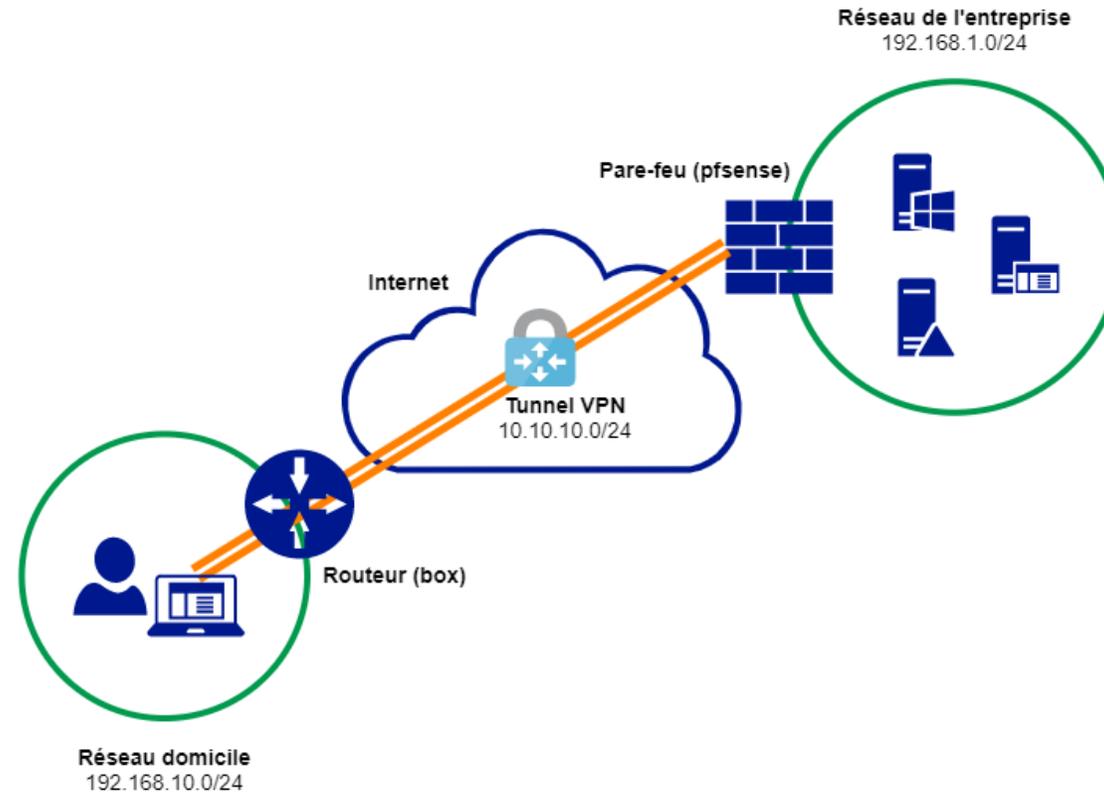




# Mise en place d'un VPN sous PfSense

# Architecture réseau à reproduire variant selon les IP

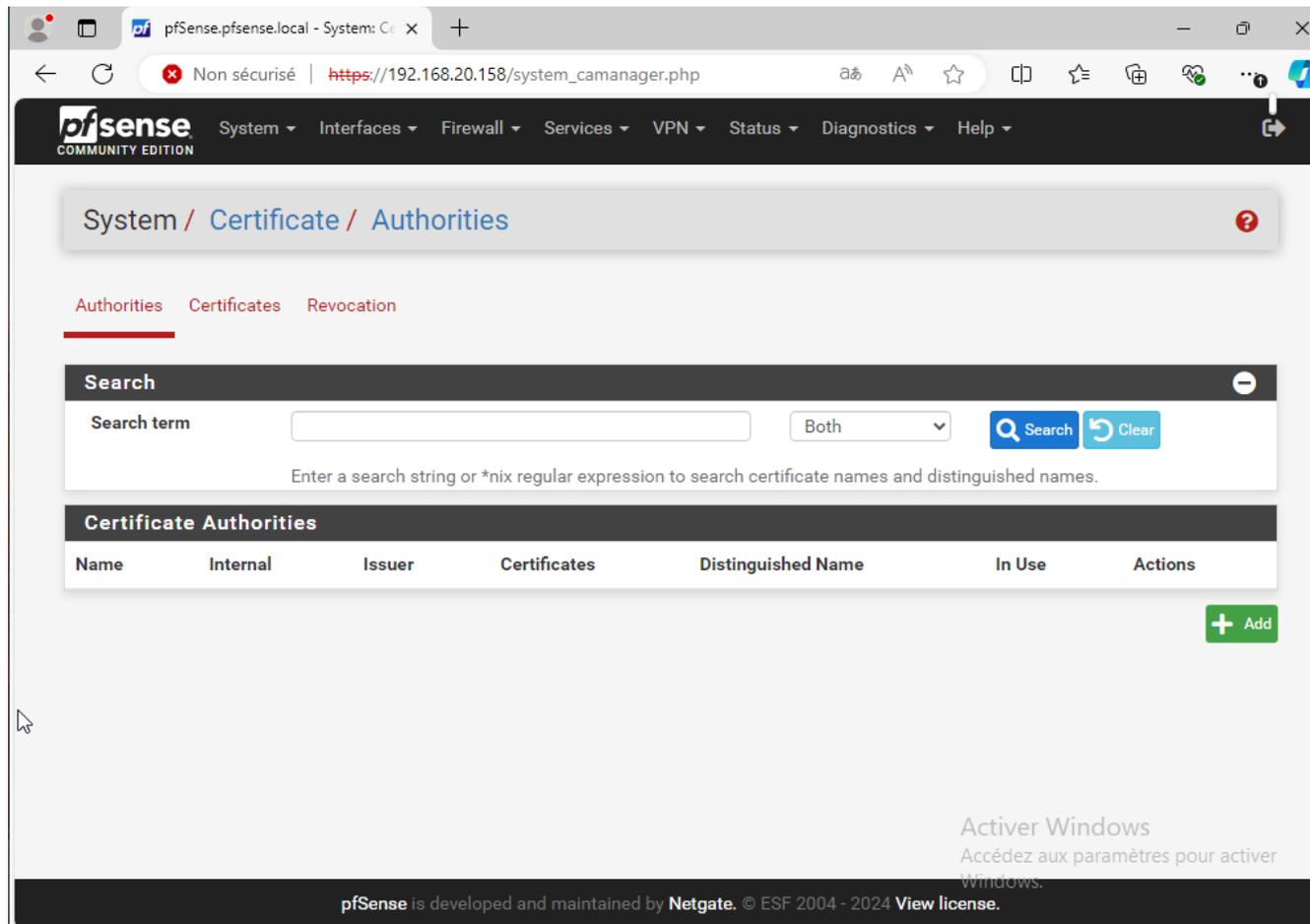




# La gestion des certificats

# Créer l'autorité de certification

- Cliquez sur Add



pfSense COMMUNITY EDITION

System / Certificate / Authorities

Authorities Certificates Revocation

**Search**

Search term  Both

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

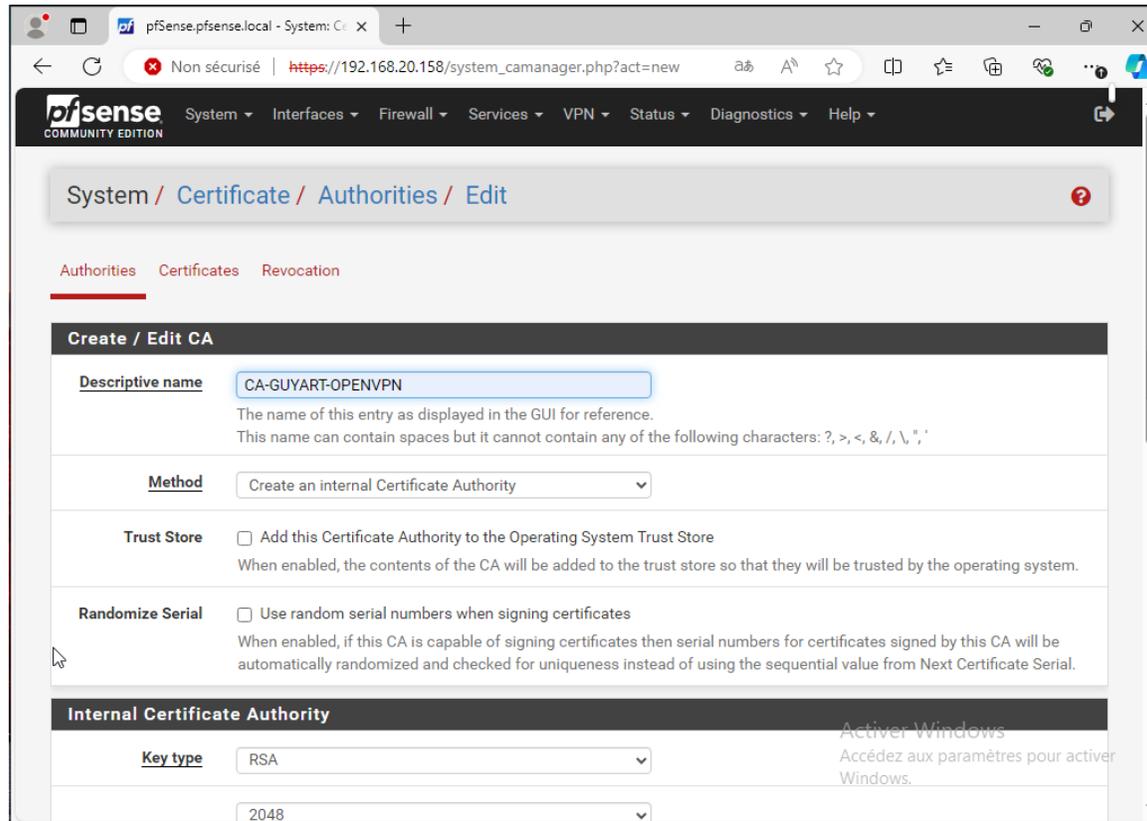
**Certificate Authorities**

Name	Internal	Issuer	Certificates	Distinguished Name	In Use	Actions
------	----------	--------	--------------	--------------------	--------	---------

Activer Windows  
Accédez aux paramètres pour activer Windows.

pfSense is developed and maintained by Netgate. © ESF 2004 - 2024 [View license.](#)

# Configurez comme ici



pfSense COMMUNITY EDITION

System / Certificate / Authorities / Edit

Authorities Certificates Revocation

### Create / Edit CA

**Descriptive name**   
The name of this entry as displayed in the GUI for reference.  
This name can contain spaces but it cannot contain any of the following characters: ?, >, <, &, /, \, ", '.

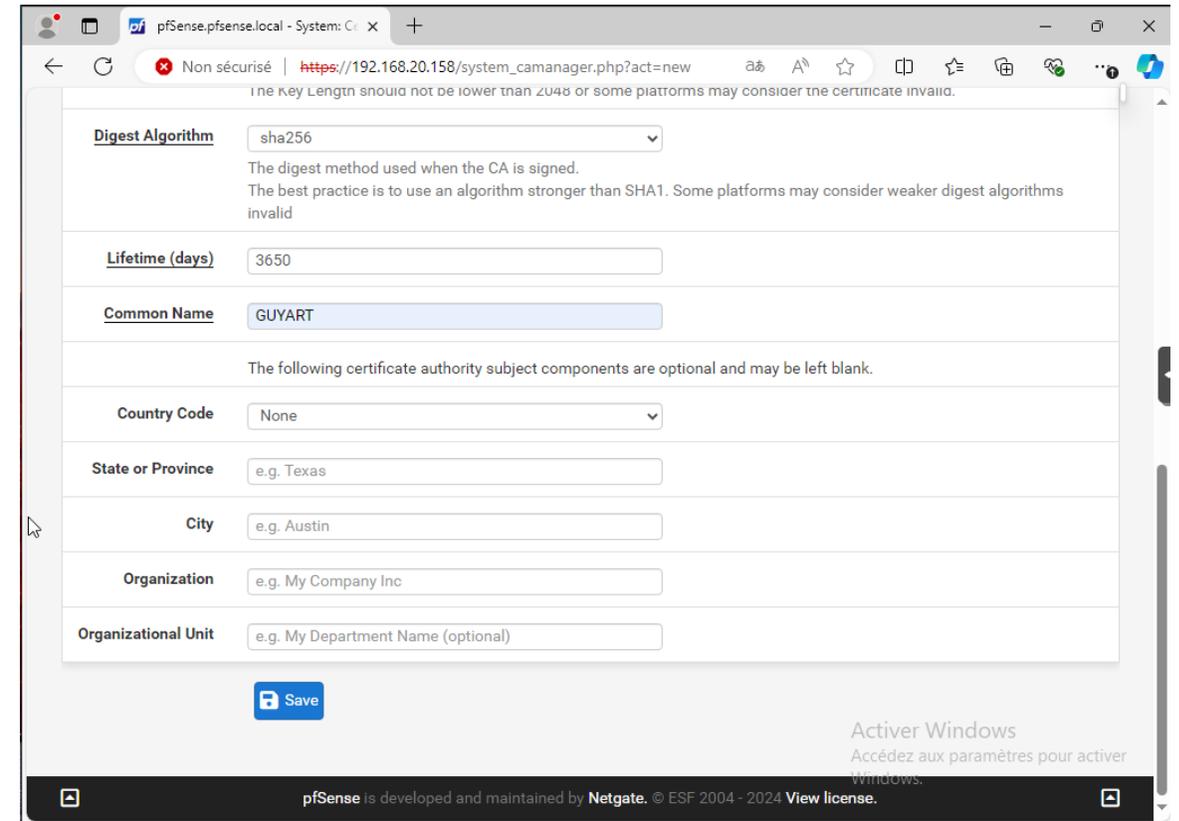
**Method**

**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 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.

### Internal Certificate Authority

**Key type**



pfSense COMMUNITY EDITION

System / Certificate / Authorities / Edit

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 CA is signed.  
The best practice is to use an algorithm stronger than SHA1. Some platforms may consider weaker digest algorithms invalid.

**Lifetime (days)**

**Common Name**

The following certificate authority subject components are optional and may be left blank.

**Country Code**

**State or Province**

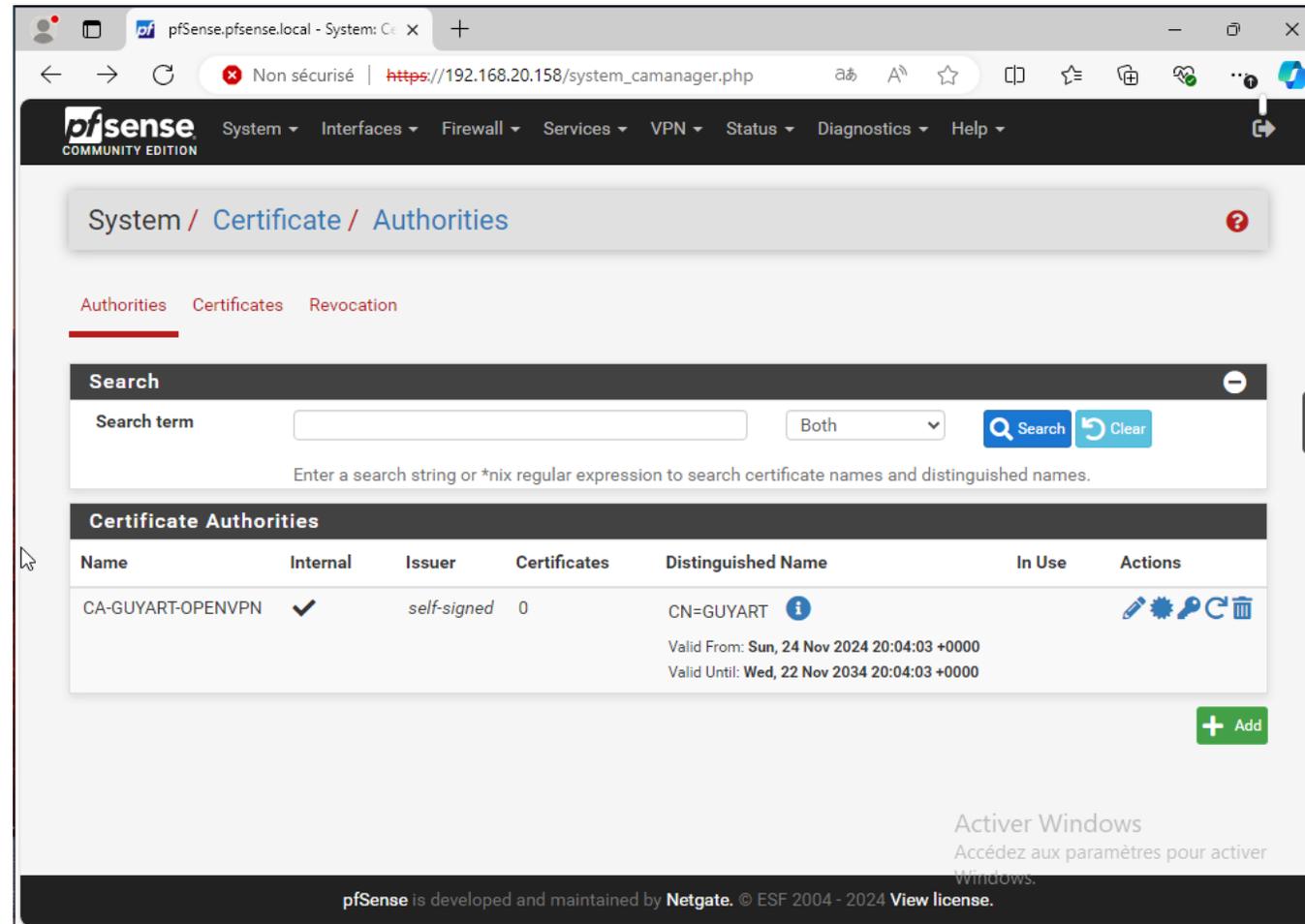
**City**

**Organization**

**Organizational Unit**

pfSense is developed and maintained by Netgate. © ESF 2004 - 2024 View license.

# Le voilà créé



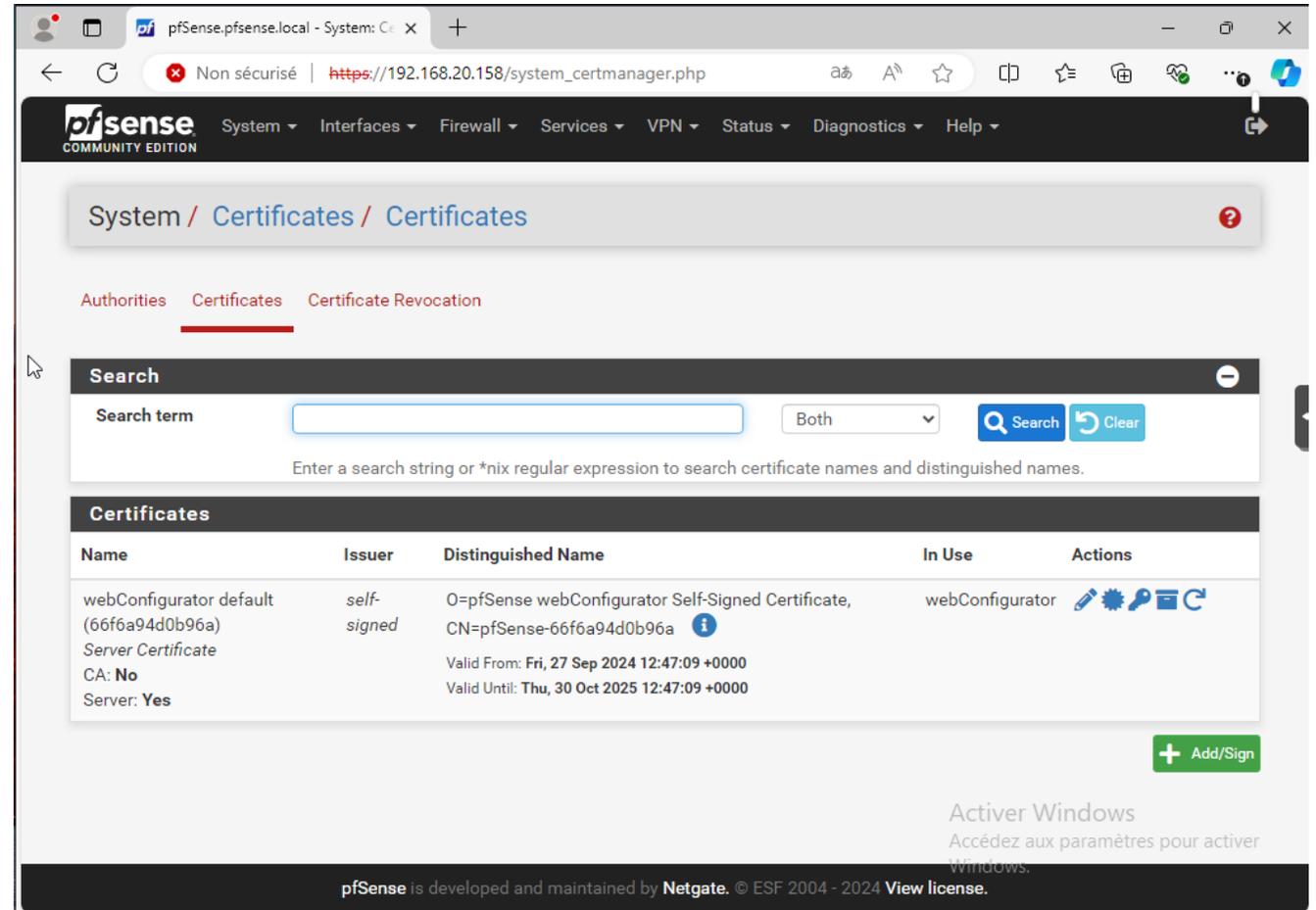
The screenshot shows the pfSense web interface for managing Certificate Authorities. The breadcrumb trail is System / Certificate / Authorities. The 'Authorities' tab is selected. A search bar is present with a search term field, a dropdown menu set to 'Both', and 'Search' and 'Clear' buttons. Below the search bar is a table of Certificate Authorities.

Name	Internal	Issuer	Certificates	Distinguished Name	In Use	Actions
CA-GUYART-OPENVPN	✓	self-signed	0	CN=GUYART Valid From: Sun, 24 Nov 2024 20:04:03 +0000 Valid Until: Wed, 22 Nov 2034 20:04:03 +0000		    

A green '+ Add' button is located at the bottom right of the table. The footer of the interface includes the text: 'pfSense is developed and maintained by Netgate. © ESF 2004 - 2024 View license.'

# Créer le certificat Server

- Cliquez sur Add/Sign



System / Certificates / Certificates

Authorities Certificates Certificate Revocation

Search

Search term  Both

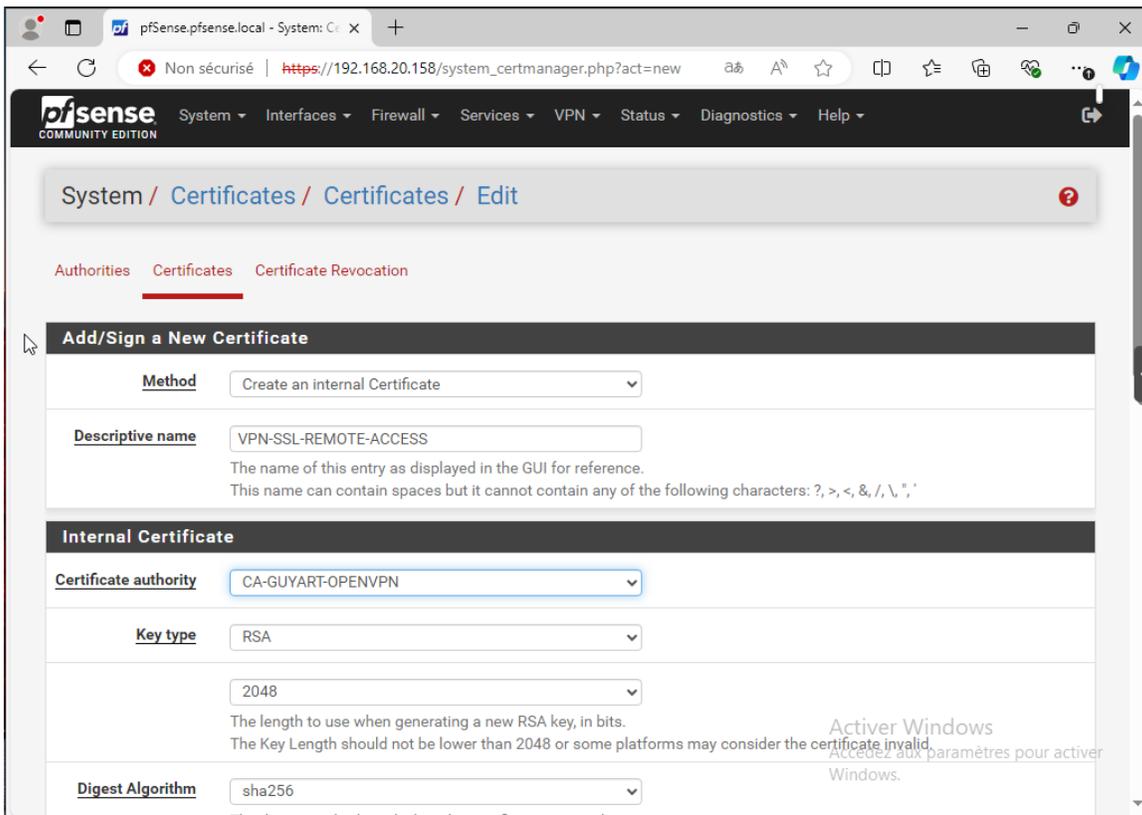
Enter a search string or \*nix regular expression to search certificate names and distinguished names.

Name	Issuer	Distinguished Name	In Use	Actions
webConfigurator default (66f6a94d0b96a) Server Certificate CA: No Server: Yes	self-signed	O=pfSense webConfigurator Self-Signed Certificate, CN=pfSense-66f6a94d0b96a Valid From: Fri, 27 Sep 2024 12:47:09 +0000 Valid Until: Thu, 30 Oct 2025 12:47:09 +0000	webConfigurator	  

pfSense is developed and maintained by Netgate. © ESF 2004 - 2024 View license.

Activer Windows  
Accédez aux paramètres pour activer Windows.

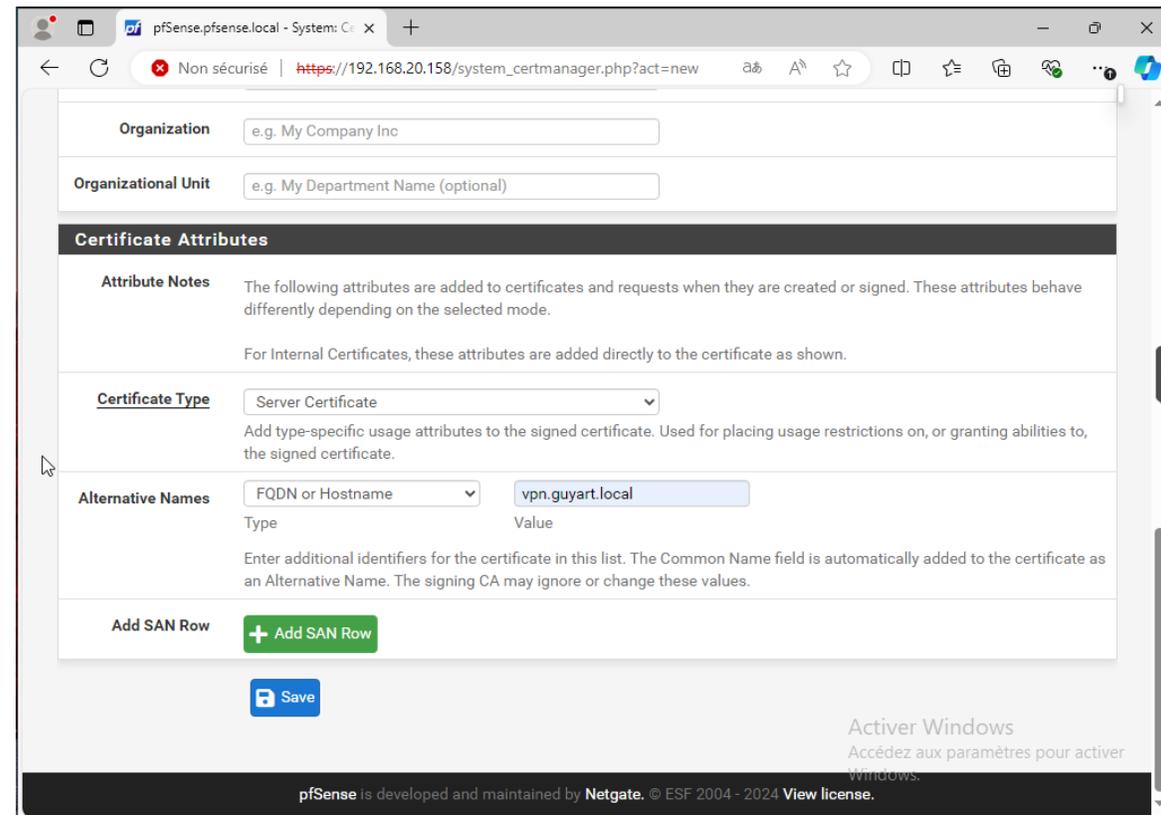
# Configurez comme ici



The screenshot shows the pfSense web interface for adding a new certificate. The browser address bar shows `https://192.168.20.158/system_certmanager.php?act=new`. The navigation menu includes System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, and Help. The breadcrumb trail is System / Certificates / Certificates / Edit. The main content area has tabs for Authorities, Certificates, and Certificate Revocation. The 'Add/Sign a New Certificate' section is active, showing the following configuration:

- Method:** Create an internal Certificate
- Descriptive name:** VPN-SSL-REMOTE-ACCESS
- Internal Certificate:**
  - Certificate authority:** CA-GUYART-OPENVPN
  - Key type:** RSA
  - Key length:** 2048
  - Digest Algorithm:** sha256

An 'Active Windows' watermark is visible at the bottom right of the screenshot.

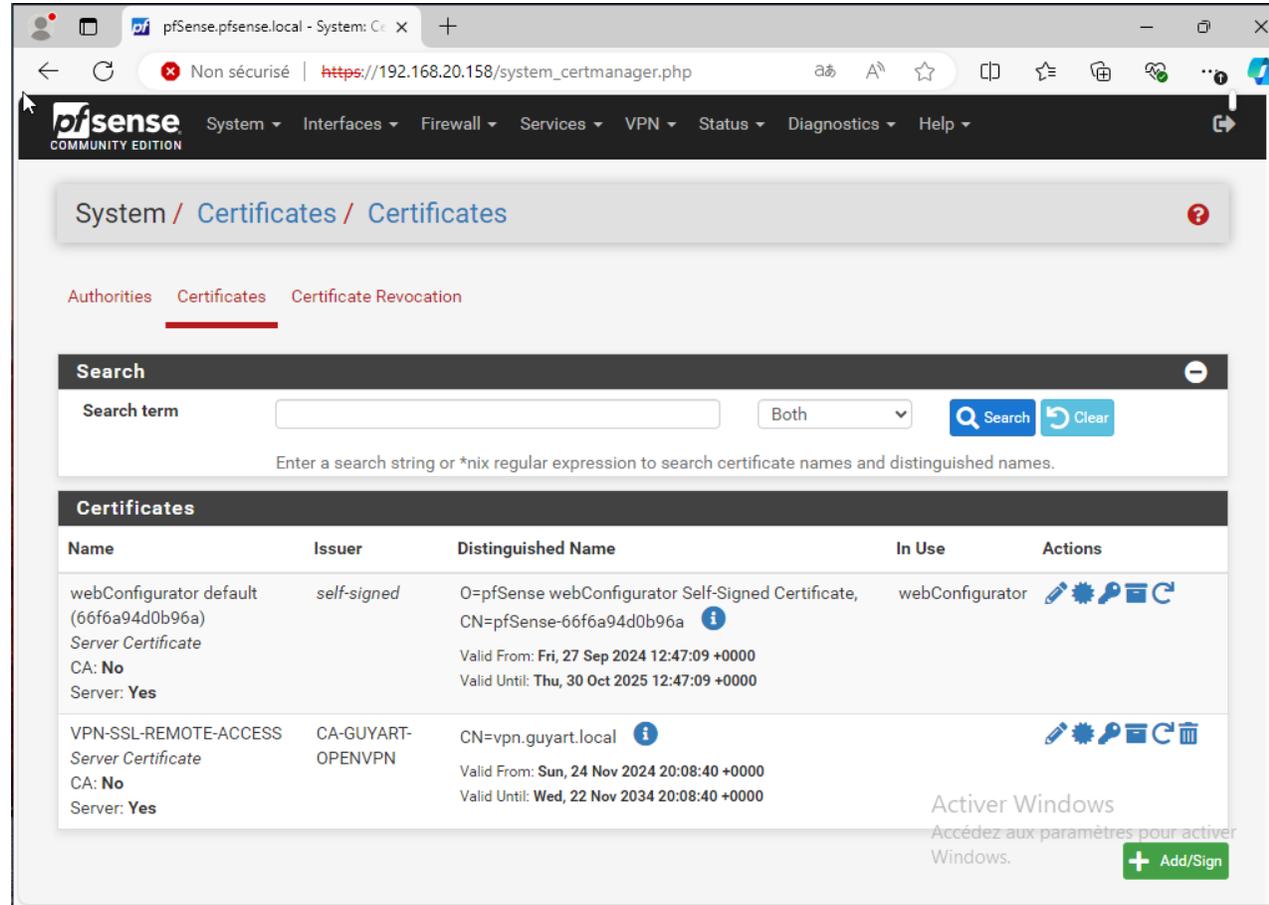


The screenshot shows the 'Certificate Attributes' section of the pfSense web interface. The browser address bar shows `https://192.168.20.158/system_certmanager.php?act=new`. The 'Certificate Attributes' section is active, showing the following configuration:

- Organization:** e.g. My Company Inc
- Organizational Unit:** e.g. My Department Name (optional)
- Certificate Attributes:**
  - Attribute Notes:** The following attributes are added to certificates and requests when they are created or signed. These attributes behave differently depending on the selected mode. For Internal Certificates, these attributes are added directly to the certificate as shown.
  - Certificate Type:** Server Certificate
  - Alternative Names:** FQDN or Hostname (Type) with value `vpn.guyart.local` (Value)

At the bottom, there is a '+ Add SAN Row' button and a 'Save' button. An 'Active Windows' watermark is visible at the bottom right of the screenshot.

# Le voilà créé



pfSense COMMUNITY EDITION

System / Certificates / Certificates

Authorities Certificates Certificate Revocation

**Search**

Search term  Both

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

**Certificates**

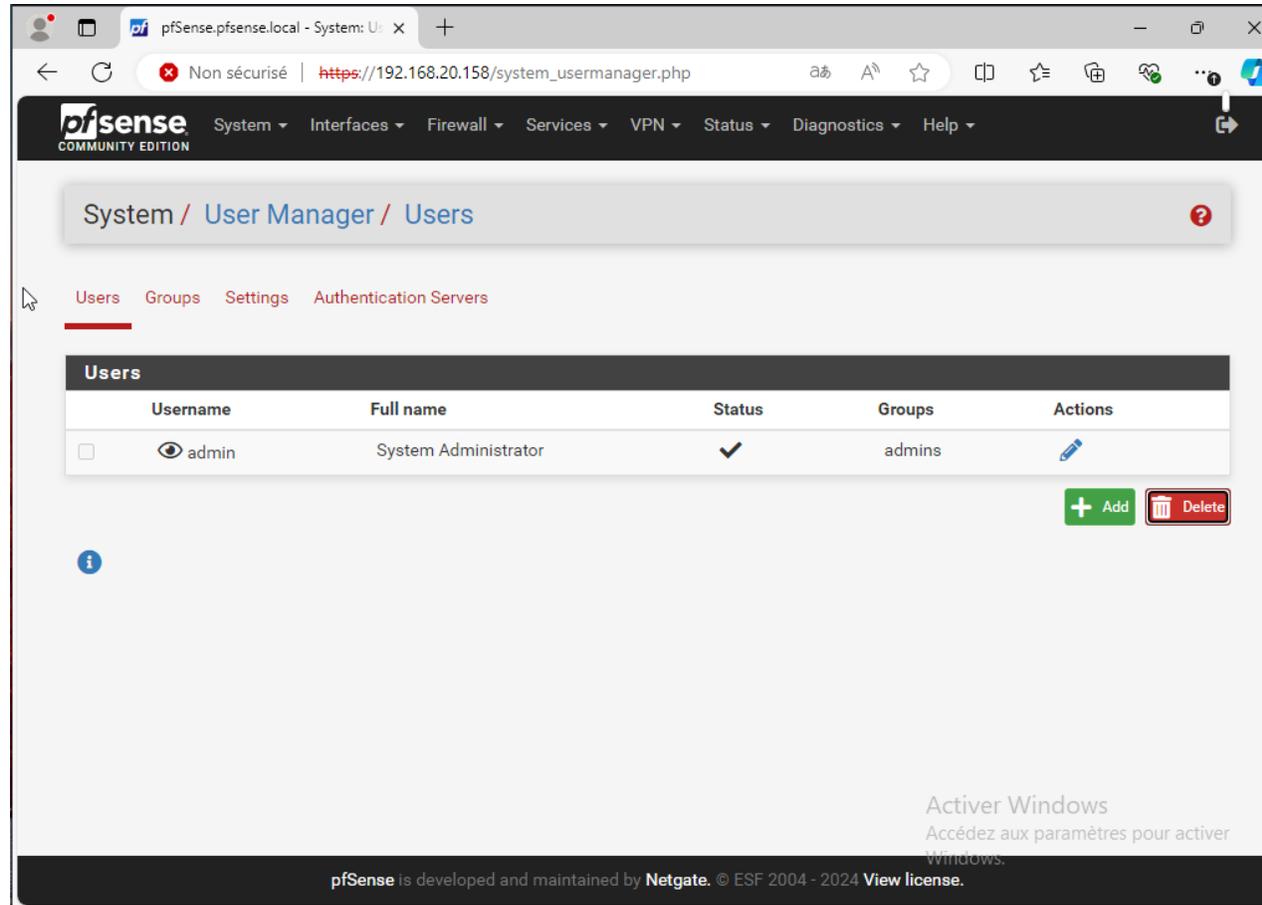
Name	Issuer	Distinguished Name	In Use	Actions
webConfigurator default (66f6a94d0b96a) Server Certificate CA: No Server: Yes	self-signed	O=pfSense webConfigurator Self-Signed Certificate, CN=pfSense-66f6a94d0b96a 	webConfigurator	   
VPN-SSL-REMOTE-ACCESS Server Certificate CA: No Server: Yes	CA-GUYART- OPENVPN	CN=vpn.guyart.local  Valid From: Sun, 24 Nov 2024 20:08:40 +0000 Valid Until: Wed, 22 Nov 2034 20:08:40 +0000		    

Activer Windows  
Accédez aux paramètres pour activer Windows.



# Créer l'utilisateur test du VPN

# Cliquez sur Add

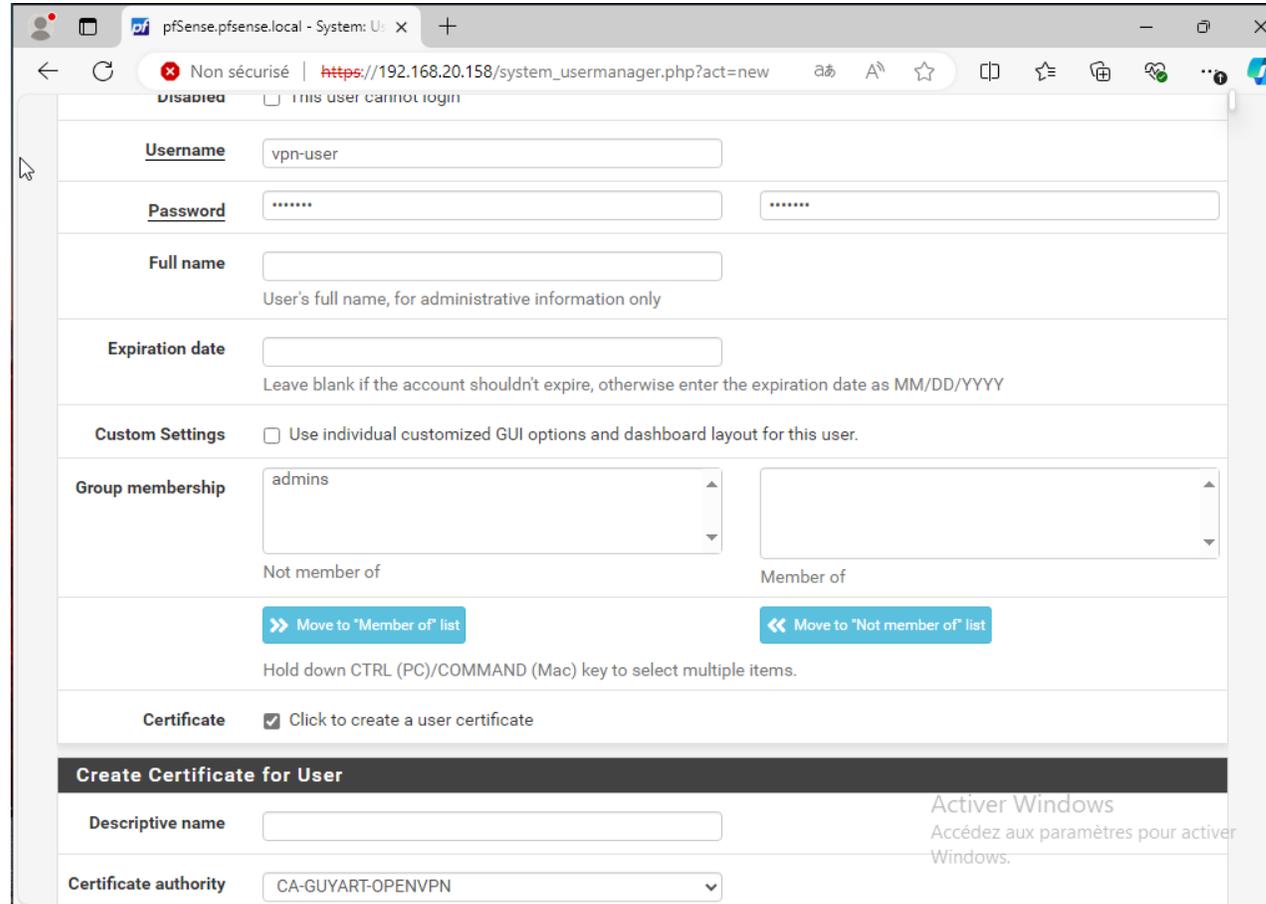


The screenshot shows the pfSense web interface for the User Manager Users page. The breadcrumb trail is "System / User Manager / Users". The main navigation menu includes "Users", "Groups", "Settings", and "Authentication Servers". The "Users" section contains a table with the following data:

	Username	Full name	Status	Groups	Actions
<input type="checkbox"/>	admin	System Administrator	✓	admins	

Below the table are two buttons: a green "+ Add" button and a red "Delete" button. At the bottom of the page, there is a footer that reads "pfSense is developed and maintained by Netgate. © ESF 2004 - 2024 View license." and a Windows activation notice.

# Cochez bien la case en bas puis configurez comme ici



The screenshot shows the pfSense system user manager interface for creating a new user. The browser address bar shows the URL `https://192.168.20.158/system_usermanager.php?act=new`. The user name is set to "vpn-user". The password field is masked with dots. The "Full name" field is empty, with a note that it is for administrative information only. The "Expiration date" field is empty, with a note to leave it blank if the account shouldn't expire. The "Custom Settings" section has a checkbox for "Use individual customized GUI options and dashboard layout for this user." which is unchecked. The "Group membership" section shows "admins" in the "Not member of" dropdown and an empty "Member of" dropdown. There are buttons to "Move to 'Member of' list" and "Move to 'Not member of' list". The "Certificate" section has a checked checkbox for "Click to create a user certificate". Below this is a section titled "Create Certificate for User" with a "Descriptive name" field and a "Certificate authority" dropdown set to "CA-GUYART-OPENVPN".

Non sécurisé | `https://192.168.20.158/system_usermanager.php?act=new`

**Disabled**  This user cannot login

**Username**

**Password**

**Full name**   
User's full name, for administrative information only

**Expiration date**   
Leave blank if the account shouldn't expire, otherwise enter the expiration date as MM/DD/YYYY

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

**Group membership**    
Not member of Member of

[Move to "Member of" list](#) [Move to "Not member of" list](#)

Hold down CTRL (PC)/COMMAND (Mac) key to select multiple items.

**Certificate**  Click to create a user certificate

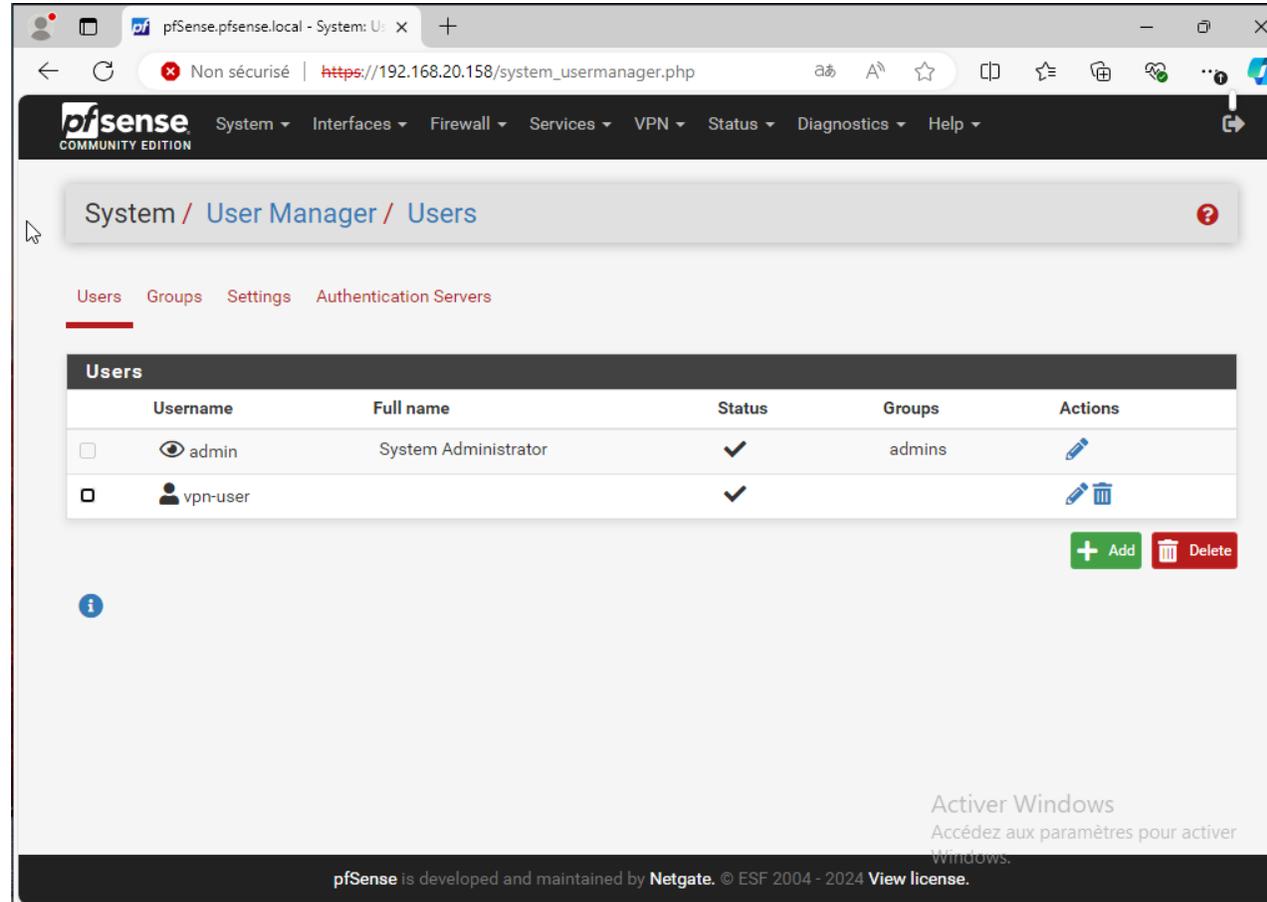
**Create Certificate for User**

**Descriptive name**

**Certificate authority**

Activer Windows  
Accédez aux paramètres pour activer Windows.

# Votre USER est créé



The screenshot shows the pfSense web interface for the User Manager Users page. The browser address bar indicates the URL is `https://192.168.20.158/system_usermanager.php`. The page title is "System / User Manager / Users". The navigation menu includes "Users", "Groups", "Settings", and "Authentication Servers". The "Users" section contains a table with the following data:

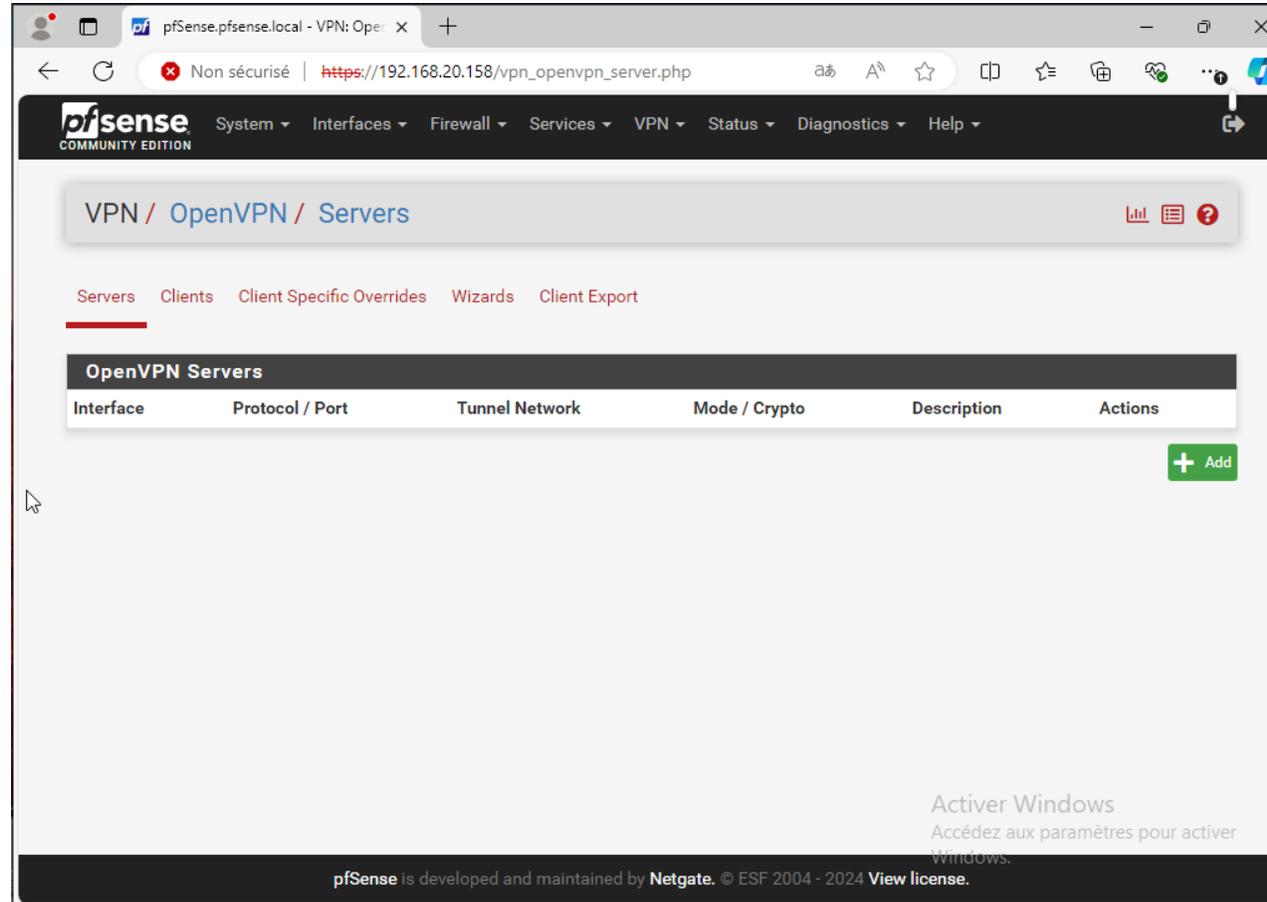
	Username	Full name	Status	Groups	Actions
<input type="checkbox"/>	admin	System Administrator	✓	admins	
<input type="checkbox"/>	vpn-user		✓		 

Below the table are buttons for "+ Add" and "Delete". At the bottom of the page, there is a footer: "pfSense is developed and maintained by Netgate. © ESF 2004 - 2024 View license." and a Windows watermark: "Activer Windows Accédez aux paramètres pour activer Windows."



# Configurer le serveur OpenVPN

# Cliquez sur Add



pfSense COMMUNITY EDITION

System ▾ Interfaces ▾ Firewall ▾ Services ▾ VPN ▾ Status ▾ Diagnostics ▾ Help ▾

VPN / OpenVPN / Servers

Servers Clients Client Specific Overrides Wizards Client Export

**OpenVPN Servers**

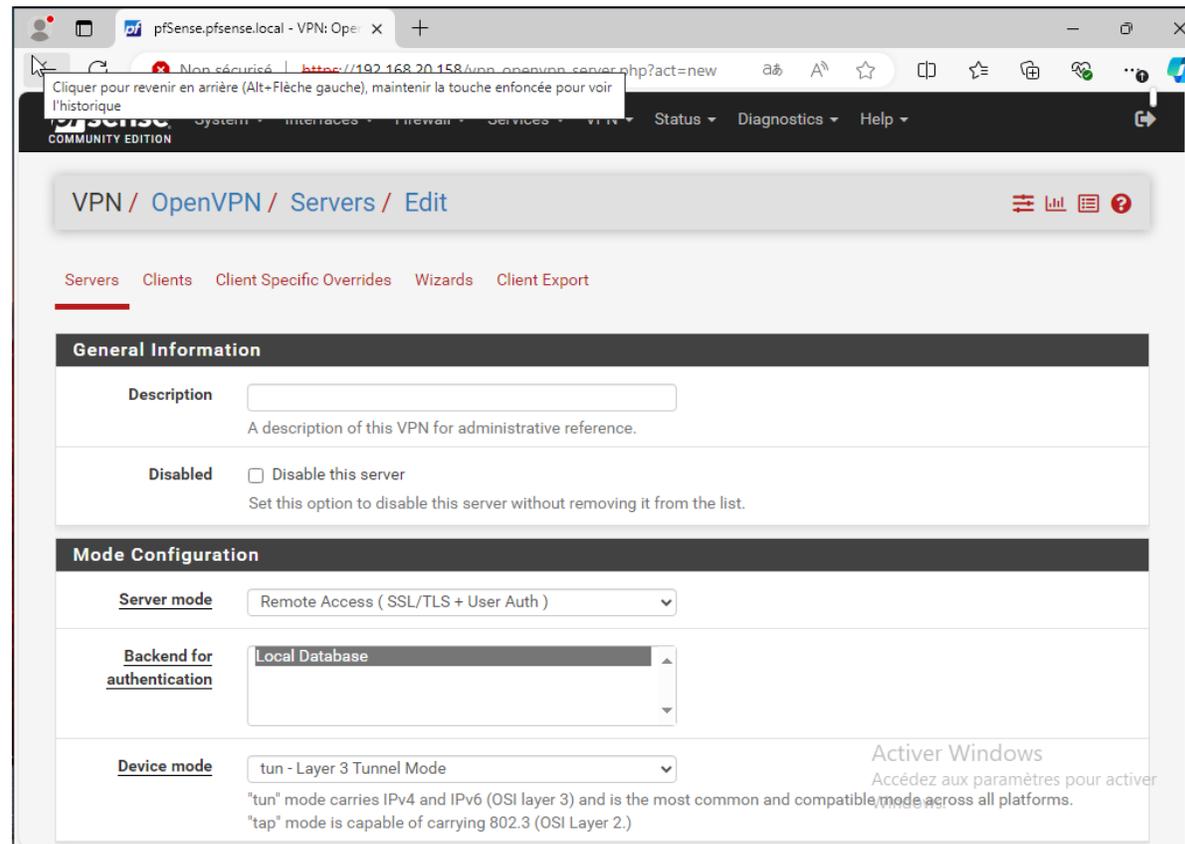
Interface	Protocol / Port	Tunnel Network	Mode / Crypto	Description	Actions
-----------	-----------------	----------------	---------------	-------------	---------

+ Add

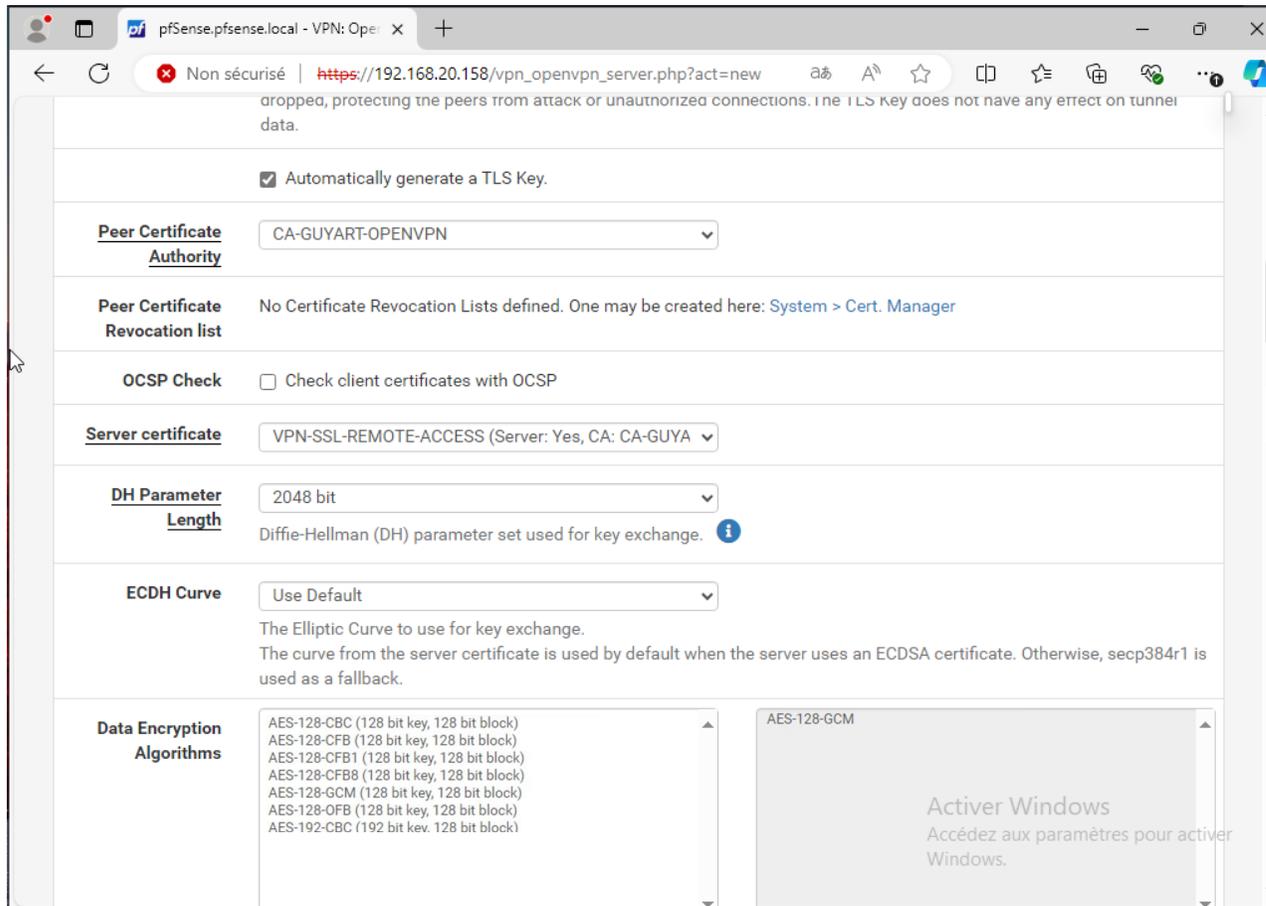
Activer Windows  
Accédez aux paramètres pour activer Windows.

pfSense is developed and maintained by Netgate. © ESF 2004 - 2024 [View license.](#)

# Choisir le "Server Mode" suivant : Remote Access (SSL/TLS + User Auth).



# Complétez tout comme il faut



Non sécurisé | [https://192.168.20.158/vpn\\_openvpn\\_server.php?act=new](https://192.168.20.158/vpn_openvpn_server.php?act=new)

dropped, protecting the peers from attack or unauthorized connections. The TLS key does not have any effect on tunnel data.

Automatically generate a TLS Key.

**Peer Certificate Authority**  
CA-GUYART-OPENVPN

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

**OCSP Check**  
 Check client certificates with OCSP

**Server certificate**  
VPN-SSL-REMOTE-ACCESS (Server: Yes, CA: CA-GUYA)

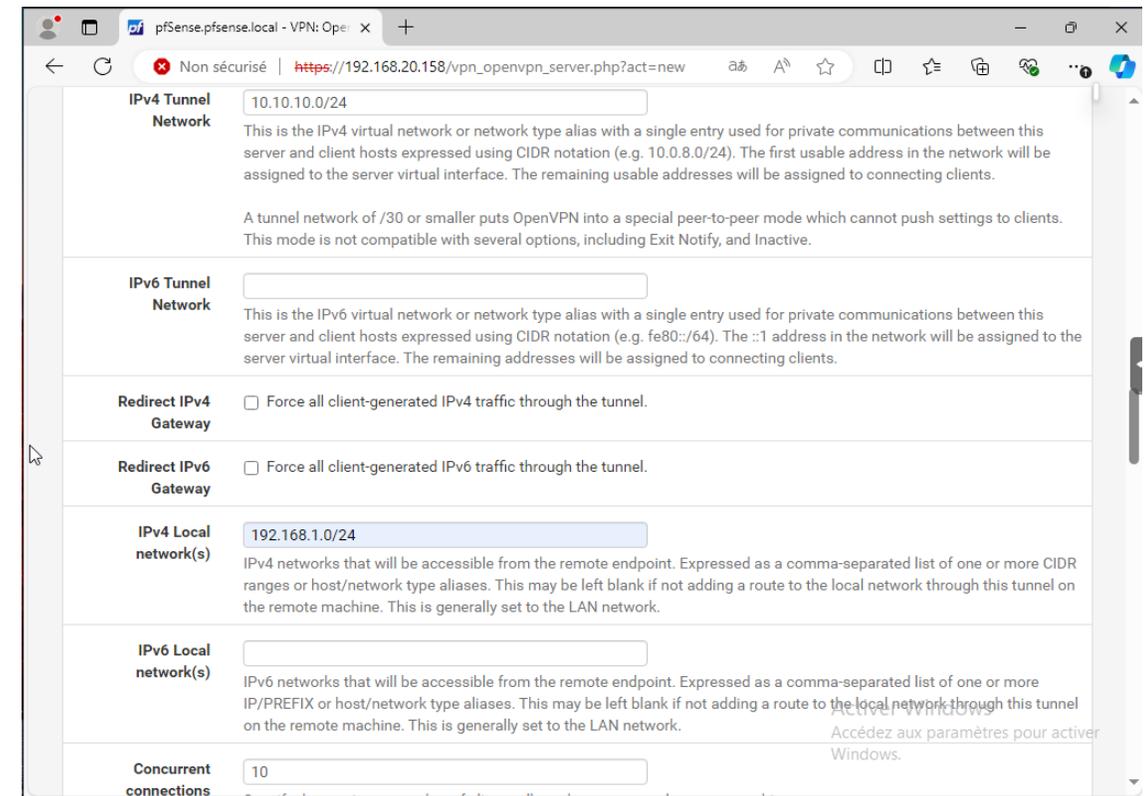
**DH Parameter Length**  
2048 bit  
Diffie-Hellman (DH) parameter set used for key exchange.

**ECDH Curve**  
Use Default  
The Elliptic Curve to use for key exchange.  
The curve from the server certificate is used by default when the server uses an ECDSA certificate. Otherwise, secp384r1 is used as a fallback.

**Data Encryption Algorithms**

AES-128-CBC (128 bit key, 128 bit block)	AES-128-GCM
AES-128-CFB (128 bit key, 128 bit block)	
AES-128-CFB1 (128 bit key, 128 bit block)	
AES-128-CFB8 (128 bit key, 128 bit block)	
AES-128-GCM (128 bit key, 128 bit block)	
AES-128-OFB (128 bit key, 128 bit block)	
AES-192-CBC (192 bit key, 128 bit block)	

Active Windows  
Accédez aux paramètres pour activer Windows.



Non sécurisé | [https://192.168.20.158/vpn\\_openvpn\\_server.php?act=new](https://192.168.20.158/vpn_openvpn_server.php?act=new)

**IPv4 Tunnel Network**  
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.  
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.

**IPv6 Tunnel Network**  
  
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.

**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  
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.

**IPv6 Local network(s)**  
  
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.

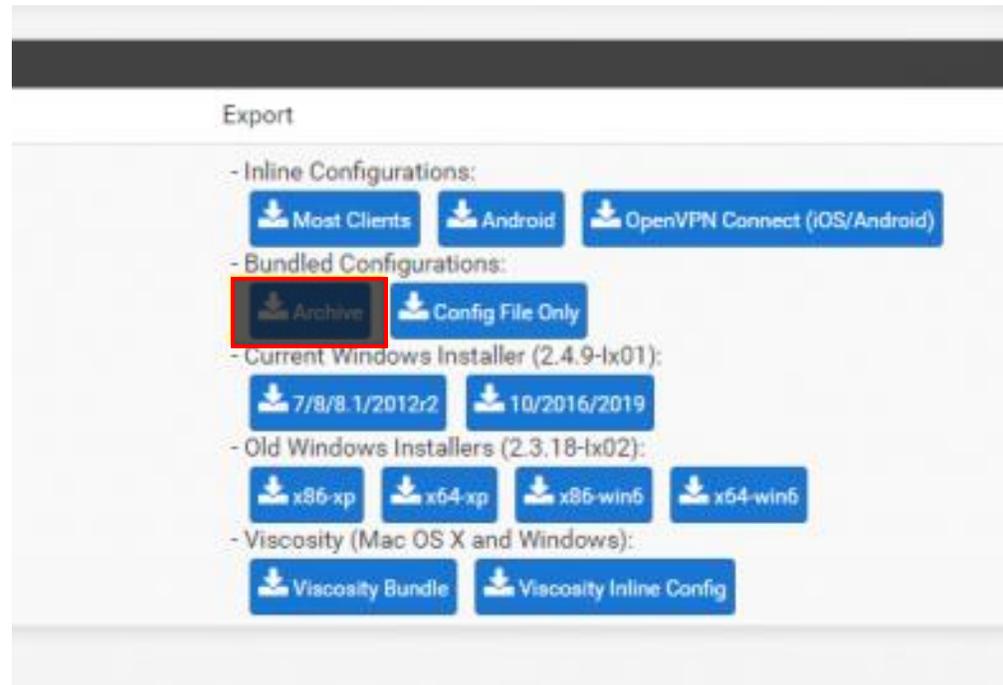
**Concurrent connections**  
10

Active Windows  
Accédez aux paramètres pour activer Windows.



# Exporter la configuration OpenVPN

# Pour utiliser OpenVPN , il faudra prendre la configuration "Bundled Configuration"





# Tester l'accès distant depuis un poste client

- Installer le client OpenVPN,
- Extraire le contenu de l'archive ZIP téléchargée depuis le Pfsense et qui contient la configuration,
- Sur l'icône OpenVPN faire un clic droit et cliquez sur "Connecter",
- User et password sont à rentrer,
- Dans l'invite de commande, taper "ipconfig", l'ip devrait être dans le réseau entré pendant la configuration.