BETA – VPN SSL 5.1.0

Présentation de la version BETA

Table des matières

Merci pour votre participation à ce programme BETA de la version VPN SSL 5.1.0.

Vos retours seront précieux pour assurer la sortie d'une version officielle qui répondra aux attentes de nos utilisateurs.

Ce document a pour objectif de vous guider dans ce programme BETA.

1 Usage de la version BETA

Cette version BETA n'est PAS destinée à être utilisée en production.

Les tests réalisés par vos soins sur cette version devraient être faits dans des conditions aussi réalistes que possible, mais ne pas venir en remplacement de votre solution de production !

2 Où trouver les fichiers de la version BETA ?

Vous trouverez les différents fichiers d'installation du client VPN SSL dans la section Téléchargements sur MyStormshield.

3 Quelles informations nous remonter et comment ?

Nous souhaitons connaître le périmètre de vos tests : veuillez nous indiquer les fonctionnalités que vous avez utilisées, avec succès ou non.

Tout comportement anormal ou suspect doit nous être signalé. Nous sommes également à l'écoute de toute suggestion d'amélioration.

Dans tous les cas, nous vous demandons de préciser autant que possible :

- votre contexte d'utilisation (OS utilisé, modèle de firewall concerné, cluster HA…),
- les éléments pouvant nous aider à comprendre votre retour : capture d'écran, courte vidéo, logs…

Pour tout problème de fonctionnement, ouvrez un ticket auprès de notre support technique.

Pour toute autre remontée (piste d'amélioration, retour sur le périmètre des tests, bug graphique…), envoyez un message à beta@stormshield.eu.

4 Principales fonctions du VPN SSL 5.1.0

Cette version du client VPN SSL est une évolution du client VPN SSL Stormshield avec 3 évolutions majeures :

1. Une interface graphique actualisée,
2. Compatibilité avec les 3 principaux OS d'ordinateurs portables (Windows, MAC, Linux)
3. Le support d'un nouveau mode d'authentification via le portail web (qui permet en particulier l'authentification via EntraID). Ce nouveau mode est disponible sur les versions SNSv5

4.1 Caractéristiques clés

Le VPN SSL 5.1.0 est une évolution du client VPN SSL Stormshield version 4.0., qui est basée sur Open VPN tout en ayant enrichi cette base avec des fonctions propres à Stormshield. En particulier, voici les caractéristiques qui distinguent la version 5.1.0 :

- **Compatibilité versions SNS**
    - Firmware en version SNS 4.3 ou supérieure
- **Compatibilité multi plateformes**
    - Windows 10 / 11
      Note: l'installation est volontairement bloquée sur Windows server
    - Linux (x86-64)
        - Ubuntu 22.04 / 24.04
        - Red Hat RHEL 8 et RHEL 9
    - MacOS 14/15 ARM uniquement
- Installation / cycle de vie utilisant les **outils natifs de chaque environnement** (.msi sous Windows, .deb / .rpm pour Linux, et .pkg pour MacOS)
- **CLI** disponible pour démarrer / stopper / superviser l'état d'un tunnel, ainsi que pour importer / exporter une liste de connexions enregistrées
- Fonctionnement en mode **Multi utilisateurs** :
    - Une installation "poste" globale
    - Chaque utilisateur a sa configuration (voir ci-après carnet d'adresses en particulier)

- Seul l'utilisateur actif peut établir un tunnel
  ⚠ La notion d'utilisateur actif n'existe que sous Windows
- Le tunnel est automatiquement stoppé s'il y a un changement d'utilisateur actif (Windows seulement)
- Le tunnel est automatiquement stoppé à l'arrêt de l'agent (IHM)

- **Configuration de tunnels VPN SSL**
  - Mode "OVPN" (mode "manuel" en v4), par import d'un fichier .ovpn
  - Mode "Stormshield" (mode "automatique" en v4)
    - Support du Hostcheck / ZTNA (à partir de SNSv4.8)
      - Périmètre ZTNA Windows équivalent à celui de l'agent v4.0
      - Périmètre ZTNA minimal sous Linux / Mac (version de l'agent et OS)
    - Bascule automatique en "legacy" si le SNS ne gère pas le mode Hostcheck
    - Support de TOTP
    - Support du mode Authentification Portail Web de SNSv5
- **Carnet d'adresses**
  - Entrées de type "Stormshield", avec toutes les options possibles de ce mode (Authentification portail, TOTP, mot de passe fourni ou non, etc.....)
  - Entrées de type "OVPN"
  - Possibilité de configurer des favoris
  - Sélection possible d'une entrée à monter automatiquement au démarrage de l'agent (IHM)
- Possibilité de monter un tunnel en connexion directe (sans devoir créer d'entrée dans le carnet d'adresses)

4.2 Points importants du fonctionnement de l'agent

L'agent v5 est pensé pour être utilisé principalement via le menu rapide du systray, avec la dernière connexion utilisée ou une connexion enregistrée et marquée favorite.

4.2.1 Logique de récupération du carnet d'adresses v4:

- Au démarrage de l'agent v5 (frontend), s'il y a un carnet d'adresses v5, on l'utilise
- Sinon, s'il y a un carnet d'adresses v4 (ou v3), alors on importe ses infos dans le carnet d'adresses v5
  ⚠ Du coup, si votre compte dispose d'un carnet d'adresses v3/v4, mais que celui ci est protégé par mot de passe, c'est ce mot de passe là qui est demandé lors du premier démarrage de l'agent v5 !
  L'ancien carnet d'adresses n'est ni modifié, ni effacé lors de ce processus, ni dans la suite de l'utilisation de l'agent v5.

4.2.2 Validation de certificats (mode "Stormshield", anciennement mode "automatique"):

- Quand on accepte un certificat, l'information (et l'empreinte du certificat) est liée à l'entrée du carnet d'adresse (la connexion directe est vue comme une entrée de carnet d'adresses dans ce cas), et est donc spécifique à cette entrée.
- quand un certificat est affiché pour validation (ou pas), sa chaîne de certification complète est affichée

4.2.3 Autres nouveautés

Les événements de production ("tunnel établi", etc.....) sont désormais dans l'interface de l'agent, dans "journaux d'événements", au lieu d'être remontés via les événements système

5 Installation

5.1 Windows

L'agent est supporté sur les systèmes Windows 10 et Windows 11, en version x86_64.

L'installation se fait de façon classique, via le fichier .msi fourni.
Il existe 2 versions du fichier .msi: Fr et En. La différence de langage n'impacte que les écrans d'installation de l'agent.

5.2 Linux

L'agent est supporté sur les distributions Ubuntu (22.04 et 24.04) ainsi que sur les distributions RedHat Entreprise Linux (RHEL, dernière v8 et dernière v9).
Dans tous les cas, l'architecture x86_64 est supportée.

Dans les 2 cas, un paquet au format natif de la distribution est fourni (un .deb pour Ubuntu, un .rpm pour RHEL), et s'installe via les outils habituels de la plateforme.
Note: le paquet a des dépendances, il est donc préférable, sous Ubuntu, de l'installer via une méthode qui gérera automatiquement ces dépendances, comme par exemple:

```
$ sudo apt install ./stormshield-sslvpnagent-5.1.0.deb
```

Sous RHEL, la commande d'installation dnf fournit la gestion des dépendances :

```
$ sudo dnf install ./stormshield-sslvpnagent-5.1.0.rpm
```

Note : les outils apt et dnf nécessitent tous les deux de fournir un chemin de fichier pour le paquet (ici « ./ », en considérant que le paquet est disponible dans le répertoire courant).

Sous RHEL9, la dépendance « openvpn » n'est pas disponible par défaut. Le moyen le plus simple pour la fournir est d'activer le dépôt EPEL (« Extra Packages for Enterprise Linux »), via les commandes suivantes :

```
$ sudo dnf install https://dl.fedoraproject.org/pub/epel/epel-release-latest-9.noarch.rpm
$ sudo dnf update -y
```

Selon l'environnement de bureau et la configuration de ce dernier, il peut être nécessaire d'ajouter des paquets ou d'activer des options pour avoir le support des icones "systray".
Par exemple, sous RHEL dans l'environnement par défaut, on doit installer et activer un tel paquet, comme par exemple gnome-shell-extension-appindicator.

⚠Si votre passerelle OpenVPN fournit une configuration DNS spécifique à utiliser, celle-ci n'est pas prise en compte nativement par OpenVPN dans l'environnement Linux.
Il est alors nécessaire de fournir localement un script qui effectuera les manipulations requises, en fonction de la distribution et de la configuration DNS locale (démon et configuration utilisés, etc.....).

Les scripts de connexion / déconnexion sont à placer dans les emplacements suivants:

```
/opt/stormshield/sslvpnclient/modules/ssl-vpn/etc/sslvpn_connect.sh

/opt/stormshield/sslvpnclient/modules/ssl-vpn/etc/sslvpn_disconnect.sh
```

Par exemple, sous Ubuntu 22.04 / 24.04, qui utilise systemd-resolver dans sa configuration par défaut, un tel script est fourni par le paquet openvpn-systemd-resolved, et est déployé à l'emplacement /etc/openvpn/update-systemd-resolved.
Il peut donc être mis en place via les commandes suivantes :

```
$ sudo apt install openvpn-systemd-resolved

$ sudo ln -s /etc/openvpn/update-systemd-resolved
/opt/stormshield/sslvpnclient/modules/ssl-vpn/etc/sslvpn_connect.sh

$ sudo ln -s /etc/openvpn/update-systemd-resolved
/opt/stormshield/sslvpnclient/modules/ssl-vpn/etc/sslvpn_disconnect.sh
```

5.3 MacOS

L'installation se fait via le fichier .pkg (stormshield-sslvpnclient-arm64-X.X.X.X.pkg).
L'application est installée classiquement sous /Applications/Stormshield/SSL\ VPN\ Client.app/.

La désinstallation peut se faire en plaçant "SSL VPN Client.app" dans la corbeille depuis le menu Applications du Finder.
Aucun désinstalleur n'est actuellement disponible, une désinstallation MacOs traditionnelle conservera donc les fichiers installés ailleurs que dans le .app.

⚠ Si votre passerelle OpenVPN fournit une configuration DNS spécifique à utiliser, celle-ci n'est pas prise en compte nativement par OpenVPN dans l'environnement MacOS (voir par exemple https://forums.openvpn.net/viewtopic.php?t=34612)
Il est alors nécessaire de fournir localement un script qui effectuera les manipulations requises, comme par exemple https://github.com/andrewgdotcom/openvpn-mac-dns.

Les scripts de connexion / déconnexion sont à placer dans les emplacements suivants:

```
/Applications/Stormshield/SSL\ VPN\ Client.app/Contents/MacOS/Modules/ssl-
vpn/etc/sslvpn_connect.sh

/Applications/Stormshield/SSL\ VPN\ Client.app/Contents/MacOS/Modules/ssl-
vpn/etc/sslvpn_disconnect.sh
```

6 Limitations connues et améliorations en cours

Les points suivants sont en cours de correction / d'amélioration pour une version ultérieure :

- Pas de valeurs par défaut à l'installation de l'agent (fonctionnalité agent v4)
  Il est cependant possible de déployer un carnet d'adresses après l'installation de l'agent via la commande cli fournie avec l'agent.
- Support partiel des modes "push" / "inwebo"
- Ne fonctionne pas avec un SNS en version antérieure à 4.3.35
- Sous Windows, le déploiement de l'agent par GPO peut échouer ou effectuer une installation non fonctionnelle dans certains cas.
- Sous Windows, l'installation n'est actuellement pas bloquée sur une version non supportée (version antérieure à Windows10 ou version Windows Server). Le bon fonctionnement de l'agent dans ces conditions n'est cependant pas garanti.
- Sous Linux, l'agent dépend d'un paquet OpenVPN fourni par l'environnement. Il n'existe pas de dépôt officiel pour fournir ce paquet dans la version minimale requise (2.5.0) sur RHEL8.
- Le support du mode Authentification Portail est pour l'instant désactivé sur la version Mac.
- Une connexion enregistrée de type "OVPN" nécessite l'enregistrement de l'identifiant et du mot de passe pour être fonctionnelle.
- Si un tunnel était actif au moment où l'ordinateur part en veille, le comportement de l'agent en sortie de veille n'est pas toujours nominal.
- Si la résolution de l'écran est faible, ou si un ratio d'affichage global est appliqué, l'emplacement et la taille des écrans de l'agent ne sont pas optimaux.
- Dans de rares cas, il peut être nécessaire de stopper et relancer le tunnel manuellement (en particulier en mode TOTP).
- Sur les environnements Linux et Mac, il est nécessaire d'arrêter l'IHM manuellement avant d'effectuer la mise à jour.

7 Vulnérabilités

S'agissant d'une version BETA, cette version n'a pas finalisé les tests de qualité et de sécurité et peut contenir des vulnérabilités.

Elle ne doit donc pas être utilisée en production, et les corrections de ces possibles vulnérabilités ne seront pas déclarées dans des CVE.

Merci

www.stormshield.com