STORMSHIELD

STORMSHIELD NETWORK SECURITY

STORMSHIELD NETWORK VPN CLIENT EXCLUSIVE

NOTES DE VERSION

Version 7

Dernière mise à jour du document : 12 septembre 2022

Référence : sns-fr-vpn_client-exclusive-notes_de_version-v7.00.115

Table des matières

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

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

Historique des modifications

Date	Description
12 septembre 2022	Ajout de la compatibilité avec le mode "Diffusion Restreinte (DR)" des versions SNS 4.2 et supérieures
23 mai 2022	Nouveau document

Introduction à SN VPN Client Exclusive v7.0

SN VPN Client Exclusive est une solution de type client VPN. Installée sur un ordinateur Windows, elle permet de monter un tunnel VPN avec un pare-feu Stormshield Network Security afin de sécuriser une communication entre un utilisateur distant et un réseau protégé par un pare-feu SNS.

La solution SN VPN Client Exclusive peut être installée sur les environnements suivants :

- Windows 10 64 bits,
- Windows 11 64 bits.

Pour plus d'information concernant SN VPN Client Exclusive 7.0, consultez le *Guide de l'administrateur* sur le site de Documentation Technique Stormshield.

Fonctionnalités principales

La version SN VPN Client Exclusive 7.0 fournit les fonctionnalités principales suivantes.

Haut niveau de sécurité

Le client SN VPN Client Exclusive a été développé en suivant les recommandations du NIST et de l'ANSSI. Il prend en compte les fonctions d'authentification disponibles sur le système d'information, et inclus à ce titre des mécanismes d'intégration avec les PKI existantes. L'ensemble des protocoles et algorithmes mis en œuvre dans le logiciel en font un client universel pour se connecter à toutes les passerelles VPN du marché, qu'elles soient logicielles ou matérielles.

Mode GINA

Le mode GINA permet d'ouvrir des connexions VPN avant l'ouverture d'une session Windows. Cette fonction permet par exemple d'établir une connexion sécurisée vers un serveur de gestion des droits d'accès de façon à obtenir les droits d'accès au poste utilisateur avant l'ouverture de la session utilisateur.

TND (Trusted Network Detection)

Cette fonctionnalité consiste à détecter que le poste est connecté au réseau de l'entreprise (réseau de confiance) ou non. Lorsque le Client VPN détecte que le poste n'est pas sur le réseau de l'entreprise, le tunnel prédéfini est ouvert automatiquement.

TrustedConnect utilise les deux méthodes suivantes pour détecter si le poste est sur un réseau de confiance ou non :

- Vérification que l'un des suffixes DNS des interfaces réseau présentes sur le poste fait partie de la liste des suffixes DNS de confiance (liste configurée dans le logiciel, cf. ci-dessous),
- Accès automatique en HTTPS à un serveur Web de confiance, et vérification de la validité de son certificat.

Mode Always-On

La fonctionnalité Always-On assure le maintien de la sécurité de la connexion à chaque changement d'interface réseau.

Les type d'interfaces réseaux pris en charge sont les suivants :

- Adaptateur virtuel (ex : vmware),
- Wi-Fi,
- Ethernet,
- Modem USB (type smartphone),
- Modem Bluetooth (type smartphone).

Les événements réseau déclenchant la reconnexion automatique du tunnel (et la détection du réseau de confiance, le cas échéant) sont les suivants :

- Connexion à un réseau (adresses APIPA ignorées),
- Déconnexion d'un réseau,
- Un adaptateur change d'adresse IP ou passage DHCP à statique et vice versa,
- ipconfig /release,
- ipconfig /renew,
- Passage en mode avion.

Microsoft Windows Installer (MSI)

En s'appuyant sur les capacités offertes par l'installeur Windows (MSI), les administrateurs peuvent déployer et administrer le Client SN VPN Client Exclusive avec des outils de gestion de parc et des groupes d'utilisateurs (GPO). Outre l'installation silencieuse, les scripts, les multiples options de personnalisation et de pré-configuration comme la personnalisation de l'interface utilisateur, le paramétrage des fonctions PKI sont gérables de manière totalement centralisée.

Certificat sur carte à puce ou sur token

Le client SN VPN Client Exclusive implémente un mécanisme de détection automatique de l'insertion d'une carte à puce. Ainsi, les tunnels associés au certificat contenu sur la carte à puce sont montés automatiquement à l'insertion de cette carte à puce. Réciproquement, l'extraction de la carte à puce ferme automatiquement tous les tunnels associés.

Logs administrateur, console et traces

Le client SN VPN Client Exclusive propose trois types de logs :

- Les logs "administrateur" sont spécifiquement dédiés au rapport d'activité et d'utilisation du logiciel. Les logs collectés peuvent être au choix et/ou simultanément :
  - Stockés dans un fichier local,
  - Journalisés dans le journal d'évènements Windows,
  - Envoyés au format syslog à un serveur Syslog.
- La "Console" détaille les informations et les étapes des ouvertures et fermeture des tunnels. Elle est principalement constituée des messages IKE et apporte une information de haut niveau sur l'établissement du tunnel VPN. Elle est destinée à l'administrateur, pour l'aider à identifier d'éventuels incidents de connexions VPN.
- Le mode "traçant" fait produire par chaque composant du logiciel le log de son fonctionnement interne. Ce mode est destiné au support éditeur pour le diagnostic d'incident logiciels.

Compatibilité

Stormshield Network Firewall

3.7, 3.11 et 4.x

Systèmes d'exploitation

Windows 10 64 bits
Windows 11 64 bits

NOTE
SN VPN Client Exclusive n'est pas compatible avec les ordinateurs, téléphones et tablettes équipés d'un processeur ARM.

Mode "Diffusion Restreinte (DR)" des firewalls SNS

SN VPN Client Exclusive est compatible avec le mode "Diffusion Restreinte (DR)" des versions SNS 4.2 et supérieures.

Limitations et précisions sur les cas d'utilisation

- Mode USB : l'option **Avec cet ordinateur uniquement** n'est pas disponible.
- Les fichiers de configuration CISCO (**.pcf*) ne peuvent pas être importés dans le **Panneau de Configuration**.
- Le mode *Auto* OpenVPN ne s'adapte pas correctement aux paramètres des passerelles.
- Un **Local ID** de type *ID_DER_ASN1_DN* ne peut pas être utilisé avec des clés partagées.
- Authentification : les clés partagées ne peuvent pas contenir des caractères spéciaux.
- Si la fenêtre **À propos...** est ouverte juste après une installation en ligne de commande, la mention *Version d'évaluation* apparaît toujours même si l'activation s'est correctement déroulée.
- La barre de défilement peut parfois disparaître de l'onglet **Automatisation**.
- En configurant le mode **EAP** (*Extensible Authentication Protocol*), les Autorités de Certification (CA) renseignées précédemment sont effacées.
- Avec certaines résolutions d'écran, la barre d'état du **Panneau de Configuration** peut ne pas s'afficher la première fois que le client est lancé.
- Le changement de langue dans le **Panneau de Configuration** ne s'applique pas au **Mode GINA**.
- Désinstaller le client en double-cliquant sur le paquet MSI n'est pas supporté.
- En configuration VPN SSL, le choix de la suite de chiffrement ne doit pas être configuré en "auto" mais sélectionné spécifiquement parmi la liste des suites de chiffrement proposées.

Ressources documentaires

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

Guides

- Guide de l'administrateur SN VPN Client Exclusive

Notes techniques

- VPN IPsec - Mode Diffusion Restreinte

Télécharger cette version

Se rendre sur votre espace personnel MyStormshield

Vous devez vous rendre sur votre espace personnel MyStormshield afin de télécharger la version 7.00.115 de SN VPN Client Exclusive :

1. Connectez-vous à votre espace MyStormshield avec vos identifiants personnels.
2. Dans le panneau de gauche, sélectionnez la rubrique **Téléchargements**.
3. Dans le panneau de droite, sélectionnez le produit qui vous intéresse puis la version souhaitée.

Vérifier l'intégrité des binaires

Afin de vérifier l'intégrité des binaires SN VPN Client Exclusive :

1. Entrez l'une des commandes suivantes en remplaçant `filename` par le nom du fichier à vérifier :
   - Système d'exploitation Linux : `sha256sum filename`
   - Système d'exploitation Windows : `CertUtil -hashfile filename SHA256`
2. Comparez le résultat avec les empreintes (hash) indiquées sur l'espace client MyStormshield, rubrique Téléchargements.

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** > **Rapporter un incident / Suivre un incident**.

- +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.

STORMSHIELD