

Introduction

L'authentification AD nous permettra de d'avoir un groupe d'admin qui pourront modifier ou visionner les règles du pare-feu.

D'avoir un groupe d'user qui pourront utiliser le VPN.

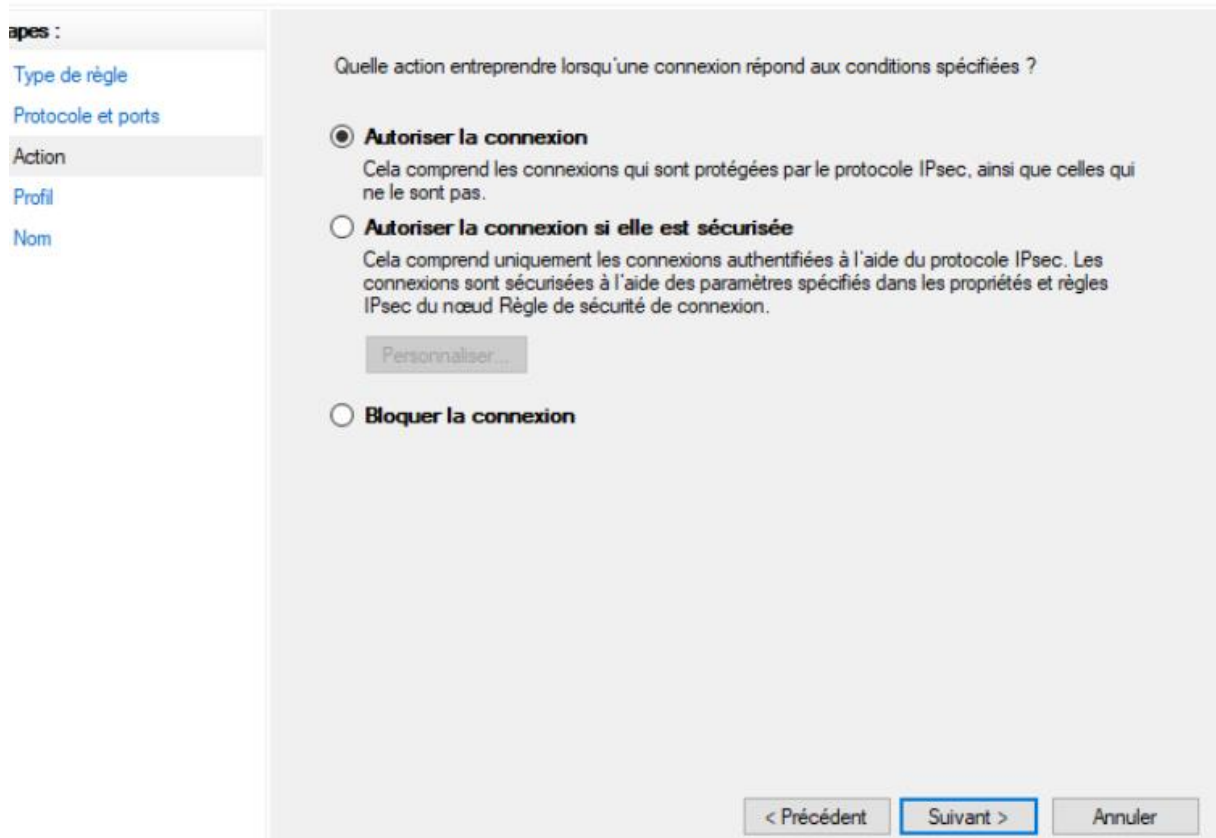
Déclaration de l'AD

Avant pour que ça fonctionne il faut définir deux règles pare-feu une entrante l'autre sortant pour autoriser le trafic entrant et sortant vers le port 389 de l'AD sois LDAP je parle bien ici du pare feu windows

The screenshot shows the 'Protocole et ports' configuration step in pfSense. On the left, a sidebar lists the configuration steps: 'Type de règle', 'Protocole et ports' (selected), 'Action', 'Profil', and 'Nom'. The main area contains the following options:

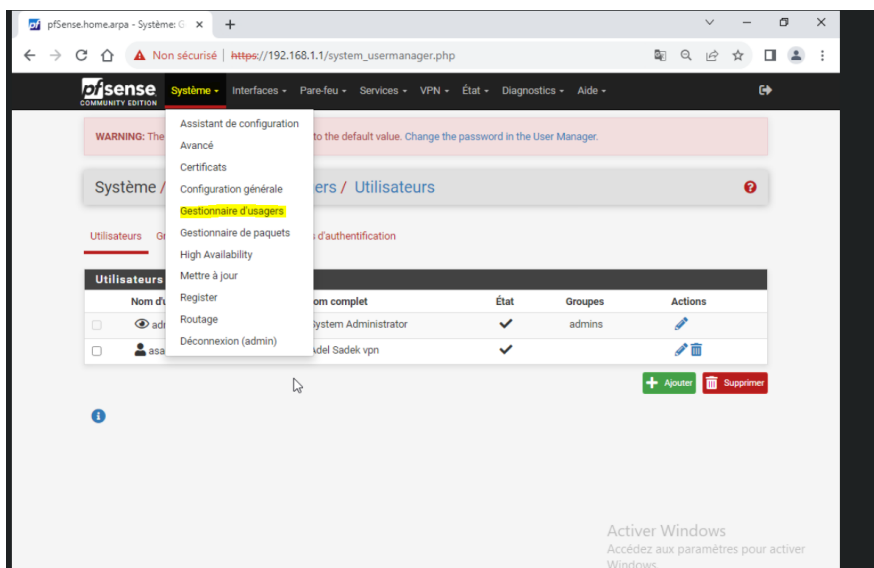
- 'Cette règle s'applique-t-elle à TCP ou UDP ?' with radio buttons for 'TCP' and 'UDP' (selected).
- 'Cette règle s'applique-t-elle à tous les ports locaux ou à des ports locaux spécifiques ?' with radio buttons for 'Tous les ports locaux' and 'Ports locaux spécifiques :'. The 'Ports locaux spécifiques' option is selected, and a text input field contains '389'. Below the input field, an example is provided: 'Exemple : 80, 443, 5000-5010'.

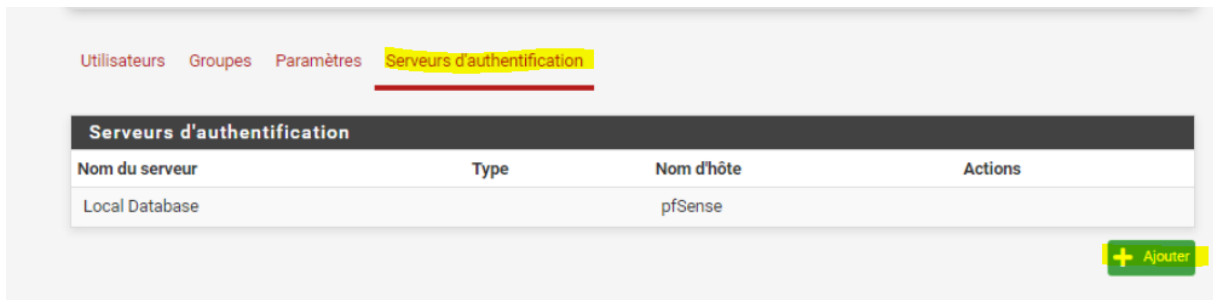
At the bottom right, there are three buttons: '< Précédent', 'Suivant >' (highlighted), and 'Annuler'.



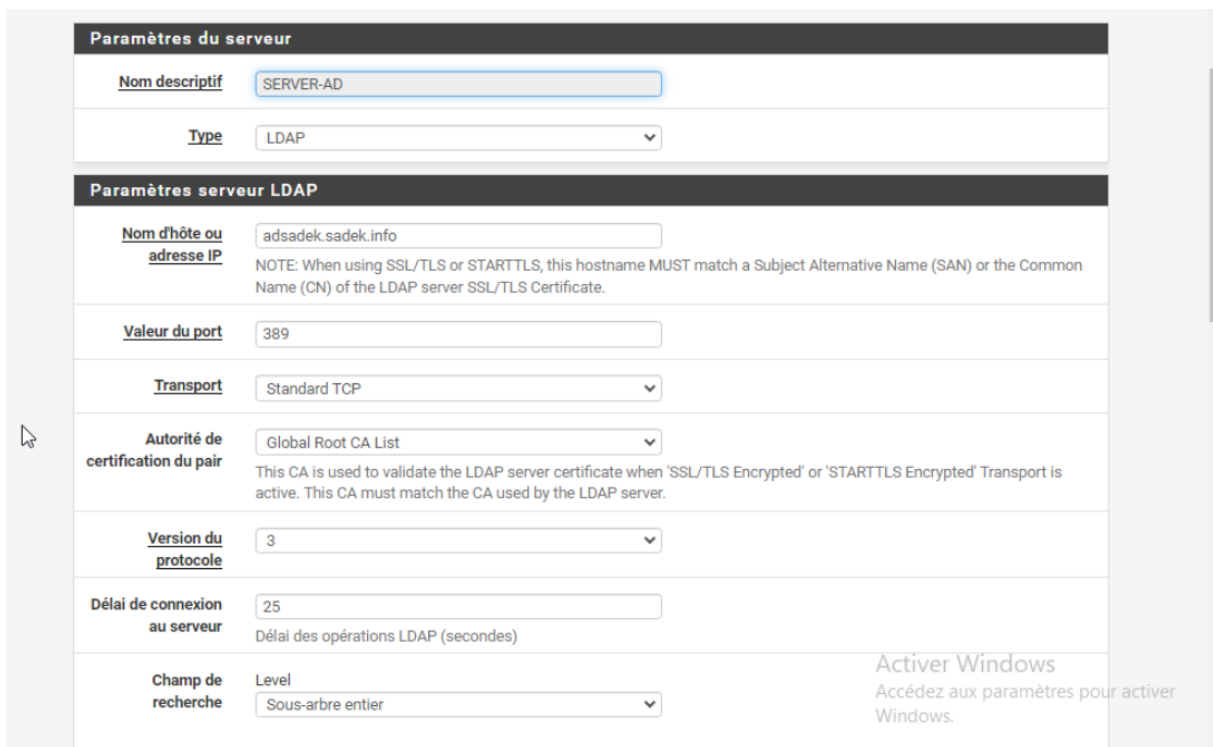
Pareil pour la sortie

D'abord on va déclarer l'AD





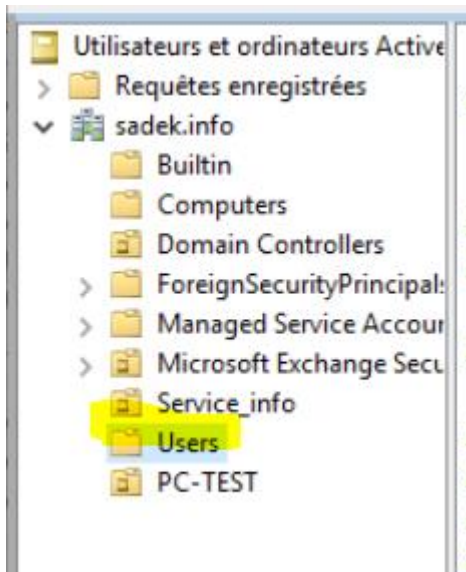
Ensuite remplir les champs dans cette partie IP ou FQDN du controleur de domaine



Puis pour la seconde partie il y'a plusieurs choses à remplir

Il faut renseigner le domaine sous cette forme et les UO dans lesquels PFSense pourra regarder pour chercher des users

Mes users sont dans l' UO Services_info



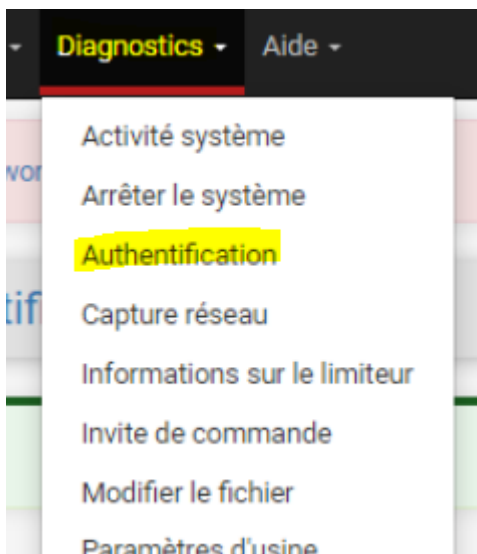
Base DN	DC=sadek,DC=info	
Conteneurs d'authentification	OU=Service_info,DC=sadek,DC=info	<input type="button" value="Sélectionner un conteneur"/>
Remarque: Semi-Colon séparé. Cela sera remplacé par la base de recherche dn ci-dessus ou le chemin de conteneur complet peut être spécifié contenant un composant dc =. Exemple: CN=Utilisateurs; DC=exemple, DC=com ou OU=Personal; OU = Freelancers		
Requêtes étendues	<input type="checkbox"/> Activer les requêtes étendues	
Lier anonyme	<input type="checkbox"/> Utilisez des liens anonymes pour résoudre des noms distincts	
Lier les informations d'identification	CN=wds,OU=Service_info,DC=sadek,DC=info	*****
*Attribut de nommage utilisateur	samAccountName	
Attribut de nommage de groupe	cn	
Attribut de membre du groupe	memberOf	
Groupes RFC 2307	<input type="checkbox"/> Le serveur LDAP utilise des appartenances aux groupes de type RFC 2307 L'appartenance à un groupe de style RFC 2307 comporte des membres listés sur l'objet de groupe plutôt que d'utiliser des groupes répertoriés sur un objet utilisateur. Laissez désactiver pour l'appartenance au groupe de style Active Directory (RFC 2307bis).	

Ensuite on registre

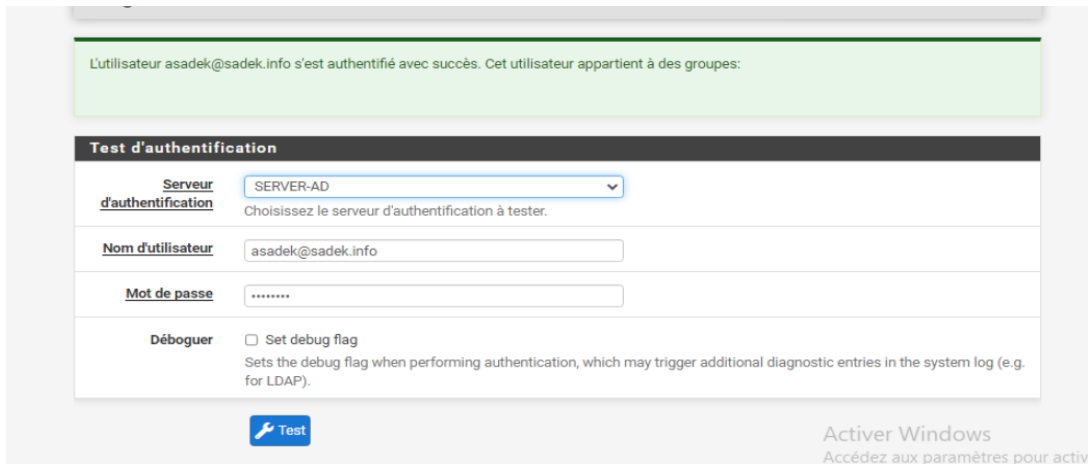
Attribut de membre du groupe	<input type="text" value="memberOf"/>
Groupes RFC 2307	<input type="checkbox"/> Le serveur LDAP utilise des appartenances aux groupes de type RFC 2307 L'appartenance à un groupe de style RFC 2307 comporte des membres listés sur l'objet de groupe plutôt que d'utiliser des groupes répertoriés sur un objet utilisateur. Laissez désactiver pour l'appartenance au groupe de style Active Directory (RFC 2307bis).
Classe d'objet de groupe	<input type="text" value="group"/> Classe d'objet utilisée pour les groupes en mode RFC2307. Généralement, "posixGroup" ou "groupe".
Shell Authentication Group DN	<input type="text"/> If LDAP server is used for shell authentication, user must be a member of this group and have a valid posixAccount attributes to be able to login. Example: CN=Remoteshellusers,CN=Users,DC=example,DC=com
Encodage UTF8	<input type="checkbox"/> UTF8 encode les paramètres LDAP avant de les envoyer au serveur. Nécessaire pour prendre en charge les caractères internationaux, mais peut ne pas être pris en charge par chaque serveur LDAP.
Altérations de nom d'utilisateur	<input type="checkbox"/> Ne pas oublier la partie du nom d'utilisateur après le symbole @ p. ex. utilisateur@hôte devient utilisateur lorsque décoché.
Allow unauthenticated bind	<input type="checkbox"/> Allow unauthenticated bind Unauthenticated binds are bind with an existing login but with an empty password. Some LDAP servers (Microsoft AD) allow this type of bind without any possibility to disable it.

Activer Windows

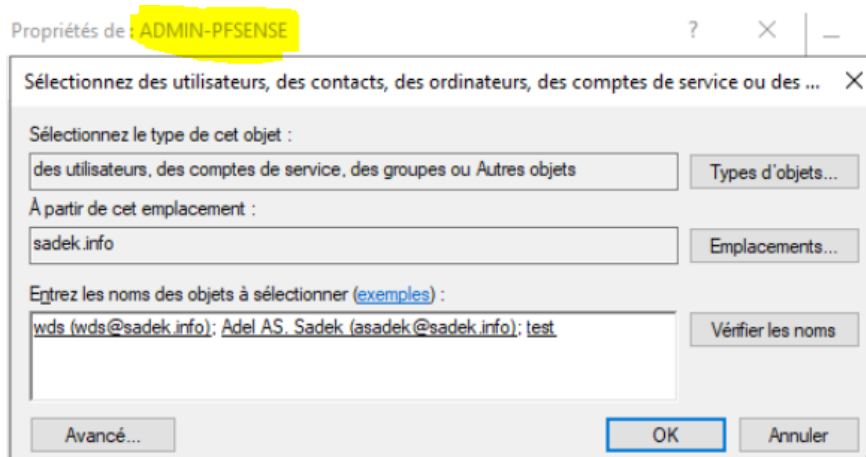
Ensuite je test



Parfait

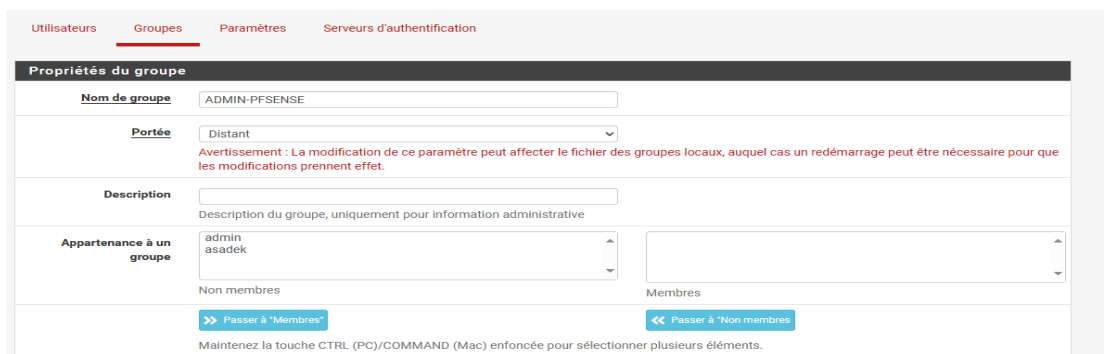


Créer un groupe Admin dans l'AD dans l'UO Services_Info






Créer groupe dans pfSense

Dans PfSense il faut créer un groupe local qui possède exactement le même nom que le groupe dans l'AD



Ensuite appuyer sur modifier et attribuer des droits à ce groupe

Groupes			
Nom du groupe	Description	Nombre de membres	Actions
ADMIN-PFSENSE		0	  








Privileges attribués		
Nom	Description	Action
+ Ajouter		
Enregistrer		

Ensuite on a une liste de privilèges que l'on peut affecter

Privileges de groupe	
Groupe	ADMIN-PFSENSE
Privileges assignés	<ul style="list-style-type: none">WebCfg - Système: Passerelles: Modifier les Groupes de PasserellesWebCfg - Système: Configuration généraleWebCfg - Système: Gestion de GroupeWebCfg - Système: Gestion de Groupe: Ajouter des privilègesWebCfg - Système: Synchronisation haute disponibilitéCfgWeb - Système : Connexion / Déconnexion / Tableau de bordCfgWeb - Système : Gestionnaire de paquetsCfgWeb - Système : Gestionnaire de paquets : Installer le paquetCfgWeb - Système : Gestionnaire de paquets : Paquets installésWebCfg - Système: Routes StatiquesWebCfg - Système: Routes Statiques: Modifier routeCfgWeb - Système - Mise à jour: ParamètresWebCfg - Système: Gestion des UtilisateursWebCfg - Système: Gestion des Utilisateurs: Ajouter des privilègesWebCfg - Système: Gestion des Utilisateurs: ParamètresWebCfg - Système: Gestionnaire des Mots de passe UtilisateursWebCfg - Système: Paramètres UtilisateurWebCfg - VPN: IPsecWebCfg - VPN: IPsec: Modifier la phase 1WebCfg - VPN: IPsec: Modifier la phase 2

Maintenez la touche CTRL (PC)/COMMAND (Mac) enfoncée pour sélectionner plusieurs éléments.

Je vais attribuer que les droits sur le serveur VPN openvpn la partie client, dans le cas dans une entreprise ou il y'a des techniciens, admin et inge les techniciens ne peuvent que voir et les admins de niveau 1 ne peuvent que ajouter des users openvpn voir exporter la config.

Privileges attribués		
Nom	Description	Action
WebCfg - OpenVPN: Client Export Utility	Allow access to the OpenVPN: Client Export Utility page.	
WebCfg - OpenVPN: Clients	Allow access to the 'OpenVPN: Clients' page.	
WebCfg - OpenVPN: Client Specific Override	Allow access to the 'OpenVPN: Client Specific Override' page.	
WebCfg - OpenVPN: Client Specific Override Edit Advanced	Allow edit access to the 'OpenVPN: Client Specific Override' advanced settings field. (Privilège administrateur)	
WebCfg - OpenVPN: Clients Edit Advanced	Allow edit access to the 'OpenVPN: Clients' Advanced settings field. (Privilège administrateur)	
WebCfg - Status: OpenVPN	Allow access to the 'Status: OpenVPN' page.	
WebCfg - Status: System Logs: OpenVPN	Allow access to the 'Status: System Logs: OpenVPN' page.	
Avis de sécurité: les utilisateurs de ce groupe ont effectivement un accès au niveau administrateur		
+ Ajouter		

Ensuite je définis le serveur d'authentification utiliser pour ce loguer sur la page pfsense

The screenshot shows the 'Paramètres' (Parameters) page in the pfSense web interface. The breadcrumb trail is 'Système / Gestionnaire d'utilisateurs / Paramètres'. The 'Paramètres' tab is selected. The configuration is as follows:

- Expiration de la session:** A dropdown menu with a downward arrow.
- Temps en d'expiration en minutes des sessions de gestion suspendue:** A text input field with a value of 4. A note below states: 'La valeur par défaut est de 4 heures (240 minutes). Entrez 0 pour ne jamais que les sessions n'expirent jamais. REMARQUE: Ceci est risqué niveau sécurité !'
- Serveur d'authentification:** A dropdown menu with 'SERVER-AD' selected.
- Password Hash Algorithm:** A dropdown menu with 'bcrypt - Blowfish-based crypt' selected. A note below states: 'Selects which algorithm the firewall will use when creating hashes for local user passwords. The most secure option is currently bcrypt. Some users may prefer SHA-512-based crypt hashes for compatibility or compliance purposes.'
- Shell Authentication:** A checkbox labeled 'Use Authentication Server for Shell Authentication' is unchecked. A note below states: 'If RADIUS or LDAP server is selected it is used for console and SSH authentication. Otherwise, the Local Database is used. To allow logins with RADIUS credentials, equivalent local users with the expected privileges must be created first. To allow logins with LDAP credentials, Shell Authentication Group DN must be specified on the LDAP server configuration page.'
- Fréquence de rafraichissement de l'authentification:** A text input field with a value of 30. A note below states: 'Temps en secondes pour mettre en cache les résultats d'authentification. La valeur par défaut est de 30 secondes, maximum 3600 (une heure). Des temps plus courts entraînent des requêtes plus fréquentes aux serveurs d'authentification'

At the bottom, there are two buttons: 'Enregistrer' (Save) and 'Sauver & Tester' (Save & Test).

Phase de test :

Je me deconnecte et me reconnecte

The screenshot shows a login page with a dark blue background. The text 'SIGN IN' is displayed in white at the top. Below it, the email address 'asadek@sadek.info' is entered in a white input field. Underneath the email field is a password field represented by a series of white dots and a cursor. At the bottom, there is a green button with the text 'SIGN IN' in white.

Me voila connecter c'est parfait.

OpenVPN / Client Export Utility

Client Ré-écritures spécifiques au client Client Export

Serveur OpenVPN

Remote Access Server Server UDP4:1194

Client Connection Behavior

Host Name Resolution Autre

Nom d'hôte dedier.agrepe.com
Enter the hostname or IP address the client will use to connect to this server.

Verify Server CN Automatic - Use verify-x509-name where possible
Optionally verify the server certificate Common Name (CN) when the client connects.

Bloquer DNS Extérieur Block access to DNS servers except across OpenVPN while connected, forcing clients to use only VPN DNS servers.
Requiert Windows 10 et OpenVPN 2.3.9 ou ultérieur. Seul Windows 10 est sujet à une telle fuite DNS, les autres clients vont ignorer cette option puisqu'ils ne sont pas concernés

Legacy Client Do not include OpenVPN 2.5 and later settings in the client configuration.
When using an older client (OpenVPN 2.4.x), check this option to prevent the exporter from placing known-incompatible settings into the client configuration.

Silent Installer Create Windows installer for unattended deploy.
Create a silent Windows installer for unattended deploy, installer must be run with elevated permissions. Since this installer is not signed, you may need special software to deploy it correctly.

Bind Mode Do not bind to the local port
If OpenVPN client binds to the default OpenVPN port (1194), two clients may not run concurrently.

Certificate Export Options

PKCS#11 Certificate Storage Use PKCS#11 storage device (cryptographic token, HSM, smart card) instead of local files.

Microsoft Certificate Use Microsoft Certificate Storage instead of local files.