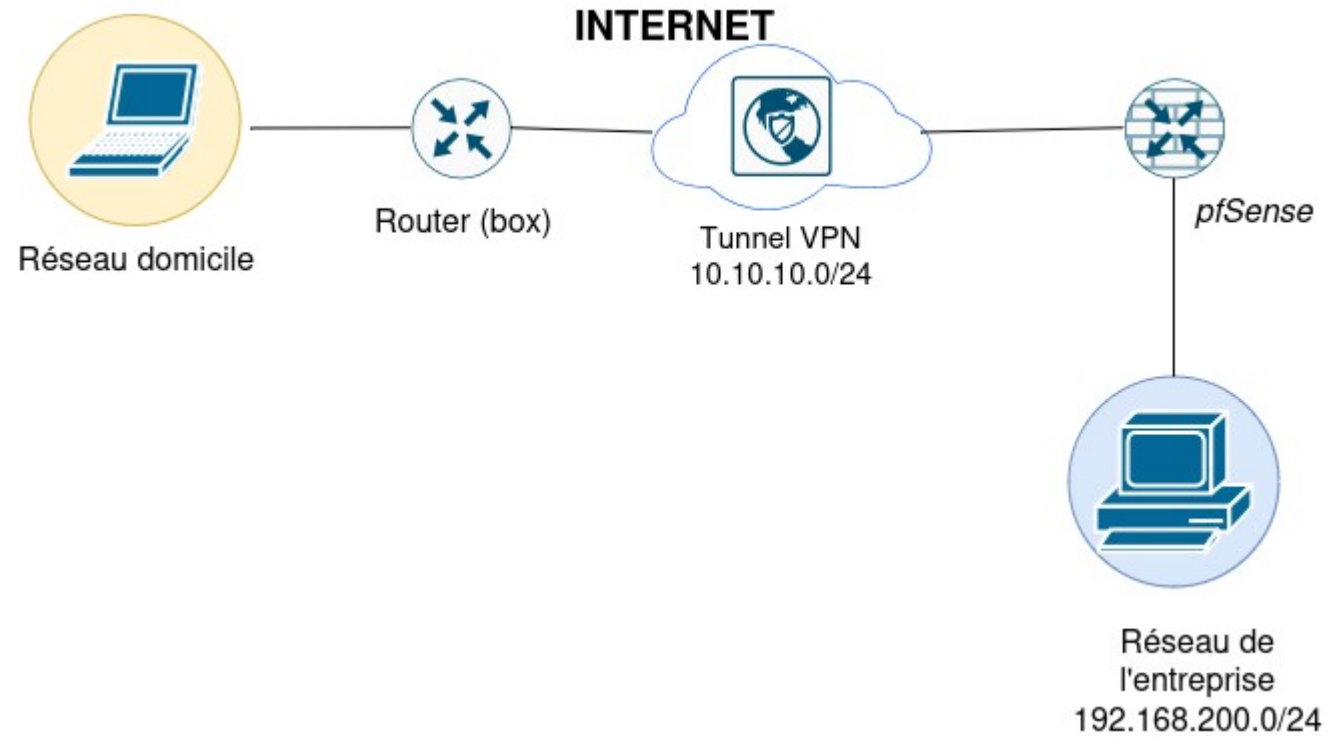




VPN

THOMAS GRZESINSKI

Schéma réseau



C'est quoi un VPN

VPN signifie « Virtual Private Network » décrit la possibilité d'établir une connexion réseau protégée lors de l'utilisation de réseaux publics. Les VPN chiffrent votre trafic Internet et camouflent votre identité en ligne . Il est ainsi plus difficile pour des tiers de suivre les activités

Mise en place du VPN

Nous allons mettre en place un VPN sur notre pfSense pour que nos développeur puissent accéder facilement a notre réseau

Configuration :

Nous allons d'abord créer une autorité de certification Pfsense :

- Pour faire cela aller dans le menu System → Certificate → Autorites->créer une autorisation de certificat

Active

Certificate Authorities						
Name	Internal	Issuer	Certificates	Distinguished Name	In Use	Actions
CA-Thomasg	✓	self-signed	2	CN=thomasg Valid From: Wed, 20 Nov 2024 20:36:10 +0100 Valid Until: Sat, 18 Nov 2034 20:36:10 +0100		

Mise en place du VPN

- Une fois le certificat établit nous allons maintenant établir un certificat pour notre serveur:

- System → Certificate → Certificates

Add/Sign a New Certificate

Method:

Descriptive name:
The name of this entry as displayed in the GUI for references.
This name can contain spaces but it cannot contain any of the following characters: !, *, <, >, /, \, ;

Internal Certificate

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 consider the certificate invalid.

Digest Algorithm:
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.

Lifetime (days):
The length of time the signed certificate will be valid in days.
Server certificates should not have a lifetime over 365 days or some platforms may consider the certificate invalid.

Common Name:
The following certificate subject components are optional and may be left blank.

Country Code:

State or Province:

City:

Organization:

Organizational Unit:

Certificate Type:
Add type-specific usage attributes to the signed certificate. Used for placing usage restrictions on, or granting abilities to, the signed certificate.

Alternative Names	Type	Value
<input type="text" value=""/>	<input type="text" value=""/>	<input type="text" value=""/>

Enter additional identifiers for the certificate in this list. The Common Name field is automatically added to the certificate as an Alternative Name. The signing CA may ignore or change these values.

Mise en place du VPN

- Normalement quand le certificat est correctement créer comme si dessous

webConfigurator default (66f11953090c4) Server Certificate CA: No Server: Yes	self-signed	O=pfSense webConfigurator Self-Signed Certificate, CN=pfSense-66f11953090c4 Valid From: Wed, 20 Nov 2024 20:26:14 +0100 Valid Until: Tue, 23 Dec 2025 20:26:14 +0100	webConfigurator
Certificat-OPENVPN Server Certificate CA: No Server: Yes	CA-Thomasg	CN=thomasg-fwwall Valid From: Wed, 20 Nov 2024 20:37:07 +0100 Valid Until: Sat, 18 Nov 2024 20:37:07 +0100	OpenVPN Server

- Il va vous falloir ensuite créer un utilisateur dans System → User manager → Créer un utilisateur

User Properties

Defined by: USER

Disabled: This user cannot login

Username: vpn.thomasg

Password: [masked]

Full name: [empty]

Expiration date: [empty]

Custom Settings: Use individual customized GUI options and dashboard layout for this user.

Group membership: admins

Certificate: Click to create a user certificate

Il ne faut surtout pas oublier de cocher case « certificate » car celle-ci nous mettra de créer son certificat

Mise en place du VPN

- Créer alors son certificat

Create Certificate for User

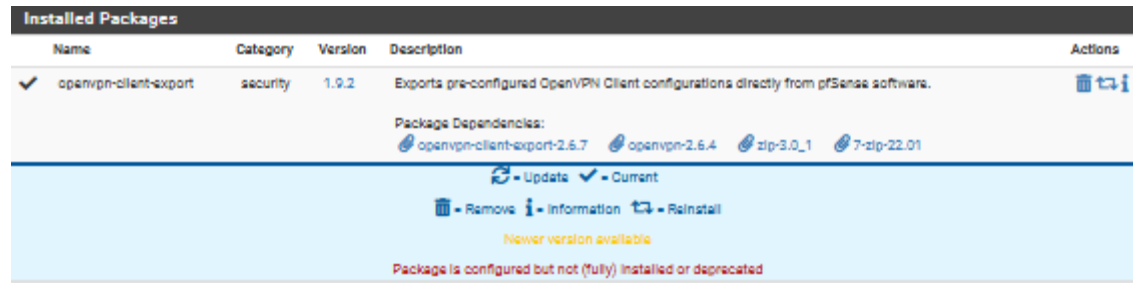
Descriptive name	Certificat-VPN-THOMASG
Certificate authority	CA-Thomasg
Key type	RSA
Key length	2048 <small>The length to use when generating a new RSA key, in bits. The Key Length should not be lower than 2048 or some platforms may consider the certificate invalid.</small>
Digest Algorithm	sha256 <small>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.</small>
Lifetime	3650

- Vérifier la création de certificat dans « System -> Certificates → Certificates »

Certificat-VPN-THOMASG User Certificate CA: No Server: No	CA-Thomasg	CN=vpn.thomasg Valid From: Wed, 20 Nov 2024 20:36:58 +0100 Valid Until: Sat, 18 Nov 2034 20:36:58 +0100	User Cert
--	------------	---	-----------

Mise en place du VPN

- Vous allez ensuite dans « System → Package Manager → Installed Packages » et installé le paquet « openvpn-client-export »



- Si vous avez des problèmes d'installations de paquets allez dans « Diagnostics → Command Prompt » et entrer les commandes suivantes qui permettront de mettre à jour les paquets pfSense :

```
certctl rehash  
pkg-static update -f  
pkg-static install -fy pkg pfSense-repo pfSense-upgrade
```

Mise en place du VPN

- Vous allez maintenant ensuite dans la section « VPN → OpenVPN → Servers → ajoutez » et on va appliquer la configuration

General Information	
Description	Accès distant OpenVPN <small>A description of this VPN for administrative reference.</small>
Disabled	<input type="checkbox"/> Disable this server <small>Set this option to disable this server without removing it from the list.</small>
Unique VPN ID	Server 1 (ovpn1)
Mode Configuration	
Server mode	Remote Access (SSL/TLS + User Auth)
Backend for authentication	Local Database
Device mode	tun - Layer 3 Tunnel Mode <small>"tun" mode carries IPv4 and IPv6 (OSI layer 3) and is the most common and compatible mode across all platforms. "tap" mode is capable of carrying 802.3 (OSI Layer 2.)</small>
Endpoint Configuration	
Protocol	UDP on IPv4 only
Interface	WAN <small>The Interface or Virtual IP address where OpenVPN will receive client connections.</small>
Local port	1194 <small>The port used by OpenVPN to receive client connections.</small>

Pour le server mode nous allons choisir « Remote Access (Ssl/TLS +User Auth) cela permet un accès distant par certificat et vérification

Il serait plus avantageux aussi de modifier le port pour des raisons de sécurité

Mise en place du VPN

The screenshot shows the 'Cryptographic Settings' page. The 'Use a TLS Key' checkbox is checked. The 'TLS Key' field contains a 2048-bit static key. The 'TLS Key Usage Mode' is set to 'TLS Authentication'. The 'TLS KeyDir Direction' is set to 'Use default direction'. The 'Peer Certificate Authority' is set to 'CA-Thomsg'. The 'Server certificate' is set to 'Certificate-OPENVPN (Server: Yes, CA: CA-Thomsg, In Use)'. The 'DH Parameter Length' is set to '2048 bit'. The 'ECDH Curve' is set to 'Use Default'. The 'Data Encryption Algorithms' list includes AES-128-CBC, AES-128-CFB, AES-128-CFB1, AES-128-CFB128, AES-128-GCM, AES-128-OCB, AES-192-CBC, and AES-192-CFB. The 'Active Window' is visible in the background.

- Vous devez donc choisir votre certificat

- Choisissez un protocole de chiffrement AES-256-CBC(256 bit key, 128 bit block). Cela permettra un meilleur chiffrement même si on a un risque de perte de latence comme le chiffrement est lourd

Mise en place du VPN

IPv4 Tunnel Network	<input type="text" value="10.10.10.0/24"/>
<small>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. 10.0.0.0/24). 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.</small>	
<small>A tunnel network of /30 or smaller puts OpenVPN into a special peer-to-peer mode which cannot push settings to clients. This mode is not compatible with several options, including Exit Notify, and Inactive.</small>	
IPv6 Tunnel Network	<input type="text"/>
<small>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.</small>	
Redirect IPv4 Gateway	<input type="checkbox"/> Force all client-generated IPv4 traffic through the tunnel.
Redirect IPv6 Gateway	<input type="checkbox"/> Force all client-generated IPv6 traffic through the tunnel.
IPv4 Local network(s)	<input type="text" value="192.168.200.0/24"/>
<small>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.</small>	
IPv6 Local network(s)	<input type="text"/>
<small>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.</small>	
Concurrent connections	<input type="text" value="10"/>
<small>Specify the maximum number of clients allowed to concurrently connect to this server.</small>	
Allow Compression	<input type="checkbox"/> Refuse any non-stub compression (Most secure)
<small>Allow compression to be used with this VPN instance. Compression can potentially increase throughput but may allow an attacker to extract secrets if they can control compressed plaintext traversing the VPN (e.g. HTTP). Before enabling compression, consult information about the VORACLE, CRIME, TIME, and BREACH attacks against TLS to decide if the use case for this specific VPN is vulnerable to attack.</small>	
<small>Asymmetric compression allows an easier transition when connecting with older peers.</small>	
Type-of-Service	<input type="checkbox"/> Set the TOS IP header value of tunnel packets to match the encapsulated packet value.
Inter-client communication	<input type="checkbox"/> Allow communication between clients connected to this server
Duplicate Connection	<input type="checkbox"/> Allow multiple concurrent connections from the same user
<small>When set, the same user may connect multiple times. When unset, a new connection from a user will disconnect the previous session.</small>	
<small>Users are identified by their username or certificate properties, depending on the VPN configuration. This practice is discouraged security reasons, but may be necessary in some environments.</small>	

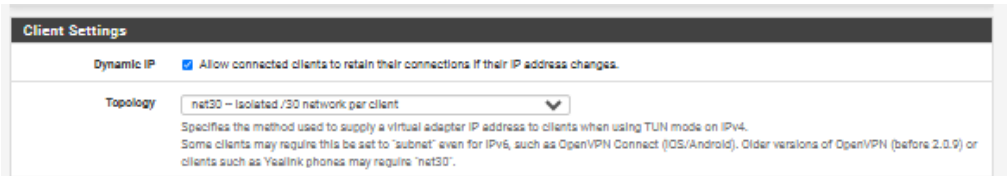
Active
Accédez

- Le IPV4 Tunnel Network est le réseau que l'on veut utiliser pour le tunnel VPN

- Le IPV4 Local Network sont donc les réseaux que l'on veut rendre accessible a travers le VPN

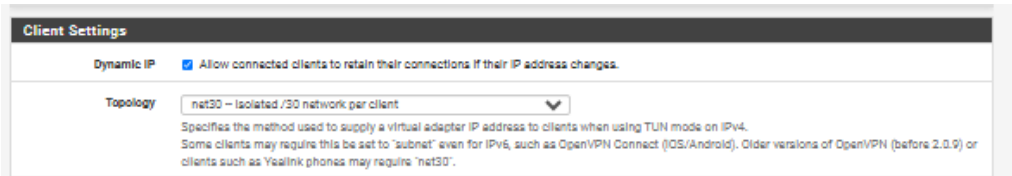
- Concurrent connections c'est le nombre de connexion maxium que l'on souhaite mettre en place

Mise en place du VPN



- Activer le Dynamic IP si vos utilisateurs se déplacent et connectent un peu partout permettra de maintenir la connexion VPN
- Activer le protocole net30 cette option permettra a chaque client de se situer dans un sous réseau isolé pour ne pas communiquer avec les autres pc en VPN

Mise en place du VPN



- Activer le Dynamic IP si vos utilisateurs se déplacent et connectent un peu partout permettra de maintenir la connexion VPN

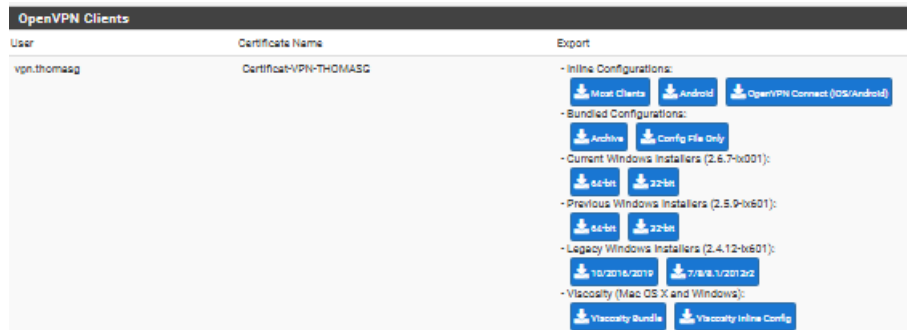
- Activer le protocole net30 cette option permettra a chaque client de se situer dans un sous réseau isolé pour ne pas communiquer avec les autres pc en VPN



- Ajouter l'option auth-nocache qui permettra d'empêcher la mise en de l'authentification et donc une fuite de ses authentifications

Exporter la configuration VPN

- Pour exporter la configuration aller dans VPN → OpenVPN → client export
- Mettez en Host Name Resolution « Interface IP address »
- Cochez legacy client pour que les utilisateurs possédant une version antérieure de OPN puisse se connecter
- Save as default
- Télécharger la version archive pour exporter la configs et les logs VPN pour le USER



Modifier les règles de par-feu

- Modifier les règles de par-feu pour autoriser la connexion VPN

Configuration :

- Firewall → Rules → Wan - > Ajouter une règle

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 (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.

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
 Choose which IP protocol this rule should match.

Source

Invert match

The Source Port Range for a connection is typically random and almost never equal to the destination port. In most cases this setting must remain at its default value, any.

Destination

Invert match

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

Extra Options

Log **Log packets that are handled by this rule**
 Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the Status: System Logs: Settings page).

Description
 A description may be entered here for administrative reference. A maximum of 52 characters will be used in the rule set and displayed in the firewall log.

Ajouter une deuxième règle

- Ajouter une autre règle dans Firewall → Rules → OpenVPN pour accéder aux ressources internes de l'entreprises

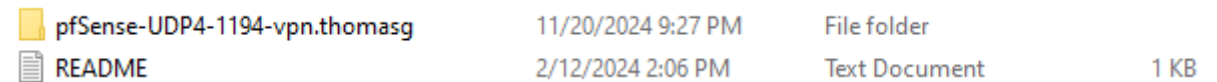
The screenshot shows the 'Edit Firewall Rule' configuration window in Mikrotik WinBox. The rule is named 'OpenVPN' and is currently disabled. The configuration is as follows:

- Action:** Pass
- Disabled:** Disable this rule
- Interface:** OpenVPN
- Address Family:** IPv4
- Protocol:** TCP
- Source:** Invert match, Source Address: any
- Destination:** Invert match, Destination: 192.168.200.0
- Destination Port Range:** MS RDP (3389) to MS RDP (3389)
- Extra Options:** Log packets that are handled by this rule
- Description:** Autoriser le RDP vers PC Windows 10

A watermark 'Active Accédez Window' is visible on the right side of the screenshot.

Ajouter une deuxième règle

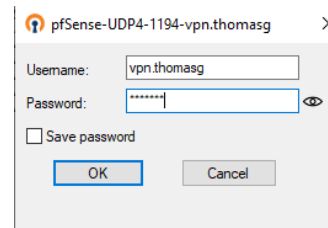
- Installer OpenVPN sur votre machine cliente
- Exporter le fichier de configuration dans `C:\Program Files \OpenVPN\config`



- Maintenant cliquer sur cette icône-ci dans votre barre des tâches



- Entrer les logs et mot de passe du User



Si vous êtes correctement connecté votre icône précédente deviendra verte



- Faites un `ipconfig /all` et l'adresse de passerelle apparaîtra `IPv4 Address. : 10.10.10.6(Preferred)`