STORMSHIELD

STORMSHIELD NETWORK SECURITY

STORMSHIELD CLIENT VPN IPSEC

NOTES DE VERSION

Version 1

Dernière mise à jour du document : 11 mai 2026

Référence : sns-fr-client_vpn_ipsec-notes_de_version-v1.0

Table des matières

Dans la documentation, "Stormshield Client VPN IPsec" est nommé "client VPN IPsec Stormshield", et "Stormshield Network Security" est désigné sous la forme abrégée "SNS".

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

Historique des modifications

Date	Description
11 mai 2026	Nouveau document

Fonctionnalités principales de Stormshield Client VPN IPsec 1.0

Le client VPN IPsec Stormshield vous permet de vous connecter de manière sécurisée à votre réseau d'entreprise. Selon la licence dont vous disposez, Essential ou Premium, vous bénéficiez de fonctionnalités avancées supplémentaires pour améliorer l'expérience de vos administrateurs et de vos utilisateurs.

Compatibilité et interopérabilité du client VPN IPsec Stormshield

- Systèmes d'exploitation : Windows 11, version 22H2 et supérieure. Il est recommandé d'utiliser Windows 11 Professionnel ou Windows 11 Entreprise.
- Firewalls SNS : versions 4.8 LTSB et versions 5, en IPsec standard ou en IPsec DR. L'IPsec DR (Diffusion Restreinte) impose au firewall SNS de respecter les recommandations de l'ANSSI.

Fonctionnalités incluses avec la licence Essential

Profils IPsec / IKEv2

Les algorithmes et fonctions cryptographiques suivants sont pris en charge :

Chiffrement	Échange de clés (Diffie-Hellman)
• AES CBC (128, 192 ou 256 bits) • AES CTR (128, 192 ou 256 bits) • AES GCM-16 (128, 192 ou 256 bits)	• Groupe 14 (MODP 2048 bits) • Groupe 15 (MODP 3072 bits) • Groupe 16 (MODP 4096 bits) • Groupe 17 (MODP 6144 bits) • Groupe 18 (MODP 8192 bits) • Groupe 19 (ECP 256 bits) • Groupe 20 (ECP 384 bits) • Groupe 21 (ECP 521 bits) • Groupe 28 (Brainpool ECP 256 bits) • Groupe 29 (Brainpool ECP 384 bits) • Groupe 30 (Brainpool ECP 512 bits)
Intégrité	
• SHA2 256 bits • SHA2 384 bits • SHA2 512 bits	
PRF (Pseudo-Random Function)	
• SHA 256 bits • SHA 384 bits • SHA 512 bits	

Fragmentation

La fragmentation des paquets IKEv2 est activée par défaut avec une taille maximale de 1280 octets. Il est possible de modifier cette taille ou de désactiver la fragmentation dans la configuration d'un VPN (paramètre **Fragmentation**).

NAT-T (*NAT-Traversal*)

Le NAT-T est pris en charge avec un port configurable pour IKE et ESP encapsulé (par défaut UDP/4500). Le NAT-T permet le passage du protocole IPsec au travers d'un réseau réalisant de la translation d'adresses dynamique.

Authentification

Les authentifications suivantes sont prises en charge :

- Authentification utilisateur par certificat X.509 v3, stocké dans le magasin de certificats Windows,
- Authentification utilisateur par clé pré-partagée selon les profils IPsec / IKEv2 compatibles.

Mécanisme de vérification et de révocation des certificats (OCSP)

Le mécanisme de vérification et de révocation des certificats, à l'aide du protocole OCSP, peut être activé dans la configuration d'un VPN (paramètre **Vérification de la révocation du serveur**).

Interface graphique

Le client VPN IPsec Stormshield dispose d'une interface graphique qui permet de configurer localement ses paramètres.

Configuration VPN

- Avec la licence Essential, vous pouvez ajouter une seule configuration VPN.
- La configuration VPN peut être exportée ou importée dans le client VPN IPsec Stormshield. Le format pris en charge est le JSON. Notez que les secrets de la configuration VPN (PSK et certificats) ne sont pas exportés.
- Un mode automatique (également appelé "*Configuration Payloads*" dans IKEv2, RFC 7296) permet de récupérer la configuration réseau (adresse IP, masque, serveurs DNS) auprès du serveur distant. Cette configuration réseau peut également être définie manuellement.

Mode de connexion

Le tunnel VPN doit être établi manuellement par l'utilisateur après l'ouverture de sa session Windows. L'établissement automatique sera disponible dans une prochaine version du client VPN IPsec Stormshield. Une licence Premium sera requise.

Installation

Le client VPN IPsec Stormshield peut être installé et mis à jour via un package MSI :

- Soit localement sur un poste de travail en exécutant le package MSI,
- Soit de manière administrée, avec une stratégie de groupe (GPO, EMM ou MDM) ou en ligne de commande (CLI).

Pour plus d'informations, reportez-vous au Guide d'installation et d'utilisation Stormshield Client VPN IPsec v1.

Journaux

Les journaux du client VPN IPsec Stormshield sont disponibles dans l'Observateur d'événements Windows.

Gestion des licences (Beta)

La gestion des licences du client VPN IPsec Stormshield, permettant l'activation et le suivi du nombre de postes activés, est prise en charge actuellement en Beta. En l'absence d'une clé de licence valide, un bandeau d'avertissement non bloquant est affiché.

Mécanisme de *split tunneling*

Le mécanisme de *split tunneling* est pris en charge. Il permet de définir les flux qui doivent traverser le tunnel VPN pour atteindre des réseaux distants définis par des adresses IP ou des masques de sous-réseau de destination.

Fonctionnalités incluses avec la licence Premium

Fonctionnalités de la licence Essential

Toutes les fonctionnalités de la licence Essential sont incluses.

Profil IPsec DR (Diffusion Restreinte)

Un profil IPsec DR (Diffusion Restreinte) est proposé lors de l'ajout d'une configuration VPN. Ce profil permet de configurer un VPN, tout en respectant le référentiel IPsec DR de l'ANSSI. Les suites cryptographiques suivantes sont proposées :

Suite	Chiffrement	Intégrité	Échange de clés (Diffie-Hellman)	PRF
1	AES GCM-16 256 bits	Aucune*	Groupe 19 (ECP 256 bits)	SHA 256 bits
2	AES GCM-16 256 bits	Aucune*	Groupe 28 (Brainpool ECP 256 bits)	SHA 256 bits
3	AES CTR 256 bits	SHA2 256 bits	Groupe 19 (ECP 256 bits)	SHA 256 bits
4	AES CTR 256 bits	SHA2 256 bits	Groupe 28 (Brainpool ECP 256 bits)	SHA 256 bits

(*) L'intégrité est nativement assurée par le mode de chiffrement GCM.

Configuration multi-tunnels VPN

Avec la licence Premium, vous pouvez ajouter plusieurs configurations VPN. Notez qu'un seul tunnel VPN ne peut être établi à la fois.

Négociation ESN

La négociation ESN (*Extended Sequence Number*, RFC 4304) peut être activée dans la configuration d'un VPN (paramètre **Exiger l'ESN**). Elle permet l'utilisation de compteurs 64 bits anti-rejeu sur IKEv2 et CHILD_SA. La négociation ESN est conçue pour gérer des débits élevés et de longues sessions.

Childless IKEv2

L'initiation IKEv2 sans CHILD_SA (RFC 6023) peut être activée dans la configuration d'un VPN (paramètre **Mode childless**). Activez ce paramètre pour des cas d'interopérabilité avancés.

Configuration administrée

Un serveur tiers de gestion centralisée peut être utilisé pour configurer en masse un parc de clients VPN IPsec Stormshield. Notez que les paramètres récupérés depuis le serveur ne peuvent pas être modifiés par l'utilisateur dans son client VPN IPsec Stormshield.

Compatibilité

Pour plus d'informations, reportez-vous à la section **VPN IPsec Client** du document *Cycle de vie produits Network Security & Tools*.

Problèmes connus

La liste actualisée des problèmes connus relatifs à cette version du client VPN IPsec Stormshield 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.

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).

Installer cette version

Pour installer ou mettre à jour le client VPN IPsec Stormshield, reportez-vous au **Guide d'installation et d'utilisation Stormshield Client VPN IPsec v1**.

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.

STORMSHIELD