

TP-VPN



SOMMAIRE

- Contexte
- Création vpn
- Création utilisateurs
- openvpn
- Installation du pack
- Configuration vpn
- Test

CONTEXTE

- **Qu'es qu'un vpn:** VPN: « Virtual Private Network » ca permet d'établir une connexion de manière sécurisé entre des ordinateurs distants connectés a des réseaux différents
- **Réalisation :** nous allons utiliser le logiciel pfsense pour effectuer un Access vpn

CREATION VPN

Descriptive name

Method

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.

Randomize Serial Use random serial numbers when signing certificates
When enabled, if this CA is capable of signing certificates the serial numbers will be automatically randomized and checked for uniqueness inside the CA.

Internal Certificate Authority

Key type

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 not support it.

Digest Algorithm
The digest method used when the CA is signed.
The best practice is to use an algorithm stronger than SHA1.
invalid

Lifetime (days)

Common Name

- pour effectuer un vpn nous allons dans un premier temps créer une autorisation de certification ce qui va nous permettre d'avoir une autorisation, pour ce faire nous allons nous rendre dans **system > Cert Manager > CAs** nous allons cliquer sur ajouter
- nous allons ajouter un nom dans **descriptive name** laissez la méthode par défaut ajouter un common name
- Ce qui nous donnera :

Certificate Authorities						
Name	Internal	Issuer	Certificates	Distinguished Name	In Use	Actions
romain-lheureux-vpn	✓	self-signed	0	CN=romain-lheureux  Valid From: Wed, 20 Nov 2024 08:07:25 +0000 Valid Until: Sat, 18 Nov 2034 08:07:25 +0000		    

CREATION VPN

Method Create an internal Certificate

Descriptive name VPN-SSL-REMOTE-ACCESS

Internal Certificate

Certificate authority remain-lheureux-vpn

Certificate Type Server Certificate

Add type-specific usage attributes to the signed certificate. Use the signed certificate

webConfigurator default (673d904059776) Server Certificate CA: No Server: Yes	self-signed	O=pfSense webConfigurator Self-Signed Certificate, CN=pfSense-673d904059776 Valid From: Wed, 20 Nov 2024 07:31:12 +0000 Valid Until: Tue, 23 Dec 2025 07:31:12 +0000	webConfigurator
VPN-SSL-REMOTE-ACCESS Server Certificate CA: No Server: Yes	remain-lheureux-vpn	CN=romain-lheureux Valid From: Wed, 20 Nov 2024 08:21:53 +0000 Valid Until: Sat, 18 Nov 2034 08:21:53 +0000	

- ensuite un fois l'autorisation effectuer nous allons créer un certificat pour cela nous allons nous diriger dans system > certificate manager > certificates > edit
- il est important de choisir server certificate

CREATIONS DES UTILISATEURS

Certificate Click to create a user certificate

Create Certificate for User

Descriptive name

Certificate authority

- Pour créer des utilisateurs nous allons nous rendre dans **system > user manager**
- Pour la création des utilisateurs nous allons cocher la case **certificate**; ce qui va être important pour télécharger le fichier pour la connexion vpn, Pour créer le certificat, on se base sur notre autorité de certification.

OPENVPN

Mode Configuration

Server mode Remote Access (SSL/TLS + User Auth)

Backend for authentication Local Database

Automatically generate a TLS Key.

Peer Certificate Authority romain-lheureux-vpn

Peer Certificate Revocation list No Certificate Revocation Lists defined. One may be created here: [System > Cert. M](#)

OCSP Check Check client certificates with OCSP

Server certificate VPN-SSL-REMOTE-ACCESS (Server: Yes, CA: romain-l...

Tunnel Settings

IPv4 Tunnel Network 10.10.10.0/24

IPv6 Tunnel Network

Redirect IPv4 Gateway Force all client-generated IPv4 traffic through the tunnel.

Redirect IPv6 Gateway Force all client-generated IPv6 traffic through the tunnel.

IPv4 Local network(s) 192.168.1.0/24

IPv6 Local network(s)

Concurrent connections 10

- Maintenant nous allons procéder a la configuration du VPN pour se faire nous allons nous rendre dans **vpn > OpenVPN > servers**
- **Dans le ip local network:** nous allons indiquer l'adresse reseau du lan
- indiquez : **auth-nocache**. Cette option offre une protection supplémentaire contre le vol des identifiants en refusant la mise en cache.

Advanced Configuration

Custom options

auth-nocache

INSTALLATION DU PACK

OpenVPN / Client Export Utility

Server Client Client Specific Overrides Wizards Client Export

OpenVPN Server

Remote Access Server: Server UDP4:1194

Client Connection Behavior

Host Name Resolution: **Interface IP Address**

Verify Server CN: Automatic - Use verify-x509-name where possible

Block Outside DNS: Block access to DNS servers except across OpenVPN while connected, forcing clients to use only VPN DNS servers. Requires Windows 10 and OpenVPN 2.3.9 or later. Only Windows 10 is prone to DNS leakage in this way, other clients will ignore the option as they are not affected.

- Inline Configurations:

- Most Clients
- Android
- OpenVPN Connect (iOS/Android)

- Bundled Configurations:

- Archive**
- Config File Only

- Current Windows Installers (2.6.7-1x001):

- 64-bit
- 32-bit

- Previous Windows Installers (2.5.9-1x601):

- 64-bit
- 32-bit

- Legacy Windows Installers (2.4.12-1x601):

- 10/2016/2019
- 7/8/8.1/2012:2

- Viscosity (Mac OS X and Windows):

- Viscosity Bundle
- Viscosity Inline Config

- Nous allons maintenant procéder à l'installation du paquet qui va nous permettre de nous connecter au VPN avec une machine cliente pour ce faire nous allons nous rendre dans **System > package manager > installed packages** afin d'installer le paquet OpenVPN
- Dans **OpenVPN > client export Utility** utiliser l'adresse IP publique pour vous connecter, utilisez l'option "**Interface IP Address**" pour l'option "Host Name Résolution" ensuite nous allons télécharger le paquet d'installation pour l'utilisateur créé précédemment

CONFIGURATION VPN

Firewall / Rules / Edit

Edit Firewall Rule

Action
 Choose what to do with packets that match the criteria specified below.
 Hint: the difference between block and reject is that with reject, a packet returned to the sender, whereas with block the packet is dropped silently.

Disabled Disable this rule
 Set this option to disable this rule without removing it from the list.

Interface
 Choose the interface from which packets must come to match this rule.

Address Family
 Select the Internet Protocol version this rule applies to.

Protocol

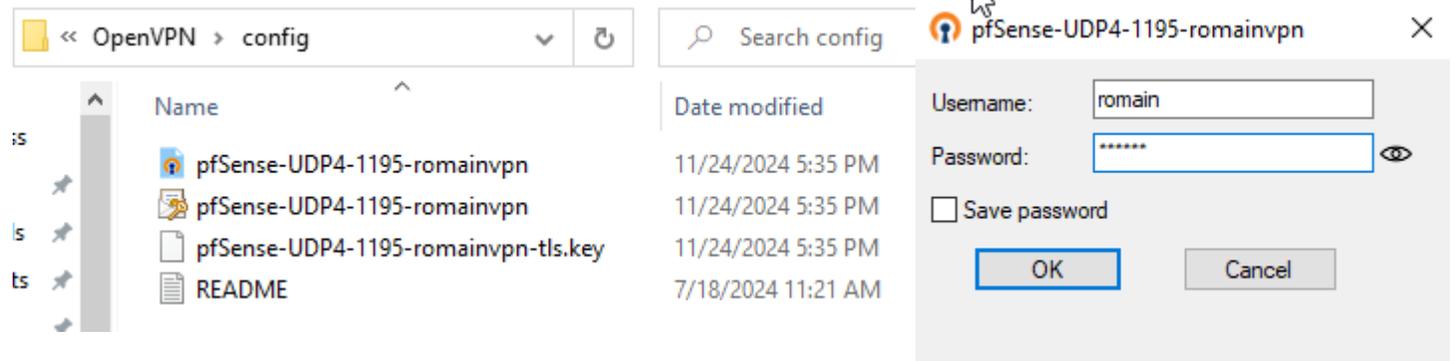
Destination Invert match

Destination Port Range
 From Custom To
 Specify the destination port or port range for this rule. The "To" field may be left empty if only filtering a single port.

Destination Invert match
 /
 (other) Custom (other) Custom
 From Custom To Custom
 Specify the destination port or port range for this rule. The "To" field may be left empty if only filtering a single port.

- nous devons créer une règle pour autoriser les clients à monter la connexion VPN, et d'autre part nous devons créer une ou plusieurs règles pour autoriser l'accès aux ressources : serveur en RDP, serveur de fichiers, application web, etc.
- Pour se faire nous allons nous rendre dans firewall > rules > edit
- La destination ce sera notre adresse IP publique donc sélectionnez "WAN address".
- Nous allons indiquer sur quelle machine le vpn doit être ici : 192,168,1,3 et le port 3389 qui correspond au port rdp

TEST



- Une fois la configuration effectuer nous allons faire le teste sur une machine client
- Dans un premier temps nous allons installer openvpn
- Ensuite le fichier installer précédemment depuis le pfsense qui contient la configuration nous allons le définir dans « C:\Programmes\OpenVPN\Config »
- Ensuite il nous reste plus qu'a installer openvpn et rentre les identifiant de l'utilisateur ce qui nous donne

