NOTE TECHNIQUE

STORMSHIELD NETWORK SECURITY

CONFIGURER ET UTILISER LE VPN SSL DES FIREWALLS SNS

Produits concernés : SNS 3.x, SNS 4.x, SSL VPN Client 3.x

Dernière mise à jour du document : 18 janvier 2024

Référence : sns-fr-tunnels_vpn_ssl_note_technique

Table des matières

Historique des modifications

Date	Description
18 janvier 2024	- Modification de la section "Activer et paramétrer le service VPN SSL" (informations concernant le TPM).
14 décembre 2023	- Modification de la section "Activer et paramétrer le service VPN SSL".
20 juillet 2023	- Sortie de SN SSL VPN Client 3.2.3 - Modification des sections "Fonctionnement et limitations", "Installer SN SSL VPN Client", "Établir un tunnel VPN SSL avec SN SSL VPN Client" et "Résoudre les problèmes".
25 mai 2023	- Modification des sections "Configurer l'authentification", "Installer SN SSL VPN Client" et "Résoudre les problèmes"
21 février 2023	- Modifications des sections "Fonctionnement et limitations" et "Établir un tunnel VPN SSL"
2 février 2023	- Modification de la section "Configurer l'authentification"
26 janvier 2023	- Sortie de SN SSL VPN Client 3.2
10 janvier 2023	- Ajout de la compatibilité avec TOTP - Modification des sections "Prérequis", "Fonctionnement et limitations", "Configurer le firewall SNS" et "Établir un tunnel VPN SSL"
19 août 2022	- Modification de la section "Configurer l'authentification"
12 juillet 2022	- Modification des sections "Prérequis", "Configurer le firewall SNS", "Installer et configurer le client VPN SSL", "Établir un tunnel VPN SSL" et "Consulter les journaux (logs)"
12 mai 2022	- Ajout de la compatibilité avec Windows 11 64 bits
22 février 2022	- Sortie de SN SSL VPN Client 3.0 - Modification de la section "Prérequis"

Avant de commencer

Le VPN SSL permet à des utilisateurs distants d'accéder de manière sécurisée à des ressources, internes à une entreprise ou non, en passant par le firewall SNS. Pour qu'un tunnel VPN SSL puisse s'établir avec le firewall SNS, un client VPN SSL doit être installé sur le poste de travail ou le terminal mobile de l'utilisateur.

Les communications entre le firewall SNS et l'utilisateur sont alors encapsulées et protégées via un tunnel TLS chiffré. L'établissement de ce tunnel est basé sur la présentation de certificats serveur et client signés par une autorité de certification de confiance (CA). Cette solution garantit donc authentification, confidentialité, intégrité et non-répudiation.

Cette note technique présente la configuration du service VPN SSL des firewalls SNS, ainsi que l'installation et la configuration d'un client VPN SSL jusqu'à l'établissement d'un tunnel VPN SSL.

Prérequis

Les prérequis pour réaliser les manipulations de cette note technique sont les suivants.

Avoir connecté le firewall SNS à un annuaire

Le firewall SNS doit être connecté à un annuaire afin d'afficher dans ses modules les listes d'utilisateurs et groupes d'utilisateurs. Ceci permettra de définir lors de la configuration du VPN SSL les utilisateurs et groupes d'utilisateurs qui pourront établir des tunnels VPN SSL.

Vous pouvez vérifier cette connexion dans l'interface d'administration du firewall SNS dans **Configuration > Utilisateurs > Authentification > Méthodes disponibles**. Une ligne **LDAP** doit apparaître dans la grille. Pour plus d'informations, reportez-vous à la section *Authentification* du manuel utilisateur **v4** ou **v3** de la version SNS utilisée.

Permettre aux utilisateurs d'accéder au portail captif du firewall SNS

Le portail captif du firewall SNS doit être activé et les utilisateurs qui se connecteront en VPN SSL doivent pouvoir y accéder. Cet accès permet notamment de récupérer la configuration VPN.

Vous pouvez vérifier la configuration du portail captif dans l'interface d'administration du firewall SNS dans **Configuration > Utilisateurs > Authentification**, onglets **Portail captif** et **Profils du portail captif**. Pour plus d'informations, reportez-vous à la section *Authentification* du manuel utilisateur **v4** ou **v3** de la version SNS utilisée.

Avoir configuré les éléments pour utiliser une authentification multifacteur (facultatif)

Si vous souhaitez utiliser une authentification multifacteur pour les connexions VPN SSL, les éléments suivants doivent déjà être configurés :

- La solution d'authentification multifacteur choisie,
- Le serveur RADIUS, permettant de faire le lien entre le firewall SNS et la solution d'authentification multifacteur choisie.

Fonctionnement et limitations

Clients VPN SSL compatibles

- **SN SSL VPN Client**, dans sa version 3.x la plus récente. SN SSL VPN Client est compatible avec Windows 8.1 64 bits, Windows 10 64 bits et Windows 11 64 bits,
- **OpenVPN Connect**, compatible avec Windows, macOS, Linux, iOS et Android. Pour plus d'informations, reportez-vous au site web d'OpenVPN,
- **SN VPN Client Standard**, dans sa version 6.x la plus récente. SN VPN Client Standard est compatible avec Windows 10 et Windows 11 avec processeur Intel 64 bits. Pour plus d'informations sur sa configuration et son utilisation, reportez-vous au Guide d'utilisation SN VPN Client Standard (disponible en anglais).

Nombre maximal de tunnels VPN SSL autorisés par les firewalls SNS

Ce nombre est différent selon le modèle de firewall SNS utilisé. Retrouvez cette information sur le site de Stormshield, rubrique Tous nos produits > Protection des réseaux.

Spécificités du client VPN SSL Stormshield

Mode de connexion automatique

SN SSL VPN Client dispose d'un mode de connexion automatique lui permettant de récupérer de manière sécurisée sa configuration VPN SSL. Ce mode fonctionne de la manière suivante :

- **À la première connexion en Mode Automatique :**
  - SN SSL VPN Client s'authentifie une première fois sur le firewall SNS et récupère automatiquement sa configuration VPN SSL,
  - SN SSL VPN Client s'authentifie une seconde fois sur le firewall SNS afin d'établir le tunnel VPN SSL.
- **Lors des connexions suivantes :**
  - S'il n'existe pas de nouvelle configuration VPN SSL, SN SSL VPN Client s'authentifie sur le firewall SNS afin d'établir le tunnel VPN SSL,
  - Si une nouvelle configuration VPN SSL est disponible, SN SSL VPN Client s'authentifie comme lors d'une première connexion afin de récupérer la nouvelle configuration.

SN SSL VPN Client dispose également d'un mode de connexion manuel où la configuration VPN SSL doit être intégrée manuellement. À noter qu'OpenVPN Connect dispose seulement d'un mode de connexion manuel.

Exécution de scripts

SN SSL VPN Client peut exécuter des scripts sur le poste de travail de l'utilisateur (Windows uniquement) à chaque ouverture et fermeture d'un tunnel VPN SSL.

Méthodes d'authentification multifacteur compatibles avec SN SSL VPN Client

Ce tableau récapitule les méthodes d'authentification multifacteur compatibles selon la version installée sur le firewall SNS et le mode de connexion utilisé par SN SSL VPN Client.

Version SNS	Mode de connexion utilisé par SN SSL VPN Client	Mot de passe + Code OTP	Code OTP seulement	Mode Push	TOTP
4.5 ou supérieure	Tous les modes	✓	✓	✓	✓
4.3, 4.4	Tous les modes	✓	✓	✓	✗
3.x, 4.2 ou inférieure	Mode Automatique	✗	✗	✗	✗
	Mode Manuel	✓	✓	✗	✗

Les modes de connexion de SN SSL VPN Client sont : Mode Automatique (avec ou sans utilisation du carnet d'adresses) et le Mode Manuel.

Configurer le firewall SNS

La mise en œuvre de tunnels VPN SSL nécessite de configurer plusieurs modules du firewall SNS. Même si certains sont déjà configurés, assurez-vous que les éléments décrits dans ce chapitre y sont bien configurés :

- Configurer l'authentification,
- Attribuer les droits d'accès au VPN SSL,
- Activer et paramétrer le service VPN SSL,
- Créer les règles de filtrage et de NAT.

Réalisez les manipulations de ce chapitre dans l'interface d'administration du firewall SNS.

Configurer l'authentification

Rendez-vous dans **Configuration > Utilisateurs > Authentification**.

Ajouter la méthode d'authentification RADIUS (facultatif)

Si vous utilisez une authentification multifacteur pour les connexions VPN SSL, la méthode RADIUS permet de connecter le firewall SNS à votre serveur RADIUS (préalablement configuré), lui-même connecté à votre solution d'authentification multifacteur (préalablement configurée).

1. Positionnez-vous dans l'onglet **Méthodes disponibles**.
2. Cliquez sur **Ajouter une méthode** ou **Activer une méthode**, puis cliquez sur **RADIUS**.
3. Suivez les indications. Pour plus d'informations sur les champs à remplir, reportez-vous à la section Authentification du manuel utilisateur v4 ou v3 de la version SNS utilisée.
4. Si une méthode d'authentification multifacteur **Mode Push** est utilisée, vous devez modifier le *timeout* RADIUS afin de laisser aux utilisateurs un délai suffisant pour s'authentifier. Par exemple pour 30 secondes, utilisez les commandes CLI / Serverd suivantes :

```
CONFIG AUTH RADIUS timeout=30000
CONFIG AUTH RADIUS btimeout=30000
CONFIG AUTH ACTIVATE
```

Configurer la politique d'authentification

1. Positionnez-vous dans l'onglet **Politique d'authentification**.
2. Dans la zone **Méthode par défaut**, champ **Méthode à utiliser si aucune règle ne peut être appliquée**, repérez la méthode spécifiée. Poursuivez ensuite selon le cas qui s'applique.

Le firewall utilise la méthode par défaut LDAP et j'utilise exclusivement cette méthode

La configuration actuelle est suffisante. Poursuivez vers la section Configurer le portail captif.

Dans tous les autres cas

Dans tous les autres cas (restriction au strict nécessaire de l'authentification, utilisation de l'authentification multifacteur, TOTP, ...), vous devez ajouter 2 règles. Vous pouvez aussi créer des règles pour des groupes d'utilisateurs spécifiques pour augmenter la sécurité. À noter que les règles sont examinées dans l'ordre de leur numérotation lors d'une authentification.

Ajoutez une première règle :

1. Cliquez sur **Nouvelle règle > Règle standard**.
2. Dans l'onglet **Utilisateur**, champ **Utilisateur ou groupe**, sélectionnez le groupe d'utilisateurs concerné. *Any user@* concerne tous les utilisateurs du domaine.
3. Dans l'onglet **Source**, cliquez sur **Ajouter une interface** et sélectionnez l'interface externe par laquelle l'authentification sera réalisée (par exemple *out*).
4. Dans l'onglet **Méthodes d'authentification**, dans la grille, sélectionnez la ligne *Méthode par défaut* et cliquez sur **Supprimer**.
5. Cliquez sur **Autoriser une méthode** et sélectionnez la méthode (*LDAP*, *RADIUS*, ...) permettant de se connecter au portail captif du firewall et de récupérer la configuration VPN.

Ajoutez une seconde règle :

1. Cliquez sur **Nouvelle règle > Règle standard**.
2. Dans l'onglet **Utilisateur**, champ **Utilisateur ou groupe**, sélectionnez le groupe d'utilisateurs concerné. *Any user@* concerne tous les utilisateurs du domaine.
3. Dans l'onglet **Source**, cliquez sur **Ajouter une interface** et sélectionnez *VPN SSL*.
4. Dans l'onglet **Méthodes d'authentification**, dans la grille, sélectionnez la ligne *Méthode par défaut* et cliquez sur **Supprimer**.
5. Cliquez sur **Autoriser une méthode** et sélectionnez la méthode (*LDAP*, *RADIUS*, ...) permettant d'établir les tunnels VPN SSL.

Configurer le portail captif

1. Positionnez-vous dans l'onglet **Portail captif**, grille **Correspondance entre profil d'authentification et interface**, et cliquez sur **Ajouter**.
2. Dans la colonne **Interface**, sélectionnez l'interface de provenance des clients VPN SSL. Pour une interface PPPoE ou VLAN, sélectionnez-la plutôt que l'interface physique parente.
3. Dans la colonne **Méthode ou annuaire par défaut**, vérifiez l'annuaire renseigné. S'il est correct, le profil sélectionné est correctement pré-configuré. Poursuivez vers la section Attribuer les droits d'accès au VPN SSL.
   En cas contraire, sélectionnez un autre profil, comme *default05*, et rendez-vous dans l'onglet **Profils du Portail captif**. Sélectionnez cet autre profil, choisissez le bon annuaire dans le champ **Méthode ou annuaire par défaut** et activez le portail captif dans la zone **Configuration avancée**.

Attribuer les droits d'accès au VPN SSL

Rendez-vous dans **Configuration > Utilisateurs > Droits d'accès**.

Pour autoriser tous les utilisateurs à établir des tunnels VPN SSL

1. Dans l'onglet **Accès par défaut**, champ **Politique VPN SSL**, sélectionnez **Autoriser**.

Pour autoriser certains utilisateurs et groupes d'utilisateurs à établir des tunnels VPN SSL

1. Dans l'onglet **Accès par défaut**, champ **Politique VPN SSL**, sélectionnez **Interdire**.
2. Dans l'onglet **Accès détaillé**, cliquez sur **Ajouter** pour créer une règle d'accès personnalisée.
3. Sélectionnez l'utilisateur ou le groupe d'utilisateurs concerné.
4. Dans la colonne **VPN SSL**, sélectionnez l'action **Autoriser**.
5. Activez la règle en effectuant un double-clic dans la colonne **État** de la ligne concernée.

Activer et paramétrer le service VPN SSL

Pour activer le service VPN SSL sur le firewall SNS :

1. Rendez-vous dans **Configuration > VPN > VPN SSL**.
2. Positionnez le curseur d'état sur **ON**.

Plusieurs zones sont disponibles pour paramétrer le service VPN SSL du firewall SNS.

Zone Paramètres réseaux

1. Dans le champ **Adresse IP (ou FQDN) de l'UTM utilisée**, indiquez l'adresse que les utilisateurs devront utiliser pour joindre le firewall SNS afin d'établir les tunnels VPN SSL.
   - Si vous renseignez une adresse IP, elle doit être publique, donc accessible sur Internet,
   - Si vous renseignez un FQDN (exemple : *ssl.company.tld*), il doit être déclaré dans les serveurs DNS utilisés par le terminal client lorsque celui-ci est en dehors du réseau de l'entreprise. Si vous disposez d'une adresse IP publique dynamique, vous pouvez recourir aux services d'un fournisseur comme *DynDNS* ou *No-IP*. Dans ce cas, paramétrez ce FQDN sur le firewall SNS dans **Configuration > Réseau > DNS dynamique**.
2. Dans le champ **Réseaux ou machines accessibles**, sélectionnez l'objet représentant les réseaux ou machines qui seront joignables au travers du tunnel VPN SSL. Cet objet permet de définir automatiquement sur le terminal client les routes nécessaires pour joindre les ressources accessibles via le VPN.
   Des règles de filtrage seront nécessaires pour autoriser ou interdire plus finement les flux entre les clients distants et les ressources internes. Il peut également être nécessaire de définir des routes statiques d'accès au réseau attribué aux clients VPN sur les équipements de l'entreprise situés entre le firewall SNS et les ressources internes mises à disposition.
3. Dans les champs **Réseau assigné aux clients (UDP)** et **Réseau assigné aux clients (TCP)**, sélectionnez l'objet correspondant au réseau qui sera assigné aux clients VPN. La taille minimale du masque réseau est de /29 pour les versions SNS 3.x ou 4.2 et inférieures, et de /28 pour les versions SNS 4.3 et supérieures.
   Vous pouvez assigner un réseau différent aux clients VPN en UDP et en TCP. Le client VPN choisira toujours en premier le réseau UDP pour de meilleures performances.
   Concernant le choix du réseau ou des sous-réseaux :
   - Choisissez un réseau dédié aux clients VPN SSL et n'appartenant pas aux réseaux internes existants ou déclarés par une route statique sur le firewall SNS. L'interface utilisée pour le VPN SSL étant protégée, le firewall SNS détecterait alors une tentative d'usurpation d'adresse IP (*spoofing*) et bloquerait les flux correspondants,
   - Choisissez des sous-réseaux peu communément utilisés (comme 10.**60.77**.0/24) afin d'éviter des conflits de routage sur les terminaux clients lors de la connexion au VPN SSL. De nombreux réseaux d'accès à Internet filtrés (Wi-Fi public, hôtels) ou réseaux locaux privés utilisent déjà les premières plages d'adresses réservées.
4. Le nombre maximal de tunnels simultanés autorisés s'affiche automatiquement. Il correspond à la valeur minimale entre le nombre maximal de tunnels autorisés sur le firewall SNS (voir Fonctionnement et limitations) et le nombre de sous-réseaux disponibles pour les clients VPN. Pour ce dernier, cela représente pour les versions SNS :
   - **3.x ou 4.2 et inférieures** le quart du nombre d'adresses IP, moins 1. Un tunnel VPN SSL consomme 4 IP, mais le serveur réserve 1 sous-réseau pour son propre usage.
   - **4.3 et supérieures** le quart du nombre d'adresses IP, moins 2. Un tunnel VPN SSL consomme 4 IP, mais le serveur réserve 2 sous-réseaux pour son propre usage.

Zone Paramètres DNS envoyés au client

1. Dans le champ **Nom de domaine**, indiquez le nom de domaine attribué aux clients VPN SSL pour leur permettre d'effectuer leurs résolutions de noms d'hôtes.
2. Dans les champs **Serveur DNS primaire** et **Serveur DNS secondaire**, sélectionnez l'objet représentant le serveur DNS à attribuer.

Zone Configuration avancée

1. Dans le champ **Adresse IP de l'UTM pour le VPN SSL (UDP)**, notamment dans l'un des cas suivants :
   - L'adresse IP utilisée pour établir les tunnels VPN SSL (UDP) n'est pas l'adresse IP principale de l'interface externe,
   - L'adresse IP utilisée pour établir les tunnels VPN SSL (UDP) est portée par une interface externe qui n'est pas en lien avec la passerelle par défaut du firewall.

   Sélectionnez l'objet représentant l'adresse IP utilisée pour établir les tunnels VPN SSL (UDP). Par défaut, le service VPN SSL écoute sur toutes les adresses IP du firewall SNS.
2. Dans les champs **Port (UDP)** et **Port (TCP)**, vous pouvez modifier les ports d'écoute du service VPN SSL. Certains ports sont réservés à un usage interne du firewall SNS et ne peuvent pas être sélectionnés. Si vous modifiez les ports par défaut, le VPN SSL pourrait ne plus être accessible depuis un réseau avec filtrage d'accès à Internet (hôtels, Wi-Fi public). Pour les **versions 4.3 et supérieures**, le port 443 est le seul port inférieur à 1024 qui peut être utilisé.
3. Dans le champ **Délai avant renégociation des clés (secondes)**, vous pouvez modifier le délai au terme duquel les clés utilisées par les algorithmes de chiffrement sont renégociées. La valeur par défaut est de 4 heures (14400 secondes). Cette opération est transparente pour l'utilisateur : le tunnel actif n'est pas interrompu lors de la renégociation.
4. Lorsque **Utiliser les serveurs DNS fournis par le firewall** est coché, le client VPN SSL inscrit dans la configuration réseau du poste de travail (Windows uniquement) les serveurs DNS récupérés via le VPN SSL. Ceux déjà définis sur le poste de travail pourront être interrogés.
5. Lorsque **Interdire l'utilisation de serveurs DNS tiers** est coché, les serveurs DNS déjà définis dans la configuration du poste de travail (Windows uniquement) sont exclus par le client VPN SSL. Seuls ceux envoyés par le firewall SNS pourront être interrogés.

Scripts à exécuter sur le client

Sur des postes de travail Windows, SN SSL VPN Client peut exécuter des scripts *.bat* à l'ouverture et à la fermeture d'un tunnel VPN SSL. Vous pouvez utiliser dans ces scripts :

- Les variables d'environnement Windows (**%USERDOMAIN%**, **%SystemRoot%**, ...),
- Les variables liées au VPN SSL : **%NS_USERNAME%** (nom d'utilisateur servant à l'authentification) et **%NS_ADDRESS%** (adresse IP attribuée au client VPN SSL).

Exemple de script pour connecter le lecteur réseau *Z:* au partage *\\myserver\myshare* :

```
NET USE Z: \\myserver\myshare
```

Exemple de script pour déconnecter le lecteur réseau *Z:* du partage *\\myserver\myshare* :

```
NET USE Z: /delete
```

Certificats utilisés

Sélectionnez les certificats que le service VPN SSL du firewall SNS et le client VPN SSL doivent présenter pour établir un tunnel. Par défaut, l'autorité de certification dédiée au VPN SSL ainsi qu'un certificat serveur et un certificat client créés à l'initialisation du firewall sont proposés.

Si vous choisissez d'utiliser votre propre autorité de certification, vous devez créer une identité client et une identité serveur. S'il ne s'agit pas d'une autorité racine, les deux certificats correspondants doivent être issus de la même sous-autorité.

Pour les firewalls équipés d'un module TPM et en version SNS 4.7 et supérieure :

- Vous pouvez choisir un **certificat serveur** dont la clé privée est protégée par le TPM. L'icône indique les certificats dont la clé privée est protégée par le TPM,
- Vous ne pouvez pas choisir un **certificat client** dont la clé privée est protégée par le TPM car la clé privée de ce certificat doit être disponible en clair (non chiffrée) dans la configuration VPN distribuée aux clients VPN.

Pour plus d'informations sur la protection par le TPM des clés privées de certificats du firewall jusqu'à la configuration de ces certificats dans les modules du firewall, reportez-vous à la note technique Configurer le module TPM et protéger les clés privées de certificats du firewall SNS.

Configuration

Le bouton **Exporter le fichier de configuration** exporte la configuration VPN SSL au format *.ovpn*.

Créer les règles de filtrage et de NAT

Rendez-vous dans **Configuration > Politique de sécurité > Filtrage et NAT**.

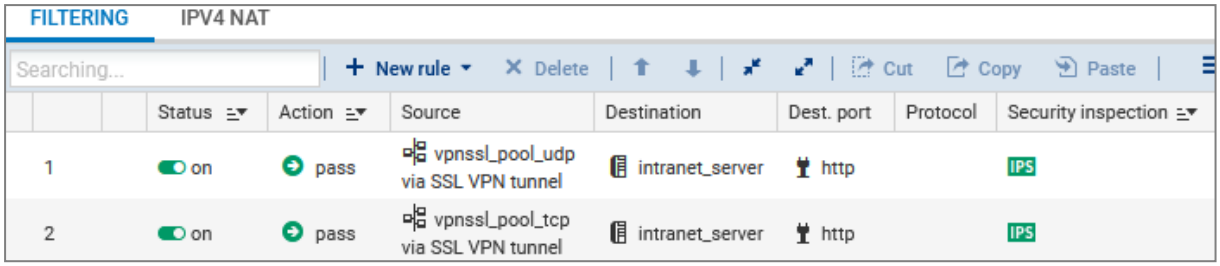
Configurer la politique de filtrage

Vous devez définir des règles autorisant ou interdisant les clients VPN SSL à accéder aux ressources internes. Dans notre exemple, nous ajoutons 2 règles afin d'autoriser les connexions à partir des clients VPN SSL en UDP et en TCP vers notre intranet en HTTP.

Pour augmenter la sécurité, vous pouvez aussi créer des règles pour des groupes d'utilisateurs spécifiques (champ **Utilisateur**) et faire appel aux fonctions avancées de filtrage (profils d'inspection, proxies applicatifs, contrôle antiviral, etc.).

1. Dans l'onglet **Filtrage**, cliquez sur **Nouvelle règle > Règle simple**.
2. Double cliquez sur le numéro de la règle pour ouvrir sa fenêtre d'édition.
3. Dans l'onglet **Général**, champ **État**, sélectionnez *On*.
4. Dans l'onglet **Action**, champ **Action**, sélectionnez *passer*.
5. Dans l'onglet **Source**, sous-onglet **Général**, champ **Machines sources**, sélectionnez l'objet représentant les adresses IP des clients VPN SSL en UDP pour la première règle. Pour la seconde règle, sélectionnez l'objet représentant les adresses IP des clients VPN SSL en TCP.
6. Dans le sous-onglet **Configuration avancée**, champ **Via**, sélectionnez *Tunnel VPN SSL*.
7. Dans l'onglet **Destination**, champ **Machines destinations**, sélectionnez l'objet représentant le serveur interne ou le réseau intranet.
8. Dans l'onglet **Port / Protocole**, champ **Port destination**, sélectionnez *http*.
9. Cliquez sur **OK**.

Écran de la politique de filtrage sur un firewall SNS en version 4 (similaire en version 3).

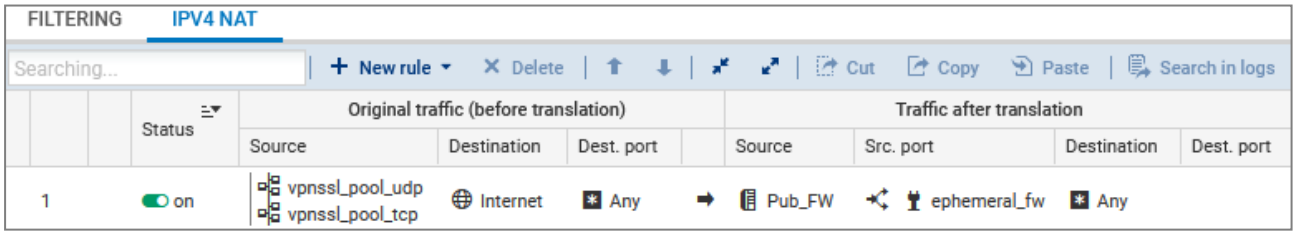


Configurer la politique de NAT

Vous devez mettre en place une règle de translation d'adresses (NAT) si les clients VPN SSL en UDP et en TCP doivent accéder à Internet.

1. Dans l'onglet **NAT** ou **IPv4 NAT**, cliquez sur **Nouvelle règle > Règle simple**.
2. Double cliquez sur le numéro de la nouvelle règle pour ouvrir sa fenêtre d'édition.
3. Dans l'onglet **Général**, champ **État**, sélectionnez *On*.
4. Dans l'onglet **Source originale**, champ **Machines sources**, sélectionnez les objets représentant les adresses IP des clients VPN SSL en UDP et en TCP.
5. Dans le champ **Interface de sortie**, sélectionnez *VPN SSL*.
6. Dans l'onglet **Destination originale**, champ **Machines destinations**, sélectionnez *Internet*.
7. Dans l'onglet **Source translatée**, champ **Machine source translatée**, sélectionnez l'objet représentant l'adresse IP publique.
8. Dans le champ **Port source translaté**, sélectionnez *ephemeral_fw* et cochez la case **choisir aléatoirement le port source translaté**.
9. Cliquez sur **OK**.

Écran de la politique de NAT sur un firewall SNS en version 4 (similaire en version 3).



Installer et configurer le client VPN SSL

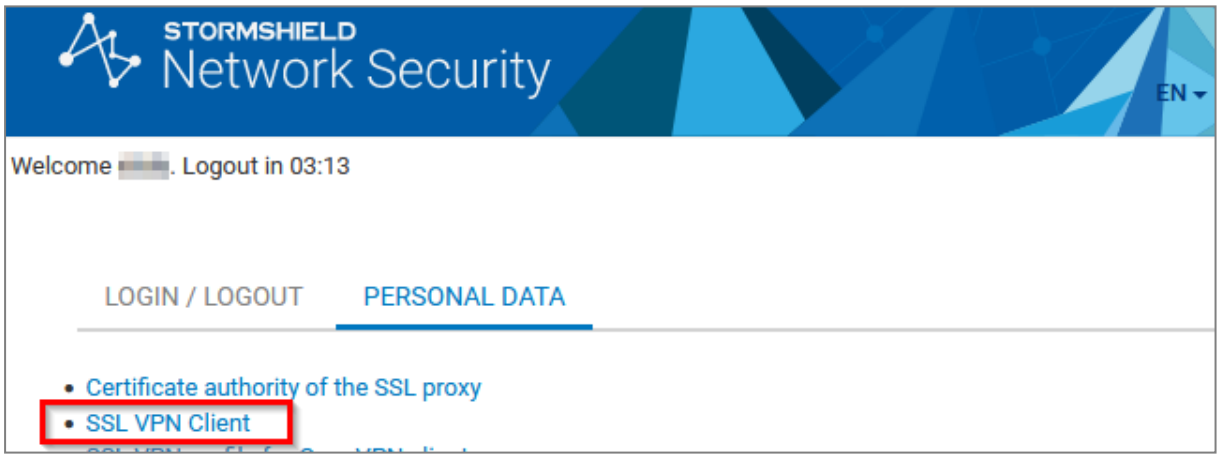
Ce chapitre explique comment installer et configurer SN SSL VPN Client et OpenVPN Connect.

Installer et configurer SN SSL VPN Client

Télécharger SN SSL VPN Client

- **Depuis le site Stormshield VPN SSL.**
  Connectez-vous à l'adresse *https://vpn.stormshield.eu/* et suivez les indications.
- **Depuis l'espace personnel MyStormshield.**
  Connectez-vous à votre espace personnel MyStormshield et rendez-vous dans **Téléchargements > Téléchargements > Stormshield Network Security > VPN SSL**.
- **Depuis le portail captif du firewall SNS hébergeant le service VPN SSL.**
  Authentifiez-vous à l'adresse *https://adresseIP_du_firewall/auth*, puis dans l'onglet **Données personnelles**, cliquez sur **VPN SSL Client**.

Écran du portail captif sur un firewall SNS en version 4 (similaire en version 3).



Installer SN SSL VPN Client

SN SSL VPN Client ne peut être utilisé que par un seul profil utilisateur Windows. Il doit être impérativement installé sur le profil de son utilisateur final via l'une des méthodes suivantes. L'installation requiert d'être administrateur local sur la machine ou de fournir le nom et le mot de passe d'un compte administrateur.

Installation classique

1. Exécutez le package *msi* téléchargé au préalable sur le poste de travail.
2. Suivez les étapes de l'assistant d'installation.

Déploiement via une stratégie de groupe (GPO)

En déployant SN SSL VPN Client via une stratégie de groupe (GPO), son installation se réalise automatiquement lorsque la machine se connecte au réseau de l'entreprise. Pour mettre en place ce déploiement, récupérez au préalable le package *msi*.

SN SSL VPN Client n'étant pas multi-utilisateur, vous devez définir sa stratégie d'installation dans l'arborescence de **Configuration utilisateur** du contrôleur de domaine : **Éditeur de gestion**

de stratégie de groupe > **Stratégie Default Domain Policy** > **Configuration utilisateur** > **Stratégies** > **Paramètres du logiciel** > **Installation de logiciel**.

Pour faciliter la connexion des utilisateurs au VPN SSL, vous pouvez pré-remplir le champ **Adresse du firewall** de la fenêtre de connexion du SN SSL VPN Client en modifiant la valeur de la clé de registre **HKEY_CURRENT_USER\Software\STORMSHIELD\SSL VPN Client\address**.

Configurer SN SSL VPN Client

Il existe plusieurs modes de connexion que SN SSL VPN Client peut utiliser. Reportez-vous à la section Spécificités du client VPN SSL Stormshield pour vérifier la compatibilité des modes avec l'authentification multifacteur.

Configurer le Mode Automatique

En **Mode Automatique**, SN SSL VPN Client récupère automatiquement la configuration VPN après authentification et validation du droit à l'utilisation du VPN SSL.

1. Effectuez un clic-droit sur l'icône SN SSL VPN Client dans la barre des tâches Windows.
2. Cliquez sur **Mode Automatique** pour utiliser ce mode.

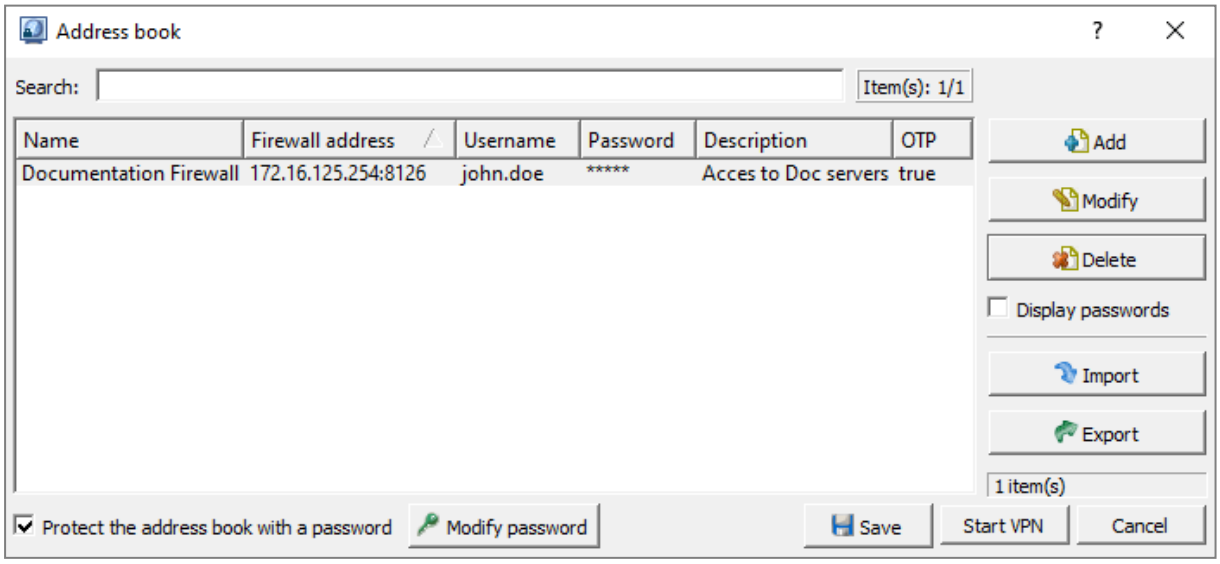
Pour renseigner les informations de connexion et établir un tunnel VPN SSL, poursuivez vers la section Établir un tunnel VPN SSL avec SN SSL VPN Client. Vous pouvez aussi renseigner les informations de connexion dans le carnet d'adresses (voir la section suivante).

Configurer le carnet d'adresses (Mode Automatique requis)

SN SSL VPN Client dispose d'un carnet d'adresses permettant de mémoriser sur le profil de l'utilisateur des adresses (adresse du firewall, identifiant et mot de passe). Le **Mode Automatique** doit être activé pour utiliser le carnet d'adresses.

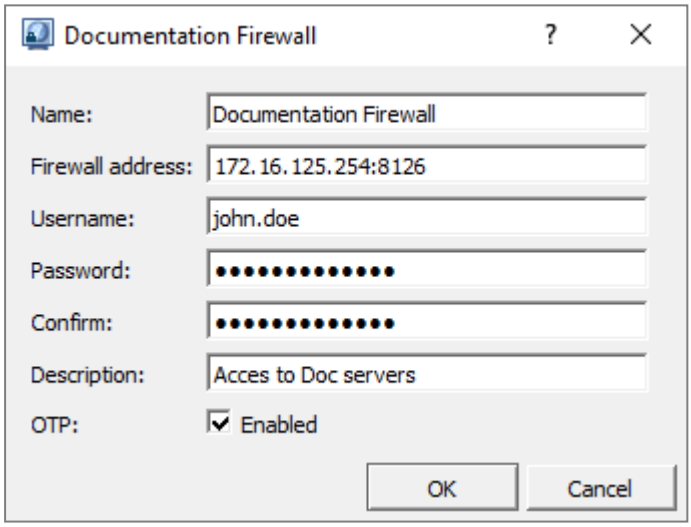
Ouvrir le carnet d'adresses

1. Effectuez un clic-droit sur l'icône SN SSL VPN Client dans la barre des tâches Windows.
2. Cliquez sur **Carnet d'adresses**.
3. Si le carnet d'adresses est protégé par un mot de passe, renseignez-le pour l'ouvrir. Si ce n'est pas le cas, vous pouvez protéger l'accès au carnet d'adresses grâce aux options **Protéger le carnet d'adresses par un mot de passe** et **Modifier le mot de passe**.



Ajouter ou modifier une adresse dans le carnet d'adresses

1. Pour ajouter une nouvelle adresse, cliquez sur **Ajouter**. Pour modifier une adresse existante, sélectionnez-la puis cliquez sur **Modifier**.
2. Dans le champ **Nom**, définissez un nom à l'adresse.
3. Dans le champ **Adresse du firewall**, indiquez l'adresse du firewall SNS (IP ou FQDN) à joindre pour établir le tunnel VPN SSL. Si le port du portail captif du firewall n'est pas celui par défaut (TCP/443), renseignez l'adresse et le port séparés par deux points (adresse:port).
4. Dans le champ **Identifiant**, renseignez l'identifiant de l'utilisateur.
5. Dans les champs **Mot de passe** et **Confirmer**, renseignez le mot de passe de l'utilisateur. Laissez ces champs vides si une méthode d'authentification multifacteur **Code OTP seulement** ou **Mode Push** est utilisée pour la connexion au VPN SSL.
6. Dans le champ **Description**, précisez si nécessaire une description à l'adresse.
7. Cochez **OTP** si une méthode d'authentification multifacteur est utilisée pour la connexion au VPN SSL.
8. Cliquez sur **OK**.



Une fois configuré, poursuivez vers la section Établir un tunnel VPN SSL avec SN SSL VPN Client.

Configurer le Mode Manuel

En **Mode Manuel**, vous importez les éléments de configuration (CA, certificat, clé privée, ...) que SN SSL VPN Client doit utiliser, rassemblés dans un fichier *.ovpn*. Le **Mode Automatique** doit être désactivé pour utiliser ce mode.

1. Récupérez le fichier *.ovpn* :
   - **Depuis le portail captif du firewall SNS hébergeant le service VPN SSL.**
     Authentifiez-vous à l'adresse *https://adresseIP_du_firewall/auth*, puis dans l'onglet **Données personnelles**, cliquez sur *Profil VPN SSL pour clients mobile OpenVPN Connect (fichier unique .ovpn)*,
   - **Depuis l'interface d'administration du firewall SNS.**
     Rendez-vous dans **Configuration > VPN > VPN SSL > Configuration avancée** et cliquez sur **Exporter le fichier de configuration**.
2. Effectuez un clic-droit sur l'icône SN SSL VPN Client dans la barre des tâches Windows et cliquez sur **Mode Manuel > Ajouter un profil**.
3. Sélectionnez le fichier *.ovpn*.

4. Définissez un nom au profil de connexion.
5. Cliquez sur **OK**.

Une fois configuré, poursuivez vers la section Établir un tunnel VPN SSL avec SN SSL VPN Client.

Installer et configurer OpenVPN Connect

Installer OpenVPN Connect

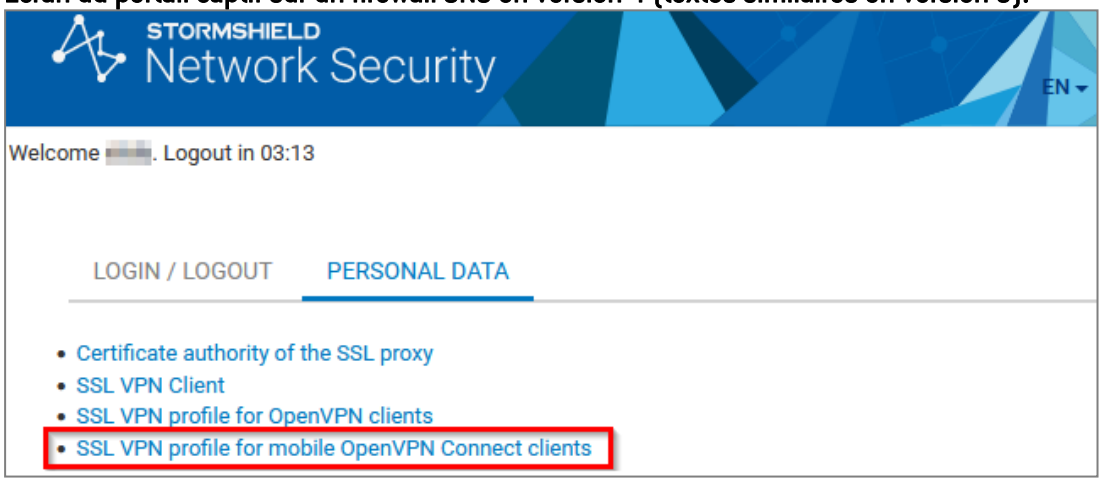
- Sur un poste de travail : téléchargez le logiciel depuis le site web d'OpenVPN et installez-le,
- Sur un terminal mobile : installez l'application depuis le *Google Play Store* ou l'*App Store*.

Configurer OpenVPN Connect

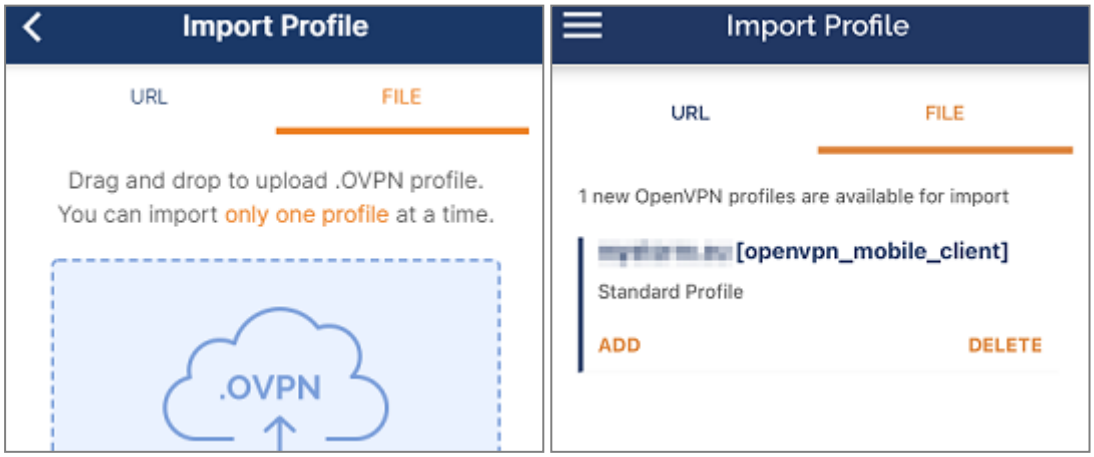
Cette opération est à réaliser à la première connexion ou dès que la configuration VPN SSL du firewall SNS est modifiée, comme après un changement de certificat.

1. Sur votre appareil, authentifiez-vous à l'adresse *https://adresseIP_du_firewall/auth*, puis dans l'onglet **Données personnelles**, cliquez ou appuyez sur **Profil VPN SSL pour clients mobile OpenVPN Connect (fichier unique .ovpn)**.

   Écran du portail captif sur un firewall SNS en version 4 (textes similaires en version 3).



2. Importez le fichier *.ovpn* dans OpenVPN Connect :
   - Sur un poste de travail, ouvrez le logiciel et réalisez l'import dans **Import Profile > File**,
   - Sur un mobile, tentez d'ouvrir le fichier, puis dans les choix proposés par l'appareil, choisissez OpenVPN Connect. La fenêtre **Import Profile > File** apparaît.



3. Suivez ensuite les indications. Aidez-vous du site web d'OpenVPN si nécessaire.

Une fois configuré, poursuivez vers la section Établir un tunnel VPN SSL avec OpenVPN Connect.

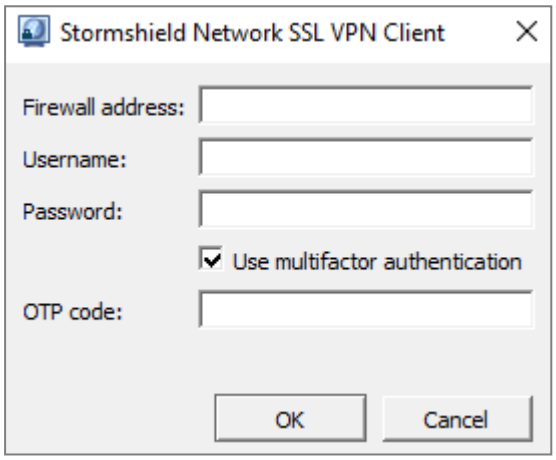
Établir un tunnel VPN SSL

Le firewall SNS et le client VPN SSL étant configurés, vous pouvez établir un tunnel VPN SSL.

Établir un tunnel VPN SSL avec SN SSL VPN Client

Connecter le tunnel VPN SSL en Mode Automatique

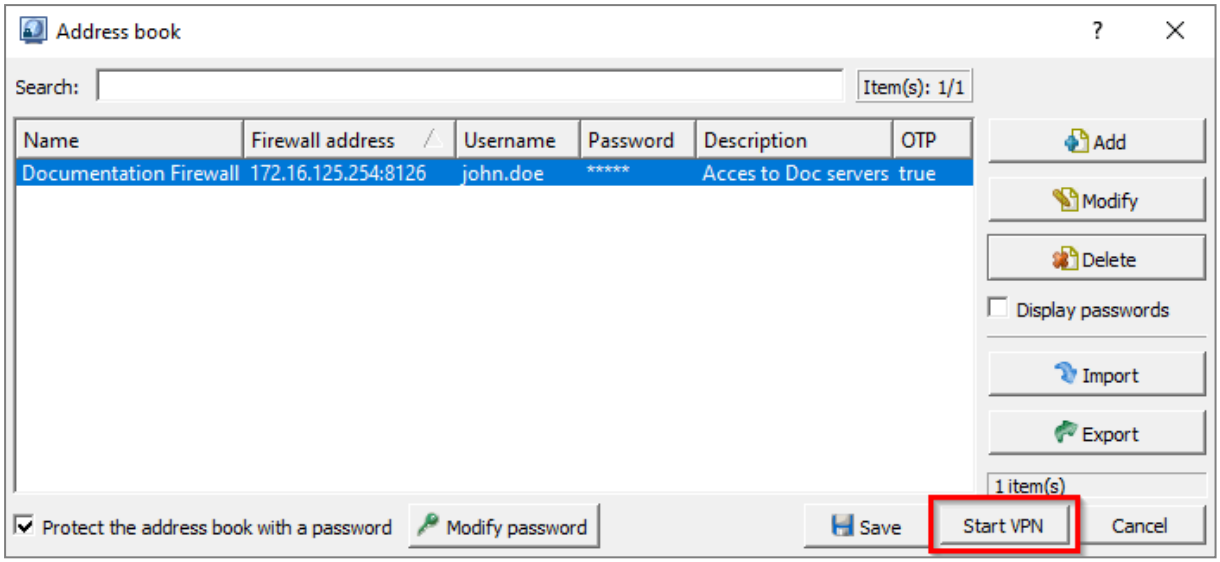
1. Double cliquez sur l'icône SN SSL VPN Client dans la barre des tâches Windows pour ouvrir la fenêtre de connexion.



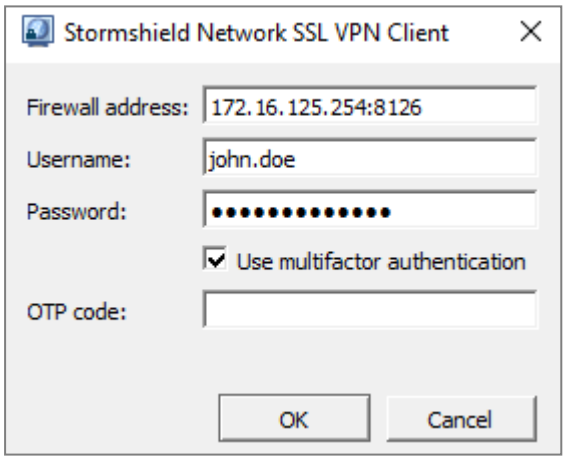
2. Dans le champ **Adresse du firewall**, indiquez l'adresse du firewall SNS (IP ou FQDN) à joindre pour établir le tunnel VPN SSL. Si le port du portail captif du firewall n'est pas celui par défaut (TCP/443), renseignez l'adresse et le port séparés par deux points (adresse:port).
3. Dans le champ **Identifiant**, renseignez l'identifiant de l'utilisateur.
4. Dans le champ **Mot de passe**, renseignez le mot de passe de l'utilisateur. Laissez ce champ vide si une méthode d'authentification multifacteur **Code OTP seulement** ou **Mode Push** est utilisée pour la connexion au VPN SSL.
5. Cochez **Utiliser une authentification multifacteur** si une méthode d'authentification multifacteur est utilisée pour la connexion au VPN SSL.
6. Dans le champ **Code OTP** (apparaît si **Utiliser une authentification multifacteur** est coché), renseignez un mot de passe à usage unique, sauf si une méthode d'authentification multifacteur **Mode Push** est utilisée pour la connexion au VPN SSL.
7. Cliquez sur **OK**. SN SSL VPN Client s'authentifie sur le firewall SNS. Si l'authentification n'aboutit pas, vérifiez les informations de connexion ou que le code OTP (si renseigné) n'est pas expiré.

Connecter le tunnel VPN SSL en utilisant le carnet d'adresses

1. Effectuez un clic-droit sur l'icône SN SSL VPN Client dans la barre des tâches Windows, puis cliquez sur **Carnet d'adresses** pour ouvrir le carnet d'adresses. Le **Mode Automatique** doit être activé pour utiliser le carnet d'adresses.
2. Si le carnet d'adresses est protégé par un mot de passe, renseignez-le pour l'ouvrir.
3. Sélectionnez l'adresse sur laquelle vous connecter et cliquez sur **Connecter**.



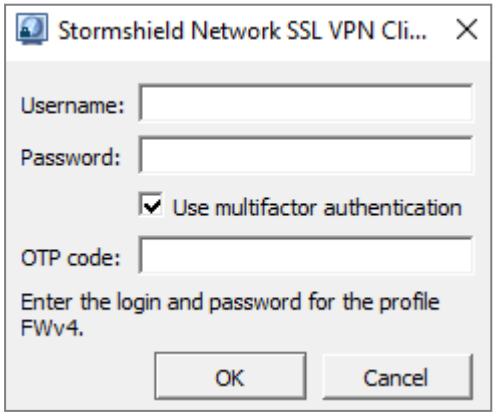
4. Si une méthode d'authentification multifacteur (OTP) est utilisée pour la connexion à cette adresse, renseignez dans le champ **Code OTP** un mot de passe à usage unique. Laissez ce champ vide si une méthode **Mode Push** est utilisée. Cliquez sur **OK**.



5. SN SSL VPN Client s'authentifie sur le firewall SNS. Si l'authentification n'aboutit pas, vérifiez les informations de l'adresse ou que le code OTP (si renseigné) n'est pas expiré.

Connecter le tunnel VPN SSL en Mode Manuel

1. Effectuez un clic-droit sur l'icône SN SSL VPN Client dans la barre des tâches Windows, cliquez sur **Mode Manuel** et sur le profil sur lequel vous connecter.



2. Dans le champ **Identifiant**, renseignez l'identifiant de l'utilisateur.
3. Dans le champ **Mot de passe**, renseignez le mot de passe de l'utilisateur. Laissez ce champ vide si une méthode d'authentification multifacteur **Code OTP seulement** ou **Mode Push** est utilisée pour la connexion au VPN SSL.
4. Cochez **Utiliser une authentification multifacteur** si une méthode d'authentification multifacteur est utilisée pour la connexion au VPN SSL.
5. Dans le champ **Code OTP** (apparaît si **Utiliser une authentification multifacteur** est coché), renseignez un mot de passe à usage unique, sauf si une méthode d'authentification multifacteur **Mode Push** est utilisée pour la connexion au VPN SSL.
6. Cliquez sur **OK**. SN SSL VPN Client s'authentifie sur le firewall SNS selon les informations renseignées dans la fenêtre de connexion et les éléments de configuration du profil. Si l'authentification n'aboutit pas, vérifiez les informations de connexion ou que le code OTP (si renseigné) n'est pas expiré.

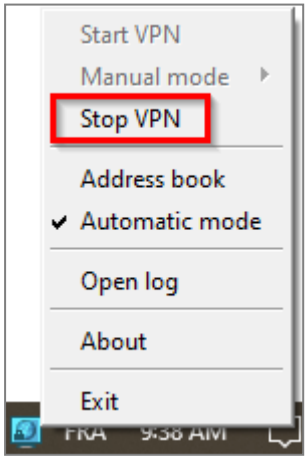
Afficher les informations de connexion du tunnel VPN SSL

La couleur de l'icône du SN SSL VPN Client permet de connaître son état de connexion.

	SN SSL VPN Client est connecté. Survolez l'icône avec la souris afin d'afficher des informations sur le tunnel VPN SSL (nom d'utilisateur et l'adresse du firewall SNS, heure où la connexion s'est établie avec le firewall SNS, adresse IP du poste au travers du tunnel VPN SSL et nombre d'octets échangés).
	SN SSL VPN Client est en train de se connecter.
	SN SSL VPN Client n'est pas connecté ou une tentative de connexion a échoué.

Déconnecter le tunnel VPN SSL

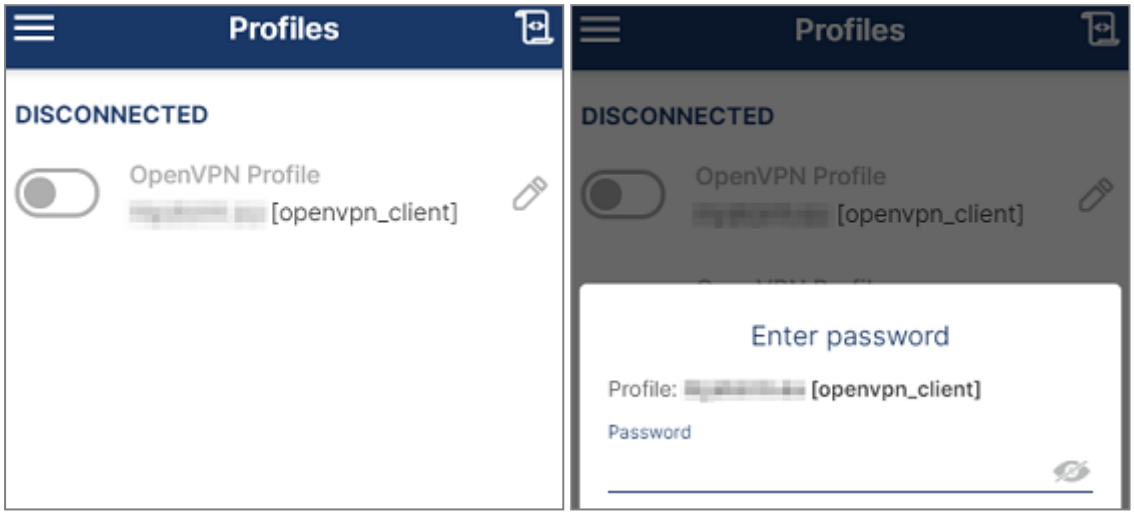
1. Effectuez un clic-droit sur l'icône SN SSL VPN Client  dans la barre des tâches Windows.
2. Cliquez sur **Déconnecter**.



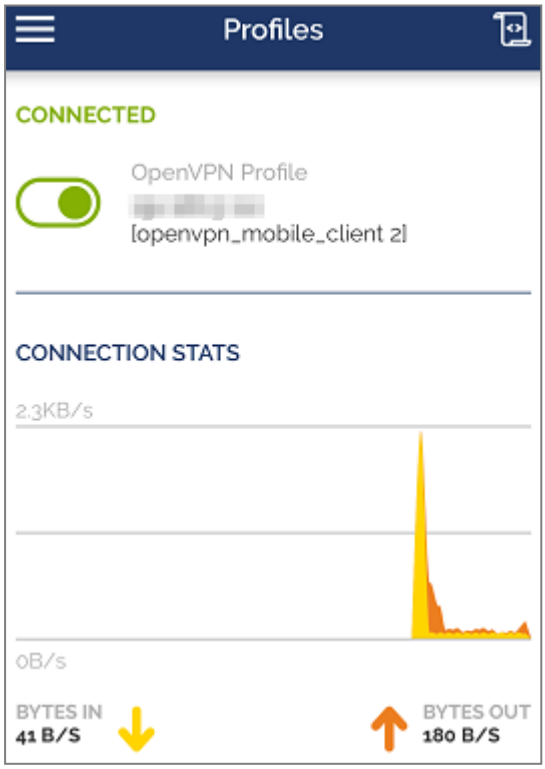
Établir un tunnel VPN SSL avec OpenVPN Connect

Connecter le tunnel VPN SSL

1. Lancez le logiciel ou l'application OpenVPN Connect.
2. Pour le profil souhaité, glissez le curseur de connexion vers la droite ou cliquez dessus.
3. Si le mot de passe de l'utilisateur n'a pas été sauvegardé, renseignez-le.



4. OpenVPN Connect s'authentifie sur le firewall SNS. Lorsque la connexion est établie, des informations concernant le tunnel VPN SSL s'affichent.



Déconnecter le tunnel VPN SSL

Glissez le curseur de connexion vers la gauche ou cliquez dessus.

Consulter les journaux (logs)

Sur l'interface d'administration du firewall SNS

Certaines informations sont accessibles uniquement 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** en version SNS 4 ou sur **Accès restreint aux logs** en version SNS 3 dans le bandeau supérieur. Pour plus d'informations, reportez-vous sur la note technique Se conformer aux règlements sur les données personnelles.

En version SNS 4.x

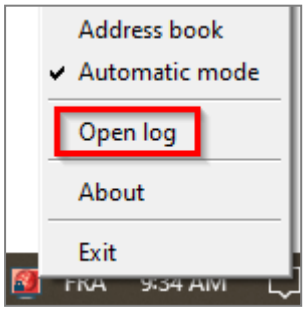
- Dans **Monitoring > Logs - Journaux d'audit > VPN**, ce journal affiche les informations relatives aux différents types de tunnels VPN (SSL, IPsec),
- Dans **Monitoring > Supervision > Utilisateurs**, ce journal affiche notamment les événements liés aux authentifications via tunnels VPN SSL. Filtrez le contenu du journal sur la méthode d'authentification *Open VPN* pour les afficher,
- Dans **Monitoring > Supervision > Tunnels VPN SSL**, ce journal affiche des informations concernant les sessions des utilisateurs actuellement connectés en VPN SSL.

En version SNS 3.x

- Dans **Logs - Journaux d'Audit > Vues > VPN**, cette vue affiche les informations relatives aux différents types de tunnels VPN (SSL, IPsec),
- Dans **Journaux d'Audit > Journaux > VPN SSL**, ce journal affiche les événements d'authentification d'utilisateurs, de création et de suppression de tunnels VPN SSL,
- Dans **Supervision > Utilisateurs**, ce journal affiche notamment les événements liés aux authentifications via tunnels VPN SSL. Filtrez le contenu du journal sur la méthode d'authentification *Open VPN* pour les afficher,
- Dans **Supervision > Tunnels VPN SSL**, ce journal affiche des informations concernant les sessions des utilisateurs actuellement connectés en VPN SSL.

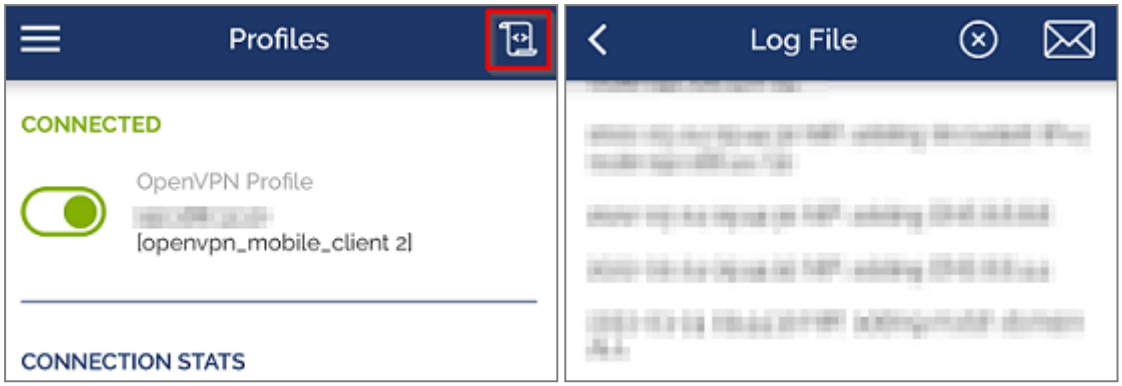
Sur SN SSL VPN Client

1. Effectuez un clic-droit sur l'icône SN SSL VPN Client dans la barre des tâches Windows.
2. Cliquez sur **Journaux (logs)**.



Sur OpenVPN Connect

Pour accéder aux journaux (logs) d'OpenVPN Connect, sur la fenêtre des profils, cliquez sur l'icône en forme de journal située en haut à droite.


Profiles
CONNECTED
OpenVPN Profile
[openvpn_mobile_client 2]
CONNECTION STATS
Log File

Résoudre les problèmes

Ce chapitre liste certains problèmes fréquemment rencontrés lors de l'utilisation du SN SSL VPN Client. Si celui que vous rencontrez ne se trouve pas dans ce chapitre, nous vous recommandons de consulter la Base de connaissances Stormshield.

Le tunnel ne s'établit pas et le message "*Veuillez patienter pendant la connexion au service local*" reste affiché.

- *Situation* : Lors de la tentative de connexion au VPN SSL, le tunnel ne s'établit pas et le message "*Connexion au firewall impossible : Echec de résolution du nom de l'UTM*" persiste.
- *Cause* : L'utilisateur qui se connecte n'est pas dans le groupe "OpenVPN Administrators" sur le poste de travail qu'il utilise.
- *Solutions* :
  - Mettre à jour SN SSL VPN Client en version 3.2.3.
  - Pour une version inférieure à 3.2.3, vérifiez que l'utilisateur appartient au groupe local "OpenVPN Administrators" en exécutant dans l'invite de commandes Windows `net localgroup "OpenVPN Administrators"`. Pour ajouter manuellement l'utilisateur au groupe, exécutez `net localgroup "OpenVPN Administrators" "myuser" /add` (remplacez myuser par l'utilisateur concerné).

Le tunnel ne s'établit pas et le message "*Connexion au firewall impossible : Echec de résolution du nom de l'UTM*" s'affiche.

- *Situation* : Lors de la tentative de connexion au VPN SSL, le tunnel ne s'établit pas et le message "*Connexion au firewall impossible : Echec de résolution du nom de l'UTM*" s'affiche.
- *Cause* : L'adresse renseignée est incorrecte ou n'est pas joignable.
- *Solution* : Vérifiez que l'adresse du firewall renseignée est correcte.

Le tunnel ne s'établit pas et le message "*Identifiant ou mot de passe incorrect*" s'affiche.

- *Situation* : Lors de la tentative de connexion au VPN SSL, le tunnel ne s'établit pas et le message "*Identifiant ou mot de passe incorrect*" s'affiche.
- *Cause* : Le mot de passe de l'utilisateur est incorrect ou ce dernier ne dispose pas des droits pour s'authentifier en VPN SSL.
- *Solutions* :
  - Vérifiez que l'identifiant et le mot de passe sont corrects.
  - Sur le firewall SNS, vérifiez que la **Politique VPN SSL** est paramétrée sur **Autoriser** dans **Configuration > Utilisateurs > Droits d'accès**, onglet **Accès par défaut** et que l'utilisateur ou le groupe d'utilisateurs concerné est autorisé à établir un tunnel VPN SSL dans **Configuration > Utilisateurs > Droits d'accès**, onglet **Accès détaillé**.

Le tunnel ne s'établit pas et le message "*Erreur lors de la connexion au service : Connection refused*" s'affiche.

- *Situation* : Lors de la tentative de connexion au VPN SSL, le tunnel ne s'établit pas et le message "*Erreur lors de la connexion au service : Connection refused*" s'affiche.
- *Cause* : Le service **Stormshield SSL VPN Service** n'est pas démarré ou ne fonctionne pas.
- *Solution* : Vérifiez que le service Windows **Stormshield SSL VPN Service** est bien démarré sur le poste de travail. Vous pouvez également essayer de redémarrer le service.

Le tunnel ne s'établit pas et les journaux contiennent le message "*Route: Waiting for TUN/TAP interface to come up...*".

- *Situation* : Lors de la tentative de connexion au VPN SSL, le tunnel ne s'établit pas et le message "*Erreur lors de la connexion au service : Connection refused*" s'affiche dans les journaux.
- *Cause* : Un problème avec l'interface **TAP-Windows Adapter** empêche le tunnel VPN de s'établir.
- *Solution* : Dans le **Centre Réseau et Partage** Windows, cliquez sur **Modifier les paramètres de la carte**, effectuez un clic-droit sur l'interface **TAP-Windows Adapter** et cliquez sur **Diagnostiquer**.

Une ressource de l'entreprise n'est pas accessible via le tunnel VPN

- *Situation* : Le tunnel est établi, mais une ressource de l'entreprise n'est pas accessible.
- *Cause* : La politique de filtrage du firewall bloque l'accès à cette ressource ou cette dernière n'est plus accessible. D'autres raisons peuvent être la cause de cette situation.
- *Solutions* :
  - Sur le firewall SNS, vérifiez que les règles de filtrage autorisent l'accès à la ressource et que les journaux ne contiennent pas de trace d'un éventuel blocage de flux (dans **Monitoring > Logs - Journaux d'audit > Filtrage** pour les versions SNS 4.x ou dans **Journaux d'Audit > Journaux > Filtrage** pour les versions SNS 3.x),
  - Assurez-vous que la ressource demandée est bien physiquement disponible,
  - Videz le cache ARP de la machine en tapant la commande `arp -d *` dans une console.

Le tunnel VPN se ferme lors de l'envoi d'un fichier dont le poids est très important

- *Situation* : Lors de l'envoi d'un fichier volumineux, le tunnel VPN se ferme.
- *Cause* : Le fichier envoyé est trop volumineux.
- *Solution* : Réalisez l'envoi du fichier en utilisant un protocole qui utilise des blocs plus petits (comme FTP) ou en établissant le tunnel en UDP.

Pour aller plus loin

Des informations complémentaires et réponses à vos éventuelles questions sur le VPN SSL sont disponibles dans la **base de connaissances Stormshield** (authentification nécessaire).

STORMSHIELD

documentation@stormshield.eu