NOTE TECHNIQUE

STORMSHIELD NETWORK SECURITY

CONFIGURER ET UTILISER LE VPN SSL DES FIREWALLS SNS

Produits concernés : SN SSL VPN Client 4 et SNS 4

Dernière mise à jour du document : 13 novembre 2024

Référence : sns-fr-tunnels_vpn_ssl_note_technique

Table des matières

Historique des modifications

Date	Description

13 novembre 2024	• Sortie du client VPN SSL Stormshield 4.0.9 EA.
	• Ajout d'un paragraphe "Limitations et précisions sur les cas d'utilisation" dans la section "Spécificités du client VPN SSL Stormshield".
	• Modification des informations concernant l'utilisation du Mode Push :
	  ◦ Avec le carnet d'adresses dans la section "Configurer le client VPN SSL Stormshield",
	  ◦ Dans la section "Établir un tunnel VPN avec le client VPN SSL Stormshield".
	• Suppression de la note concernant les utilisateurs partageant un poste de travail Windows avec d'autres utilisateurs dans la section "Établir un tunnel VPN avec le client VPN SSL Stormshield".

7 octobre 2024	• Ajout de précisions sur le délai avant renégociation des clés dans la section "Configurer le service VPN SSL".
	• Ajout de précisions concernant l'utilisation du Mode Push :
	  ◦ Avec le carnet d'adresses dans la section "Configurer le client VPN SSL Stormshield",
	  ◦ Dans la section "Établir un tunnel VPN avec le client VPN SSL Stormshield".

22 août 2024	• Sortie du client VPN SSL Stormshield 4.0.
	• Le contenu lié à OpenVPN Connect a été déplacé dans une annexe et celui du client VPN SSL Stormshield dispose à présent de ses propres sections.
	• Le contenu lié au client VPN SSL Stormshield a été enrichi :
	  ◦ Ajout de nouvelles spécificités,
	  ◦ Ajout du format *.exe* pour le programme d'installation,
	  ◦ Ajout des procédures de déploiement via une stratégie de groupe (GPO) et via un script,
	  ◦ Modification du nom de certains champs dans les procédures,
	  ◦ Ajout d'informations concernant les journaux disponibles.
	• Le contenu de la section "Suivre les utilisateurs connectés au VPN SSL sur le firewall SNS" a été enrichi.
	• Ajout du cas de la mise en œuvre d'un accès réseau *Zero Trust* (ZTNA).

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 l'authentification de l'utilisateur dans un canal de communication TLS chiffré par des certificats serveur et client communs signés par une autorité de certification (CA) présente sur le firewall SNS. Cette solution garantit donc confidentialité, intégrité et non-répudiation.

Cette note technique présente :

- L'activation et la configuration du service VPN SSL des firewalls SNS en version 4.x,
- La mise en œuvre d'un accès réseau *Zero Trust* (ZTNA) avec des firewalls SNS en version 4.8 ou supérieure et des clients VPN SSL Stormshield en version 4.0 ou supérieure,
- L'installation du client VPN SSL Stormshield en version 4.x, sa configuration, son utilisation jusqu'à l'établissement d'un tunnel VPN SSL, certaines de ses spécificités (compatibilités, modes de connexion, ...) et l'accès à ses journaux,
- Le suivi des utilisateurs connectés au VPN SSL,
- Certaines informations concernant le logiciel OpenVPN Connect.

Dans la suite du document, SN SSL VPN Client peut également être nommé "client VPN SSL Stormshield".

NOTE
Si vous utilisez le client VPN SSL Stormshield en version 3.x, reportez-vous à la note technique Configurer et utiliser le VPN SSL des firewalls SNS avec le VPN SSL Client v3 (PDF uniquement).

Prérequis

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

Disposer d'un client VPN SSL compatible

Chaque poste de travail ou terminal mobile doit disposer d'un client VPN compatible pour établir des tunnels VPN SSL avec le firewall SNS. Les clients VPN compatibles sont :

- **SN SSL VPN Client** : cette note technique présente son installation, sa configuration, son utilisation jusqu'à l'établissement d'un tunnel VPN SSL, certaines de ses spécificités (compatibilités, modes de connexion, ...) et l'accès à ses journaux,
- **OpenVPN Connect** : pour plus d'informations, reportez-vous à la section Annexe : installer, configurer et utiliser OpenVPN Connect,
- **SN VPN Client Standard** : pour plus d'informations, reportez-vous au document SN VPN Client Standard User Guide (anglais uniquement),
- **SN VPN Client Exclusive** : pour plus d'informations, reportez-vous au Guide de l'administrateur SN VPN Client Exclusive.

Pour plus d'informations sur les versions et les systèmes d'exploitation compatibles des logiciels Stormshield, reportez-vous au Guide de cycle de vie Network Security & Tools.

Disposer d'un firewall SNS adapté

Le nombre maximal de tunnels VPN SSL autorisés par les firewalls SNS est différent selon le modèle utilisé. Choisissez un modèle adapté à vos besoins. Retrouvez cette information sur le site de Stormshield, rubrique Gamme produits (SNS) en sélectionnant votre modèle.

Avoir connecté le firewall SNS à un annuaire

Le firewall SNS doit être connecté à un annuaire pour afficher dans ses modules les listes d'utilisateurs et groupes d'utilisateurs. Ceci permettra de définir les utilisateurs et groupes d'utilisateurs autorisés à établir des tunnels VPN SSL.

Vérifiez cette connexion dans l'interface d'administration du firewall SNS dans **Configuration > Utilisateurs > Authentification**, onglet **Méthodes disponibles**. Une ligne **LDAP** doit apparaître dans la grille. Pour plus d'informations sur la configuration des annuaires, reportez-vous à la section Configuration des annuaires du *manuel utilisateur 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 :

- Aux clients VPN SSL Stormshield de récupérer leur configuration VPN SSL,
- Au firewall SNS et aux clients VPN SSL Stormshield d'appliquer la politique de vérification de la conformité des postes clients dans le cas où un accès réseau *Zero Trust* est utilisé.

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 sur la configuration du portail captif, reportez-vous à la section Authentification du *manuel utilisateur de la version SNS utilisée*.

Cas de l'authentification multifacteur

Dans le cas où une authentification multifacteur pour les connexions VPN SSL est utilisée :

Pour une authentification multifacteur utilisant la solution TOTP Stormshield

- Le firewall SNS doit être en version 4.5 ou supérieure,
- La solution TOTP doit être déjà configurée. Pour plus d'informations, reportez-vous à la note technique Configurer et utiliser la solution TOTP Stormshield.

Pour une authentification multifacteur utilisant une solution tierce et un serveur RADIUS

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

Cas de la mise en œuvre d'un accès réseau *Zero Trust* (ZTNA)

Dans le cas où un accès réseau *Zero Trust* est utilisé :

- Le firewall SNS doit être en version 4.8 ou supérieure,
- Chaque poste de travail doit utiliser le client VPN SSL Stormshield en version 4.0 ou supérieure,
- Le Client VPN SSL Stormshield doit être configuré en mode automatique.

NOTE

Un accès réseau *Zero Trust* (ZTNA) consiste à ne faire confiance aux utilisateurs et aux appareils qu'après leur vérification. On parle d'accès réseau *Zero Trust* (ZTNA) lorsque plusieurs composantes sont réunies :

- Une garantie de la conformité du canal de communication grâce au chiffrement TLS des tunnels VPN,
- Une vérification des utilisateurs grâce à l'authentification multifacteur (par exemple avec la solution TOTP Stormshield),
- Une politique de vérification de la conformité des postes clients et des utilisateurs,
- Un filtrage fin pour limiter l'accès des utilisateurs aux seules ressources nécessaires.

Les sections suivantes de cette note technique abordent la configuration de ces éléments. Il est indispensable de tous les configurer pour mettre en œuvre un accès réseau *Zero Trust* (ZTNA).

Spécificités du client VPN SSL Stormshield

Cette section présente certaines spécificités du client VPN SSL Stormshield.

Compatibilité

Versions et systèmes d'exploitation compatibles

Pour plus d'informations, reportez-vous au Guide de cycle de vie Network Security & Tools.

Méthodes d'authentification multifacteur compatibles

- Mot de passe + Code OTP.
  Cette méthode est compatible avec la solution TOTP Stormshield. Le firewall SNS doit être en version 4.5 ou supérieure pour utiliser cette solution,
- Code OTP seulement,
- Mode Push (utilisation d'une application tierce pour approuver la connexion).

Modes de connexion

Mode automatique

Avec ce mode, le client VPN SSL Stormshield récupère automatiquement et de manière sécurisée sa configuration VPN SSL sur le firewall SNS. Il fonctionne de la manière suivante :

À la première connexion :

- Le client VPN SSL Stormshield s'authentifie une première fois sur le firewall SNS :
  - Le client VPN SSL Stormshield récupère automatiquement sa configuration VPN ,
  - Le firewall SNS et le client VPN SSL Stormshield appliquent la politique de vérification de la conformité des postes clients (cas du ZTNA).
- Si la première authentification aboutit, le client VPN SSL Stormshield s'authentifie une seconde fois sur le firewall SNS afin d'établir le tunnel VPN SSL.

Lors des connexions suivantes :

- Le client VPN SSL Stormshield vérifie si une nouvelle configuration VPN est disponible :
  - S'il n'existe pas de nouvelle configuration, le client VPN SSL Stormshield s'authentifie sur le firewall SNS afin d'établir le tunnel VPN SSL,
  - Si une nouvelle configuration est disponible, le client VPN SSL Stormshield s'authentifie deux fois comme lors d'une première connexion.

Mode manuel

Avec ce mode, vous devez importer la configuration VPN dans un profil de connexion.

Vous pouvez récupérer la configuration VPN (fichier *.ovpn*) depuis le portail captif du firewall hébergeant le service VPN SSL ou depuis l'interface d'administration du firewall. Cette manipulation est décrite dans la section Récupérer la configuration VPN SSL (fichier .ovpn).

Matrice de compatibilité des modes de connexion

Ce tableau récapitule les fonctionnalités compatibles selon le mode de connexion utilisé.

Fonctionnalité	Mode automatique	Mode manuel
Carnet d'adresses	✓	✗
Gestion des profils	✗	✓
Vérification de la conformité des postes clients (ZTNA) *Version SNS 4.8 ou supérieure requise*	✓	✗

Fonctionnalités du client VPN SSL Stormshield

Carnet d'adresses (Mode automatique requis)

Le client VPN SSL Stormshield dispose d'un carnet d'adresses permettant de mémoriser les informations de connexion à différents firewalls : adresse de connexion au firewall (adresse IPv4 ou FQDN), identifiant, mot de passe et utilisation d'une authentification multifacteur.

Exécution de scripts

Sous Windows, le client VPN SSL Stormshield peut exécuter automatiquement des scripts sur le poste de travail de l'utilisateur à chaque ouverture et fermeture d'un tunnel VPN SSL. Pour cela, vous devez au préalable ajouter les scripts à exécuter dans la configuration du service VPN SSL du firewall SNS. Cette manipulation est décrite dans la section Scripts à exécuter sur le client.

Limitations et précisions sur les cas d'utilisation

Mise à jour vers une version inférieure à la version 4

La mise à jour vers une version inférieure à la version 4 de SN SSL VPN Client n'est pas supportée.

Lorsqu'un carnet d'adresses provenant d'une version 3 de SN SSL VPN Client est ouvert avec une version 4, son format est mis à jour automatiquement et il ne peut plus être utilisé avec une version 3. Si nécessaire, vous pouvez conserver une copie du fichier du carnet d'adresses en version 3 avant de mettre à jour SN SSL VPN Client en version 4.

Affichage de l'icône dans la barre des tâches sous Windows 11

Sous Windows 11, assurez-vous que l'affichage de l'icône de SN SSL VPN Client dans la barre des tâches Windows est activé dans **Paramètres de la barre des tâches > Autres icônes de barre d'état système > Menu d'icône masqué**. Dans le cas contraire, les fonctionnalités de SN SSL VPN Client sont inaccessibles car elles nécessitent un accès à l'icône du logiciel pour en ouvrir le menu.

Configurer le firewall SNS

La mise en œuvre de tunnels VPN SSL nécessite de configurer plusieurs modules dans l'interface web d'administration du firewall SNS.

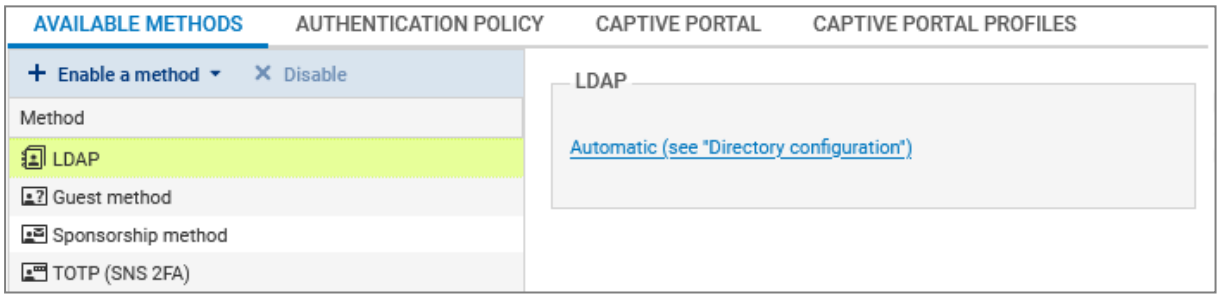
Configurer l'authentification

Même si certains éléments mentionnés dans la section Prérequis sont déjà configurés, prenez quelques instants pour les vérifier.

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

Cas de l'authentification multifacteur et de l'accès réseau *Zero Trust* (ZTNA)

Pour les cas de l'authentification multifacteur et de l'accès réseau *Zero Trust*, vous devez avoir déjà configuré la méthode permettant d'utiliser l'authentification multifacteur choisie. Vous pouvez le vérifier dans l'onglet **Méthodes disponibles**.



Pour une authentification multifacteur utilisant la solution TOTP Stormshield

Vous devez avoir configuré la méthode TOTP. Pour plus d'informations, reportez-vous à la note technique Configurer et utiliser la solution TOTP Stormshield.

Pour une authentification multifacteur utilisant une solution tierce et un serveur RADIUS

Vous devez avoir configuré :

- La solution d'authentification multifacteur tierce connectée à votre serveur RADIUS,
- La méthode RADIUS permettant de connecter le firewall SNS à votre serveur RADIUS. Pour plus d'informations sur la configuration de la méthode RADIUS, reportez-vous à la section Authentification du *manuel utilisateur de la version SNS utilisée*.

Par défaut, le délai d'inactivité autorisé pour se connecter à un serveur RADIUS est de 3000 millisecondes (3 secondes). Dans le cas où une authentification multifacteur **Mode Push** est utilisée, vous devez modifier ce délai pour laisser aux utilisateurs suffisamment de temps pour s'authentifier. Par exemple pour 30 secondes, utilisez les commandes CLI / Serverd suivantes :

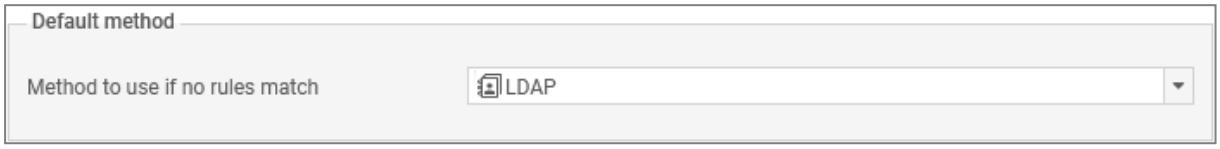
```
CONFIG AUTH RADIUS timeout=30000 btimeout=30000
CONFIG AUTH ACTIVATE
```

Pour un accès réseau *Zero Trust* (ZTNA)

Du fait que la mise en œuvre d'un accès réseau *Zero Trust* nécessite une vérification des utilisateurs grâce à l'authentification multifacteur, vous devez avoir configuré la méthode TOTP ou RADIUS. Pour plus d'informations, reportez-vous aux cas ci-dessus.

Configurer la politique d'authentification

Vous retrouvez dans l'onglet **Politique d'authentification** le champ **Méthode à utiliser si aucune règle ne peut être appliquée**. Poursuivez 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 d'une authentification multifacteur, ...), vous devez ajouter au moins deux règles en cliquant sur **Nouvelle règle > Règle standard**.

Pour augmenter la sécurité, vous pouvez créer des règles spécifiques pour des groupes d'utilisateurs différents. À noter que les règles sont examinées dans l'ordre de leur numérotation lors d'une authentification.

Pour la première règle :

1. Dans l'onglet **Utilisateur**, champ **Utilisateur ou groupe**, sélectionnez le groupe d'utilisateurs concerné. *Any user@* concerne tous les utilisateurs du domaine,
2. Dans l'onglet **Source**, ajoutez l'interface externe par laquelle l'authentification sera réalisée (par exemple *out*),
3. Dans l'onglet **Méthodes d'authentification** :
   - Supprimez la ligne *Méthode par défaut* et activez la méthode (*LDAP*, *RADIUS*, ...) permettant de se connecter au portail captif du firewall et de récupérer la configuration VPN,
   - Dans le cas où la solution TOTP Stormshield est utilisée, positionnez à "**On**" l'utilisation d'un mot de passe à usage unique.

Pour la seconde règle :

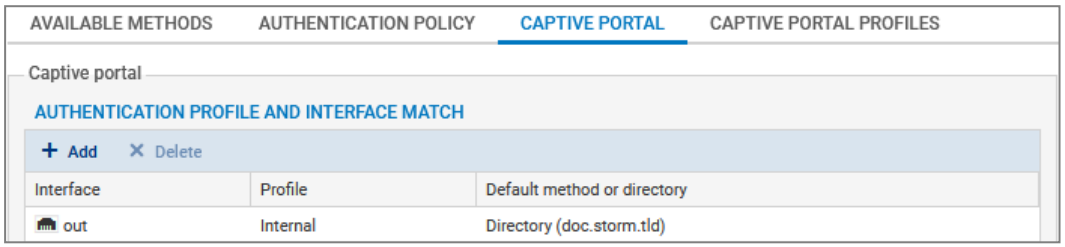
1. Dans l'onglet **Utilisateur**, champ **Utilisateur ou groupe**, sélectionnez le groupe d'utilisateurs concerné. *Any user@* concerne tous les utilisateurs du domaine,
2. Dans l'onglet **Source**, ajoutez l'interface *VPN SSL*,
3. Dans l'onglet **Méthodes d'authentification** :
   - Supprimez la ligne *Méthode par défaut* et activez la méthode (*LDAP*, *RADIUS*, ...) permettant d'établir les tunnels VPN SSL,
   - Dans le cas où la solution TOTP Stormshield est utilisée, positionnez à "**On**" l'utilisation d'un mot de passe à usage unique.

Configurer le portail captif

Correspondance entre profil d'authentification et interface

1. Dans l'onglet **Portail captif**, grille **Correspondance entre profil d'authentification et interface**, 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 correspond à celui des utilisateurs se connectant au VPN SSL : le profil est correctement pré-configuré. Les utilisateurs pourront simplement indiquer dans la fenêtre de connexion du client VPN SSL leur identifiant pour se connecter,



   - En cas contraire : les utilisateurs devront indiquer en plus de leur identifiant le domaine concerné (par exemple : *identifiant@domain.tld*). Pour changer ce comportement :
     - Sélectionnez un autre profil (par exemple *default05*),
     - Rendez-vous dans l'onglet **Profils du Portail captif** et sélectionnez cet autre profil,
     - Choisissez le bon annuaire dans le champ **Méthode ou annuaire par défaut**,
     - Activez le portail captif dans la zone **Configuration avancée**.

Serveur SSL - Certificat (clé privée) du portail captif

Vous pouvez sélectionner le certificat présenté par le portail captif du firewall SNS dans le champ correspondant.

Dans le cas où l'un des critères ci-dessous s'applique au certificat sélectionné :

- Le certificat n'est pas signé par une autorité de certification compétente,
- L'autorité de certification n'est pas déployée sur le poste de travail des utilisateurs,
- Le **CN** du certificat ne correspond pas à l'adresse du firewall qui sera utilisée pour les connexions au VPN SSL.

Alors, à la première connexion au VPN SSL, chaque utilisateur verra une fenêtre s'afficher indiquant que le certificat n'est pas de confiance. Pour se connecter, chaque utilisateur devra alors indiquer que le certificat est de confiance. Même si ce message n'est pas bloquant, il est recommandé de sensibiliser vos utilisateurs s'il s'agit d'un comportement attendu.

Par exemple, si vous utilisez le certificat auto-signé créé à l'initialisation du firewall SNS et qui est présenté par défaut par le firewall, ce message s'affichera.

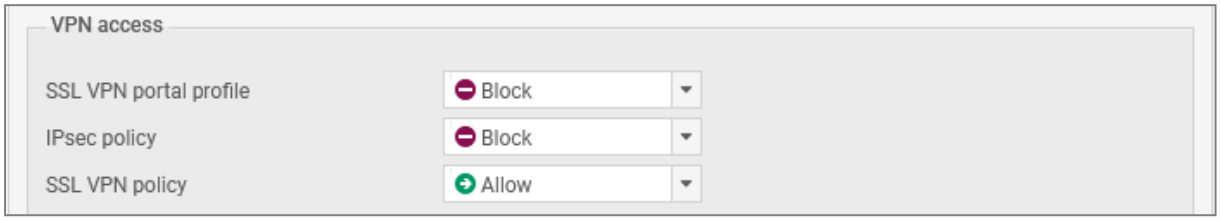
Attribuer les droits d'accès au VPN SSL

Vous devez attribuer des droits pour autoriser les utilisateurs à établir des tunnels VPN SSL.

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

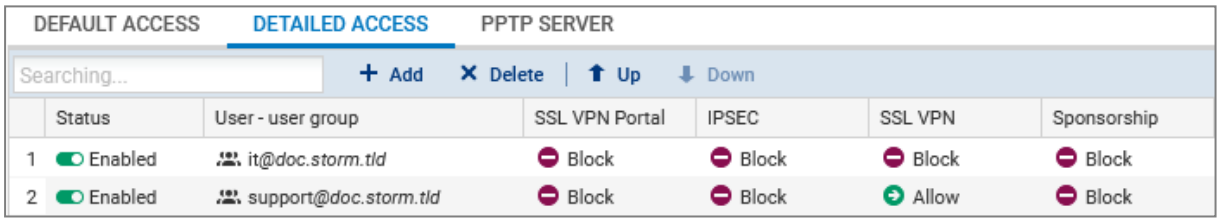
Autoriser tous les utilisateurs à établir des tunnels VPN SSL

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



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.



Configurer le service VPN SSL

Cette section explique comment activer le service VPN SSL et configurer ses paramètres généraux. Pour le cas du ZTNA, cette section présente également la configuration d'une politique de vérification de la conformité des postes clients et des utilisateurs.

Rendez-vous dans le module **Configuration > VPN > VPN SSL**.

Activer le service VPN SSL

Positionnez le curseur d'état sur **ON** pour activer le service VPN SSL.

En version SNS 4.8 ou supérieure, deux onglets permettent respectivement de configurer les paramètres généraux du service VPN SSL et de configurer la politique de vérification de la conformité des postes clients (cas du ZTNA).

Configurer les paramètres généraux du service

Plusieurs zones sont disponibles. Modifiez la configuration selon les informations ci-dessous.

Zone Paramètres réseaux

Champ	Description
Adresse IP (ou FQDN) de l'UTM utilisée	Indiquez l'adresse que les utilisateurs devront utiliser pour joindre le firewall SNS afin d'établir des tunnels VPN SSL. • Pour une adresse IP : elle doit être publique, donc accessible sur Internet, • Pour un FQDN (exemple : *ssl.company.tld*) : il doit être déclaré dans les serveurs DNS utilisés par le poste de travail 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 dans le module **Configuration > Réseau > DNS dynamique**.
Réseaux ou machines accessibles	Sélectionnez l'objet représentant les réseaux ou machines qui seront joignables au travers du tunnel VPN. Cet objet permet de définir automatiquement sur le poste de travail 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 postes de travail 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.
Réseau assigné aux clients (UDP) **Réseau assigné aux clients (TCP)**	Sélectionnez l'objet correspondant au réseau qui sera assigné aux clients VPN en UDP et en TCP. Vous pouvez assigner un réseau différent, mais le client VPN choisira toujours en premier le réseau UDP pour de meilleures performances. Concernant le choix du réseau ou des sous-réseaux : • La taille minimale du masque réseau est de /28, • Le réseau dédié aux clients VPN ne doit pas appartenir aux réseaux internes existants ou déclarés par une route statique sur le firewall. L'interface utilisée pour le VPN SSL étant protégée, le firewall détecterait alors une tentative d'usurpation d'adresse IP (*spoofing*) et bloquerait les flux correspondants, • Afin d'éviter des conflits de routage, choisissez des sous-réseaux peu communément utilisés (comme 10.**60.77**.0/24) car de nombreux réseaux d'accès à Internet filtrés (Wi-Fi public, hôtels) ou réseaux locaux privés utilisent déjà les premières plages d'adresses réservées.
Maximum de tunnels simultanés autorisés	Le nombre s'affiche automatiquement. Il correspond à la valeur minimale entre : • Le nombre maximal de tunnels autorisés sur le firewall SNS (voir Prérequis), • Le nombre de sous-réseaux disponibles pour les clients VPN. Cela représente 1/4 des adresses IP, moins 2. Un tunnel VPN SSL consomme en effet 4 IP et le serveur réserve 2 sous-réseaux pour son propre usage.

Zone Paramètres DNS envoyés au client

Champs	Description
Nom de domaine	Indiquez le nom de domaine attribué aux clients VPN SSL pour leur permettre d'effectuer leurs résolutions de noms d'hôtes.

Champs	Description
Serveur DNS primaire **Serveur DNS secondaire**	Sélectionnez l'objet représentant le serveur DNS à attribuer.

Zone Configuration avancée

Champ	Description
Adresse IP de l'UTM pour le VPN SSL (UDP)	Dans l'un des cas suivants, vous devez sélectionner l'objet représentant l'adresse IP à utiliser pour établir les tunnels VPN SSL en UDP : • 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.
Port (UDP) **Port (TCP)**	Vous pouvez modifier les ports d'écoute du service VPN SSL. À noter que : • Certains ports sont réservés à un usage interne du firewall SNS et ne peuvent pas être sélectionnés, • Le port 443 est le seul port inférieur à 1024 qui peut être utilisé, • 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).
Délai avant renégociation des clés (secondes)	Vous pouvez modifier le délai (par défaut 14400 secondes, soit 4 heures) au terme duquel les clés utilisées par les algorithmes de chiffrement sont renégociées. Pendant cette opération : • Le tunnel VPN SSL ne répondra pas pendant quelques secondes, • Si une authentification multifacteur est utilisée, l'utilisateur devra renseigner un nouveau code OTP ou approuver la nouvelle connexion sur son application tierce (Mode Push) afin de rester connecté. Il peut être intéressant d'augmenter le délai pour l'aligner sur la durée moyenne d'une journée travaillée, par exemple à 28800 secondes (8 heures).
Utiliser les serveurs DNS fournis par le firewall	Vous pouvez indiquer aux clients VPN d'inscrire 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.
Interdire l'utilisation de serveurs DNS tiers	Vous pouvez indiquer aux clients VPN d'exclure les serveurs DNS déjà définis dans la configuration du poste de travail (Windows uniquement). Seuls ceux envoyés par le firewall SNS pourront être interrogés.

Scripts à exécuter sur le client

Sous Windows, le client VPN SSL Stormshield 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 client VPN SSL Stormshield : **%NS_USERNAME%** (nom d'utilisateur servant à l'authentification) et **%NS_ADDRESS%** (adresse IP attribuée au client VPN SSL).

Champ	Description
Script à exécuter lors de la connexion	Sélectionnez le script à exécuter à l'ouverture du tunnel VPN. Exemple de script permettant de connecter le lecteur réseau Z: à un partage : `NET USE Z: \\myserver\myshare`

Champ	Description
Script à exécuter lors de la déconnexion	Sélectionnez le script à exécuter à la fermeture du tunnel VPN. Exemple de script permettant de déconnecter le lecteur réseau Z: d'un partage : `NET USE Z: /delete`

Certificats utilisés

Sélectionnez les certificats que le service VPN SSL du firewall SNS et le client VPN SSL Stormshield doivent présenter pour établir un tunnel. Ils doivent être issus de la même autorité de certification. 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.

Champ	Description
Certificat serveur	Sélectionnez le certificat souhaité. L'icône indique les certificats dont la clé privée est protégée par le TPM. Pour plus d'informations, reportez-vous à la note technique Configurer le module TPM et protéger les clés privées de certificats du firewall SNS.
Certificat client	Sélectionnez le certificat souhaité. Vous ne pouvez pas choisir un certificat 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.

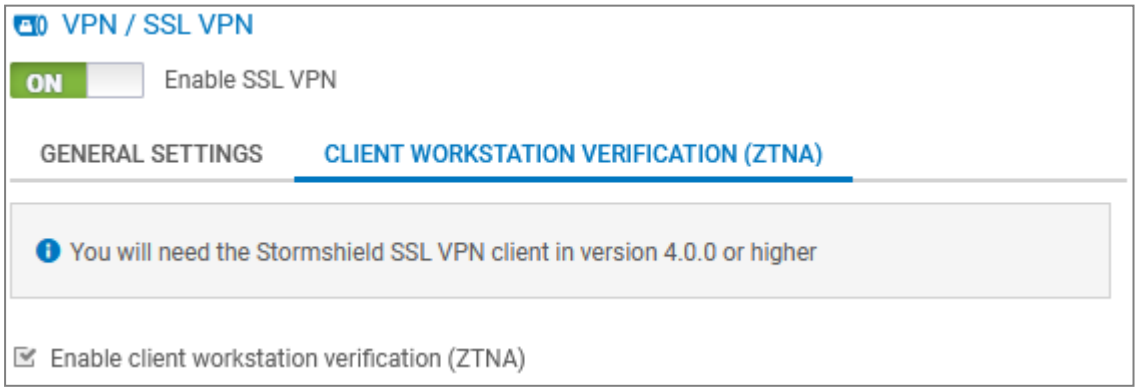
Configuration

Champ	Description
Exporter le fichier de configuration	Cliquez sur ce bouton pour exporter la configuration VPN SSL au format *.ovpn*.

Configurer la politique de vérification de la conformité des postes clients (cas du ZTNA)

Pour le cas du ZTNA, vous devez définir dans l'onglet **Vérification des postes clients (ZTNA)** une politique de vérification de la conformité des postes clients et des utilisateurs. Lorsqu'elle est activée, un poste de travail ou un utilisateur non conforme aux critères de la politique ne peut pas établir de tunnel VPN SSL avec le firewall SNS.

Ce cas nécessite d'utiliser un firewall SNS en version 4.8 ou supérieure et le client VPN SSL Stormshield en version 4.0 ou supérieure sur chaque poste de l'entreprise.



Modifiez la configuration selon les informations ci-dessous.

Champ	Description
Activer la vérification des postes clients (ZTNA)	Cochez la case pour activer la fonctionnalité de vérification de la conformité des postes clients et des utilisateurs. Lorsqu'elle est activée : • Un client VPN SSL compatible peut établir un tunnel VPN SSL avec le firewall **uniquement si tous** les critères définis dans la politique sont respectés, • Un client VPN SSL non compatible ne peut pas établir de tunnel VPN SSL avec le firewall, **sauf si** le mode permissif est activé (voir ci-dessous).
Autoriser l'établissement de tunnels pour des clients non compatibles avec ZTNA	Cochez la case pour activer le mode permissif autorisant les clients VPN SSL non compatibles avec la fonctionnalité de vérification des postes clients à établir des tunnels VPN SSL avec le firewall SNS. Ce mode permissif permet : • De mettre à jour progressivement un parc de clients VPN SSL Stormshield vers une version compatible, • De continuer à utiliser d'autres clients VPN SSL sur les systèmes d'exploitation non compatibles avec le client VPN SSL Stormshield.

Zone Paramètres de vérification des postes clients et des utilisateurs

Vous devez cocher au moins un critère de vérification des postes clients et des utilisateurs.

Champ / Critère	Description
Antivirus du poste client actif et à jour	Le poste de travail doit disposer d'un logiciel antiviral actif **avec** les dernières mises à jour de base de données antivirale. Cette information se base sur l'état de l'antivirus reconnu par le centre de Sécurité Windows. Les antivirus tiers sont donc pris en charge tant que le centre de Sécurité Windows reconnait leur état.
Firewall actif sur le poste client	Le Pare-feu Windows doit être en cours d'exécution sur le poste de travail et les profils *Réseau avec domaine*, *Réseau privé* et *Réseau public* doivent être activés. Si un profil est inactif, le critère sera considéré comme non conforme.
SES installé sur le poste client	Dans les infrastructures ayant déployé la solution SES Evolution, l'agent SES doit être installée sur le poste de travail. À noter que la configuration et l'état de l'agent SES ne sont pas pris en compte.
Interdire les utilisateurs possédant les droits d'administration du poste client	Un utilisateur disposant de droits d'administration sur le poste de travail ne peut pas établir de tunnels VPN SSL avec le firewall.

Champ / Critère	Description
Vérifier les versions (numéro de build) de Windows 10 / Windows 11	Le poste de travail sous Windows 10 ou Windows 11 doit disposer des versions de Windows spécifiées (numéros de *builds*) pour établir un tunnel VPN SSL avec le firewall. En cochant cette case, vous activez la zone de paramétrage des versions exigibles. **Onglets Windows 10 et Windows 11** • **Autoriser une plage de versions** : si vous choisissez cette option : ◦ Vous devez préciser la **Version minimale** que doit posséder le poste de travail (par défaut 10000 pour Windows 10 et 20000 pour Windows 11), ◦ Vous pouvez préciser la **Version maximale** que doit posséder le poste de travail. Laissez ce champ vide pour autoriser toutes les versions égales ou supérieures à la version minimale précisée. • **N'autoriser qu'une seule version** : si vous choisissez cette option, vous devez préciser la version exacte de Windows que le poste de travail doit posséder.
Onglet Machine rattachée à un domaine	Si vous cochez la case **La machine doit être rattachée à un domaine d'entreprise**, vous devez ajouter dans la grille **Liste des domaines Active Directory** les domaines d'appartenance des postes de travail autorisés à établir un tunnel VPN SSL avec le firewall. À noter que ce critère n'est pas lié à la configuration d'un annuaire sur le firewall.
Onglet Utilisateur rattaché à un domaine	Si vous cochez la case **L'utilisateur doit être rattaché à un domaine d'entreprise**, vous devez ajouter dans la grille **Liste des domaines Active Directory** les domaines d'appartenance des utilisateurs autorisés à établir un tunnel VPN SSL avec le firewall. Avec ce critère, le nom complet de l'utilisateur composé du domaine est vérifié. Ainsi, même si le poste de travail est rattaché à un domaine, un utilisateur local du poste de travail ne pourra pas établir de tunnel VPN SSL avec le firewall. À noter que ce critère n'est pas lié à la configuration d'un annuaire sur le firewall.
Version du client VPN SSL Stormshield	Le poste de travail doit disposer des versions du Client VPN SSL Stormshield spécifiées pour établir un tunnel VPN SSL avec le firewall. En cochant la case **Vérifier la version du client VPN SSL Stormshield**, vous activez la zone de paramétrage des versions exigibles. • **Autoriser une plage de versions** : si vous choisissez cette option : ◦ Vous devez préciser la **Version minimale** du client VPN SSL Stormshield autorisée (la version minimale autorisée est 4.0.0), ◦ Vous pouvez préciser la **Version maximale** du client VPN SSL Stormshield autorisée. Laissez ce champ vide pour autoriser toutes les versions égales ou supérieures à la version minimale précisée. • **N'autoriser qu'une seule version** : si vous choisissez cette option, vous devez préciser la version exacte du client VPN SSL Stormshield autorisée (la version minimale autorisée est 4.0.0).

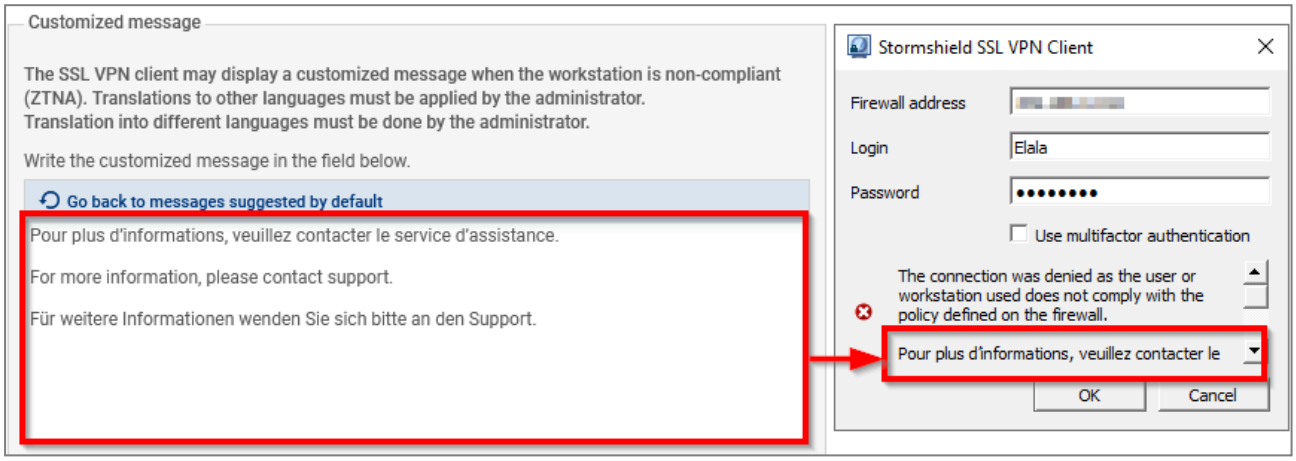
Zone Message personnalisé

En cas d'échec d'établissement d'un tunnel VPN SSL du fait d'une non-conformité du poste de travail ou de l'utilisateur, le client VPN SSL Stormshield affiche le message "*La connexion a été refusée car l'utilisateur ou le poste client utilisé n'est pas conforme à la politique définie sur le firewall*" suivi d'un message additionnel en français, anglais et allemand.

Dans la zone de saisie, vous pouvez :

- Modifier le message additionnel pour le personnaliser. Aucun mécanisme de traduction automatique n'est mis en place, vous devez donc prendre en charge sa traduction,
- Supprimer le contenu si vous ne souhaitez pas afficher un message additionnel.

Vous pouvez réinitialiser le message additionnel en cliquant sur **Revenir aux messages proposés par défaut**.



Créer les règles de filtrage et de NAT

Vous devez configurer la politique de sécurité du firewall SNS.

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

Configurer la politique de filtrage

Dans l'onglet **Filtrage**, vous devez définir des règles permettant d'autoriser ou d'interdire les clients VPN SSL à accéder aux ressources internes de l'entreprise.

Pour le cas du ZTNA, vous devez mettre en place un filtrage fin afin de limiter l'accès des utilisateurs aux seules ressources nécessaires.

Dans l'exemple ci-dessous, nous ajoutons deux règles afin d'autoriser les connexions de tous les utilisateurs à partir des clients VPN SSL en UDP et en TCP vers un intranet en HTTP. Pour augmenter la sécurité, vous pouvez créer des règles spécifiques pour des groupes d'utilisateurs différents (champ **Utilisateur**).

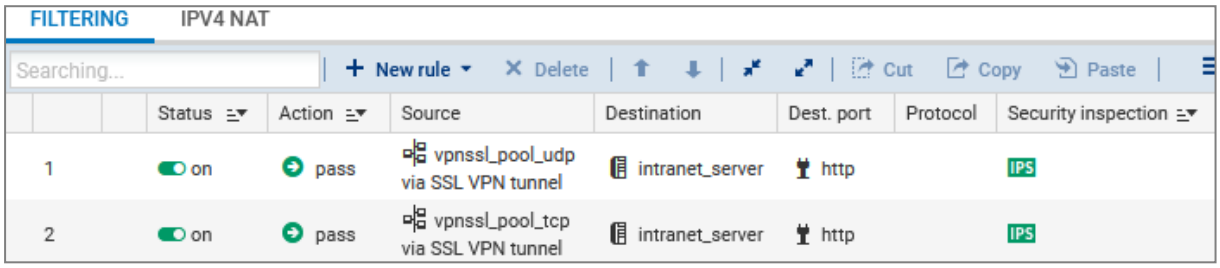
À noter que les règles sont examinées dans l'ordre de leur numérotation. Vous pouvez également faire appel aux fonctions avancées de filtrage (profils d'inspection, proxies applicatifs, contrôle antiviral, ...).

Pour ajouter une règle :

1. Cliquez sur **Nouvelle règle** > **Règle simple** et double cliquez sur le numéro de la règle pour ouvrir sa fenêtre d'édition.
2. Dans l'onglet **Général**, champ **État**, sélectionnez *On*.
3. Dans l'onglet **Action**, champ **Action**, sélectionnez *passer*.
4. Dans l'onglet **Source** :
   - Sous-onglet **Général**, champ **Machines sources**, sélectionnez l'objet représentant les adresses IP des clients VPN SSL en UDP,
   - Sous-onglet **Configuration avancée**, champ **Via**, sélectionnez *Tunnel VPN SSL*.

5. Dans l'onglet **Destination**, champ **Machines destinations**, sélectionnez l'objet représentant le serveur interne ou le réseau intranet.
6. Dans l'onglet **Port / Protocole**, champ **Port destination**, sélectionnez *http*.
7. Cliquez sur **OK**.

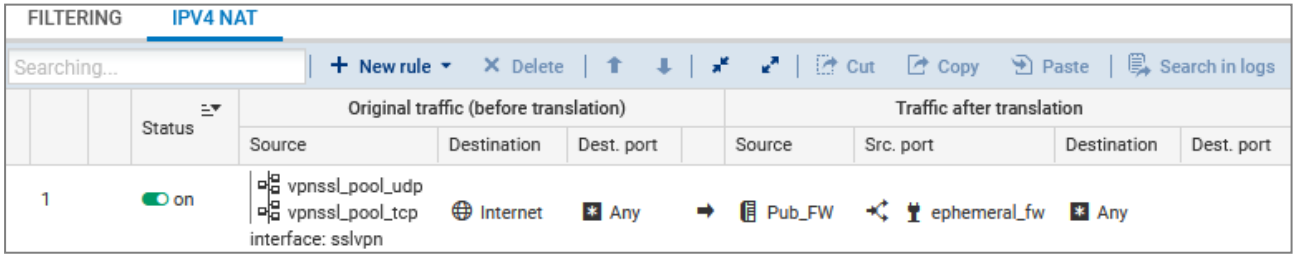
Pour la seconde règle, dans l'onglet **Source**, sous-onglet **Général**, champ **Machines sources**, sélectionnez l'objet représentant les adresses IP des clients VPN SSL en TCP.



Configurer la politique de NAT

Dans l'onglet **NAT** ou **IPv4 NAT**, si les clients VPN SSL en UDP et en TCP doivent accéder à Internet, vous devez mettre en place une règle de translation d'adresses (NAT).

1. Cliquez sur **Nouvelle règle > Règle de partage d'adresse source (masquerading)** et double cliquez sur le numéro de la règle pour ouvrir sa fenêtre d'édition.
2. Dans l'onglet **Général**, champ **État**, sélectionnez *On*.
3. Dans l'onglet **Source originale** :
   - Champ **Machines sources**, sélectionnez les objets représentant les adresses IP des clients VPN SSL en UDP et en TCP,
   - Champ **Interface d'entrée**, sélectionnez *VPN SSL*.
4. Dans l'onglet **Destination originale**, champ **Machines destinations**, sélectionnez *Internet*.
5. Dans l'onglet **Source translatée**, champ **Machine source translatée**, sélectionnez l'objet représentant l'adresse IP publique.
6. Dans le champ **Port source translaté**, cochez **choisir aléatoirement le port source translaté**.
7. Cliquez sur **OK**.



Installer le client VPN SSL Stormshield

Cette section explique comment installer le client VPN SSL Stormshield de manière classique avec le programme d'installation, via une stratégie de groupe (GPO) ou via un script.

NOTE
Le retour à une version précédente du client VPN SSL Stormshield n'est pas supporté. De plus, une fois le client VPN SSL installé, assurez-vous qu'il dispose d'un accès à la zone de notification de la barre des tâches sous Windows 11. Pour plus d'informations, reportez-vous à la section Limitations et précisions sur les cas d'utilisation.

Télécharger le client VPN SSL Stormshield

Le programme d'installation du client VPN SSL Stormshield est disponible dans deux formats :

Format	Description
.exe	Un seul fichier exécutable regroupant toutes les langues et les versions de Windows supportées. À utiliser pour une installation classique ou un déploiement via un script.
.msi	Plusieurs packages *.msi* disponibles selon les langues et les versions de Windows supportées. À utiliser pour un déploiement via une stratégie de groupe (GPO) ou via un script.

Vous pouvez télécharger le client VPN SSL Stormshield au format souhaité depuis :

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

Vous pouvez vérifier l'intégrité des binaires récupérés grâce à l'une des commandes suivantes :

- Système d'exploitation Linux :
  ```
  sha256sum <filename>
  ```
- Système d'exploitation Windows :
  ```
  CertUtil -hashfile <filename> SHA256
  ```

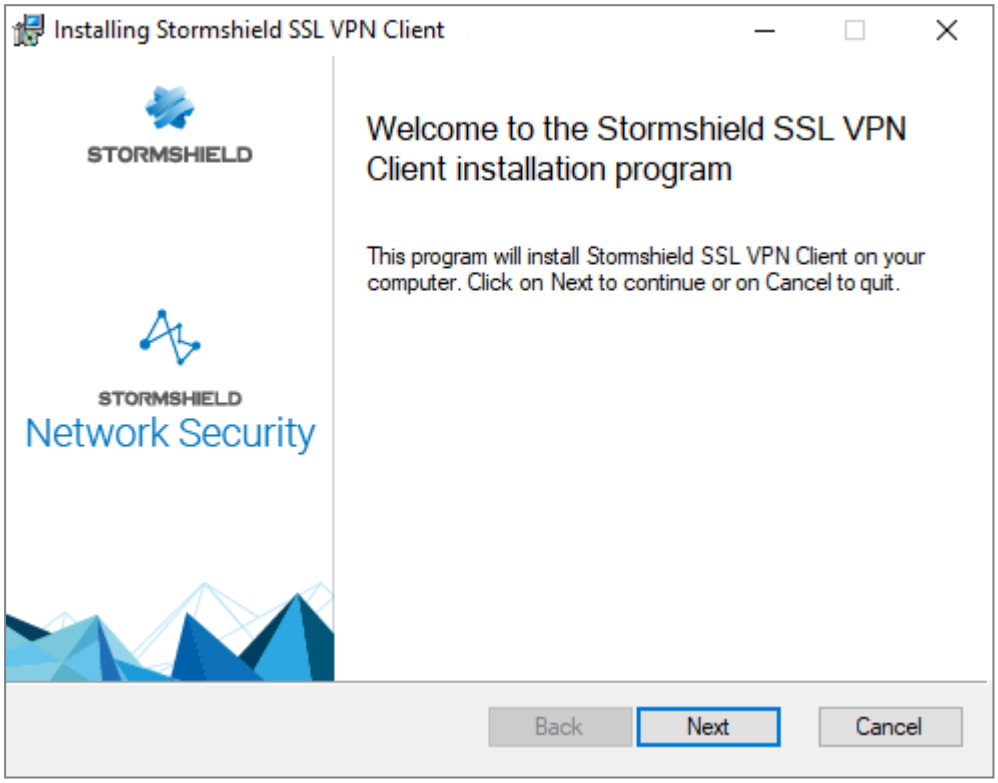
Comparez le résultat obtenu avec l'empreinte (hash) indiquée sur le site Stormshield VPN SSL ou dans votre espace MyStormshield dans la colonne **SHA256** du tableau des téléchargements.

Installer le client VPN SSL Stormshield avec le programme d'installation *.exe*

Vous devez être administrateur local du poste de travail ou fournir le nom et le mot de passe d'un compte administrateur pour installer le client VPN SSL Stormshield.

1. Connectez-vous à la session utilisateur sur laquelle installer le client VPN SSL Stormshield.
2. Exécutez le programme d'installation (fichier *.exe*) téléchargé au préalable.

3. Suivez les étapes de l'assistant d'installation.
   Vous pouvez personnaliser les paramètres à utiliser par défaut pour se connecter au VPN :
   - L'adresse IP ou le FQDN du firewall,
   - Si la configuration VPN est récupérée avec le mode automatique,
   - Si une authentification multifacteur est utilisée,
   - Si l'utilisateur Windows de la session en question est utilisé comme identifiant.



Déployer le client VPN SSL Stormshield via une stratégie de groupe (GPO)

Vous pouvez déployer directement le package *.msi* téléchargé au préalable ou le modifier pour faciliter la connexion des utilisateurs au VPN SSL en personnalisant certains paramètres.

Créer un package *.mst* pour personnaliser les paramètres à utiliser par défaut pour se connecter au VPN

Vous pouvez personnaliser les paramètres suivants :

- L'adresse IP ou le FQDN du firewall,
- Si la configuration VPN est récupérée avec le mode automatique,
- Si une authentification multifacteur est utilisée,
- Si l'utilisateur Windows de la session en question est utilisé comme identifiant.

Pour créer le package *.mst* :

1. Depuis un poste de travail disposant de l'outil Microsoft Orca, accédez au dossier où se trouve le package *.msi* du client VPN SSL Stormshield, faites un clic-droit et choisissez **Edit with Orca**.
2. Cliquez sur **Transform** > **New Transform**.

3. Sélectionnez la table **Property**.
4. Pour que l'utilisateur Windows de la session en question soit utilisé comme identifiant, indiquez dans le champ **Value** de la propriété *USE_DEFAULT_USERNAME* la valeur *1*.
5. Pour que le client VPN SSL utilise par défaut le mode manuel, indiquez dans le champ **Value** de la propriété *AUTOMATIC_MODE* la valeur *0*,
6. Pour personnaliser l'adresse IP ou le FQDN du firewall :
   1. Faites un clic droit et choisissez **Add Row**.
   2. Dans le champ **Property**, indiquez *DEFAULT_ADDRESS*.
   3. Dans le champ **Value**, indiquez l'adresse IP ou le FQDN du firewall.
   4. Cliquez sur **OK**.
7. Pour indiquer si une authentification multifacteur doit être utilisée :
   1. Faites un clic droit et choisissez **Add Row**.
   2. Dans le champ **Property**, indiquez *ENABLE_OTP*.
   3. Dans le champ **Value**, indiquez *1* pour utiliser une authentification multifacteur ou *0* pour ne pas l'utiliser.
   4. Cliquez sur **OK**.
8. Cliquez sur **Transform > Generate Transform**.
9. Enregistrez le package *.mst* dans le même répertoire que le package *.msi*.

Configurer le déploiement par GPO

1. Sur le contrôleur de domaine, lancez le gestionnaire de serveur.
2. Dans la barre supérieure de menu, cliquez sur **Outils > Gestion des stratégies de groupe**.
3. Dans la liste de gauche, faites un clic droit sur le nom du domaine Microsoft Active Directory et sélectionnez **Créer un objet GPO dans ce domaine, et le lier ici...**.
4. Nommez la GPO et cliquez sur **OK**.
5. Dans la liste de gauche, faites un clic droit sur le nom de la GPO que vous venez de créer et sélectionnez **Modifier**.
   La fenêtre d'édition de la GPO s'ouvre.
6. Dans le menu de gauche de la GPO, dépliez le menu **Configuration ordinateur > Stratégies > Paramètres du logiciel**.
7. Faites un clic droit sur **Installation de logiciel**, sélectionnez **Nouveau > Package**, puis sélectionnez le package *msi* d'installation du client VPN SSL Stormshield.
8. Choisissez le mode **Avancé** et cliquez sur **OK**.
   La fenêtre d'édition de la GPO s'ouvre.
9. Vous pouvez renommer cette instance d'installation si vous le souhaitez.
10. Dans l'onglet **Modifications**, vous pouvez associer le package *.mst* précédemment créé à la GPO d'installation du client VPN SSL Stormshield. Pour cela, cliquez sur **Ajouter...**, sélectionnez le package *.mst* et cliquez sur *Ouvrir*.
11. Cliquez sur **OK**.

L'installation est automatique lorsqu'un poste de travail se connecte au réseau de l'entreprise.

Déployer le client VPN SSL Stormshield via un script

1. Ouvrez une invite de commande en tant qu'administrateur.
2. Allez dans le dossier où se trouve le fichier *.exe* ou le package *.msi* téléchargé au préalable.
3. Tapez la commande correspondante :
   - Pour un fichier *.exe* :
     ```
     Stormshield_SSLVPN_Client_4.X.Y_x64.exe [PARAMETERS]
     ```
   - Pour un package *.msi* :
     ```
     msiexec /i Stormshield_SSLVPN_Client_4.X.Y_language_x64.msi
     [PARAMETERS] /qn
     ```

   Vous pouvez faciliter la connexion des utilisateurs au VPN SSL en complétant la commande avec les paramètres suivants :
   - DEFAULT_ADDRESS=[adresse IP ou FQDN du firewall],
   - AUTOMATIC_MODE=[0 pour le mode manuel, 1 pour le mode automatique],
   - USE_DEFAULT_USERNAME=[0 pour que le champ reste vide, 1 pour que l'utilisateur Windows de la session en question soit utilisé comme identifiant],
   - ENABLE_OTP=[0 pour ne pas utiliser une authentification multifacteur, 1 pour en utiliser une].
4. Exécutez la commande.

Exemple de commande permettant de déployer le fichier *.exe* :

```
Stormshield_SSLVPN_Client_4.0.0_x64.exe DEFAULT_ADDRESS=vpn.company.tld
```

Exemple de commande permettant de déployer un package *.msi* :

```
msiexec /i Stormshield_SSLVPN_Client_4.0.0_en_x64.msi DEFAULT_
ADDRESS=vpn.company.tld AUTOMATIC_MODE=1 ENABLE_OTP=0 /qn
```

L'installation est automatique lorsqu'un poste de travail se connecte au réseau de l'entreprise. Une invite de commande s'affiche sur le bureau et une barre de progression indique l'état de l'installation.

Configurer le client VPN SSL Stormshield

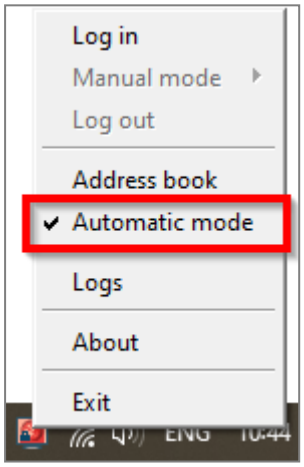
Vous devez configurer le client VPN SSL Stormshield selon le mode de connexion souhaité. Reportez-vous à la section Matrice de compatibilité des modes de connexion pour vérifier les fonctionnalités compatibles selon le mode de connexion utilisé.

Activer le Mode automatique

En **Mode automatique**, le client VPN SSL Stormshield 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 dans la barre des tâches Windows.
2. Cliquez sur **Mode automatique**.

Pour vous connecter, poursuivez vers la section Établir un tunnel VPN en Mode automatique.

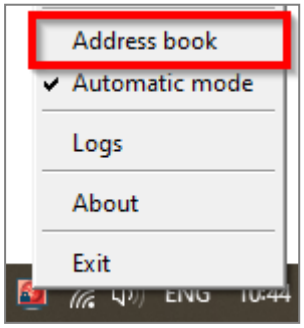


Configurer le carnet d'adresses (Mode automatique requis)

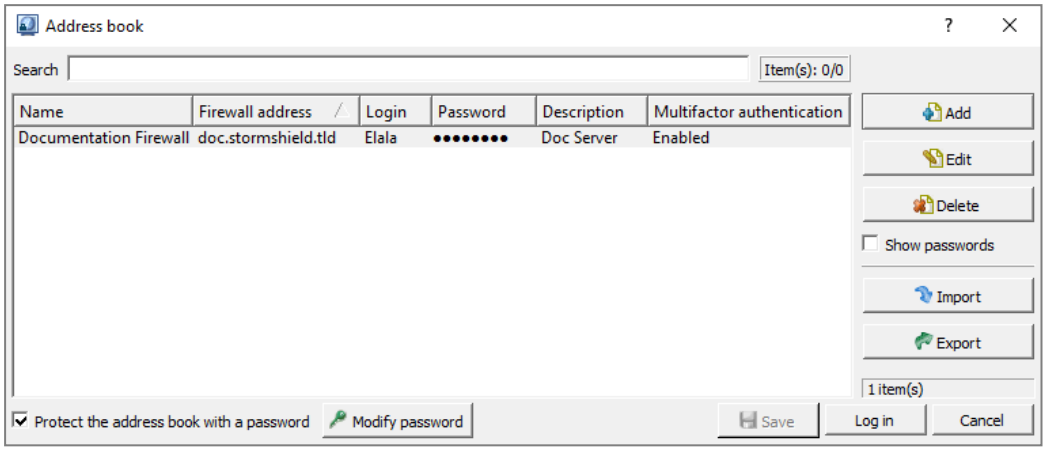
Le client VPN SSL Stormshield dispose d'un carnet d'adresses permettant de mémoriser les informations de connexion à différents firewalls : adresse de connexion au firewall (adresse IPv4 ou FQDN), identifiant, mot de passe et utilisation d'une authentification multifacteur.

Ouvrir le carnet d'adresses

1. Effectuez un clic-droit sur l'icône dans la barre des tâches Windows.
2. Cliquez sur **Carnet d'adresses**. Le **Mode automatique** doit être activé.



3. Si le carnet d'adresses est protégé par un mot de passe, renseignez-le pour l'ouvrir. Vous pouvez protéger le carnet d'adresses grâce aux options **Protéger le carnet d'adresses par un mot de passe** et **Modifier le mot de passe**.

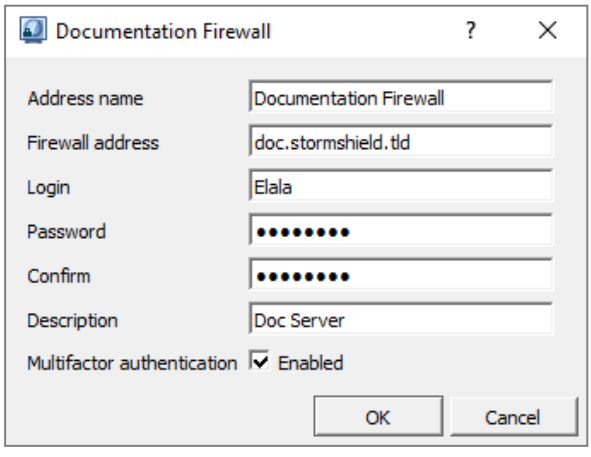


Ajouter ou modifier une adresse dans le carnet d'adresses

1. Cliquez sur **Ajouter** pour ajouter une nouvelle adresse. Pour modifier une adresse existante, sélectionnez-la puis cliquez sur **Modifier**.
2. Complétez les champs.

Champ / Case	Description
Nom de l'adresse	Nom de l'adresse.
Adresse du firewall	Adresse IPv4 ou FQDN du firewall SNS à joindre pour établir le tunnel VPN. 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).
Identifiant	Identifiant de l'utilisateur.
Mot de passe Confirmer	Mot de passe de l'utilisateur. Si une authentification multifacteur **Code OTP seulement** ou **Mode Push** est utilisée, laissez ces champs vides.
Description	Description de l'adresse, si nécessaire.
Authentification multifacteur	Si une authentification multifacteur est utilisée (**Mot de passe + Code OTP**, **Code OTP seulement** ou **Mode Push**), cochez la case **Activée**.

3. Cliquez sur **OK**, puis sur **Sauvegarder**.



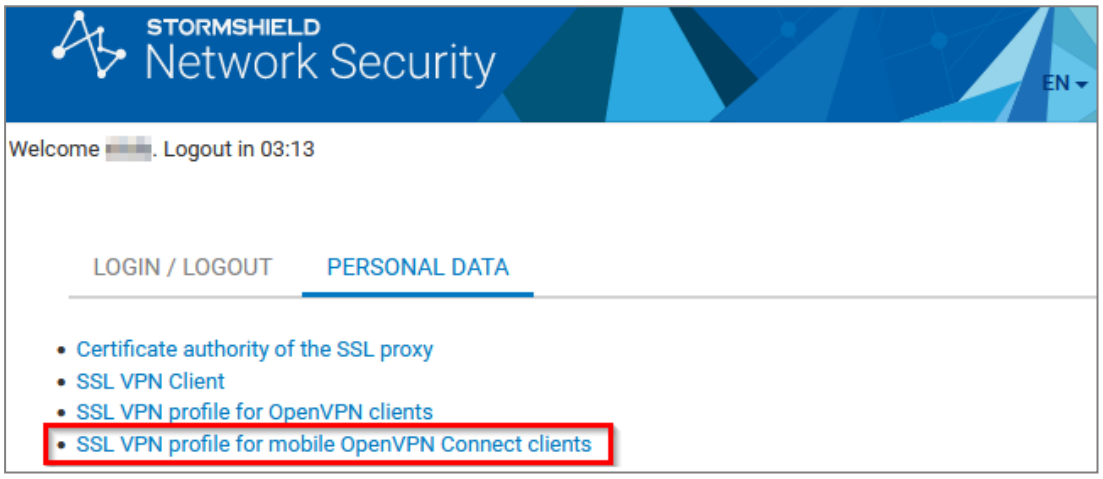
Configurer le Mode manuel

En **Mode manuel**, vous devez importer les éléments de configuration (autorité de certification, certificat, clé privée, ...) que le client VPN SSL Stormshield doit utiliser, rassemblés dans un fichier *.ovpn*.

Récupérer la configuration VPN SSL (fichier *.ovpn*)

Vous pouvez récupérer la configuration VPN SSL Stormshield depuis :

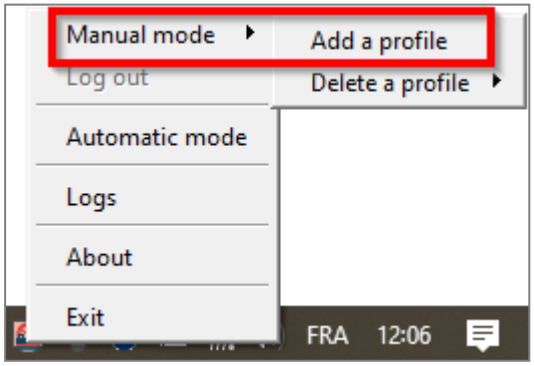
- **Le portail captif du firewall SNS hébergeant le service VPN SSL.**
  En étant connecté sur le réseau de l'entreprise, authentifiez-vous à l'adresse *https://adresseIP_du_firewall/auth*, puis dans l'onglet **Données personnelles**, cliquez sur *Profil VPN SSL pour clients mobile OpenVPN Connect (fichier unique .ovpn)*,



- **L'interface d'administration du firewall SNS.**
  Rendez-vous dans **Configuration > VPN > VPN SSL > Configuration avancée** et cliquez sur **Exporter le fichier de configuration**.

Ajouter un profil de connexion

1. Effectuez un clic-droit sur l'icône dans la barre des tâches Windows.
2. Cliquez sur **Mode manuel > Ajouter un profil**. Le **Mode automatique** doit être désactivé.



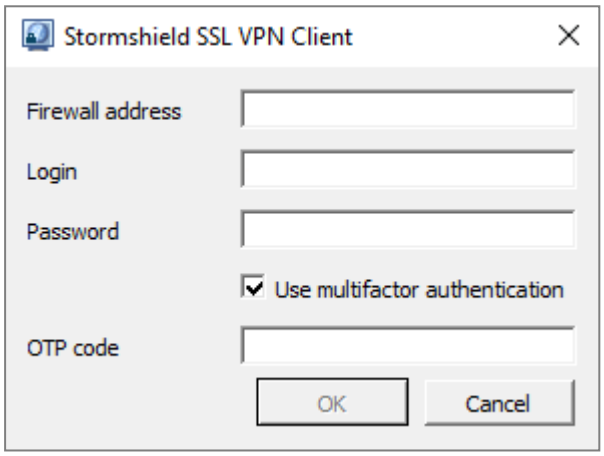
3. Sélectionnez le fichier *.ovpn*.
4. Définissez un nom au profil de connexion.
5. Cliquez sur **OK**.

Établir un tunnel VPN avec le client VPN SSL Stormshield

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

Établir un tunnel VPN en Mode automatique

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



2. Dans le champ **Adresse du firewall**, indiquez l'adresse IPv4 ou le FQDN du firewall SNS à joindre pour établir le tunnel VPN. 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. Complétez le reste des champs selon l'authentification qui s'applique.
Dans le tableau, ✅ signifie que les champs doivent être renseignés, ❌ signifie qu'ils doivent rester vides, et - signifie qu'ils ne sont pas visibles.

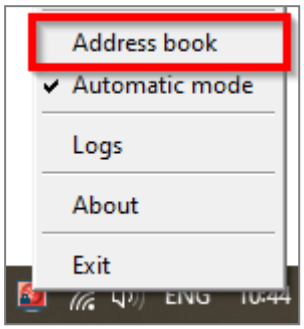
Authentification	Mot de passe	Authentification multifacteur	Code OTP
Classique	✅	❌	-
Multifacteur **Mot de passe + Code OTP**	✅	✅	✅
Multifacteur **Code OTP seulement**	❌	✅	✅
Multifacteur **Mode Push**	❌	✅	❌

5. Cliquez sur **OK**.

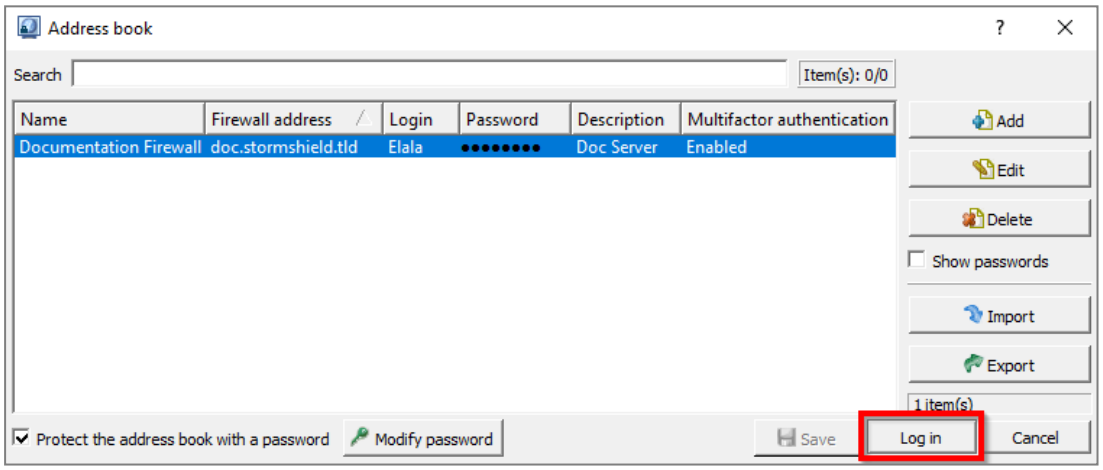
Le client VPN SSL Stormshield s'authentifie sur le firewall SNS. Si l'authentification n'aboutit pas, consultez la section Que faire si le tunnel VPN ne s'établit pas.

Établir un tunnel VPN en utilisant le carnet d'adresses

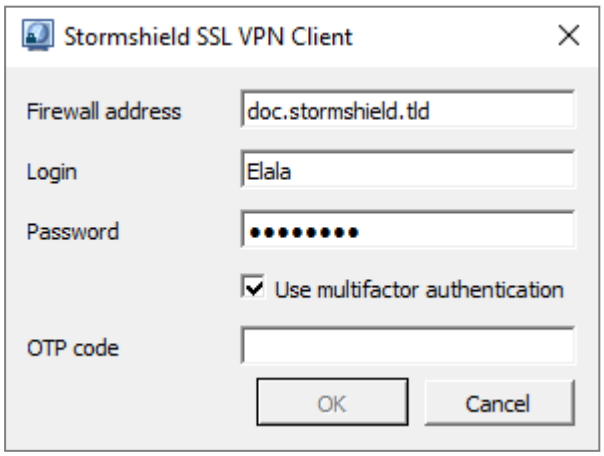
1. Effectuez un clic-droit sur l'icône dans la barre des tâches Windows, puis cliquez sur **Carnet d'adresses**. Pour rappel, le **Mode automatique** doit être activé.



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 **Se connecter**.



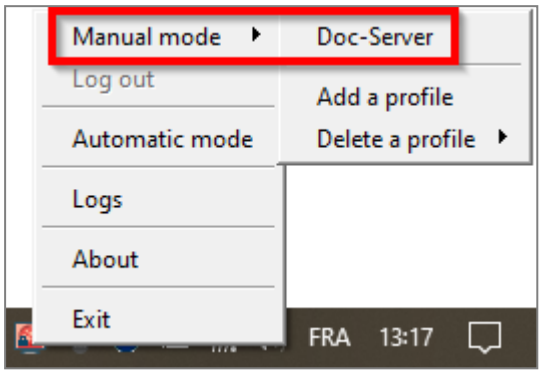
4. La fenêtre de connexion s'affiche.
   - Pour une authentification classique, la connexion se lance automatiquement,
   - Pour une authentification multifacteur **Mot de passe + Code OTP** ou **Code OTP seulement**, renseignez un **Code OTP** (mot de passe à usage unique) et cliquez sur **OK**,
   - Pour une authentification multifacteur **Mode Push**, cliquez sur **OK** et approuvez la connexion sur l'application tierce.



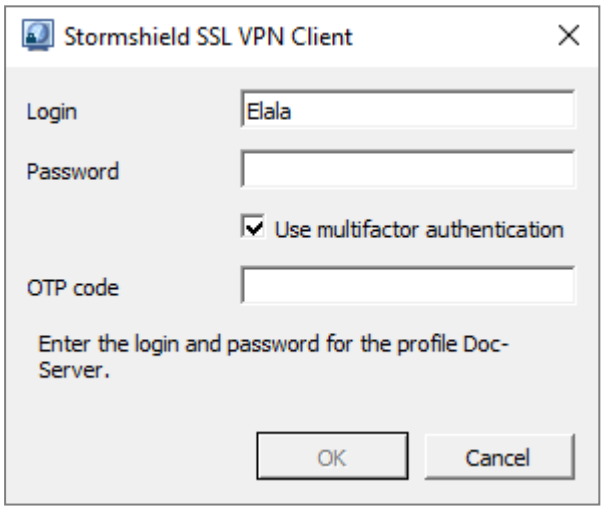
Le client VPN SSL Stormshield s'authentifie sur le firewall SNS. Si l'authentification n'aboutit pas, consultez la section Que faire si le tunnel VPN ne s'établit pas.

Établir un tunnel VPN en Mode manuel

1. Effectuez un clic-droit sur l'icône dans la barre des tâches Windows, puis cliquez sur **Mode manuel** et sur le profil concerné.



La fenêtre de connexion s'ouvre.



2. Dans le champ **Identifiant**, renseignez l'identifiant de l'utilisateur.
3. Complétez le reste des champs selon l'authentification qui s'applique.
Dans le tableau, ✅ signifie que les champs doivent être renseignés, ❌ signifie qu'ils doivent rester vides, et - signifie qu'ils ne sont pas visibles.

Authentification	Mot de passe	Authentification multifacteur	Code OTP
Classique	✅	❌	-
Multifacteur **Mot de passe + Code OTP**	✅	✅	✅
Multifacteur **Code OTP seulement**	❌	✅	✅
Multifacteur **Mode Push**	❌	✅	❌

4. Cliquez sur **OK**.

Le client VPN SSL Stormshield s'authentifie sur le firewall SNS. Si l'authentification n'aboutit pas, consultez la section Que faire si le tunnel VPN ne s'établit pas.

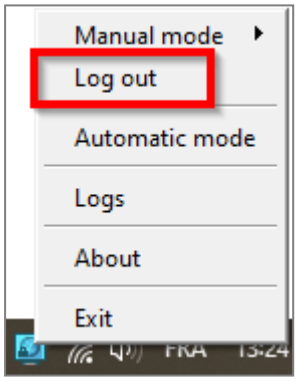
Afficher les informations de connexion du tunnel VPN SSL

La couleur de l'icône du client VPN SSL Stormshield située dans la barre des tâches Windows permet de connaître son état de connexion.

Icône	Description
	Le client VPN SSL Stormshield 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).
	Le client VPN SSL Stormshield est en train de se connecter.
	Le client VPN SSL Stormshield n'est pas connecté ou une tentative de connexion a échoué.

Déconnecter le tunnel VPN SSL

1. Effectuez un clic-droit sur l'icône  dans la barre des tâches Windows.
2. Cliquez sur **Se déconnecter**.



Que faire si le tunnel VPN ne s'établit pas

Dans le cas où le tunnel VPN ne s'établit pas, suivez ces quelques recommandations :

- Prenez connaissance du message d'erreur qui s'affiche,
- Vérifiez les informations de connexion dans la fenêtre de connexion ainsi que dans le carnet d'adresses si utilisé,
- Vérifiez la validité du code OTP si renseigné. Le client VPN SSL Stormshield effectue plusieurs tentatives de connexion en cas de non réponse, le code OTP peut donc avoir expiré entre temps,
- Vérifiez la configuration du profil de connexion importé (pour le Mode manuel). Par exemple, si la configuration VPN SSL du firewall SNS a été modifiée, cette dernière doit être importée sur le client VPN SSL Stormshield,
- Consultez la section Résoudre les problèmes.

Consulter les journaux du client VPN SSL Stormshield

Cette section présente les journaux disponibles du client VPN SSL Stormshield.

Journaux en cas d'erreurs d'installation, de désinstallation ou de mise à jour

Des journaux sont créés lorsqu'une erreur est rencontrée lors de l'installation, la désinstallation ou la mise à jour du client VPN SSL Stormshield. Vous pouvez les retrouver à cet emplacement :

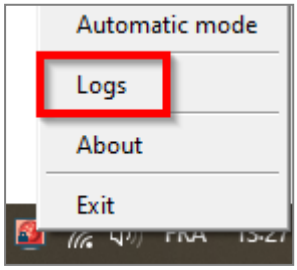
```
%programfiles%\Stormshield\Stormshield SSL VPN Client\install_logs
```

Nom du fichier	Contenu
install_driver.log	Erreurs rencontrées lors de l'installation du driver OpenVPN
uninstall_driver.log	Erreurs rencontrées lors de la suppression du driver OpenVPN
backward_update_sites.log	Erreurs rencontrées lors de la copie des profils de connexion depuis le client VPN SSL Stormshield en version 3.2.3 ou inférieure
generate_ovpn_auth.log	Erreurs rencontrées lors de la génération de la clé privée utilisée pour sécuriser l'accès à l'interface de gestion OpenVPN
tap_create.log	Erreurs rencontrées lors de l'installation de l'interface réseau pour OpenVPN
tap_delete.log	Erreurs rencontrées lors de la suppression de l'interface réseau pour OpenVPN
update_ovpn_admin.log	Erreurs rencontrées lors de la mise à jour de la valeur *ovpn_admin_group* dans la clé *HKEY_LOCAL_MACHINE\SOFTWARE\StormshieldSSLVPN*
clean_previous_version.log	Informations de la désinstallation de la version 3.2.3 ou inférieure
install_certs.log	Erreurs rencontrées lors de l'installation du certificat
set_dacls.log	Erreurs rencontrées lors de la mise à jour des droits d'accès aux dossiers
service_update.log	Erreurs rencontrées lors de la mise à jour du service VPN SSL

Journal disponible après l'établissement d'un tunnel VPN SSL

Un journal est créé systématiquement après chaque établissement d'un tunnel VPN SSL. Vous pouvez le retrouver à l'emplacement ci-dessous ou l'ouvrir directement en effectuant un clic-droit sur l'icône dans la barre des tâches Windows puis en cliquant sur **Journaux (logs)**.

```
%programdata%\Stormshield\Stormshield SSL VPN Client\log\openvpn_
client.log
```



Journaux accessibles dans l'observateur d'événements Windows

Les journaux liés au client VPN SSL Stormshield sont accessibles par l'intermédiaire de l'observateur d'événements Windows sur les postes des utilisateurs.

Par défaut, seuls les journaux d'erreur sont accessibles dans l'observateur d'événements.

Pour accéder aux journaux du client VPN SSL Stormshield :

1. Ouvrez l'**Observateur d'événements** Windows.
2. Sélectionnez **Journaux des applications et des services > Stormshield SSL VPN service**.

Pour modifier les journaux accessibles dans l'observateur d'événements Windows :

1. Ouvrez l'**Éditeur de Registre** Windows.
2. Modifiez la valeur *log_level* de la clé de registre suivante :

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\
StormshieldSSLVPNService\Parameters
```

- 0 : affiche les journaux d'erreur. Il s'agit de la valeur par défaut,
- 1 : affiche les journaux d'erreur et d'information,
- 2 : affiche les journaux d'erreur, d'information et de dépannage.

Suivre les utilisateurs connectés au VPN SSL sur le firewall SNS

Vous pouvez suivre dans l'interface d'administration du firewall SNS les utilisateurs connectés ou qui se sont connectés au VPN SSL. Pour le cas de l'accès réseau *Zero Trust* (ZTNA), cette section présente également des informations sur l'identification de l'état de conformité d'un poste client lors d'une connexion au VPN SSL.

Pour permettre une meilleure lisibilité des images, certaines colonnes des tableaux ont été masquées. L'affichage par défaut sur votre firewall SNS peut être légèrement différent.

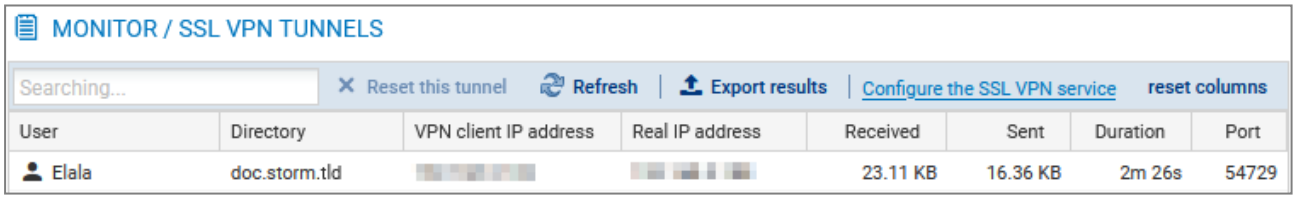
Informations concernant l'accès aux données personnelles

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**. Pour plus d'informations, reportez-vous sur la note technique Se conformer aux règlements sur les données personnelles.

Afficher les utilisateurs actuellement connectés au VPN SSL

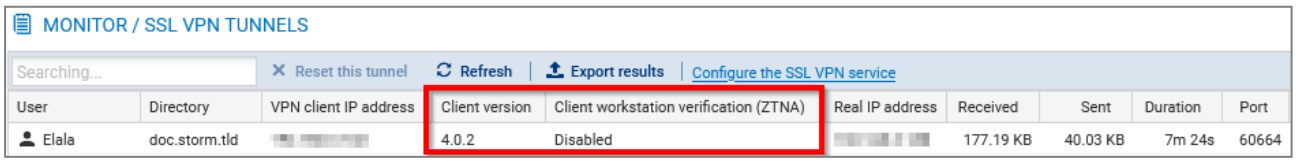
Cette vue affiche en temps réel des informations concernant les sessions des utilisateurs connectés au VPN SSL.

Rendez-vous dans **Monitoring > Supervision > Tunnels VPN SSL**.



En version SNS 4.8 ou supérieure :

- La colonne "*Version du client*" affiche la version du client VPN SSL Stormshield utilisé. La valeur indiquée pour un client VPN SSL tiers ou non compatible est N/A.
- La colonne "*Vérification des postes clients (ZTNA)*" affiche l'état de conformité du poste client. Plusieurs valeurs sont possibles :
  - **Désactivé** : la politique de vérification des postes clients n'est pas activée,
  - **Non vérifié** : le client VPN SSL utilisé pour établir le tunnel n'est pas compatible avec la fonctionnalité de vérification des postes clients mais l'établissement de tunnels pour des clients non compatibles est explicitement autorisé (mode permissif),
  - **Conforme** : le poste client est conforme aux critères définis dans la politique de vérification des postes clients.

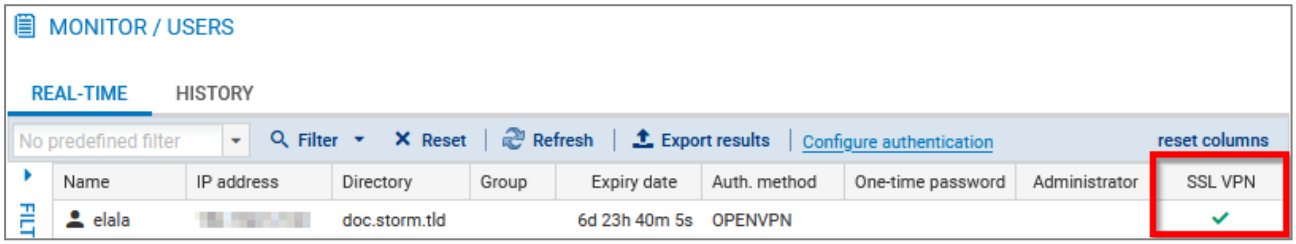


Afficher les utilisateurs actuellement authentifiés sur le firewall SNS

Cette vue affiche en temps réel les utilisateurs authentifiés sur le firewall SNS.

Rendez-vous dans **Monitoring > Supervision > Utilisateurs**.

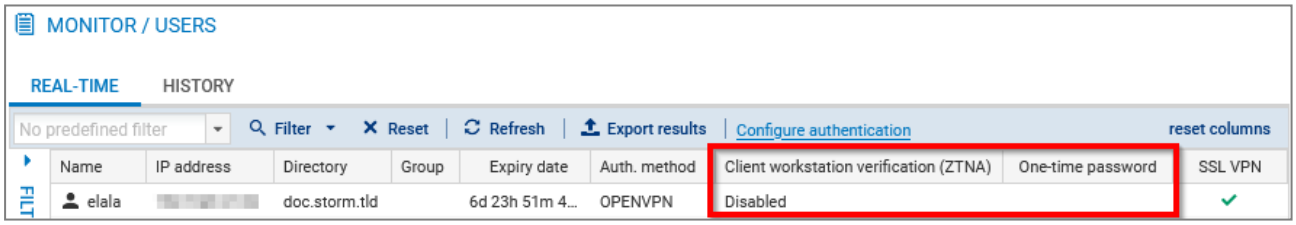
La colonne "*VPN SSL*" permet d'identifier les utilisateurs connectés au VPN SSL.



En version SNS 4.5 ou supérieure, la colonne "*Mot de passe à usage unique*" indique si l'utilisateur a utilisé un mot de passe TOTP de la solution TOTP Stormshield pour se connecter.

En version SNS 4.8 ou supérieure, la colonne "*Vérification des postes clients (ZTNA)*" affiche l'état de conformité du poste client. Plusieurs valeurs sont possibles :

- **Désactivé** : la politique de vérification des postes clients n'est pas activée,
- **Non vérifié** : le client VPN SSL utilisé pour établir le tunnel n'est pas compatible avec la fonctionnalité de vérification des postes clients mais l'établissement de tunnels pour des clients non compatibles est explicitement autorisé (mode permissif),
- **Conforme** : le poste client est conforme aux critères définis dans la politique de vérification des postes clients.



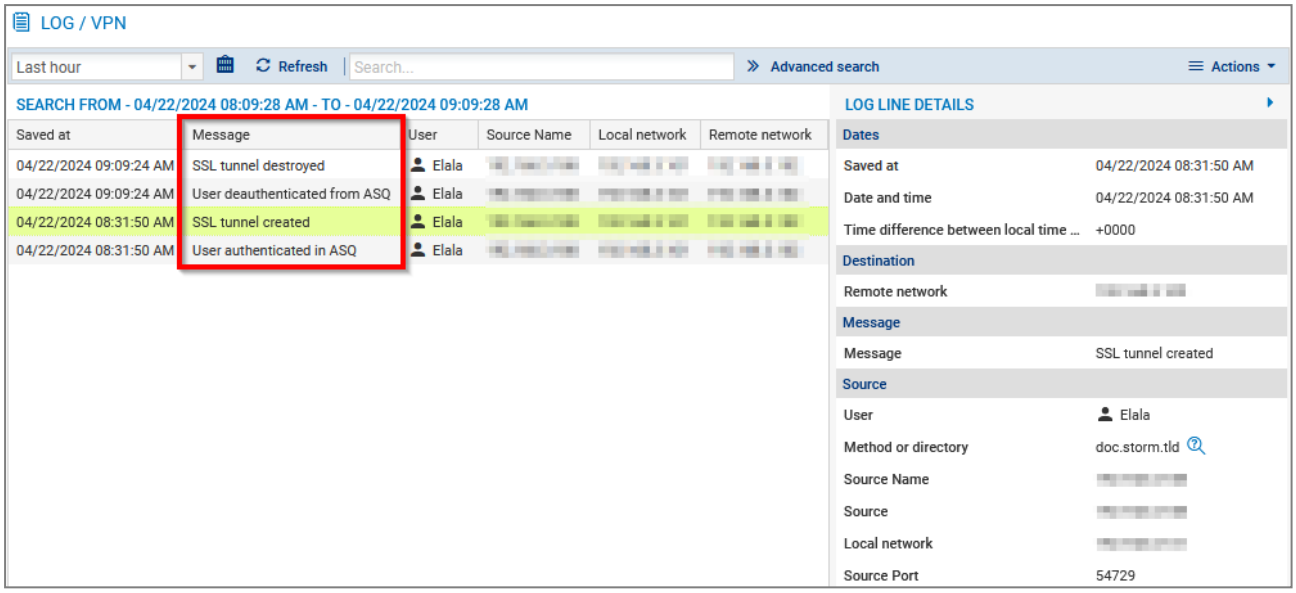
Afficher les journaux VPN (SSL, IPsec) et identifier les critères de vérification non conformes d'un poste client

Ce journal affiche les événements liés aux différents types de tunnels VPN (SSL, IPsec).

Rendez-vous dans **Monitoring > Logs - Journaux d'audit > VPN**.

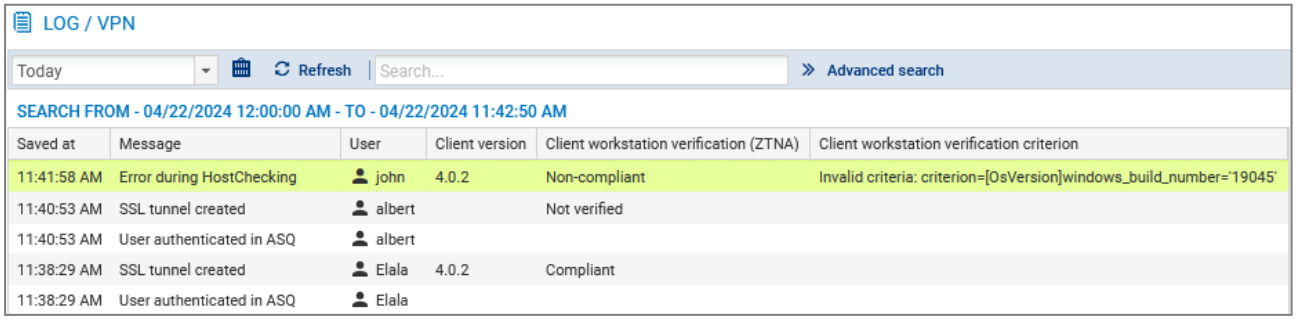
Les colonnes "*Message*" et "*Utilisateur*" affichent l'utilisateur qui a généré l'événement et le message de l'événement (tunnel VPN connecté ou déconnecté, authentification de l'utilisateur dans le moteur d'authentification du firewall, ...).

Vous pouvez afficher les détails d'un événement dans le panneau de droite en cliquant dessus.



En version SNS 4.8 ou supérieure :

- La colonne "*Message*" peut contenir des messages liés à la vérification de la conformité d'un poste client (fonction *HostChecking*) :
  - "*Error during HostChecking*" avec un poste client "*Non conforme*" : indique qu'un ou plusieurs critères définis dans la politique de vérification de la conformité des postes clients ne sont pas conformes,
  - "*Error during authentication : HostChecking failed*" avec un poste client "*Non vérifié*" : indique que le client VPN SSL utilisé n'est pas compatible avec la fonctionnalité de vérification des postes clients et que l'établissement de tunnels pour des clients non compatibles n'est pas explicitement autorisé (mode permissif),
- La colonne "*Vérification des postes clients (ZTNA)*" affiche l'état de conformité du poste client. Plusieurs valeurs sont possibles :
  - **Désactivé** : la politique de vérification des postes clients n'est pas activée,
  - **Non vérifié** : l'état de conformité du poste client n'a pas été vérifié car le client VPN SSL utilisé n'est pas compatible avec la fonctionnalité de vérification des postes clients. Pour savoir si le tunnel a été établi, reportez-vous à la colonne "*Message*",
  - **Non conforme** : le poste client n'est pas conforme aux critères définis dans la politique de vérification des postes clients,
  - **Conforme** : le poste client est conforme aux critères définis dans la politique de vérification des postes clients.
- La colonne "*Critère de vérification des postes clients*" affiche les critères non conformes en cas d'échec d'établissement d'un tunnel VPN SSL du fait d'une non-conformité du poste client ou de l'utilisateur.



Résoudre les problèmes

Ce chapitre liste certains problèmes fréquemment rencontrés lors de l'utilisation du client VPN SSL Stormshield. 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 "*La connexion a été refusée car l'utilisateur ou le poste client utilisé n'est pas conforme à la politique définie sur le firewall*" s'affiche.

- *Situation* : Lors de la tentative de connexion au VPN SSL, le tunnel ne s'établit pas et le message "*La connexion a été refusée car l'utilisateur ou le poste client utilisé n'est pas conforme à la politique définie sur le firewall*" s'affiche.
- *Cause* : Le poste client utilisé ne respecte pas tous les critères définis dans la politique de vérification de la conformité des postes clients et des utilisateurs (ZTNA).
- *Solutions* :
  - Vérifiez les critères non conformes en vous reportant à la section Afficher les journaux VPN (SSL, IPsec) et identifier les critères de vérification non conformes d'un poste client, puis mettez en conformité le poste client concerné,
  - Vérifiez la configuration de la politique de vérification de la conformité des postes clients en vous reportant à la section Configurer la politique de vérification de la conformité des postes clients (cas du ZTNA).

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* : Les services **Stormshield SSL OpenVPN Service** et **Stormshield SSL VPN Service** ne sont pas démarrés ou ne fonctionnent pas.
- *Solution* : Vérifiez que les services Windows sont bien démarrés sur le poste de travail ou essayez de les redémarrer.

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, activez temporairement sur la règle du flux concerné le niveau de trace **Avancé** pour collecter des logs (dans **Configuration > Politique de sécurité > Filtrage et NAT > Filtrage**), puis vérifiez dans les logs que la règle s'applique pour ce flux (dans **Monitoring > Logs - Journaux d'audit > Filtrage**),
  - Assurez-vous que la ressource demandée est bien physiquement disponible,
  - Videz le cache ARP du poste de travail en exécutant 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).

Annexe : installer, configurer et utiliser OpenVPN Connect

Cette annexe présente l'installation d'OpenVPN Connect, sa configuration, son utilisation jusqu'à l'établissement d'un tunnel VPN SSL et la consultation de ses journaux (logs). Complétez ces informations avec celles disponibles sur le site web de l'éditeur OpenVPN.

Installer OpenVPN Connect

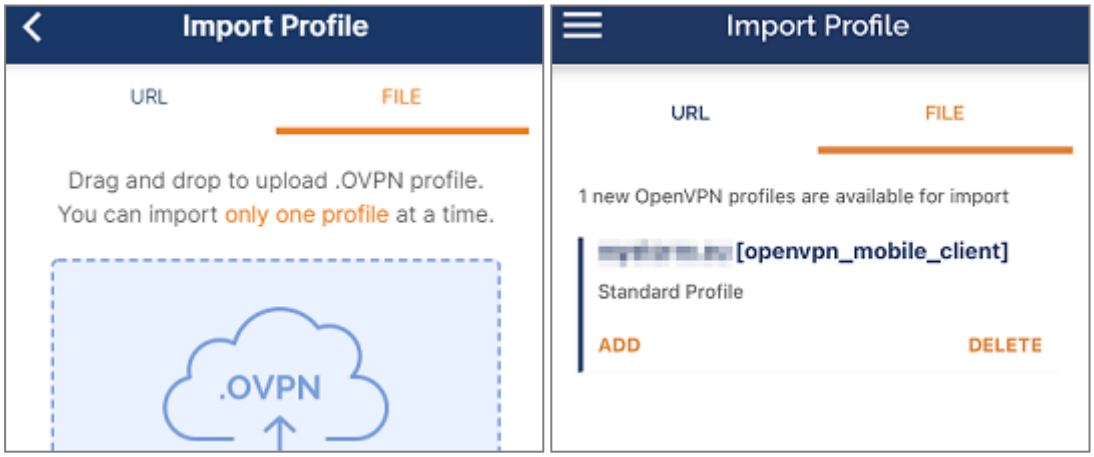
Sur un poste de travail : téléchargez le logiciel depuis le site web d'OpenVPN et installez-le.

Sur un mobile : installez l'application depuis le *Google Play Store* ou l'*App Store*.

Configurer OpenVPN Connect

Vous devez importer les éléments de configuration (CA, certificat, clé privée, ...) qu'OpenVPN Connect doit utiliser, rassemblés dans un fichier *.ovpn*.

1. Récupérez le fichier *.ovpn*. Suivez la méthode décrite dans la section Récupérer la configuration VPN SSL (fichier .ovpn).
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.

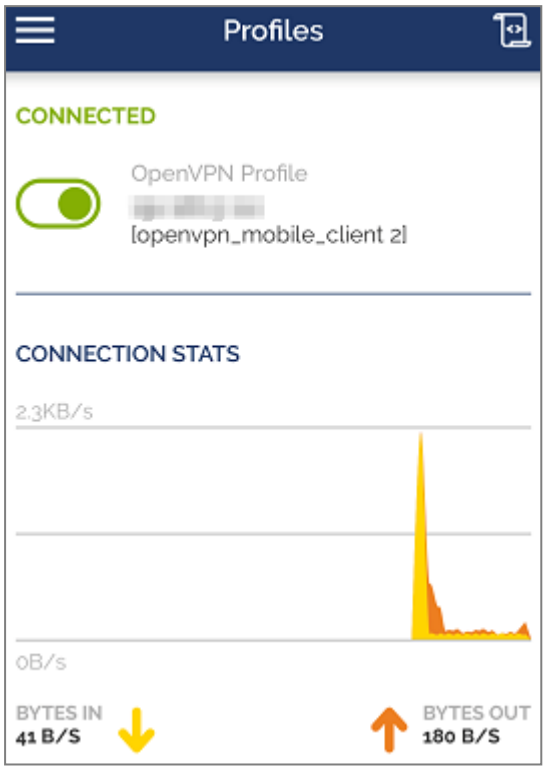
Vous devez réaliser cette configuration à la première connexion, mais aussi dès que la configuration VPN SSL du firewall SNS est modifiée, comme après un changement de certificat.

Établir un tunnel VPN SSL avec OpenVPN Connect

Connecter le tunnel VPN SSL

1. Lancez 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.

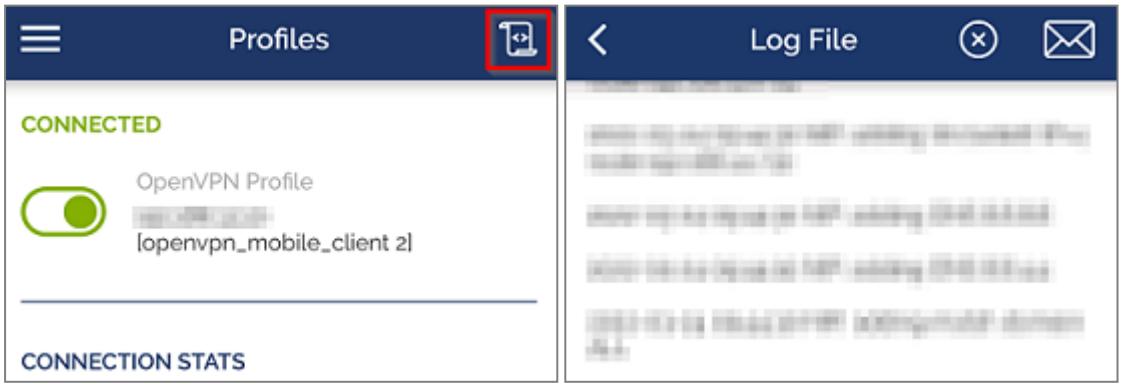


Déconnecter le tunnel VPN SSL

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

Consulter les journaux (logs) d'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.



STORMSHIELD

documentation@stormshield.eu