
SSL AND VPN

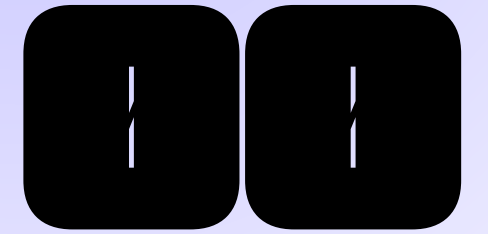
Réalisé par:

- Daoud ELLAILI
- Anas EL GHANDOUR

Encadré par:

- M. Mohammed BOUGRINE

PLAN



- INTRODUCTION
- CONTEXTE ET ORIGINE
- Définition et Fonctionnement de SSL
- Définition et Types de VPN
- Différences entre SSL et VPN
- Comment SSL et VPN fonctionnent ensemble
- SSL VPN - LAB
- CONCLUSION

INTRODUCTION

L'internet est essentiel mais comporte des risques (vol de données, piratage). Deux technologies sécurisent nos échanges :

- SSL (Secure Sockets Layer) : protège les communications en ligne (ex. sites sécurisés).
- VPN (Virtual Private Network) : masque l'identité et chiffre les connexions.

Nous verrons leur fonctionnement et comment les combiner pour renforcer la sécurité des données.

CONTEXTE ET ORIGINE

Avec Internet, les échanges de données, essentiels, restent vulnérables aux pirates (mots de passe, données bancaires, etc.).

Deux solutions combattent ces risques :

- SSL (années 1990) : sécurise les connexions (ex. sites web).
- VPN (conçu pour les entreprises) : chiffre les données et protège l'anonymat.

Ensemble, ils forment un pilier de la cybersécurité moderne.



DÉFINITION DE SSL

SSL (Netscape, 1994) : chiffre les échanges web pour garantir confidentialité, intégrité et authentification.

⚠ Ses premières versions (1.0 à 3.0) avaient des failles. Remplacé en 1999 par TLS (Transport Layer Security), aujourd'hui standard.

- Reconnaissable au cadenas et au « https:// » dans l'URL.
- Protège : transactions bancaires, connexions sécurisées, données sensibles.

FONCTIONNEMENT DE SSL

1. Établissement de la connexion (Handshake SSL)

En accédant à un site https:// :

- Vérification du certificat SSL (authenticité du site).
- Négociation d'un algorithme de chiffrement (ex. AES).
- Création d'une clé de session unique.

2. Chiffrement des données

Toutes les données (mots de passe, paiements, messages) sont chiffrées, les rendant illisibles même interceptées.

3. Transmission sécurisée

Le site et le navigateur utilisent la clé de session pour chiffrer/déchiffrer les échanges en temps réel.

DÉFINITION DE VPN

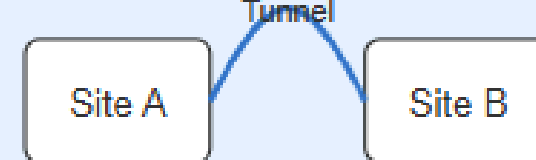
- Un VPN (Virtual Private Network) est un outil qui crée une connexion sécurisée entre votre appareil et Internet. Il permet de :
 - _Chiffrer vos données pour les protéger des pirates.
 - _Cacher votre adresse IP pour naviguer anonymement.
 - _Contourner les restrictions géographiques en se connectant aux serveurs dans D'autres pays.
- En résumé, un VPN agit comme un tunnel sécurisé entre vous et le web, empêchant toute surveillance ou interception de vos informations.

TYPES DE VPN

VPN Types Comparison

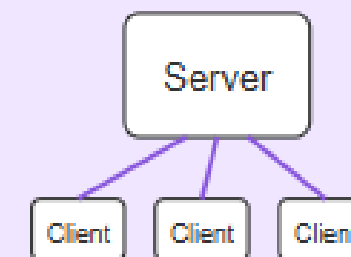
Topology-Based VPN Types

Site-to-Site VPN



- Connects entire networks
- Always-on connection
- Used by businesses/organizations
- Requires dedicated equipment

Site-to-Client VPN



- Connects individual clients to network
- On-demand connection
- Used for remote work/personal use

OSI Layer-Based VPN Types

Layer 2 VPN

Data Link Layer (Ethernet frames)

- Operates at OSI Layer 2 (Data Link)
- Transports Ethernet frames
- Supports broadcast/multicast traffic
- Often used for extending LANs
- Examples: L2TP, VPLS, VXLAN
- Appears as one logical LAN

Layer 3 VPN

Network Layer (IP packets)

- Operates at OSI Layer 3 (Network)
- Transports IP packets
- Requires routing between networks
- More scalable for larger networks
- Examples: IPsec, GRE, MPLS L3VPN
- Better security isolation

TYPES DE VPN

SSL VPN vs Other VPN Technologies

Feature	SSL VPN	IPsec VPN	L2TP/PPTP
Protocol	TLS/SSL (TCP 443)	ESP/AH (IP 50/51)	L2TP/PPTP
Deployment	Easy, web-based	Complex setup	Moderate complexity
Firewall Traversal	Excellent	Often blocked	Often blocked

DIFFÉRENCES ENTRE SSL ET VPN

Le SSL et le VPN ont des rôles distincts en matière de sécurité.

- Le SSL protège uniquement les échanges entre un utilisateur et un site web sécurisé (via HTTPS), comme les transactions bancaires ou les connexions à un compte. Il chiffre les données échangées avec le site (mots de passe, formulaires), mais ne masque pas l'adresse IP de l'utilisateur.
- En revanche, un VPN sécurise toute la connexion Internet d'un appareil, chiffrant l'intégralité du trafic (applications, services en ligne) et masquant l'adresse IP pour naviguer de manière anonyme.

COMMENT SSL ET VPN FONCTIONNENT ENSEMBLE

Les technologies SSL et VPN peuvent être combinées via les VPN SSL, qui utilisent le protocole SSL/TLS pour sécuriser les communications.

Fonctionnement :

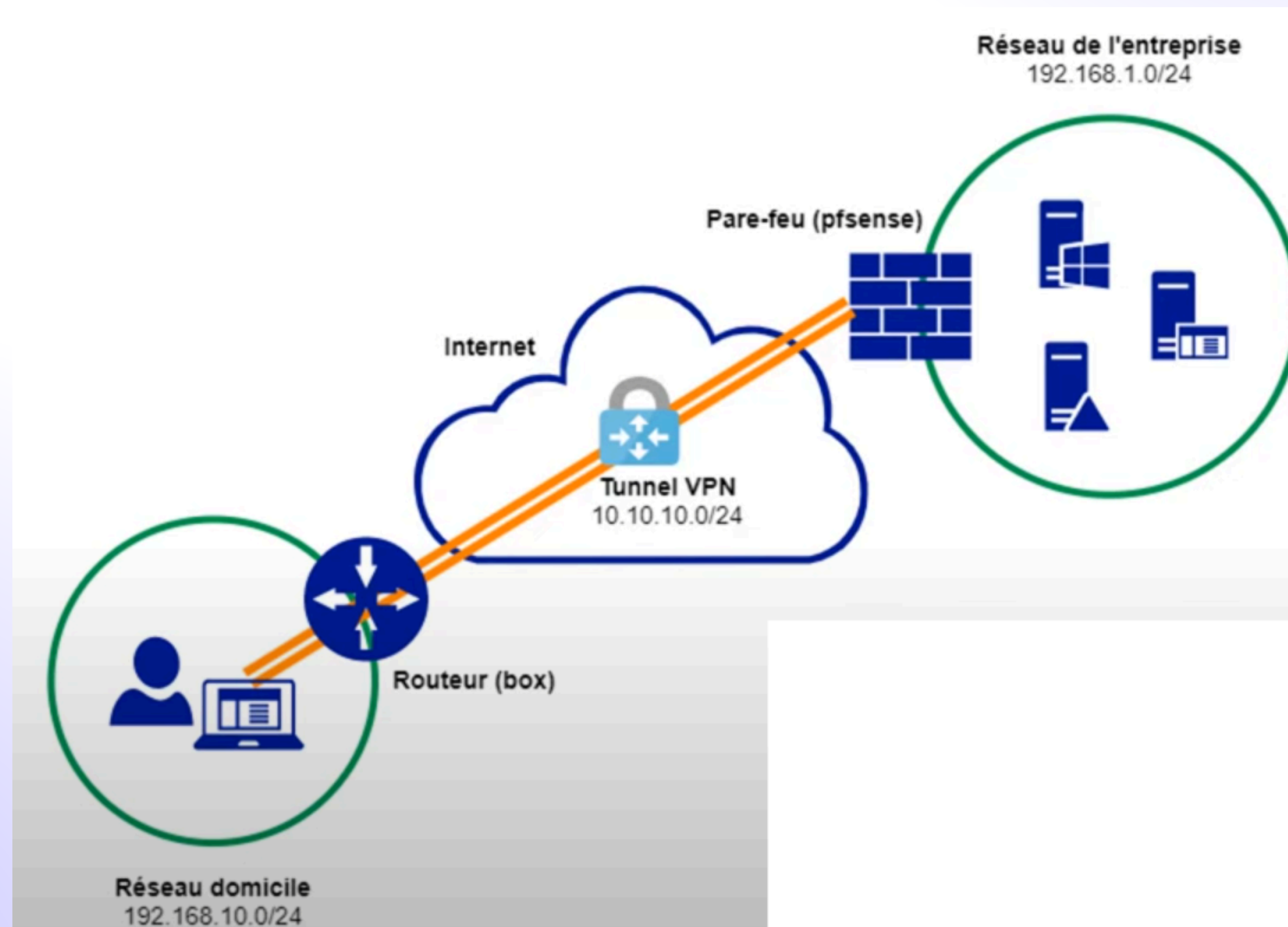
- L'utilisateur se connecte à un portail web sécurisé (HTTPS) pour lancer une session SSL/TLS.
- Le serveur authentifie l'utilisateur (identifiants ou certificats).
- Un tunnel chiffré est créé entre l'appareil et le réseau cible, protégeant les données échangées.

Cette hybridation offre une sécurité renforcée, idéale pour l'accès distant aux ressources d'entreprise ou la protection sur les réseaux publics.

SSL VPN - LAB

ARCHITECTURE

10



CONFIGURATION DE PFSENSE

11

```
pfSense_Firewall x
Starting syslog...done.
Starting CRON... done.
pfSense 2.7.2-RELEASE amd64 20231206-2010
Bootup complete

FreeBSD/amd64 (pfSense.home.arp) (ttyv0)

VMware Virtual Machine - Netgate Device ID: c7920ef86ec6107d3da3

*** Welcome to pfSense 2.7.2-RELEASE (amd64) on pfSense ***

WAN (wan)      -> em0      -> v4/DHCP4: 192.168.208.19/24
LAN (lan)      -> em1      -> v4: 192.168.1.1/24

0) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults  13) Update from console
5) Reboot system              14) Enable Secure Shell (sshd)
6) Halt system                 15) Restore recent configuration
7) Ping host                   16) Restart PHP-FPM
8) Shell

Enter an option: █
```



GÉNÉRATION DES CERTIFICATS

12

https://192.168.1.1/system_certmanager.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.](#)

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
GUI default (67d0ea8507a04) Server Certificate CA: No Server: Yes	self-signed	O=pfSense GUI default Self-Signed Certificate, CN=pfSense-67d0ea8507a04 Valid From: Wed, 12 Mar 2025 01:59:33 +0000 Valid Until: Tue, 14 Apr 2026 02:59:33 +0100	i webConfigurator	   
Certificat-OpenVPN Server Certificate CA: No Server: Yes	CA-VPNTTest	ST=Rabat, OU=VPNConfig, O=VPNs, L=Rabat, CN=vpn-test, C=MA Valid From: Wed, 12 Mar 2025 01:58:16 +0000 Valid Until: Sat, 10 Mar 2035 02:58:16 +0100	i OpenVPN Server	   
Certificat-VPNTTest User Certificate CA: No Server: No	CA-VPNTTest	ST=Rabat, OU=VPNConfig, O=VPNs, L=Rabat, CN=userVPNTTest, C=MA Valid From: Wed, 12 Mar 2025 02:02:42 +0000 Valid Until: Sat, 10 Mar 2035 03:02:42 +0100	i User Cert	   

[+ Add/Sign](#)

CONFIGURATION DU MODE

13

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.](#)

VPN / OpenVPN / Servers / Edit

Servers

Clients

Client Specific Overrides

Wizards

General Information

Description

A description of this VPN for administrative reference.

Disabled

☐ Disable this server

Set this option to disable this server without removing it from the list.

Mode Configuration

Server mode

Peer to Peer (SSL/TLS) ▾

Device mode

Peer to Peer (SSL/TLS)

Peer to Peer (Shared Key)

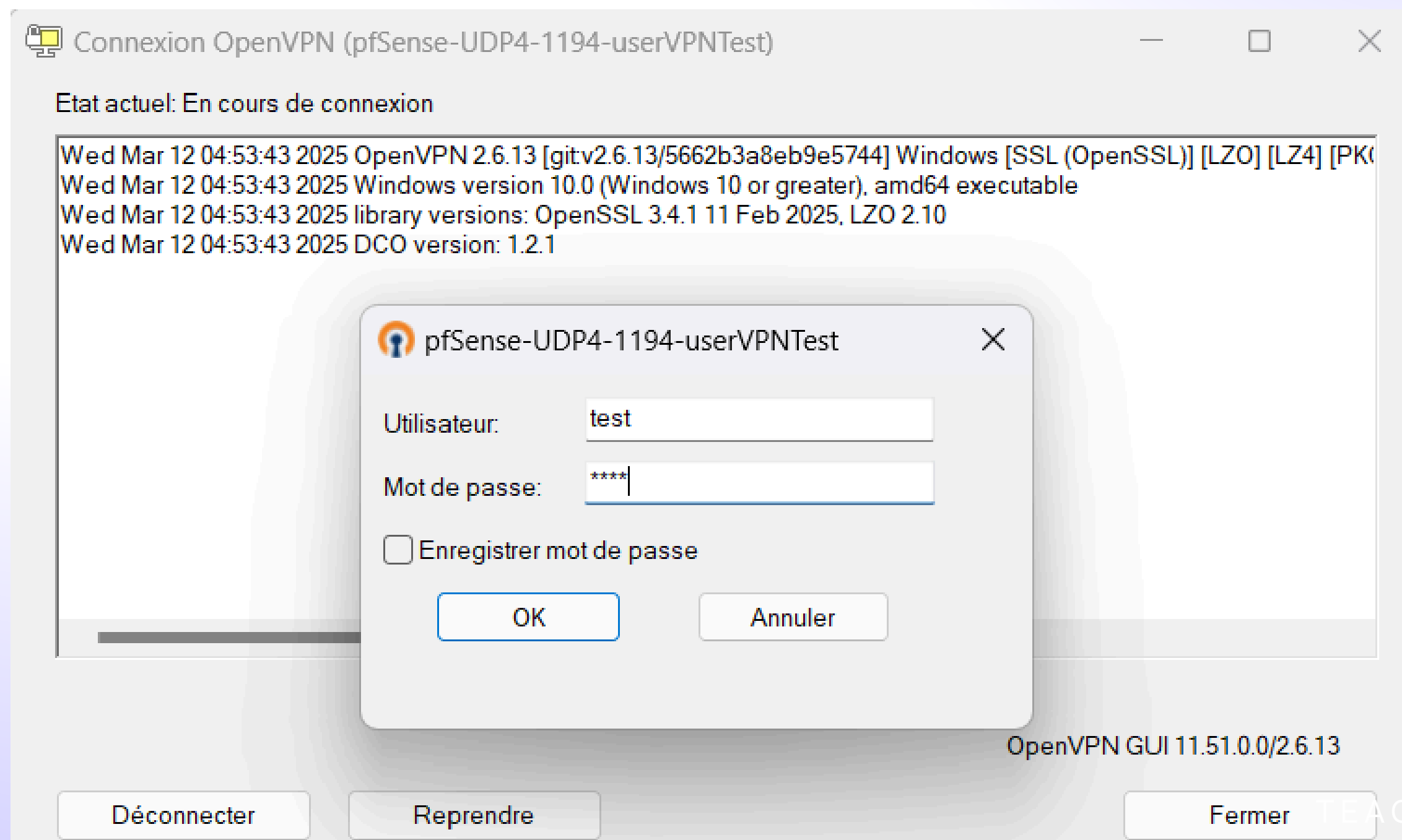
Remote Access (SSL/TLS)

Remote Access (User Auth)

Remote Access (SSL/TLS + User Auth)

and compatible mode across all platforms.

AUTHENTIFICATION DE L'UTILISATEUR



SOUÇIS RENCONTRÉ

Port Forwarding Tester

your external address

105.152.58.27

open port finder

Remote Address

Port Number

 Use Current IP

 Port 1194 is closed on 105.152.58.27.

Use [Connected](#) to monitor this port.

common ports

21 FTP

22 SSH

23 TELNET

25 SMTP

53 DNS

80 HTTP

110 POP3

115 SFTP

135 RPC

139 NetBIOS

143 IMAP

194 IRC

443 SSL

445 SMB

CONCLUSION

La combinaison de SSL/TLS et VPN renforce la sécurité en ligne en apportant une protection à plusieurs niveaux : SSL sécurise les échanges sensibles en garantissant leur confidentialité et leur intégrité, tandis que le VPN protège l'ensemble de la connexion, masque l'adresse IP et prévient les interceptions sur les réseaux publics. Leur complémentarité souligne qu'aucune technologie seule n'est suffisante face aux cybermenaces croissantes, rendant leur utilisation conjointe essentielle pour une protection optimale.



MERCI !