

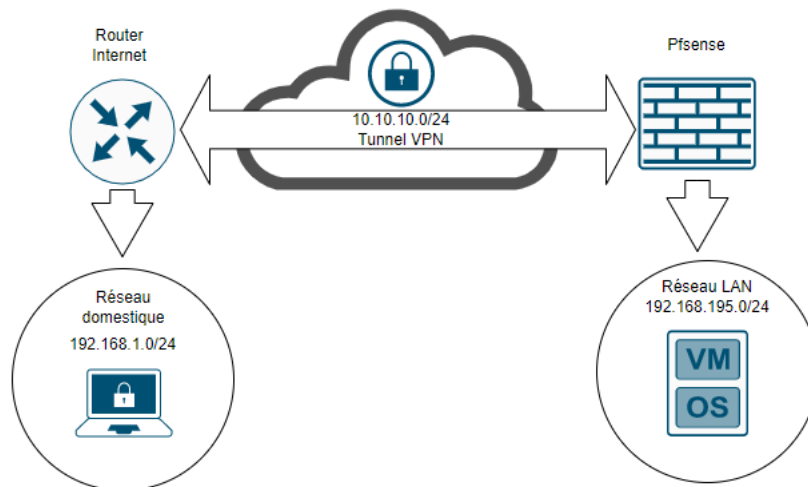
Cours Virtualisation des réseaux

Nantes Ynov Campus – 2022-2023

Activité Pratique 3

Mise en place d'un client VPN avec le logiciel Open Source Pfsense

Objectif : Tester de façon pratique la mise en place d'un tunnel VPN entre deux sites distincts.

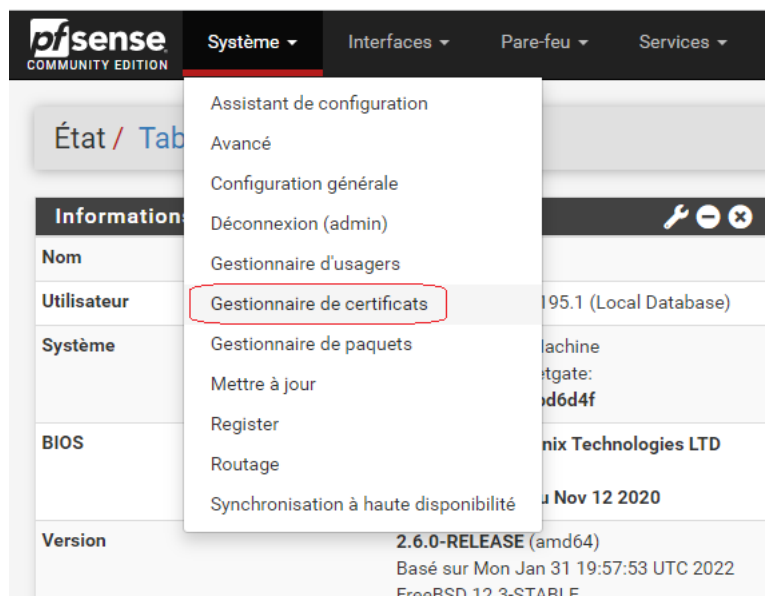


Pré requis

Pour réaliser cet exercice, vous devrez disposer d'au moins une machine disponible sous le LAN de Pfsense et d'une machine qui fera office de client pour réaliser les tests de connexion.

Etape 1 : Créer l'autorité de certification depuis Pfsense

Se rendre dans le gestionnaire de certificat pour commencer



Ajouter une nouvelle autorité de certification

pfSense COMMUNITY EDITION

Système ▾ Interfaces ▾ Pare-feu ▾ Services ▾ VPN ▾ État ▾ Diagnostics ▾ Aide ▾

Système / Gestionnaire de certificats / ACs

ACs Certificats Révocation de certificat

Recherche

Terme de recherche Les deux

Enter a search string or *nix regular expression to search certificate names and distinguished names.

Autorités de certification

Nom	Interne	Émetteur	Certificats	Nom distinctif	En cours d'utilisation	Actions
+ Ajouter						

Donner un nom à la nouvelle autorité et prendre le reste des options par défaut puis valider la création. Vous pouvez en plus modifier le Code du Pays « FR », le nom commun et le reste des paramètres si vous le souhaitez.

Système / Gestionnaire de certificats / ACs / Modifier

ACs Certificats Révocation de certificat

Créer / Modifier l'AC

Nom descriptif

Méthode

Trust Store ☐ Add this Certificate Authority to the Operating System Trust Store
When enabled, the contents of the CA will be added to the trust store so that they will be trusted by the operating system.

Randomize Serial ☐ Use random serial numbers when signing certificates
When enabled, if this CA is capable of signing certificates then serial numbers for certificates signed by this CA will be automatically randomized and checked for uniqueness instead of using the sequential value from Next Certificate Serial.

Autorité de certification interne

Key type

pfSense
COMMUNITY EDITION

Système ▾ Interfaces ▾ Pare-feu ▾ Services ▾ VPN ▾ État ▾ Diagnostics ▾ Aide ▾

Système / Gestionnaire de certificats / ACs

ACs Certificats Révocation de certificat

Recherche

Terme de recherche Les deux

Enter a search string or *nix regular expression to search certificate names and distinguished names.

Autorités de certification

Nom	Interne	Émetteur	Certificats	Nom distinctif	En cours d'utilisation	Actions
YNOV-CA	✓	auto-signé	0	CN=internal-ca, C=FR Valable depuis: Thu, 19 Jan 2023 22:53:17 +0100 Valable jusqu'au: Sun, 16 Jan 2033 22:53:17 +0100		

Etape 2 : Créer un certificat server PfSense

Pour créer un certificat server se rendre dans la rubrique « Certificats ».
L'autorité de certificat précédemment créé devrait apparaître.

Système / Gestionnaire de certificats / Certificats

ACs **Certificats** Révocation de certificat

Recherche

Terme de recherche Les deux

Enter a search string or *nix regular expression to search certificate names and distinguished names.

Certificats

Nom	Émetteur	Nom distinctif	En cours d'utilisation	Actions
webConfigurator default (63c9b30304b79) Server Certificate CA: No Serveur: Yes	auto-signé	O=pfSense webConfigurator Self-Signed Certificate, CN=pfSense-63c9b30304b79 Valable depuis: Thu, 19 Jan 2023 22:15:47 +0100 Valable jusqu'au: Wed, 21 Feb 2024 22:15:47 +0100		

Attribuer un nom au nouveau certificat serveur

Système / Gestionnaire de certificats / Certificats / Modifier ?

ACs **Certificats** Révocation de certificat

Ajouter/Signer un nouveau certificat

Méthode Créer un certificat interne ▼

Nom descriptif Certificat-server-OpenVPN

Certificat interne

Autorité de certification YNOV-CA ▼

Key type RSA ▼

2048 ▼
The length to use when generating a new RSA key, in bits.
The Key Length should not be lower than 2048 or some platforms may consider the certificate invalid.

Algorithme de hachage sha256 ▼

Dans la section Attributs de certificat, modifier le type de certificat pour préciser qu'il s'agit d'un certificat serveur puis enregistrer

Attributs de certificat

Notes d'attributs Les attributs suivants sont ajoutés aux certificats et aux requêtes lorsqu'ils sont créés ou signés. Ces attributs se comportent différemment en fonction du mode sélectionné.

Pour les certificats internes, ces attributs sont ajoutés directement au certificat comme indiqué.

Type de certificat Server Certificate ▼
Ajoutez les attributs d'utilisation spécifiques au certificat signé. Utilisez pour placer les restrictions d'utilisation ou l'octroi de capacités au certificat signé.

Noms alternatifs FQDN ou nom d'hôte ▼ Valeur

Type Valeur

Entrez des identifiants supplémentaires pour le certificat dans cette liste. Le champ Nom commun est automatiquement ajouté au certificat en tant que nom alternatif. La signature CA peut ignorer ou modifier ces valeurs.

Ajouter + Ajouter

Enregistrer

Système / Gestionnaire de certificats / Certificats ?

Created internal certificate Certificat-server-OpenVPN ×

ACs **Certificats** Révocation de certificat

Recherche

Terme de recherche Les deux ▼ Recherche Effacer

Enter a search string or *nix regular expression to search certificate names and distinguished names.

Certificats

Nom	Émetteur	Nom distinctif	En cours d'utilisation	Actions
webConfigurator default (63c9b30304b79) Server Certificate CA: No Serveur: Yes	auto-signé	O=pfSense webConfigurator Self-Signed Certificate, CN=pfSense-63c9b30304b79 i Valable depuis: Thu, 19 Jan 2023 22:15:47 +0100 Valide jusqu'à: Wed, 21 Feb 2024 22:15:47 +0100		✎ ⚙ 🔑 🔄 🗑
Certificat-server-OpenVPN Server Certificate CA: No Serveur: Yes	YNOV-CA	CN=interne-ca, C=FR i Valable depuis: Thu, 19 Jan 2023 23:03:09 +0100 Valide jusqu'à: Sat, 27 Nov 2023 23:03:09 +0100		✎ ⚙ 🔑 🔄 🗑

Etape 3 : se créer un compte utilisateur pour l'accès distant

Maintenant que nous disposons d'une autorité de certificat et d'un certificat serveur, nous pouvons procéder à la création de l'utilisateur et de son certificat lui permettant de se connecter

The screenshot shows the pfSense web interface. In the top navigation bar, the 'Système' menu is open, and 'Gestionnaire d'utilisateurs' is highlighted with a red box. Below this, the 'Utilisateurs' page is displayed. It features a breadcrumb trail: 'Système / Gestionnaire d'utilisateurs / Utilisateurs'. There are tabs for 'Utilisateurs', 'Groupes', 'Paramètres', and 'Serveurs d'authentification'. The 'Utilisateurs' tab is active, showing a table with the following data:

	Nom d'utilisateur	Nom complet	État	Groupes	Actions
<input type="checkbox"/>	admin	System Administrator	✓	admins	

At the bottom right of the table, there are two buttons: '+ Ajouter' (highlighted with a red box) and 'Supprimer'.

Dans la rubrique « Propriétés utilisateur » saisir les informations d'identification de votre utilisateur, le mot de passe lui permettant de se connecter au VPN et cocher la case permettant de créer un certificat client

Utilisateurs Groupes Paramètres Serveurs d'authentification

Propriétés utilisateur

Défini par: USER

Désactivé: ☐ Cet utilisateur ne peut pas s'authentifier

Nom d'utilisateur: wilfried.vpn

Mot de passe: [masqué] [masqué]

Nom complet: wilfried M
Nom complet de l'utilisateur, à des fins administratives uniquement

Date d'expiration: [vide]
Laissez vide si le compte ne doit pas expirer, sinon entrez la date d'expiration sous la forme MM/JJ/AAAA

Paramètres personnalisés: ☐ Utilisez les options GUI individuelles personnalisées et la disposition du tableau de bord pour cet utilisateur.

Appartenance à un groupe: admins
Pas un membre de: [vide] Membre de: [vide]

>> Déplacer vers la liste "Membre de" << Déplacer vers la liste "Non membre de"

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

Certificat: ☒ Cliquez pour créer un certificat client

Donner un nom au certificat client, conserver les informations par défaut puis cliquer sur enregistrer.

Créer un certificat pour l'utilisateur

Nom descriptif: certificat-utilisateur-wm

Autorité de certification: YNOV-CA

Key type: RSA

2048
The length to use when generating a new RSA key, in bits.
The Key Length should not be lower than 2048 or some platforms may consider the certificate invalid.

Algorithme de hachage: sha256
The digest method used when the certificate is signed.
The best practice is to use an algorithm stronger than SHA1. Some platforms may consider weaker digest algorithms invalid

Durée de vie: 3650

Clés

Clés SSH autorisées: [vide]
Entrez les clés SSH autorisées pour cet utilisateur

Clé pré-partagée IPsec: [vide]

Enregistrer

Système / Gestionnaire d'usagers / Utilisateurs

Utilisateurs

Groupes

Paramètres

Serveurs d'authentification

Utilisateurs

	Nom d'utilisateur	Nom complet	État	Groupes	Actions
<input type="checkbox"/>	admin	System Administrator	✓	admins	
<input type="checkbox"/>	wilfried.vpn	wilfried M	✓		

Ajouter

Supprimer

Pour vérifier que votre certificat utilisateur a bien été créé, se rendre dans le gestionnaire de certificat

Système / Gestionnaire de certificats / Certificats

ACsCertificatsRévocation de certificat

Recherche

Terme de recherche

Les deux

Recherche

Effacer

Enter a search string or *nix regular expression to search certificate names and distinguished names.

Certificats

Nom	Émetteur	Nom distinctif	En cours d'utilisation	Actions
webConfigurator default (63c9b30304b79) Server Certificate CA: No Serveur: Yes	auto-signé	O=pfSense webConfigurator Self-Signed Certificate, CN=pfSense-63c9b30304b79 Valable depuis: Thu, 19 Jan 2023 22:15:47 +0100 Valide jusqu'au: Wed, 21 Feb 2024 22:15:47 +0100		
Certificat-server-OpenVPN Server Certificate CA: No Serveur: Yes	YNOV-CA	CN=interne-ca, C=FR Valable depuis: Thu, 19 Jan 2023 23:03:09 +0100 Valide jusqu'au: Sat, 27 Nov 2023 23:03:09 +0100		
certificat-utilisateur-wm User Certificate CA: No Serveur: No	YNOV-CA	CN=wilfried.vpn, C=FR Valable depuis: Thu, 19 Jan 2023 23:14:08 +0100 Valide jusqu'au: Sun, 16 Jan 2023 23:14:08 +0100	Certificat utilisateur	

Etape 4 : Créer la configuration serveur OpenVPN

Se rendre dans la rubrique

pfSense

COMMUNITY EDITION

Système ▾

Interfaces ▾

Pare-feu ▾

Services ▾

VPN ▾

État ▾

Diagnostics ▾

Aide ▾

Système / Gestionnaire de certificats / Certificats

ACs

Certificats

Révocation de certificat

Recherche

Terme de recherche

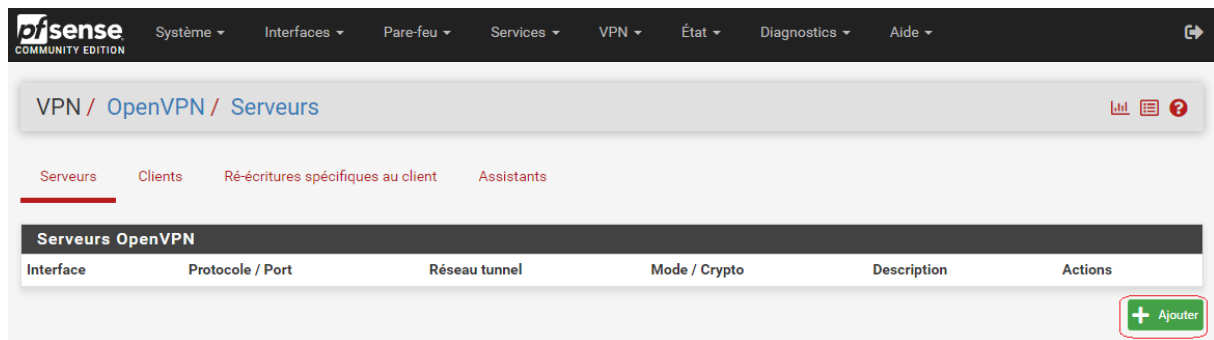
Les deux ▾

Recherche

Effacer

Enter a search string or *nix regular expression to search certificate names and distinguished names.

Cliquer sur ajouter



Dans le cadre de ce TP il ne sera pas nécessaire de modifier toutes les options. Nous procéderons dans ce cas à la modification des options nécessaires pour réaliser nos tests

Dans la section cryptographique, sélectionner le certificat serveur créé précédemment et conserver le reste des informations par défaut de cette section

Paramètres cryptographiques	
Configuration TLS	<input checked="" type="checkbox"/> Utiliser une clé TLS Une clé TLS améliore la sécurité d'une connexion OpenVPN en demandant aux deux parties d'avoir une clé commune avant qu'un pair puisse effectuer une négociation TLS. Cette couche d'authentification HMAC permet de transférer les paquets de canal de contrôle sans que la clé appropriée soit supprimée, protégeant les pairs contre les attaques ou les connexions non autorisées. La clé TLS n'a aucun effet sur les données du tunnel.
	<input checked="" type="checkbox"/> Générer automatiquement une clé TLS.
Autorité de certification du pair	YNOV-CA
Liste des Certificats de Révocation de pairs.	No Certificate Revocation Lists defined. One may be created here: System > Cert. Manager
OCSP Check	<input type="checkbox"/> Check client certificates with OCSP
Certificat du serveur	Certificat-server-OpenVPN (Serveur : Oui, CA : YNOV-CA)
Longueur du paramètre *DH	2048 bit Ensemble de paramètres Diffie-Hellman (DH) utilisé pour l'échange de clés. i
Courbe ECDH	Utiliser les valeurs par défaut La courbe elliptique à utiliser pour l'échange de clés. La courbe du certificat du serveur est utilisée par défaut lorsque le serveur utilise un certificat ECDSA. Sinon, secp384r1 est utilisé comme un repli.
Data Encryption Negotiation	<input checked="" type="checkbox"/> Enable Data Encryption Negotiation This option allows OpenVPN clients and servers to negotiate a compatible set of acceptable cryptographic data encryption algorithms from those selected in the Data Encryption Algorithms list below. Disabling this feature is deprecated.
Data Encryption Algorithms	<div> AES-128-CBC (128 bit key, 128 bit block) AES-128-CFB (128 bit key, 128 bit block) </div> <div> AES-256-GCM AES-128-GCM </div>

Dans la section paramètre du tunnel nous devons choisir le sous-réseau qui correspondra au tunnel VPN qui sera ici 10.10.10.0/24 et le réseau à rendre accessible ici notre LAN 192.168.195.0/24

L'option « Rediriger la passerelle » va permettre de rediriger tous les flux d'échange dans le tunnel VPN

Paramètres du tunnel	
Réseau Tunnel IPv4	10.10.10.0/24 This is the IPv4 virtual network or network type alias with a single entry used for private communications between this server and client hosts expressed using CIDR notation (e.g. 10.0.8.0/24). The first usable address in the network will be assigned to the server virtual interface. The remaining usable addresses will be assigned to connecting clients.
Tunnel réseau IPv6	 This is the IPv6 virtual network or network type alias with a single entry used for private communications between this server and client hosts expressed using CIDR notation (e.g. fe80::/64). The ::1 address in the network will be assigned to the server virtual interface. The remaining addresses will be assigned to connecting clients.
Rediriger la passerelle IPv4	<input type="checkbox"/> Force all client-generated IPv4 traffic through the tunnel.
Rediriger la passerelle IPv6	<input type="checkbox"/> Force all client-generated IPv6 traffic through the tunnel.
Réseau(x) local/locaux IPv4	192.168.195.0/24 IPv4 networks that will be accessible from the remote endpoint. Expressed as a comma-separated list of one or more CIDR ranges or host/network type aliases. This may be left blank if not adding a route to the local network through this tunnel on the remote machine. This is generally set to the LAN network.
Réseau(x) local/locaux IPv6	 IPv6 networks that will be accessible from the remote endpoint. Expressed as a comma-separated list of one or more IP/PREFIX or host/network type aliases. This may be left blank if not adding a route to the local network through this tunnel on the remote machine. This is generally set to the LAN network.
Connexions simultanées	 Spécifier le nombre maximum de clients autorisés à se connecter en même temps à ce serveur.
Allow Compression	Refuse any non-stub compression (Most secure)

Dans la section client dans le cas où il s'agirait d'un utilisateur nomade l'option ci-dessous devrait lui permettre de se connecter depuis n'importe quel périphérique

L'option sélectionnée en topologie va permettre d'isoler l'utilisateur connecté au réseau des autres utilisateurs VPN

Paramètres du client

IP dynamique ☒ Autoriser les clients connectés à conserver leurs connexions si leur adresse IP change.

Topologie net30 - Réseau /30 isolé par client

Spécifie la méthode utilisée pour fournir une adresse IP d'adaptateur virtuel aux clients lors de l'utilisation du mode TUN sur IPv4. Certains clients peuvent exiger que cela soit mis en «sous-réseau» même pour IPv6, par exemple OpenVPN Connect (iOS / Android). Les anciennes versions d'OpenVPN (avant 2.0.9) ou les clients tels que les téléphones Yealink peuvent nécessiter "net30".

Dans les paramètres clients avancés définir le domaine et le serveur dns si vous en disposez ou votre serveur pfsense

Paramètres clients avancés

Domaine DNS par défaut ☒ Renseigner un nom de domaine par défaut aux clients.

Domaine DNS par défaut

Activer le Serveur DNS ☒ Fournir une liste de serveur DNS pour les clients. Les adresses peuvent être en IPv4 ou IPv6.

Serveur DNS 1

Serveur DNS 2

Serveur DNS 3

Serveur DNS 4

Bloquer DNS Extérieur ☐ Bloquer aux clients Windows 10 l'accès aux serveurs DNS sauf à travers OpenVPN pendant qu'ils sont connectés, forçant les clients à n'utiliser que les serveurs DNS du VPN.
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

Forcer une mise à jour du cache DNS ☐ Exécuter "net stop dnscache", "net start dnscache", "ipconfig /flushdns" et "ipconfig /registerdns" après avoir initialisé la connexion.
Ceci est connu pour permettre à Windows de reconnaître les serveurs DNS poussés.

Activer Serveur NTP ☐ Fournir une liste de serveurs NTP aux clients

Activer NetBIOS ☐ Activer NetBIOS sur TCP/IP
Si cette option n'est pas définie, toutes les options NetBIOS-over-TCP/IP (incluant WINS) seront désactivées.

Empêcher la mise en cache des informations d'identification par mesure de sécurité puis valider la création de la configuration

Configuration avancée

Options personnalisés

auth-nocache

Entrez toutes les options supplémentaires à ajouter à la configuration du serveur OpenVPN ici, séparées par un point-virgule.
EXEMPLE: appuyez sur "route 10.0.0.0 255.255.255.0"

Username as Common Name

☐ Use the authenticated client username instead of the certificate common name (CN).

When a user authenticates, if this option is enabled then the username of the client will be used in place of the certificate common name for purposes such as determining Client Specific Overrides.

UDP Fast E/S

☐ Utilisez des opérations d'E/S rapides avec des écritures UDP sur tun / tap. Expérimental.

Optimise la boucle d'événements d'écriture de paquets, améliorant l'efficacité du processeur de 5% à 10%. Non compatible avec toutes les plateformes, et non compatible avec la limitation de bande passante OpenVPN.

Exit Notify

Reconnect to this server / Retry once

Send an explicit exit notification to connected clients/peers when restarting or shutting down, so they may immediately disconnect rather than waiting for a timeout. In SSL/TLS Server modes, clients may be directed to reconnect or use the next server. This option is ignored in Peer-to-Peer Shared Key mode and in SSL/TLS mode with a blank or /30 tunnel network as it will cause the server to exit and not restart.

Tampon d'envoi/réception

Par défaut

Configurez une taille de mémoire tampon d'envoi et de réception pour OpenVPN. La taille de la mémoire tampon par défaut peut être trop faible dans de nombreux cas, selon les vitesses de liaison montante du matériel et du réseau. Trouver la meilleure taille de mémoire tampon peut faire quelques expériences. Pour tester la meilleure valeur pour un site, commencez à 512KiB et testez des valeurs plus élevées et plus faibles.

Création d'une passerelle




☒ Les deux
☐ IPv4 uniquement
☐ IPv6 uniquement

If you assign a virtual interface to this OpenVPN server, this setting controls which gateway types will be created. The default setting is "both".

Niveau de verbosité




défaul


[VPN](#) / [OpenVPN](#) / [Serveurs](#)

[Serveurs](#)
[Clients](#)
[Ré-écritures spécifiques au client](#)
[Assistants](#)

Serveurs OpenVPN

Interface	Protocole / Port	Réseau tunnel	Mode / Crypto	Description	Actions
WAN	UDP4 / 1194 (TUN)	10.10.10.0/24	Mode: Remote Access (SSL/TLS + User Auth) Data Ciphers: AES-256-GCM, AES-128-GCM, CHACHA20-POLY1305, AES-256-CBC Digest: SHA256 D-H Params: 2048 bits	Configuration VPN Distant	  

 Ajouter

Etape 5 : Créer les règles de firewall pour OpenVPN

The screenshot shows the pfSense web interface. At the top, the navigation bar includes 'Système', 'Interfaces', 'Pare-feu' (highlighted), and 'Services'. Below the navigation bar, the main content area shows 'État / Tableau de bord' (Status / Dashboard). A table titled 'Informations système' (System Information) is visible, with columns for 'Nom' (Name) and 'Utilisateur' (User). The 'Nom' row shows 'router.home.lab' and the 'Utilisateur' row shows 'admin@192.168.1.1'. A dropdown menu is open from the 'Pare-feu' tab, showing options: 'Alias', 'IPs virtuels', 'NAT', 'Plannings', 'Règles' (highlighted with a red box), and 'Régulateur de flux'.

Configurer une nouvelle règle permettant d'accéder au sous réseau souhaité

Pare-feu / Règles / WAN

Flottant(e) **WAN** LAN OPT1 OpenVPN

Règles (Faire glisser pour changer l'ordre)

☐	États	Protocole	Source	Port	Destination	Port	Passerelle	File d'attente	Ordonnancement	Description	Actions
✗	0 / 20 KiB	*	Réseaux RFC 1918	*	*	*	*	*		Bloquer les réseaux privés	⚙️
✗	0 / 2 KiB	*	Réservée Non assignées par l'IANA	*	*	*	*	*		Bloquer les réseaux invalides	⚙️

Aucune règle n'est définie pour cette interface
Toute connexion entrante vers cette interface sera bloquée jusqu'à ce que des règles de passage soient ajoutées. Cliquez sur le bouton pour ajouter une nouvelle règle.

↑ Ajouter ↓ Ajouter 🗑 Supprimer 📁 Enregistrer + Séparateur

Autoriser le trafic depuis l'interface WAN via le protocole UDP

Pare-feu / Règles / Modifier

Modifier la règle de Pare-Feu

Action Autoriser
Choisissez que faire des paquets qui correspondent aux critères ci-dessous.
Aide : La différence entre bloquer et rejeter est qu'avec 'Rejeter', un paquet (TCP, RST ou ICMP port unreachable pour UDP) est retourné à l'expéditeur, alors qu'avec 'Bloquer', le paquet est supprimé silencieusement. Dans tous les cas, le paquet est supprimé.

Désactivé ☐ Désactiver cette règle
Choisissez cette option pour désactiver cette règle sans la supprimer de la liste.

Interface WAN
Choisissez l'interface d'où les paquets doivent provenir pour correspondre à cette règle.

Famille d'adresse IPv4
Choisissez la version du protocole IP à laquelle cette règle s'applique.

Protocole UDP
Choisissez quel protocole IP cette règle devrait correspondre.

Source

Source ☐ Invert match tout Source Address /

[Afficher les options avancées](#)

La **plage de ports source** d'une connexion est généralement aléatoire et presque jamais égale au port de destination. Dans la plupart des cas, ce paramètre doit rester à sa valeur par défaut, **any**.

Destination

Destination ☐ Invert match WAN address Destination Address /

Plage de port de destination (autre) 1194 (autre) 1194
De Personnalisé(e) À Personnalisé(e)

Spécifiez le port destination ou la plage de port pour cette règle. Le champ « A » peut rester vide seulement si le filtre est sur un seul port.

Options additionnelles

Journalise ☐ Journaliser les paquets gérés par cette règle
Suggestion : Le pare-feu a un espace de journalisation limité. N'activez pas la journalisation de tout. Si vous faites beaucoup de journalisation considérez l'utilisation d'un serveur syslog distant (voir la page [Statut: Journaux système : Paramètres](#)).

Description
Une description est proposée ici pour aider l'administrateur. Un maximum de 52 caractères sera utilisé dans l'ensemble de règles et affiché dans le journal du pare-feu.

Options Avancées [Afficher les options avancées](#)

Appliquer la nouvelle règle

Pare-feu / Règles / WAN

La configuration de la règle de pare-feu a été modifiée
Ces modifications doivent être appliquées pour prendre effet.

✓ Appliquer les modifications

Flottant(e) WAN LAN OPT1 OpenVPN

Règles (Faire glisser pour changer l'ordre)

	États	Protocole	Source	Port	Destination	Port	Passerelle	File d'attente	Ordonnancement	Description	Actions
<input checked="" type="checkbox"/>	✗	0/21 KIB	*		Réseaux RFC 1918	*	*	*		Bloquer les réseaux privés	⚙️
<input checked="" type="checkbox"/>	✗	0/2 KIB	*		Réservee Non assignées par l'IANA	*	*	*		Bloquer les réseaux invalides	⚙️
<input type="checkbox"/>	✓	0/0 B	IPv4 UDP	*	WAN address	1194 (OpenVPN)	*	aucun			📌 🛠️ 🔄 🗑️

↑ Ajouter ↓ Ajouter 🗑️ Supprimer 📁 Enregistrer + Séparateur

Ensuite dans l'onglet OpenVPN créer la règle permettant d'indiquer le sous réseau qu'il sera possible d'accéder

Pare-feu / Règles / OpenVPN

Flottant(e) WAN LAN OPT1 OpenVPN

Règles (Faire glisser pour changer l'ordre)

	États	Protocole	Source	Port	Destination	Port	Passerelle	File d'attente	Ordonnancement	Description	Actions
--	-------	-----------	--------	------	-------------	------	------------	----------------	----------------	-------------	---------

Aucune règle n'est définie pour cette interface
Toute connexion entrante vers cette interface sera bloquée jusqu'à ce que des règles de passage soient ajoutées. Cliquez sur le bouton pour ajouter une nouvelle règle.

↑ Ajouter ↓ Ajouter 🗑️ Supprimer 📁 Enregistrer + Séparateur

Ici j'ai créé une nouvelle règle pour accéder au sous réseau LAN 192.168.195.0/24 et uniquement en SSH

Pare-feu / Règles / OpenVPN

Flottant(e) WAN LAN OPT1 OpenVPN

Règles (Faire glisser pour changer l'ordre)

	États	Protocole	Source	Port	Destination	Port	Passerelle	File d'attente	Ordonnancement	Description	Actions
<input type="checkbox"/>	✓	0/0 B	IPv4 TCP	*	192.168.195.0/24	22 (SSH)	*	aucun			📌 🛠️ 🔄 🗑️

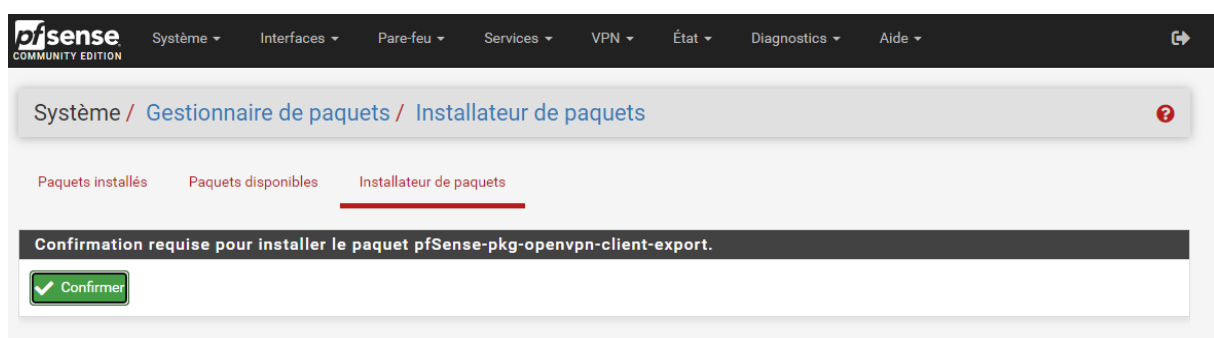
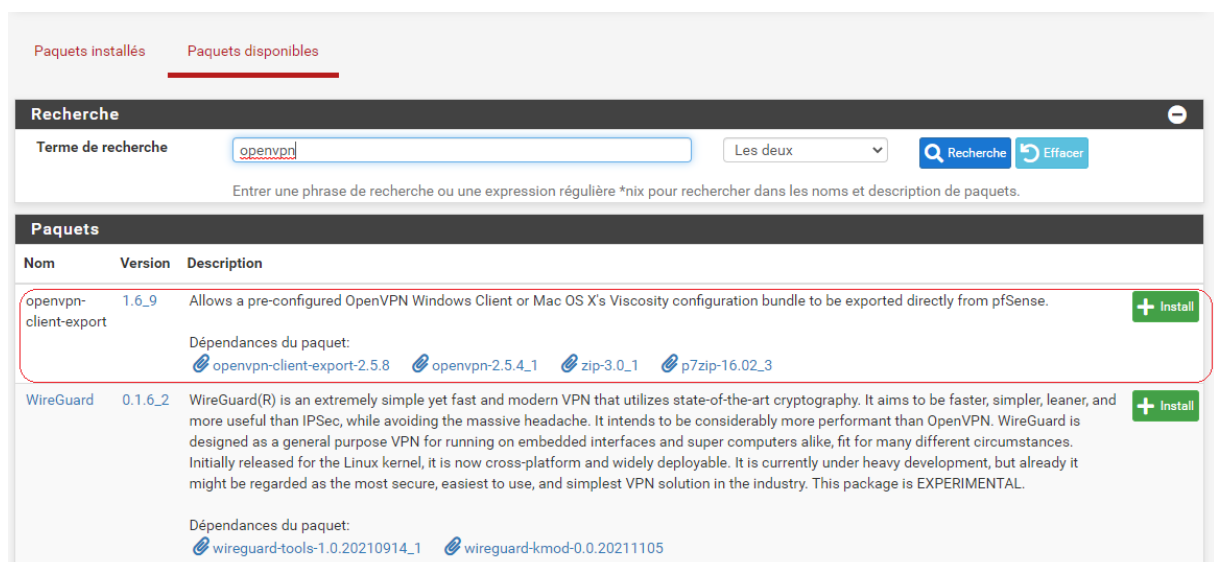
↑ Ajouter ↓ Ajouter 🗑️ Supprimer 📁 Enregistrer + Séparateur

Etape 6 : Exporter la configuration

Se rendre dans le gestionnaire de paquets pour installer le client permettant d'exporter la configuration



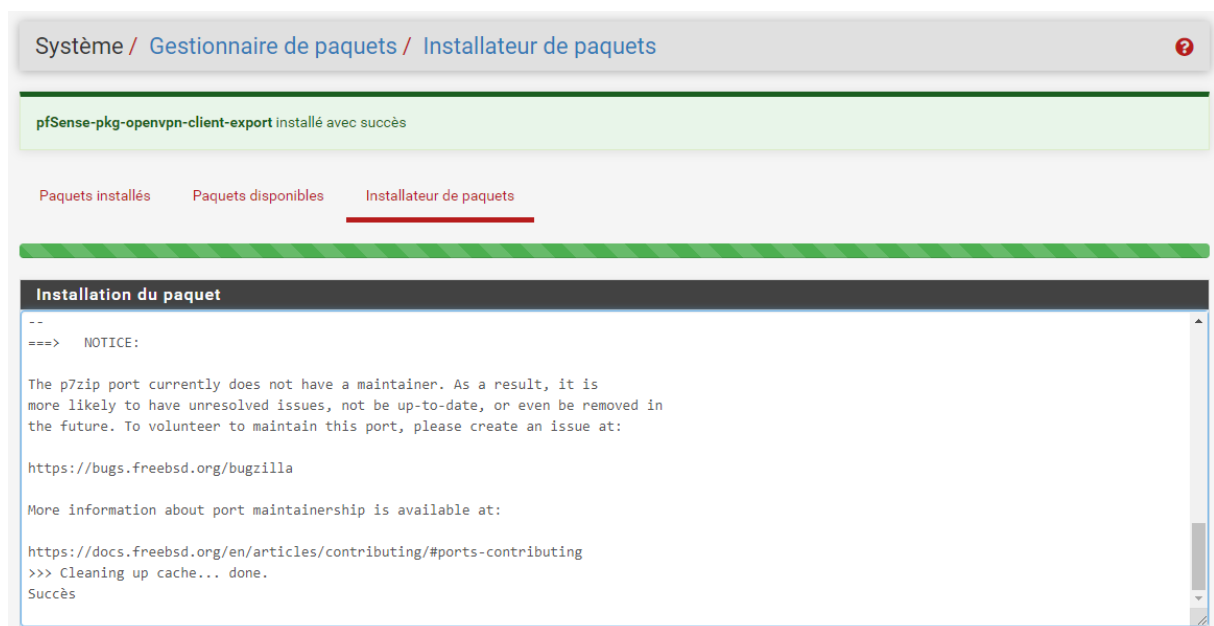
Rechercher le client openvpn puis cliquer sur installer



Suivre la progression de l'installation



Message de fin d'installation



Maintenant vous pouvez vous rendre dans la rubrique VPN -> OpenVPN pour constater que vous pouvez maintenant exporter la configuration

OpenVPN / Client Export Utility

[Serveur](#)
[Client](#)
[Ré-écritures spécifiques au client](#)
[Assistants](#)
[Client Export](#)
[Shared Key Export](#)

Serveur OpenVPN

Remote Access Server: Configuration VPN Distant UDP4:1194

Client Connection Behavior

Host Name Resolution: Interface IP Address

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 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.

Dans les options avancées ajoutez la suppression du cache puis valider la configuration

Certificate Export Options

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

Microsoft Certificate Storage: ☐ Use Microsoft Certificate Storage instead of local files.

Password Protect Certificate: ☐ Use a password to protect the pkcs12 file contents or key in Viscosity bundle.

Proxy Options

Use A Proxy: ☐ Use proxy to communicate with the OpenVPN server.

Avancé

Additional configuration options:

Enter any additional options to add to the OpenVPN client export configuration here, separated by a line break or semicolon.
EXAMPLE: remote-random;

[Save as default](#)

Vous disposez maintenant dans la rubrique tout en bas de l'option vous permettant d'exporter la configuration de l'utilisateur que vous avez créé

Clients OpenVPN		
Utilisateur	Nom du certificat	Export
wilfried.vpn	certificat-utilisateur-wm	<p>- Inline Configurations:</p> <p> Most Clients Android OpenVPN Connect (iOS/Android) </p> <p>- Bundled Configurations:</p> <p> Archive Config File Only </p> <p>- Current Windows Installers (2.5.8-1x04):</p> <p> 64-bit 32-bit </p> <p>- Legacy Windows Installers (2.4.12-1x01):</p> <p> 10/2016/2019 7/8/8.1/2012r2 </p> <p>- Viscosity (Mac OS X and Windows):</p> <p> Viscosity Bundle Viscosity Inline Config </p>

Etape 7 : Tester l'accès

Depuis votre poste installer le client puis tester la connexion sur la machine se trouvant dans le réseau configuré