NOTE TECHNIQUE
STORMSHIELD NETWORK SECURITY

CONFIGURER LES SERVICES WEB SUR LES FIREWALLS SNS

Produits concernés : SNS 4.5 et versions supérieures

Dernière mise à jour du document : 27 février 2024

Référence : sns-fr-configurer-services-web-firewall-SNS-note_technique

Table des matières

Historique des modifications

Date	Description
27 février 2024	- Ajout de nouveaux firewalls concernant le nombre de lignes autorisées dans un fichier d'import dans la section "Fichier d'import : format, structure et limitations"
3 novembre 2022	- Nouveau document

Avant de commencer

Le firewall SNS peut identifier à quels services sont associés certains flux Web. Ces services sont appelés des services Web sur le firewall. Leur identification permet :

- De définir pour chaque service Web des politiques fines d'engagement *SLA* (*Service Level Agreement*) SD-WAN, de qualité de service (*QoS*) et de routage afin d'assurer une connectivité optimale pour les flux Web prioritaires,
- De ne pas faire passer par le proxy les flux de certains services Web afin de décharger le proxy au profit d'autres flux,
- De bloquer ou d'autoriser les flux de certains services Web.

Cette note technique présente la gestion des services Web sur le firewall SNS ainsi que les cas d'usage les plus courants liés à l'utilisation des services Web avec le firewall SNS.

Prérequis et fonctionnement

Versions SNS compatibles avec les services Web

- SNS 4.5 et versions supérieures

Vue en clair des flux DNS

Le firewall SNS doit pouvoir voir en clair (non chiffrés) les flux DNS le traversant car le principe d'identification des services Web repose sur la reconnaissance des FQDN. Sans cela, le firewall SNS ne peut pas identifier les services Web basés sur des FQDN.

L'analyse protocolaire DNS doit être activée sur les flux DNS (niveau d'inspection IPS ou IDS).

Blocage des protocoles DoH et DoT

Le firewall SNS bloque par défaut les protocoles DNS chiffrés DoH et DoT afin de forcer un retour (*fallback*) vers le protocole DNS classique dans le but de voir les flux DNS en clair.

Ce retour intervient seulement si le navigateur Web utilisé l'autorise et après un certain nombre d'essais successifs, ce qui peut entraîner une latence jusqu'à l'apparition de la page Web demandée. À noter que le nombre d'essais et la durée de la latence dépendent du navigateur Web et ne sont pas configurables sur le firewall SNS.

Le blocage des protocoles DoH et DoT sur le firewall SNS est possible grâce à la détection de signatures contextuelles (module **Configuration > Protection applicative > Applications et protections**). Le blocage du protocle DoT est également possible lorsqu'il est détecté dans l'extension ALPN du protocole TLS (module **Configuration > Protection applicative > Protocoles > SSL**, onglet **IPS**, cadre **Application-Layer Protocol Negotiation (ALPN)**).

IMPORTANT
Il est indispensable de maintenir le blocage de ces protocoles pour que l'identification des services Web s'effectue correctement.

Utilisation d'adresses IP publiques

Seules des adresses IP publiques peuvent être utilisées dans les bases des services Web officiels et personnalisés. L'utilisation d'adresses IP privées n'est pas possible.

Principe de dépendance des services Web

Certains services Web peuvent être dépendants d'autres services Web, par exemple lorsqu'un fournisseur héberge son service chez un autre fournisseur ou encore lorsqu'un fournisseur propose plusieurs services.

Lors de l'utilisation de services Web dans la configuration du firewall SNS, et afin d'éviter de bloquer ou d'autoriser à tort certains flux Web, nous vous recommandons de vérifier au préalable si un service Web est dépendant d'un autre ou si des services Web dépendent de lui. Les dépendances connues sont affichées sur le site Stormshield Security Portal.

Gérer les services Web

Les services Web sont répartis dans deux bases sur le firewall SNS :

- **La base de services Web officiels** : ils sont créés et maintenus par Stormshield grâce aux informations que les fournisseurs communiquent,
- **La base de services Web personnalisés** : ils sont importés manuellement par un administrateur sur le firewall SNS.

Les services Web étant utilisés dans la configuration du firewall SNS, les gérer vous permet de disposer de tous les services Web nécessaires à la réalisation des configurations souhaitées et de pouvoir les maintenir à jour dans le temps.

Consulter la base de services Web officiels et vérifier si elle est à jour

Cette section explique comment consulter la base de services Web officiels et comment vérifier si elle est à jour.

Consulter la base de services Web officiels

Depuis le site Stormshield Security Portal

1. Connectez-vous à l'adresse https://security.stormshield.eu/index.php/webservices/.
2. Consultez les services Web officiels dans le tableau. Vous retrouvez pour chaque service Web le nombre d'adresses IP et de FQDN qu'il contient ainsi que ses éventuelles dépendances connues à d'autres services Web.

Depuis l'interface d'administration du firewall SNS

1. Rendez-vous dans **Configuration > Objets > Services Web**, onglet **Liste des services Web**.
2. Les services Web officiels apparaissent. Survolez-en un pour afficher ses caractéristiques :
   - **Nom** : nom du service Web officiel,
   - **Description** : courte description du contenu du service Web,
   - **En lecture seule** : les services Web officiels sont toujours en lecture seule,
   - **Numéro de révision** et **Date de révision** : ces éléments changent dès qu'une nouvelle version des informations du service Web est récupérée par le firewall SNS,
   - **URL** : liste d'URL où consulter les informations du service Web chez le fournisseur.

Vérifier si la base de services Web officiels est à jour

La base de services Web officiels se met à jour régulièrement et automatiquement grâce au module **Active Update** du firewall SNS. Pour vérifier si la base officielle est à jour :

1. Dans l'interface d'administration du firewall SNS, rendez-vous dans **Monitoring > Supervision > Système**, cadre **Active Update**.
2. Vérifiez que l'état **À jour** apparaît pour les modules **Géolocalisation / Réputation & Services Web et Icônes des Applications** et **Icônes des Applications et Services Web**.
   Si l'état **Désactivé** ou **Échec** apparaît, vérifiez dans **Configuration > Système > Active Update** que la mise à jour automatique des modules concernés est activée et que le firewall SNS peut contacter les serveurs de mise à jour visibles dans la zone **Configuration avancée**.

Demander à Stormshield d'ajouter un service Web dans la base officielle

1. Connectez-vous à votre espace personnel MyStormshield.
2. Rendez-vous dans **Support technique > Demande de reconnaissance Webservice**.
3. Complétez les informations demandées. Les champs **Nom du service web** et **URL du service web** sont obligatoires. Le fournisseur doit mettre à disposition sur une URL publique les informations (adresses IP et FQDN) du service Web concerné. Sans cela, Stormshield ne sera pas en mesure d'ajouter le service Web à la base officielle.
4. Cliquez sur **Envoyer**.

Vous recevrez une réponse dans les meilleurs délais sur l'adresse e-mail associée à votre compte MyStormshield. En attendant, vous pouvez ajouter le service Web dans la base personnalisée de votre firewall SNS (voir le chapitre Consulter et gérer la base de services Web personnalisés). Si le service Web est finalement ajouté à la base officielle, n'oubliez pas de le supprimer de la base personnalisée.

Consulter et gérer la base de services Web personnalisés

Cette section explique comment consulter et gérer (import, export, suppression) la base de services Web personnalisés.

IMPORTANT
La base personnalisée est toujours prioritaire sur la base officielle. En utilisant une base personnalisée, la recherche dans les bases s'arrête dès qu'une correspondance est trouvée dans la base personnalisée. Soyez donc attentif à la maintenir à jour.

Consulter la base de services Web personnalisés

1. Dans l'interface d'administration du firewall SNS, rendez-vous dans **Configuration > Objets > Services Web**, onglet **Liste des services Web**.
2. Les services Web personnalisés apparaissent en-dessous des officiels. Survolez-en un pour afficher ses caractéristiques. Elles proviennent du dernier import réalisé.
3. Vous pouvez consulter les adresses IP et FQDN des services Web personnalisés en exportant la base. Pour cela, cliquez sur **Exporter la base personnalisée**, acceptez le téléchargement du fichier CSV puis retrouvez les informations souhaitées dans le fichier.

Si aucun service Web personnalisé ne s'affiche ou si vous souhaitez ajouter, modifier ou retirer un service Web de la base existante, vous devez importer une nouvelle base personnalisée.

Importer une base de services Web personnalisés

Avant de réaliser tout import, prenez connaissances des éléments suivants :

- Vous ne pouvez disposer que d'une seule base personnalisée sur le firewall SNS,
- L'import se réalise avec un fichier CSV contenant les informations des services Web,
- L'import réussi d'une base personnalisée **supprime et remplace** la base personnalisée existante. Dans ce cas, assurez-vous que le fichier d'import utilisé contienne tous les services Web personnalisés que vous souhaitez conserver, sinon ils seront perdus,
- Vous pouvez télécharger la base existante en cliquant sur **Exporter la base personnalisée** afin de l'utiliser comme modèle pour créer le nouveau fichier d'import.

Fichier d'import : format, structure et limitations

- Le fichier doit être au format CSV,
- Chaque ligne du fichier est constituée de plusieurs champs, tous séparés par des virgules,
- Les champs optionnels vides sont inclus entre deux virgules,
- Le fichier doit comporter une ligne vide après le dernier enregistrement.

```
#name,#ip/fqdn,#date,#revision,#comment
```

Champ	Description
Nom du service (obligatoire)	Chaîne de texte respectant les critères suivants : • Maximum 20 caractères alphanumériques, • Non sensible à la casse, le nom est toujours considéré en minuscule. Les majuscules ne sont pas conservées sur le firewall SNS lors de l'import.
Adresse IP ou FQDN (obligatoire)	Adresse IPv4 / IPv6 publique ou un FQDN. Un FQDN ne peut contenir qu'**un seul** méta-caractère (*wildcard*) ***** en début ou au milieu de son nom. Si un service Web repose sur plusieurs adresses IP ou FQDN, la ligne le décrivant doit être dupliquée autant de fois que le service Web comporte d'adresses IP ou de FQDN. Seules les informations optionnelles de la première ligne seront conservées.
Date de révision (optionnel)	Date et heure de révision au format **YYYY/MM/DD** ou **YYYY/MM/DD hh:mm** (exemple : *2022/10/15 10:30*).
Numéro de révision (optionnel)	Numéro de révision pouvant contenir jusqu'à 3 chiffres : **major.minor.patch** (exemple : *10.2*).
Commentaire (optionnel)	Chaîne de texte libre pouvant être encadrée de guillemets si elle contient une virgule.

```
name1,1.1.1.1,2021/09/21 11:00,1.1.1,Simple case
name2,2.2.2.2,2021/12/31,2,"Comment, with comma"
name2,domain.tld,2022/01/01,3,"Date, revision and comment are discarded"
name3,*.newdomain.tld,,,No date and revision
```

Une limitation sur le nombre de lignes autorisées dans le fichier d'import existe :

Firewalls physiques SNS

SN160(W)	5 000
SN210(W), SN310	10 000
SN-S-Series-220, SN-S-Series-320, SN510, SN710, SNi20, SNi40	100 000
SN-M-Series-520, SN-M-Series-720, SN910, SN-M-Series-920, SN1100, SN2000, SN2100, SN3000, SN3100, SN6000, SN6100	1 000 000

Firewalls virtuels EVA

EVA avec 1 Go de RAM	10 000
EVA avec 2 Go à 6 Go de RAM	100 000
EVA avec 8 Go à 64 Go de RAM	1 000 000

Une limitation sur le nombre de lignes possédant un FQDN avec un méta-caractère ***** au milieu existe : 10 % du nombre de lignes autorisées dans le fichier d'import.

Réaliser l'import du fichier CSV

1. Dans l'interface d'administration du firewall SNS, rendez-vous dans **Configuration > Objets > Services Web**, onglet **Liste des services Web**.
2. Si une base personnalisée existe déjà, nous vous recommandons d'en télécharger une copie en cliquant sur **Exporter la base personnalisée**.
3. Dans l'onglet **Import de services personnalisés**, cadre **Importer**, sélectionnez le fichier d'import. Si une base personnalisée existe déjà, le fichier doit contenir les services Web que vous souhaitez conserver, sinon ils seront supprimés. Assurez-vous que les services Web qui seront supprimés ne sont plus utilisés dans la configuration du firewall SNS (règles de la politique de filtrage, groupes de services Web).
4. Cliquez sur **Importer la base**. L'import peut être annulé tant qu'il n'est pas terminé. Si une erreur s'affiche, prenez-en connaissance et vérifiez votre fichier d'import. Privilégiez un éditeur de texte plutôt que le logiciel Excel pour vérifier le fichier.

Un message signale que l'import s'est terminé avec succès. Si une base personnalisée existait déjà, celle-ci a été supprimée et remplacée par la nouvelle.

> **ASTUCE**
> Vous pouvez demander à Stormshield d'ajouter un service Web dans la base officielle.

Supprimer la base de services Web personnalisés

1. Dans l'interface d'administration du firewall SNS, assurez-vous que les services Web personnalisés ne sont plus utilisés dans la configuration du firewall SNS (règles de la politique de filtrage, groupes de services Web).
2. Rendez-vous dans **Configuration > Objets > Services Web**, onglet **Liste des services Web**.
3. Nous vous recommandons de télécharger une copie de la base personnalisée avant de la supprimer en cliquant sur **Exporter la base personnalisée**.
4. Cliquez sur **Supprimer la base personnalisée** et validez la suppression.

Gérer les groupes de services Web

Cette section explique comment consulter et gérer (ajout, suppression, modification des membres) les groupes de services Web.

Les manipulations de cette section sont à réaliser dans l'interface d'administration du firewall SNS dans **Configuration > Objets > Services Web**, onglet **Groupes**.

Consulter les groupes de services Web et leurs membres

Les groupes disponibles s'affichent dans la grille **Liste des groupes**. Il en existe deux types :

- **Les groupes prédéfinis** : ils sont créés et maintenus par Stormshield et contiennent uniquement des services Web officiels. Ces groupes sont toujours en lecture seule,
- **Les groupes personnalisés** : ils sont créés et gérés par un administrateur sur le firewall SNS et peuvent contenir des services Web officiels et personnalisés.

Vous retrouvez pour chaque groupe le nombre de membres qu'il contient. Double cliquez sur un groupe pour afficher ses membres dans la grille **Membres du groupe** à droite.

Ajouter un groupe de services Web

1. Dans la grille **Liste des groupes**, cliquez sur **Ajouter**.
2. Définissez un nom au groupe de services Web. Précisez un commentaire si besoin.
3. Cliquez sur **Appliquer**.

Le groupe est créé sans aucun membre. La grille **Membres du groupe** s'affiche à droite, vous donnant la possibilité d'ajouter des membres.

Gérer les membres d'un groupe de services Web

1. Dans la grille **Liste des groupes**, double cliquez sur le groupe concerné.
2. Dans la grille **Membres du groupe** à droite :
   - Pour ajouter des membres : cliquez sur **Ajouter** et sélectionnez les services Web officiels et personnalisés à ajouter,
   - Pour supprimer des membres : sélectionnez les services Web dans la grille puis cliquez sur **Supprimer** (sélection multiple possible avec la touche **[Ctrl]** du clavier).

La prise en compte des modifications est immédiate après chaque action.

Supprimer un groupe de services Web

1. Avant de supprimer un groupe, assurez-vous qu'il n'est plus utilisé dans la configuration du firewall SNS (règles de la politique de filtrage).
2. Dans la grille **Liste des groupes**, cliquez sur le groupe concerné.
3. Cliquez sur **Supprimer**.

Utiliser les services Web avec du SD-WAN ou de la QoS

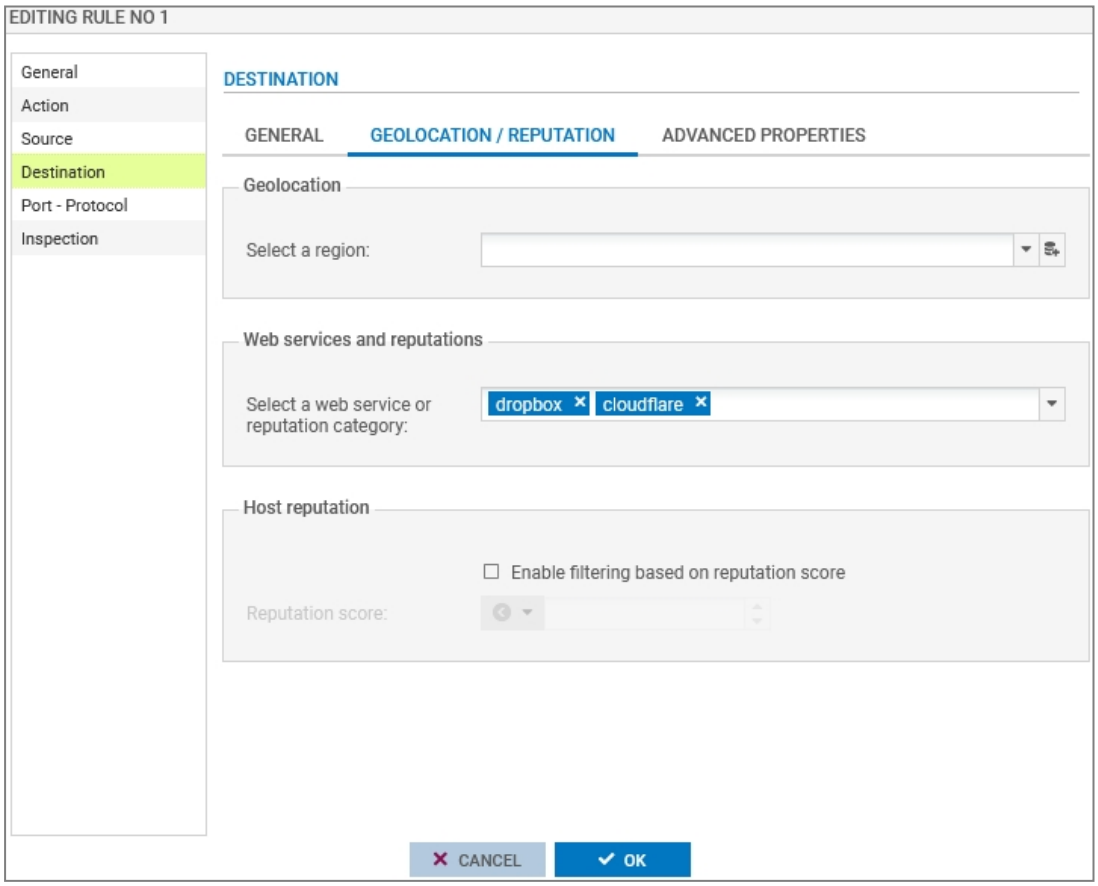
Si vous avez configuré sur votre firewall SNS une politique de qualité de service (QoS) ou d'engagement *SLA* SD-WAN, vous pouvez spécifier dans les règles de filtrage concernées des services Web en tant que critère de destination.

Avec de la QoS, vous pouvez réserver ou limiter la bande passante pour chaque service Web afin d'assurer une connectivité optimale pour les flux Web prioritaires. Pour plus d'informations, reportez-vous à la note technique Configurer la QoS sur les firewalls SNS.

Avec du SD-WAN, vous pouvez définir pour chaque service Web les liens réseau à emprunter de manière automatique et transparente selon leurs contraintes de performances associées (latence acceptée, taux de disponibilité, ...). Pour plus d'informations, reportez-vous à la note technique SD-WAN - Sélectionner le meilleur lien réseau.

De manière générale, pour ajouter dans une règle de filtrage existante un service Web en tant que critère de destination :

1. Rendez-vous dans **Configuration > Politique de sécurité > Filtrage et NAT**, onglet **Filtrage**.
2. Double cliquez sur le numéro de la règle concernée.
3. Dans la fenêtre d'édition, rendez-vous sur l'onglet **Destination** situé à gauche, puis dans le sous-onglet **Géolocalisation / Réputation**, cadre **Services Web et Réputations**, sélectionnez les services Web concernés (officiels, personnalisés ou groupes). Pour rappel, vous pouvez vérifier les dépendances des service Web officiels sur le site Stormshield Security Portal.
4. Cliquez sur **OK**.



Éviter que les flux d'un service Web ne passent par le proxy

Vous pouvez définir de ne pas faire passer par le proxy les flux d'un service Web afin de décharger le proxy au profit d'autres flux. Réalisez cette manipulation uniquement pour les services Web en lesquels vous avez une totale confiance.

1. Rendez-vous dans **Configuration > Politique de sécurité > Filtrage et NAT**, onglet **Filtrage**.
2. Cliquez sur **Nouvelle règle > Règle simple**.
3. Double cliquez sur le numéro de la nouvelle règle.
4. Dans la fenêtre d'édition, complétez les informations suivantes :
   - Onglet **Général**, champ **État** : sélectionnez *On*,
   - Onglet **Action**, champ **Action** : sélectionnez *passer*,
   - Onglet **Source**, champ **Machines sources** : sélectionnez *Network_in*,
   - Onglet **Destination** :
     - Sous-onglet **Général**, champ **Machines destinations** : sélectionnez *Any*,
     - Sous-onglet **Géolocalisation / Réputation**, cadre **Services Web et Réputations** : sélectionnez le service Web concerné. Pour rappel, afin d'éviter d'autoriser à tort certains flux Web, vérifiez les dépendances du service Web concerné sur le site Stormshield Security Portal.
5. Cliquez sur **OK**.
6. Positionnez la règle en haut de la politique de filtrage, en amont des règles utilisant le proxy du firewall SNS.

Bloquer ou autoriser les flux d'un service Web

Vous pouvez bloquer ou autoriser les flux d'un service Web en ajoutant une règle dans la politique de filtrage du firewall SNS.

1. Rendez-vous dans **Configuration > Politique de sécurité > Filtrage et NAT**, onglet **Filtrage**.
2. Cliquez sur **Nouvelle règle > Règle simple**.
3. Double cliquez sur le numéro de la nouvelle règle.
4. Dans la fenêtre d'édition, complétez les informations suivantes :
   - Onglet **Général**, champ **État** : sélectionnez *On*,
   - Onglet **Action**, champ **Action** : sélectionnez *passer* ou *bloquer*,
   - Onglet **Source**, champ **Machines sources** : sélectionnez les objets souhaités (par exemple *Network_in*),
   - Onglet **Destination** :
     - Sous-onglet **Général**, champ **Machines destinations** : sélectionnez les objets souhaités (par exemple *Any*),
     - Sous-onglet **Géolocalisation / Réputation**, cadre **Services Web et Réputations** : sélectionnez le service Web concerné. Pour rappel, afin d'éviter de bloquer ou d'autoriser à tort certains flux Web, vérifiez les dépendances du service Web concerné sur le site Stormshield Security Portal.
5. Cliquez sur **OK**.
6. Positionnez les règles autorisant les flux des services Web au-dessus des règles bloquantes du fait que les règles sont évaluées dans l'ordre de leur numérotation.

Suivre l'activité des services Web

Ce chapitre explique comment suivre l'activité des services Web dans l'interface d'administration du firewall SNS. Ces éléments vous permettent d'ajuster vos configurations selon l'activité des services Web que vous constatez.

Dans la supervision du firewall

La supervision permet de visionner en temps réel pour chaque service Web supervisé :

- Le nombre de connexions réalisées,
- La bande passante entrante consommée,
- La bande passante sortante consommée.

Pour superviser un service Web :

1. Rendez-vous dans **Configuration > Notifications > Configuration de la supervision**, onglet **Configuration des services Web**.
2. Cliquez sur **Ajouter** et sélectionnez un service Web. Vous pouvez en ajouter 10 maximum.
3. Cliquez sur **Appliquer**.

Pour consulter les courbes des services Web supervisés :

1. Rendez-vous dans **Monitoring > Supervision > Services Web**.
2. Cliquez sur l'onglet des données que vous souhaitez voir.

Dans les rapports du firewall

Les rapports permettent de visionner pour une échelle de temps spécifique (dernière heure, dernier jour, 7 derniers jours et 30 derniers jours) le top 10 des services Web pour lesquels :

- Le trafic est le plus important en termes de volume de données échangés,
- Le nombre de connexions relevées est le plus important.

Pour consulter les rapports :

1. Vérifiez dans **Configuration > Notifications > Configuration des rapports** que **Rapports statiques** est activé et que les rapports **Services Web** sont activés.
2. Rendez-vous dans **Monitoring > Rapports > Services Web** et cliquez sur le rapport que vous souhaitez visionner.
3. Sur le rapport, modifiez l'échelle de temps si nécessaire. Si vous venez d'activer les rapports, patientez quelques minutes le temps que le firewall SNS récupère suffisamment de données afin de créer les rapports.

Dans les journaux d'audit (logs) du firewall

Certains journaux peuvent afficher le service Web source ou destination. Pour consulter un journal, rendez-vous dans **Monitoring > Logs - Journaux d'audit** et sélectionnez le journal concerné.

Certaines informations sont accessibles sous réserve d'activer le droit de consulter les données personnelles. Si vous disposez de ce droit ou d'un code d'accès aux données personnelles, cliquez sur **Logs : accès restreint** dans le bandeau supérieur. Pour plus d'informations, reportez-vous à la note technique Se conformer aux règlements sur les données personnelles.

Pour aller plus loin

Des informations complémentaires et réponses à vos éventuelles questions peuvent être disponibles sur les liens suivants :

- Note technique Configurer la QoS sur les firewalls SNS.
- Note technique SD-WAN - Sélectionner le meilleur lien réseau.
- Base de connaissances Stormshield (authentification nécessaire).

documentation@stormshield.eu