NOTE TECHNIQUE

STORMSHIELD NETWORK SECURITY

SE CONFORMER AUX RÈGLEMENTS SUR LES DONNÉES PERSONNELLES

Produits concernés : SNS 3.4 et versions supérieures, SNS 4.x

Date : 09 décembre 2019

Référence : sns-fr-conformité_aux_règlements_sur les_données_personnelles_note technique

Table des matières

Avant de commencer

SNS vous aide à appliquer les règlements sur les données personnelles, notamment le Règlement Européen Général sur la Protection des Données (i.e., RGPD, ou GDPR en anglais) au sein de votre infrastructure. Ce règlement exige notamment que les données personnelles des utilisateurs restent confidentielles, et que tout traitement de leurs données soit tracé. SNS assure l'anonymisation - et donc la confidentialité - des données personnelles présentes dans les logs, les rapports, les écrans de supervision (e.g., utilisateur, nom de machine, adresse IP source). Par défaut, seul le superviseur visualise ces informations. Les autres administrateurs (les opérateurs) ne sont autorisés à accéder aux logs complets que sur justificatif et après avoir fait la demande d'un code individuel et temporaire. Toutes les opérations qu'ils effectuent après activation de ce code sont enregistrées.

Différents niveaux de responsabilité

SNS vous permet de définir différents rôles et niveaux de responsabilité afin d'assurer la conformité aux règlements sur les données personnelles.

Superviseur

Le superviseur est un administrateur de SNS qui dispose des droits *Accès aux données personnelles* et *Gestion des accès aux données personnelles*. Il peut visualiser les données personnelles contenues dans les logs. Lorsque c'est nécessaire, il accorde des accès aux opérateurs sous la forme de tickets temporaires.

Opérateur

Un opérateur est un administrateur SNS qui par défaut ne peut visualiser que des données anonymisées et n'a pas accès aux données personnelles. En cas de besoin, il peut demander un ticket d'accès temporaire au superviseur. L'utilisation de ce ticket génère un événement système visible dans les alarmes et sur le tableau de bord.

Client utilisateur

Chaque utilisateur est assuré que l'accès à ses données personnelles est protégé et contrôlé. Des logs détaillés fournissent des informations sur chaque accès : date, identité de l'opérateur, actions effectuées.

Cas d'usage

Les différents cas d'usage de conformité aux règlements sur les données personnelles sont couverts par les fonctionnalités de SNS. Dans les deux exemples décrits ici, le client fait appel à un fournisseur de services pour la configuration et la maintenance de son firewall.

Modification de la configuration du firewall

Un client demande à son fournisseur de service une modification dans la configuration de son firewall.

L'opérateur qui effectue la modification n'a accès à aucune donnée sensible : tous les noms d'utilisateurs, adresses IP source, noms de machines etc., sont masqués.

Dépannage suite à un problème réseau

Un client demande à son fournisseur de service de résoudre un problème réseau.

L'opérateur doit disposer d'un accès complet aux logs pour effectuer ce dépannage. Il demande un ticket d'accès temporaire au superviseur qui le lui transmet sous la forme d'un code composé de 16 caractères. L'opérateur résout le problème et libère le ticket temporaire. Toutes les actions effectuées par l'opérateur sont enregistrées et contrôlables.

Gestionnaire d'événements (SIEM)

SNS n'effectue pas d'anonymisation des données personnelles pour les logs qui sont exportés vers un outil de collecte et de gestion des événements de type SIEM (Security Information and Event Management). Si vous utilisez un SIEM, vous devez configurer celui-ci afin qu'il respecte les règlements sur les données personnelles. En revanche, SNS permet de chiffrer toutes les connexions entre le firewall et le SIEM.

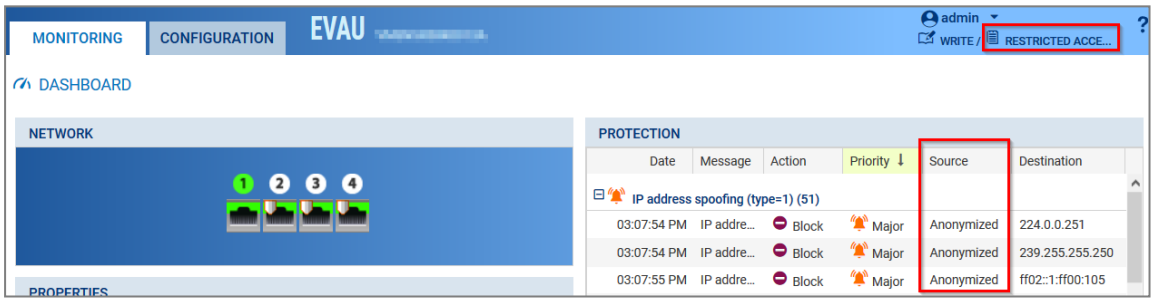
Vous êtes superviseur

Si vous êtes le superviseur du firewall, vous êtes connecté à l'interface Web d'administration avec le compte *admin*. Les opérations que vous devez effectuer en lien avec les règlements sur les données personnelles sont les suivantes :

- Accéder aux logs complets,
- Créer des opérateurs,
- Autoriser un opérateur à accéder aux logs complets,
- Vérifier les actions d'un opérateur.

Accéder aux logs complets

1. Connectez-vous à l'interface Web d'administration avec le compte *admin*. Le tableau de bord s'affiche. Les données personnelles sont masquées par défaut, comme l'indique la mention **Accès restreint aux logs** dans le bandeau supérieur.



2. Dans le bandeau, cliquez sur le nom du compte *admin*, puis sur **Obtenir le droit d'accès aux données personnelles (logs)**.
3. Cliquez sur **Obtenir**.
   Vous visualisez maintenant les données personnelles, comme l'indique la mention **Accès complet aux logs (données personnelles)** dans le bandeau supérieur.

Créer des opérateurs

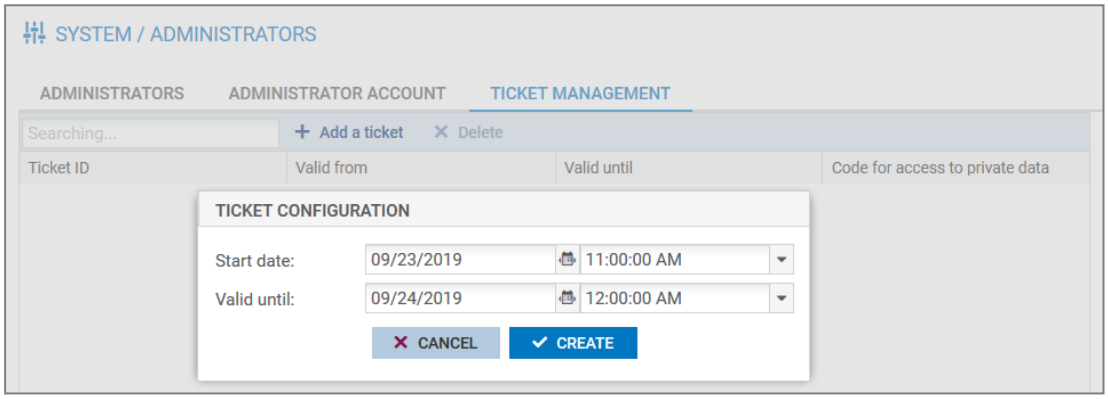
Vous pouvez créer des administrateurs de type opérateurs qui pourront effectuer des opérations de maintenance sans visualiser de données personnelles.

1. Connectez-vous à l'interface Web d'administration avec le compte *admin*.
2. Dans le module **Configuration > Système > Administrateurs**, ajoutez un administrateur sans accès aux données personnelles. Par défaut, cet administrateur ne dispose que des droits de visualiser les logs (traces) et les rapports.
3. Accordez-lui d'autres droits si vous le souhaitez, à l'exception des droits **Accès aux données personnelles** et **Gestion des accès aux données personnelles**. Ceux-ci apparaissent en **Vue avancée**.
4. Recommencez ces opérations pour chaque opérateur que vous souhaitez créer.
5. Cliquez sur **Appliquer**.

Autoriser un opérateur à accéder aux logs complets

En cas de besoin, vous pouvez fournir aux opérateurs des tickets d'accès pour leur permettre de visualiser temporairement les données personnelles contenues dans les logs.

1. Connectez-vous à l'interface Web d'administration avec un compte de superviseur (i.e., un administrateur disposant des droits *Accès aux données personnelles* et *Gestion des accès aux données personnelles*).
2. Dans le module **Configuration > Système > Administrateurs**, cliquez sur l'onglet **Gestion des tickets**, puis sur **Ajouter un ticket**.
3. Dans la fenêtre **Paramètres du ticket**, entrez les dates et heures de début et fin de validité du ticket.

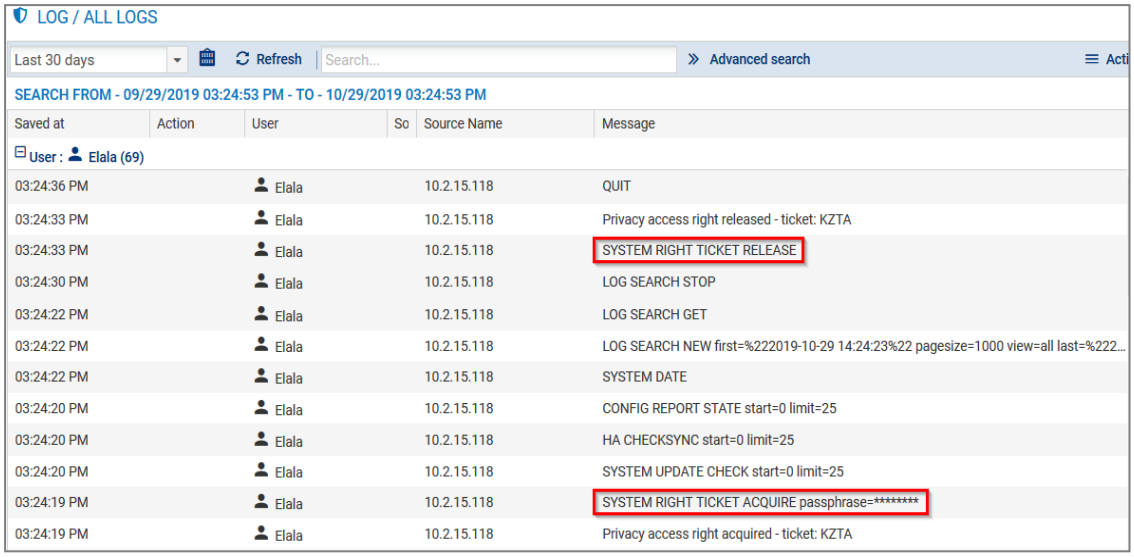


4. Cliquez sur **Créer** puis sur **Appliquer**.
5. Dans la colonne **Code d'accès aux données personnelles**, copiez le code en cliquant sur l'icône présent.
6. Fournissez le code à 16 chiffres à l'opérateur qui pourra alors l'utiliser pour avoir un accès complet aux logs.

Vérifier les actions d'un opérateur

Vous pouvez vérifier les actions d'un opérateur à qui vous avez fourni un ticket d'accès temporaire aux données personnelles.

1. Connectez-vous à l'interface Web d'administration avec le compte *admin*.
2. Dans le bandeau supérieur de la page, cliquez le nom du compte, puis sur **Obtenir le droit d'accès aux données personnelles (logs)**. Confirmez alors la demande.
3. Choisissez le module **Logs-Journaux d'audit > Logs-Journaux > Administration**.
4. Dans l'entête de la colonne **Utilisateur**, cliquez sur la flèche puis sur **Grouper par ce champ**, pour visualiser uniquement les logs correspondant à l'opérateur dont vous souhaitez vérifier les actions.
5. Dans les logs, l'entrée *SYSTEM RIGHT TICKET ACQUIRE passphrase=********* indique le début d'utilisation du ticket d'accès aux données personnelles, tandis que l'entrée *SYSTEM RIGHT TICKET RELEASE* en indique la fin. Entre les deux, les données personnelles étaient visibles pour l'opérateur.



LOG / ALL LOGS

Last 30 days | Refresh | Search... | Advanced search | Acti

SEARCH FROM - 09/29/2019 03:24:53 PM - TO - 10/29/2019 03:24:53 PM

Saved at	Action	User	So	Source Name	Message
User : Elala (69)					
03:24:36 PM		Elala		10.2.15.118	QUIT
03:24:33 PM		Elala		10.2.15.118	Privacy access right released - ticket: KZTA
03:24:33 PM		Elala		10.2.15.118	SYSTEM RIGHT TICKET RELEASE
03:24:30 PM		Elala		10.2.15.118	LOG SEARCH STOP
03:24:22 PM		Elala		10.2.15.118	LOG SEARCH GET
03:24:22 PM		Elala		10.2.15.118	LOG SEARCH NEW first=%222019-10-29 14:24:23%22 pagesize=1000 view=all last=%222...
03:24:22 PM		Elala		10.2.15.118	SYSTEM DATE
03:24:20 PM		Elala		10.2.15.118	CONFIG REPORT STATE start=0 limit=25
03:24:20 PM		Elala		10.2.15.118	HA CHECKSYNC start=0 limit=25
03:24:20 PM		Elala		10.2.15.118	SYSTEM UPDATE CHECK start=0 limit=25
03:24:19 PM		Elala		10.2.15.118	SYSTEM RIGHT TICKET ACQUIRE passphrase=********
03:24:19 PM		Elala		10.2.15.118	Privacy access right acquired - ticket: KZTA

Vous êtes opérateur

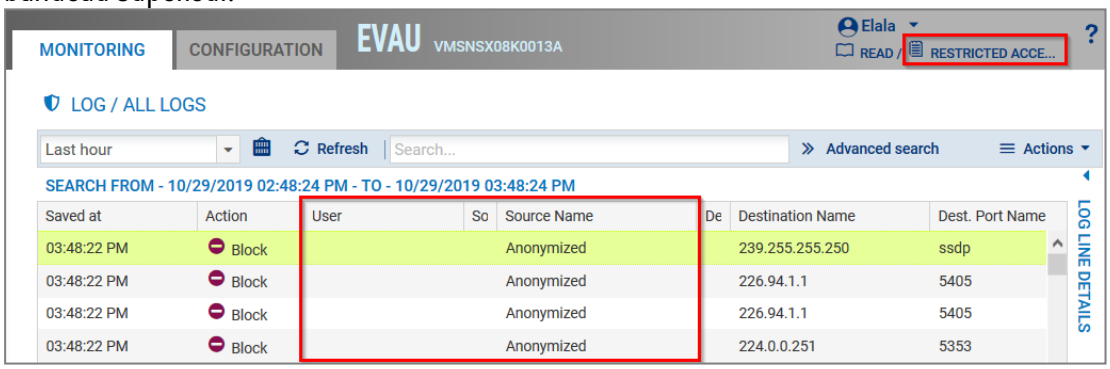
Les opérateurs sont des utilisateurs auxquels le super-administrateur du firewall (*admin*) a accordé certains droits d'administration. Par défaut, ils n'ont pas accès aux données personnelles mais ils peuvent en faire la demande auprès du superviseur en cas de besoin

Si vous vous connectez à l'interface Web d'administration en tant qu'opérateur, les données personnelles sont masquées, comme l'indique la mention **Accès restreint aux logs** dans le bandeau supérieur.

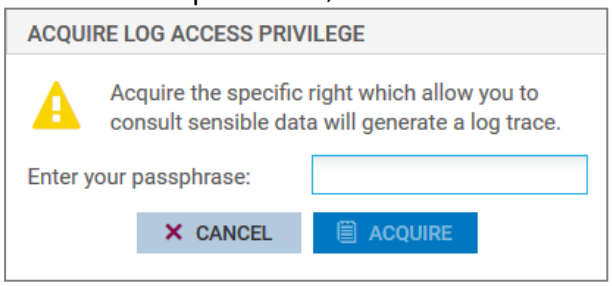
Accédez aux logs complets

Pour certaines opérations de maintenance ou de dépannage, vous devez pouvoir accéder aux logs complets, ainsi qu'à tous les rapports et écrans de supervision contenant des données personnelles.

1. Demandez au superviseur du firewall un ticket d'accès complet aux logs. Celui-ci vous fera parvenir un code d'accès aux données personnelles composé de 16 chiffres.
2. Connectez-vous à l'interface Web d'administration pour visualiser les logs. Les données personnelles sont masquées, comme l'indique la mention **Accès restreint aux logs** dans le bandeau supérieur.



3. Dans le bandeau supérieur de la page, cliquez le nom du compte, puis sur **Obtenir le droit d'accès aux données personnelles (logs)**.
4. Dans la fenêtre qui s'affiche, saisissez votre code d'accès aux données personnelles.



5. Cliquez sur **Obtenir**.
   Vous visualisez maintenant les données personnelles dans tous les modules, comme l'indique la mention **Accès complet aux logs (données personnelles)** dans le bandeau supérieur.

Si vous souhaitez visualiser les écrans de rapports et de supervision contenant des données personnelles, vous pouvez également saisir votre code lors de l'accès à ces écrans.

Désactiver l'accès complet aux logs

Le ticket d'accès complet aux logs a une durée de validité définie par l'administrateur. Lorsque la fin de validité est atteinte, le code d'accès n'est plus fonctionnel.

Il est recommandé de désactiver manuellement l'accès complet aux logs lorsque vous n'en avez plus l'utilité.

1. Dans le bandeau supérieur de l'interface Web d'administration, cliquez sur **Accès complet aux logs (données personnelles)**. Une fenêtre de confirmation s'affiche.
2. Cliquez sur **Relâcher** pour désactiver l'accès complet aux logs.

Vous ne visualisez plus les données personnelles, comme l'indique la mention **Accès restreint aux logs** dans le bandeau supérieur.

STORMSHIELD

documentation@stormshield.eu