



STORMSHIELD



NOTE TECHNIQUE

STORMSHIELD NETWORK SECURITY

TUNNELS VPN SSL VERSION 2

Version du document : 1.0

Référence : snfrtno_VPN-SSL-Tunnel-v2



Table des matières

Introduction	3
Fonctionnement	4
Prérequis	4
Avantages de Stormshield Network SSL VPN Client	4
Etablissement de tunnel avec Stormshield Network SSL VPN Client	4
Configuration du Firewall Stormshield Network	5
Paramètres du service VPN SSL	5
Paramètres réseaux	5
Paramètres DNS envoyés au client	6
Configuration avancée	7
Scripts à exécuter sur le client	7
Certificats utilisés	7
Droits d'accès VPN	8
Méthode d'authentification	8
Règles de filtrage et NAT	9
Installation et configuration du client VPN SSL	9
Stormshield Network SSL VPN Client sous Windows	9
Remarques avant installation	9
Installation	10
Déploiement via une GPO	10
Utilisation du carnet d'adresses	11
Client tiers compatible OpenVPN sous Windows	12
Client OpenVPN Connect sous Android	13
Client OpenVPN Connect sous IOS	13
Connexion d'un tunnel SSL	14
Stormshield Network SSL VPN Client sous Windows	14
Client OpenVPN Connect sous Android	15
Client OpenVPN Connect sous IOS	16
Consultation des événements	17
Stormshield Network Real Time Monitor	17
Traces du Firewall	17
Traces de Stormshield Network SSL VPN Client	18
Problèmes fréquemment rencontrés	19
Annexes	21
Autre méthode d'authentification	21
Exemple de script de connexion d'un lecteur réseau Windows	22



Introduction



Le VPN SSL permet à des utilisateurs distants d'accéder de manière sécurisée aux ressources internes de l'entreprise : partages réseaux, bases de données, applications, intranet, etc. Toutes les communications entre l'utilisateur distant et le site central sont alors encapsulées et protégées via un tunnel chiffré en SSL.

L'établissement de ce tunnel est basé sur la présentation de certificats serveur et client signés par une autorité de confiance (CA). Cette solution garantit donc authentification, confidentialité, intégrité et non-répudiation.

Les communications entre l'utilisateur et le site central sont gérées par un client VPN SSL installé sur le poste de travail de l'utilisateur. Le fonctionnement de ce client est similaire à celui d'un client VPN IPSec, mais il présente l'avantage d'une configuration simplifiée. D'autre part, il utilise uniquement le port TCP 443, et offre ainsi un accès aisé depuis les réseaux avec filtrage d'accès à Internet (hôtels, wifi public, connexion 3G, etc.). Ce mode de fonctionnement, très ouvert, est accessible sur tout type de terminal (Windows, IOS, Android, etc.), ce qui est devenu une nécessité dans les environnements BYOD (Bring Your Own Device).

Le trafic réseau empruntant un tunnel VPN SSL bénéficie en outre des fonctionnalités avancées des Firewalls Stormshield Network telles que le filtrage de flux niveau 7 et la prévention d'intrusion.



Fonctionnement

Prérequis

Un Firewall Stormshield Network en version 1.0 ou supérieure.

Pour le terminal client :

- Poste de travail Windows 7 ou supérieur, équipé du logiciel Stormshield Network SSL VPN Client (fichier exécutable compatible 32/64 bits),
- Poste de travail équipé d'un client tiers compatible OpenVPN,
- Smartphone ou tablette (Android ou IOS) équipé du client OpenVPN Connect (disponible sur Google Play Store et Apple Store).

Avantages de Stormshield Network SSL VPN Client

Stormshield Network SSL VPN Client récupère à chaque connexion, de manière automatique et sécurisée, sa configuration. Ces éléments sont intégrés au client de manière totalement transparente pour l'utilisateur.

Pour les clients tiers compatibles OpenVPN ainsi qu'OpenVPN Connect pour Android ou IOS, ces éléments de configuration doivent être récupérés et intégrés manuellement lors d'une première connexion au portail d'authentification (https://adresse_IP_du_firewall/auth). Il en est de même lors d'un changement de configuration du service VPN SSL (modifications des certificats, adresse IP du Firewall, etc.).

Stormshield Network SSL VPN Client peut également exécuter des scripts sur le terminal de l'utilisateur à chaque connexion et/ou déconnexion d'un tunnel VPN SSL.

Enfin, SN SSL VPN Client propose un carnet d'adresses permettant de stocker plusieurs profils de connexions. Ce carnet d'adresses peut être chiffré.

Etablissement de tunnel avec Stormshield Network SSL VPN Client

L'utilisateur configure les trois champs de SN SSL VPN Client (adresse IP du Firewall à joindre, nom d'utilisateur, mot de passe), et lance la connexion.

Le client VPN SSL se connecte alors au serveur d'authentification du Firewall. Celui-ci vérifie les informations d'identification et contrôle dans les règles de politique d'authentification (UAC : User Access Control) le droit de l'utilisateur à établir un tunnel VPN SSL.

Stormshield Network SSL VPN Client récupère ensuite de manière transparente sa configuration (archive au format « zip » contenant : profil de connexion, certificat, clé privée, autorité de certification, scripts éventuels à exécuter lors de la connexion et/ou déconnexion) pour négocier l'établissement d'un tunnel.

Cette négociation se déroule ainsi :

1. Le client et le service VPN SSL du Firewall Stormshield Network s'identifient mutuellement par le biais des certificats (Handshake SSL) et négocient les algorithmes de chiffrement,
2. Le service VPN SSL vérifie une seconde fois les accès de l'utilisateur (identifiant, mot de passe et droits d'accès aux tunnels VPN SSL),
3. Le service VPN SSL enregistre l'utilisateur dans la table utilisateurs de l'ASQ,



4. Le tunnel monte : le client se voit attribuer une adresse IP et reçoit les routes nécessaires pour joindre les ressources internes autorisées via le tunnel.

Dès lors, tous les flux entre le client et les ressources autorisées transitent via le tunnel VPN SSL établi.

Configuration du Firewall Stormshield Network

La mise en œuvre de tunnels VPN SSL nécessite de configurer différents modules sur le Firewall:

- Activation et paramétrage du module VPN SSL,
- Configuration des droits d'accès au VPN SSL,
- Choix de la méthode d'authentification. Le cas échéant, paramétrage de l'annuaire LDAP (interne ou externe),
- Définition des règles de filtrage pour autoriser/interdire les flux entre les clients VPN SSL et les ressources internes,
- Eventuellement, mise en place de translation d'adresses.

Paramètres du service VPN SSL

Cliquez sur le menu **Configuration > VPN > VPN SSL** et cochez la case **Activer le VPN SSL**.

Paramètres réseaux

SSL VPN	
<input checked="" type="checkbox"/> Enable SSL VPN	
Network settings	
UTM IP address (or FQDN) used :	192.168.56.250
Port :	https
Available networks or hosts :	Network_internals
Network assigned to clients :	Network_HauteDispo
Maximum number of simultaneous tunnels allowed :	20

1. Indiquez l'adresse IP (ou un FQDN. Exemple : *sslvpnserver.mycompany.com*) par laquelle le Firewall Stormshield Network sera joignable pour établir les tunnels VPN SSL. Ce doit être une adresse IP publique (accessible sur Internet).

NOTE

Si vous renseignez un FQDN, il doit être déclaré dans les serveurs DNS utilisés par le poste client lorsque celui-ci est en dehors du réseau de l'entreprise. Si votre entreprise dispose d'une adresse IP publique dynamique, vous pouvez recourir aux services d'un fournisseur comme DynDNS ou No-IP. Dans ce cas, paramétrez ce FQDN dans le menu **Configuration > Réseau > DNS dynamique**.

2. Indiquez le port d'écoute du service VPN SSL. L'objet HTTPS, correspondant au port par défaut [TCP/443], est présélectionné.



3. Sélectionnez (ou créez) ensuite l'objet correspondant au réseau réservé aux clients VPN SSL.

! IMPORTANT

Choisissez un réseau entièrement dédié aux clients VPN SSL et n'appartenant pas aux réseaux internes existants ou déclarés par une route statique.

En effet, l'interface utilisée pour le VPN SSL étant protégée, le Firewall détecterait alors une tentative d'usurpation d'adresse IP (spoofing) et bloquerait les flux correspondants.

! IMPORTANT

Afin d'éviter des conflits de routage sur les postes clients lors de la connexion au VPN, choisissez plutôt, pour vos clients VPN, des sous-réseaux peu communément utilisés (exemple : 10.60.77.0/24, 172.22.38.0/24, etc.). En effet, de nombreux réseaux d'accès internet filtrés (wifi public, hôtels...) ou réseaux locaux privés utilisent les premières plages d'adresses réservées à ces usages (exemple : 10.0.0.0/24, 192.168.0.0/24).

4. Le nombre maximum de tunnels simultanés est automatiquement calculé et affiché. Par exemple, pour une plage en /24, seules 63 adresses sont disponibles. Cela correspond au minimum des deux valeurs suivantes :
- Le quart du nombre d'adresses IP, moins une, incluses dans le réseau client choisi. Un tunnel SSL utilise en effet 4 adresses IP,
 - Le nombre maximal de tunnels autorisés selon le modèle de Firewall utilisé.
5. Dans le champ **Réseaux ou machines accessibles**, sélectionnez l'objet représentant les réseaux et/ou machines qui seront joignables au travers du tunnel SSL. Cet objet peut être un réseau, une machine ou un groupe incluant des réseaux et/ou des machines.

i NOTE

Il s'agit ici de définir, sur la machine cliente, les routes nécessaires pour joindre l'ensemble des ressources. Cependant, des règles de filtrage seront nécessaires pour autoriser ou interdire plus finement les flux entre les clients distants provenant d'un tunnel SSL et les ressources internes.

i NOTE

Il peut être nécessaire de définir des routes statiques d'accès au réseau attribué aux clients VPN SSL sur les éventuels équipements du réseau de l'entreprise (routeurs, firewalls) situés entre le Firewall et les ressources internes mises à disposition.

Paramètres DNS envoyés au client

Indiquez le suffixe DNS qui sera utilisé par les clients pour réaliser leurs résolutions de noms d'hôtes.

Précisez ensuite les serveurs DNS primaire et secondaire à lui attribuer.

DNS settings sent to client	
Domain name :	<input type="text" value="netasq.com"/>
Primary DNS server :	<input type="text" value="Configured by default"/>
Secondary DNS server :	<input type="text" value="Configured by default"/>



Configuration avancée

Il vous est possible de personnaliser le laps de temps (en secondes) au terme duquel les clés utilisées par les algorithmes de chiffrement seront renégociées (étapes 1 et 2 de l'établissement de tunnel). La valeur par défaut est de 4 heures (14400 secondes).

Advanced configuration

Maximum lifetime (seconds) : 14400

NOTE

Cette opération est transparente pour le client : le tunnel actif n'est pas interrompu lors de la renégociation.

Scripts à exécuter sur le client

Vous pouvez sélectionner des scripts que Stormshield Network SSL VPN Client exécutera lors de la connexion et/ou déconnexion au Firewall. Il est possible, par exemple, de connecter/déconnecter automatiquement un lecteur réseau Windows par cette méthode. Un exemple de script est présenté en annexe.

Scripts to run on the client

Script to run when connecting :

Script to run when disconnecting :

Reset

L'exécution de ces scripts n'est possible que sur des machines clientes fonctionnant sous Windows; le format de ces scripts est obligatoirement du type Microsoft Batch (extension « .bat »).

Toutes les variables d'environnement Windows peuvent être utilisées au sein des scripts de connexion/déconnexion (exemple : %USERDOMAIN%, %SystemRoot%, etc.).

Deux variables d'environnement liées au tunnel VPN SSL sont également utilisables :

- **%NS_USERNAME%** : le nom d'utilisateur servant à l'authentification,
- **%NS_ADDRESS%** : l'adresse IP attribuée au client.

Certificats utilisés

Sélectionnez les certificats que doivent présenter le service VPN SSL du Firewall et le client pour établir un tunnel. Par défaut, une autorité de certification (CA) dédiée au VPN SSL ainsi qu'un certificat serveur et un certificat client créés à l'initialisation du Firewall sont proposés.

Used certificates

Server certificate : sslvpn-full-default-authority:openvpnserver

Client certificate : sslvpn-full-default-authority:openvpnclient

Si vous choisissez de créer votre propre CA, vous devez utiliser deux certificats, et leur clé privée respective, signés par celle-ci. S'il ne s'agit pas d'une autorité racine, les deux certificats doivent être issus de la même sous-autorité.



Droits d'accès VPN

Dans le menu **Configuration > Utilisateurs > Droits d'accès VPN**, l'onglet *Accès par défaut* permet d'autoriser ou d'interdire l'utilisation du VPN SSL à l'ensemble des utilisateurs sans aucune distinction.

Pour autoriser des utilisateurs spécifiques, sélectionnez l'onglet *Accès VPN* et cliquez sur **Ajouter** afin de créer une règle d'accès personnalisée.

Activez la règle (colonne *État*), sélectionnez les utilisateurs ou le groupe d'utilisateurs autorisés (colonne *Utilisateur – groupe d'utilisateurs*) et choisissez l'action **Autoriser** dans la colonne *VPN SSL*.

DEFAULT ACCESS VPN ACCESS PPTP SERVER					
Searching... [X] + Add [X] Delete [Up] Up [Down] Down					
Status	User - user group	SSL VPN Portal	IPSEC	SSL VPN	
1 ● Enabled	VPN SSL Users	Block	Block	Allow	

Méthode d'authentification

Dans le module **Configuration > Utilisateurs > Authentification**, la méthode d'authentification proposée par défaut est « LDAP » (onglet *Méthodes Disponibles*).

Si votre Firewall est déjà connecté à un annuaire Microsoft Active Directory, vous pouvez directement passer à la [mise en œuvre des règles de filtrage et NAT](#).

Pour connecter votre Firewall à un annuaire externe, Microsoft Active Directory (AD) dans notre exemple, cliquez sur le menu **Configuration > Utilisateurs > Configuration de l'annuaire**.

- Sélectionnez **Connexion à un annuaire Microsoft Active Directory**,

Server :	<input type="text"/>
Port :	<input type="text" value="ldap"/>
Root domain (Base DN) :	<input type="text" value="Example: dc=mydomain,dc=com"/>
Login (user DN) :	<input type="text" value="Example: cn=Administrator,cn=users"/>
Password :	<input type="password"/>

- Dans le champ **Serveur**, choisissez ou créez l'objet correspondant à votre serveur AD,
- Dans le champ **Port**, choisissez le port utilisé pour se connecter à l'annuaire AD (valeur par défaut : *ldap*),
- Pour le champ **Domaine racine (Base DN)**, renseignez le nom du domaine AD (Exemple : *dc=mydomain, dc=com* pour le domaine *mydomain.com*),
- Dans le champ **Identifiant (user DN)**, sélectionnez un compte utilisateur du domaine AD (Exemple : *cn=myuser, cn=users* pour l'utilisateur *myuser*),



NOTE

Pour des raisons de sécurité, il est fortement déconseillé de choisir l'utilisateur « Administrateur ». Sélectionnez un compte que vous aurez créé spécifiquement pour le Firewall.

- Dans le champ **Mot de passe**, saisissez le mot de passe de ce compte.

**i NOTE**

Pour vérifier que le paramétrage est correct, vous pouvez cliquer sur le bouton **Tester l'accès à l'annuaire**.

La liste des utilisateurs et groupes est désormais disponible dans le module Utilisateurs (**Configuration > Utilisateurs > Utilisateurs**).

Règles de filtrage et NAT

Il est nécessaire de définir des règles de filtrage autorisant ou interdisant l'accès des clients VPN SSL aux ressources internes joignables par le tunnel.

	Status	Action	Source	Destination	Dest. port	Protocol	Security inspection
1	on	pass	vpn_ssl_tunnel_pool via SSL VPN tunnel	intranet_server	http		IPS
2	on	pass	vpn_ssl_tunnel_pool	database_server	postgresql		IPS
3	on	block	vpn_ssl_tunnel_pool	database_server	ssh		IPS

i NOTE

Les tunnels VPN SSL sont compatibles avec les fonctions avancées de filtrage du Firewall Stormshield Network. Les règles de filtrage peuvent donc faire appel aux profils d'inspection, proxies applicatifs, contrôle antiviral, etc.

De même, si les clients doivent utiliser le VPN SSL pour accéder à internet, il sera nécessaire de mettre en place une règle de translation d'adresses (NAT) du type :

	Status	Source	Destination	Dest. port	Source	Src. port	Destination	Dest. port
1	on	vpn_ssl_tunnel_pool interface: sslvpn	Internet interface: bridge	Any	Pub_FW	ephemeral_fw	Any	Any

Installation et configuration du client VPN SSL

Stormshield Network SSL VPN Client sous Windows

Remarques avant installation

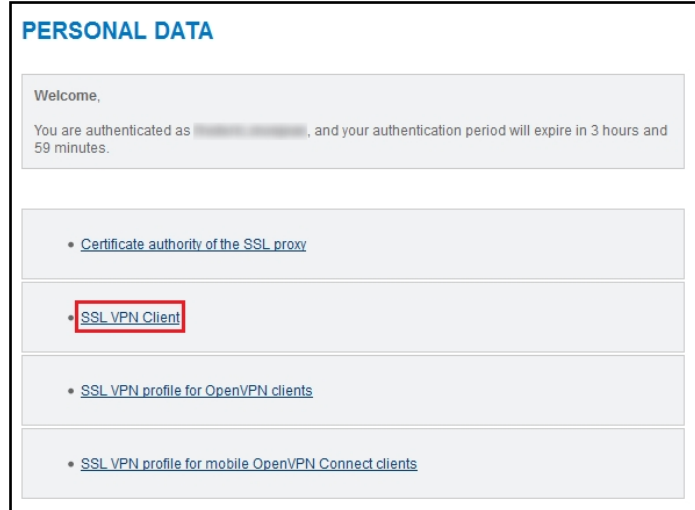
SN VPN SSL Client ne peut être utilisé que sous un seul profil utilisateur Windows. Il doit donc être impérativement installé sous le profil Windows de l'utilisateur final du logiciel.

D'autre part, cette installation requiert une élévation de privilèges. Si l'utilisateur ne possède pas les droits d'administration sur le poste de travail, il devra fournir, au cours de l'installation, le nom et le mot de passe d'un compte ayant les droits d'administration.



Installation

Téléchargez le logiciel Stormshield Network SSL VPN Client depuis le portail d'authentification du Firewall (ou depuis votre espace privé sur le site web).



Faites un double clic sur l'exécutable enregistré sur votre poste de travail (il est nécessaire d'être administrateur local de son poste de travail ou de fournir le mot de passe d'un compte administrateur). Suivez les différentes fenêtres proposées par l'assistant d'installation; seuls le chemin d'installation et un groupe de programme à associer sont à personnaliser si vous le souhaitez.

Le téléchargement et l'intégration des fichiers de configuration sont réalisés automatiquement lors de l'utilisation de Stormshield Network SSL VPN Client. Après authentification et validation du droit à l'utilisation du VPN SSL, le client récupère en effet l'ensemble des données nécessaires pour se configurer.

Déploiement via une GPO

Dans un environnement Microsoft Active Directory, Stormshield Network SSL VPN Client peut être déployé de façon automatique par le biais d'une stratégie de groupe (GPO : Global Policy Object). L'installation peut ainsi être réalisée de manière silencieuse (invisible pour l'utilisateur), avec les droits d'administration nécessaires, et ce à l'occasion du passage d'un client nomade sur le réseau de l'entreprise.

Pour préparer ce type de déploiement, il est nécessaire de convertir l'exécutable d'installation du Stormshield Network SSL VPN Client en fichier Microsoft System Installer (extension « .msi »). Notez que l'exécutable d'origine dispose de l'option « /S » pour une installation silencieuse.

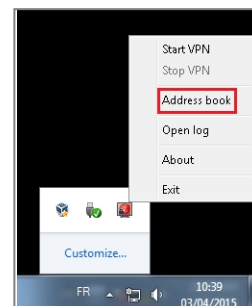
Dans le cadre d'une GPO, vous pouvez également renseigner la clé de registre HKEY_CURRENT_USER\Software\STORMSHIELD\SSL VPN Client\address du poste client avec l'adresse IP ou le FQDN du Firewall. Dès sa première utilisation, Stormshield Network SSL VPN Client lit alors cette clé et renseigne automatiquement le champ **Firewall Address**.



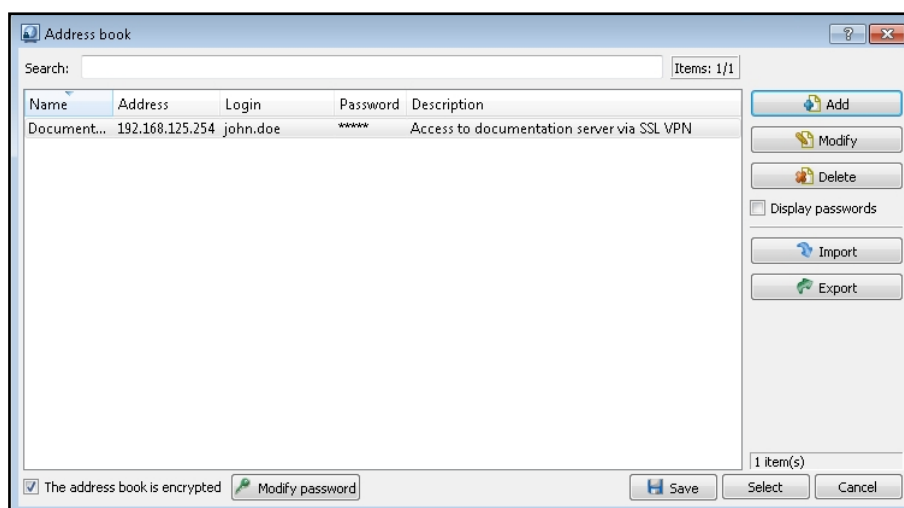
Utilisation du carnet d'adresses

Ouverture

Pour ouvrir le carnet d'adresses, faites un clic droit sur l'icône de SN SSL VPN Client située dans la barre des tâches de la machine Windows et sélectionnez le menu **Carnet d'adresses**.



Vous avez la possibilité d'y mémoriser les informations de connexion sur vos différents firewalls via VPN SSL. Ces informations sont stockées sur le poste client où est installé le client. Elles peuvent être chiffrées si vous cochez l'option **Le carnet d'adresses est chiffré**. Dans ce cas, une clé de chiffrement vous est demandée. Les informations mémorisées pour chaque entrée du carnet d'adresses sont le nom du profil de connexion créé, l'adresse IP du firewall, le login et le mot de passe de connexion ainsi qu'une description optionnelle.



! IMPORTANT

Si vous modifiez l'option **Le carnet d'adresses est chiffré**, il faut enregistrer à nouveau le carnet pour prendre en compte les modifications.

Cochez l'option **Afficher les mots de passe** pour vérifier les mots de passe utilisés pour chacun des firewalls enregistrés dans le carnet d'adresses (les mots de passe sont affichés en clair).

Les boutons **Import** et **Export** permettent également d'importer un carnet d'adresses existant ou d'exporter le carnet courant.



Ajout / modification d'un profil de connexion

Pour ajouter un profil de connexion au carnet, cliquez sur Ajouter, renseignez les différents champs de la fenêtre et validez en cliquant sur **OK**.

Lorsque le port d'écoute du serveur VPN SSL est différent du port par défaut (TCP/443), renseignez le champ **Adresse** à l'aide de l'adresse IP du firewall et du port d'écoute, séparés par deux points (« : »).

Vous pouvez à tout moment modifier un profil en le sélectionnant puis en cliquant sur le bouton **Modifier**:

Client tiers compatible OpenVPN sous Windows

Téléchargez un logiciel client compatible OpenVPN.

Lorsque l'installation du logiciel client est terminée, connectez-vous au portail d'authentification du Firewall (https://adresse_firewall/auth) à l'aide d'un navigateur Web.

Une fois authentifié, téléchargez l'archive de configuration du client en cliquant sur le lien « Profil VPN SSL pour clients OpenVPN » situé dans le menu **Données personnelles**.

Décompressez cette archive dans le répertoire de configuration du client VPN SSL.

**i NOTE**

Cette opération n'est à réaliser qu'à la première connexion ou lorsque des paramètres du service VPN SSL ont été modifiés (changement de certificats ou d'adresse IP du Firewall par exemple).

Client OpenVPN Connect sous Android

Installez sur votre terminal l'application *OpenVPN Connect* disponible sur la boutique en ligne Google Play.

La spécificité d'un client *OpenVPN Connect* réside dans le fait que toutes les informations (configuration, CA, certificat et clé privée) doivent obligatoirement être rassemblées en un seul et même fichier portant l'extension « .ovpn ».

Depuis votre terminal, connectez-vous au portail d'authentification du Firewall (https://adresse_firewall/auth) à l'aide d'un navigateur web.

Une fois authentifié, téléchargez le fichier de configuration (extension « .ovpn ») du client en cliquant sur le lien « Profil VPN SSL pour clients mobiles OpenVPN Connect » situé dans le menu **Données personnelles**:

PERSONAL DATA

Welcome,

You are authenticated as [redacted], and your authentication period will expire in 3 hours and 59 minutes.

- [Certificate authority of the SSL proxy](#)
- [SSL VPN Client](#)
- [SSL VPN profile for OpenVPN clients](#)
- [SSL VPN profile for mobile OpenVPN Connect clients](#)

Votre terminal détecte automatiquement ce fichier et vous propose de l'importer dans le client VPN SSL.

i NOTE

Cette opération n'est à réaliser qu'à la première connexion ou lorsque des paramètres du service VPN SSL ont été modifiés (changement de certificats ou d'adresse IP du Firewall par exemple).

Client OpenVPN Connect sous IOS

Installez sur votre terminal l'application *OpenVPN Connect* disponible sur la boutique en ligne App Store.

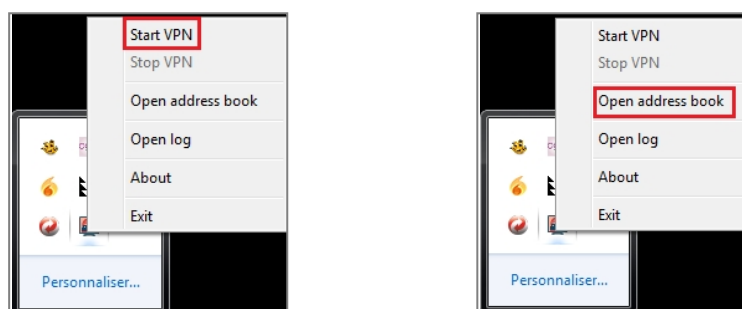
Pour la récupération et l'intégration des données de connexion, la procédure est décrite dans le paragraphe [Client OpenVPN Connect sous Android](#) du chapitre **Installation et configuration du client VPN SSL**.



Connexion d'un tunnel SSL

Stormshield Network SSL VPN Client sous Windows

Pour une connexion directe (sans passer par le carnet d'adresses), faites un clic droit sur l'icône Stormshield Network SSL VPN Client située dans la barre des tâches de la machine Windows, puis sélectionnez **Connecter**. Pour une connexion via le carnet d'adresses, sélectionnez **Ouvrir le carnet d'adresses** :

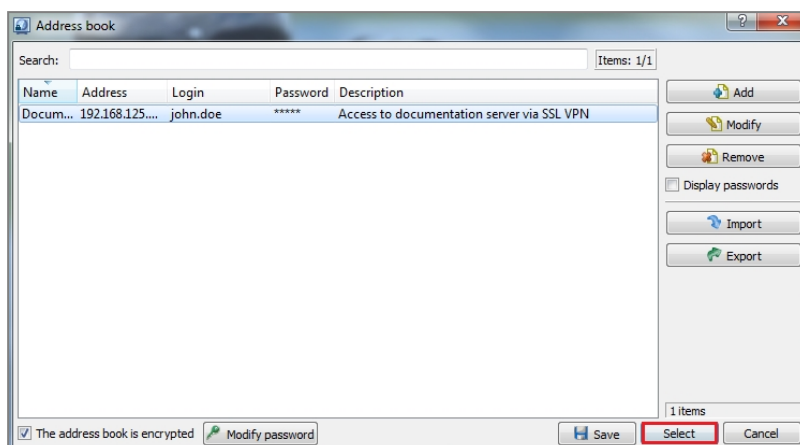


- Dans le cas d'une connexion directe, une fenêtre de dialogue s'ouvre. Indiquez l'adresse publique ou le FQDN du Firewall à joindre pour établir un tunnel SSL, le nom d'utilisateur et le mot de passe associé.

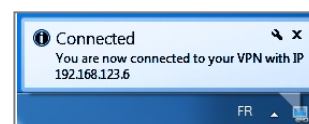
NOTE

Ces paramètres peuvent être sauvegardés en cochant la case **Mémoriser les informations de connexion**.

- Dans le cas d'une connexion via le carnet d'adresses, choisissez le profil de connexion à utiliser puis cliquez sur le bouton **Sélectionner**. La connexion se lance alors automatiquement:

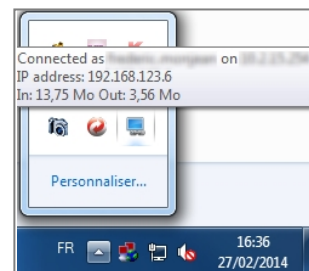


Le client s'authentifie ensuite auprès du Firewall. Il reçoit sa configuration réseau, établit le tunnel SSL et ajoute automatiquement les routes nécessaires au système pour joindre les ressources distantes. Un message de confirmation apparaît dans la barre des tâches.



Le poste distant peut désormais accéder, via le tunnel SSL, à l'ensemble des ressources autorisées sur le site central.

Il est possible d'afficher à tout moment les informations de connexion : nom d'utilisateur, adresse IP du Firewall, adresse IP reçue ainsi que le nombre d'octets échangés au travers du tunnel. Pour cela, il suffit de survoler l'icône du Stormshield Network SSL VPN Client à l'aide de la souris.

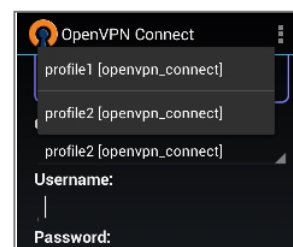


Pour mettre fin à la connexion via ce tunnel VPN SSL, faites un clic-droit sur l'icône Stormshield Network SSL VPN Client située dans la barre des tâches de la machine Windows. Sélectionnez **Stop VPN**.

Client OpenVPN Connect sous Android

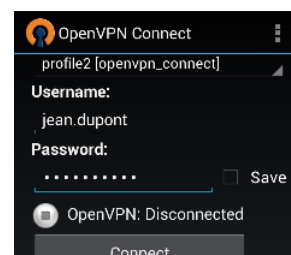
Lancez l'application *OpenVPN Connect* sur votre terminal; un profil par défaut vous est proposé.

Si vous possédez plusieurs profils de connexions, touchez brièvement le profil affiché par défaut pour faire apparaître la liste des profils disponibles et sélectionnez celui de votre choix.



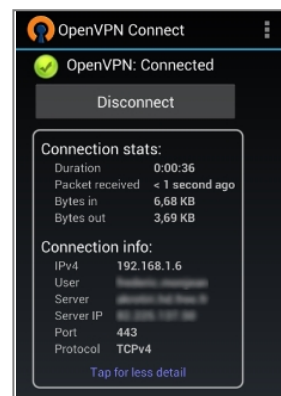


Renseignez le nom d'utilisateur et le mot de passe, puis cliquez sur **Connect**.



Lorsque la connexion est établie, des informations concernant la durée de connexion, le nombre d'octets échangés, l'adresse IP du terminal, le nom et l'adresse IP réelle du Firewall sont affichées.

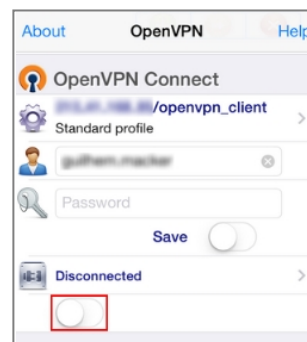
Pour mettre fin au tunnel, cliquez sur **Disconnect**.



Client OpenVPN Connect sous IOS

Lancez l'application OpenVPN Connect sur votre terminal; la liste des profils de connexions disponible s'affiche.

Renseignez le nom d'utilisateur et le mot de passe, puis glissez le curseur de connexion vers la droite.



Lorsque la connexion est établie, des informations concernant la durée de connexion et le nombre d'octets échangés sont affichées.

Pour mettre fin au tunnel, glissez le curseur vers la gauche.

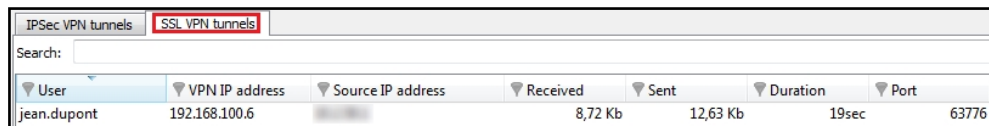




Consultation des événements

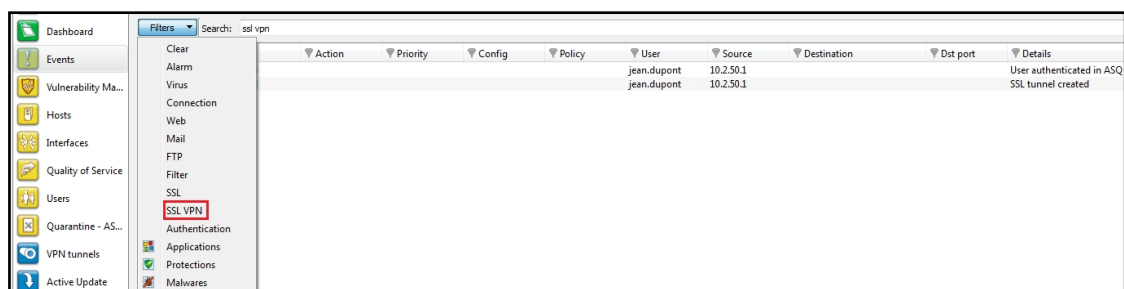
Stormshield Network Real Time Monitor

Pour visualiser les tunnels VPN SSL actifs, cliquez sur l'onglet *VPN SSL tunnels* dans le module **Tunnels VPN** :



User	VPN IP address	Source IP address	Received	Sent	Duration	Port
jean.dupont	192.168.100.6		8,72 Kb	12,63 Kb	19sec	63776

Le module **Evénements** permet de consulter les actions de type authentification et création / suppression de tunnels grâce au filtre sur le mot-clé VPN SSL (menu déroulant **Filtres**):



Action	Priority	Config	Policy	User	Source	Destination	Dst port	Details
				jean.dupont	10.2.50.1			User authenticated in ASQ
				jean.dupont	10.2.50.1			SSL tunnel created

Le module **Services** présente l'état des services du Firewall (valeurs : *activé* ou *désactivé*), dont celui du serveur OpenVPN.

Traces du Firewall

Pour accéder aux journaux de traces du Firewall, cliquez sur l'icône « Rapports d'activités » disponible dans la partie supérieure droite de l'interface d'administration:

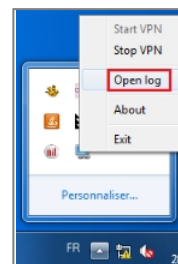


- La vue VPN (**Traces** > **Vues** > **VPN**) présente les informations relatives aux différents types de tunnels VPN (SSL, IPSec).
- Le journal VPN SSL (**Traces** > **Journaux** > **VPN SSL**) regroupe les événements d'authentification et de création/suppression de tunnels VPN SSL.
- Le journal Authentification (**Traces** > **Journaux** > **Authentification**) présente également les événements liés aux authentifications via tunnels VPN SSL par un filtre appliqué sur la méthode ayant comme valeur « OPENVPN ».



Traces de Stormshield Network SSL VPN Client

Pour accéder au fichier de traces de Stormshield Network SSL VPN Client, faites un clic droit sur l'icône de connexion située dans la barre des tâches et choisissez **Journaux (logs)**.





Problèmes fréquemment rencontrés

Symptôme :

Le tunnel SSL ne s'établit pas et le fichier de traces du client affiche les messages suivants:

Fri Feb 07 16:30:42 2014 TEST ROUTES: 0/0 succeeded len=2 ret=0 a=0 u/d=down

Fri Feb 07 16:30:42 2014 Route: Waiting for TUN/TAP interface to come up...

Solution:

Ouvrez le *Centre Réseau et Partage* de Windows et cliquez sur le menu *Modifier les paramètres de la carte*. Faites un clic droit sur l'interface TAP-Windows Adapter et sélectionnez *Diagnostiquer*.

Symptôme :

Le tunnel ne s'établit pas et le client affiche le message « Unable to connect to UTM : Socket operation timed out ».

Solution:

Vérifiez que l'adresse IP spécifiée dans le champ **Firewall address** de Stormshield Network SSL VPN Client est correcte.

Symptôme :

Le tunnel ne s'établit pas et le client affiche le message « Unable to connect to UTM : User not allowed ».

Solutions:

- Vérifiez que l'identifiant et le mot de passe spécifiés dans les champs **Login** et **Password** de Stormshield Network SSL VPN Client sont corrects,
- Sur le Firewall, vérifiez que l'utilisateur est autorisé à établir un tunnel VPN SSL (onglet **Accès VPN** du menu **Utilisateurs** > **Droits d'accès VPN**).

Symptôme :

Le tunnel SSL est établi, mais une ressource autorisée de l'entreprise n'est pas accessible (exemple : impossible d'accéder à un serveur intranet).

Solutions:

- Sur le Firewall :
 - vérifiez que les règles de filtrage autorisent bien l'accès à cette ressource,
 - consultez les traces de filtrage afin de déterminer un éventuel blocage de flux (menu **TRACES** > **Journaux** > **Filtrage**).
- Vérifiez que la ressource demandée est bien physiquement disponible,
- Videz le cache arp de la machine cliente : dans une console, tapez la commande « arp -d * ».



Symptôme :

Le tunnel SSL ne s'établit pas et le client affiche le message : « Error on service connexion: Connection refused ».

Solution:

Vérifiez que le service Stormshield SSL VPN Service est bien démarré. Redémarrez-le au besoin.



Annexes

Autre méthode d'authentification

Si vous souhaitez utiliser, pour les utilisateurs du VPN SSL, une méthode d'authentification différente de celle par défaut (LDAP), il vous faut ajouter cette méthode et configurer la politique d'authentification adéquate.

Pour ce faire, cliquez sur le menu **Configuration > Utilisateurs > Authentification**.

Onglet « Méthodes disponibles »

Cliquez sur **Ajouter une méthode** et sélectionnez une méthode basée sur la présentation d'un couple identifiant et mot de passe : LDAP, Radius ou Kerberos.

NOTE

Les méthodes d'authentification sans mot de passe telles que SPNEGO et Agent SSO ne peuvent être utilisées pour les tunnels VPN SSL.

Onglet « Politique d'authentification »

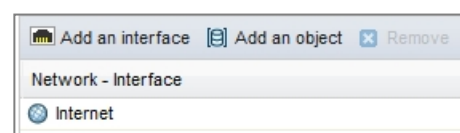
Créez une règle d'authentification pour les utilisateurs du VPN SSL afin de leur affecter la méthode sélectionnée.

Pour cela, cliquez sur **Nouvelle règle** et choisissez **Règle standard**.

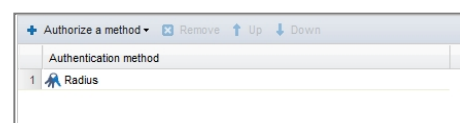
L'assistant de configuration vous propose de sélectionner un utilisateur ou un groupe d'utilisateurs. Choisissez le groupe d'utilisateurs autorisés à se connecter via les tunnels VPN SSL.






Indiquez ensuite la source des demandes d'authentification pour ce groupe d'utilisateurs. Cela peut-être un objet (un réseau, une machine, un groupe) ou une interface.



Sélectionnez la méthode d'authentification choisie, par exemple Radius. Activez cette règle et cliquez sur **Appliquer**.



La règle ainsi créée prendra donc la forme suivante :










Status	Source	Methods (assess by order)
1  Enabled	 VPN SSL Users @  Internet	1  Radius

NOTE

Il est tout à fait possible de créer plusieurs règles d'authentification basées sur des méthodes différentes, pour des groupes d'utilisateurs différents. Dans ce cas, lors d'une demande d'authentification, les règles sont examinées dans l'ordre de leur numérotation.



Exemple :

AVAILABLE METHODS		AUTHENTICATION POLICY		CAPTIVE PORTAL		INTERNAL INTERFACES	
Search by user: <input type="text"/> ✕ ➕ New rule Remove ↑ Up ↓ Down ✂ Cut 📄 Copy							
Status		Source		Methods (assess by order)			
1	● Enabled	 VPN SSL Users - Sales @  Internet	1	 Radius			
2	● Enabled	 VPN SSL Users -IT @  Internet	1	 Default method			
3	● Enabled	 Local Users @  network_internals	1	 LDAP			

Exemple de script de connexion d'un lecteur réseau Windows

Pour automatiser la connexion / déconnexion automatique d'un lecteur réseau Windows à un partage sur un serveur de l'entreprise (exemple : connexion du disque Z: au partage \\myserver\myshare), réalisez deux scripts selon le modèle suivant :

- Un script (Exemple : Zconnect.bat) exécuté lors de la connexion et contenant la ligne :

```
NET USE Z: \\myserver\myshare
```

- Un script (Exemple : Zdisconnect.bat) exécuté lors de la déconnexion et contenant la ligne :

```
NET USE Z: /delete
```

Importez ensuite ces deux scripts dans le paramétrage VPN SSL du Firewall (panneau **Configuration avancée / Scripts à exécuter sur le client** du menu **Configuration > VPN > VPNSSL**) et validez :

Script file

Executed script before client connection : Zconnect.bat

Executed script after client disconnection : Zdisconnect.bat

Reset files

Ces deux scripts seront exécutés dès la prochaine connexion des utilisateurs de tunnels VPN SSL.



STORMSHIELD