GUIDE

STORMSHIELD NETWORK SSL VPN CLIENT

GUIDE D'ADMINISTRATION VPN SSL DES FIREWALLS SNS ET DES CLIENTS VPN SSL STORMSHIELD

Dernière mise à jour du document : 22 octobre 2025

Référence : sns-fr-ssl_vpn_client_guide_administration

Table des matières

Historique des modifications

Date	Description
22 octobre 2025	Nouveau document

Avant de commencer

Bienvenue dans le guide d'administration VPN SSL des firewalls SNS et des clients VPN SSL Stormshield.

Dans ce guide, Stormshield Network Security est nommé " firewall SNS", et Stormshield Network SSL VPN Client est nommé "client VPN SSL Stormshield".

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

Une fois le tunnel VPN SSL établi, les communications entre l'utilisateur et le firewall SNS sont encapsulées et protégées via un tunnel TLS chiffré, appelé dans ce guide "tunnel VPN SSL".

Ce guide présente :

- La configuration à réaliser dans les modules **Authentification**, **Droits d'accès** et **Filtrage et NAT** du firewall SNS pour mettre en œuvre des tunnels VPN SSL,
- L'activation et la configuration du service VPN SSL du firewall SNS,
- La configuration de la fonctionnalité de vérification des postes clients, dans le cas où un accès réseau Zero Trust (ZTNA) est utilisé,
- Le suivi des utilisateurs connectés au firewall SNS en VPN SSL.

Prérequis

Cette section présente les prérequis nécessaires mettre en œuvre des tunnels VPN SSL avec un firewall SNS et des clients VPN SSL compatibles.

Disposer d'un firewall SNS correctement dimensionné

Le nombre maximal de tunnels VPN SSL autorisés par les firewalls SNS est différent selon le modèle utilisé. Vous devez disposer d'un modèle adapté à vos besoins.

Retrouvez cette information sur le site de Stormshield, rubrique Gamme produits (SNS) en sélectionnant votre modèle.

Disposer d'un client VPN SSL compatible

Chaque utilisateur doit disposer sur son poste de travail et/ou son terminal mobile d'un client VPN SSL compatible pour établir des tunnels VPN SSL avec le firewall SNS.

Les clients VPN SSL compatibles sont :

- Le **client VPN SSL Stormshield**. Pour plus d'informations sur son installation, reportez-vous au Guide d'installation du client VPN SSL Stormshield v5. Pour connaître les versions actuellement supportées, reportez-vous au Guide de cycle de vie Network Security & Tools.
- Le client **OpenVPN Connect**. Ce client VPN SSL ne dispose pas de mode permettant de récupérer automatiquement la configuration VPN SSL du firewall SNS, et n'est pas compatible avec la fonctionnalité de vérification des postes clients du firewall SNS.

NOTE
Pour tester la configuration avant le déploiement, installez dès à présent un client VPN SSL compatible sur certains de vos appareils. Pour déployer le VPN SSL dans votre organisation, vous pouvez commencer par configurer le firewall SNS, puis installer tous les clients VPN SSL.

Avoir connecté le firewall SNS à un annuaire

Le firewall SNS doit être connecté à un annuaire. Vérifiez cette connexion dans l'interface Web d'administration du firewall SNS dans **Configuration > Utilisateurs > Authentification**, onglet **Méthodes disponibles**. Une ligne LDAP doit s'afficher dans la grille.

Pour plus d'informations, reportez-vous à la section **Configuration des annuaires** du manuel utilisateur v4 ou du manuel utilisateur v5 selon la version SNS utilisée.

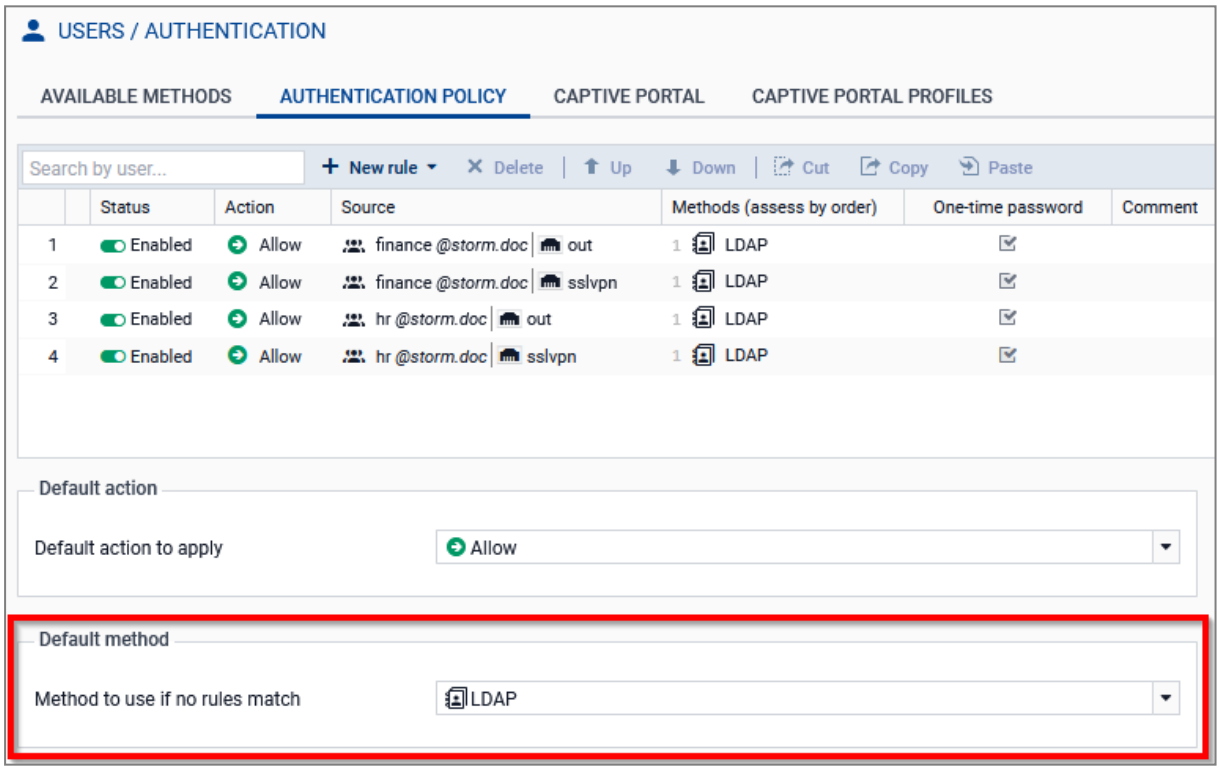
Configurer l'authentification

Cette section présente la configuration du module **Authentification** à réaliser sur le firewall SNS pour mettre en œuvre des tunnels VPN SSL.

Configurer la politique d'authentification

Cette section présente la configuration de la politique d'authentification à réaliser pour mettre en œuvre des tunnels VPN SSL. Vous pouvez cliquer sur **Appliquer** à tout moment pour sauvegarder vos modifications.

1. Rendez-vous dans **Configuration > Utilisateurs > Authentification**, onglet **Politique d'authentification**.
2. Identifiez la **Méthode à utiliser si aucune règle ne peut être appliquée**.



Poursuivez selon le cas qui s'applique.

Cas n°1 : La méthode "LDAP" est sélectionnée et seule cette méthode est utilisée sur le firewall SNS

La configuration actuelle de la politique d'authentification est suffisante. Poursuivez vers la section Configurer le portail captif.

Cas 2 : Dans tous les autres cas

Dans tous les autres cas (restriction au strict nécessaire de l'authentification sur le firewall SNS, utilisation de l'authentification multifacteur, etc.), vous devez ajouter au moins deux règles à la politique d'authentification pour permettre aux utilisateurs de s'authentifier avec le client VPN SSL Stormshield et établir des tunnels VPN SSL.

Pour renforcer la sécurité, il est recommandé de créer ces deux règles pour chaque groupe d'utilisateurs établissant des tunnels VPN SSL avec le firewall SNS. Toutefois, vous pouvez décider de créer seulement deux règles pour tous les utilisateurs, sans distinction particulière.

Concernant la première règle : elle permet aux utilisateurs et aux clients VPN SSL Stormshield configurés en mode Stormshield de se connecter au portail captif du firewall SNS. Les clients VPN SSL Stormshield peuvent ainsi récupérer automatiquement la configuration VPN SSL et transmettre au firewall SNS les informations permettant de vérifier la conformité du poste client (ZTNA).

1. Cliquez sur **Nouvelle règle > Règle standard**.
2. Dans l'onglet **Utilisateur**, sélectionnez un utilisateur ou un groupe d'utilisateurs d'un annuaire du firewall SNS (comme *finance@domain.tld*). Si souhaité, vous pouvez sélectionner tous les utilisateurs d'un annuaire avec le choix *Any user@domain.tld*. Sur les versions SNS 5, vous pouvez également sélectionner tous les utilisateurs de tous les annuaires du firewall SNS en cochant **Tous les utilisateurs (any)**.
3. Dans l'onglet **Source**, ajoutez l'interface de provenance des connexions VPN SSL (par exemple *out*).
4. Dans l'onglet **Méthodes d'authentification** :
   a. Supprimez la ligne *Méthode par défaut*.
   b. Activez la méthode permettant aux utilisateurs et aux clients VPN SSL Stormshield de se connecter au portail captif du firewall SNS, par exemple *LDAP* ou *RADIUS*.
   c. Si une authentification multifacteur est utilisée (authentification avec un code à usage unique), positionnez le sélecteur **Mot de passe à usage unique** sur **ON**  .
5. Cliquez sur **OK**.

Concernant la seconde règle : elle permet aux utilisateurs d'établir des tunnels VPN SSL depuis leurs clients VPN SSL vers le firewall SNS.

1. Cliquez sur **Nouvelle règle > Règle standard**.
2. Dans l'onglet **Utilisateur**, sélectionnez le même utilisateur ou groupe d'utilisateurs que celui de la première règle.
3. Dans l'onglet **Source**, ajoutez l'interface *VPN SSL*.
4. Dans l'onglet **Méthodes d'authentification** :
   a. Supprimez la ligne *Méthode par défaut*.
   b. Activez la méthode permettant aux utilisateurs d'établir des tunnels VPN SSL depuis leurs clients VPN SSL vers le firewall SNS, par exemple *LDAP* ou *RADIUS*.
   c. Si une authentification multifacteur est utilisée (authentification avec un code à usage unique), positionnez le sélecteur **Mot de passe à usage unique** sur **ON**  .
5. Cliquez sur **OK**.

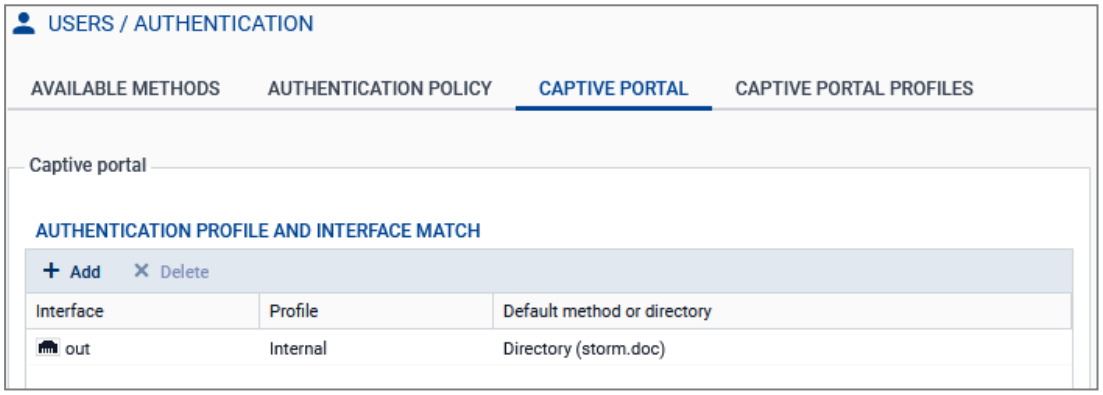
> **NOTE**
> Lors d'une authentification sur le firewall SNS, les règles de la politique d'authentification sont examinées dans l'ordre de leur numérotation.

Configurer le portail captif

Cette section présente la configuration du portail captif à réaliser pour mettre en œuvre des tunnels VPN SSL. Vous pouvez cliquer sur **Appliquer** à tout moment pour sauvegarder vos modifications.

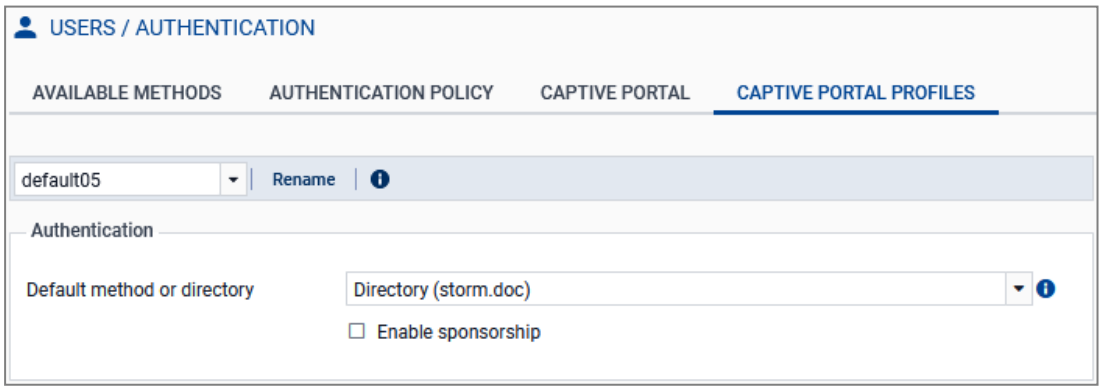
Configurer la correspondance entre profil d'authentification et interface

1. Rendez-vous dans **Configuration > Utilisateurs > Authentification**, onglet **Portail captif**.
2. Dans la grille **Correspondance entre profil d'authentification et interface**, cliquez sur **Ajouter**.
3. Dans la colonne **Interface**, sélectionnez l'interface de provenance des connexions VPN SSL (par exemple *out*). Pour une interface PPPoE ou VLAN, sélectionnez-la plutôt que l'interface physique parente.
4. Dans la colonne **Méthode ou annuaire par défaut**, si l'annuaire renseigné correspond à celui des utilisateurs établissant des tunnels VPN SSL avec le firewall SNS, vous n'avez pas besoin de modifier la valeur de la colonne **Profil**. Cette configuration permet aux utilisateurs de renseigner simplement leur identifiant dans leur client VPN SSL pour établir le tunnel VPN SSL.



Dans le cas contraire, les utilisateurs doivent renseigner leur identifiant avec le domaine d'authentification de l'annuaire (*identifiant@domain.tld*) dans leur client VPN SSL pour établir le tunnel VPN SSL. Si vous souhaitez que les utilisateurs renseignent simplement leur identifiant, vous devez adapter la configuration :

a. Dans la colonne **Profil**, sélectionnez un autre profil (par exemple *default05*).
b. Dans l'onglet **Profils du portail captif**, sélectionnez cet autre profil et choisissez dans le champ **Méthode ou annuaire par défaut** le bon annuaire.



Vérifier si le portail captif est activé

1. Rendez-vous dans **Configuration > Utilisateurs > Authentification**, onglet **Profils du portail captif**.
2. Sélectionnez le profil utilisé pour les connexions VPN SSL.
3. Dans la zone **Configuration avancée**, assurez-vous que la case **Activer le portail captif** est cochée.

Personnaliser le certificat du portail captif

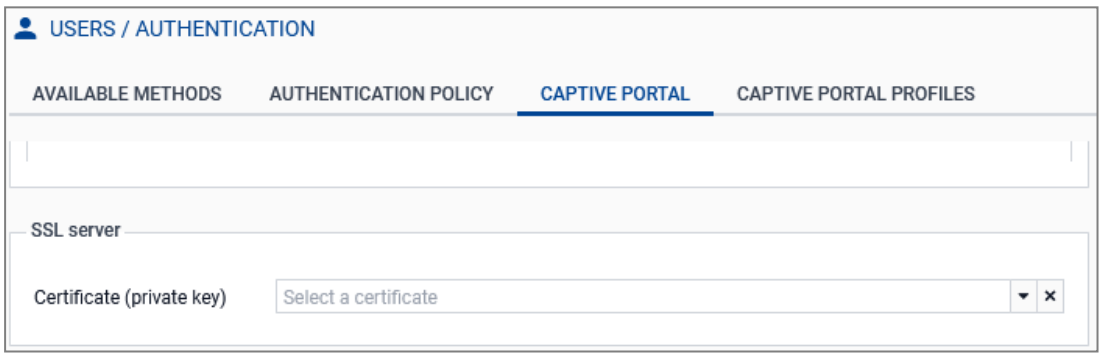
Vous pouvez personnaliser le certificat présenté par le firewall SNS lors d'un accès au portail captif. Si ce certificat n'est pas personnalisé, le firewall SNS présente un certificat par défaut :

- Sur les versions SNS 4, c'est un certificat correspondant au numéro de série du firewall SNS,
- Sur les versions SNS 5, c'est un certificat auto-généré pour cet accès.

Pour personnaliser le certificat du portail captif :

1. Rendez-vous dans **Configuration > Utilisateurs > Authentification**, onglet **Portail captif**.
2. Dans le champ **Certificat (clé privée)**, sélectionnez le nouveau certificat. Si besoin, vous pouvez ajouter un nouveau certificat (identité serveur) dans le module **Configuration > Objets > Certificats et PKI**.

   Sur les versions SNS 4.8 LTSB et 5, l'icône indique les certificats dont la clé privée est protégée par le module TPM. Pour plus d'informations sur cette protection, reportez-vous à la note technique Configurer le module TPM et protéger les clés privées de certificats du firewall SNS.



Si l'un des critères suivants s'applique au certificat sélectionné :

- Le certificat n'est pas signé par une autorité de certification de confiance,
- 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 SNS qui est utilisée pour les connexions VPN SSL. C'est par exemple le cas du certificat par défaut présenté par le firewall SNS.

Alors le certificat ne peut pas être validé automatiquement par le client VPN SSL Stormshield ou par le navigateur Web et une fenêtre indiquant un risque probable de sécurité s'affiche. Chaque utilisateur doit alors s'assurer que la connexion est sûre en vérifiant les informations du certificat, puis indiquer faire confiance au certificat présenté par le firewall SNS pour établir le tunnel VPN SSL. Même si ce message n'est pas bloquant, il est recommandé de sensibiliser vos utilisateurs à ce comportement attendu.

Utiliser une authentification multifacteur

Cette section présente certaines solutions d'authentification multifacteur que vous pouvez utiliser pour établir des tunnels VPN SSL avec le firewall SNS. Si vous ne souhaitez pas utiliser une authentification multifacteur, poursuivez vers la section suivante.

Informations générales sur l'authentification multifacteur

L'authentification multifacteur permet de renforcer l'authentification des utilisateurs établissant des tunnels VPN SSL grâce à un second facteur d'authentification.

Ce second facteur est généralement un code à usage unique, appelé code OTP ou TOTP, que l'utilisateur doit renseigner en plus de son mot de passe pour établir le tunnel VPN SSL. Stormshield dispose de sa propre solution TOTP.

Il est également possible d'utiliser une solution externe avec un serveur RADIUS ou une application tierce à installer sur un appareil de confiance. Par exemple, la solution Trustbuilder (anciennement inWebo) est compatible et permet aux utilisateurs de générer des codes OTP ou d'approuver l'établissement d'une connexion (notification *push*) dans leur application.

Ce document aborde certaines de ces solutions. Poursuivez selon le cas qui s'applique.

NOTE
Pour configurer l'utilisation de l'authentification multifacteur sur le client VPN SSL Stormshield, reportez-vous au Guide de configuration et d'utilisation du client VPN SSL Stormshield v5.

Utiliser la solution TOTP Stormshield

Reportez-vous à la note technique Configurer et utiliser la solution TOTP Stormshield qui présente la configuration et la gestion de la solution TOTP sur le firewall SNS, ainsi que la procédure d'enrôlement des utilisateurs à la solution TOTP.

Assurez-vous de suivre les étapes décrites dans cette note technique pour utiliser la solution TOTP Stormshield pour établir des tunnels VPN SSL avec le firewall SNS.

Utiliser une solution tierce avec un serveur RADIUS

Configurer la solution d'authentification multifacteur tierce

Vous devez configurer la solution d'authentification multifacteur tierce choisie et la connecter à votre serveur RADIUS. Si vous avez besoin d'aide pour cette configuration, reportez-vous à la documentation de la solution choisie.

Activer la méthode RADIUS sur le firewall SNS

Vous devez activer et configurer la méthode RADIUS sur le firewall SNS pour le connecter à votre serveur RADIUS. Pour cela, rendez-vous dans **Configuration > Utilisateurs > Authentification**, onglet **Méthodes disponibles**.

Pour plus d'informations, reportez-vous à la section **Authentification > Onglet Méthodes disponibles > RADIUS** du manuel utilisateur v4 ou du manuel utilisateur v5 selon la version SNS utilisée.

Personnaliser le délai d'inactivité autorisé pour la connexion au serveur RADIUS

Par défaut, le délai d'inactivité autorisé pour la connexion à un serveur RADIUS est de 3000 millisecondes (3 secondes).

Dans le cas où la solution d'authentification multifacteur choisie implique d'utiliser une application tierce pour se connecter (mode Push), vous devez personnaliser le délai d'inactivité afin de laisser aux utilisateurs suffisamment de temps pour se connecter. Par exemple, pour définir un délai d'inactivité de 30 secondes, utilisez les commandes CLI / Serverd suivantes :

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

Utiliser une authentification avec certificat utilisateur

Cette section explique comment utiliser une authentification avec certificat utilisateur pour établir des tunnels VPN SSL avec le firewall SNS. Si vous ne souhaitez pas utiliser une authentification avec certificat utilisateur, poursuivez vers la section suivante.

Cette authentification permet aux utilisateurs d'établir des tunnels VPN SSL en s'authentifiant sur le firewall SNS avec leur certificat utilisateur.

Prérequis

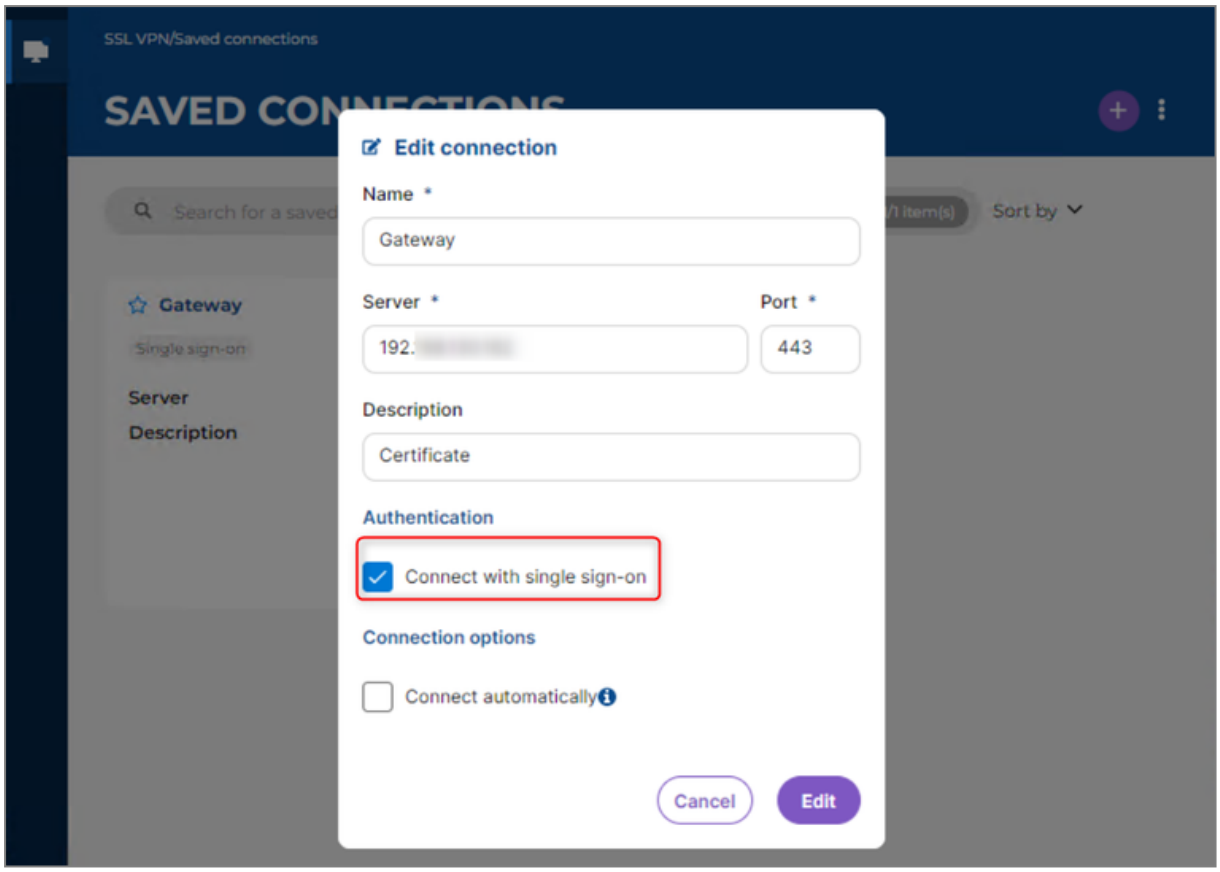
Pour utiliser l'authentification avec certificat utilisateur, vous devez vous conformer aux prérequis suivants :

- Disposer d'un firewall SNS en version 5.
- Disposer de clients VPN SSL Stormshield en version 5. Les versions antérieures du client VPN SSL Stormshield et les clients VPN SSL tiers, comme OpenVPN Connect, ne sont pas compatibles.
- Avoir activé et configuré la méthode **Certificat SSL** dans le module **Authentification > Méthodes disponibles** du firewall SNS. Pour plus d'informations, reportez-vous à la section **Authentification > Onglet Méthodes disponibles > Certificat (SSL)** du manuel utilisateur v4 ou du manuel utilisateur v5 selon la version SNS utilisée.
- Avoir créé des règles permettant aux utilisateurs de s'authentifier via la méthode **Certificat SSL** dans le module **Authentification > Politique d'authentification** du firewall SNS. Adaptez les informations de la section Configurer la politique d'authentification pour réaliser cette configuration.
- Avoir activé et configuré le service VPN SSL dans le module **VPN SSL** du firewall SNS. Cette configuration est décrite dans les sections suivantes.
- Avoir installé sur le poste de travail des utilisateurs concernés leur certificat. Vous pouvez télécharger l'identité utilisateur du certificat au format P12 dans le module **Objets > Certificats et PKI** du firewall SNS.

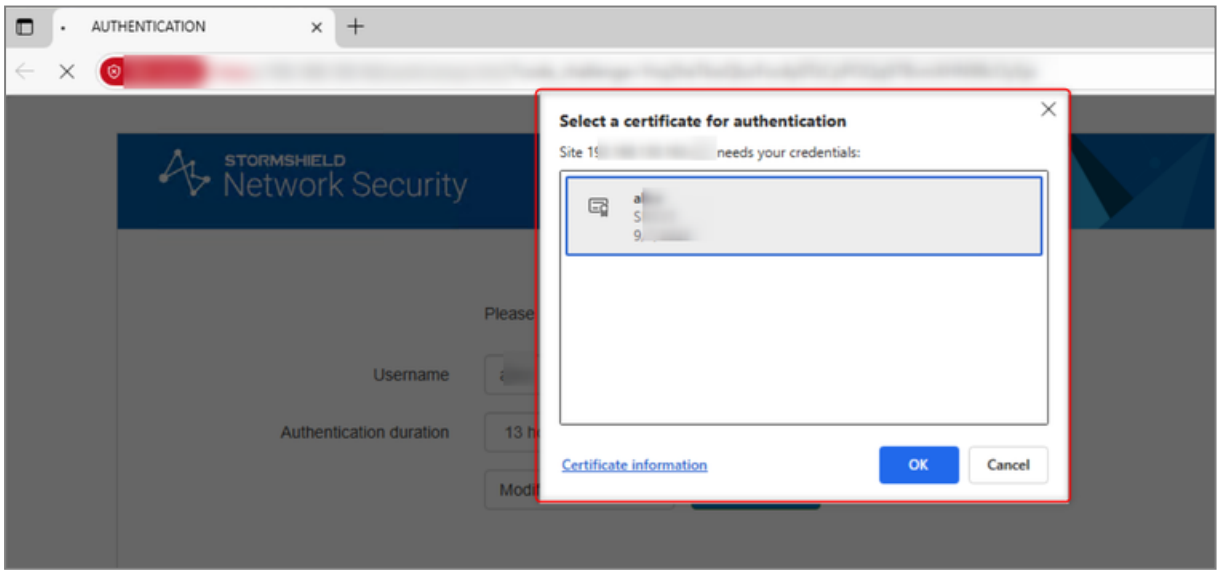
Établir un tunnel VPN SSL en utilisant l'authentification avec certificat utilisateur

Sur le client VPN SSL Stormshield, la connexion (enregistrée ou directe) doit être établie avec les paramètres suivants :

- Le **Mode Stormshield** doit être sélectionné. Les connexions de type OpenVPN (import de fichier OVPN) ne sont pas compatibles.
- La case **Se connecter avec l'authentification unique** doit être cochée.



Une fois l'établissement du tunnel VPN SSL initié, le portail captif du firewall SNS s'ouvre automatiquement dans le navigateur Web de l'utilisateur. Ce dernier s'authentifie sur le portail en suivant les étapes.



Une fois authentifié, le tunnel VPN SSL est établi. La date d'expiration de l'authentification de l'utilisateur s'affiche dans l'interface graphique du client VPN SSL Stormshield. Tant que cette date n'est pas atteinte et que l'authentification est toujours effective sur le firewall SNS, l'utilisateur n'a pas besoin de s'authentifier de nouveau pour établir le tunnel VPN SSL.

Pour plus d'informations, reportez-vous à la section **Établir une connexion sécurisée** du *Guide de configuration et d'utilisation du client VPN SSL Stormshield v5*.

Limitations connues

Incompatibilité TLS 1.3

Avec la version SNS 5.0.2, l'authentification avec certificat utilisateur n'est pas prise en charge via TLS 1.3. Cette limitation sera corrigée dans une prochaine version SNS.

Des solutions de contournement existent selon le navigateur Web utilisé par vos utilisateurs :

- Pour Firefox, activez le paramètre suivant dans la configuration de Firefox :
```
security.tls.enable_post_handshake_auth
```
- Pour les autres navigateurs tels que Chrome ou Edge, vous devez forcer le portail captif du firewall SNS à utiliser TLS 1.2. Pour cela, exécutez les commandes suivantes en SSH sur le firewall SNS :
```
setconf /usr/Firewall/ConfigFiles/auth Config TLSv13 0
ensl
```

Saisie du nom d'utilisateur lors de l'authentification

L'utilisateur doit actuellement renseigner sur le portail captif son nom d'utilisateur avant de pouvoir sélectionner le certificat à utiliser pour s'authentifier. Cette limitation sera améliorée dans une prochaine version SNS.

Configurer les droits d'accès au VPN SSL

Cette section explique comment attribuer aux utilisateurs le droit d'établir des tunnels VPN SSL. Vous pouvez attribuer ce droit à tous les utilisateurs ou à certains utilisateurs et groupes d'utilisateurs.

Poursuivez selon le cas qui s'applique. Vous pouvez cliquer sur **Appliquer** à tout moment pour sauvegarder vos modifications.

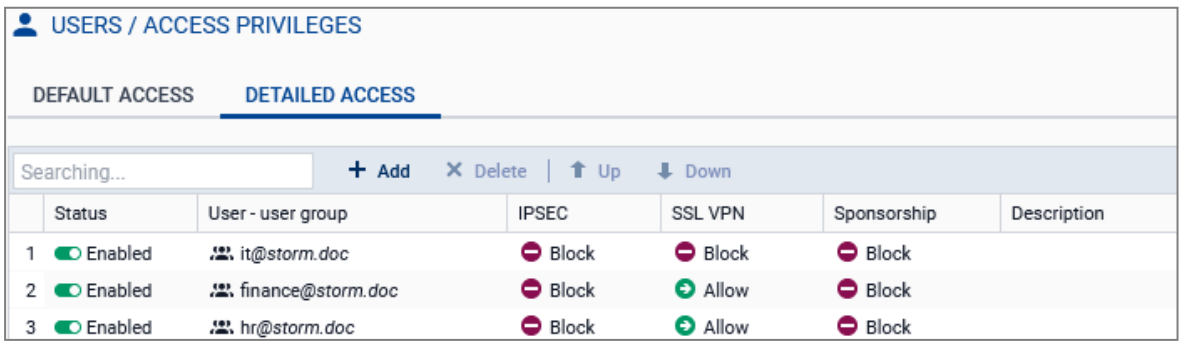
Autoriser tous les utilisateurs à établir des tunnels VPN SSL

1. Rendez-vous dans **Configuration > Utilisateurs > Droits d'accès**, onglet **Accès par défaut**.
2. Dans le champ **Politique VPN SSL**, sélectionnez **Autoriser**.

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

1. Rendez-vous dans **Configuration > Utilisateurs > Droits d'accès**, onglet **Accès par défaut**.
2. Dans le champ **Politique VPN SSL**, sélectionnez **Interdire**.
3. Rendez-vous dans l'onglet **Accès détaillé**.
4. Cliquez sur **Ajouter** pour créer une règle d'accès personnalisée.
5. Dans la fenêtre qui s'affiche, sélectionnez un utilisateur ou un groupe d'utilisateurs d'un annuaire du firewall SNS (comme *finance@domain.tld*). Si souhaité, vous pouvez sélectionner tous les utilisateurs d'un annuaire avec le choix *Any user@domain.tld*. Cliquez sur **Appliquer** ou **OK** selon la version SNS utilisée.

   Une nouvelle ligne s'affiche dans la grille.
6. Dans la colonne **VPN SSL** de la nouvelle ligne, sélectionnez l'action **Autoriser**.
7. Activez la règle en effectuant un double-clic dans la cellule **État** de la ligne concernée.



Configurer le service VPN SSL et la vérification des postes clients (ZTNA)

Cette section explique comment configurer le service VPN SSL et la vérification des postes clients (ZTNA) du firewall SNS.

Configurer le service VPN SSL

Cette section explique comment activer et configurer le service VPN SSL du firewall SNS.

Rendez-vous dans le module **Configuration > VPN > VPN SSL**. Des différences existent entre les versions SNS. Une mention précise ces différences lorsque cela est pertinent. Vous pouvez cliquer sur **Appliquer** à tout moment pour sauvegarder vos modifications.

Activer le service VPN SSL

Champ	Description
Activer le VPN SSL 	Positionnez le sélecteur sur **ON** pour activer le service VPN SSL.

Configurer les paramètres généraux du service VPN SSL

Sur les versions SNS 4.8 LTSB et 5, cette configuration s'effectue dans l'onglet **Paramètres généraux**. Sur les versions SNS 4.3 LTSB, il n'existe pas d'onglet.

> **NOTE**
> Depuis la version SNS 4.8.5, un avertissement vous invite à désactiver la fonctionnalité de compression LZ4 si elle est activée. Ce cas est décrit dans la section Résoudre les problèmes.

Champ	Description
Activer la vérification des postes clients (ZTNA) 	Sur les versions SNS 5, positionnez le sélecteur sur **ON** pour activer la vérification de la conformité des postes clients. Sur les versions SNS 4.8 LTSB, l'activation s'effectue dans l'onglet **Vérification des postes clients (ZTNA)**. Cette fonctionnalité n'est pas disponible sur les versions SNS 4.3 LTSB. Lorsque la vérification des postes clients est activée : • Les clients VPN SSL compatibles avec cette fonctionnalité (voir Configurer la vérification des postes clients (ZTNA)) peuvent établir des tunnels VPN SSL avec le firewall SNS **seulement si tous** les critères de la politique sont respectés, • Les clients VPN SSL non compatibles avec cette fonctionnalité ne peuvent pas établir de tunnels VPN SSL avec le firewall SNS, **sauf** s'ils y sont explicitement autorisés en activant le paramètre **Clients VPN SSL non compatibles avec ZTNA**.

Zone Paramètres réseaux

Champ	Description
Adresse IP publique (ou FQDN) de l'UTM utilisée	Indiquez l'adresse que les utilisateurs doivent utiliser dans leur client VPN SSL pour joindre le firewall SNS et établir des tunnels VPN SSL. Vous pouvez indiquer un FQDN ou une adresse IP. • Pour un FQDN : il doit être déclaré dans les serveurs DNS utilisés par l'appareil de l'utilisateur. Si vous disposez d'une adresse IP publique dynamique, vous pouvez recourir aux services d'un fournisseur comme *DynDNS* ou *No-IP*. Paramétrez ensuite ce FQDN dans le module **Configuration > Réseau > DNS dynamique**. • Pour une adresse IP : elle doit être publique, donc accessible sur Internet.
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 les appareils de votre organisation les routes nécessaires pour joindre les ressources accessibles via le tunnel VPN SSL. Pour autoriser ou interdire plus finement les flux entre les appareils de vos utilisateurs et les ressources internes, vous devez créer des règles de filtrage (voir Configurer la politique de filtrage et de NAT). Si des appareils de votre organisation sont situés entre le firewall SNS et les ressources internes mises à disposition, vous pouvez définir sur ces appareils des routes statiques d'accès au réseau attribué aux clients VPN SSL.
Réseau assigné aux clients (UDP) **Réseau assigné aux clients (TCP)**	Sélectionnez l'objet correspondant aux réseaux UDP et TCP assignés aux clients VPN SSL. Choisissez le réseau ou sous-réseaux en fonction des critères suivants : • La taille minimale du masque réseau est de **/28**. • Si vous assignez deux réseaux, le client VPN SSL utilise toujours en premier le tunnel VPN SSL basé sur le protocole UDP pour de meilleures performances. Cet ordre est défini dans la configuration VPN SSL (OpenVPN) fourni par le firewall SNS aux clients VPN SSL. • Le réseau assigné ne doit pas appartenir 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. • Pour 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.

Champ	Description
Maximum de tunnels simultanés autorisés	Le nombre s'affiche automatiquement. Il correspond à la valeur minimale, soit du nombre de tunnels autorisés sur le firewall SNS (voir Prérequis), soit du nombre de sous-réseaux disponibles pour les clients VPN SSL. Pour ce dernier : • Sur les versions SNS 5 : cela présente le nombre total d'adresses IP, moins 3. • Sur les versions SNS 4.3 LTSB et 4.8 LTSB : cela représente 1/4 des adresses IP, moins 2. Un tunnel VPN SSL consomme 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.
Serveur DNS primaire **Serveur DNS secondaire**	Sélectionnez l'objet représentant le serveur DNS à attribuer.

Zone Configuration avancée

Champ	Description
Activer l'accélération noyau DCO	Sur les versions SNS 5 en configuration d'usine, la fonctionnalité d'accélération noyau DCO (*Data Channel Offload*) est activée par défaut. Cochez ou décochez la case pour activer ou désactiver cette fonctionnalité. Sur les versions SNS 4, cette fonctionnalité n'est pas disponible. Cette fonctionnalité permet d'améliorer les performances des **tunnels VPN SSL basés sur le protocole UDP**. Elle n'est pas compatible avec les tunnels VPN SSL basés sur le protocole TCP. Le client VPN SSL utilisé doit être compatible avec la fonctionnalité DCO pour bénéficier des améliorations. Concernant le client VPN SSL Stormshield : • La version Windows bénéficie des améliorations. • La version Linux bénéficie des améliorations **seulement si** OpenVPN est en version 2.6.0 ou supérieure et que le paquet **openvpn-dco** est installé. • La version macOS ne bénéficie pas des améliorations. **NOTE** Lorsque vous activez la fonctionnalité DCO, un message peut s'afficher vous invitant à modifier la suite de chiffrement si celle utilisée est incompatible. Acceptez la modification pour activer la fonctionnalité.
Adresse IP publique de l'UTM pour le VPN SSL (UDP)	Dans les cas suivants, vous devez sélectionner l'objet représentant l'adresse IP à joindre pour établir des tunnels VPN SSL en UDP : • L'adresse IP à joindre n'est pas l'adresse IP principale de l'interface externe, • L'adresse IP à joindre est portée par une interface externe qui n'est pas en lien avec la passerelle par défaut du firewall SNS.

Champ	Description
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 au terme duquel les clés utilisées par les algorithmes de chiffrement sont renégociées. Par défaut, ce délai est de 14400 secondes, soit 4 heures. 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 afin de rester connecté. Pour ce cas d'utilisation, il est recommandé d'augmenter le délai avant renégociation des clés pour l'aligner sur la durée moyenne d'une journée travaillée, par exemple à 28800 secondes, soit 8 heures.
Utiliser les serveurs DNS fournis par le firewall	Vous pouvez indiquer aux clients VPN SSL 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 SSL 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

Le client VPN SSL Stormshield sous Windows 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 SSL. Exemple de script permettant de connecter le lecteur réseau Z: à un partage : `NET USE Z: \\myserver\myshare`
Script à exécuter lors de la déconnexion	Sélectionnez le script à exécuter à la fermeture du tunnel VPN SSL. Exemple de script permettant de déconnecter le lecteur réseau Z: d'un partage : `NET USE Z: /delete`

Le client VPN SSL Stormshield sous Linux et macOS peut également exécuter des scripts à l'ouverture et à la fermeture d'un tunnel VPN SSL. Ces scripts sont généralement utilisés pour prendre en compte la configuration DNS lorsqu'OpenVPN ne la gère pas nativement. Pour plus d'informations sur l'utilisation de ces scripts, reportez-vous au Guide d'installation du client VPN SSL Stormshield v5.

Certificats

Sélectionnez les certificats que le service VPN SSL du firewall SNS et les clients VPN SSL doivent présenter pour établir des tunnels VPN SSL. Ces certificats doivent être issus de la même autorité de certification.

Par défaut, un certificat serveur et un certificat client, issus de la même autorité de certification dédiée au VPN SSL, sont proposés. Ces certificats et l'autorité de certification ont été créés à l'initialisation du firewall SNS.

Champ	Description
Certificat serveur	Sélectionnez le certificat souhaité. L'icône indique les certificats dont la clé privée est protégée par le module TPM. Pour plus d'informations sur cette protection, 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 module TPM car la clé privée de ce certificat doit être disponible en clair (non chiffrée) dans la configuration VPN SSL distribuée aux clients VPN SSL.

Configuration

Champ	Description
Exporter le fichier de configuration	Cliquez sur ce bouton pour exporter la configuration VPN SSL au format OVPN. Vous pouvez ensuite importer ce fichier dans les clients VPN SSL de votre organisation afin d'y ajouter une nouvelle connexion. Concernant le client VPN SSL Stormshield, cette configuration est récupérée automatiquement pour les connexions établies en **Mode Stormshield**. Pour les connexions de type OpenVPN (import de fichier OVPN), le fichier doit être importé pour établir ou enregistrer la connexion. Pour plus d'informations, reportez-vous au Guide de configuration et d'utilisation du client VPN SSL Stormshield v5.

Configurer la vérification des postes clients (ZTNA)

Cette section explique comment configurer une politique de vérification de la conformité des postes clients qui établissent des tunnels VPN SSL avec le firewall SNS. Avec cette vérification, un poste de travail ou un utilisateur non conforme aux critères de la politique définie sur le firewall SNS ne peut pas établir de tunnels VPN SSL avec le firewall SNS.

Vous pouvez cliquer sur **Appliquer** à tout moment pour sauvegarder vos modifications.

Informations générales sur l'accès réseau *Zero Trust* (ZTNA)

Le ZTNA consiste à ne faire confiance aux utilisateurs et aux appareils qu'après leur vérification. Pour cela, le ZTNA peut s'appuyer sur les composantes suivantes :

- Une garantie de la conformité du canal de communication grâce au chiffrement TLS des tunnels VPN SSL,
- Une vérification des utilisateurs, par exemple avec une authentification multifacteur comme la solution TOTP Stormshield (voir Utiliser une authentification multifacteur).
- Une politique de vérification de la conformité des postes clients et des utilisateurs. Cette configuration est abordée juste ci-dessous.

- Un filtrage fin pour limiter l'accès des utilisateurs aux seules ressources nécessaires (voir Configurer la politique de filtrage et de NAT).

Prérequis

Pour utiliser une politique de vérification de la conformité des postes clients, vous devez vous conformer aux prérequis suivants :

- Disposer d'un firewall SNS en version 4.8 LTSB ou 5.
- Disposer d clients VPN SSL compatibles avec la fonctionnalité de vérification des postes clients :
  - Le client VPN SSL Stormshield en version 4.0 ou supérieure est compatible. Il doit être configuré en **Mode Stormshield** pour les versions 5 ou en **Mode automatique** pour les versions 4.
  - Les clients VPN SSL tiers, comme OpenVPN Connect, ne sont pas compatibles.

Configurer la vérification des postes clients sur les versions SNS 5

Rendez-vous dans **Configuration > VPN > VPN SSL**. La configuration s'effectue dans les onglets **Vérifications des postes clients (ZTNA)** et **Vérification des postes clients Windows (ZTNA)**.

Onglet Vérifications des postes clients (ZTNA)

Version du client VPN SSL Stormshield

Cochez la case pour activer la zone de paramétrage des versions exigibles.

Champ	Description
Autoriser une plage de versions (v4.0.0 minimum)	Sélectionnez cette option pour autoriser plusieurs versions du client VPN SSL Stormshield à établir des tunnels VPN SSL (cas d'un parc hétérogène de clients VPN SSL Stormshield). En sélectionnant cette option : • Vous devez renseigner la **Version minimale** des clients VPN SSL Stormshield autorisés à établir des tunnels VPN SSL avec le firewall SNS, • Vous pouvez renseigner la **Version maximale**, ou laisser ce champ vide pour autoriser toutes les versions égales ou supérieures à la version minimale à établir des tunnels VPN SSL avec le firewall SNS.
N'autoriser qu'une seule version	Sélectionnez cette option pour autoriser exclusivement une seule version du client VPN SSL Stormshield. Vous devez alors renseigner la version exacte des clients VPN SSL Stormshield autorisés à établir des tunnels VPN SSL avec le firewall SNS.

Autoriser l'établissement de tunnels pour les clients additionnels suivants

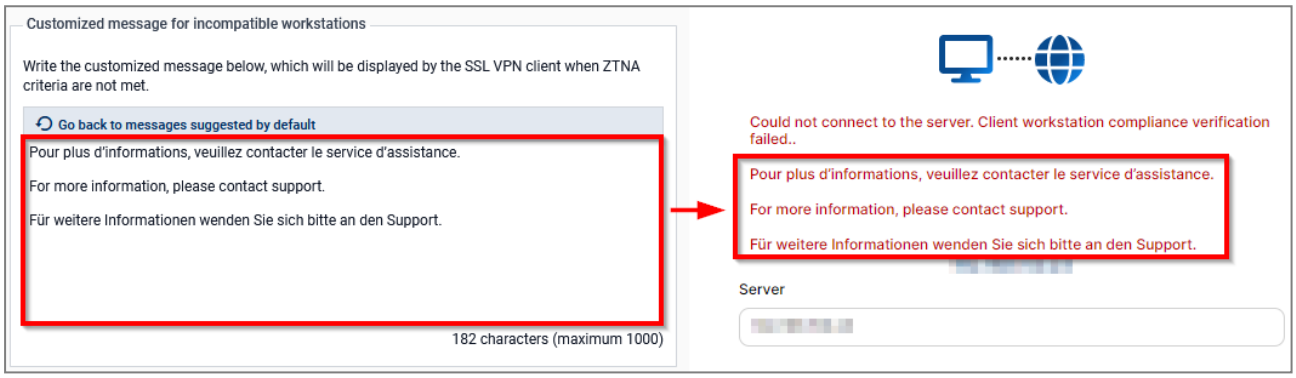
Champ	Description
Clients VPN SSL Stormshield (Linux ou macOS)	Cochez la case si le parc de clients VPN SSL Stormshield de votre organisation comporte des clients VPN SSL Stormshield sous Linux et/ou macOS. Ainsi, les critères spécifiques Windows ne sont pas pris en compte pour ces postes.
Clients VPN SSL non compatibles avec ZTNA	Cochez la case pour autoriser les clients VPN SSL non compatibles avec la fonctionnalité de vérification des postes clients à établir des tunnels VPN SSL avec le firewall SNS, par exemple pour une utilisation avec des terminaux mobiles.

Message personnalisé pour les postes non compatibles

En cas d'échec d'établissement d'un tunnel VPN SSL du fait d'une non-conformité à la politique, le client VPN SSL Stormshield affiche par défaut le message "*Pour plus d'informations, veuillez contacter le service d'assistance*" en français, anglais et allemand.

Dans la zone de saisie, vous pouvez modifier ce message ou le supprimer si vous ne souhaitez pas afficher de message additionnel. Notez qu'aucun mécanisme de traduction automatique n'est mis en place : vous devez donc prendre en charge la traduction du message.

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



Onglet Vérification des postes clients Windows (ZTNA)

IMPORTANT
Si vous sélectionnez ci-dessous plusieurs critères, ils doivent tous être respectés pour que le client VPN SSL soit autorisé à établir des tunnels VPN SSL avec le firewall SNS.

Champ	Description
Antivirus du poste client actif et à jour	En cochant cette case, 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, ce qui permet de prendre en charge les antivirus tiers tant que leur état est reconnu. **NOTE** Le service Windows permettant de vérifier l'état de l'antivirus met quelques minutes à démarrer après l'ouverture d'une session. Les utilisateurs doivent donc attendre quelques minutes après l'ouverture de leur session Windows avant d'établir un tunnel VPN SSL.
Firewall actif sur le poste client	En cochant cette case, le Pare-feu Windows du poste de travail doit être en cours d'exécution et les profils *Réseau avec domaine*, *Réseau privé* et *Réseau public* doivent être activés. Le critère est considéré comme non conforme si un profil est inactif. **NOTE** Le service Windows permettant de vérifier l'état du Pare-feu Windows met quelques minutes à démarrer après l'ouverture d'une session. Les utilisateurs doivent donc attendre quelques minutes après l'ouverture de leur session Windows avant d'établir un tunnel VPN SSL.

Champ	Description
SES installé sur le poste client	En cochant cette case, l'agent SES Evolution doit être installé 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	En cochant cette case, un utilisateur disposant de droits d'administration sur le poste de travail ne peut pas établir de tunnels VPN SSL avec le firewall SNS.

Vérifier la version de Windows 10 / Windows 11 (numéro de build)

Cochez la case pour activer la zone de paramétrage des versions exigibles de Windows 10 et Windows 11. La configuration s'effectue dans l'onglet correspondant à la version concernée.

Champ	Description
Autoriser une plage de versions (builds)	Sélectionnez cette option pour autoriser plusieurs versions de Windows (cas d'un parc hétérogène de postes de travail Windows). En sélectionnant cette option : • Vous devez renseigner la **Version minimale** que doit posséder le poste de travail pour être autorisé à établir des tunnels VPN SSL avec le firewall SNS. Les versions par défaut sont : 10000 pour Windows 10 et 20000 pour Windows 11. • Vous pouvez renseigner la **Version maximale**, ou laisser ce champ vide pour autoriser toutes les versions égales ou supérieures à la version minimale à établir des tunnels VPN SSL avec le firewall SNS.
N'autoriser qu'une seule version	Sélectionnez cette option pour autoriser exclusivement une seule version de Windows. Vous devez alors renseigner la version exacte de Windows des postes de travail autorisés à établir des tunnels VPN SSL avec le firewall SNS.

Appartenance à un domaine d'entreprise

Champ	Description
Vérifier que la machine est rattachée à un domaine d'entreprise	En cochant cette case, vous devez ajouter dans la grille les domaines d'appartenance des postes de travail autorisés à établir des tunnels VPN SSL avec le firewall SNS. Notez que ce critère n'est pas lié à la configuration d'un annuaire sur le firewall SNS.
Vérifier que l'utilisateur appartient à un domaine d'entreprise	En cochant cette case, vous devez ajouter dans la grille les domaines d'appartenance des utilisateurs autorisés à établir des tunnels VPN SSL avec le firewall SNS. Avec ce critère, le nom complet de l'utilisateur incluant le 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 tunnels VPN SSL. Notez que ce critère n'est pas lié à la configuration d'un annuaire sur le firewall SNS.

Configurer la vérification des postes clients sur les versions SNS 4.8 LTSB

Rendez-vous dans **Configuration > VPN > VPN SSL**. La configuration s'effectue dans l'onglet **Vérification des postes clients (ZTNA)**.

Champ	Description
Activer la vérification des postes clients (ZTNA)	Cochez la case pour activer la vérification de la conformité des postes clients. Lorsqu'elle est activée : • Les clients VPN SSL compatibles avec cette fonctionnalité peuvent établir des tunnels VPN SSL avec le firewall SNS **seulement si tous** les critères de la politique sont respectés, • Les clients VPN SSL non compatibles avec cette fonctionnalité ne peuvent pas établir de tunnels VPN SSL avec le firewall SNS, **sauf** s'ils y sont explicitement autorisés en activant le paramètre **Clients VPN SSL non compatibles avec ZTNA**.
Autoriser l'établissement de tunnels pour des clients VPN SSL Stormshield Linux ou Mac	Cochez la case si le parc de clients VPN SSL Stormshield de votre organisation comporte des clients VPN SSL Stormshield sous Linux et/ou macOS. Ainsi, les critères spécifiques Windows ne sont pas pris en compte pour ces postes.
Autoriser l'établissement de tunnels pour des clients non compatibles avec ZTNA	Cochez la case pour autoriser les clients VPN SSL non compatibles avec la fonctionnalité de vérification des postes clients à établir des tunnels VPN SSL avec le firewall SNS, par exemple pour une utilisation avec des terminaux mobiles.

Paramètres de vérification des postes clients (ZTNA)

IMPORTANT
Si vous sélectionnez ci-dessous plusieurs critères, ils doivent tous être respectés pour que le client VPN SSL soit autorisé à établir des tunnels VPN SSL avec le firewall SNS.

Champ / Critère	Description
Antivirus du poste client actif et à jour	En cochant cette case, 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, ce qui permet de prendre en charge les antivirus tiers tant que leur état est reconnu. **NOTE** Le service Windows permettant de vérifier l'état de l'antivirus met quelques minutes à démarrer après l'ouverture d'une session. Les utilisateurs doivent donc attendre quelques minutes après l'ouverture de leur session Windows avant d'établir un tunnel VPN SSL.

Champ / Critère	Description
Firewall actif sur le poste client	En cochant cette case, le Pare-feu Windows du poste de travail doit être en cours d'exécution et les profils *Réseau avec domaine*, *Réseau privé* et *Réseau public* doivent être activés. Le critère est considéré comme non conforme si un profil est inactif. **NOTE** Le service Windows permettant de vérifier l'état du Pare-feu Windows met quelques minutes à démarrer après l'ouverture d'une session. Les utilisateurs doivent donc attendre quelques minutes après l'ouverture de leur session Windows avant d'établir un tunnel VPN SSL.
SES installé sur le poste client	En cochant cette case, l'agent SES Evolution doit être installé 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	En cochant cette case, un utilisateur disposant de droits d'administration sur le poste de travail ne peut pas établir de tunnels VPN SSL avec le firewall SNS.
Vérifier les versions (numéro de build) de Windows 10 / Windows 11	Cochez la case pour activer la zone de paramétrage des versions exigibles de Windows 10 et Windows 11. La configuration s'effectue dans l'onglet correspondant à la version concernée. • **Autoriser une plage de versions (builds)** : sélectionnez cette option pour autoriser plusieurs versions de Windows (cas d'un parc hétérogène de postes de travail Windows). En sélectionnant cette option : ◦ Vous devez renseigner la **Version minimale** que doit posséder le poste de travail pour être autorisé à établir des tunnels VPN SSL avec le firewall SNS. Les versions par défaut sont : 10000 pour Windows 10 et 20000 pour Windows 11. ◦ Vous pouvez renseigner la **Version maximale**, ou laisser ce champ vide pour autoriser toutes les versions égales ou supérieures à la version minimale à établir des tunnels VPN SSL avec le firewall SNS. • **N'autoriser qu'une seule version** : sélectionnez cette option pour autoriser exclusivement une seule version de Windows. Vous devez alors renseigner la version exacte de Windows des postes de travail autorisés à établir des tunnels VPN SSL avec le firewall SNS.
Onglet Machine rattachée à un domaine	En cochant la case **La machine doit être rattachée à un domaine d'entreprise**, vous devez ajouter dans la grille les domaines d'appartenance des postes de travail autorisés à établir des tunnels VPN SSL avec le firewall SNS. Notez que ce critère n'est pas lié à la configuration d'un annuaire sur le firewall SNS.
Onglet Utilisateur rattaché à un domaine	En cochant la case **L'utilisateur doit être rattaché à un domaine d'entreprise**, vous devez ajouter dans la grille les domaines d'appartenance des utilisateurs autorisés à établir des tunnels VPN SSL avec le firewall SNS. Avec ce critère, le nom complet de l'utilisateur incluant le 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 tunnels VPN SSL. Notez que ce critère n'est pas lié à la configuration d'un annuaire sur le firewall SNS.

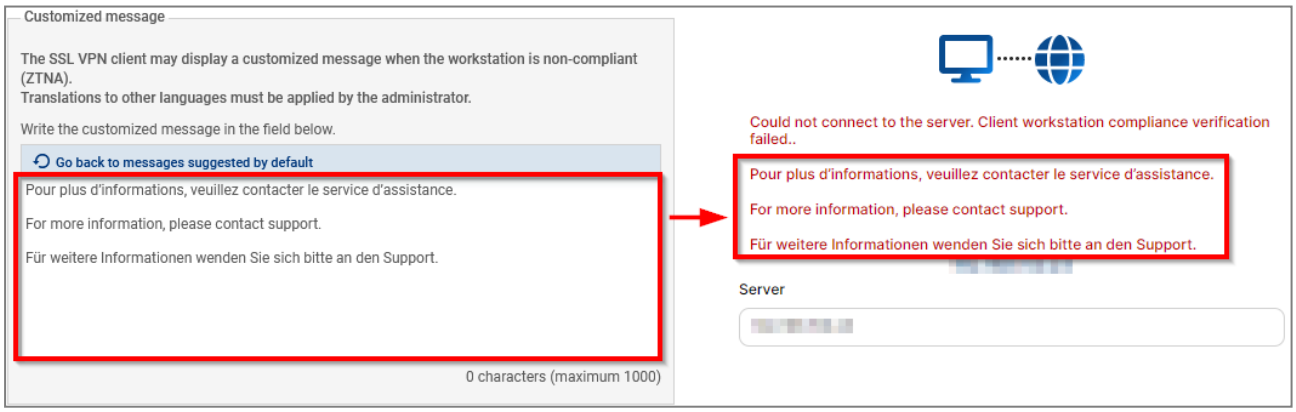
Champ / Critère	Description
Version du client VPN SSL Stormshield	Cochez la case **Vérifier la version du client VPN SSL Stormshield** pour activer la zone de paramétrage des versions exigibles. • **Autoriser une plage de versions (builds)** : sélectionnez cette option pour autoriser plusieurs versions du client VPN SSL Stormshield à établir des tunnels VPN SSL (cas d'un parc hétérogène de clients VPN SSL Stormshield). En sélectionnant cette option : ◦ Vous devez renseigner la **Version minimale** des clients VPN SSL Stormshield autorisés à établir des tunnels VPN SSL avec le firewall SNS. ◦ Vous pouvez renseigner la **Version maximale**, ou laisser ce champ vide pour autoriser toutes les versions égales ou supérieures à la version minimale à établir des tunnels VPN SSL avec le firewall SNS. • **N'autoriser qu'une seule version** : sélectionnez cette option pour autoriser exclusivement une seule version du client VPN SSL Stormshield. Vous devez alors renseigner la version exacte des clients VPN SSL Stormshield autorisés à établir des tunnels VPN SSL avec le firewall SNS.

Message personnalisé

En cas d'échec d'établissement d'un tunnel VPN SSL du fait d'une non-conformité à la politique, le client VPN SSL Stormshield affiche par défaut le message "*Pour plus d'informations, veuillez contacter le service d'assistance*" en français, anglais et allemand.

Dans la zone de saisie, vous pouvez modifier ce message ou le supprimer si vous ne souhaitez pas afficher de message additionnel. Notez qu'aucun mécanisme de traduction automatique n'est mis en place : vous devez donc prendre en charge la traduction du message.

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



Configurer la politique de filtrage et de NAT

Cette section présente la configuration de la politique de filtrage et de NAT à réaliser pour mettre en œuvre des tunnels VPN SSL. Vous pouvez cliquer sur **Appliquer** à tout moment pour sauvegarder vos modifications.

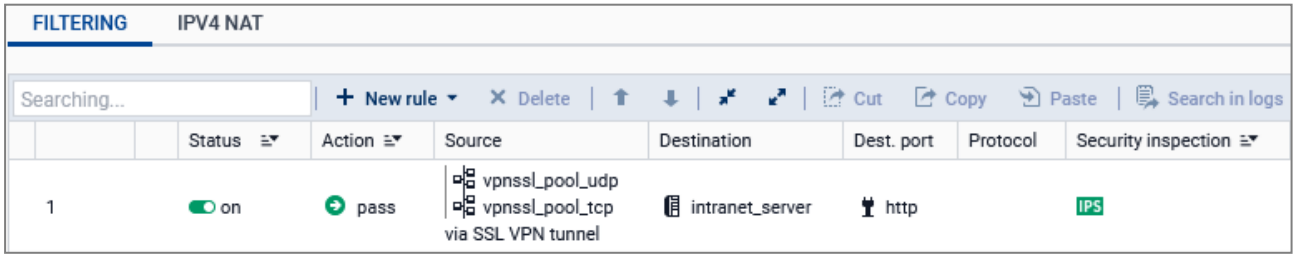
Configurer la politique de filtrage

Vous devez définir des règles pour autoriser ou interdire l'accès aux ressources internes de votre organisation aux clients VPN SSL. Dans l'exemple ci-dessous, nous ajoutons une règle 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 renforcer la sécurité, vous pouvez mettre en place un filtrage fin afin de limiter l'accès des utilisateurs aux seules ressources nécessaires. Pour cela, créez des règles pour chaque groupe d'utilisateurs établissant des tunnels VPN SSL avec le firewall SNS (dans la fenêtre d'édition de la règle : onglet **Utilisateur** sur les versions SNS 5 ou onglet **Source**, champ **Utilisateur** sur les versions SNS 4).

1. Rendez-vous dans **Configuration > Politique de sécurité > Filtrage et NAT**, onglet **Filtrage**.
2. Cliquez sur **Nouvelle règle > Règle simple** et 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** :
   a. Sous-onglet **Général**, champ **Machines sources**, sélectionnez les objets représentant les adresses IP des clients VPN SSL en UDP et TCP,
   b. Sous-onglet **Configuration avancée**, champ **Via**, sélectionnez *Tunnel VPN SSL*.
6. Dans l'onglet **Destination**, champ **Machines destinations**, sélectionnez l'objet représentant le serveur interne ou le réseau intranet.
7. Dans l'onglet **Port / Protocole**, champ **Port destination**, sélectionnez *http*.
8. Cliquez sur **OK**.

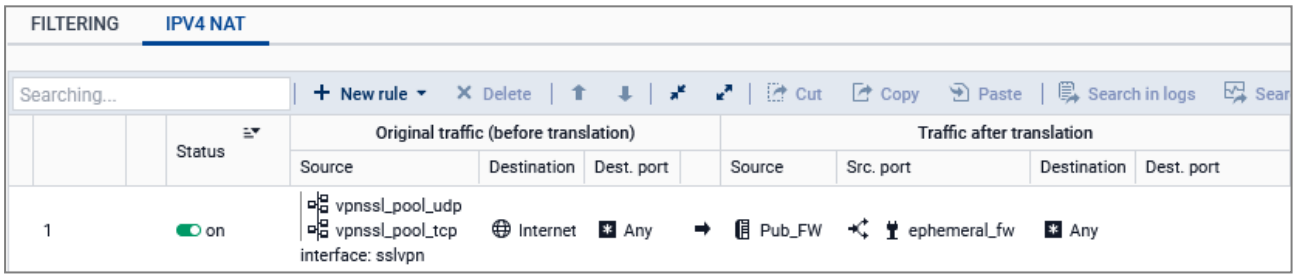
NOTE
Les règles sont examinées dans l'ordre de leur numérotation. Vous pouvez également faire appel aux fonctions avancées de filtrage (profils d'inspection, proxies applicatifs, contrôle antiviral, ...).



Configurer la politique de 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. Rendez-vous dans **Configuration > Politique de sécurité > Filtrage et NAT**, onglet **NAT**.
2. 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.
3. Dans l'onglet **Général**, champ **État**, sélectionnez *On*.
4. Dans l'onglet **Source originale** :
   a. Champ **Machines sources**, sélectionnez les objets représentant les adresses IP des clients VPN SSL en UDP et en TCP,
   b. Champ **Interface d'entrée**, sélectionnez *VPN SSL*.
5. Dans l'onglet **Destination originale**, champ **Machines destinations**, sélectionnez *Internet*.
6. Dans l'onglet **Source translatée**, champ **Machine source translatée**, sélectionnez l'objet représentant l'adresse IP publique.
7. Dans le champ **Port source translaté**, cochez **choisir aléatoirement le port source translaté**.
8. Cliquez sur **OK**.



Suivre les utilisateurs connectés

Cette section explique comment suivre dans l'interface Web d'administration du firewall SNS les utilisateurs actuellement connectés ou qui se sont connectés en VPN SSL.

Pour améliorer la lisibilité des images, certaines colonnes des tableaux ont été masquées. L'affichage sur votre firewall SNS peut donc être légèrement différent. Toutes les colonnes disponibles ne sont pas décrites dans cette section. Pour plus d'informations, reportez-vous au manuel utilisateur v4 ou au manuel utilisateur v5 selon la version SNS utilisée.

Informations concernant l'accès aux données personnelles

Certaines informations sont accessibles sous réserve d'activer le droit de consulter les données personnelles. Si vous disposez de ce droit ou d'un code d'accès aux données personnelles :

- Sur les versions SNS 5 : cliquez sur l'icône représentant un utilisateur dans le bandeau supérieur, puis cliquez sur **Obtain personal data access**. Si un code d'accès est demandé, renseignez-le puis cliquez sur **Obtenir**.
- Sur les versions SNS 4 : cliquez sur **Logs : accès restreint** dans le bandeau supérieur. Si un code d'accès est demandé, renseignez-le puis cliquez sur **Obtenir**.

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

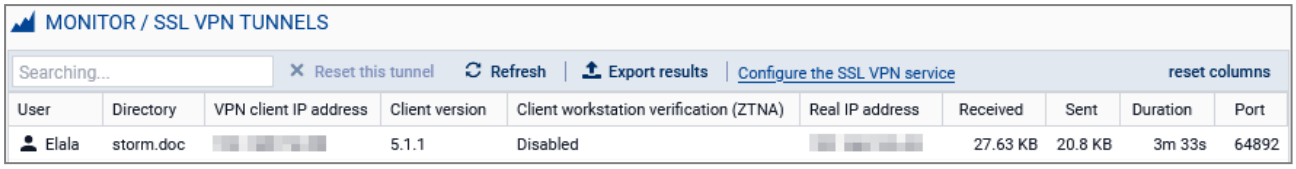
Afficher les utilisateurs actuellement connectés sur le firewall SNS en VPN SSL

Dans la supervision des tunnels VPN SSL

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

Cette vue affiche en temps réel les utilisateurs connectés sur le firewall SNS en VPN SSL et des informations concernant leur session (adresses IP, nombre d'octets émis et reçus, etc.).

Colonne	Description
Utilisateur	Indique le nom de l'utilisateur actuellement connecté sur le firewall SNS en VPN SSL.
Version du client	Indique la version du client VPN SSL Stormshield utilisé par l'utilisateur pour se connecter. Pour les clients VPN SSL non compatibles avec la fonctionnalité de vérification des postes clients, la valeur "*N/A*" s'affiche. Cette colonne est disponible uniquement sur les versions SNS 4.8 LTSB et 5.
Vérification des postes clients (ZTNA)	Indique l'état de conformité du poste client. Plusieurs valeurs sont possibles : • **Désactivé** : la fonctionnalité de vérification des postes clients n'est pas activée. • **Non vérifié** : le client VPN SSL utilisé pour établir le tunnel VPN SSL n'est pas compatible avec la fonctionnalité de vérification des postes clients, mais l'établissement de tunnels VPN SSL pour les clients non compatibles est autorisé. • **Conforme** : le poste client est conforme aux critères définis dans la politique de vérification des postes clients. Cette colonne est disponible uniquement sur les versions SNS 4.8 LTSB et 5.

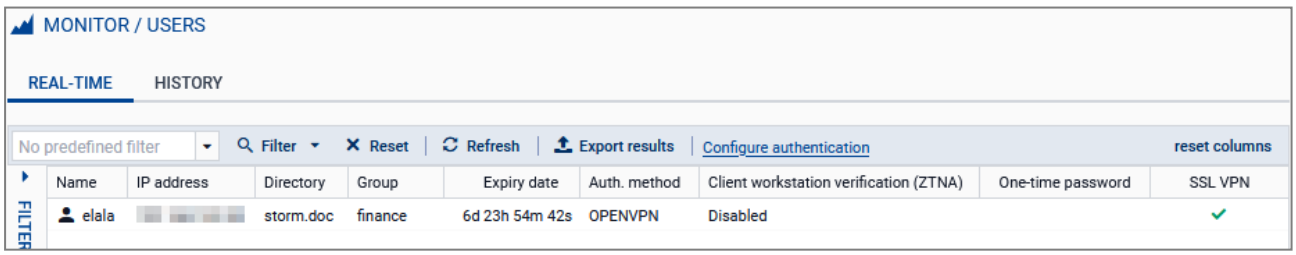


Dans la supervision des utilisateurs

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

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

Colonne	Description
Utilisateur	Indique le nom de l'utilisateur actuellement connecté sur le firewall SNS. Pour savoir si l'utilisateur s'est connecté au firewall SNS en VPN SSL, vérifiez la colonne "**VPN SSL**".
Vérification des postes clients (ZTNA)	Indique l'état de conformité du poste client. Plusieurs valeurs sont possibles : • **Désactivé** : la fonctionnalité de vérification des postes clients n'est pas activée. • **Non vérifié** : le client VPN SSL utilisé pour établir le tunnel VPN SSL n'est pas compatible avec la fonctionnalité de vérification des postes clients, mais l'établissement de tunnels VPN SSL pour les clients non compatibles est autorisé. • **Conforme** : le poste client est conforme aux critères définis dans la politique de vérification des postes clients. Cette colonne est disponible uniquement sur les versions SNS 4.8 LTSB et 5.
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. Cette colonne est disponible uniquement sur les versions SNS 4.8 LTSB et 5.
VPN SSL	Permet d'identifier les utilisateurs connectés sur le firewall SNS en VPN SSL.



Consulter les journaux des événements liés aux tunnels VPN

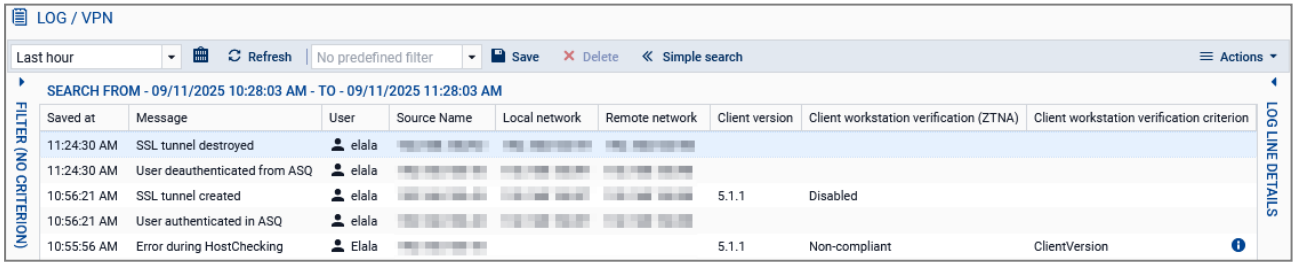
Rendez-vous dans **Monitoring > Logs - Journaux d'audit > VPN**.

Ce journal affiche les événements liés aux tunnels VPN SSL et VPN IPsec.

Par défaut, les événements de la dernière heure sont affichés. Vous pouvez modifier l'échelle de temps en sélectionnant une autre valeur dans la barre d'outils au-dessus de la grille.

Colonne	Description
Enregistré à	Indique la date et l'heure de l'événement.

Colonne	Description
Message	Indique la nature de l'événement : tunnel VPN connecté ou déconnecté, authentification de l'utilisateur dans le moteur d'authentification du firewall, etc. Sur les versions SNS 4.8 LTSB et 5, des messages liés à la fonctionnalité de vérification des postes clients peuvent s'afficher (appelée *HostChecking* dans les journaux) : • **Error during authentication : HostChecking failed** avec une valeur "*Non vérifié*" dans la colonne "**Vérification des postes clients (ZTNA)**" : la connexion ne s'est pas établie car le client VPN SSL utilisé n'est pas compatible avec la fonctionnalité de vérification des postes clients et l'établissement de tunnels VPN SSL pour les clients non compatibles n'est pas autorisé dans la politique. • "*Error during HostChecking*" avec une valeur "*Non conforme*" dans la colonne "**Vérification des postes clients (ZTNA)**" : la connexion ne s'est pas établie car le poste client n'est pas conforme aux critères définis dans la politique de vérification des postes clients.
Utilisateur	Indique l'utilisateur associé à l'événement.
Vérification des postes clients (ZTNA)	Indique l'état de conformité du poste client. Plusieurs valeurs sont possibles : • **Désactivé** : la fonctionnalité 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 VPN SSL 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. Cette colonne est disponible uniquement sur les versions SNS 4.8 LTSB et 5.
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. Cette colonne est disponible uniquement sur les versions SNS 4.8 LTSB et 5.



Résoudre les problèmes

Cette section liste certains problèmes fréquemment rencontrés lors de l'utilisation du VPN SSL. Si celui que vous rencontrez ne se trouve pas dans ce chapitre, nous vous recommandons de consulter la Base de connaissances Stormshield (authentification nécessaire).

Un utilisateur ne parvient pas à se connecter et le message "*La vérification de la conformité du poste client a échoué*" s'affiche

- *Situation* : Lorsqu'un utilisateur tente de se connecter, le tunnel VPN SSL ne s'établit pas et le message "*La vérification de la conformité du poste client a échoué*" s'affiche sur son client VPN SSL Stormshield.
- *Cause* : Le poste client utilisé ne respecte pas tous les critères définis dans la politique de vérification des postes clients (ZTNA).
- *Solutions* :
  - Vérifiez les critères non conformes en vous reportant à la section Consulter les journaux des événements liés aux tunnels VPN, puis mettez en conformité le poste client.
  - Vérifiez la configuration de la politique de vérification des postes clients en vous reportant à la section Configurer la vérification des postes clients (ZTNA).

Une ressource interne n'est pas accessible via le tunnel VPN SSL

- *Situation* : Le tunnel VPN SSL est établi, mais une ressource interne 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.

Un avertissement indique que la fonctionnalité de compression LZ4 est obsolète

- *Situation* : Dans l'interface Web d'administration d'un firewall SNS en version 4.8.5 ou supérieure, un avertissement s'affiche dans le module VPN SSL si la fonctionnalité de compression LZ4 est activée.
- *Cause* : La fonctionnalité de compression LZ4 est obsolète et il est recommandé de la désactiver.
- *Solution* : Dans la fenêtre d'avertissement, acceptez de désactiver cette fonctionnalité. Si vous avez ignoré cet avertissement, un message reste affiché tant que cette fonctionnalité n'est pas désactivée. Pour cela, vous devez utiliser les commandes CLI Serverd suivantes :

```
CONFIG OPENVPN UPDATE compress=0
CONFIG OPENVPN ACTIVATE
```

Pour aller plus loin

Pour plus d'informations sur l'installation, la mise à jour et la désinstallation du client VPN SSL Stormshield, reportez-vous au Guide d'installation du client VPN SSL Stormshield v5.

Pour configurer et utiliser le client VPN SSL Stormshield, reportez-vous au Guide de configuration et d'utilisation du client VPN SSL Stormshield v5.

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

STORMSHIELD

documentation@stormshield.eu