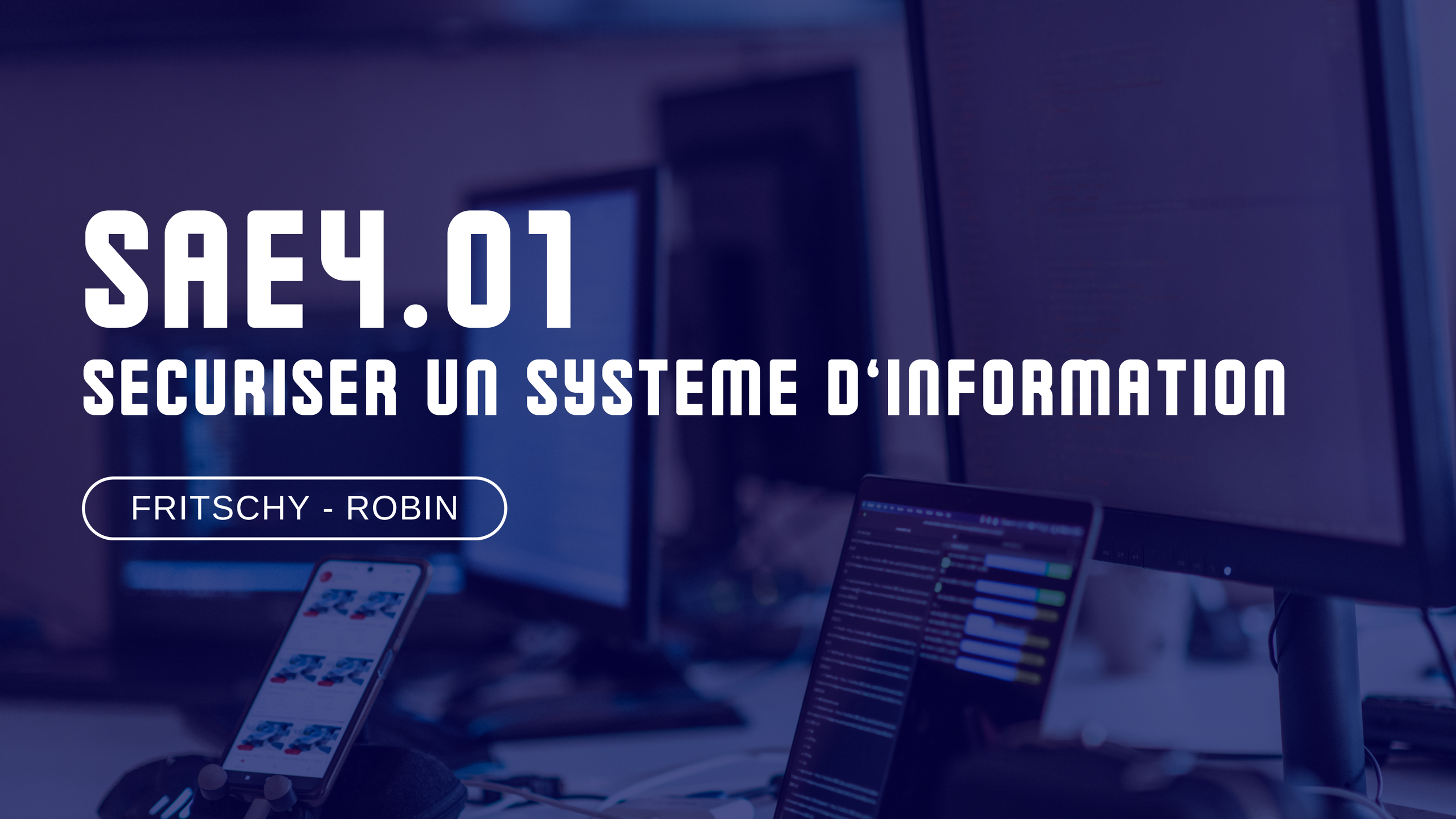
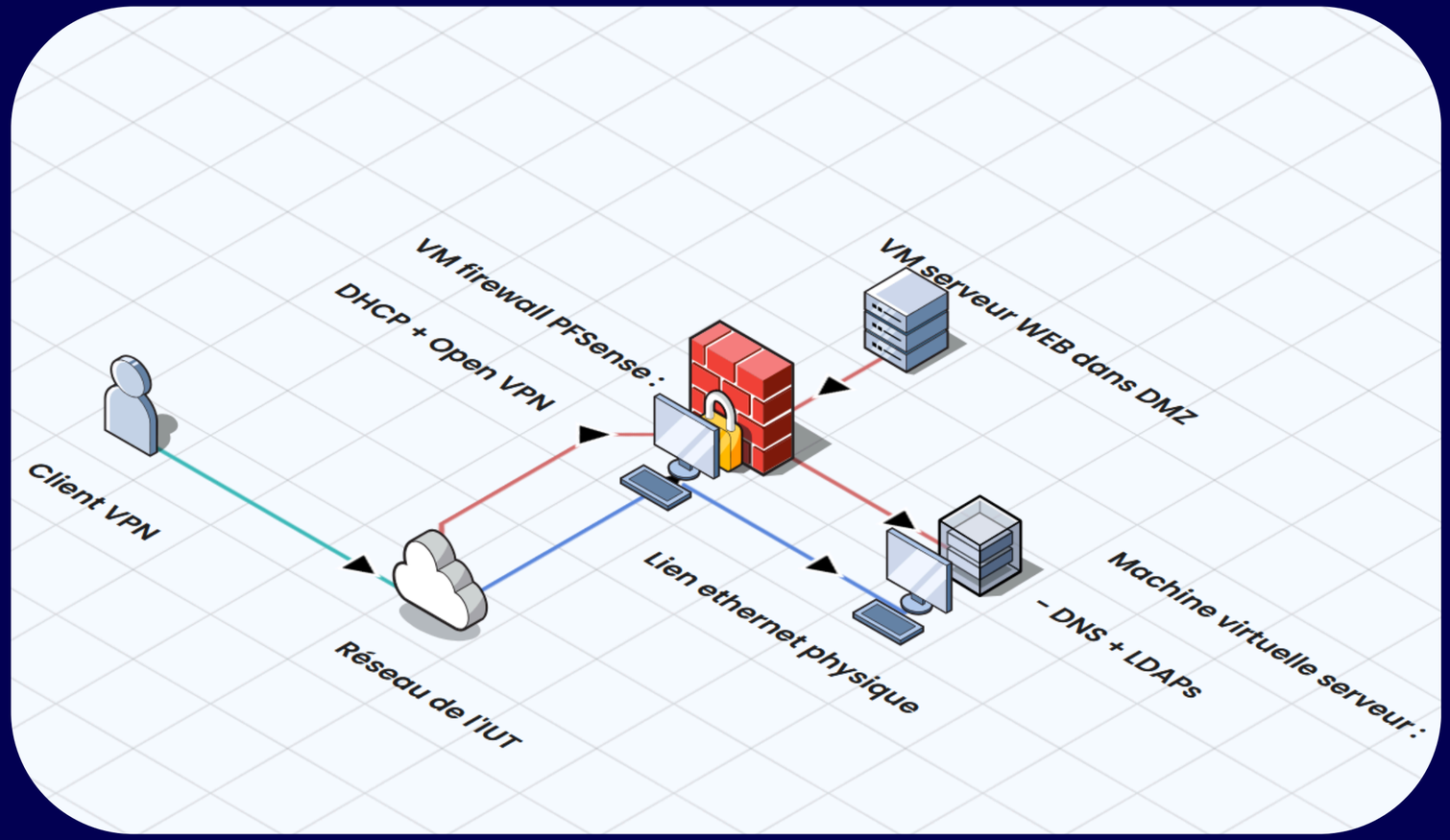
# SAE4.01

## SECURISER UN SYSTEME D'INFORMATION

FRITSCHY - ROBIN



# PLAN RÉSEAU




- Environnement virtualisé sous VMware Workstation Pro et Virtualbox.
- Ordinateurs physiquement reliés par câble ethernet
- Parefeu servant de routeur

# SERVICES MIS EN PLACE

1

DHCP + Parefeu

2

DNS + Authentification LDAPs

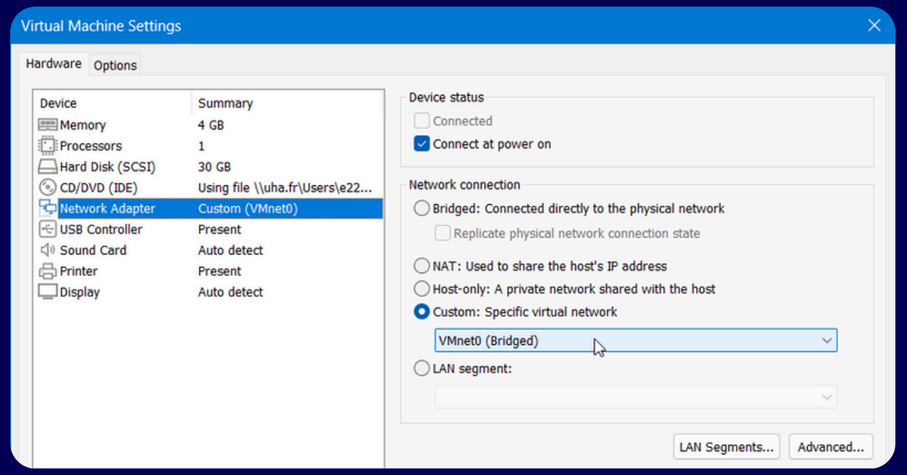
3

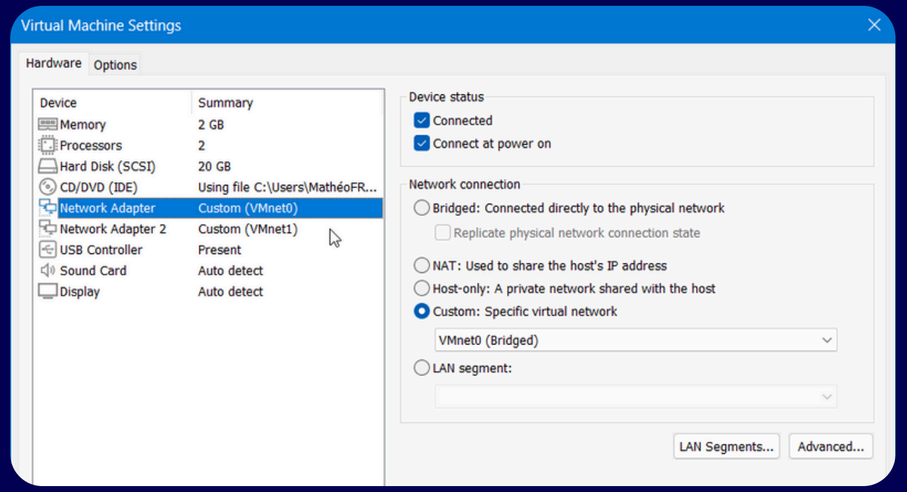
Connexion au réseau par VPN au démarrage

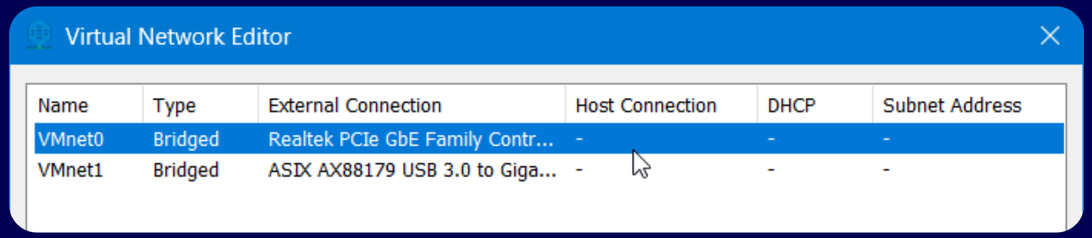
4

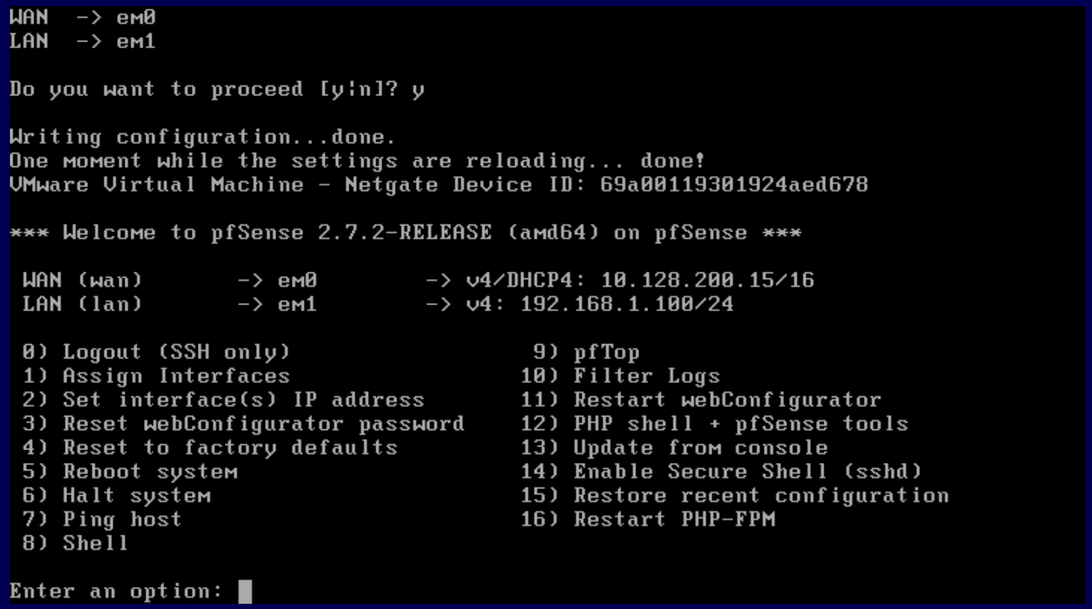
Serveur NFS

# ADRESSAGE IP



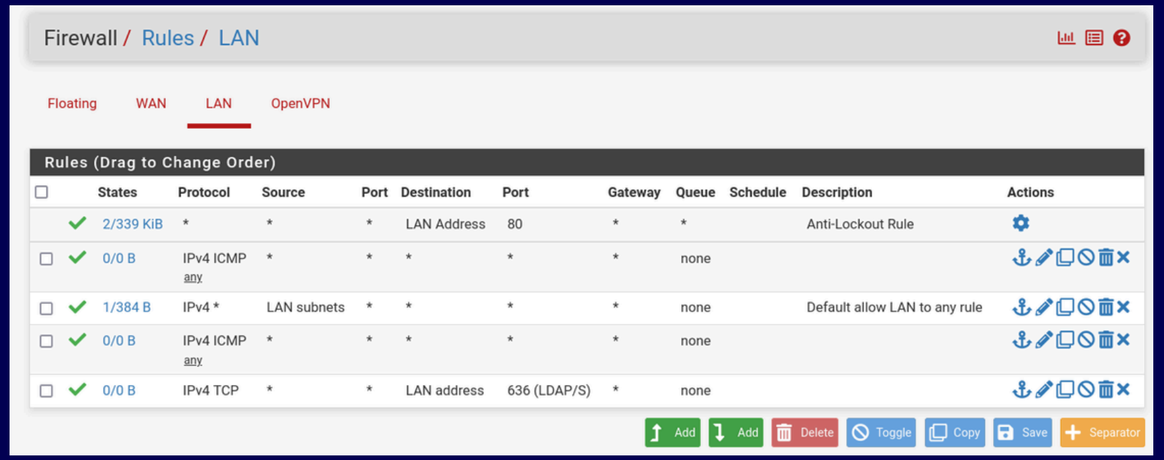



# PAREFEU

- Service DHCP dans le réseau local en de 192.168.1.115 à 192.168.1.150 qui donne l'adresse du DNS 192.168.1.112 et la route par défaut.
- Règles permettant le trafic du VPN vers le WAN et du LDAP6 (port 636) en LAN.
- Service de filtrage de sites spécifiques SquidGuard.

# CERTIFICATS

## Certificate Authorities

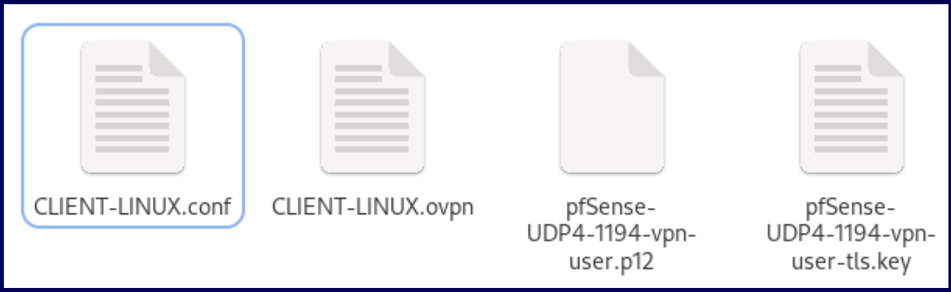
| Name | Internal | Issuer | Certificates | Distinguished Name | In Use | Actions |
|---|---|---|---|---|---|---|
| CA-VPN | ✔ | *self-signed* | 2 | ST=Alsace, OU=RT, O=UHA, L=Colmar, CN=ca-vpn, C=FR<br>Valid From: **Fri, 06 Jun 2025 07:06:20 +0000**<br>Valid Until: **Mon, 04 Jun 2035 07:06:20 +0000** | | |

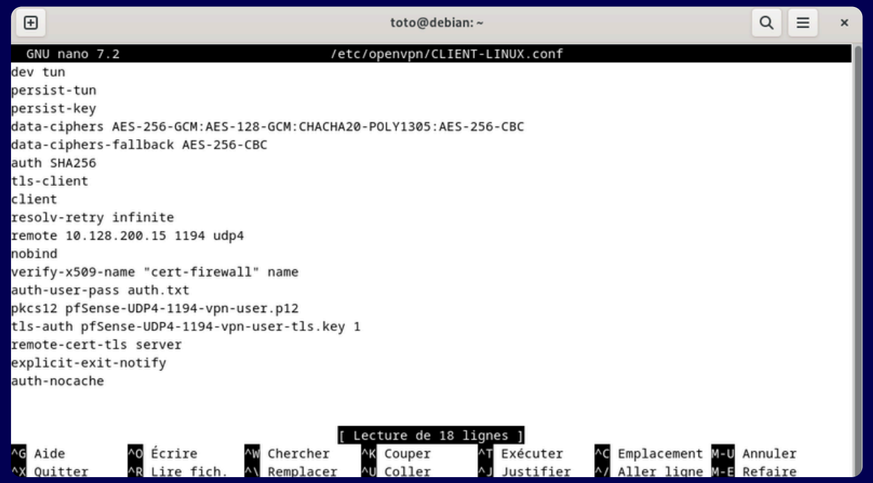
## Certificates

| Name | Issuer | Distinguished Name | In Use | Actions |
|---|---|---|---|---|
| Certificat OpenVPN<br>*Server Certificate*<br>CA: **No**<br>Server: **Yes** | CA-VPN | ST=Alsace, OU=RT, O=UHA, L=Colmar, CN=cert-firewall, C=FR<br>Valid From: **Fri, 06 Jun 2025 07:10:15 +0000**<br>Valid Until: **Mon, 04 Jun 2035 07:10:15 +0000** | OpenVPN Server | |
| Certificat-VPN-User<br>*User Certificate*<br>CA: **No**<br>Server: **No** | CA-VPN | ST=Alsace, OU=RT, O=UHA, L=Colmar, CN=vpn-user, C=FR<br>Valid From: **Fri, 06 Jun 2025 07:19:51 +0000**<br>Valid Until: **Mon, 04 Jun 2035 07:19:51 +0000** | User Cert | |

# PRESENTATION DE LA CONNEXION SECURISEE

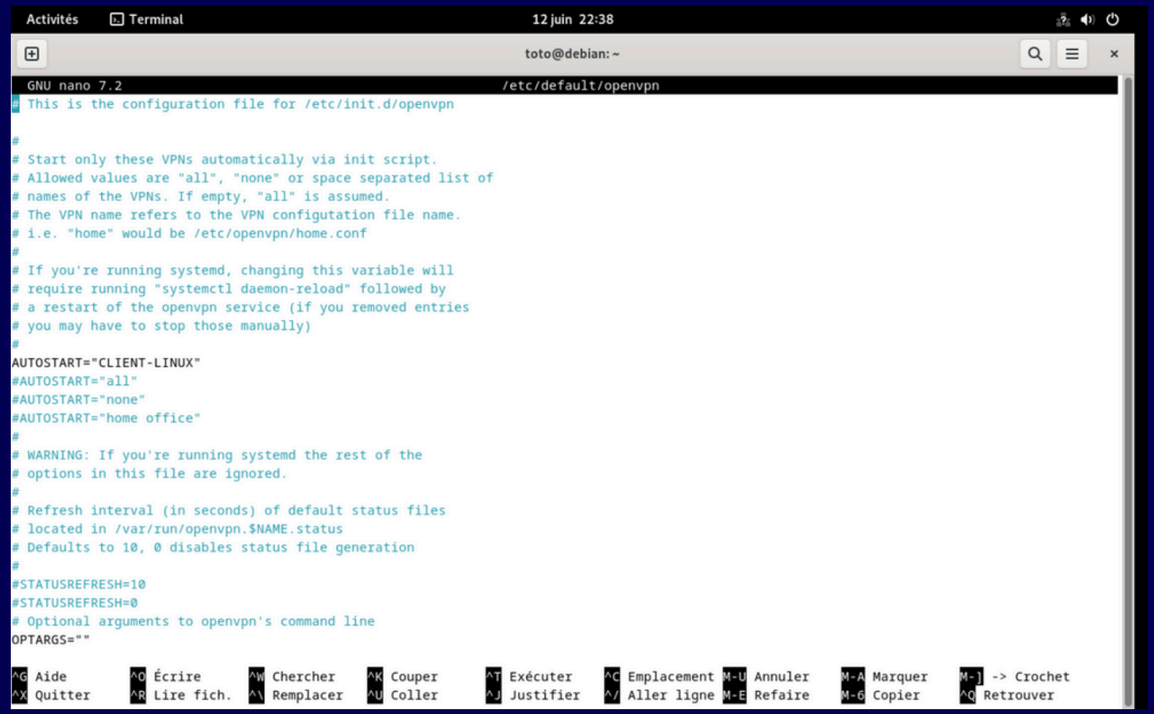
Après l’exportation de la configuration OpenVPN de pFSense, on place ces fichiers dans /etc/openvpn/

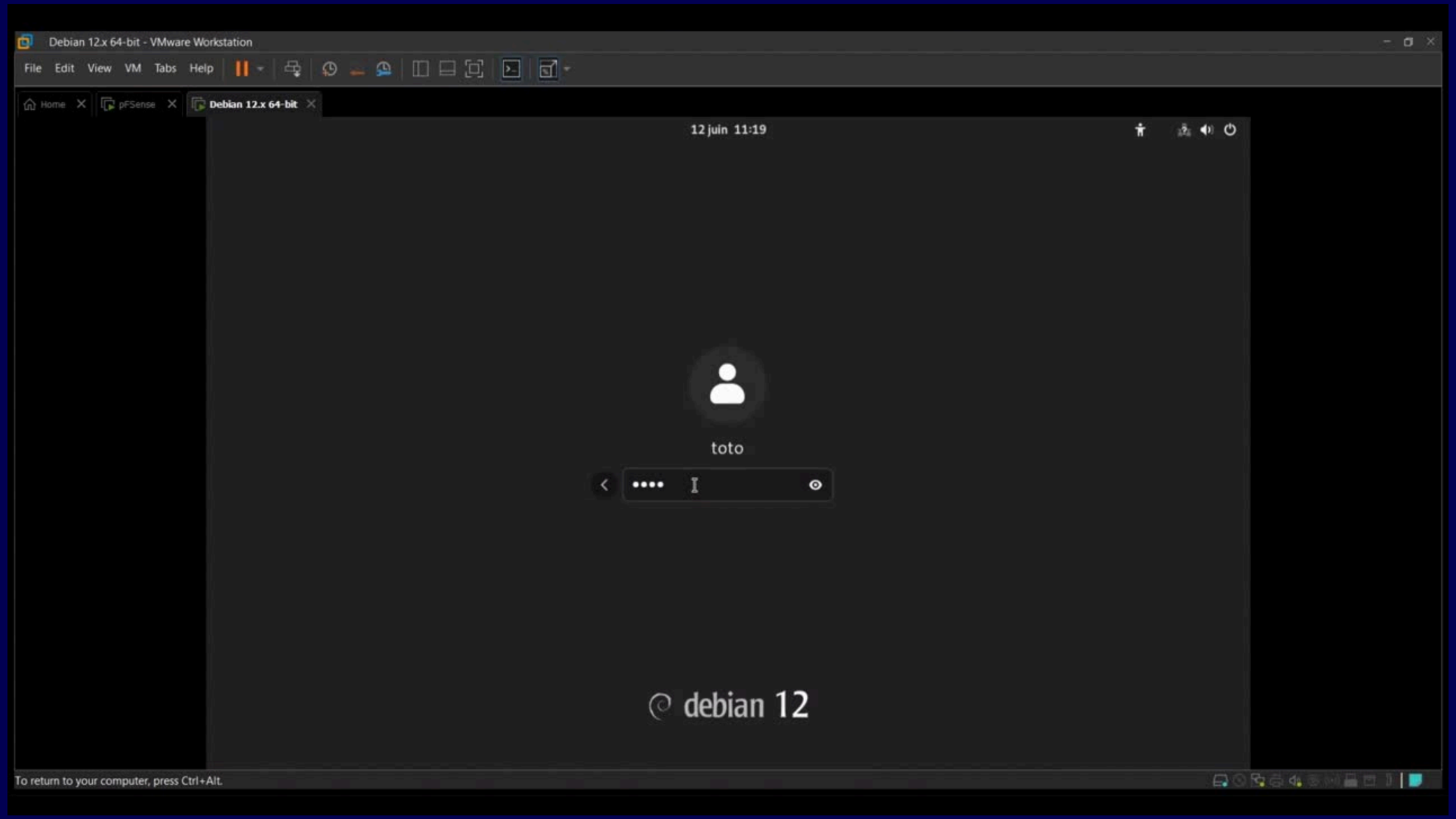


# MONTAGE DU VPN AU DÉMARRAGE DE LA MACHINE

Après l’importation des fichiers dans le dossier openvpn, il suffit de déclarer notre connexion en autostart dans le fichier /etc/default/openvpn.




Debian 12.x 64-bit - VMware Workstation
File Edit View VM Tabs Help
Home
pFSense
Debian 12.x 64-bit
12 juin 11:19
toto
debian 12
To return to your computer, press Ctrl+Alt.

# DNS

Pour la configuration DNS nous avons choisi le nom de domaine ‘sae’ et le suffixe dns ‘fr’

## Mise en place des zones principales et secondaires

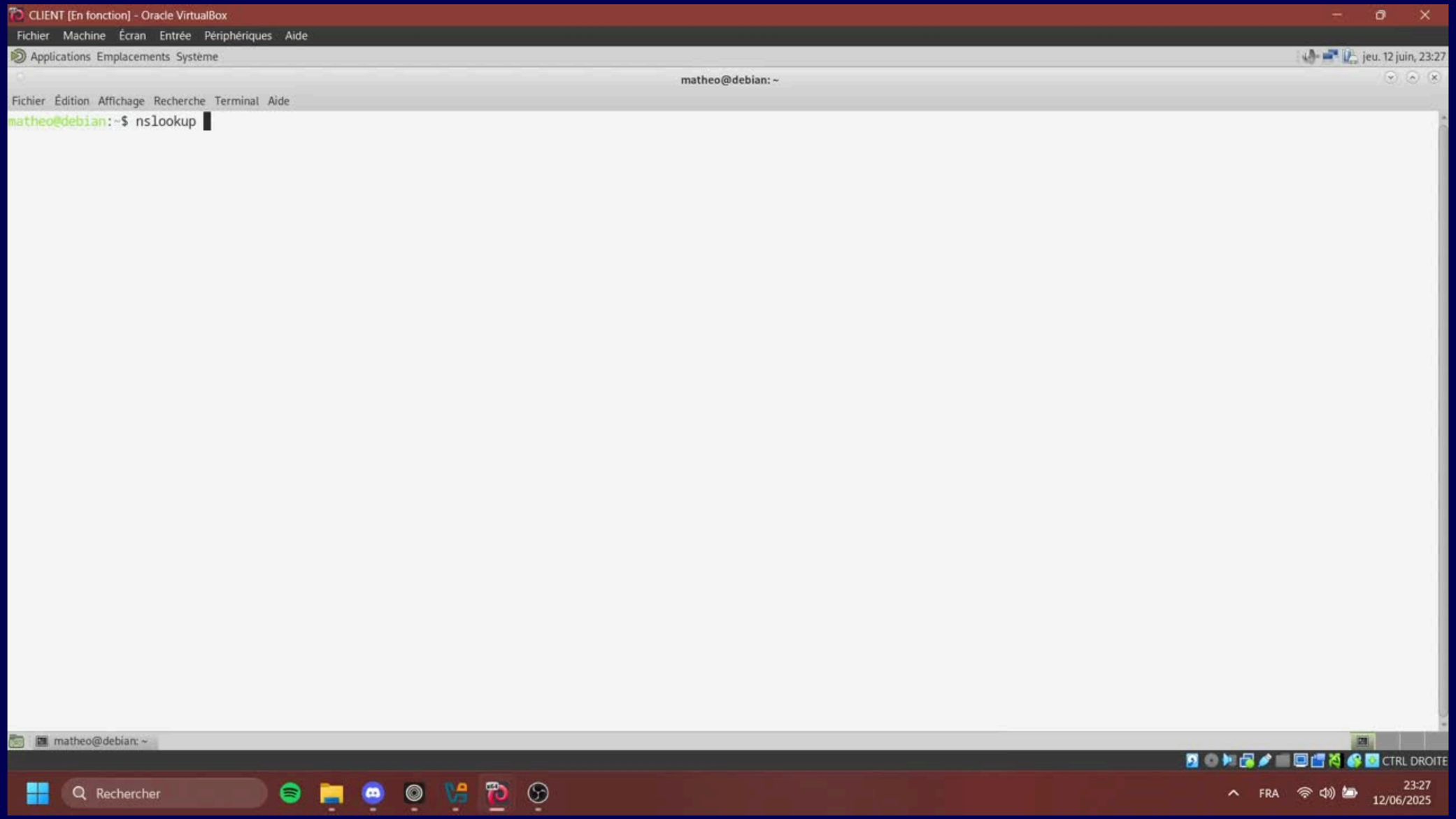
```
$TTL 1d ;
$ORIGIN 1.168.192.in-addr.arpa.

@ IN SOA ns.sae.fr. root.sae.fr. (
    2025060201  ; Serial
    7200        ; Refresh
    120         ; Retry
    2419200     ; Expire
    604800      ; Negative cache TTL
)

@   IN  NS ns.sae.fr.
112 IN PTR ns.sae.fr.
```

```
;
; BIND data file for sae.fr
;
$TTL 604800
@ IN SOA sae.fr. root.sae.fr. (
    20250602 ; Serial
    7200     ; Refresh
    120      ; Retry
    2419200  ; Expire
    604800)  ; Default TTL
;

@ IN NS ns.sae.fr.
ns.sae.fr. IN A 192.168.1.112
@ IN A 192.168.1.112
```

## Mise en place des configurations local pour les zones

```
//
// Do any local configuration here
//
zone "sae.fr" {
    type master;
    file "/etc/bind/zones/master/sae.fr.db";
};

zone "1.168.192.in-addr.arpa" {
    type master;
    file "/etc/bind/zones/master/192.168.1.rev";
};
```

# EXEMPLE DE FONCTIONNEMENT



# LDAP

Exemple du fichier user matheo.ldif contenant les configs de l'utilisateur matheo et résultat de la commande : ldapsearch -x -H ldaps://ldap.sae.fr -b dc=sae,dc=fr

```
root@debian:/etc/ssl# ldapsearch -x -H ldaps://ldap.sae.fr -b dc=sae,dc=fr
# extended LDIF
#
# LDAPv3
# base <dc=sae,dc=fr> with scope subtree
# filter: (objectclass=*)
# requesting: ALL
#

# sae.fr
dn: dc=sae,dc=fr
objectClass: top
objectClass: dcObject
objectClass: organization
o: sae
dc: sae

# Group, sae.fr
dn: ou=Group,dc=sae,dc=fr
objectClass: top
objectClass: organizationalUnit
ou: Group
description: Groupes

# myusers, Group, sae.fr
dn: cn=myusers,ou=Group,dc=sae,dc=fr
objectClass: top
objectClass: posixGroup
cn: myusers
gidNumber: 1005

# People, sae.fr
```

```
dn: uid=matheo,ou=people,dc=sae,dc=fr
objectClass: top
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: shadowAccount
uid: matheo
cn: Matheo LeCrack
sn: LeCrack
userPassword: {CRYPT}$6$lMHl4tF0PI7kp4tY$ZhYXRylMK57.zNRIj48Q8w
uidNumber: 1005
gidNumber: 1005
homeDirectory: /home/matheo
loginShell: /bin/bash
gecos: Matheo LeCrack
```

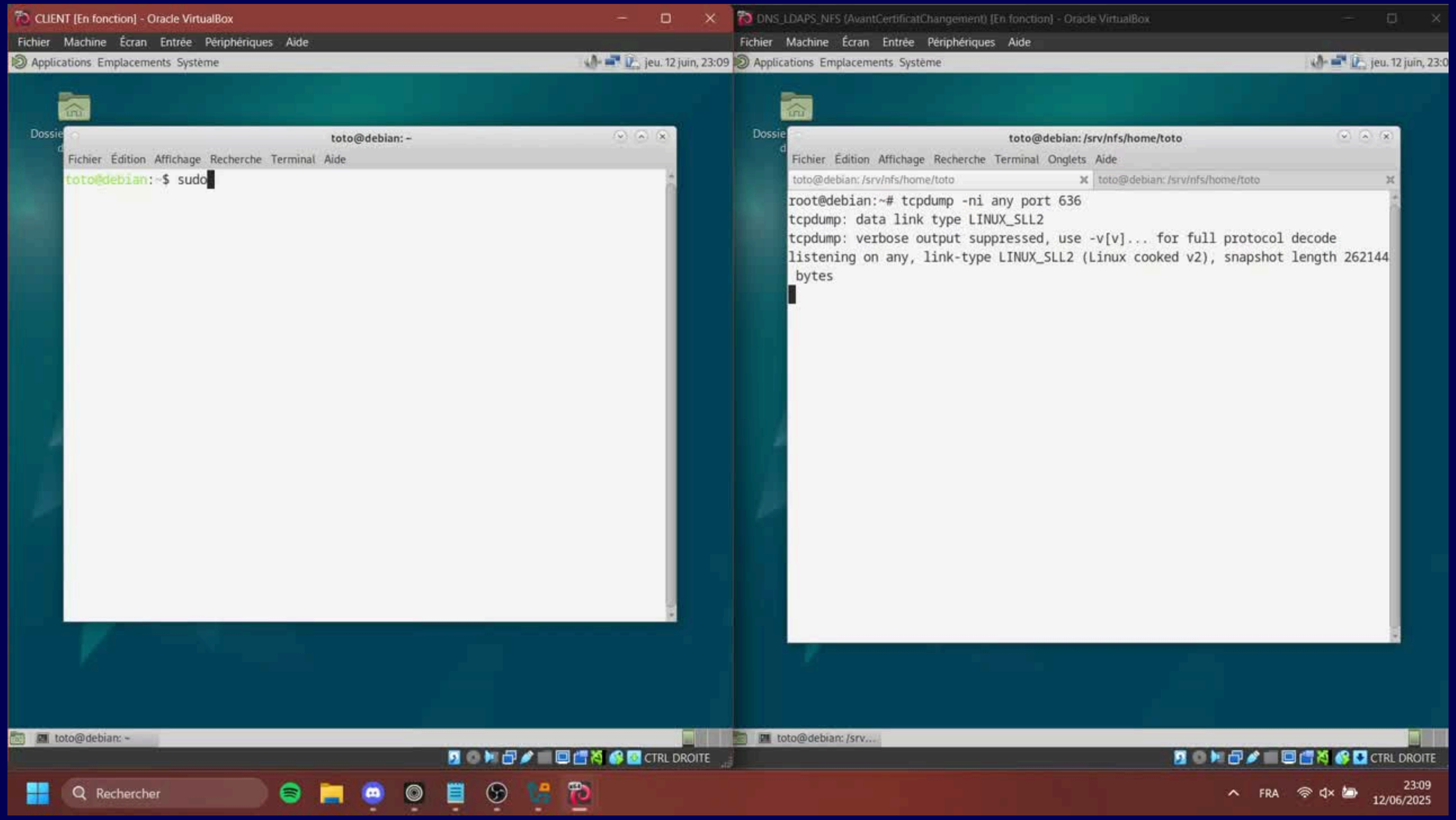
# LDAPS


Configuration des fichier pour indiquer les certificats à utiliser dans le /etc/ldap.conf et /etc/ssl/certinfo.ldif pour le fonctionnement de LDAPS

```
# See ldap.conf(5) for details
# This file should be world readable but not world writable.

BASE    dc=sae,dc=fr
URI     ldaps://ldap.sae.fr
#ldap://ldap-provider.example.com:666

#SIZELIMIT      12
#TIMELIMIT      15
#DEREF          never

# TLS certificates (needed for GnuTLS)
TLS_CACERT /etc/ssl/certs/mycacert.pem
```

```
 GNU nano 7.2                    certinfo.ldif
dn: cn=config
changetype: modify
add: olcTLSCACertificateFile
olcTLSCACertificateFile: /etc/ssl/certs/mycacert.pem
-
add: olcTLSCertificateFile
olcTLSCertificateFile: /etc/ldap/sae_slapd_cert.pem
-
add: olcTLSCertificateKeyFile
olcTLSCertificateKeyFile: /etc/ldap/sae_slapd_key.pem
```

# EXEMPLE NFS ET LDAPS



# POINTS À AMÉLIORER

- Ports du service VPN
- Connexion du VPN via le LDAPs
- Ajout des services manquants
  → Serveur Web dans DMZ
  → Service de mail