STORMSHIELD

STORMSHIELD NETWORK SECURITY

STORMSHIELD NETWORK SSL VPN CLIENT

NOTES DE VERSION

Version 4

Dernière mise à jour du document : 13 décembre 2024

Référence : sns-fr-ssl_vpn_client-notes_de_version-v4.0.9

Table des matières

Dans la documentation, Stormshield Network SSL VPN Client est désigné sous la forme abrégée : SN SSL VPN Client et Stormshield Network Security sous la forme abrégée SNS.

Ce document n'est pas exhaustif et d'autres modifications mineures ont pu être incluses dans cette version.

Historique des modifications

Date	Description
13 décembre 2024	Retrait du label « Early Adopter » (EA) de la version 4.0.9
13 novembre 2024	Nouveau document

Changements de comportement

Cette section liste les changements de comportements automatiques liés à la mise à jour de SN SSL VPN Client en version 4.0.9 depuis la dernière version 3 disponible.

Changements introduits en version 4.0.5 EA

- Carnet d'adresses - Le format du carnet d'adresses a évolué afin de renforcer la sécurité de SN SSL VPN Client en version 4. Ce nouveau format n'est pas compatible avec les versions inférieures. Pour plus d'informations, reportez-vous à la section **Limitations et précisions sur les cas d'utilisation** de la note technique *Configurer et utiliser le VPN SSL des firewalls SNS*.
- Compatibilité - SN SSL VPN Client n'est désormais plus compatible avec Windows 8.1.
- Certificats :
  - Les algorithme SHA-1 et MD5 permettant de signer les certificats étant obsolètes, ils ne seront plus supportés dans une version ultérieure de SN SSL VPN Client. Il est impératif que les administrateurs mettent à jour leurs certificats dès maintenant. Veuillez trouver la procédure dans l'article **How can I regenerate the sslvpn-full-default-authority?** de la base de connaissances Stormshield (anglais uniquement).
  - Le répertoire d'installation de SN SSL VPN Client en version 4 a été modifié. À la première connexion, certains utilisateurs devront indiquer de nouveau le certificat du firewall SNS comme étant de confiance.

Correctifs de la version 4.0.9

Système

Communication avec le processus OpenVPN

Des améliorations ont été apportées au mécanisme de vérification du port utilisé par le client VPN SSL Stormshield pour communiquer avec le processus OpenVPN. Les erreurs "Impossible de réserver le port permettant de communiquer avec le processus OpenVPN" et "Impossible de vider le fichier de log du processus OpenVPN" ne s'affichent plus de manière inopinée.

Désormais, lorsque la vérification du port échoue, le message "La connexion avec le processus OpenVPN n'est pas sécurisée" s'affiche.

Installation multi-comptes

Des améliorations ont été apportées à la fonctionnalité d'installation multi-comptes. Dorénavant, si un tunnel VPN est établi sur une session verrouillée, ce tunnel est automatiquement déconnecté lorsqu'un autre utilisateur ouvre sa propre session.

Il n'est plus nécessaire de demander à chaque utilisateur partageant un poste de travail de fermer leur session après utilisation. Chaque utilisateur peut donc établir son propre tunnel, mais un seul tunnel ne peut être établi à la fois sur le poste.

Accès aux journaux (Logs)

Lorsqu'il n'y a pas eu de tentative de connexion et qu'aucun log n'a été créé, un clic sur le menu contextuel **Journaux (Logs)** renvoie désormais correctement vers le répertoire de destination des logs.

Connexion

Connexion au firewall SNS - Port TCP ou UDP bloqué

Lorsque la connexion au firewall SNS n'aboutit pas car le port TCP ou UDP y a été bloqué, le client VPN SSL Stormshield ne tente plus à tort de se connecter de manière ininterrompue. Désormais, le message "Connexion au VPN SSL impossible : le nombre maximal de tentatives de connexion a été atteint" s'affiche après 5 tentatives de connexion.

Connexion au firewall SNS en version 4.3 - Certificat personnalisé

Référence support 84992

Il est de nouveau possible pour les utilisateurs d'établir un tunnel VPN avec un certificat personnalisé lorsque le firewall est en version SNS 4.3. Cette régression était apparue en version 4.0.5 EA.

Saisie du champ Code OTP - Mode Push

La saisie du champ **Code OTP** n'est plus obligatoire, rendant de nouveau possible la connexion via une notification *Push* (**Mode Push**). Cette régression était apparue en version 4.0.5 EA.

Mode manuel

Affichage des profils dans le menu contextuel

Les entrées contenues dans le carnet d'adresses du client VPN SSL Stormshield ne s'affichent plus à tort dans le menu contextuel **Mode manuel**.

Ajout ou suppression d'un profil lorsqu'un tunnel VPN est établi

Il n'est désormais plus possible d'ajouter ou de supprimer un profil dans le menu contextuel **Mode manuel** lorsqu'un tunnel VPN est établi. Auparavant, des éléments résiduels d'un profil pouvaient persister lorsque ce dernier était supprimé alors qu'un tunnel VPN était établi.

Compatibilité

Pour plus d'informations, reportez-vous à la section VPN SSL Client du *Guide de cycle de vie produits*.

Pour plus d'informations sur la compatibilité des méthodes d'authentification et des fonctionnalités de SN SSL VPN Client, reportez-vous à la section Spécificités du client VPN SSL Stormshield de la note technique *Configurer et utiliser le VPN SSL des firewalls SNS*.

Problèmes connus

La liste actualisée des problèmes connus relatifs à cette version de SN SSL VPN Client est consultable sur la Base de connaissances Stormshield (anglais uniquement). Pour vous connecter à la Base de connaissances, utilisez les mêmes identifiants que sur votre espace client MyStormshield.

Limitations et précisions sur les cas d'utilisation

Pour plus d'informations, reportez-vous à la section Limitations et précisions sur les cas d'utilisation de la note technique *Configurer et utiliser le VPN SSL des firewalls SNS*.

Ressources documentaires

Les ressources documentaires techniques sont disponibles sur le site de Documentation Technique Stormshield. Nous vous invitons à vous appuyer sur ces ressources pour exploiter au mieux l'ensemble des fonctionnalités de cette version.

Merci de consulter la Base de connaissances Stormshield pour obtenir des informations techniques spécifiques créées par l'équipe du support technique (Technical Assistance Center).

Télécharger cette version

Suivez les étapes ci-dessous pour télécharger la version 4.0.9 de SN SSL VPN Client.

1. Connectez-vous à votre espace personnel MyStormshield.
2. Rendez-vous dans **Téléchargements > Téléchargements**.
3. Dans les catégories, sélectionnez **Stormshield Network Security > VPN SSL**.
4. Cliquez sur le programme d'installation du SN SSL VPN Client (fichier *.msi* ou *.exe*). Le téléchargement se lance automatiquement.
5. Vérifiez 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 ensuite le résultat obtenu avec l'empreinte (hash) indiquée sur MyStormshield. Pour la visualiser, cliquez sur **Afficher** dans la colonne **SHA256** du fichier concerné.

NOTE
Vous pouvez également télécharger cette version depuis le site Stormshield VPN SSL ou depuis le portail captif du firewall SNS hébergeant le service VPN SSL. Vous devrez vous connecter à MyStormshield pour vérifier l'intégrité des binaires.

Versions précédentes de SN SSL VPN Client v4

Retrouvez dans cette section les nouvelles fonctionnalités, les vulnérabilités résolues et correctifs des versions précédentes de SN SSL VPN Client v4.

4.0.8 EA		Version non publiée	
4.0.7 EA			Correctifs
4.0.6 EA			Correctifs
4.0.5 EA	Nouvelles fonctionnalités		Correctifs
4.0.4		Version non publiée	
4.0.3		Version non publiée	
4.0.2		Version non publiée	
4.0.1		Version non publiée	
4.0.0		Version non publiée	

Version 4.0.8 EA non publiée

La version 4.0.8 EA n'est pas disponible publiquement.

Correctifs de la version 4.0.7 EA

Connexion

La présence de caractères spéciaux, tels que &, dans le mot de passe empêchait la connexion en mode automatique à SN SSL VPN Client v4. Ce problème a été corrigé.

Correctifs de la version 4.0.6 EA

Compatibilité

La compatibilité de SN SSL VPN Client v4 avec les firewalls SNS en version 4.3 a été rétablie.
Cette régression était apparue en version 4.0.5 EA.

Nouvelles fonctionnalités et améliorations de la version 4.0.5 EA

Contrôle de conformité (ZTNA)

SN SSL VPN Client est compatible avec la fonctionnalité de vérification de la conformité des postes client désormais configurable sur le firewall SNS à partir de la version 4.8.

Plus d'informations sur le contrôle de conformité du firewall SNS.

Installation

Installation multi-comptes

Vous pouvez désormais installer SN SSL VPN Client sur plusieurs profils utilisateur d'un même poste de travail Windows. Chaque utilisateur bénéficie de son propre carnet d'adresses et de ses propres journaux (logs).

Toutefois, SN SSL VPN Client ne doit pas être lancé sur plusieurs profils à la fois. Nous recommandons à chaque utilisateur partageant un poste de travail Windows avec d'autres utilisateurs de veiller à bien fermer sa session. Sinon, il sera nécessaire de redémarrer le poste pour que les autres utilisateurs puissent établir un tunnel.

À noter que :

- L'installation requiert toujours d'être administrateur local sur la machine ou de fournir le nom et le mot de passe d'un compte administrateur,
- Le répertoire d'installation de SN SSL VPN Client en version 4 a été modifié. À la première connexion, certains utilisateurs devront indiquer de nouveau le certificat du firewall SNS comme étant de confiance.

Configuration de paramètres

Désormais, lors de l'installation, vous pouvez définir les paramètres suivants :

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

Package d'installation

Un seul programme d'installation de SN SSL VPN Client regroupe désormais toutes les langues et toutes les versions de Windows supportées. L'administrateur peut toujours télécharger un package .msi pour une installation via un outil de déploiement.

Mise à jour des certificats

Les algorithmes SHA-1 et MD5 permettant de signer les certificats étant obsolètes, ils ne seront plus supportés dans une prochaine version de SN SSL VPN Client. Il est impératif que les administrateurs mettent à jour leurs certificats dès maintenant. Veuillez trouver la procédure dans l'article How can I regenerate the sslvpn-full-default-authority? de la Base de connaissances Stormshield (anglais uniquement).

Pour renforcer la sécurité, il est possible de désactiver le support de ces algorithmes dès à présent en supprimant la valeur "insecure_compat" ou en la mettant à 0 dans la clé de registre :

HKLM\SYSTEM\CurrentControlSet\Services\StormshieldSSLVPNService\Parameters

Correctifs de la version 4.0.5 EA

Certificats - Sécurité

Auparavant, si :

- SN SSL VPN Client utilisait un certificat d'autorité racine présent dans le magasin Windows,
- Le fichier de configuration de SN SSL VPN Client utilisait le nom de certificat indiqué dans le certificat du portail captif,

alors un message d'erreur de certificat s'affichait en boucle. Ce problème a été résolu.

Délai d'expiration des requêtes HTTPS

Auparavant, si :

- Le tunnel était établi pour la première fois ou que la configuration avait changé,
- L'utilisateur utilisait une authentification RADIUS,

Alors le délai d'expiration des requêtes HTTPS était trop court pour permettre à l'utilisateur de s'authentifier en utilisant une application tierce (authentification multifacteur). Désormais, il existe trois paramètres pour configurer le délai d'expiration dans la clé de registre **HKLM\SYSTEM\CurrentControlSet\Services\StormshieldSSLVPNService\Parameters** :

- https_connect_timeout : détermine le délai accordé pour la connexion au SNS. La valeur par défaut est 30 secondes.
- https_recvsend_timeout : détermine le délai accordé pour l'émission et la réception d'une réponse, notamment pour l'authentification RADIUS. La valeur par défaut est 30 secondes. Ce paramètre doit être ajouté à la clé pour modifier sa valeur par défaut.
- https_resolve_timeout : détermine le délai accordé pour la résolution d'une adresse FQDN. La valeur par défaut est 0 seconde. Ce paramètre doit être ajouté à la clé pour modifier sa valeur par défaut.

Si un paramètre a une valeur de 0 seconde, alors il n'y a pas de délai d'expiration.

Carnet d'adresses

Sauvegarde après import

Le bouton **Sauvegarder** était grisé après l'import d'un carnet d'adresses. Il est à présent disponible. Cette régression était apparue en version 3.2.3 de SN SSL VPN Client.

Traduction manquante

Le contenu de la colonne OTP est désormais traduit.

Mauvais ordonnancement des tabulations

Dans la fenêtre permettant d'ajouter une nouvelle entrée au carnet d'adresses, l'ordre de tabulation des champs a été corrigé.

Authentification par OTP

Référence support 84809

Dans le cas où :

- SN SSL VPN Client est configuré en mode automatique avec une authentification multifacteur,
- Une modification concernant le VPN SSL est réalisée côté SNS et le service VPN SSL est redémarré.

Auparavant, les tunnels VPN étaient fermés et SN SSL VPN Client essayait de reconnecter ces tunnels sans tenir compte du changement de configuration. Ce problème a été corrigé et SN SSL VPN Client demande désormais deux codes OTP dans cette situation.

Pour plus d'informations sur le mode automatique, reportez-vous à la section **Spécificités du client VPN SSL Stormshield** de la note technique *Configurer et utiliser le VPN SSL des firewalls SNS*.

Mise à jour

Désormais, suite à une mise à jour, seule la dernière version de SN SSL VPN Client est conservée. Auparavant, l'ancienne version était aussi conservée.

Logs

Auparavant, certains caractères dans les messages d'erreur des logs ne s'affichaient pas correctement. Ce problème a été corrigé.

Version 4.0.4 non publiée

La version 4.0.4 n'est pas disponible publiquement.

Version 4.0.3 non publiée

La version 4.0.3 n'est pas disponible publiquement.

Version 4.0.2 non publiée

La version 4.0.2 n'est pas disponible publiquement.

Version 4.0.1 non publiée

La version 4.0.1 n'est pas disponible publiquement.

Version 4.0.0 non publiée

La version 4.0.0 n'est pas disponible publiquement.

Contact

Pour contacter notre Technical Assistance Center (TAC) Stormshield :

- https://mystormshield.eu/

La soumission d'une requête auprès du support technique doit se faire par le biais du gestionnaire d'incidents présent dans l'espace client MyStormshield, menu **Support technique** > **Gestion des tickets**.

- +33 (0) 9 69 329 129

Afin de pouvoir assurer un service de qualité, il est recommandé de n'utiliser ce mode de communication que pour le suivi d'incidents auparavant créés par le biais de l'espace client MyStormshield.

Les images de ce document ne sont pas contractuelles, l'aspect des produits présentés peut éventuellement varier.

Copyright © Stormshield 2024. Tous droits réservés. Tous les autres produits et sociétés cités dans ce document sont des marques ou des marques déposées de leur détenteur respectif.