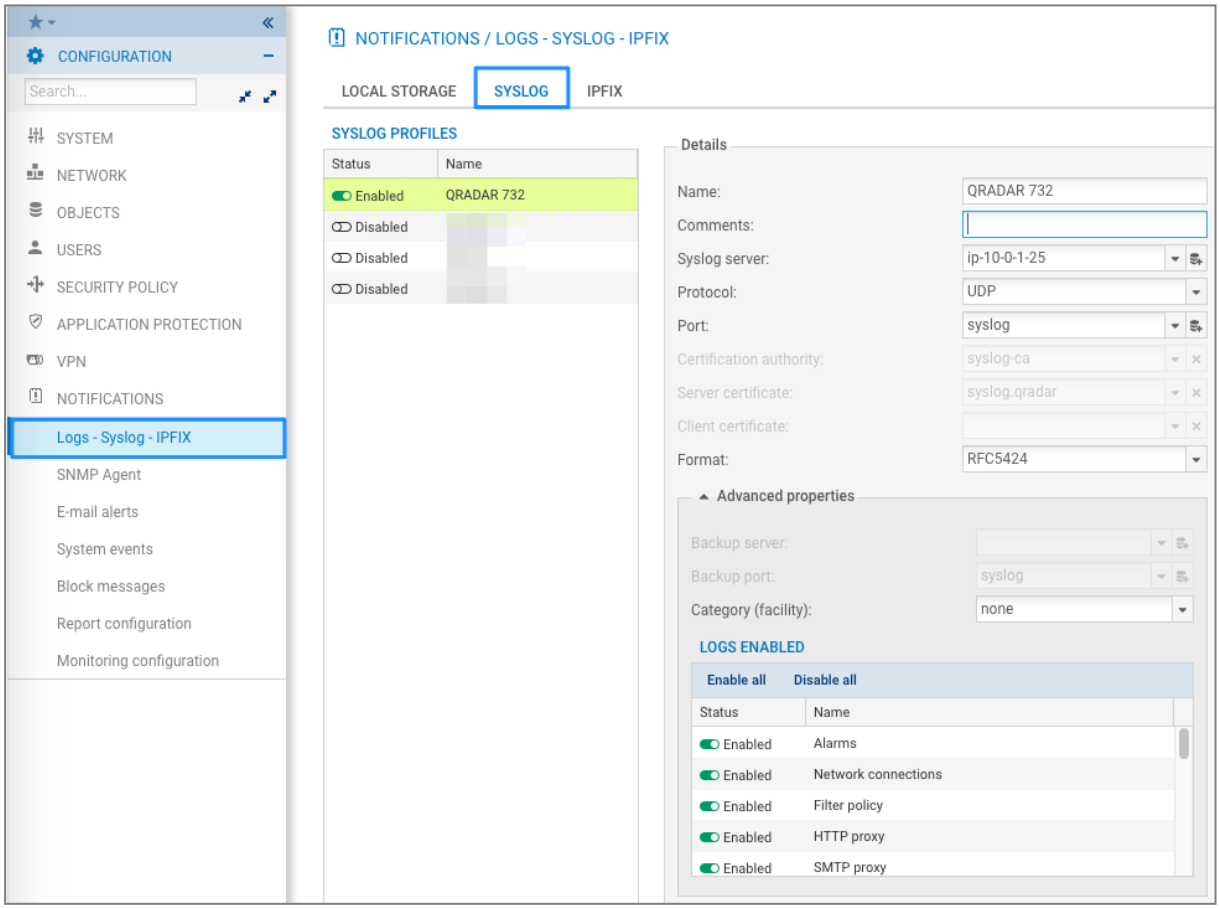
3. Passez l'affichage du panneau de réglages système du mode **Basic** au mode **Advanced**.
4. Dans le champ **Max UDP Syslog Payload Length**, indiquez **2048 :**



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.



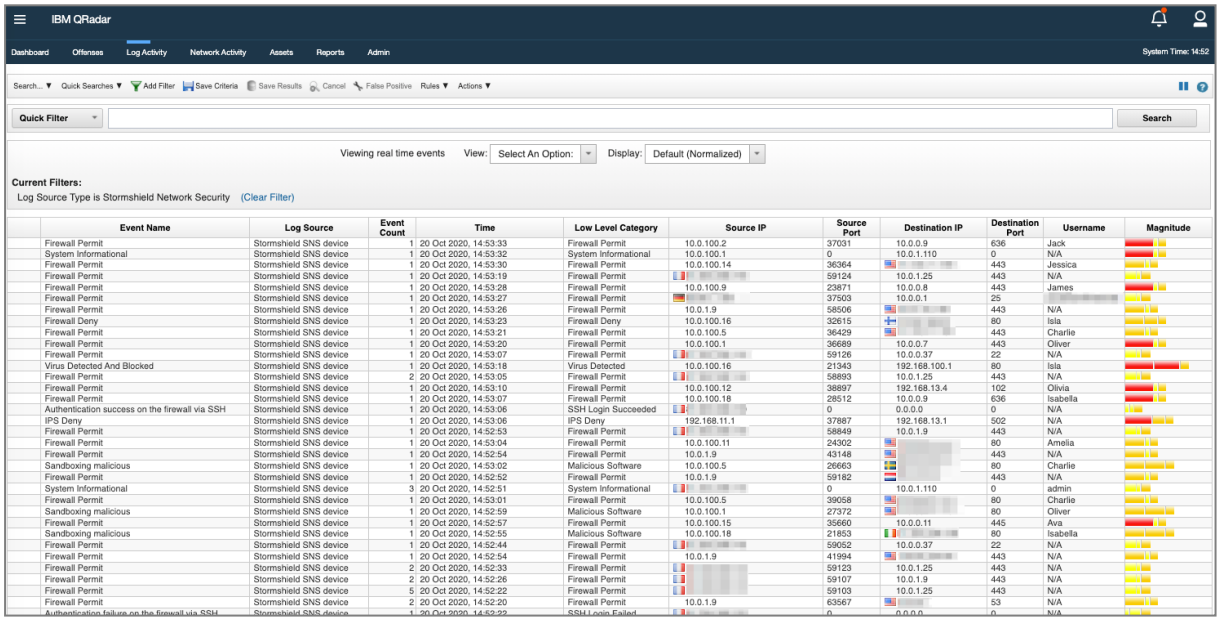
L'installation est terminée : les logs du firewall SNS sont redirigés vers la plate-forme IBM QRadar.

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.



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).

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.