

STORMSHIELD

Mise en place d'un VPN SSL

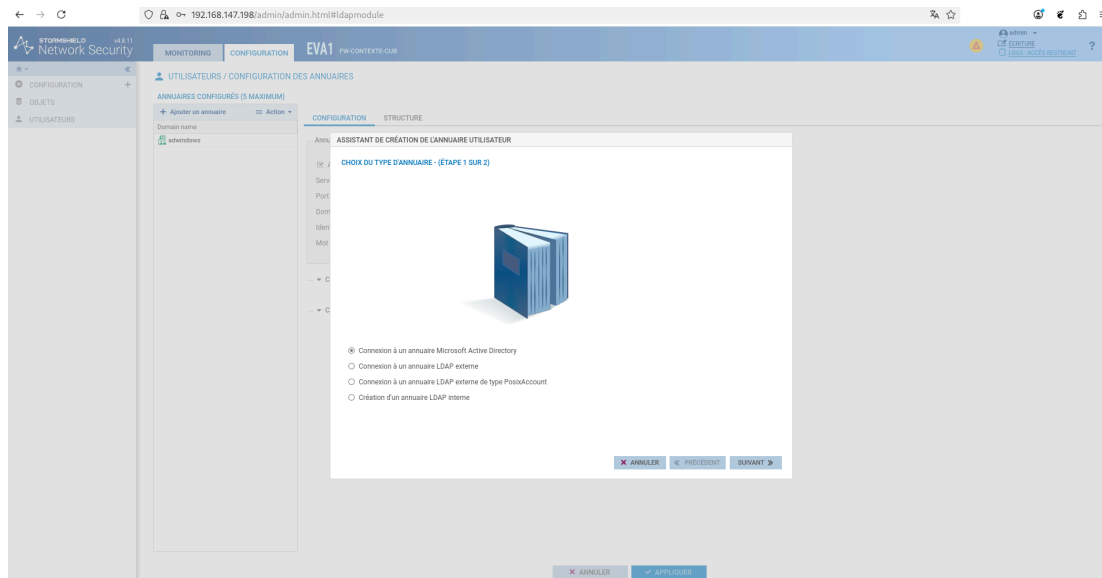
Guide de configuration — Pare-feu Stormshield / Client Windows

SOMMAIRE

- 01 Configuration de l'annuaire utilisateur
 - 02 Paramétrage de l'interface & du VPN SSL
 - 03 Téléchargement du fichier de configuration
 - 04 Vérification des droits d'accès utilisateurs
 - 05 Import & test du VPN sur Windows
 - 06 Connexion avec les identifiants utilisateur
-

01

Configuration de l'annuaire utilisateur



- 01 Accéder à la configuration de l'annuaire d'utilisateurs depuis l'interface Stormshield.
- 02 Noter les informations de connexion : serveur LDAP/AD, port, identifiants de liaison.
- 03 Noter les informations du domaine : nom de domaine, base DN.
- 04 Valider la connexion à l'annuaire avant de passer à la suite.

ASSISTANT DE CRÉATION DE L'ANNUAIRE UTILISATEUR

ACCÈS À L'ANNUAIRE - (ÉTAPE 2 SUR 2)



Nom de domaine	Exemple : stormshield.eu
Serveur	E
Port	ldap E
Domaine racine (Base DN)	Exemple: dc=stormshield,dc=eu
Identifiant (user DN)	Exemple: cn=Administrateur,cn=users
Mot de passe	
Hachage des mots de passe	SHA

- 05 Vérifier que l'interface OUT est bien sélectionnée comme interface de sortie pour le VPN.

02

Paramétrage de l'interface & du VPN SSL

VPN / VPN SSL

ON ☐ Activer le VPN SSL

PARAMÈTRES GÉNÉRAUX

VÉRIFICATION DES POSTES CLIENTS (ZTNA) (DÉSACTIVÉ)

Paramètres réseaux

Adresse IP publique (ou FQDN) de l'UTM utilisée	192.168.147.198
Réseaux ou machines accessibles	Network_internals  
Réseau assigné aux clients (UDP)	network-vpn-udp  
Réseau assigné aux clients (TCP)	network-vpn-tcp  
Maximum de tunnels simultanés autorisés	124

Paramètres DNS envoyés au client

Nom de domaine	
Serveur DNS primaire	Configuré pour le firewall  
Serveur DNS secondaire	Configuré pour le firewall  

▼ Configuration avancée

01 Naviguer dans l'onglet :

VPN > **VPN SSL**

02 Activer le VPN SSL.

03 Renseigner l'adresse du serveur VPN (adresse IP publique ou FQDN).

04 Définir la plage d'adresses IP pour UDP (tunnel principal).

05 Définir la plage d'adresses IP pour TCP (tunnel de secours).

06 Appliquer la configuration.

Les plages IP UDP et TCP doivent être sur des sous-réseaux distincts et ne pas chevaucher les réseaux existants du pare-feu.

03

Téléchargement du fichier de configuration

- 01 Depuis l'interface VPN SSL de Stormshield, localiser le bouton de téléchargement du fichier de configuration.
- 02 Télécharger le fichier .ovpn ou le bundle de configuration généré.
- 03 Conserver ce fichier — il sera importé sur le poste client Windows.

04

Vérification des droits d'accès utilisateurs

UTILISATEURS / UTILISATEURS

Rechercher... [Tous] [Ajouter un utilisateur] [Ajouter un groupe] [Supprimer] [Vérifier l'utilisation]

On

Administrateurs Hyper-V@adwindows

Opérateurs d'assistance de contrôle d'accès@ad...

Utilisateurs de gestion à distance@adwindows

Storage Replica Administrators@adwindows

Ordinateurs du domaine@adwindows

Contrôleurs de domaine@adwindows

Administrateurs du schéma@adwindows

Administrateurs de l'entreprise@adwindows

Éditeurs de certificats@adwindows

Admins du domaine@adwindows

Utilisateurs du domaine@adwindows

Invités du domaine@adwindows

Propriétaires créateurs de la stratégie de groupe...

Serveurs RAS et IAS@adwindows

Opérateurs de serveur@adwindows

Opérateurs de compte@adwindows

Accès compatible pré-Windows 2000@adwindows

Générateurs d'approbations de forêt entrante@ad...

Groupe d'accès d'autorisation Windows@adwind...

Serveurs de licences des services Terminal Serve...

Groupe de réplication dont le mot de passe ROD...

Groupe de réplication dont le mot de passe ROD...

Contrôleurs de domaine en lecture seule@adwin...

Contrôleurs de domaine d'entreprise en lecture s...

Contrôleurs de domaine clonables@adwindows

Protected Users@adwindows

Administrateurs clés@adwindows

Administrateurs clés Enterprise@adwindows

DnsAdmins@adwindows

DnsUpdateProxy@adwindows

vpnuser@adwindows

Groupe vpnuser

Nom du groupe vpnuser

Description du groupe

Filter... [Ajouter] [Supprimer] [Droits d'accès]

On

jean test@adwindows

[X] ANNULER [✓] APPLIQUER

UTILISATEURS / DROITS D'ACCÈS

ACCÈS PAR DÉFAUT ACCÈS DÉTAILLÉ SERVEUR PPTP

Comportement à adopter lorsqu'aucune règle d'accès n'est définie pour l'utilisateur

Accès VPN

Profil VPN SSL Portail [Autoriser]

Politique IPsec [Interdire]

Politique VPN SSL [Autoriser]

Parrainage

Politique de parrainage [Autoriser]

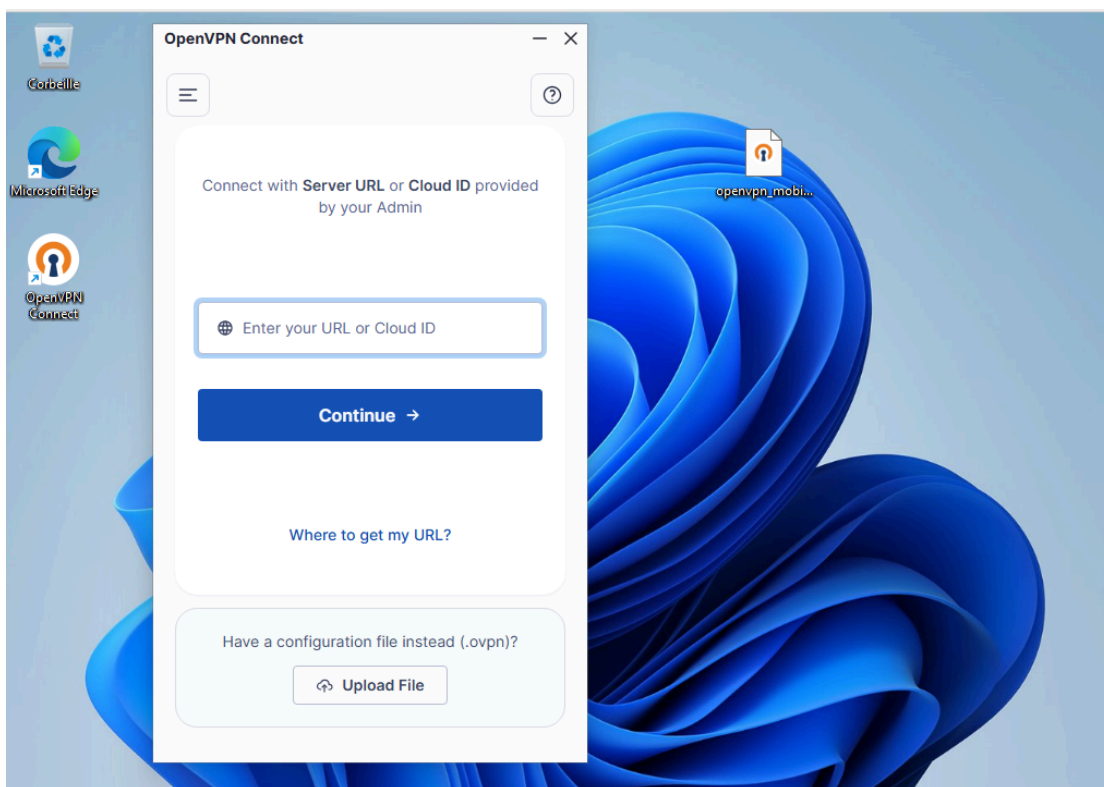
- 01 Vérifier que les utilisateurs concernés disposent bien des droits d'accès au VPN SSL.

- 02 Dans la section des droits d'accès, s'assurer que les comptes ou groupes AD sont autorisés.
- 03 Ajouter ou modifier les permissions si nécessaire avant de procéder au test.

! Un utilisateur sans droit d'accès VPN ne pourra pas s'authentifier, même avec des identifiants valides.

05

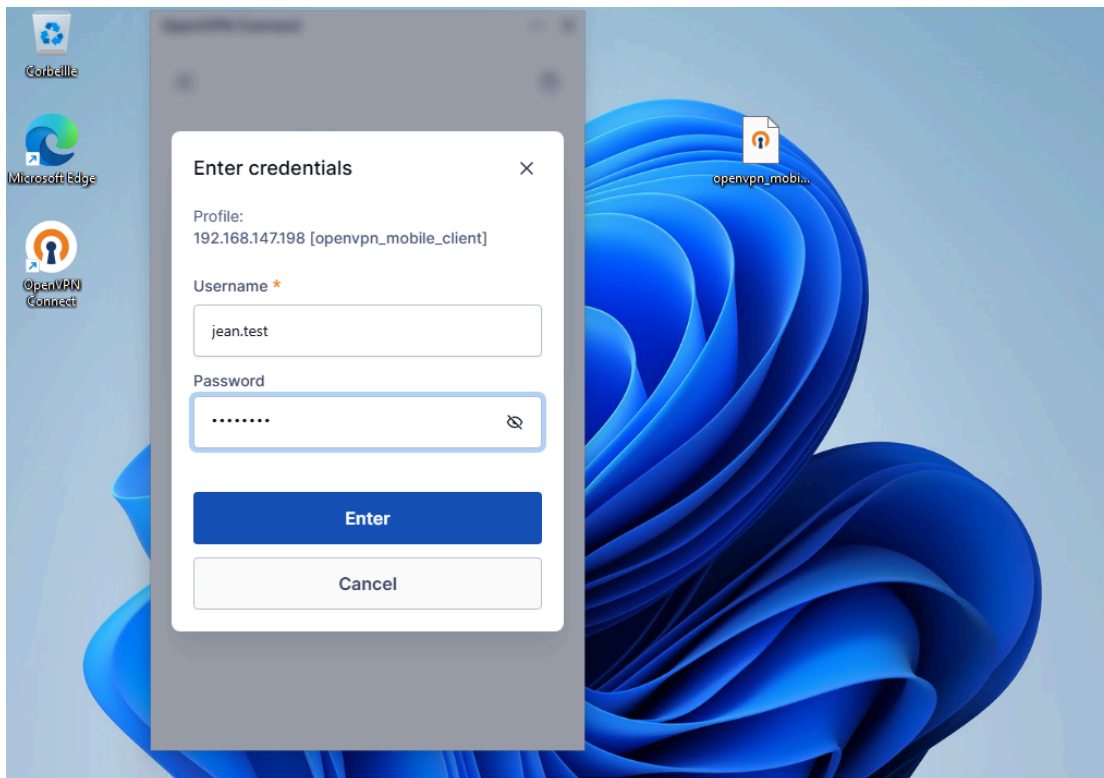
Import & test du VPN sur Windows



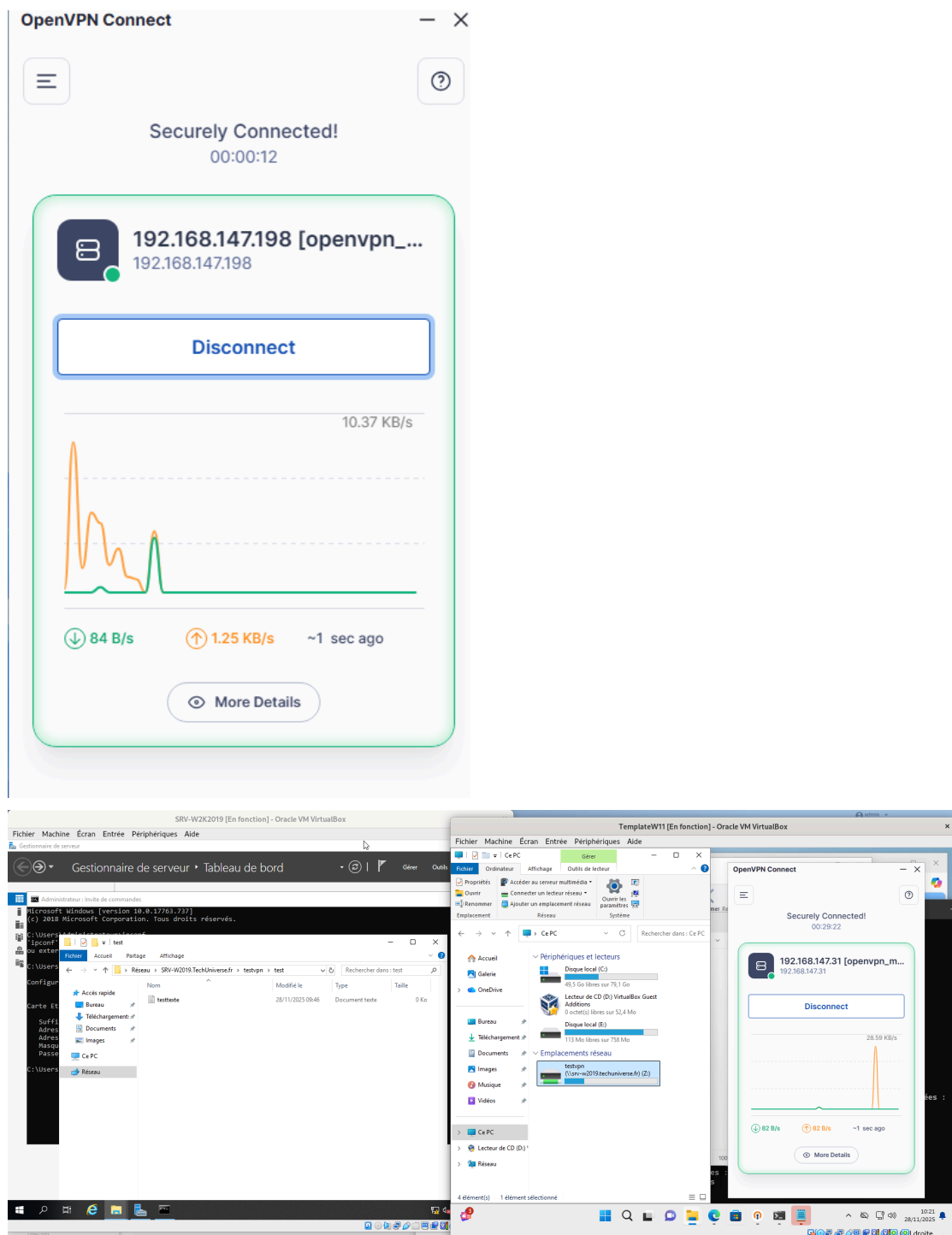
- 01 Sur le poste Windows, ouvrir le logiciel client VPN Stormshield (ou OpenVPN Connect).
- 02 Importer le fichier de configuration récupéré depuis l'interface Stormshield.
- 03 Vérifier que le profil VPN apparaît correctement dans le client.

06

Connexion avec les identifiants utilisateur



- 01 Dans le client VPN, cliquer sur « Connecter ».
- 02 Saisir les identifiants Windows d'un utilisateur ayant les droits d'accès VPN.
- 03 Valider — le tunnel VPN s'établit si la configuration est correcte.
- 04 Vérifier la connectivité réseau depuis le poste client (ping, accès aux ressources internes).



En cas d'échec, vérifier dans l'ordre : droits d'accès de l'utilisateur, validité du fichier de configuration, règles de filtrage autorisant le trafic VPN SSL.