IMPLÉMENTATION D'UNE SOLUTION VPN NOMADE SÉCURISÉE BASÉE SUR PFSENSE

Réalisé par : **SOULAIMAN Rayane**

Administrateur système, réseau et sécurité

Table des matières

1 Glossaire des Sigles et Acronymes 4

2 Introduction : 5

3 Présentation de l'environnement de travail : 5

3.1 Présentation de GNS3 : 5

3.2 Présentation de pfSense : 5

3.3 Présentation de la machine virtuelle Windows 10 : 6

3.4 Description du réseau NAT : 6

4 Analyse des besoins et conception du réseau : 6

4.1 Analyse des besoins : 6

4.2 Besoins fonctionnels : 7

4.3 Besoins en sécurité : 7

4.4 Conception de l'architecture réseau : 7

5 Mise en place de l'infrastructure réseau : 8

5.1 Configuration du réseau NAT dans GNS3 : 8

5.2 Installation et configuration de pfSense 8

5.3 Configuration des interfaces WAN et LAN : 11

5.4 Vérification de la connectivité réseau : 11

6 Implémentation du VPN nomade : 13

6.1 Choix de la technologie VPN : 13

6.2 Configuration du serveur VPN sur pfSense : 13

7 Génération du certificat serveur 15

7.1 Création des utilisateurs VPN : 19

7.2 Configuration du client VPN sur Windows 10 : 21

7.3 Tests et validation du VPN : 28

8 Sécurisation du réseau : 29

8.1 Configuration du pare-feu pfsense : 29

8.2 Règles de filtrage et NAT : 30

8.3 Journalisation et supervision : 32

9 Tests, validation et analyse : 33

9.1 1. Scénarios de tests : 33

9.2 Résultats des tests : 33

9.3 Analyse des performances et de la sécurité : 33

10 . Limites et améliorations possibles : 34

10.1 Limites de l'architecture mise en place : 34

10.2 Propositions d'amélioration : 34

11 . Conclusion : 35

1 Glossaire des Sigles et Acronymes

GNS3 (Graphical Network Simulator 3) : logiciel de simulation réseau permettant de concevoir, tester et valider des architectures réseau virtuelles.
pfSense Distribution open source basée sur FreeBSD, utilisée comme pare-feu et routeur pour la sécurisation et la gestion des réseaux informatiques.
VPN (Virtual Private Network) : réseau privé virtuel permettant d'établir une connexion sécurisée entre un utilisateur distant et un réseau interne.
VPN nomade Type de VPN permettant à un utilisateur mobile ou distant d'accéder de manière sécurisée aux ressources du réseau interne de l'entreprise.
NAT (Network Address Translation) : mécanisme de traduction des adresses IP privées en adresses IP publiques, et inversement.
WAN (Wide Area Network) : réseau étendu couvrant une grande zone géographique, généralement utilisé pour désigner la connexion vers Internet.
LAN (Local Area Network) : réseau local reliant les équipements informatiques d'un même site ou d'un même bâtiment.
OpenVPN Solution open source de réseau privé virtuel permettant de sécuriser les communications grâce au chiffrement des données.
IP (Internet Protocol) : protocole de communication assurant l'adressage et l'acheminement des paquets de données sur un réseau.
Pare-feu (Firewall) Dispositif matériel ou logiciel chargé de filtrer le trafic réseau entrant et sortant selon des règles de sécurité définies.
VM (Virtual Machine) : environnement informatique virtualisé simulant le fonctionnement d'un ordinateur physique.
Windows 10 Système d'exploitation développé par Microsoft, utilisé dans ce projet comme client VPN.
Journalisation (Logs) Processus d'enregistrement des événements système et réseau afin de faciliter la surveillance et l'analyse de la sécurité.
Supervision Ensemble des mécanismes permettant de surveiller le fonctionnement, les performances et la sécurité d'une infrastructure réseau.

2 Introduction :

Avec l'évolution des technologies de l'information et de la communication, les entreprises et les organisations ont de plus en plus besoin de permettre à leurs utilisateurs d'accéder aux ressources internes à distance, tout en garantissant un haut niveau de sécurité. Le télétravail, la mobilité des employés et l'accès distant aux systèmes d'information rendent indispensable la mise en place de solutions d'accès sécurisé.

Dans ce contexte, le **VPN nomade (Virtual Private Network)** constitue une solution efficace permettant à un utilisateur distant de se connecter de manière sécurisée à un réseau interne via Internet. Il assure la confidentialité, l'intégrité et l'authentification des communications.

Ce projet s'inscrit dans le cadre d'un **projet de fin SAE** et a pour objectif l'**implémentation d'une solution VPN nomade sécurisée basée sur pfSense**, en utilisant un environnement de simulation avec **GNS3**, un **réseau NAT** et une **machine virtuelle Windows 10** jouant le rôle de client distant.

L'objectif principal est de concevoir, configurer et tester une architecture réseau fonctionnelle et sécurisée, tout en mettant en pratique les notions théoriques vues en réseau et en cybersécurité.

3 Présentation de l'environnement de travail :

3.1 Présentation de GNS3 :

GNS3 (Graphical Network Simulator 3) est un outil de simulation réseau permettant de concevoir, configurer et tester des architectures réseau virtuelles. Il offre la possibilité d'interconnecter des équipements virtuels tels que des routeurs, des pare-feu et des machines virtuelles, sans nécessiter de matériel physique.

Dans le cadre de ce projet, GNS3 est utilisé pour simuler l'infrastructure réseau, intégrer le routeur pfSense et connecter la machine virtuelle Windows 10 via un réseau NAT. Cliquer sur ce lien pour télécharger GNS3

3.2 Présentation de pfSense :

pfSense est un pare-feu et routeur open source basée sur FreeBSD. Il est largement utilisé pour la sécurisation des réseaux informatiques grâce à ses nombreuses fonctionnalités, notamment :

- Le filtrage de paquets (pare-feu),
- La gestion du NAT,
- La mise en place de VPN (OpenVPN),
- La supervision et la journalisation des événements.

Dans ce projet, pfSense joue le rôle de **routeur principal et de serveur VPN**, assurant la sécurisation des communications entre le client distant et le réseau interne. Cliquer sur lien pour télécharger pfsense

3.3 Présentation de la machine virtuelle Windows 10 :

La machine virtuelle Windows 10 représente l'utilisateur nomade. Elle est utilisée pour :

- Tester la connectivité réseau,
- Installer et configurer le client VPN,
- Vérifier l'accès sécurisé au réseau interne via le VPN.

Cette machine permet de simuler un poste utilisateur réel se connectant à distance à l'infrastructure.
Cliquer sur ce lien pour télécharger Windows 10

3.4 Description du réseau NAT :

Le réseau NAT (Network Address Translation) permet aux machines virtuelles d'accéder à Internet en utilisant l'adresse IP de la machine hôte. Il est utilisé dans ce projet pour simuler un accès Internet réel, nécessaire au fonctionnement du VPN nomade.
Le NAT joue un rôle essentiel dans la communication entre la machine Windows 10 et le pare-feu pfSense.

4 Analyse des besoins et conception du réseau :

4.1 Analyse des besoins :

Les besoins identifiés pour ce projet sont les suivants :

- Permettre à un utilisateur distant de se connecter au réseau interne,
- Sécuriser les échanges de données sur Internet,
- Garantir l'authentification des utilisateurs VPN,
- Assurer la confidentialité et l'intégrité des communications,
- Mettre en place une architecture simple, fonctionnelle et évolutive.

4.2 Besoins fonctionnels :

Sur le plan fonctionnel, la solution doit permettre :

- L'établissement d'un tunnel VPN entre le client Windows 10 et pfSense,
- L'accès sécurisé au réseau interne après authentification,
- La gestion des utilisateurs VPN, • La supervision des connexions VPN.

4.3 Besoins en sécurité :

Les besoins en sécurité incluent :

- L'utilisation d'un protocole VPN sécurisé,
- La mise en place de règles de pare-feu adaptées,
- La restriction des accès aux seuls utilisateurs autorisés,
- La journalisation des connexions et des événements de sécurité.

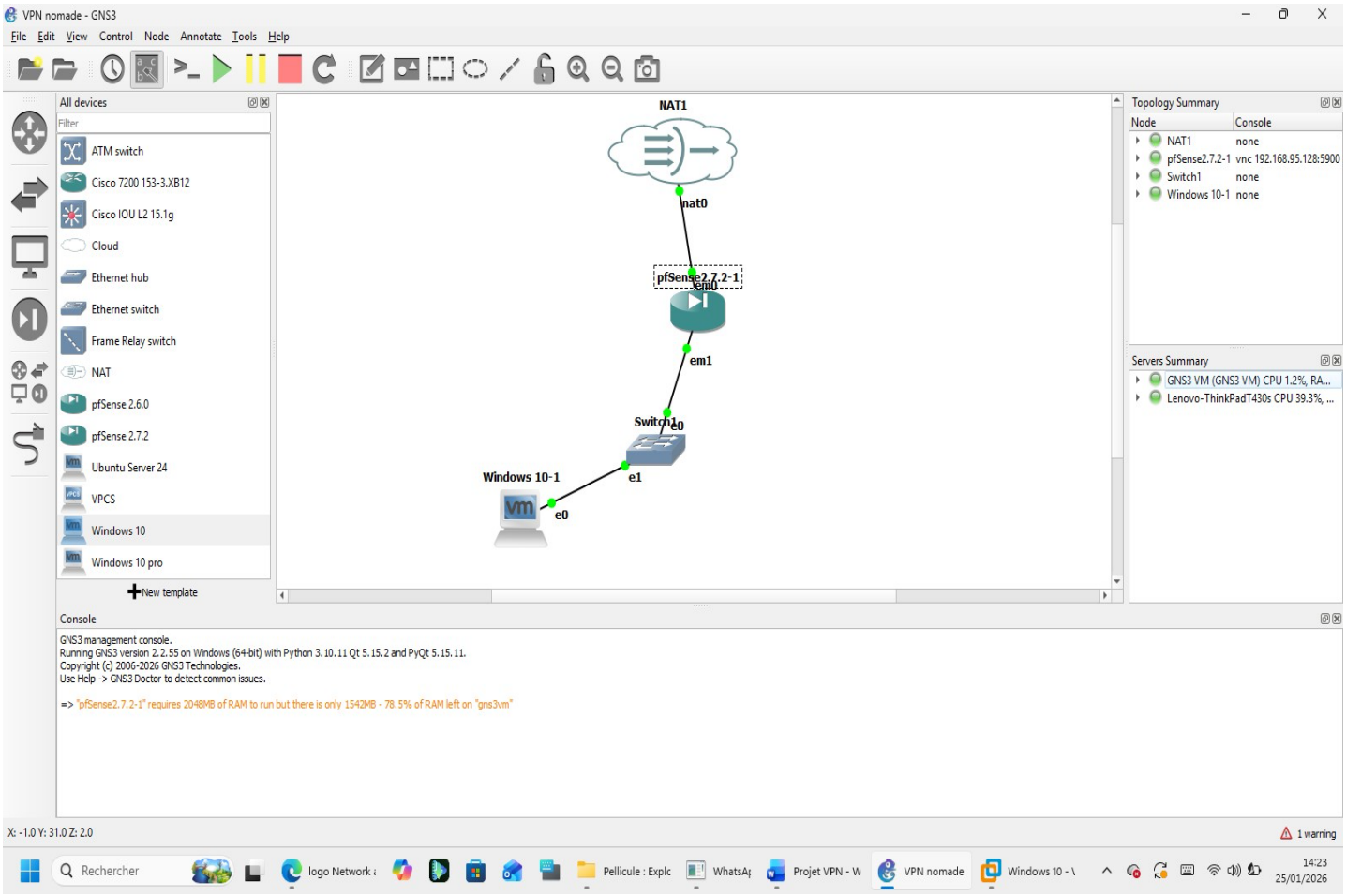
4.4 Conception de l'architecture réseau :

L'architecture réseau conçue repose sur les éléments suivants :

- Un routeur pfSense connecté à un réseau NAT (WAN),
- Un réseau local (LAN) protégé par pfSense,
- Une machine virtuelle Windows 10 jouant le rôle de client VPN nomade.

pfSense assure le routage, la sécurité du réseau et l'hébergement du serveur VPN. Le client Windows 10 se connecte au serveur VPN via Internet afin d'accéder de manière sécurisée aux ressources du réseau interne.

Cette architecture permet de simuler un cas réel d'accès distant sécurisé dans un environnement contrôlé.



5 Mise en place de l'infrastructure réseau :

5.1 Configuration du réseau NAT dans GNS3 :

Pour simuler un environnement proche du réel, un réseau NAT est configuré dans GNS3. Le réseau NAT permet aux machines virtuelles d'accéder à Internet en utilisant l'adresse IP de la machine hôte.
Cette configuration est essentielle pour :

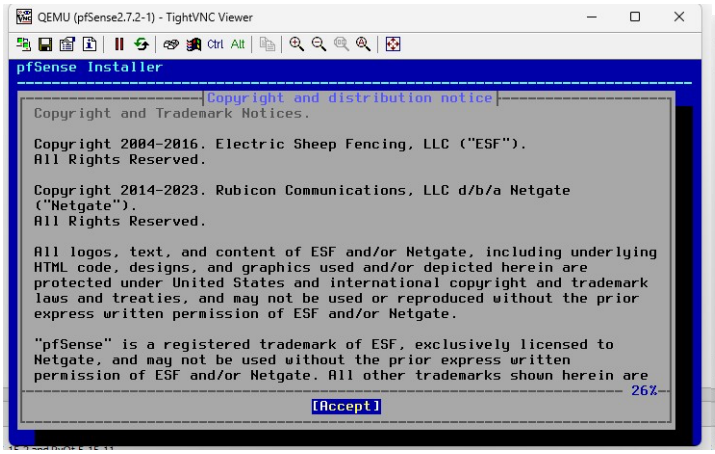
- Fournir une connexion Internet aux équipements virtuels,
- Permettre au serveur VPN pfSense d'être accessible depuis l'extérieur,
- Simuler un accès distant sécurisé depuis le client Windows 10.

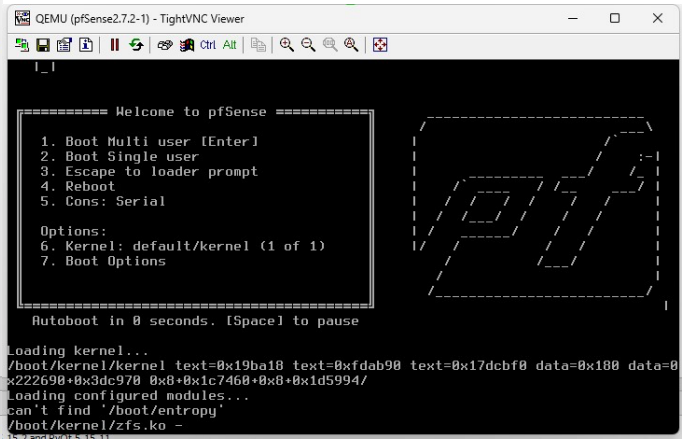
Le réseau NAT est relié à l'interface WAN de pfSense, qui servira de passerelle vers Internet.

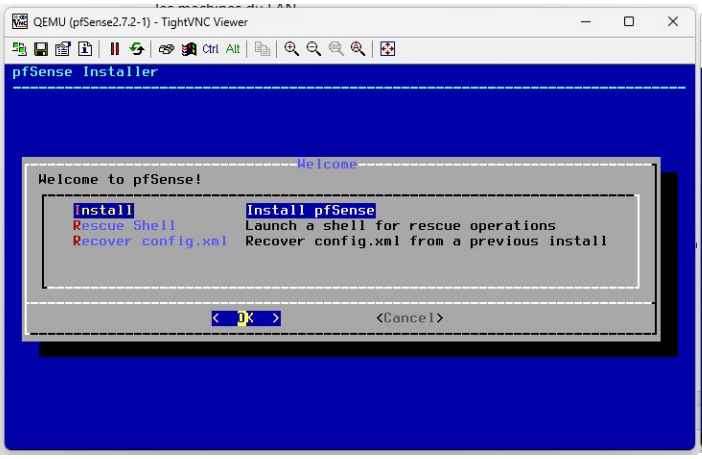
5.2 Installation et configuration de pfSense

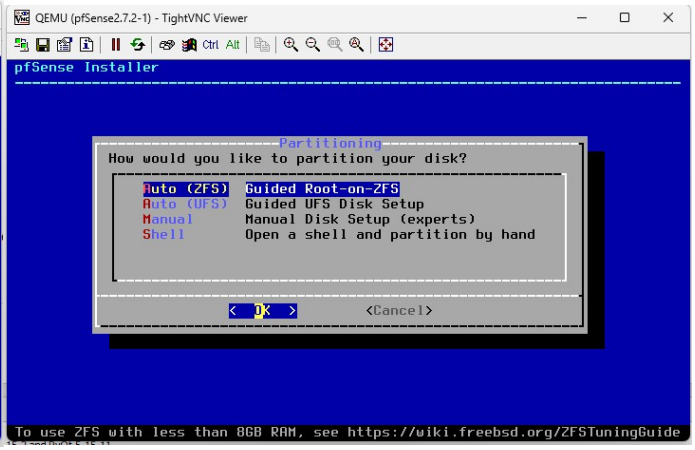
❖ installation

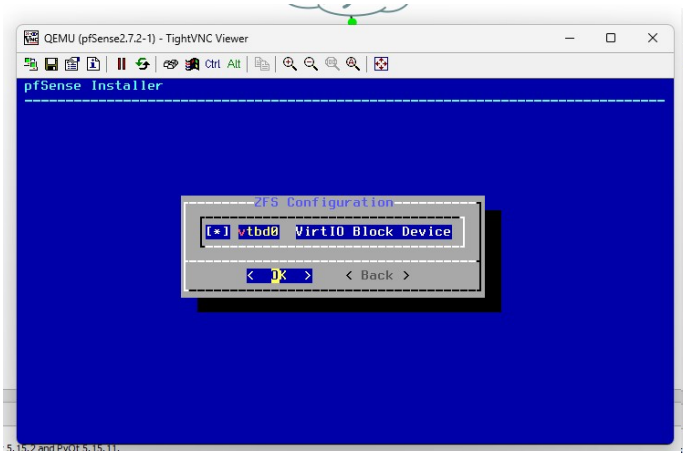
Le routeur pfSense est ajouté à GNS3 sous forme d'image virtuelle.

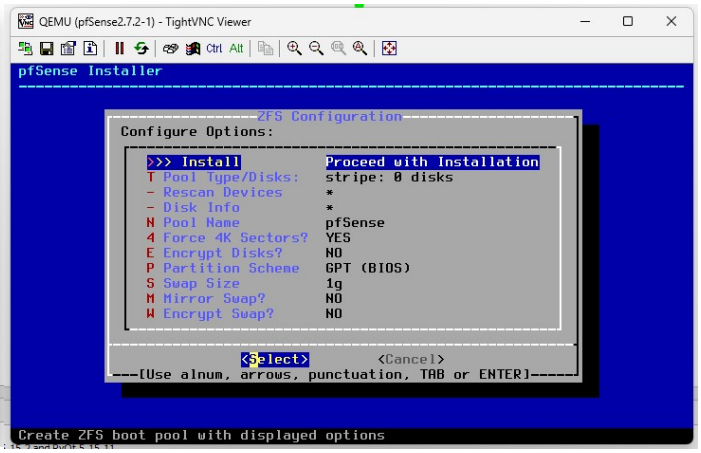

QEMU (pfSense2.7.2-1) - TightVNC Viewer
pfSense Installer
Copyright and distribution notice
Copyright and Trademark Notices.
Copyright 2004-2016. Electric Sheep Fencing, LLC ("ESF").
All Rights Reserved.
Copyright 2014-2023. Rubicon Communications, LLC d/b/a Netgate ("Netgate").
All Rights Reserved.
All logos, text, and content of ESF and/or Netgate, including underlying HTML code, designs, and graphics used and/or depicted herein are protected under United States and international copyright and trademark laws and treaties, and may not be used or reproduced without the prior express written permission of ESF and/or Netgate.
"pfSense" is a registered trademark of ESF, exclusively licensed to Netgate, and may not be used without the prior express written permission of ESF and/or Netgate. All other trademarks shown herein are
26%
[Accept]

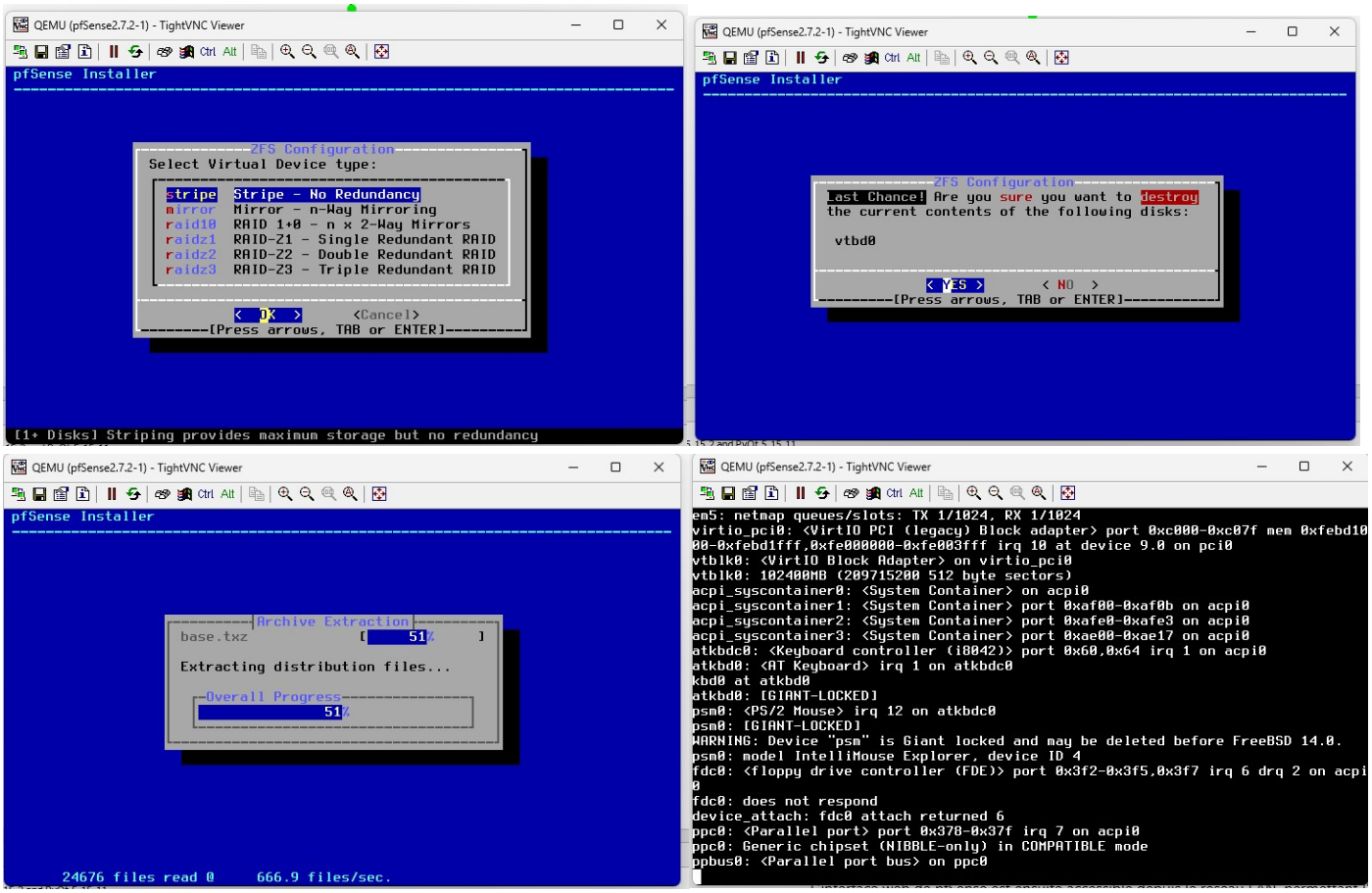

QEMU (pfSense2.7.2-1) - TightVNC Viewer
Welcome to pfSense
1. Boot Multi user [Enter]
2. Boot Single user
3. Escape to loader prompt
4. Reboot
5. Cons: Serial
Options:
6. Kernel: default/kernel (1 of 1)
7. Boot Options
Autoboot in 0 seconds. [Space] to pause
Loading kernel...
/boot/kernel/kernel text=0x19ba18 text=0xfdab90 text=0x17dcbf0 data=0x180 data=0
x222690+0x3dc970 0x8+0x1c7460+0x8+0x1d5994/
Loading configured modules...
can't find '/boot/entropy'
/boot/kernel/zfs.ko -


QEMU (pfSense2.7.2-1) - TightVNC Viewer
pfSense Installer
Welcome
Welcome to pfSense!
Install
Install pfSense
Rescue Shell
Launch a shell for rescue operations
Recover config.xml
Recover config.xml from a previous install
< OK >
<Cancel>


QEMU (pfSense2.7.2-1) - TightVNC Viewer
pfSense Installer
Partitioning
How would you like to partition your disk?
Auto (ZFS)
Guided Root-on-ZFS
Auto (UFS)
Guided UFS Disk Setup
Manual
Manual Disk Setup (experts)
Shell
Open a shell and partition by hand
< OK >
<Cancel>
To use ZFS with less than 8GB RAM, see https://wiki.freebsd.org/ZFSTuningGuide


QEMU (pfSense2.7.2-1) - TightVNC Viewer
pfSense Installer
ZFS Configuration
[*] vtbd0 VirtIO Block Device
< OK >
< Back >


QEMU (pfSense2.7.2-1) - TightVNC Viewer
pfSense Installer
ZFS Configuration
Configure Options:
>>> Install
Proceed with Installation
T Pool Type/Disks:
stripe: 0 disks
- Rescan Devices
*
- Disk Info
*
N Pool Name
pfSense
4 Force 4K Sectors?
YES
E Encrypt Disks?
NO
P Partition Scheme
GPT (BIOS)
S Swap Size
1g
M Mirror Swap?
NO
W Encrypt Swap?
NO
<Select>
<Cancel>
[Use alnum, arrows, punctuation, TAB or ENTER]
Create ZFS boot pool with displayed options

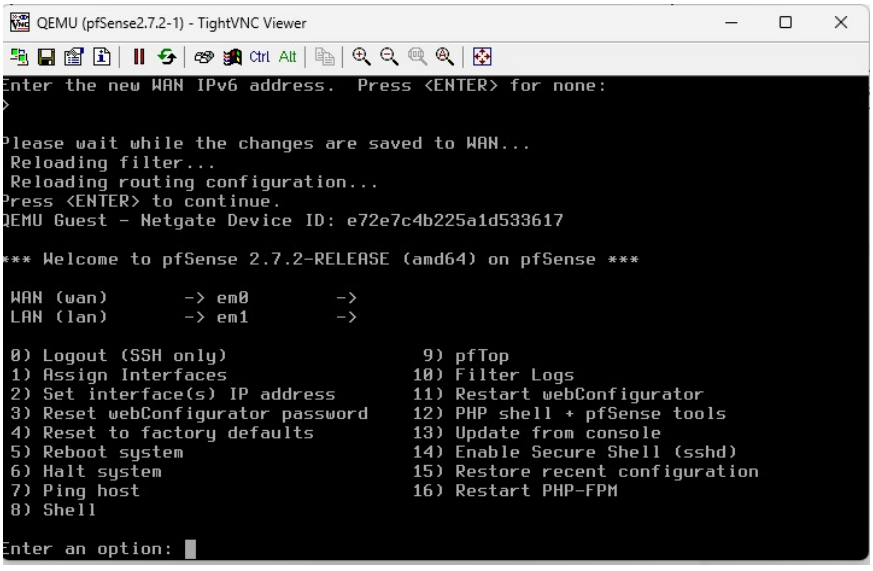


❖ **Configuration :**

Après démarrage, pfSense est configuré avec deux interfaces :

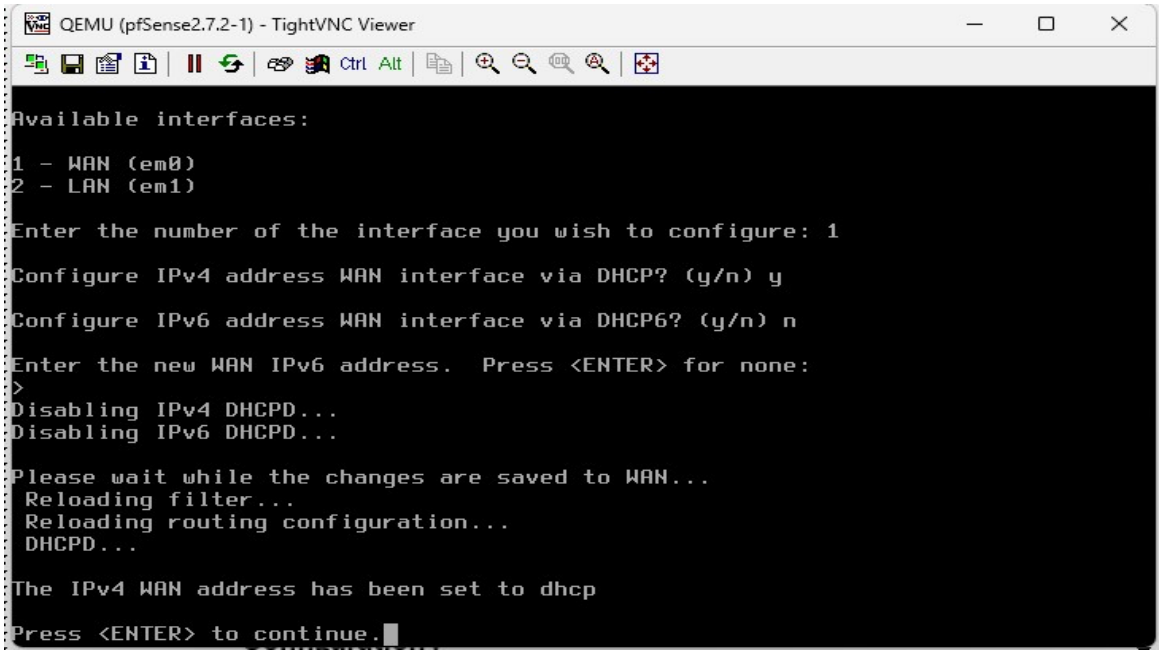
- **WAN** : connectée au réseau NAT pour l'accès Internet.
- **LAN** : connecté au réseau interne pour les machines locales.

L'interface web de pfSense est ensuite accessible depuis le réseau LAN, permettant l'administration complète du routeur et la configuration des services, dont le VPN.

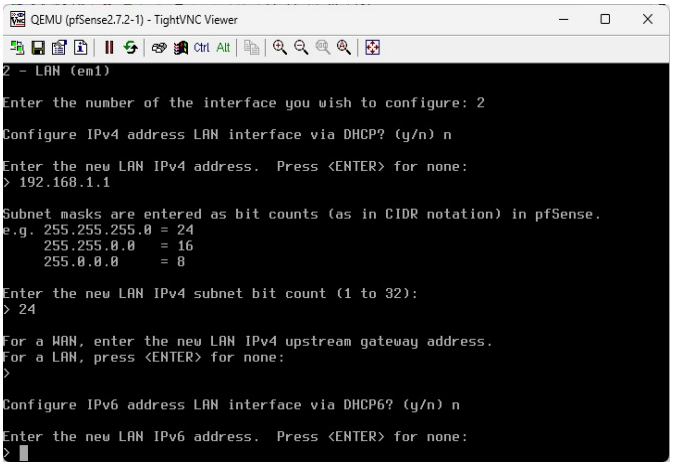


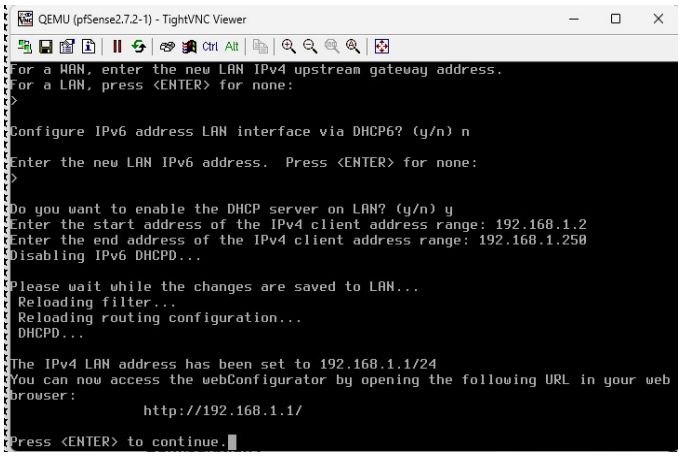
5.3 Configuration des interfaces WAN et LAN :

- L'**interface WAN** est configurée pour obtenir automatiquement une adresse IP via DHCP sur le réseau NAT. Cela permet à pfSense d'accéder à Internet facilement.



- L'**interface LAN** est configurée avec une adresse IP statique, servant de passerelle pour le réseau interne. Le plan d'adressage IP est défini afin d'assurer une communication cohérente entre pfSense et les machines du LAN.

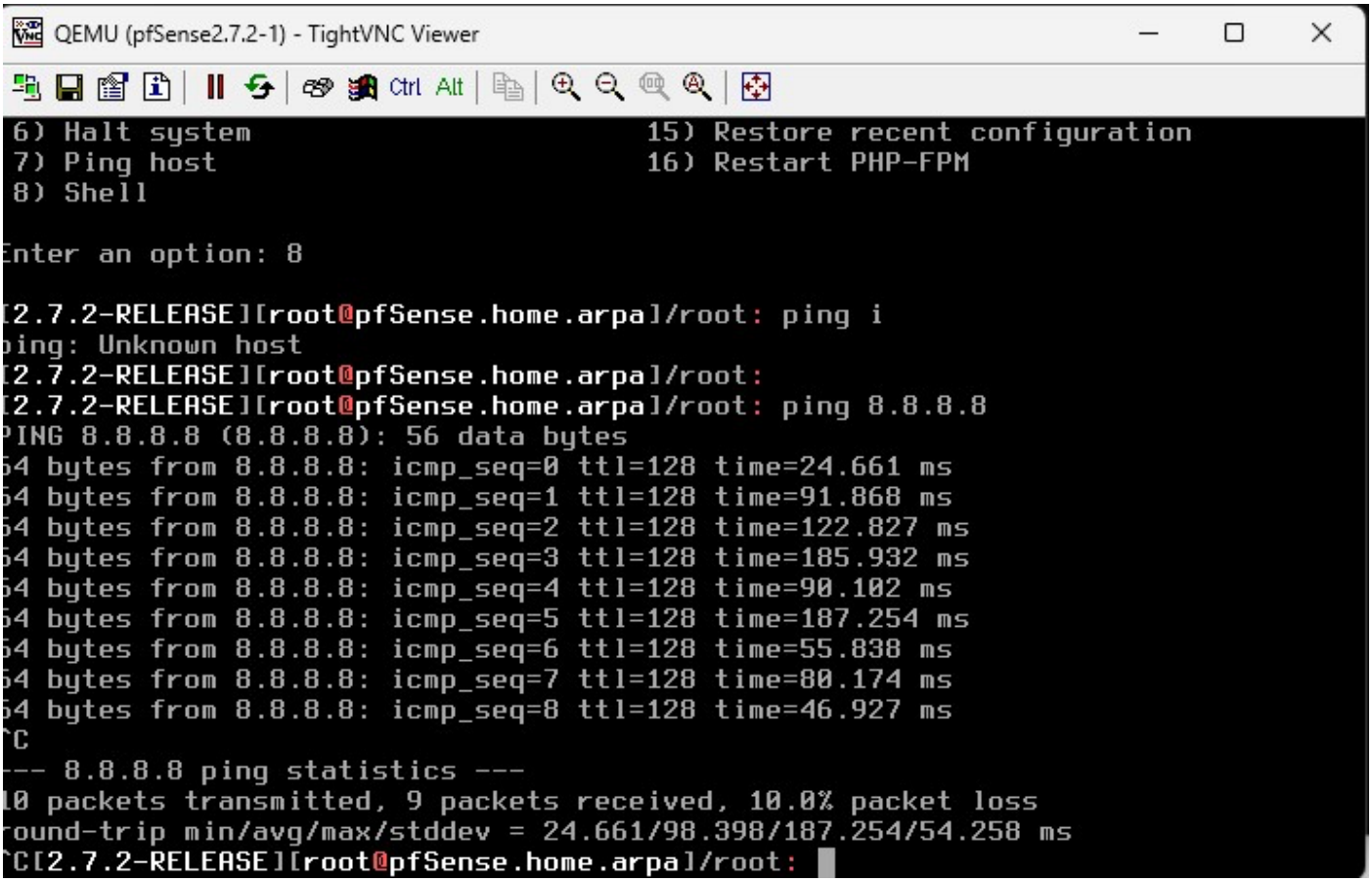




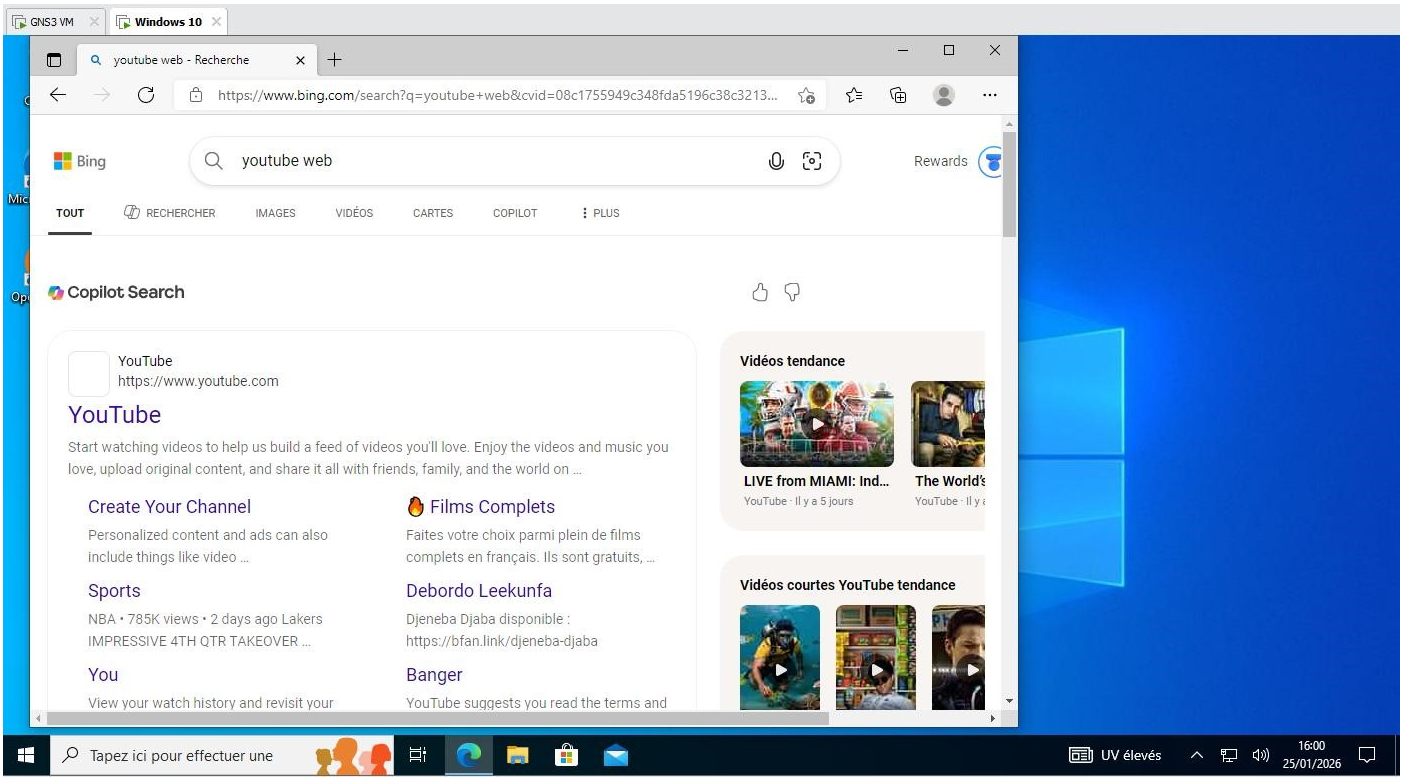
5.4 Vérification de la connectivité réseau :

Avant d'implémenter le VPN, des tests de connectivité sont réalisés :

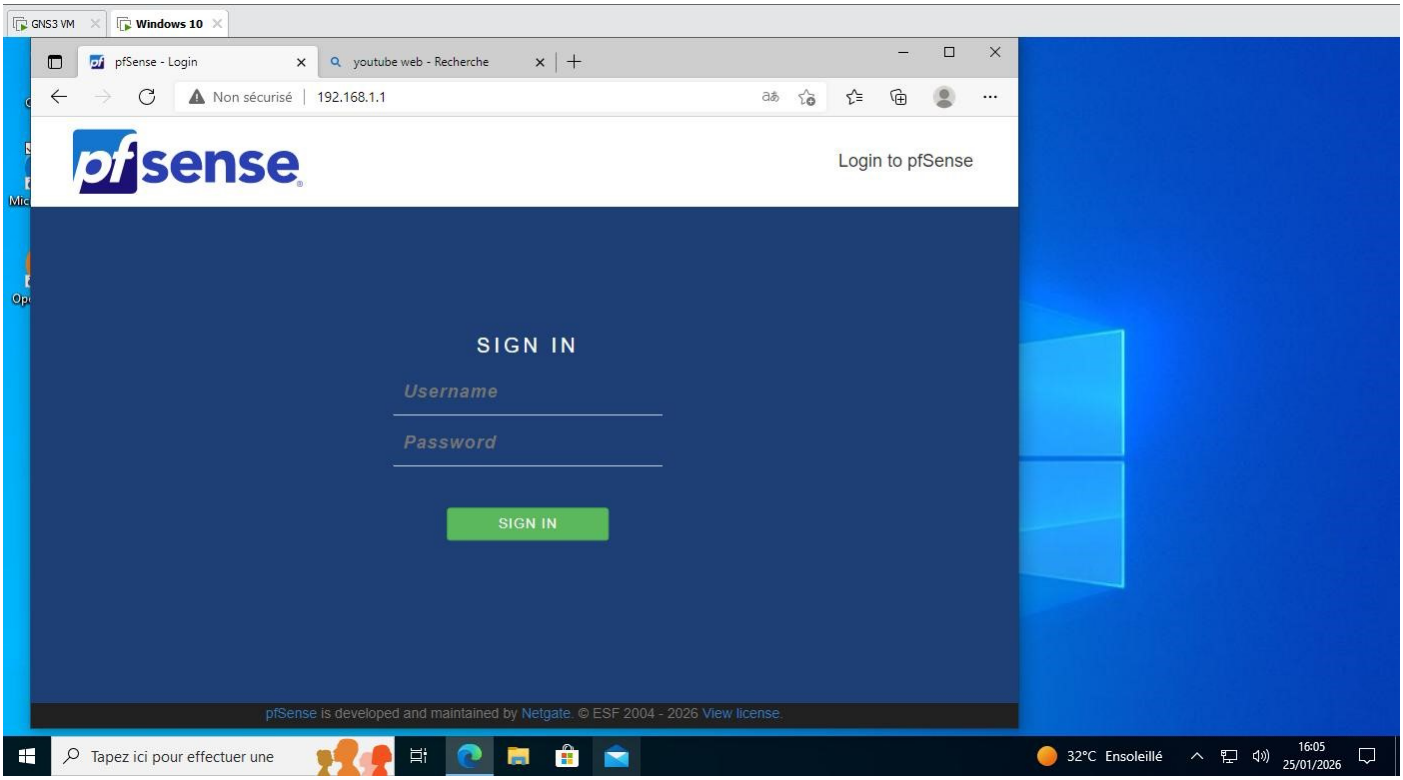
- Test de ping depuis pfSense vers Internet,



- Test de communication entre LAN et WAN,



- Vérification de l'accès à l'interface web de pfSense depuis Windows 10.



Ces tests permettent de confirmer que le réseau fonctionne correctement et que le serveur pfSense est prêt à accueillir le VPN.

6 Implémentation du VPN nomade :

6.1 Choix de la technologie VPN :

Pour ce projet, la technologie **OpenVPN** est retenue. Elle offre plusieurs avantages :

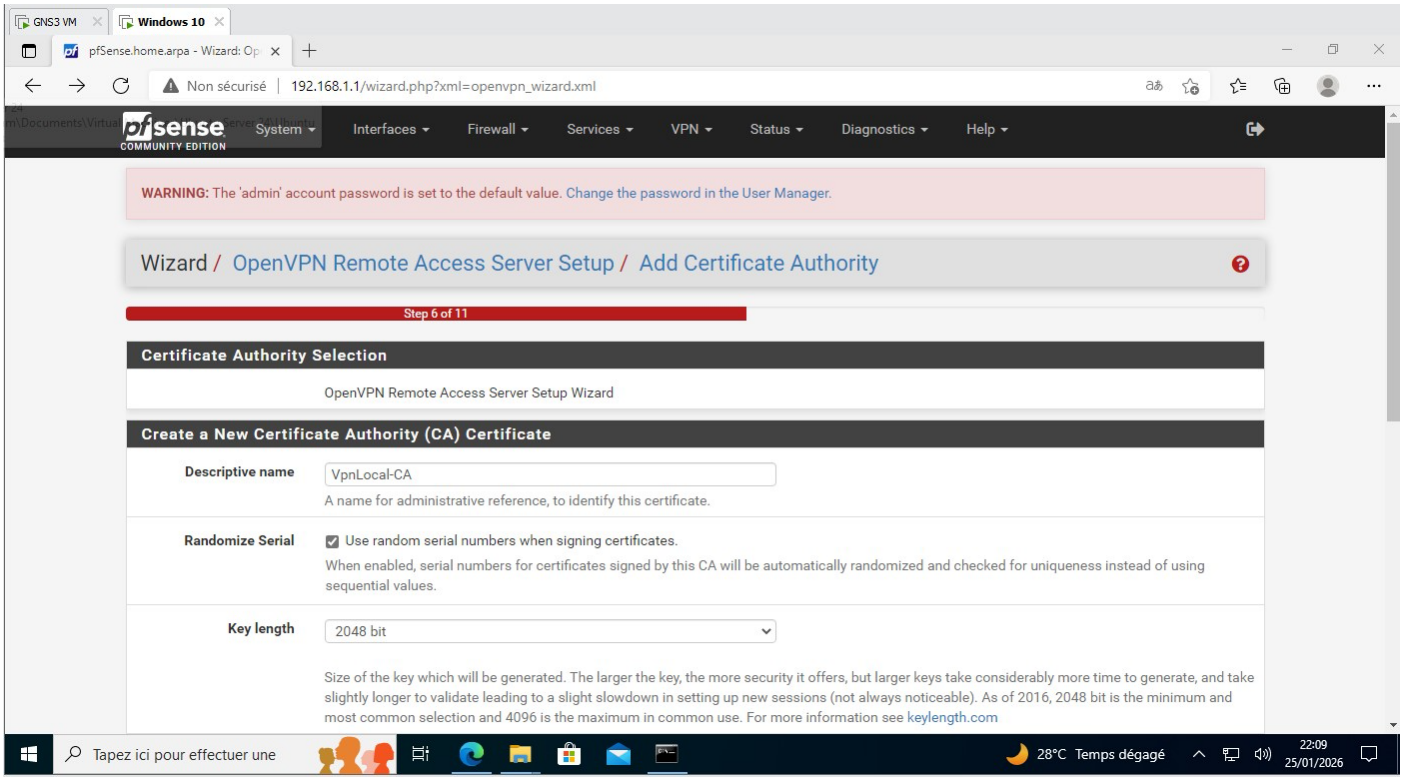
- Niveau de sécurité élevé grâce au chiffrement SSL/TLS, • Compatibilité avec Windows, Linux et macOS, • Gestion facile des certificats et utilisateurs.

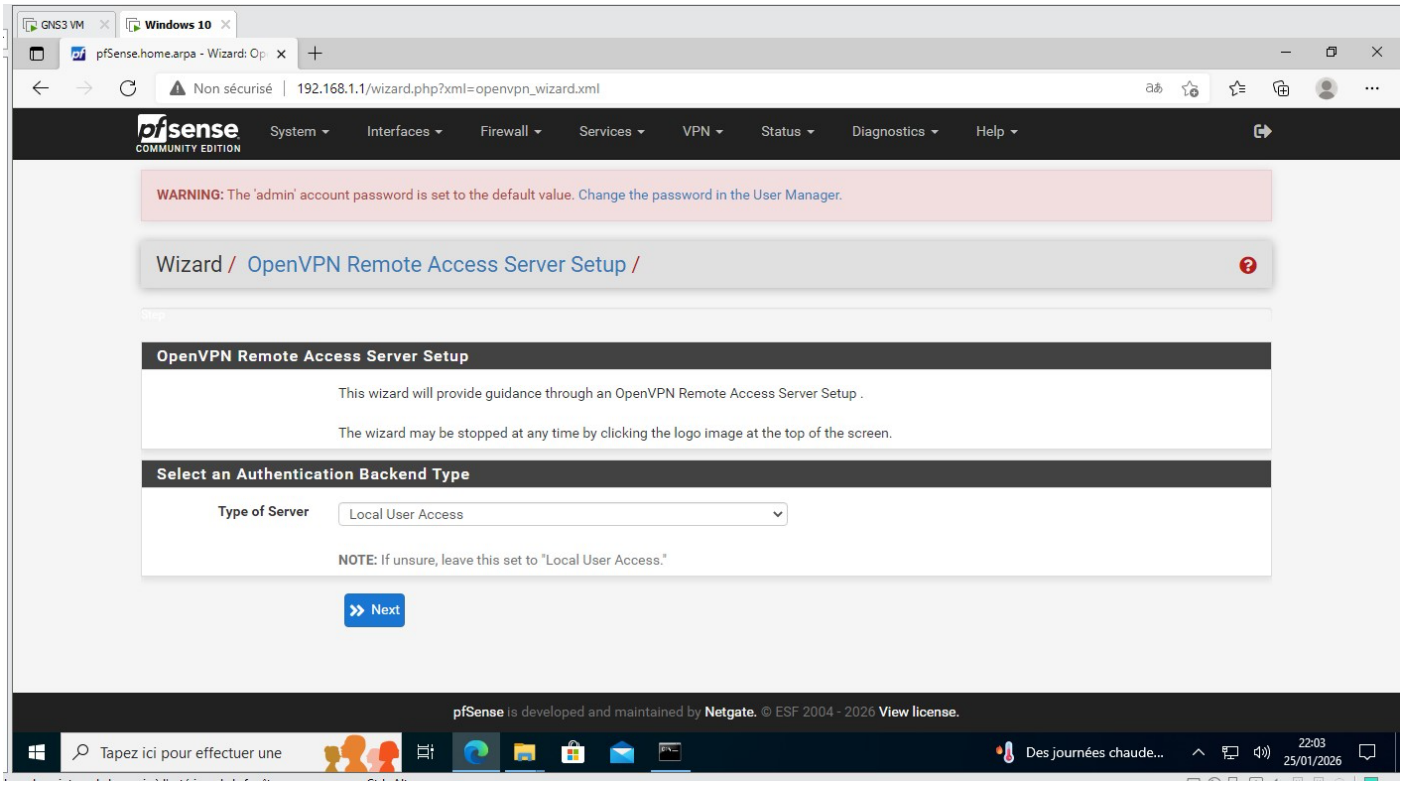
OpenVPN permettra de créer un tunnel sécurisé entre le client distant (Windows 10) et le réseau interne.

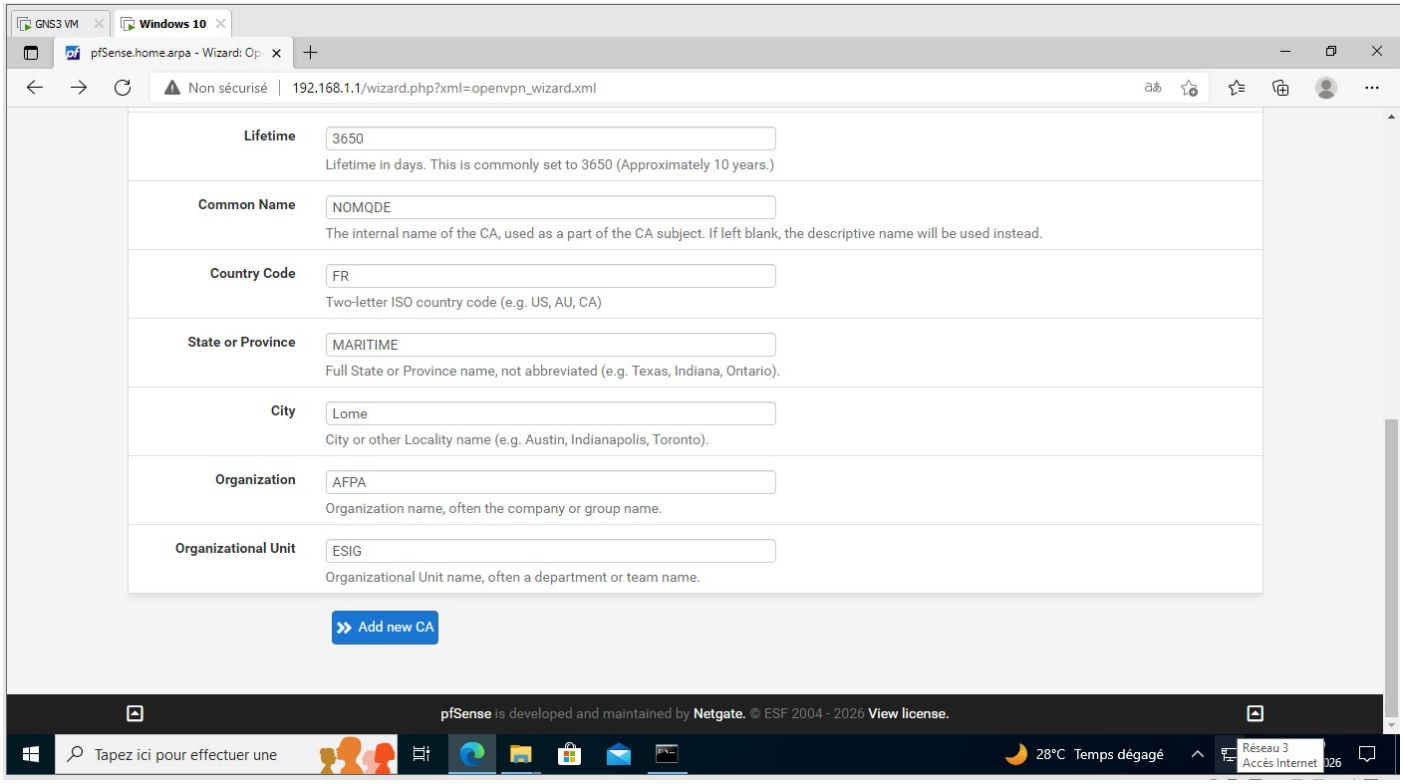
6.2 Configuration du serveur VPN sur pfSense :

La configuration du serveur VPN est effectuée à l'aide de l'assistant OpenVPN intégré à pfSense. Cette procédure débute par la création d'une autorité de certification interne afin d'assurer l'authentification sécurisée des entités du VPN. Ensuite, un certificat serveur est généré pour permettre l'établissement des connexions chiffrées. Le protocole de communication ainsi que le port d'écoute, généralement configuré en UDP sur le port 1194, sont ensuite définis. Une plage d'adresses IP est attribuée aux clients distants afin de permettre leur intégration au réseau privé. Enfin, les paramètres de chiffrement sont configurés pour garantir la confidentialité et l'intégrité des échanges. À l'issue de cette configuration, le serveur VPN est opérationnel et prêt à accepter les connexions des utilisateurs distants.

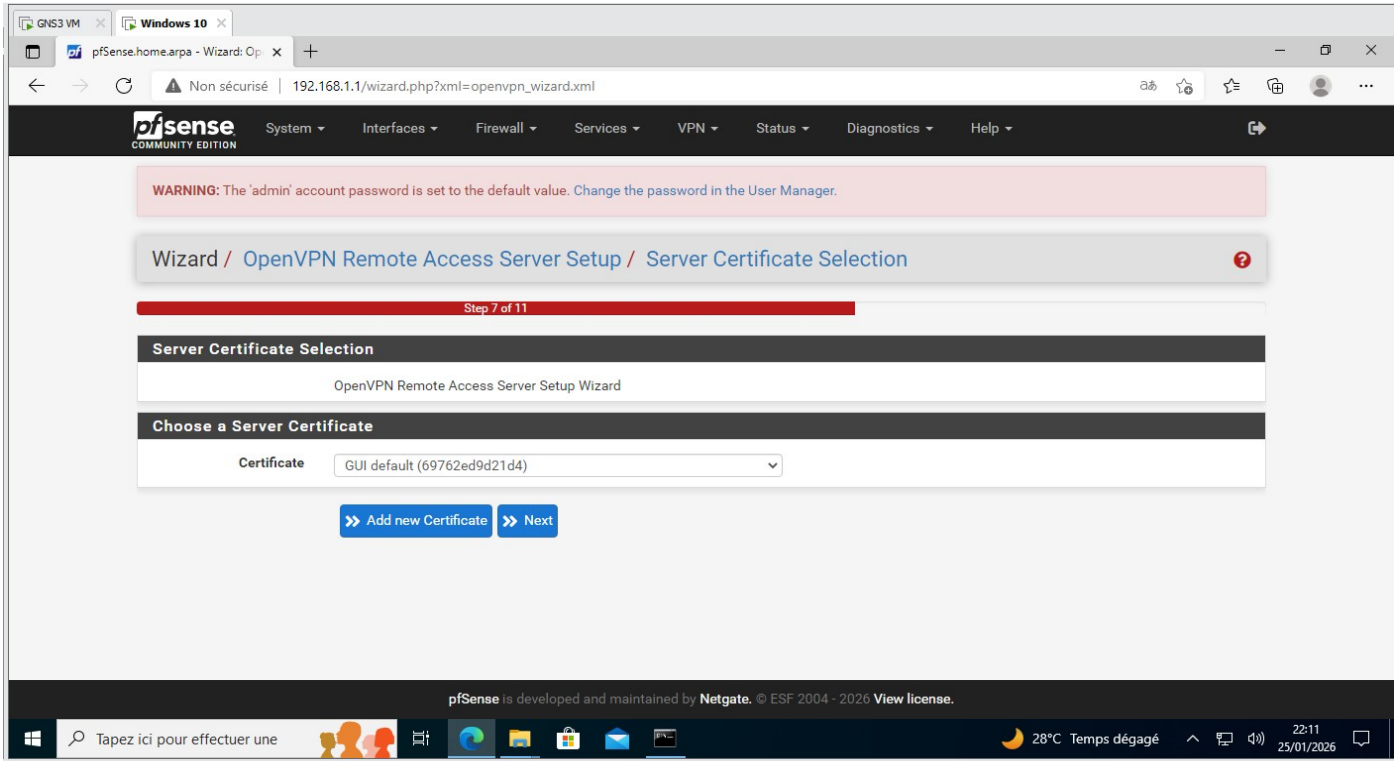
*Création d'une **autorité de certification (CA)** interne pour le VPN,

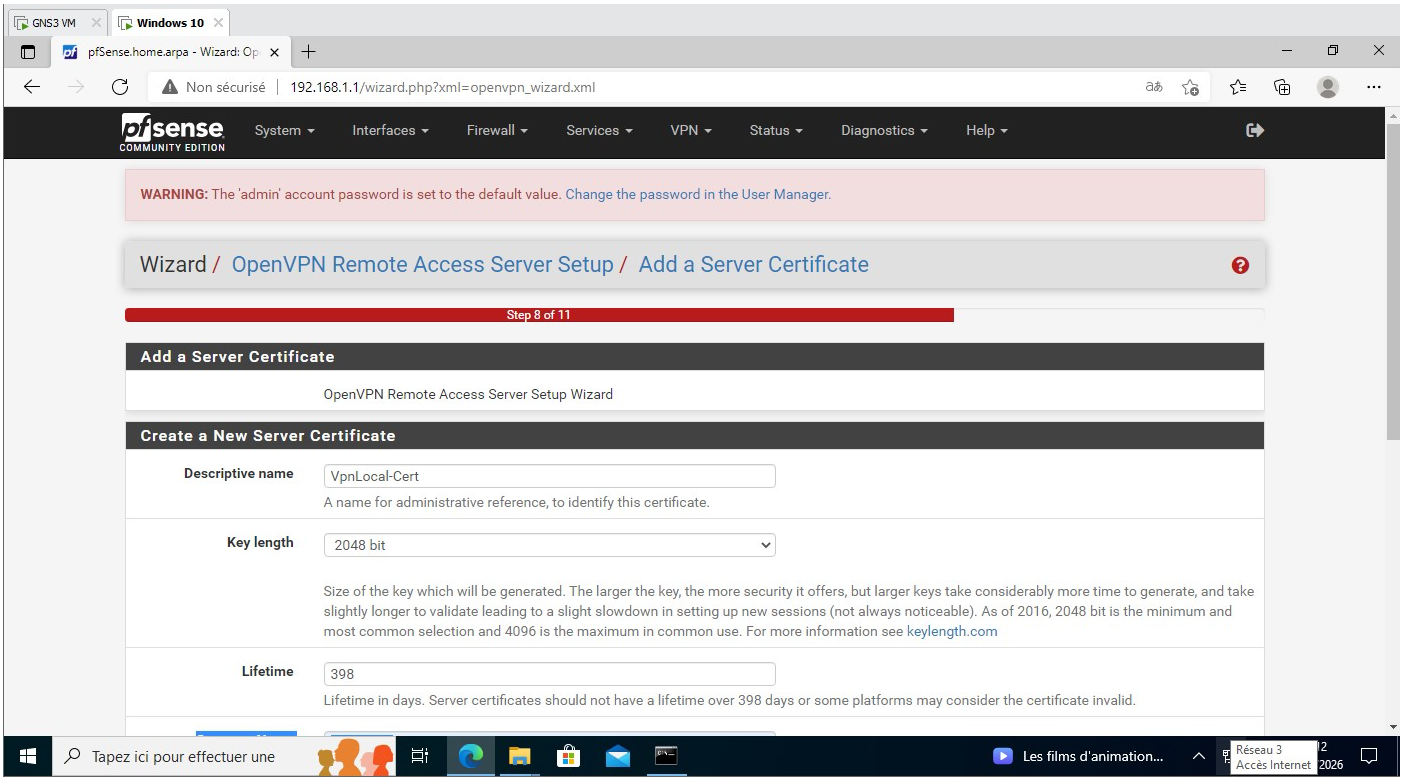

GNS3 VM
Windows 10
pfSense.home.arpa - Wizard: Op
Non sécurisé | 192.168.1.1/wizard.php?xml=openvpn_wizard.xml
pfsense COMMUNITY EDITION
System Interfaces Firewall Services VPN Status Diagnostics Help
WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.
Wizard / OpenVPN Remote Access Server Setup / Add Certificate Authority
Step 6 of 11
Certificate Authority Selection
OpenVPN Remote Access Server Setup Wizard
Create a New Certificate Authority (CA) Certificate
Descriptive name
VpnLocal-CA
A name for administrative reference, to identify this certificate.
Randomize Serial
Use random serial numbers when signing certificates.
When enabled, serial numbers for certificates signed by this CA will be automatically randomized and checked for uniqueness instead of using sequential values.
Key length
2048 bit
Size of the key which will be generated. The larger the key, the more security it offers, but larger keys take considerably more time to generate, and take slightly longer to validate leading to a slight slowdown in setting up new sessions (not always noticeable). As of 2016, 2048 bit is the minimum and most common selection and 4096 is the maximum in common use. For more information see keylength.com
Tapez ici pour effectuer une
28°C Temps dégagé
22:09
25/01/2026

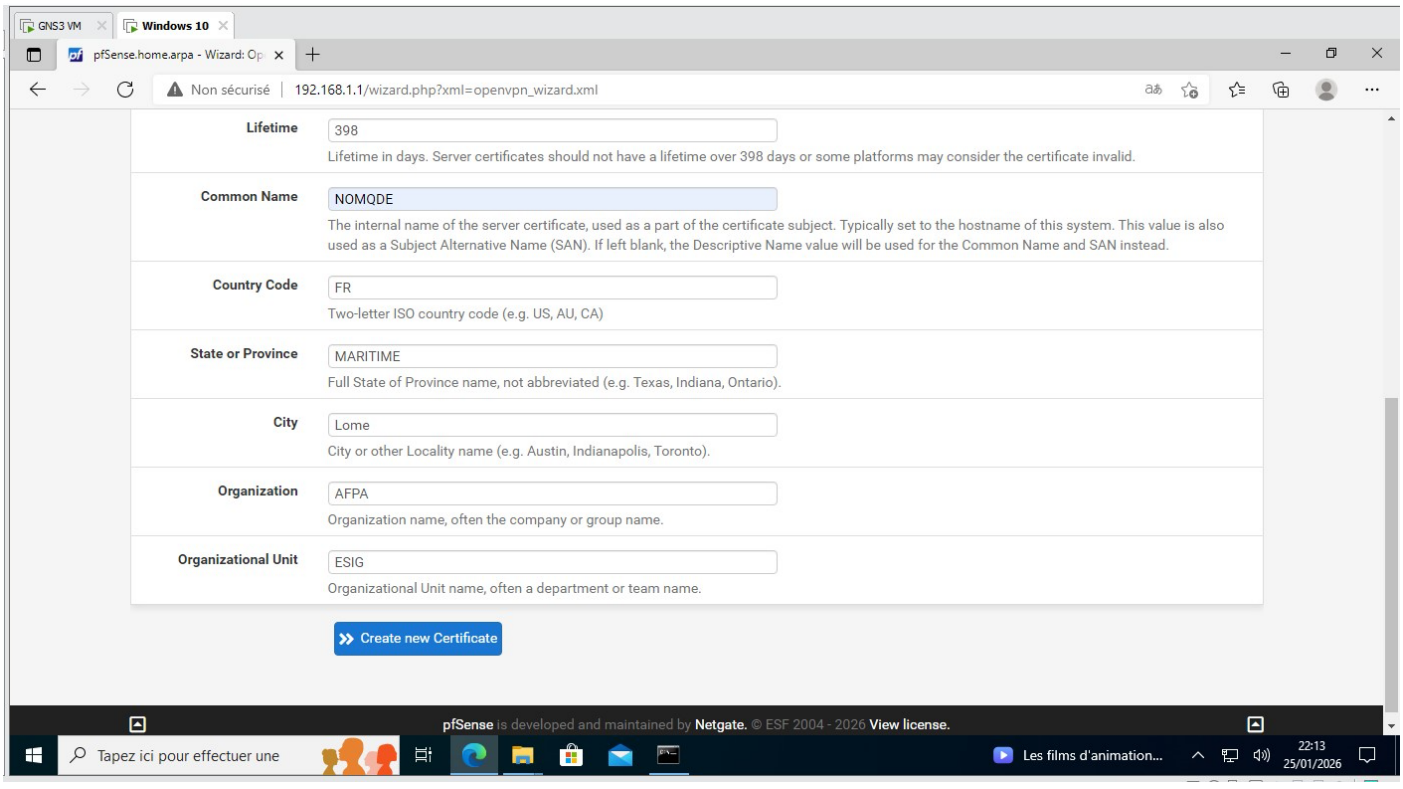

GNS3 VM
Windows 10
pfSense.home.arpa - Wizard: Op
Non sécurisé | 192.168.1.1/wizard.php?xml=openvpn_wizard.xml
pfsense COMMUNITY EDITION
System Interfaces Firewall Services VPN Status Diagnostics Help
WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.
Wizard / OpenVPN Remote Access Server Setup /
OpenVPN Remote Access Server Setup
This wizard will provide guidance through an OpenVPN Remote Access Server Setup .
The wizard may be stopped at any time by clicking the logo image at the top of the screen.
Select an Authentication Backend Type
Type of Server
Local User Access
NOTE: If unsure, leave this set to "Local User Access."
Next
pfSense is developed and maintained by Netgate. © ESF 2004 - 2026 View license.
Tapez ici pour effectuer une
Des journées chaude...
22:03
25/01/2026



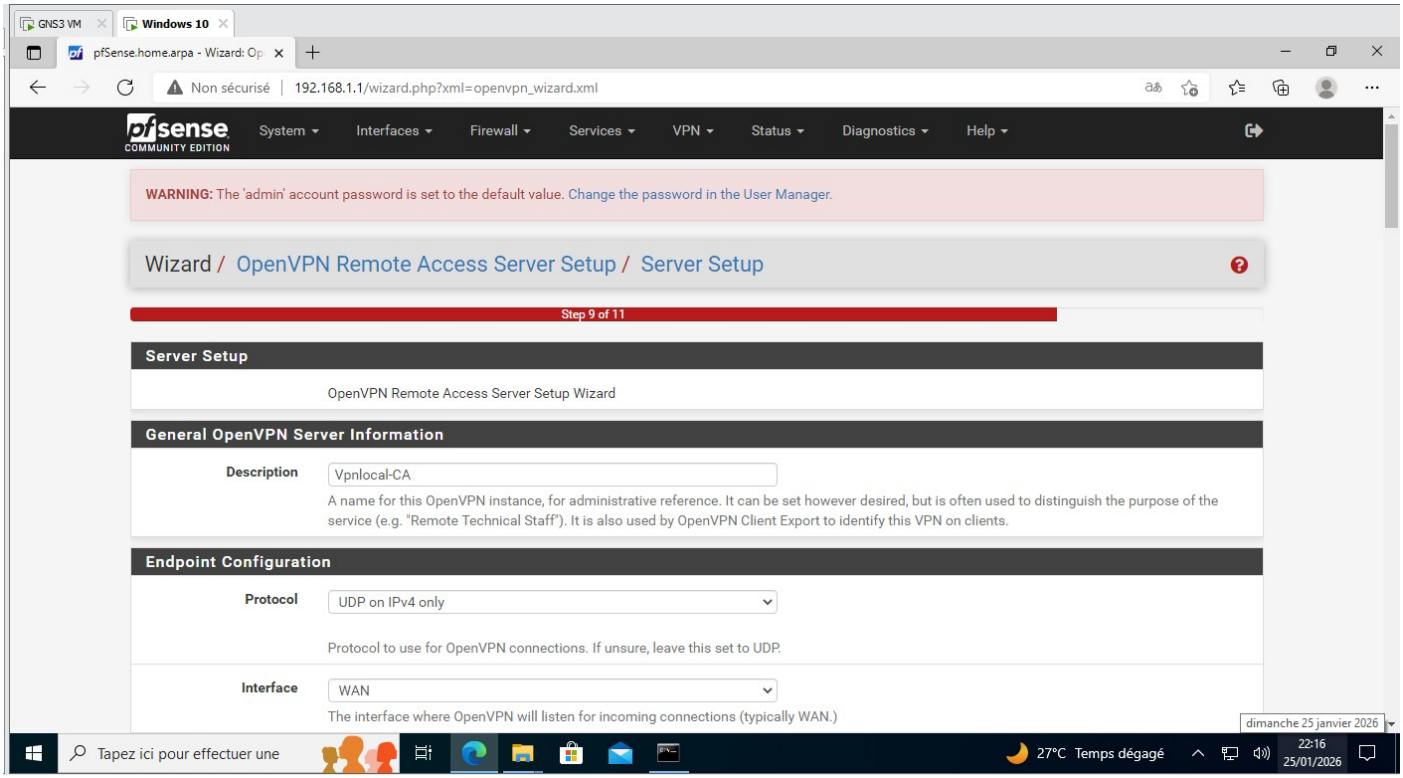
7 Génération du certificat serveur

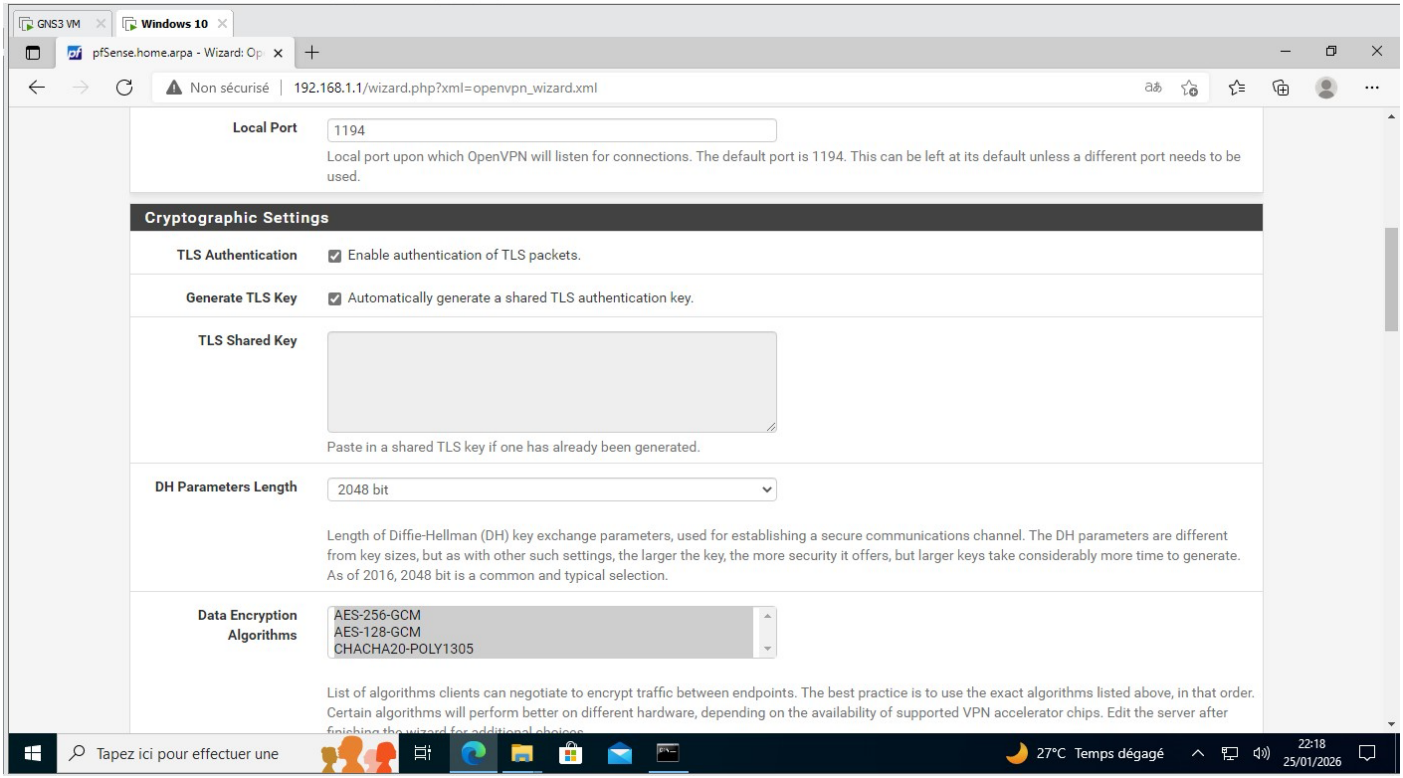


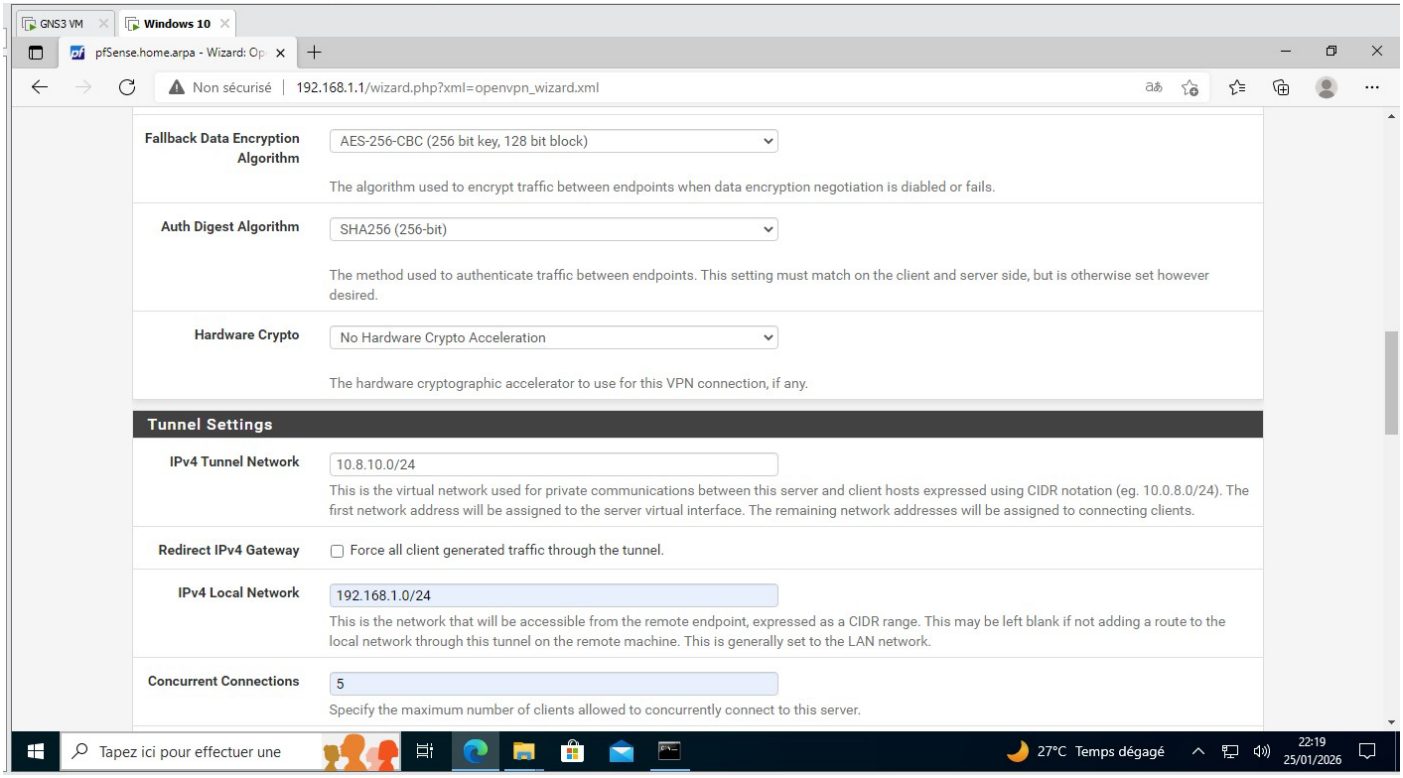


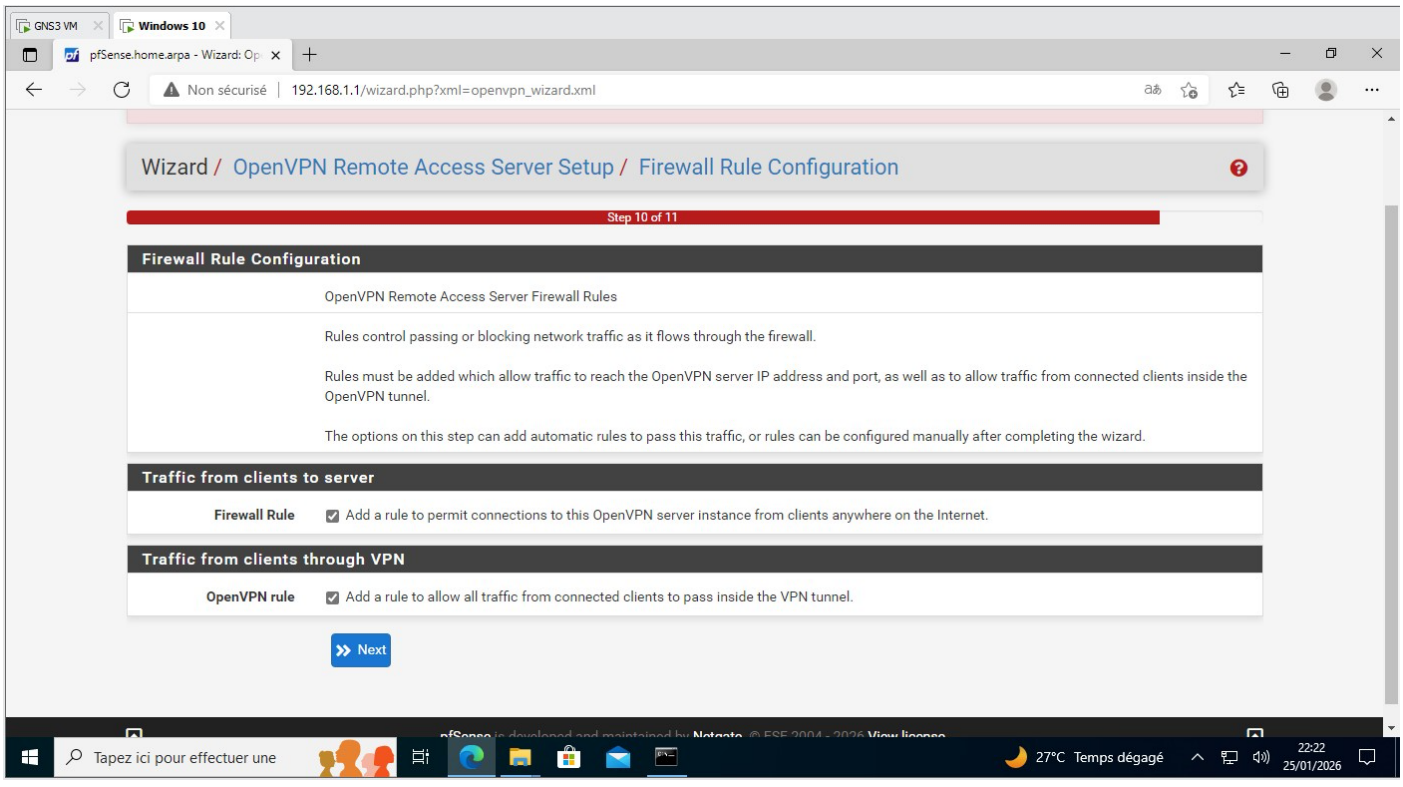


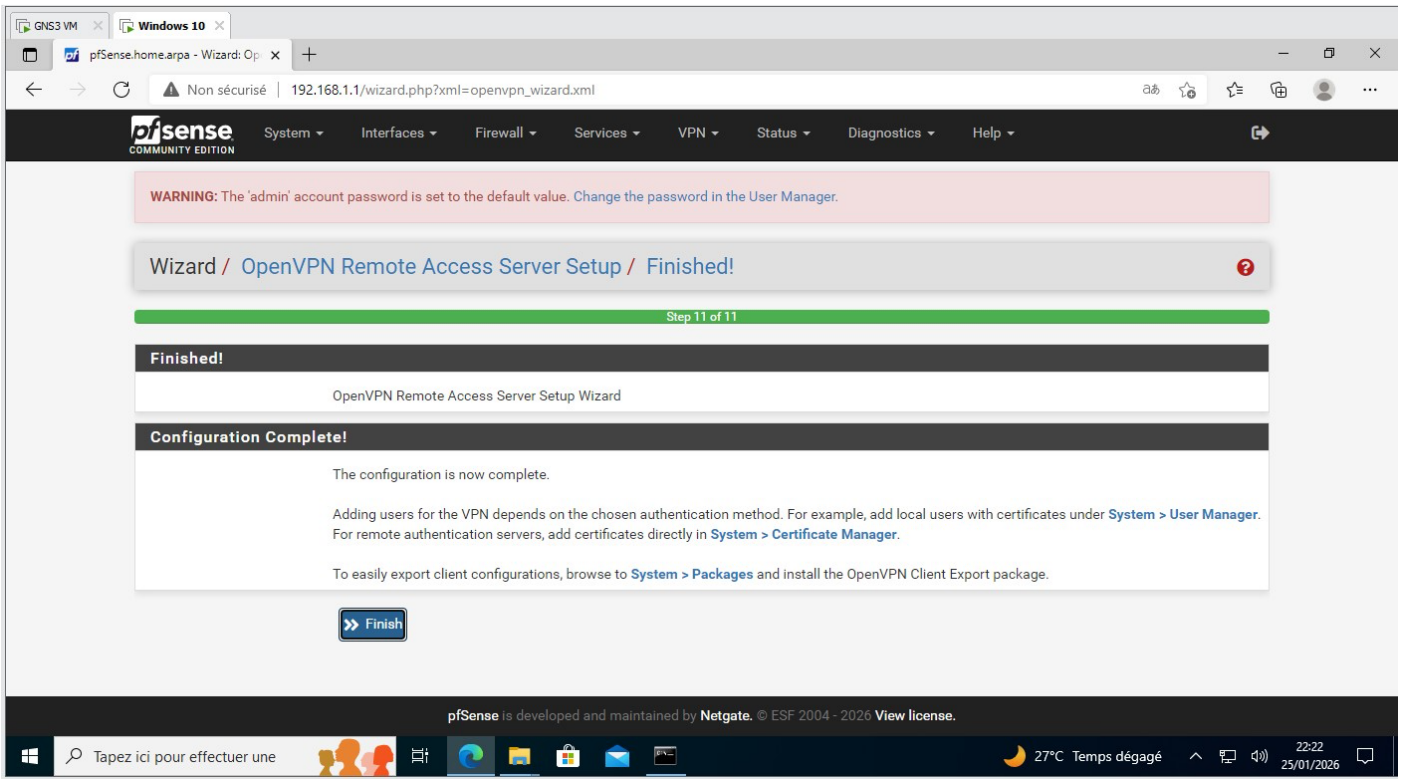
*Configuration du réseau VPN (plage d'adresses IP attribuées aux clients), Et définition du chiffrement pour sécuriser le tunnel.

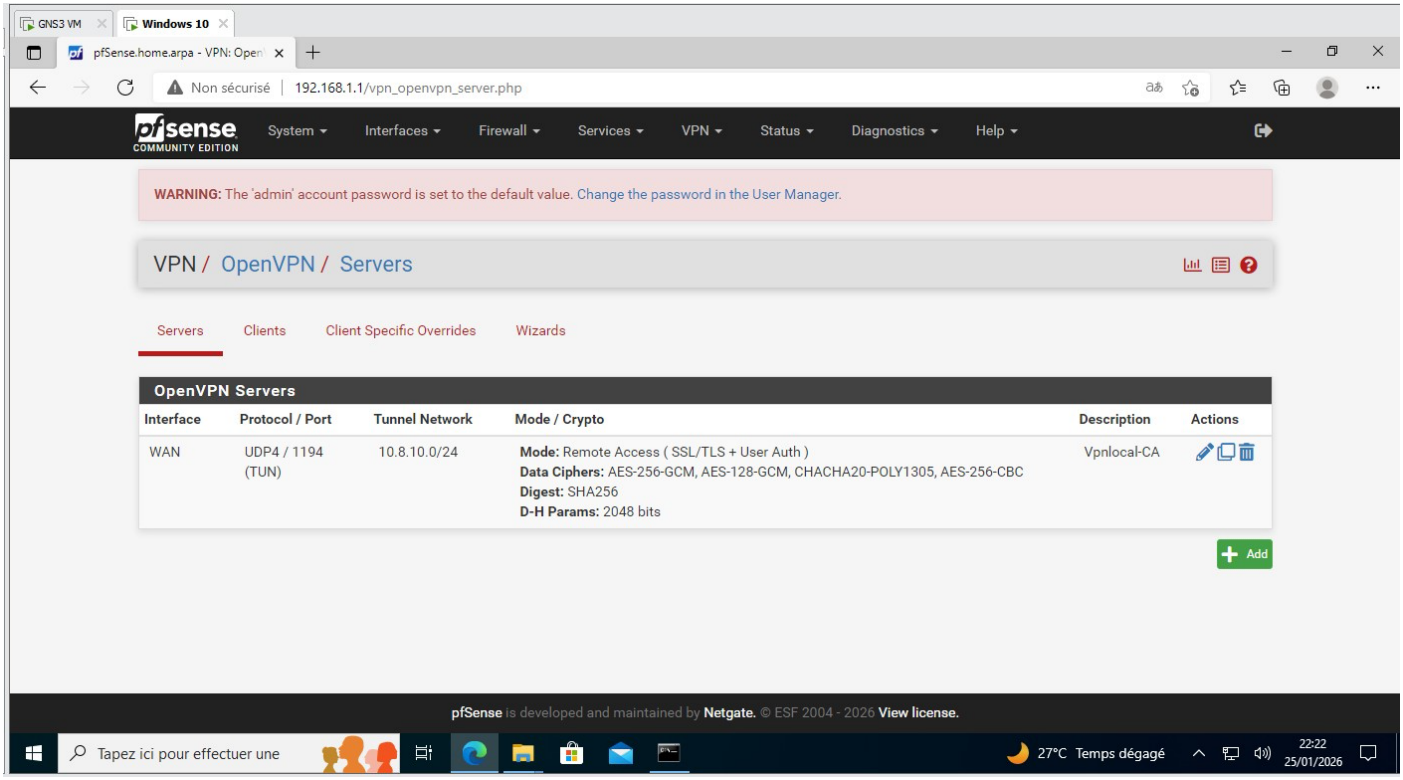

GNS3 VM
Windows 10
pfSense.home.arpa - Wizard: Op
Non sécurisé | 192.168.1.1/wizard.php?xml=openvpn_wizard.xml
pfsense COMMUNITY EDITION
System
Interfaces
Firewall
Services
VPN
Status
Diagnostics
Help
WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.
Wizard / OpenVPN Remote Access Server Setup / Server Setup
Step 9 of 11
Server Setup
OpenVPN Remote Access Server Setup Wizard
General OpenVPN Server Information
Description
Vpnlocal-CA
A name for this OpenVPN instance, for administrative reference. It can be set however desired, but is often used to distinguish the purpose of the service (e.g. "Remote Technical Staff"). It is also used by OpenVPN Client Export to identify this VPN on clients.
Endpoint Configuration
Protocol
UDP on IPv4 only
Protocol to use for OpenVPN connections. If unsure, leave this set to UDP.
Interface
WAN
The interface where OpenVPN will listen for incoming connections (typically WAN.)
dimanche 25 janvier 2026
Tapez ici pour effectuer une
27°C Temps dégagé
22:16
25/01/2026


GNS3 VM
Windows 10
pfSense.home.arpa - Wizard: Op
Non sécurisé | 192.168.1.1/wizard.php?xml=openvpn_wizard.xml
Local Port
1194
Local port upon which OpenVPN will listen for connections. The default port is 1194. This can be left at its default unless a different port needs to be used.
Cryptographic Settings
TLS Authentication
Enable authentication of TLS packets.
Generate TLS Key
Automatically generate a shared TLS authentication key.
TLS Shared Key
Paste in a shared TLS key if one has already been generated.
DH Parameters Length
2048 bit
Length of Diffie-Hellman (DH) key exchange parameters, used for establishing a secure communications channel. The DH parameters are different from key sizes, but as with other such settings, the larger the key, the more security it offers, but larger keys take considerably more time to generate. As of 2016, 2048 bit is a common and typical selection.
Data Encryption Algorithms
AES-256-GCM
AES-128-GCM
CHACHA20-POLY1305
List of algorithms clients can negotiate to encrypt traffic between endpoints. The best practice is to use the exact algorithms listed above, in that order. Certain algorithms will perform better on different hardware, depending on the availability of supported VPN accelerator chips. Edit the server after
Tapez ici pour effectuer une
27°C Temps dégagé
22:18
25/01/2026


GNS3 VM
Windows 10
pfSense.home.arpa - Wizard: Op
Non sécurisé | 192.168.1.1/wizard.php?xml=openvpn_wizard.xml
Fallback Data Encryption Algorithm
AES-256-CBC (256 bit key, 128 bit block)
The algorithm used to encrypt traffic between endpoints when data encryption negotiation is diabled or fails.
Auth Digest Algorithm
SHA256 (256-bit)
The method used to authenticate traffic between endpoints. This setting must match on the client and server side, but is otherwise set however desired.
Hardware Crypto
No Hardware Crypto Acceleration
The hardware cryptographic accelerator to use for this VPN connection, if any.
Tunnel Settings
IPv4 Tunnel Network
10.8.10.0/24
This is the virtual network used for private communications between this server and client hosts expressed using CIDR notation (eg. 10.0.8.0/24). The first network address will be assigned to the server virtual interface. The remaining network addresses will be assigned to connecting clients.
Redirect IPv4 Gateway
Force all client generated traffic through the tunnel.
IPv4 Local Network
192.168.1.0/24
This is the network that will be accessible from the remote endpoint, expressed as a CIDR range. 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
5
Specify the maximum number of clients allowed to concurrently connect to this server.
Tapez ici pour effectuer une
27°C Temps dégagé
22:19
25/01/2026


GNS3 VM
Windows 10
pfSense.home.arpa - Wizard: Op
Non sécurisé | 192.168.1.1/wizard.php?xml=openvpn_wizard.xml
Wizard / OpenVPN Remote Access Server Setup / Firewall Rule Configuration
Step 10 of 11
Firewall Rule Configuration
OpenVPN Remote Access Server Firewall Rules
Rules control passing or blocking network traffic as it flows through the firewall.
Rules must be added which allow traffic to reach the OpenVPN server IP address and port, as well as to allow traffic from connected clients inside the OpenVPN tunnel.
The options on this step can add automatic rules to pass this traffic, or rules can be configured manually after completing the wizard.
Traffic from clients to server
Firewall Rule
Add a rule to permit connections to this OpenVPN server instance from clients anywhere on the Internet.
Traffic from clients through VPN
OpenVPN rule
Add a rule to allow all traffic from connected clients to pass inside the VPN tunnel.
Next
Tapez ici pour effectuer une
27°C Temps dégagé
22:22
25/01/2026

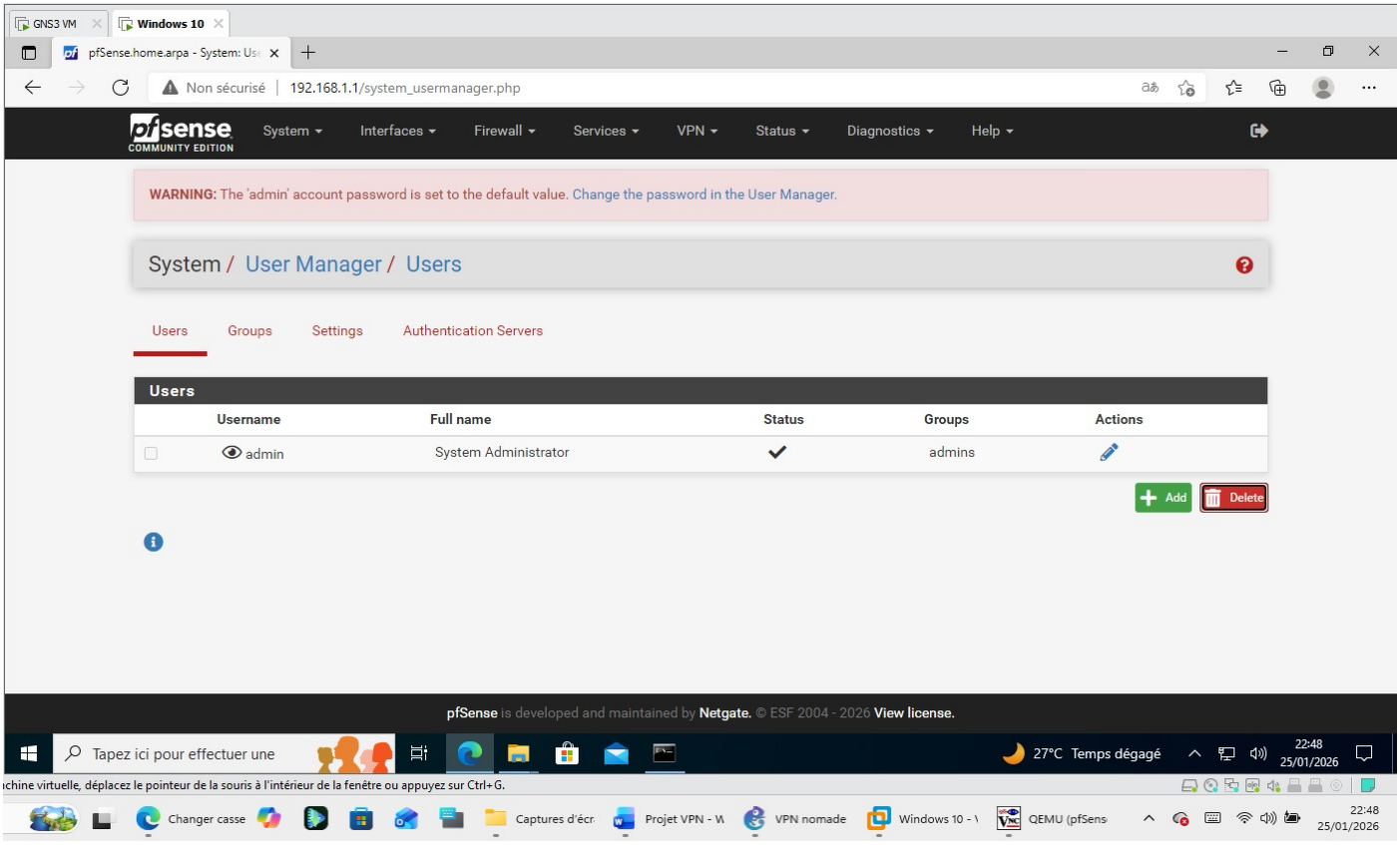


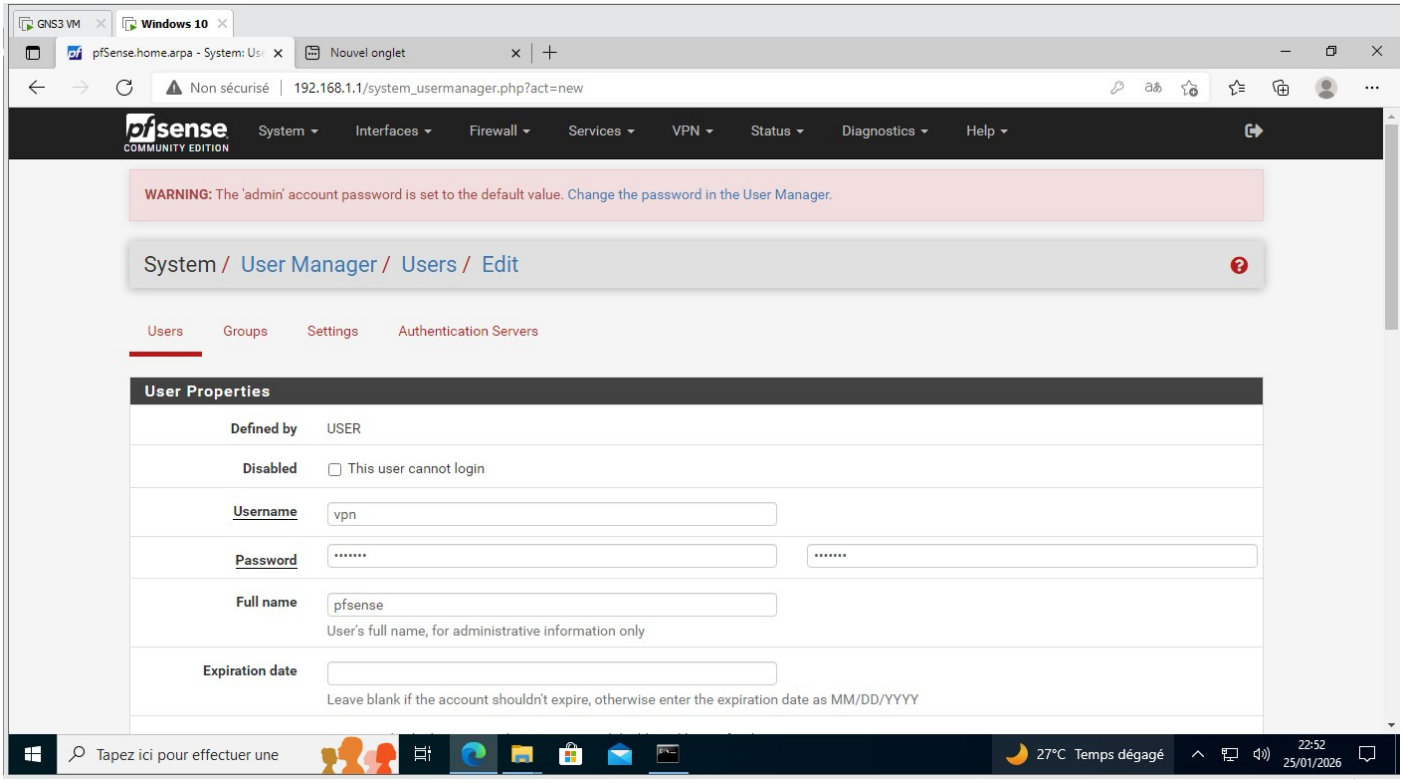


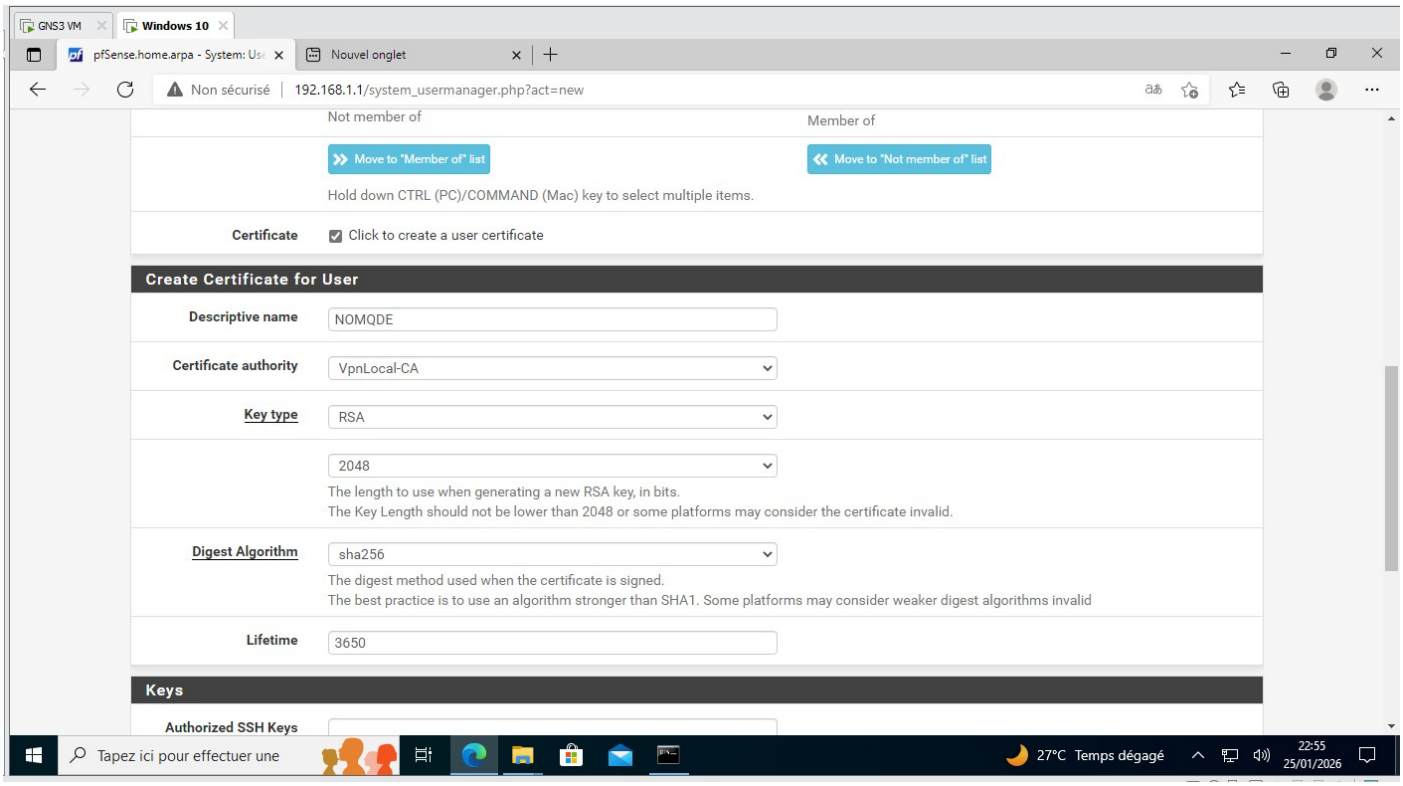
7.1 Création des utilisateurs VPN :

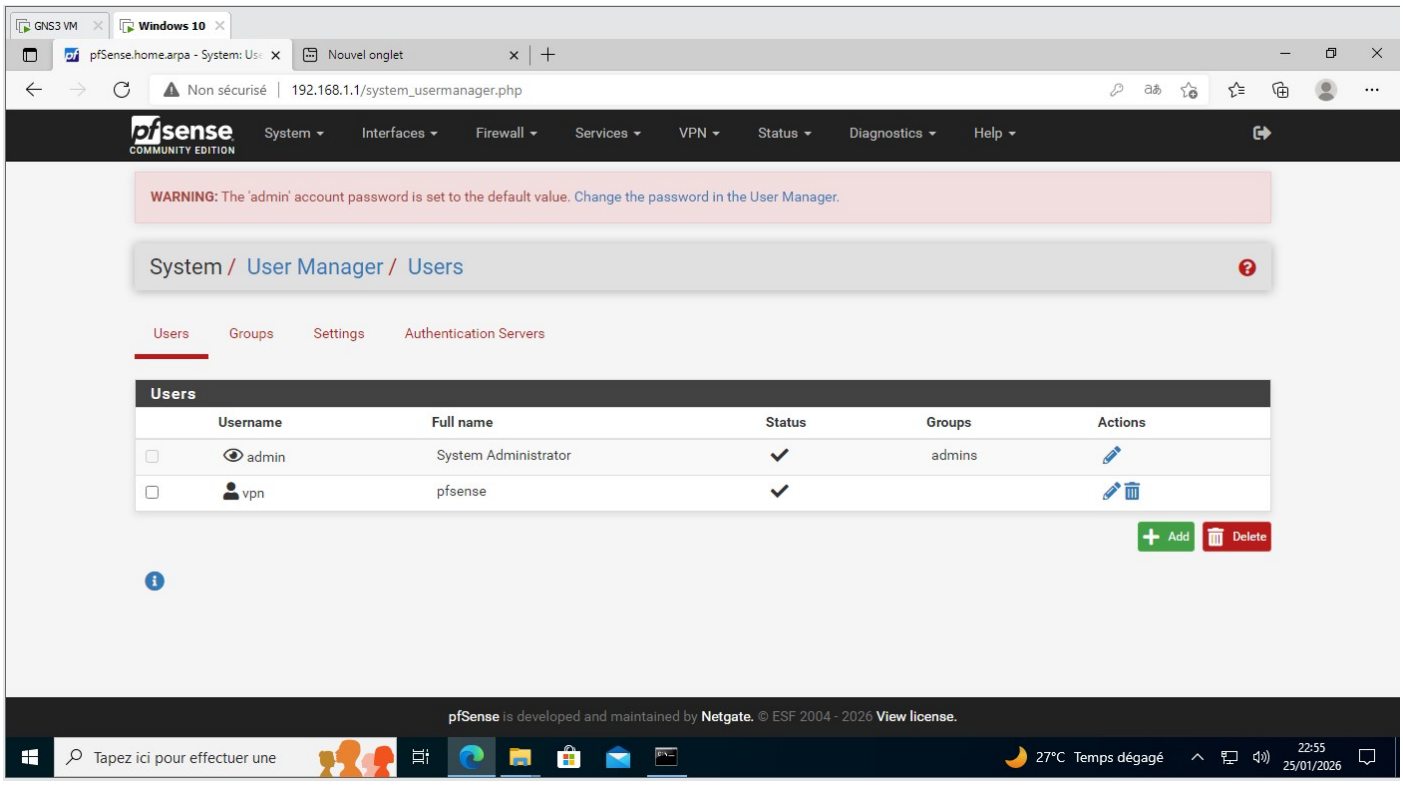
Chaque utilisateur VPN est enregistré dans pfSense à l'aide d'un identifiant unique et d'un mot de passe personnel. À chaque compte utilisateur est associé un certificat numérique généré par l'autorité de certification interne, ce qui permet de renforcer considérablement la sécurité des accès. Cette méthode de gestion offre un contrôle strict des connexions au VPN, permet la révocation rapide d'un

utilisateur en cas de compromission ou de départ, et garantit une authentification forte avant toute autorisation d'accès au réseau interne.





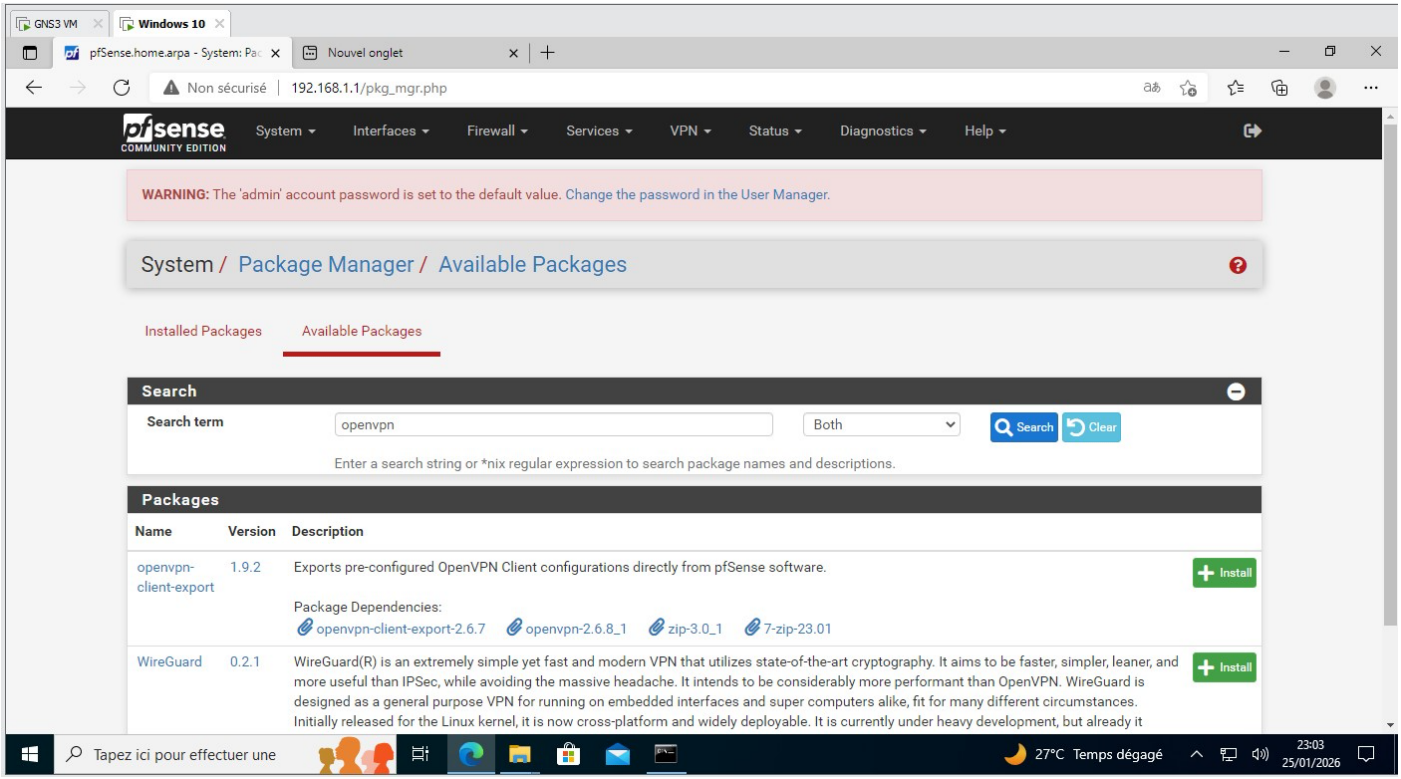


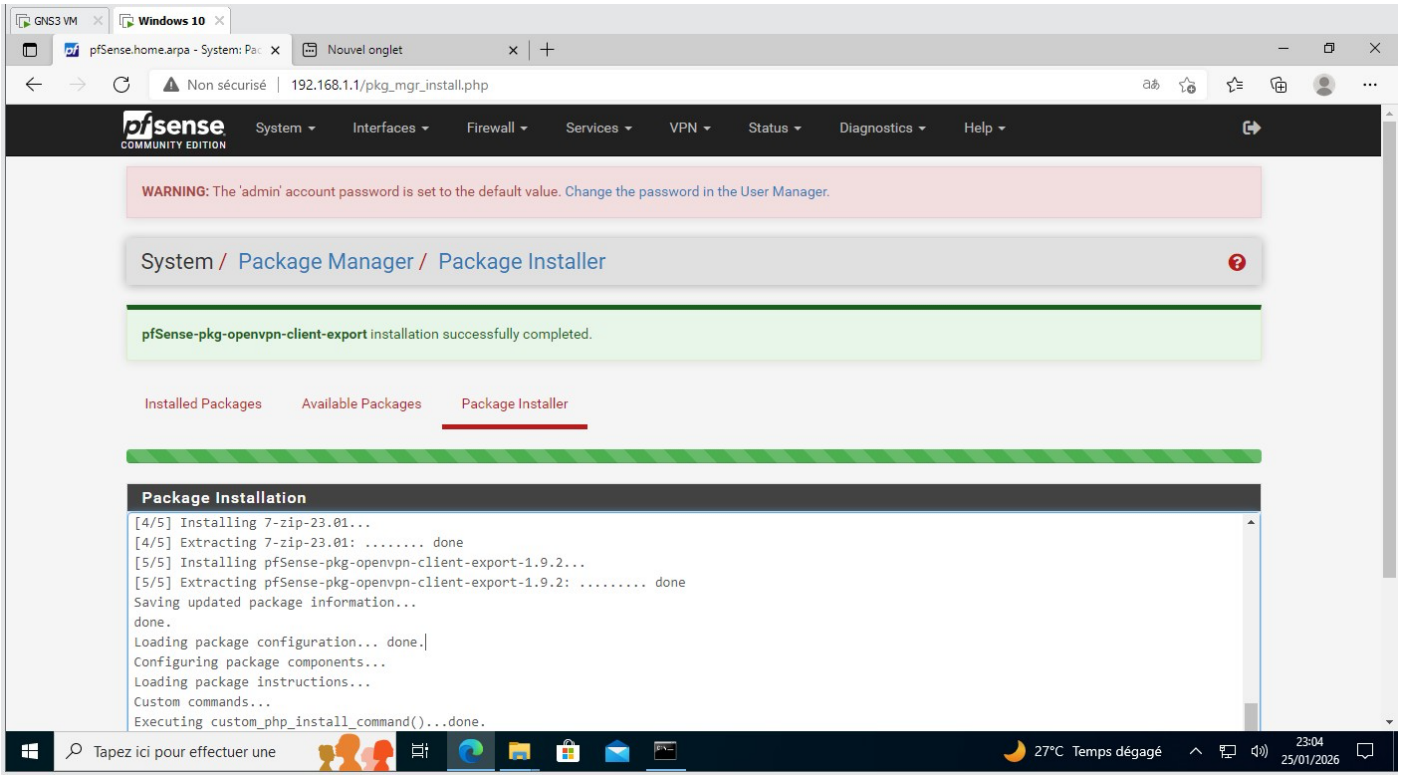


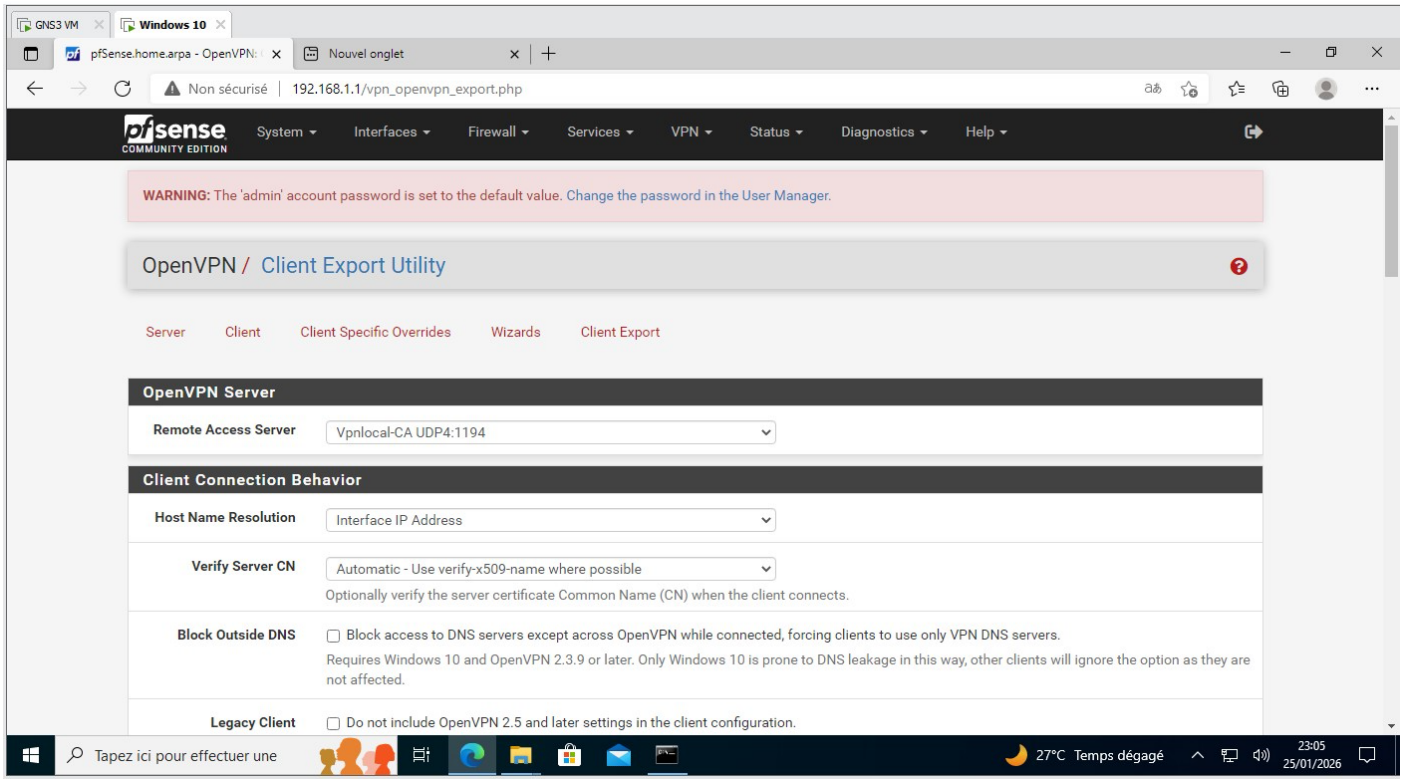
7.2 Configuration du client VPN sur Windows 10 :

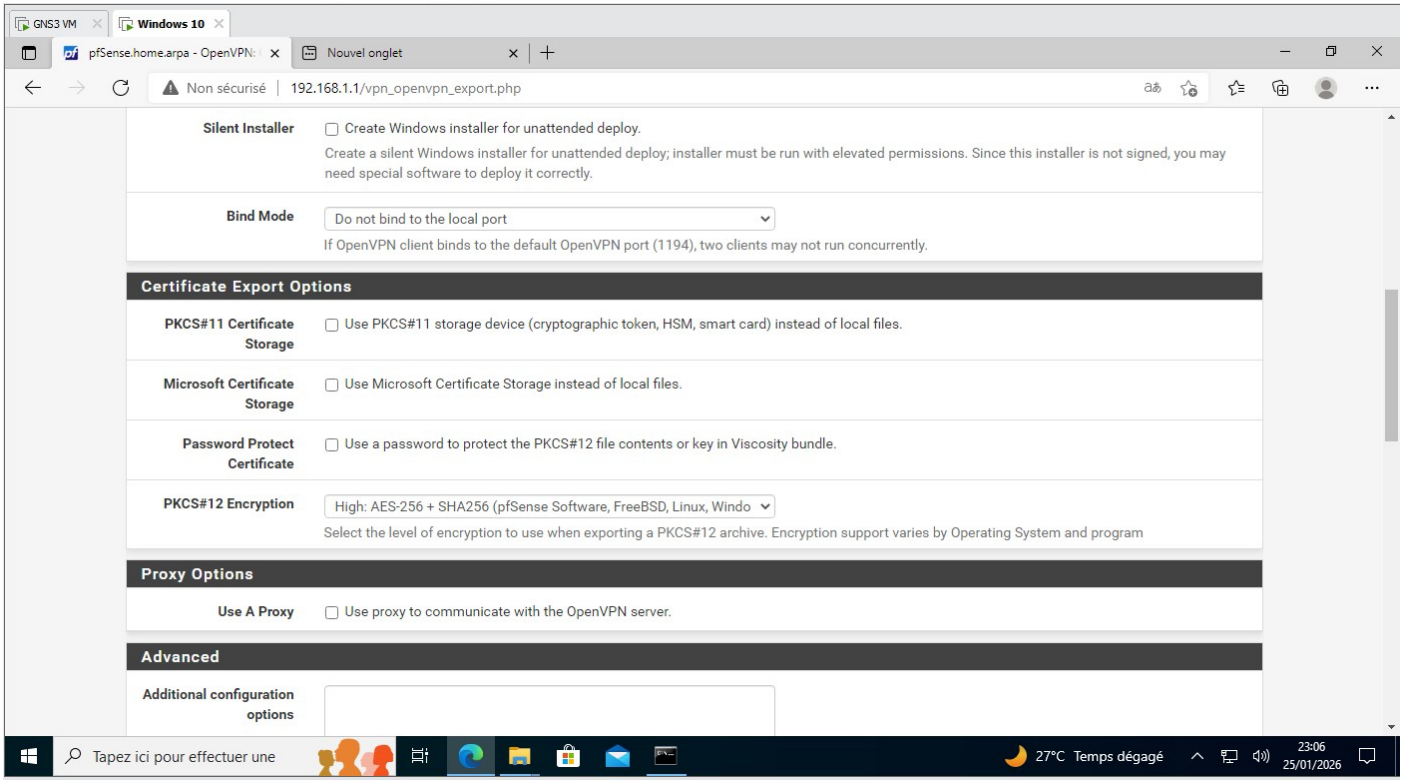
Sur la machine virtuelle Windows 10, le client OpenVPN est tout d'abord installé afin de permettre la connexion au serveur VPN pfSense. Les fichiers de configuration générés et fournis par pfSense, incluant le certificat utilisateur, la clé de sécurité et le fichier de configuration du serveur, sont ensuite importés dans le client OpenVPN. Une fois ces éléments correctement configurés, le client VPN est lancé pour établir la connexion sécurisée avec le serveur pfSense. Après l'établissement du tunnel

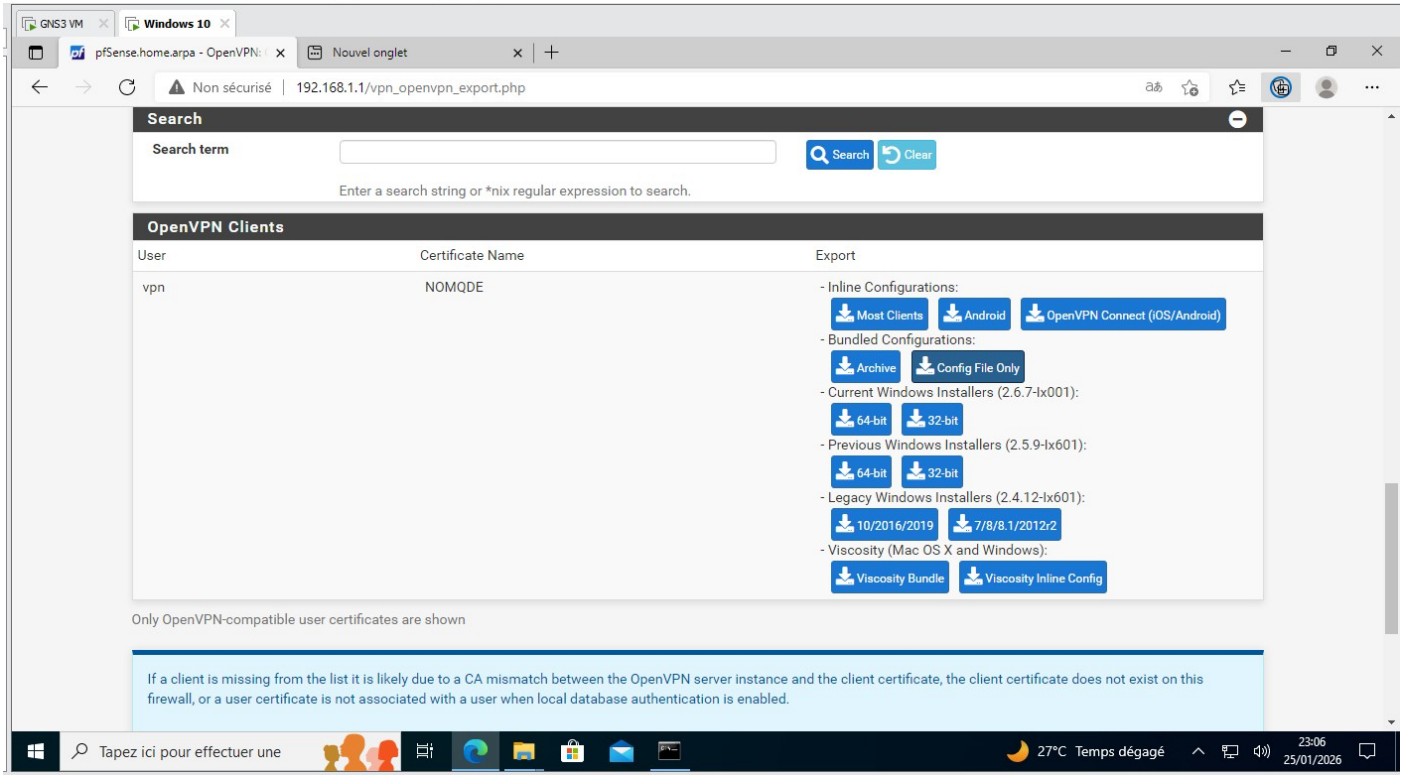
VPN, l'utilisateur distant se voit attribuer une adresse IP du réseau VPN et peut accéder de manière sécurisée aux ressources du réseau interne.

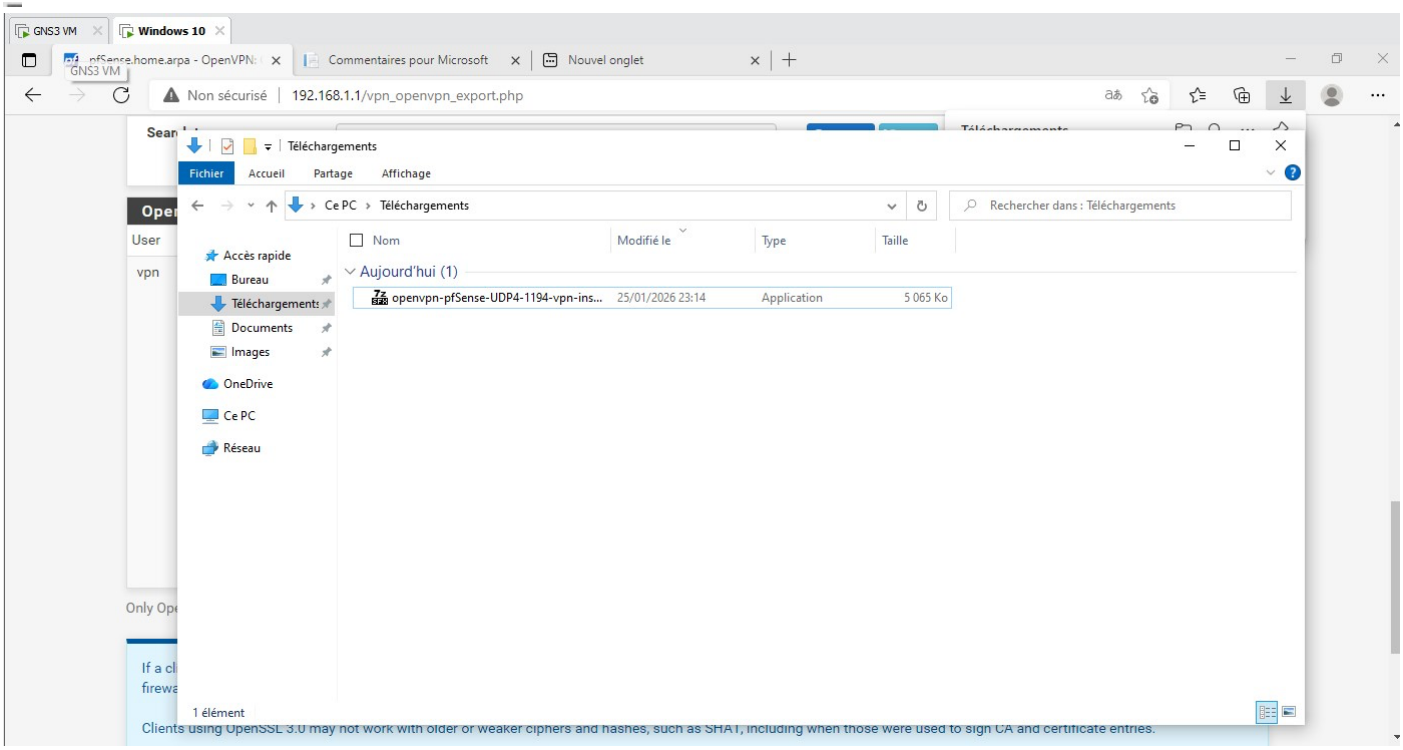


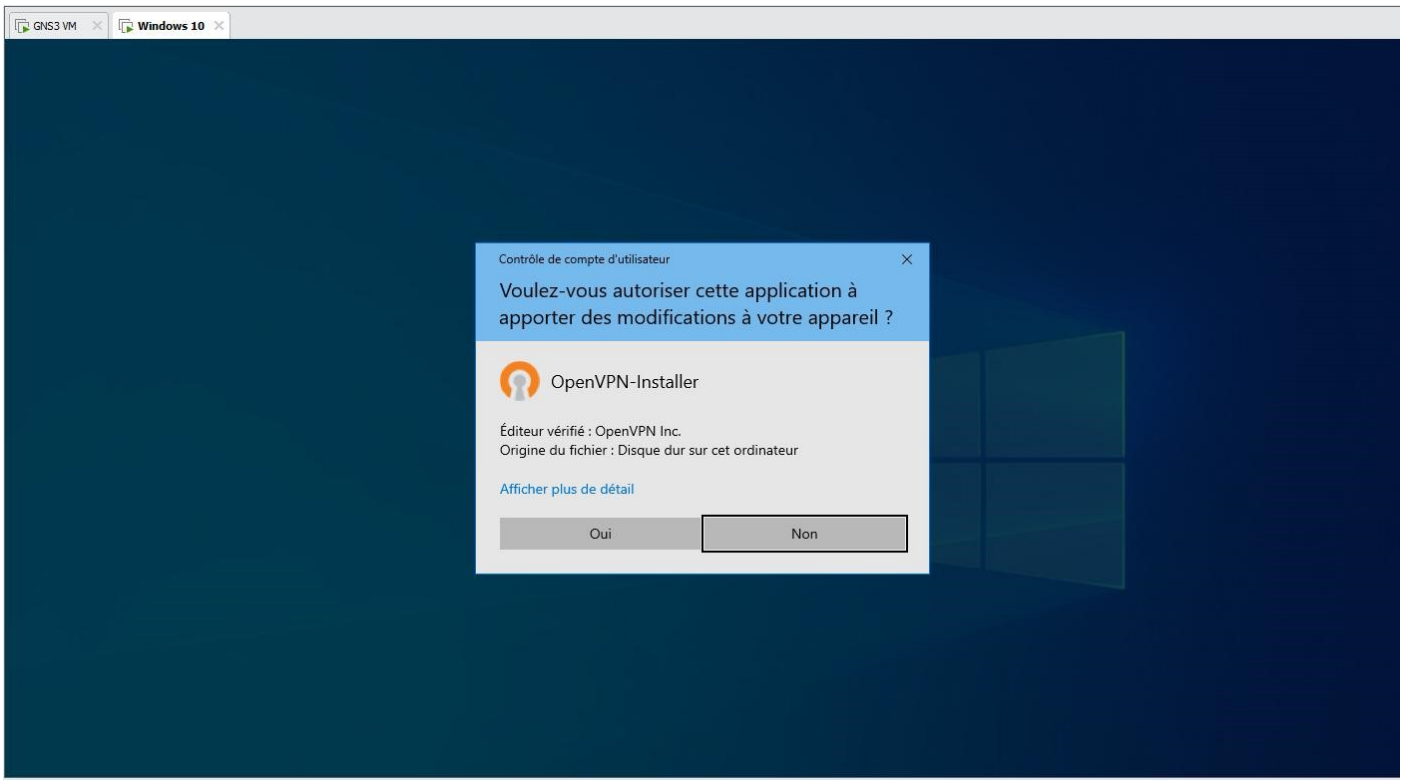


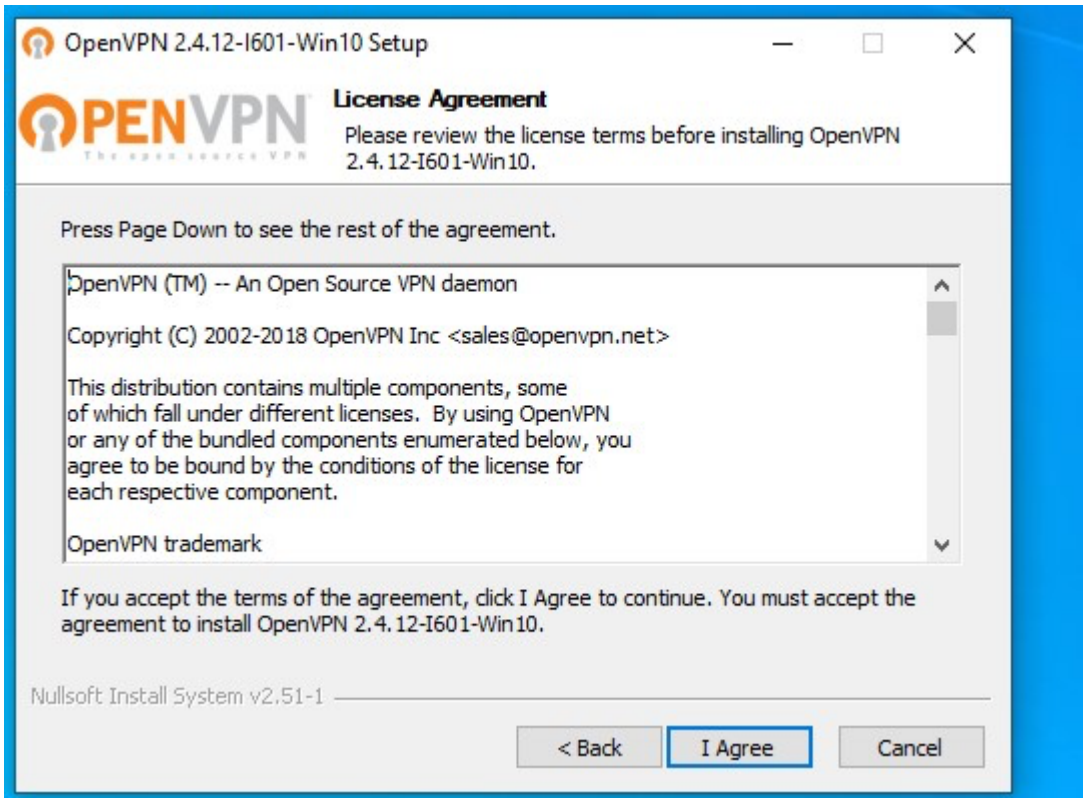

GNS3 VM
Windows 10
pfSense.home.arpa - OpenVPN:
Nouvel onglet
Non sécurisé | 192.168.1.1/vpn_openvpn_export.php
pfsense COMMUNITY EDITION
System
Interfaces
Firewall
Services
VPN
Status
Diagnostics
Help
WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.
OpenVPN / Client Export Utility
Server
Client
Client Specific Overrides
Wizards
Client Export
OpenVPN Server
Remote Access Server
Vpnlocal-CA 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.
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.
Legacy Client
Do not include OpenVPN 2.5 and later settings in the client configuration.
Tapez ici pour effectuer une
27°C Temps dégagé
23:05
25/01/2026

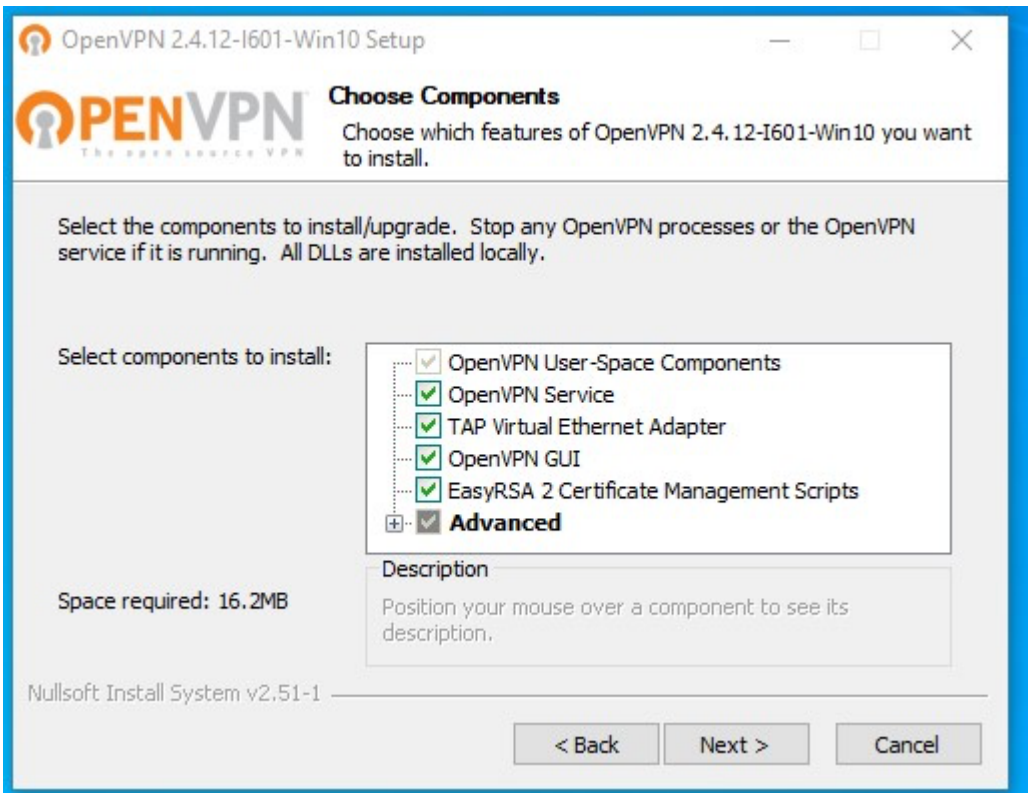

GNS3 VM
Windows 10
pfSense.home.arpa - OpenVPN:
Nouvel onglet
Non sécurisé | 192.168.1.1/vpn_openvpn_export.php
Silent Installer
Create Windows installer for unattended deploy.
Create a silent Windows installer for unattended deploy; installer must be run with elevated permissions. Since this installer 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 Storage
Use Microsoft Certificate Storage instead of local files.
Password Protect Certificate
Use a password to protect the PKCS#12 file contents or key in Viscosity bundle.
PKCS#12 Encryption
High: AES-256 + SHA256 (pfSense Software, FreeBSD, Linux, Windo
Select the level of encryption to use when exporting a PKCS#12 archive. Encryption support varies by Operating System and program
Proxy Options
Use A Proxy
Use proxy to communicate with the OpenVPN server.
Advanced
Additional configuration options
Tapez ici pour effectuer une
27°C Temps dégagé
23:06
25/01/2026

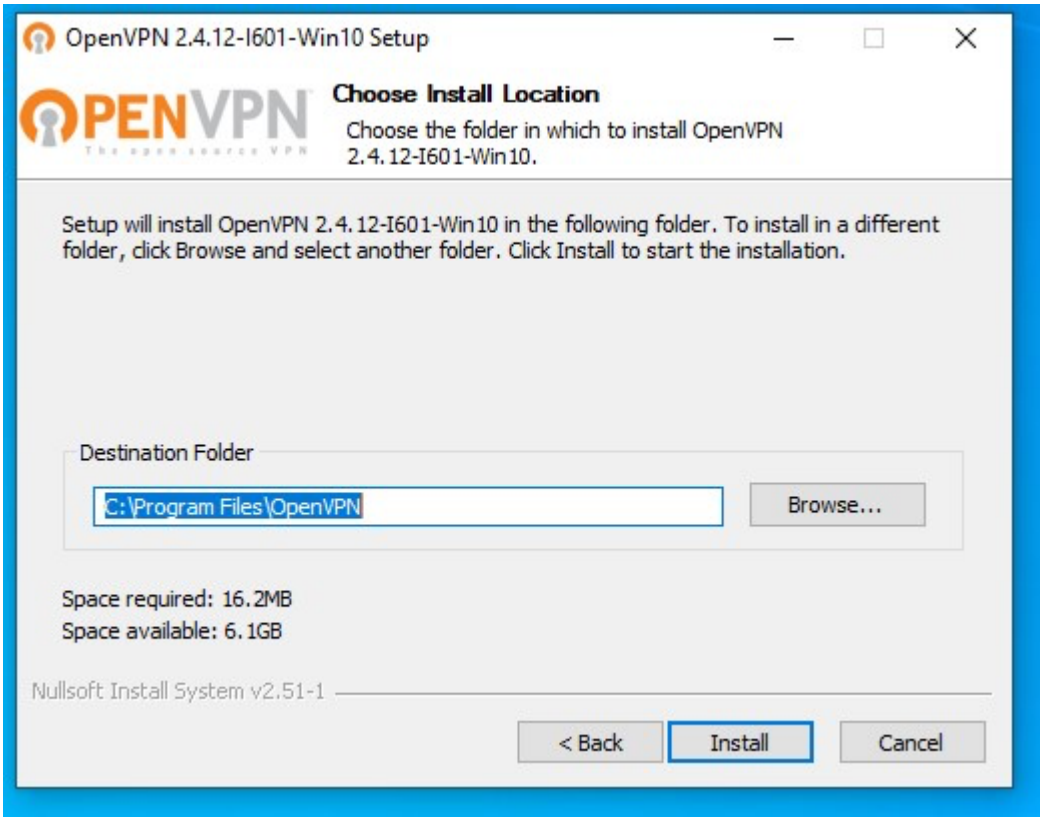

GNS3 VM
Windows 10
pfSense.home.arpa - OpenVPN
Nouvel onglet
Non sécurisé | 192.168.1.1/vpn_openvpn_export.php
Search
Search term
Search
Clear
Enter a search string or *nix regular expression to search.
OpenVPN Clients
User
Certificate Name
Export
vpn
NOMQDE
- Inline Configurations:
Most Clients
Android
OpenVPN Connect (iOS/Android)
- Bundled Configurations:
Archive
Config File Only
- Current Windows Installers (2.6.7-Ix001):
64-bit
32-bit
- Previous Windows Installers (2.5.9-Ix601):
64-bit
32-bit
- Legacy Windows Installers (2.4.12-Ix601):
10/2016/2019
7/8/8.1/2012r2
- Viscosity (Mac OS X and Windows):
Viscosity Bundle
Viscosity Inline Config
Only OpenVPN-compatible user certificates are shown
If a client is missing from the list it is likely due to a CA mismatch between the OpenVPN server instance and the client certificate, the client certificate does not exist on this firewall, or a user certificate is not associated with a user when local database authentication is enabled.
Tapez ici pour effectuer une
27°C Temps dégagé
23:06
25/01/2026

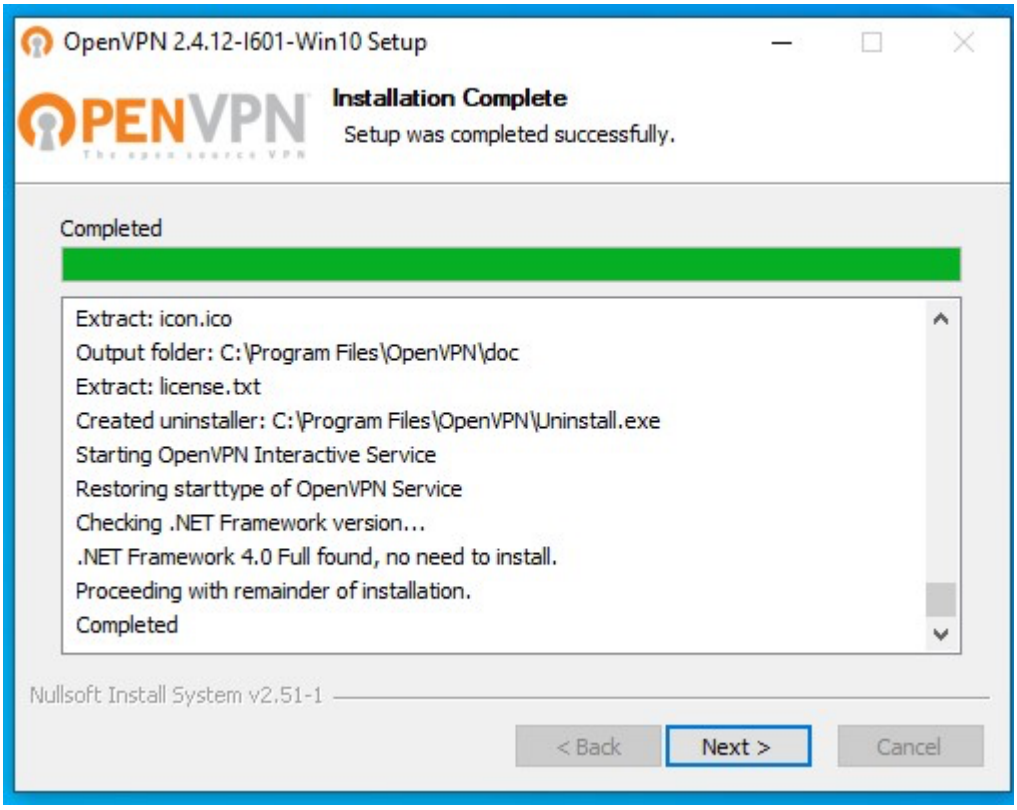

GNS3 VM
Windows 10
pfSense.home.arpa - OpenVPN
Commentaires pour Microsoft
Nouvel onglet
Non sécurisé | 192.168.1.1/vpn_openvpn_export.php
Téléchargements
Fichier
Accueil
Partage
Affichage
Ce PC › Téléchargements
Rechercher dans : Téléchargements
Accès rapide
Bureau
Téléchargements
Documents
Images
OneDrive
Ce PC
Réseau
Nom
Modifié le
Type
Taille
Aujourd'hui (1)
openvpn-pfSense-UDP4-1194-vpn-ins...
25/01/2026 23:14
Application
5 065 Ko
1 élément
Clients using OpenSSL 3.0 may not work with older or weaker ciphers and hashes, such as SHA1, including when those were used to sign CA and certificate entries.

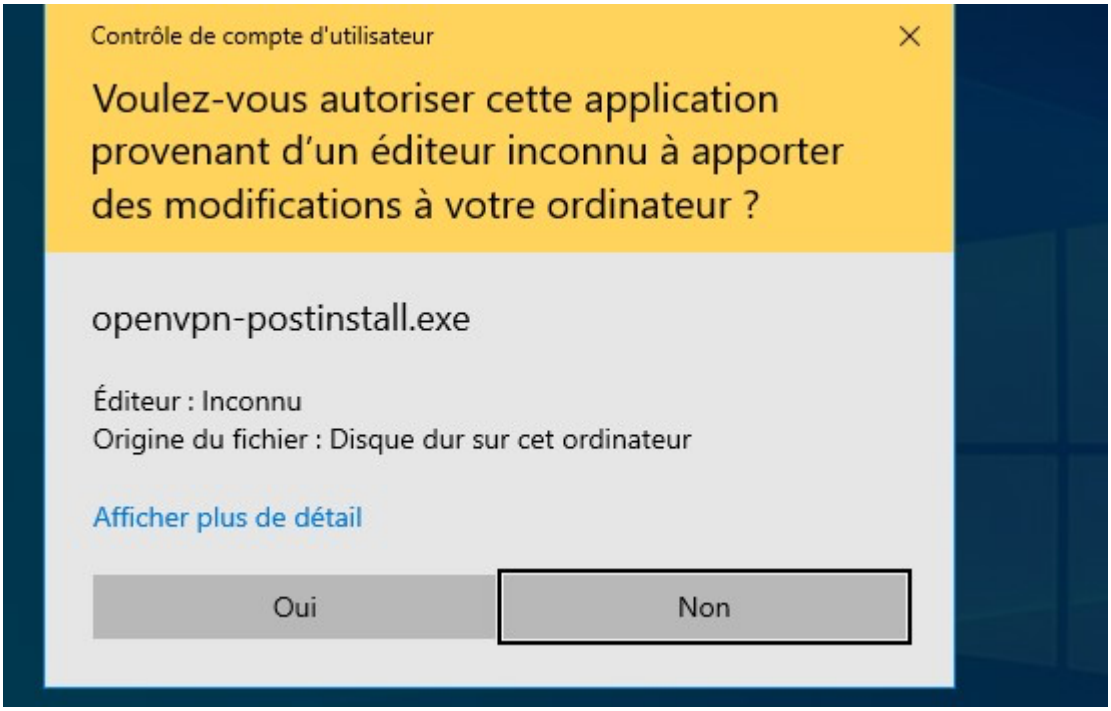

GNS3 VM
Windows 10
Contrôle de compte d'utilisateur
Voulez-vous autoriser cette application à apporter des modifications à votre appareil ?
OpenVPN-Installer
Éditeur vérifié : OpenVPN Inc.
Origine du fichier : Disque dur sur cet ordinateur
Afficher plus de détail
Oui
Non

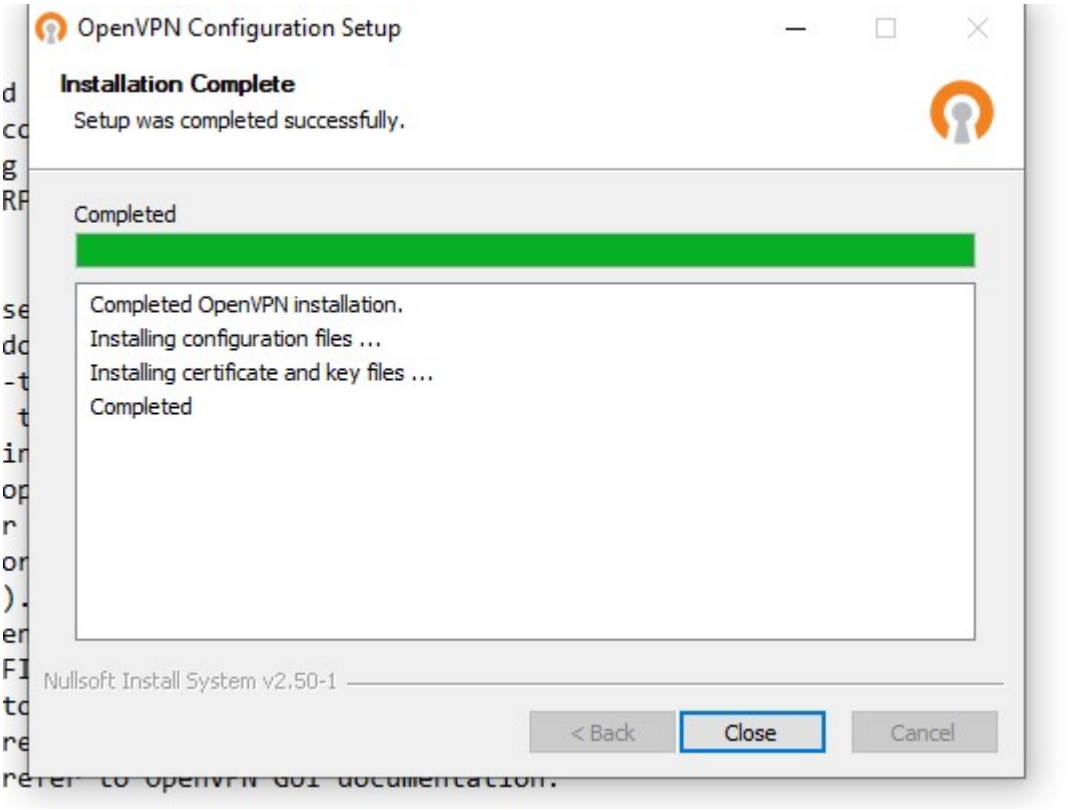

OpenVPN 2.4.12-I601-Win10 Setup
License Agreement
Please review the license terms before installing OpenVPN 2.4.12-I601-Win10.
Press Page Down to see the rest of the agreement.
OpenVPN (TM) -- An Open Source VPN daemon
Copyright (C) 2002-2018 OpenVPN Inc <sales@openvpn.net>
This distribution contains multiple components, some of which fall under different licenses. By using OpenVPN or any of the bundled components enumerated below, you agree to be bound by the conditions of the license for each respective component.
OpenVPN trademark
If you accept the terms of the agreement, click I Agree to continue. You must accept the agreement to install OpenVPN 2.4.12-I601-Win10.
Nullsoft Install System v2.51-1
< Back
I Agree
Cancel


OpenVPN 2.4.12-I601-Win10 Setup
OPENVPN
The open source VPN
Choose Components
Choose which features of OpenVPN 2.4.12-I601-Win10 you want to install.
Select the components to install/upgrade. Stop any OpenVPN processes or the OpenVPN service if it is running. All DLLs are installed locally.
Select components to install:
OpenVPN User-Space Components
OpenVPN Service
TAP Virtual Ethernet Adapter
OpenVPN GUI
EasyRSA 2 Certificate Management Scripts
Advanced
Description
Position your mouse over a component to see its description.
Space required: 16.2MB
Nullsoft Install System v2.51-1
< Back
Next >
Cancel


OpenVPN 2.4.12-I601-Win10 Setup
OPENVPN
The open source VPN
Choose Install Location
Choose the folder in which to install OpenVPN 2.4.12-I601-Win10.
Setup will install OpenVPN 2.4.12-I601-Win10 in the following folder. To install in a different folder, click Browse and select another folder. Click Install to start the installation.
Destination Folder
C:\Program Files\OpenVPN
Browse...
Space required: 16.2MB
Space available: 6.1GB
Nullsoft Install System v2.51-1
< Back
Install
Cancel

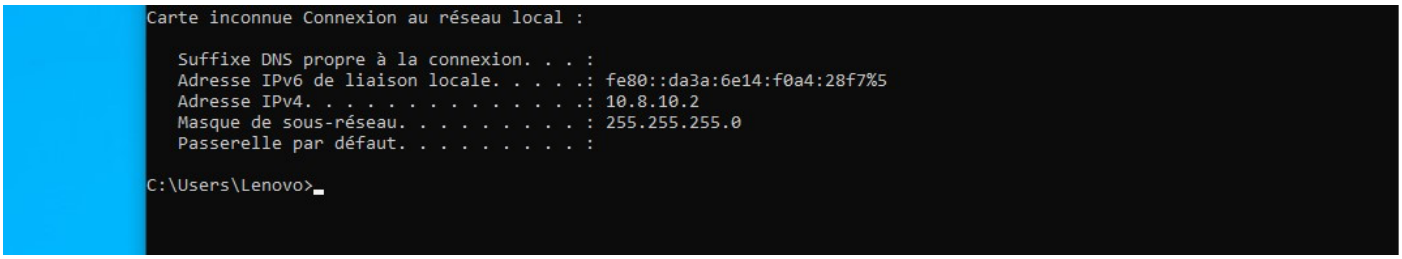

OpenVPN 2.4.12-I601-Win10 Setup
OPENVPN
Installation Complete
Setup was completed successfully.
Completed
Extract: icon.ico
Output folder: C:\Program Files\OpenVPN\doc
Extract: license.txt
Created uninstaller: C:\Program Files\OpenVPN\Uninstall.exe
Starting OpenVPN Interactive Service
Restoring starttype of OpenVPN Service
Checking .NET Framework version...
.NET Framework 4.0 Full found, no need to install.
Proceeding with remainder of installation.
Completed
Nullsoft Install System v2.51-1
< Back
Next >
Cancel

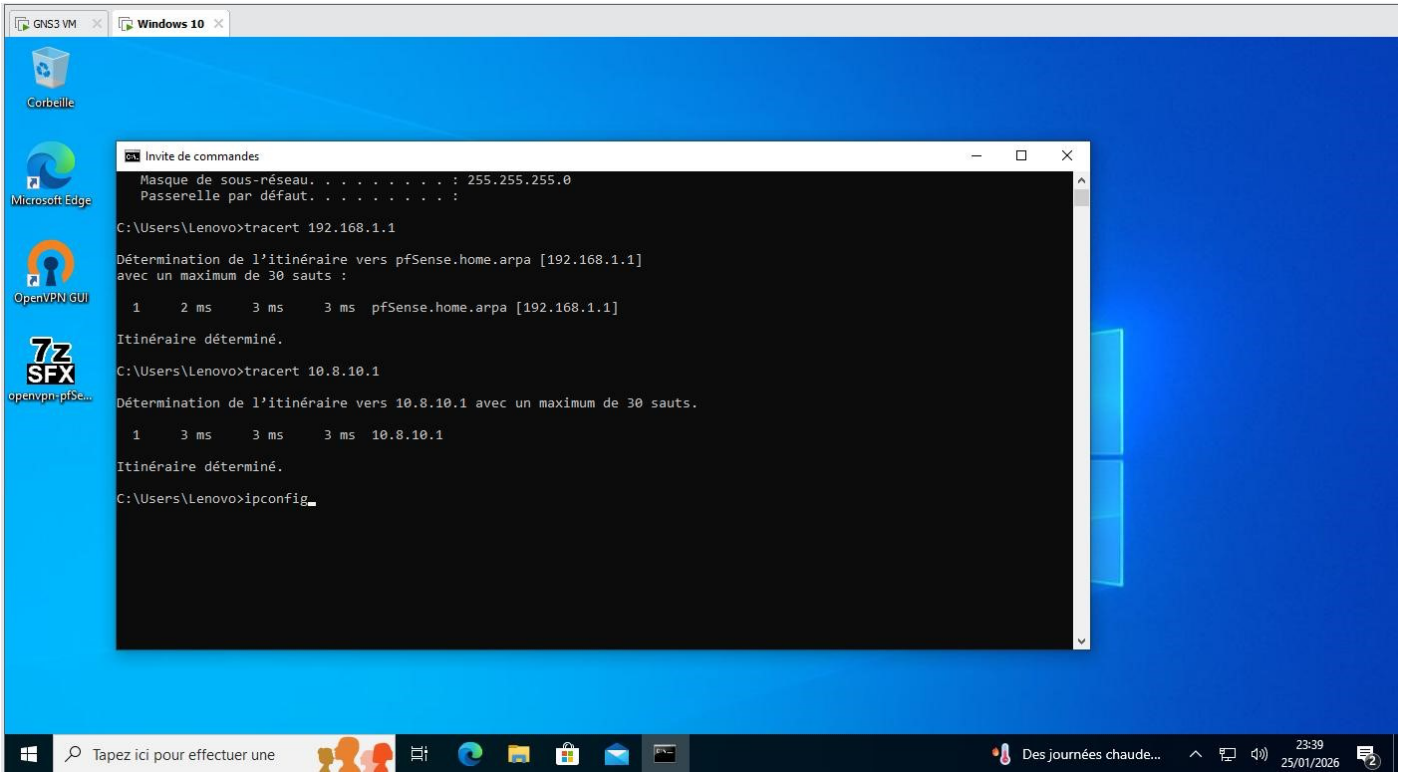

Contrôle de compte d'utilisateur
Voulez-vous autoriser cette application provenant d'un éditeur inconnu à apporter des modifications à votre ordinateur ?
openvpn-postinstall.exe
Éditeur : Inconnu
Origine du fichier : Disque dur sur cet ordinateur
Afficher plus de détail
Oui
Non



7.3 Tests et validation du VPN :

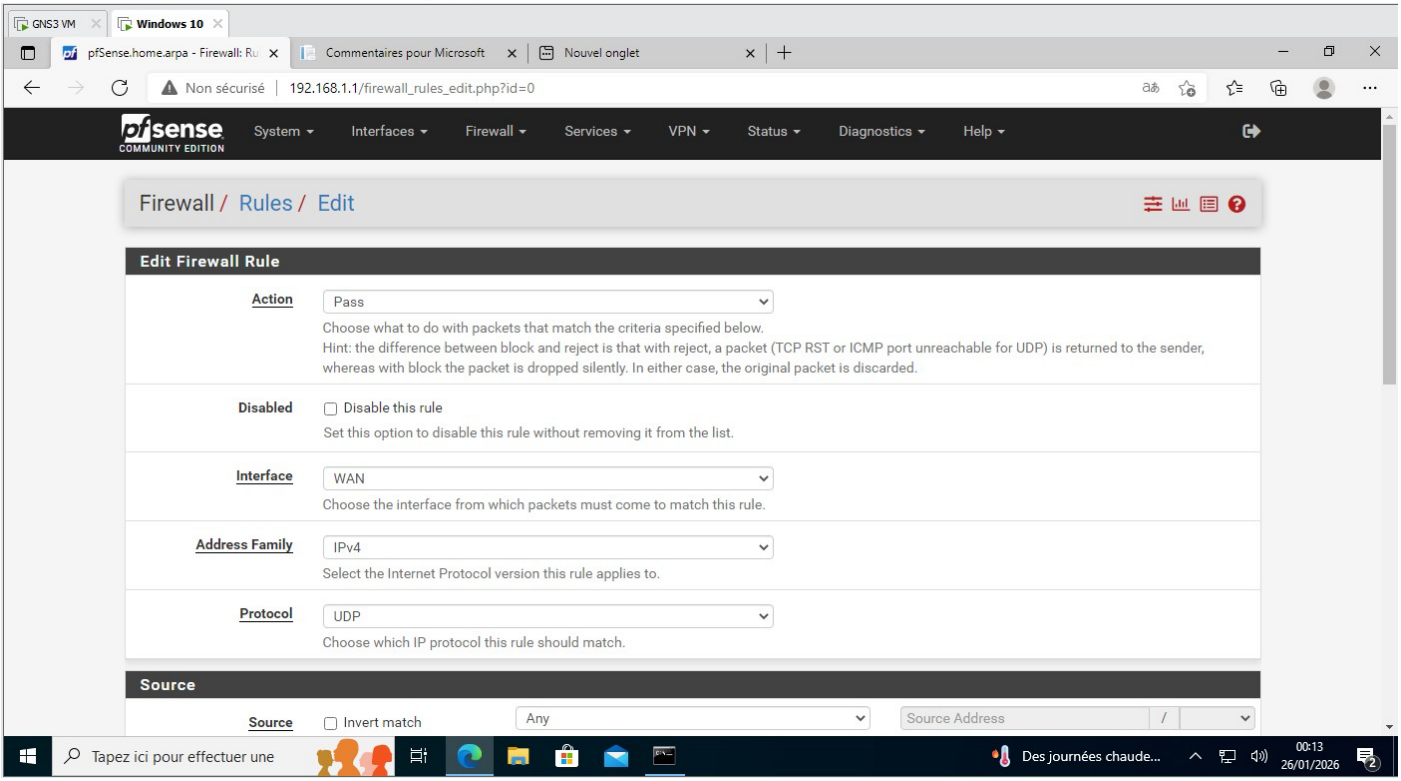
Afin de valider la solution VPN mise en place, plusieurs tests sont réalisés. La connexion VPN est établie avec succès depuis la machine Windows 10, confirmant la bonne communication avec le serveur pfSense. Une adresse IP appartenant au réseau VPN est correctement attribuée au client distant. Des tests de connectivité, notamment à l'aide de commandes de ping, ainsi que des essais d'accès aux ressources du réseau local sont effectués afin de vérifier le bon routage du trafic. Enfin, la sécurité et la confidentialité des échanges sont contrôlées, garantissant que les données transitent de manière chiffrée. L'ensemble de ces tests confirme le bon fonctionnement du VPN nomade et la sécurisation des communications sur le réseau interne.

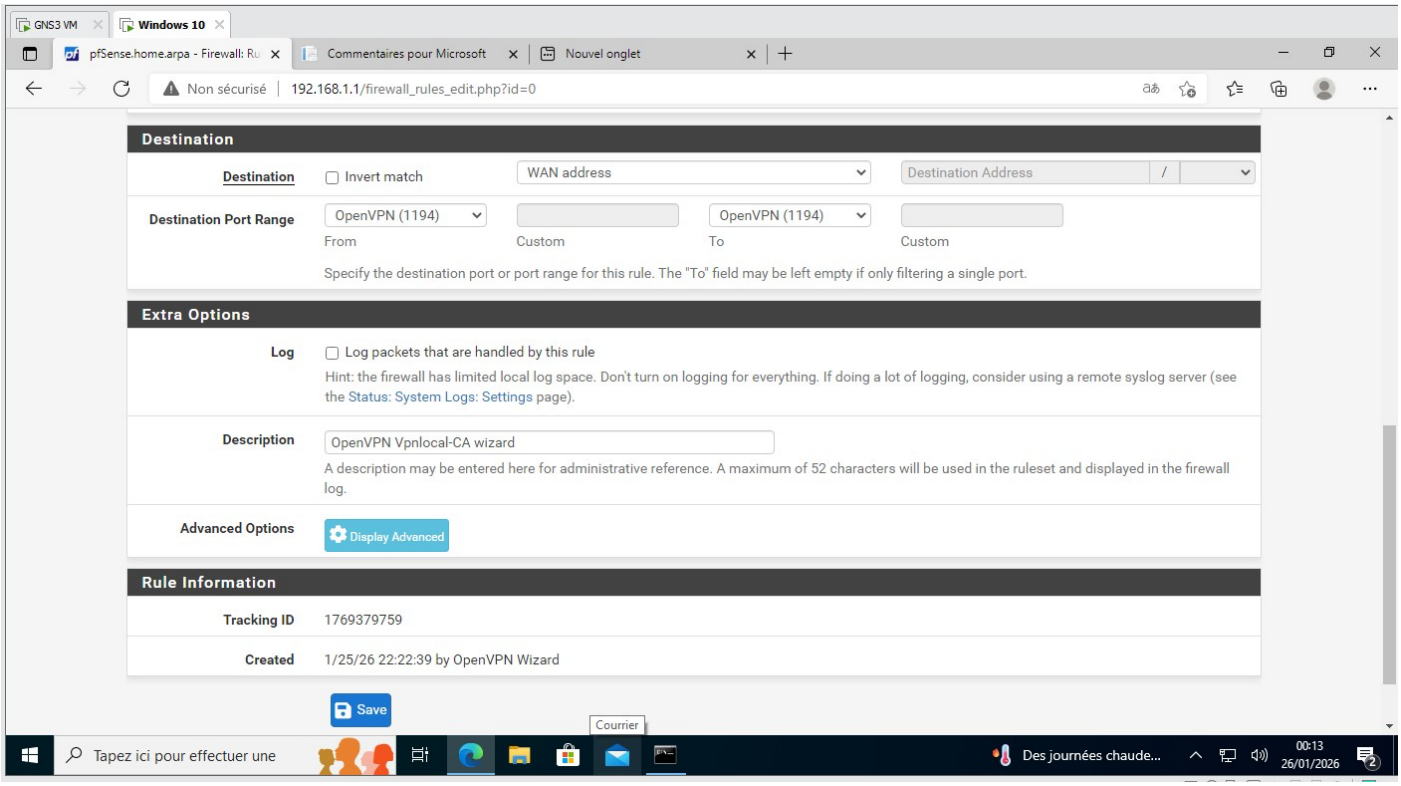




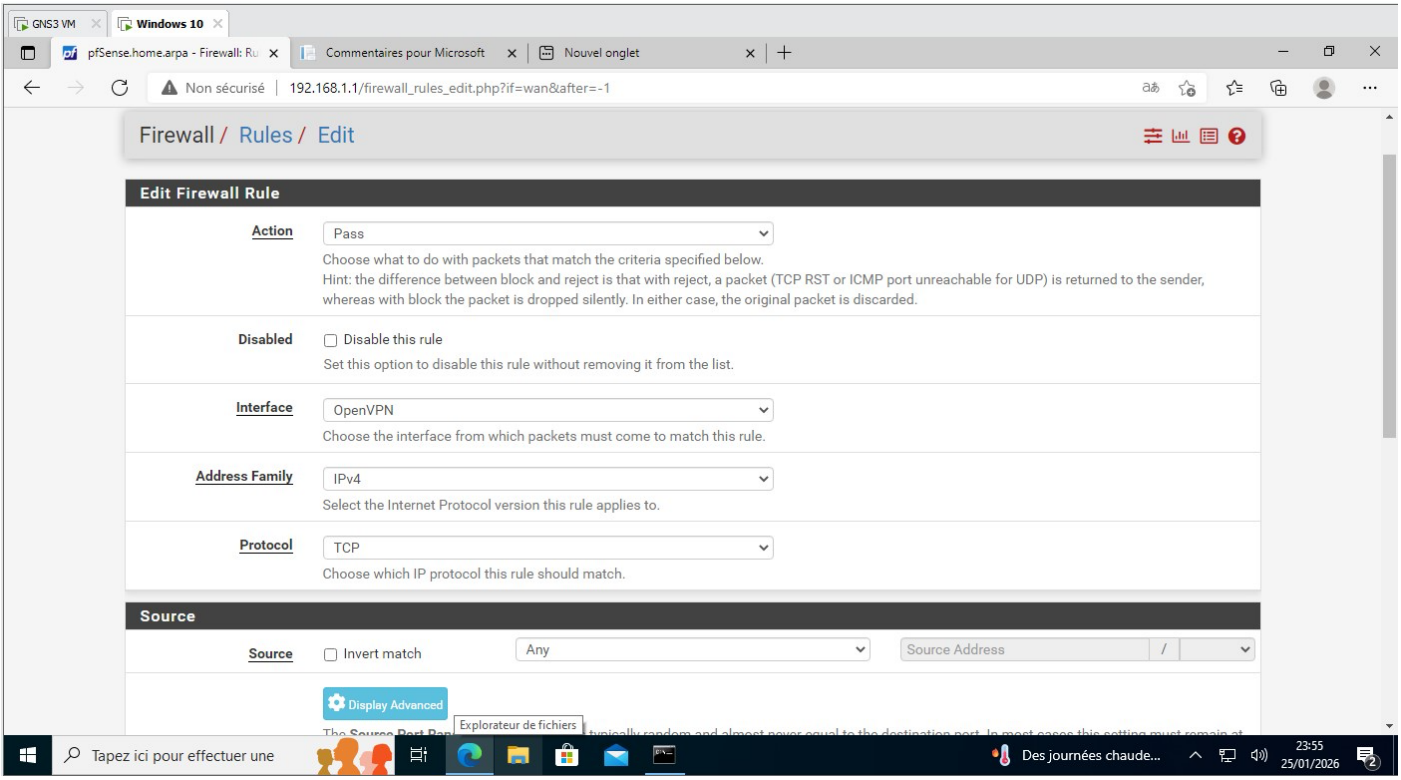
8 Sécurisation du réseau :

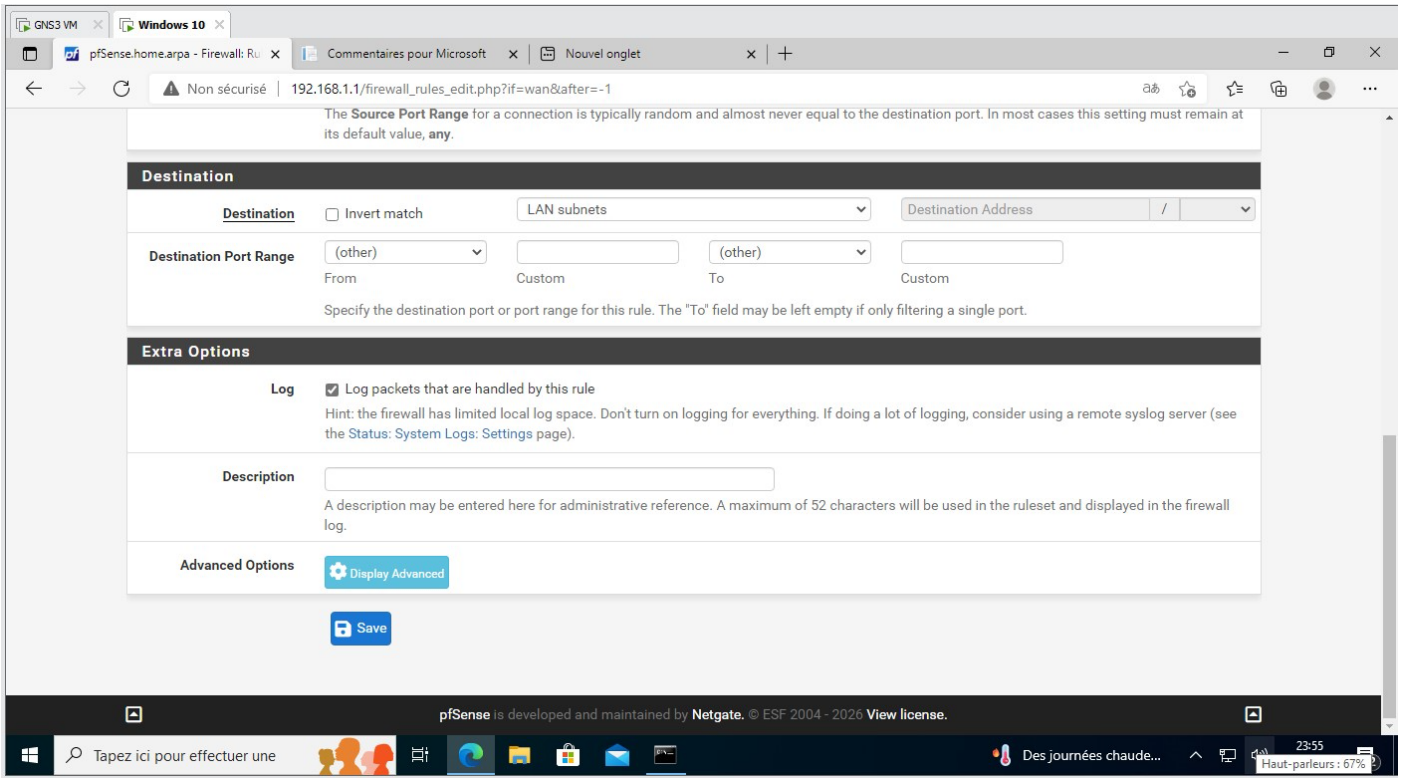
8.1 Configuration du pare-feu pfsense :

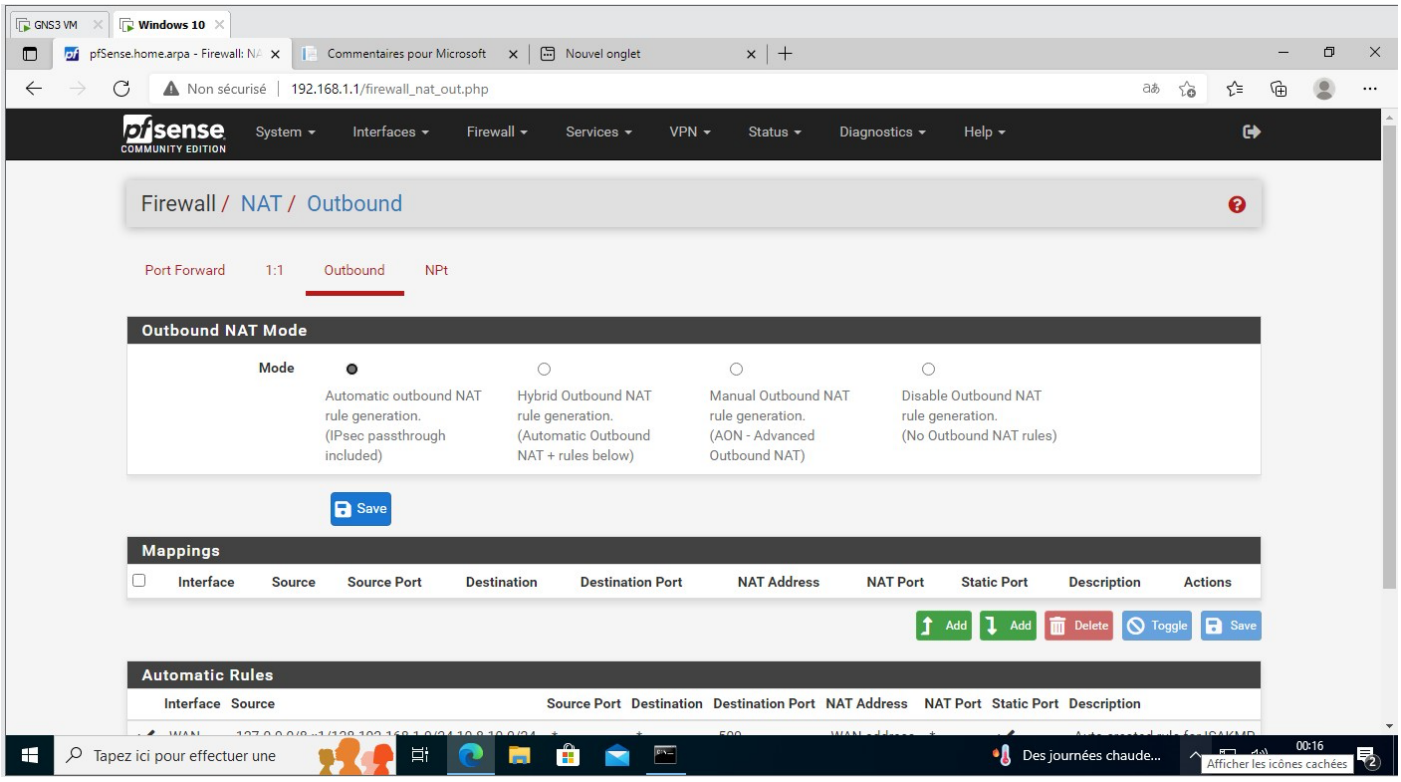


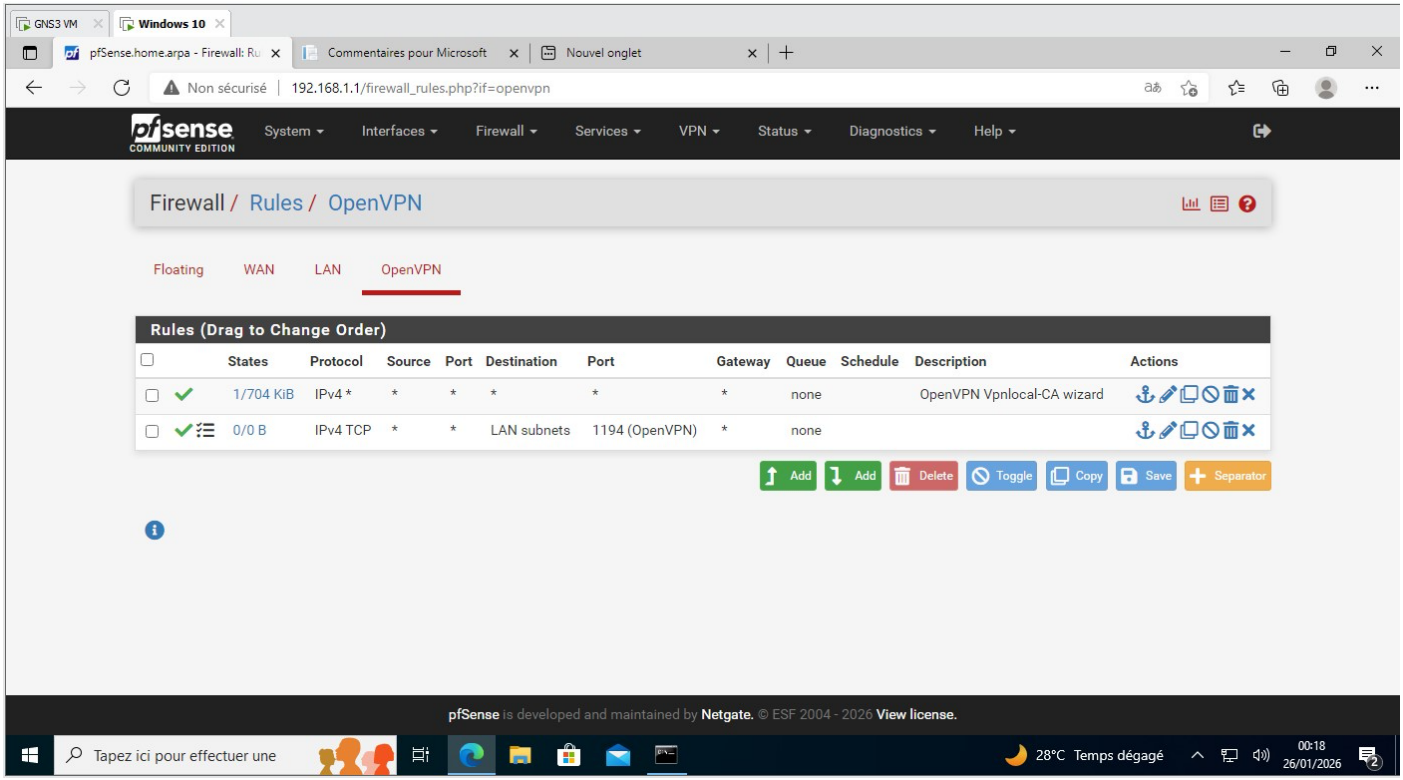


8.2 Règles de filtrage et NAT :

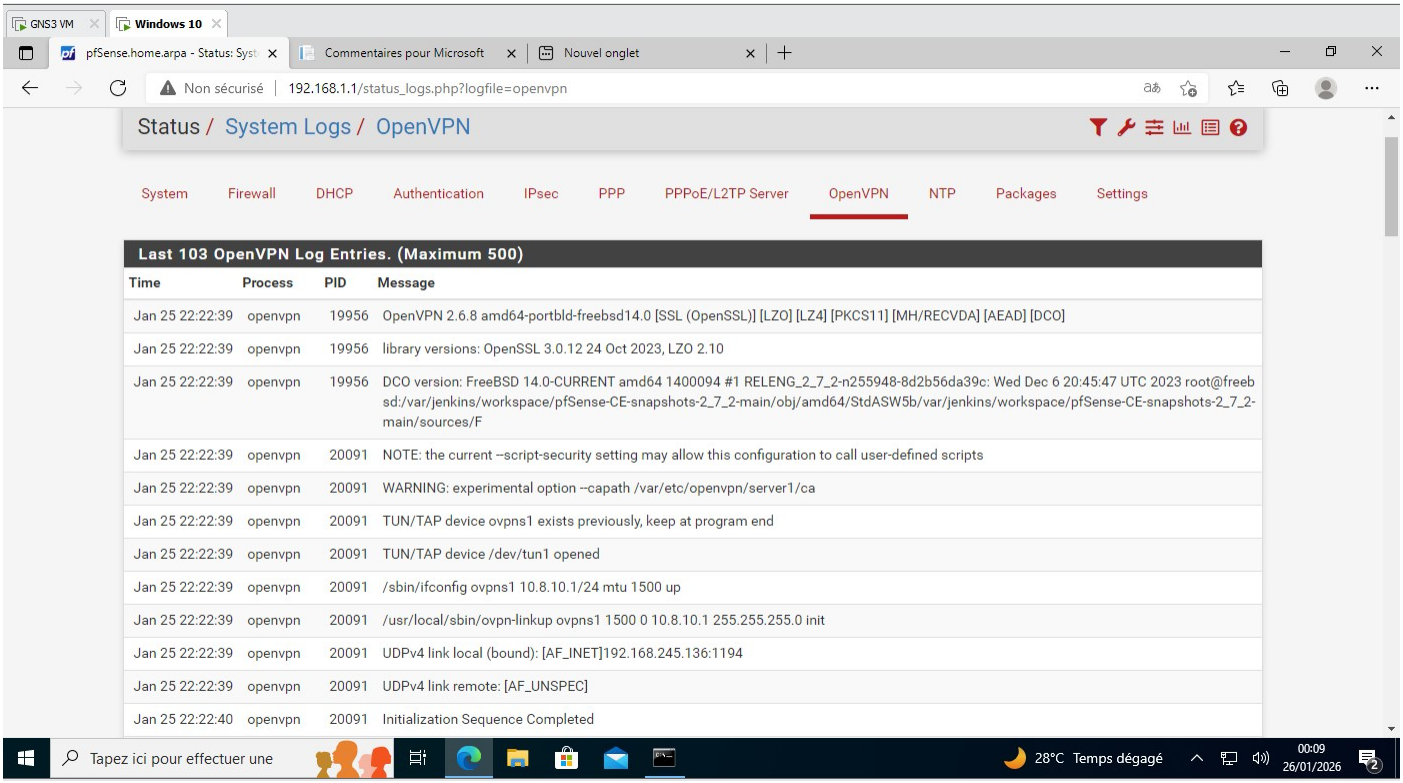



GNS3 VM
Windows 10
pfSense.home.arpa - Firewall: Ru
Commentaires pour Microsoft
Nouvel onglet
Non sécurisé | 192.168.1.1/firewall_rules_edit.php?if=wan&after=-1
The Source Port Range for a connection is typically random and almost never equal to the destination port. In most cases this setting must remain at its default value, any.
Destination
Destination
Invert match
LAN subnets
Destination Address
Destination Port Range
(other)
From
Custom
(other)
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.
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 ruleset and displayed in the firewall log.
Advanced Options
Display Advanced
Save
pfSense is developed and maintained by Netgate. © ESF 2004 - 2026 View license.
Tapez ici pour effectuer une
Des journées chaude...
23:55
Haut-parleurs : 67%


GNS3 VM
Windows 10
pfSense.home.arpa - Firewall: NA
Commentaires pour Microsoft
Nouvel onglet
Non sécurisé | 192.168.1.1/firewall_nat_out.php
pfsense COMMUNITY EDITION
System
Interfaces
Firewall
Services
VPN
Status
Diagnostics
Help
Firewall / NAT / Outbound
Port Forward
1:1
Outbound
NPt
Outbound NAT Mode
Mode
Automatic outbound NAT rule generation. (IPsec passthrough included)
Hybrid Outbound NAT rule generation. (Automatic Outbound NAT + rules below)
Manual Outbound NAT rule generation. (AON - Advanced Outbound NAT)
Disable Outbound NAT rule generation. (No Outbound NAT rules)
Save
Mappings
Interface
Source
Source Port
Destination
Destination Port
NAT Address
NAT Port
Static Port
Description
Actions
Add
Add
Delete
Toggle
Save
Automatic Rules
Interface
Source
Source Port
Destination
Destination Port
NAT Address
NAT Port
Static Port
Description
Tapez ici pour effectuer une
Des journées chaude...
00:16
Afficher les icônes cachées



8.3 Journalisation et supervision :



9 Tests, validation et analyse :

9.1 1. Scénarios de tests :

Plusieurs scénarios de tests ont été définis afin de vérifier l'ensemble des fonctionnalités du réseau et du VPN :

- **Test de connectivité Internet** :
  Vérification de l'accès à Internet depuis pfSense et depuis la machine Windows 10 sans connexion VPN.
- **Test de connexion VPN** :
  Tentative de connexion du client VPN Windows 10 au serveur OpenVPN hébergé sur pfSense.
- **Test d'attribution d'adresse IP VPN** :
  Vérification que le client VPN reçoit correctement une adresse IP du réseau VPN.
- **Test d'accès au réseau interne** :
  Vérification de la communication entre le client VPN et le réseau LAN (ping, accès aux services internes).
- **Test de sécurité** :
  Tentative d'accès au réseau interne sans authentification VPN afin de vérifier le blocage par le pare-feu.

9.2 Résultats des tests :

Les résultats obtenus lors des différents tests sont les suivants :

- La connexion Internet fonctionne correctement sur pfSense et sur la machine Windows 10.
- Le client VPN Windows 10 parvient à se connecter au serveur OpenVPN après authentification.
- Une adresse IP VPN est attribuée automatiquement au client lors de la connexion.
- Le client VPN accède au réseau interne uniquement après l'établissement du tunnel VPN.
- Les tentatives d'accès non autorisées au réseau interne sont bloquées par le pare-feu pfSense.

Ces résultats confirment que la solution VPN est fonctionnelle et correctement sécurisée.

9.3 Analyse des performances et de la sécurité :

L'analyse des performances montre que la connexion VPN est stable et permet une communication fluide entre le client distant et le réseau interne. Le temps de connexion est rapide et les échanges de données sont correctement chiffrés.

Sur le plan de la sécurité :

- Les communications sont protégées par un tunnel chiffré,
- L'authentification par identifiant, mot de passe et certificat renforce la sécurité,
- Le pare-feu pfSense filtre efficacement le trafic,
- La journalisation permet de surveiller les connexions et de détecter les anomalies.

Ainsi, l'infrastructure mise en place répond aux exigences de sécurité et de performance attendues pour un accès distant sécurisé.

10 . Limites et améliorations possibles :

Malgré le bon fonctionnement du VPN nomade mis en place, certaines limites sont observées dans l'architecture actuelle. Ce chapitre présente ces limites ainsi que des propositions d'amélioration permettant de renforcer la sécurité, la performance et l'évolutivité de la solution.

10.1 Limites de l'architecture mise en place :

La première limite concerne l'environnement de simulation. Le réseau a été conçu sous GNS3 avec un réseau NAT, ce qui ne permet pas de reproduire parfaitement un environnement Internet réel. Certaines contraintes liées au NAT peuvent limiter les tests avancés, notamment en matière de performance et de routage.

Ensuite, l'architecture repose sur un seul routeur pfSense, ce qui constitue un point de défaillance unique. En cas de panne du pare-feu, l'accès au réseau interne et au VPN devient indisponible.

Par ailleurs, le projet utilise une seule machine cliente Windows 10, ce qui ne permet pas de tester le comportement du VPN avec plusieurs utilisateurs simultanés. Les performances et la charge du serveur VPN ne peuvent donc pas être pleinement évaluées.

Enfin, les mécanismes de sécurité restent basiques pour un contexte professionnel réel. L'authentification repose principalement sur des certificats et des identifiants locaux, sans intégration d'un annuaire centralisé ou d'une authentification multifacteurs.

10.2 Propositions d'amélioration :

Plusieurs améliorations peuvent être envisagées pour renforcer l'architecture mise en place.
Il serait possible de remplacer le réseau NAT par une **connexion Cloud ou une interface bridgée**, afin de se rapprocher davantage d'un environnement réel et d'améliorer les tests d'accès distant.
L'ajout d'un **second pare-feu pfSense en haute disponibilité (CARP)** permettrait d'assurer la continuité de service en cas de panne, améliorant ainsi la fiabilité de l'infrastructure.
Pour renforcer la sécurité, l'intégration d'une **authentification multi-facteurs (MFA)** ou d'un **serveur d'authentification centralisé (LDAP / Active Directory)** pourrait être mise en place afin de mieux contrôler les accès VPN.
Il serait également pertinent d'ajouter plusieurs **clients VPN simultanés** afin de tester la montée en charge, les performances du tunnel VPN et le comportement du réseau en situation réelle.
Enfin, l'intégration d'outils de **supervision avancée** et de détection d'intrusion permettrait d'améliorer la surveillance du réseau et d'anticiper les incidents de sécurité.

11 . Conclusion :

La mise en place du VPN nomade à l'aide de pfSense a permis de sécuriser efficacement l'accès distant au réseau interne. L'installation et la configuration du serveur VPN, l'attribution des certificats aux utilisateurs et la configuration des clients Windows 10 ont été réalisées conformément aux bonnes pratiques de sécurité. Les tests de connectivité et d'accès aux ressources du LAN ont confirmé le bon fonctionnement de la solution, ainsi que la confidentialité et l'intégrité des échanges de données. Ce projet illustre l'importance des outils de sécurisation des communications dans un environnement réseau professionnel et démontre la maîtrise des procédures de configuration et de validation d'un VPN pour un usage nomade sécurisé.