Study and implementation of a solution IPSec VPN site to site using Pfsense and openVPN

Realized by:

- **Mahiri Ilham**
- **El Maizi Hassna**

Summary

Introduction

problem solution

VPN

A VPN (Virtual Private Network) is a system that creates a virtual link between remote computers, it is used for remote work. Its operation is quite simple, a VPN software creates a tunnel computers that then connect to the same virtual local network.

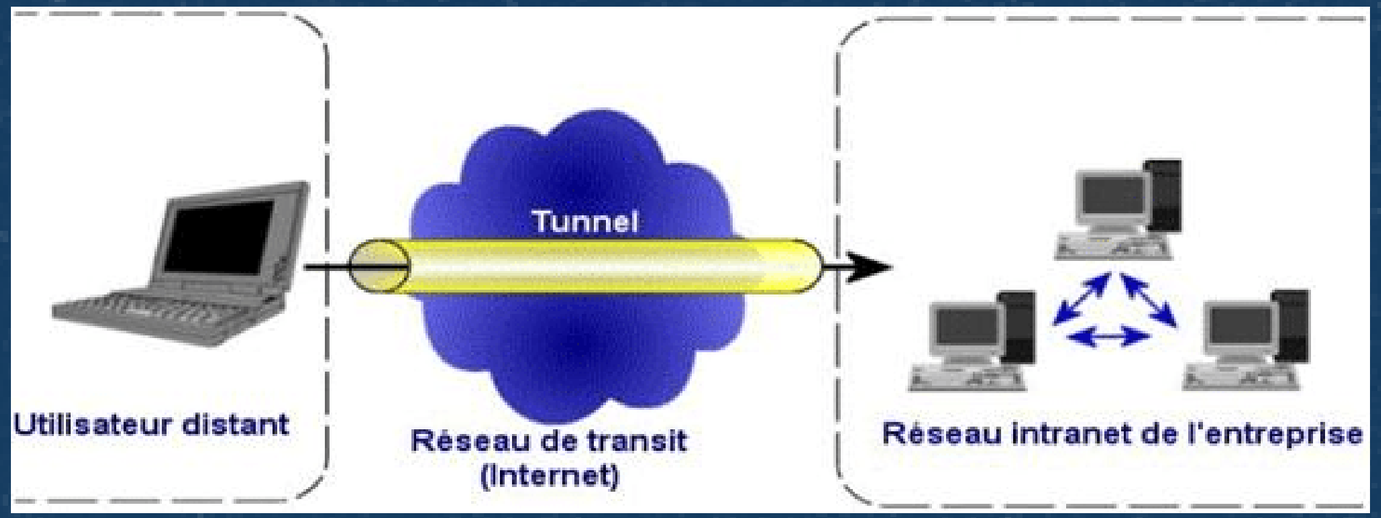
The different types of VPN

The access VPN

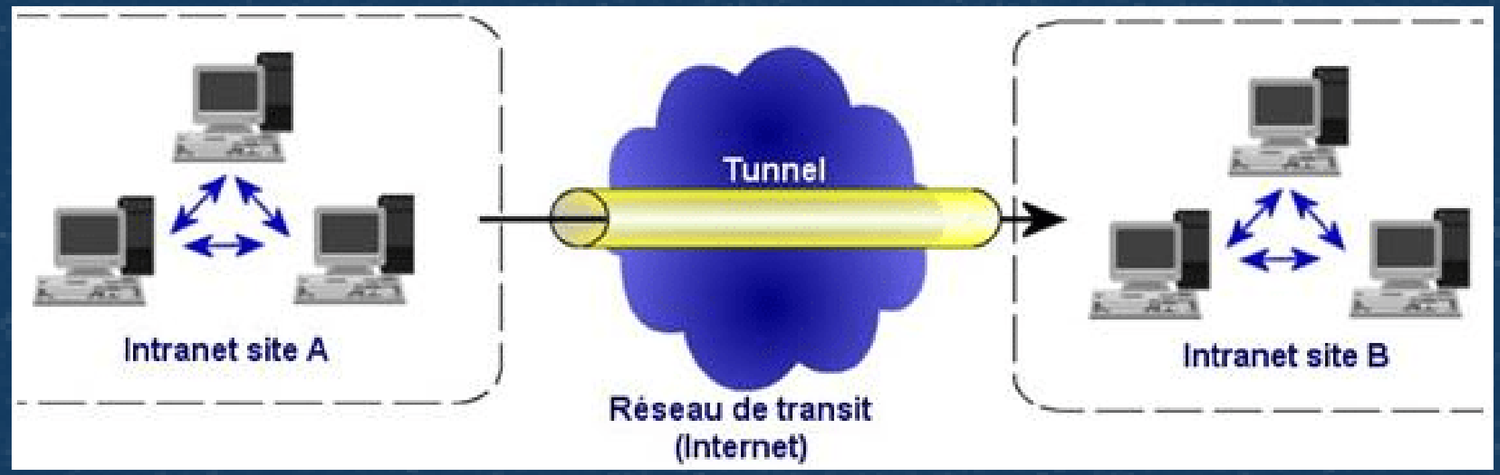
VPN intranet

VPN extranet

The access VPN



VPN intranet



The fundamental characteristics of a VPN

user authentication

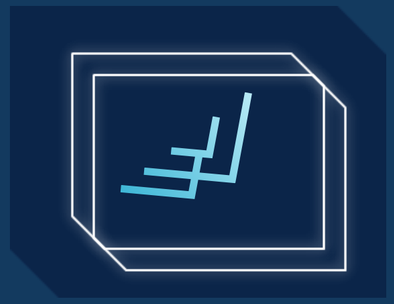
address management

data encryption

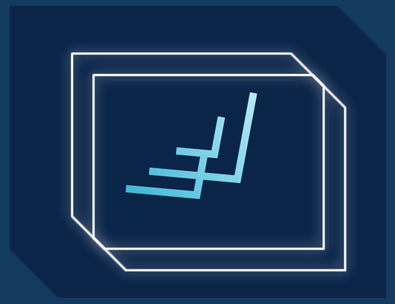
Multi-protocol support

key management

VPN : Implementation

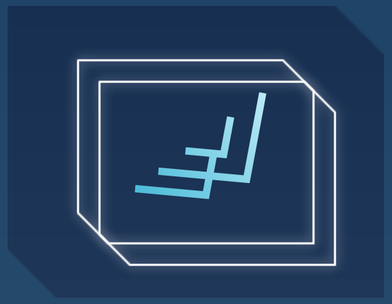


Level. 2
PPTP, L2TP

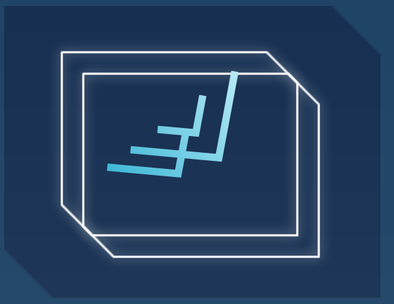


Level.. 2.5
MPLS

Level.. 3
IPsec



Level. 4
TLS

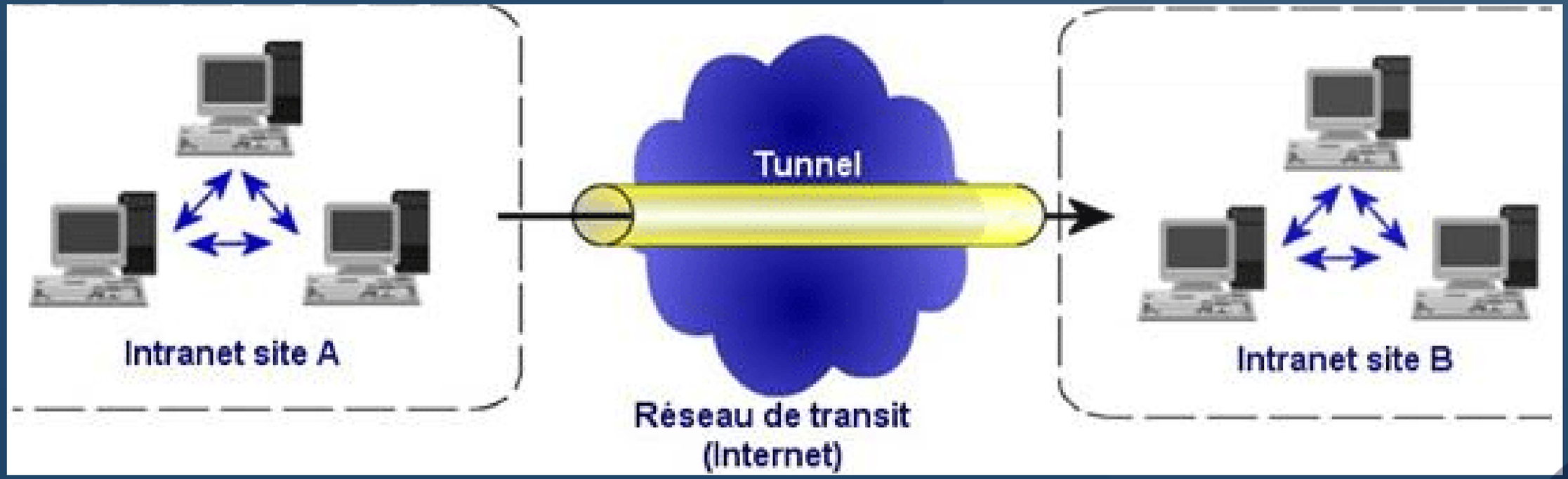


Level. 5
SSH

Tunnel

A tunnel, in the context of computer networks, is an encapsulation of data from one network protocol into another, located in the same layer of the layered model, or in a higher layer.

Example of the tunnel



IPsec

IPsec (Internet Protocol Security), defined by the IETF as a framework of open standards for ensuring private and protected communications on IP networks.

Keys management for IPSec

IKE

Internet key Exchange is a system developed specifically for Ipsec that aims to provide authentication and key exchange mechanisms.

IsaKmp

for the role of negotiation, setting and modifying and deleting security associations and their attributes.

The properties of IPsec

confidentiality

integrity

authentication

anti-replay

The two mechanisms of IPsec

ESP

can also allow authentication of data but and mainly used for encryption of information.

AH

aims to ensure the integrity and authenticity of IP datagrams.

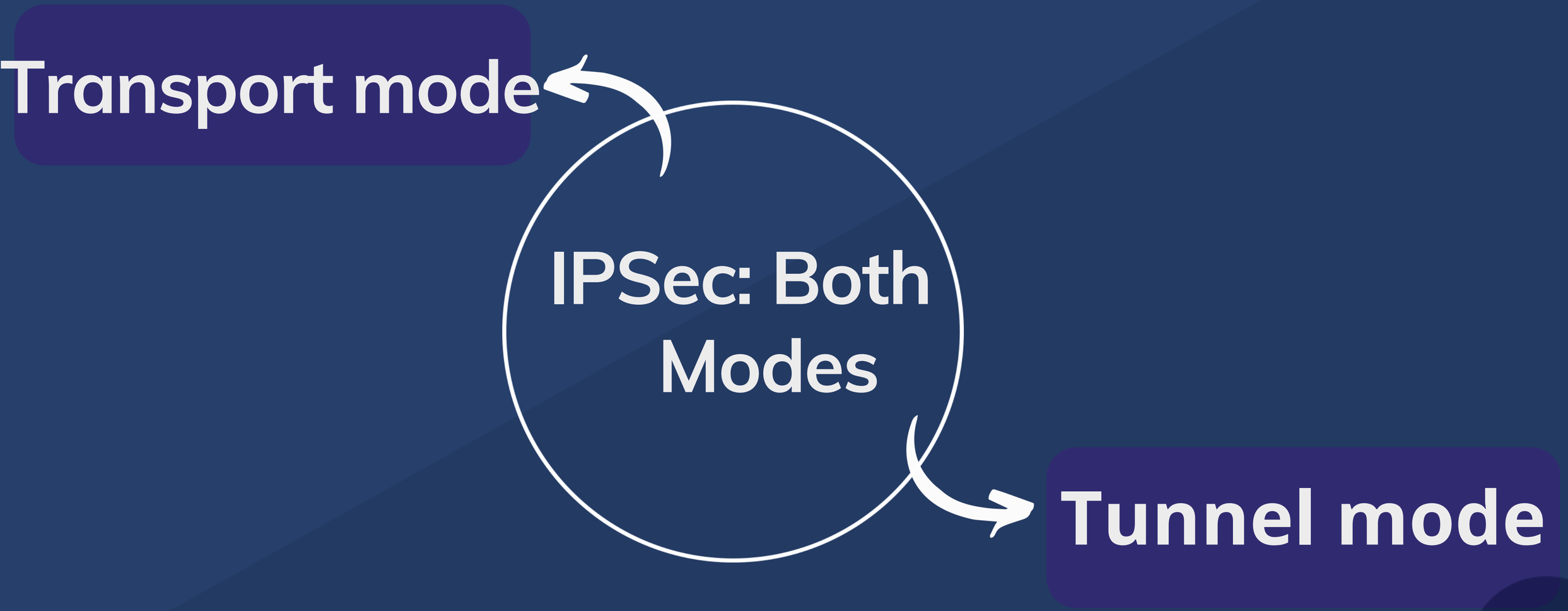
Operation of the two IPsec mechanisms

IPv4, the protocol field of the datagrams is modified to indicate the presence of one of the 2 extensions

AH =51, ESP=50

- AH and ESP will themselves contain a Next Header field which will indicate the protocol type (TCP, ...) initially contained in the IP datagram

IPSec : Modes



IPSec : Transport mode

Security is only applied to top layer data.

Layer 4

IP layer is not protected.

IPSec : Tunnel mode

IP Encapsulation

Protected IP layer

Protected layer 4

IPsec : combination

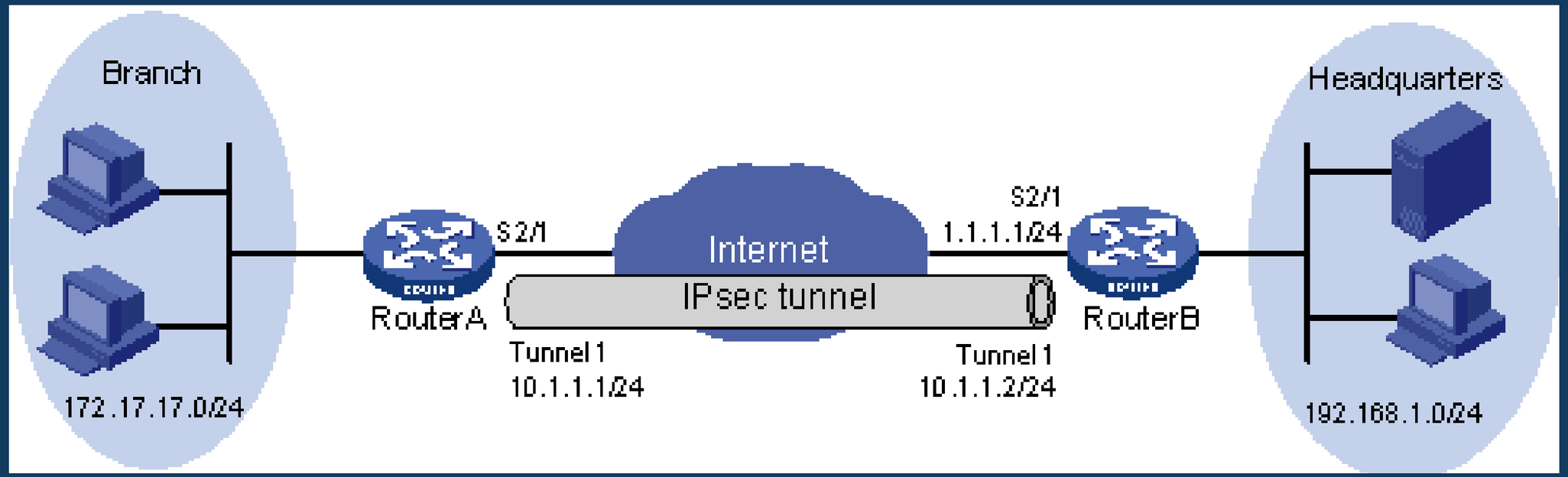
Encapsulation in tunnel mode

Receiving gateway removes 1st envloppe

Transmits datagrams to host or receiving gateway

This in turn processes the remaining protections

IPsec tunnel example



Pfsense

PfSense is a free, open source software based on FreeBSD, it can be used as a firewall or router.

The operating principles of Pfsense

FIREWALL (ITS PRIMARY FUNCTION) WHICH IS BASED ON THE PACKET FILTER

VPN FOR SECURE DATA TRANSITING THE NETWORK.

A LOCAL DATABASE CAN BE USED FOR AUTHENTICATION.

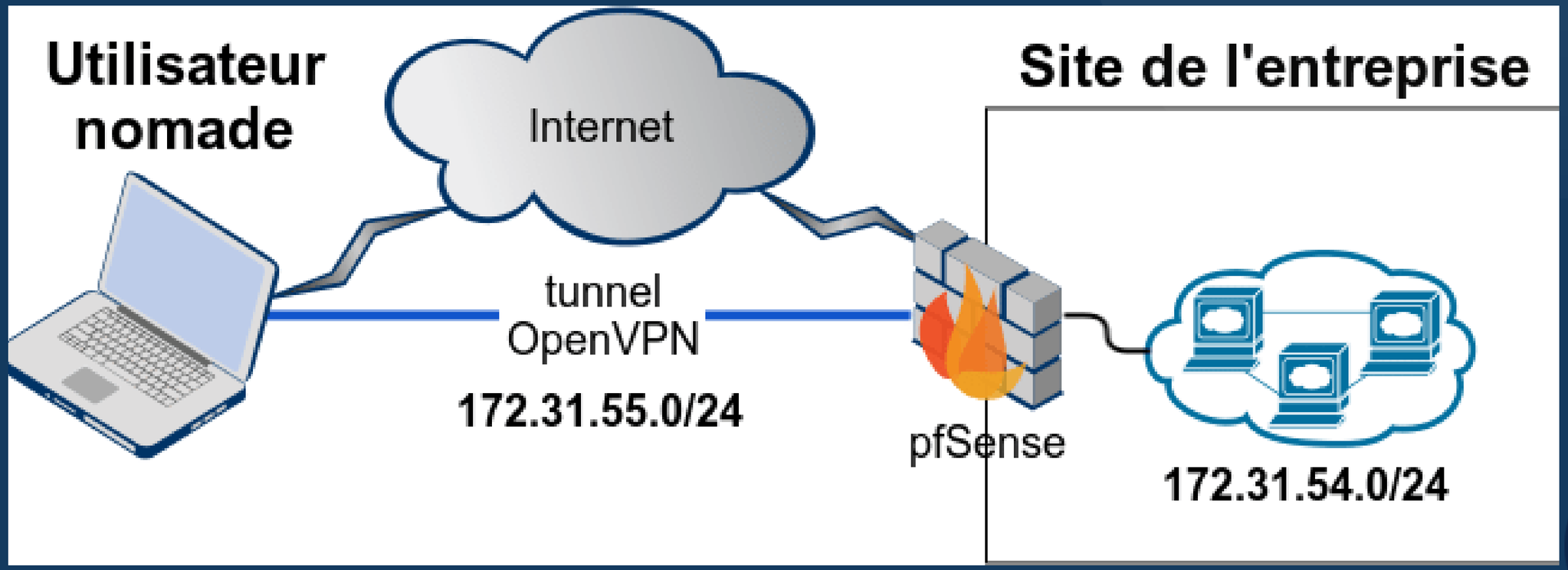
Benefits of using Pfsense

. rich and powerful solution (based on free software)

. system update without reinstalling package, downloadable from the web

. simplicity of installation and administration

Pfsense example



pfSense: Installation and configuration

#Download, from https://www.pfsense.org/download/pfSense ISO image

#Hyper-V VM configuration

#Installing pfSense

#LAN Network Card IP Address Configuration

#pfSense Base installation setup

>Type The IP address in the browser: 192.168.134.28–
Username: admin – Password: pfsense

>WAN Internet Card Configuration:
192.168.134.28 , Netmask (CIDR): 24

OpenVPN

- Open and free software to create VPNs
- Uses: OpenSSL + SSL/TLS protocol
- Offers many security and control functions
- Multi-platform (compatible with Windows, Lunix, Mac…)

VPN TLS with OpenVPN

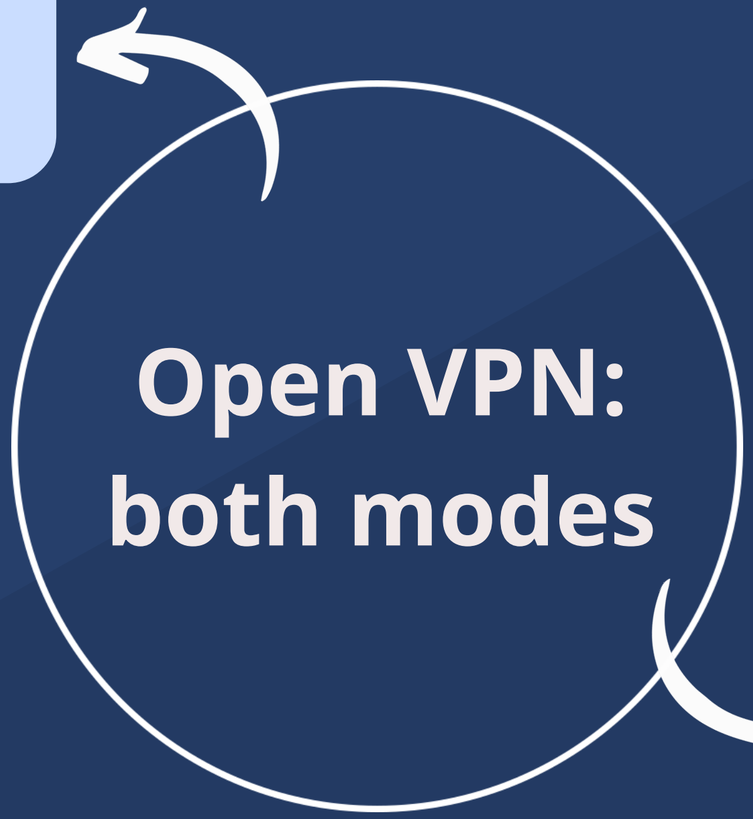
TLS VPN Principles

- establish a secure SSL connection
- create at each end a virtual network interface
- encapsulate virtual network IP traffic in the SSL connection

Virtual network interface concept (Tun/Tap)

Mode Tun

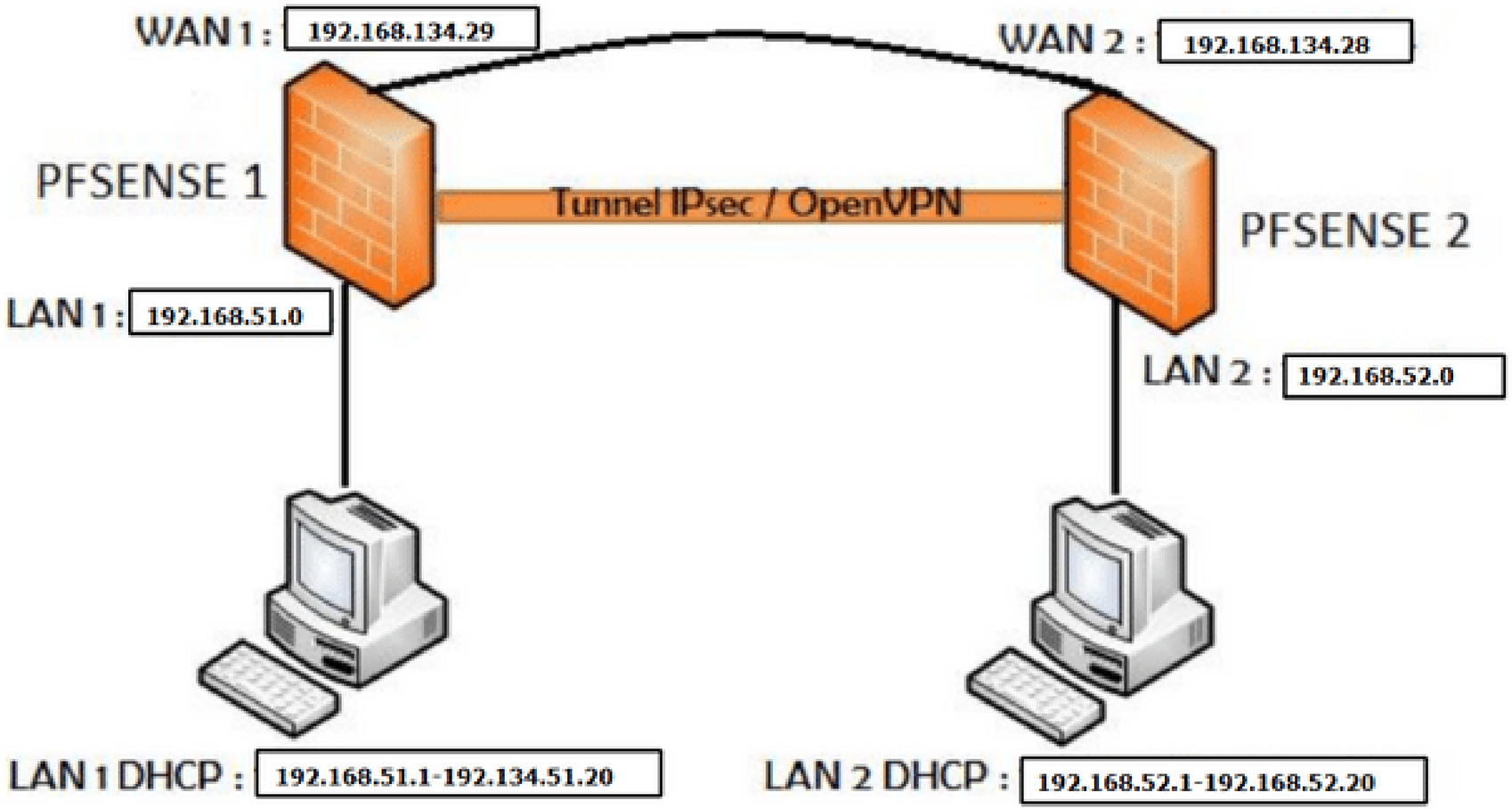
. Network level / Level 3
. Route the VPN packets



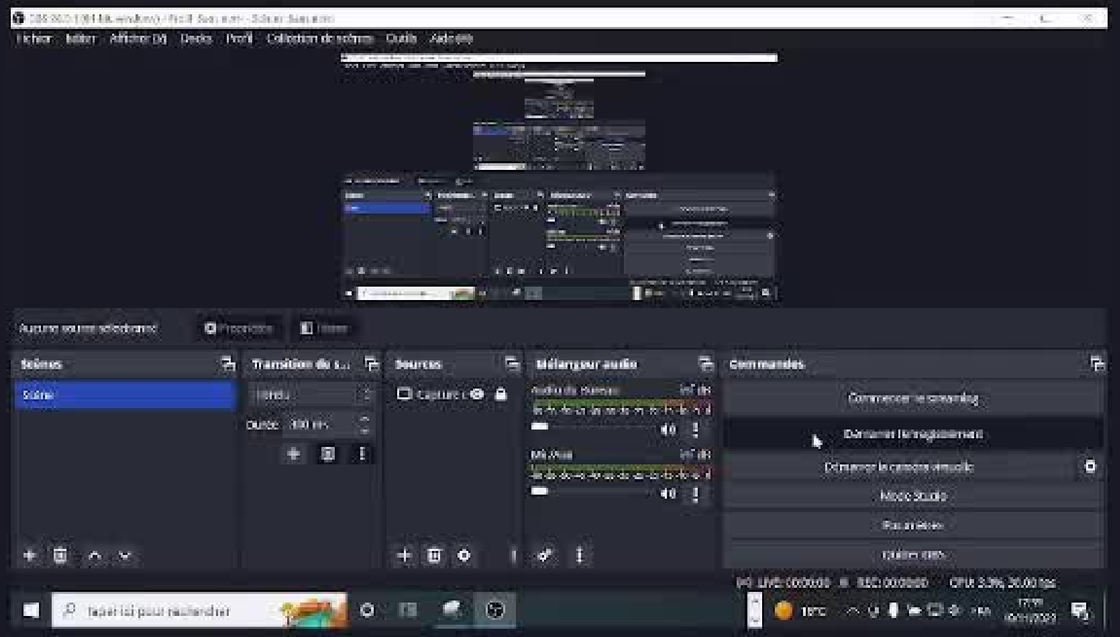
Mode Tab

. Pont / Bridge
. Ethernet Level/Level 2
. Acts as a switch

architecture of practice



Test !



cune source sélectionné

Propriétés

Filtres

Scènes

Scène

Transition de s...

Fondu

Durée 300 ms

Sources

Capture (

Mélangeur audio

Audio du Bureau -inf dB

-60 -55 -50 -45 -40 -35 -30 -25 -20 -15 -10 -5 0

Mic/Aux -inf dB

-60 -55 -50 -45 -40 -35 -30 -25 -20 -15 -10 -5 0

Commandes

Commencer le streaming

Démarrer l'enregistrement

Démarrer la caméra virtuelle

Mode Studio

Paramètres

Quitter OBS

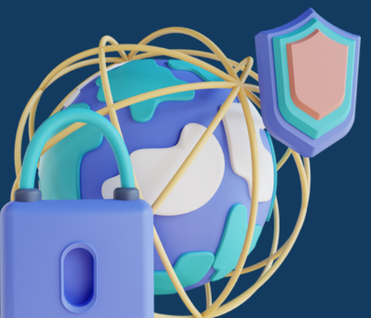
LIVE: 00:00:00 REC: 00:00:00 CPU: 3.3%, 30.00 fps

Taper ici pour rechercher

18°C FRA 17:39

Conclusion

Indeed, the implementation of site-to-site IPsec-based VPN allows private networks to extend and connect to each other through the Internet.



Thank You