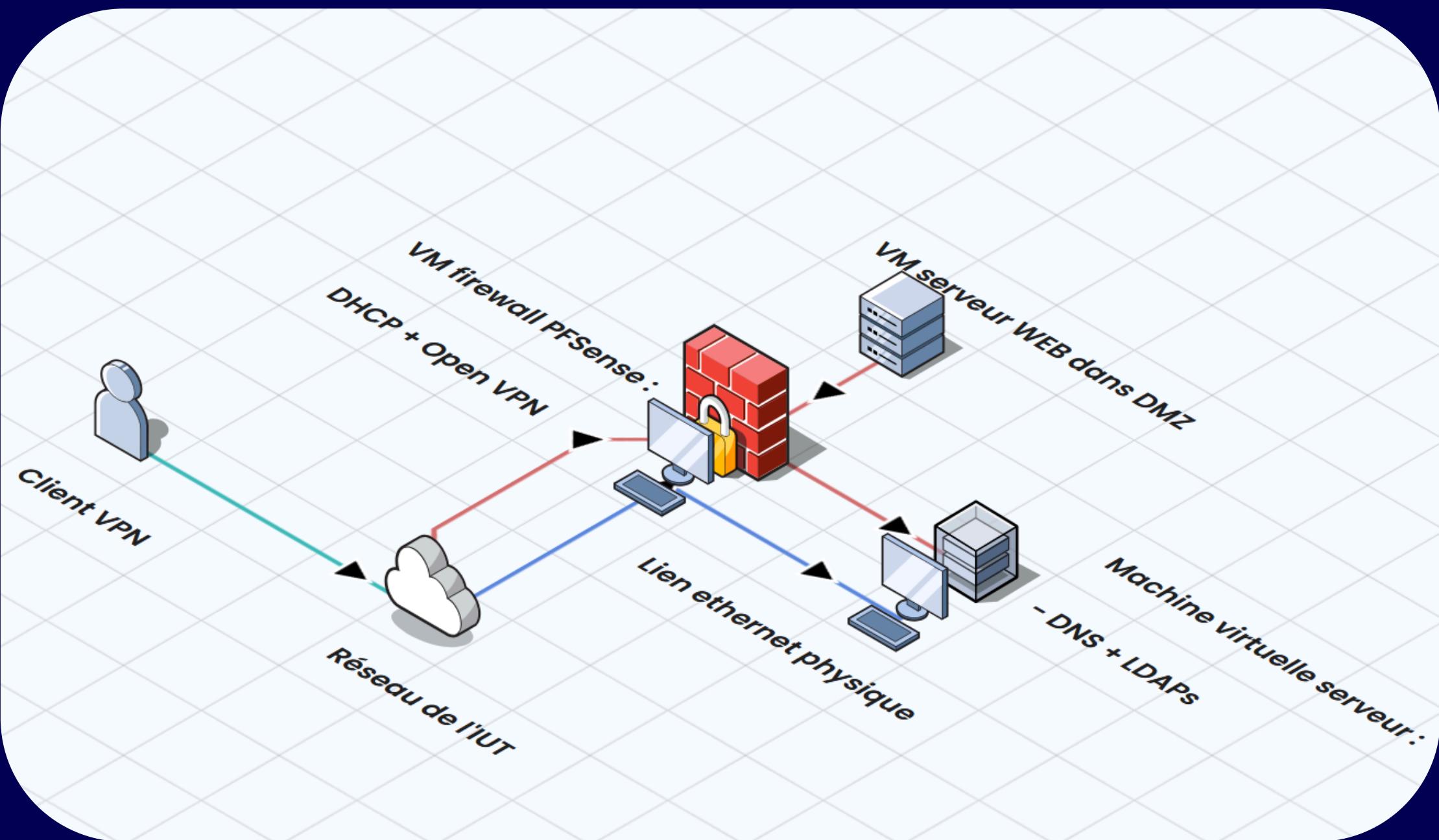


SAE4.01

SECURISER UN SYSTEME D'INFORMATION

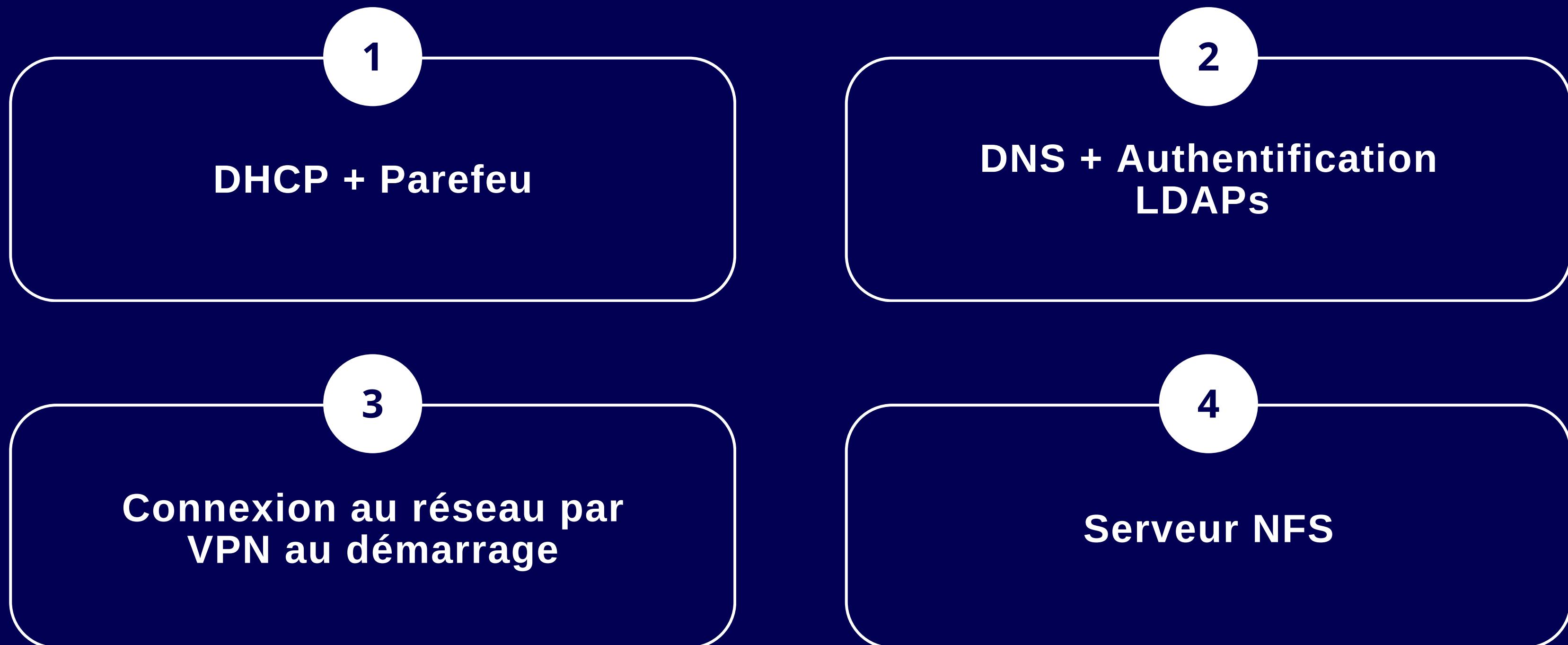
FRITSCHY - ROBIN

PLAN RÉSEAU

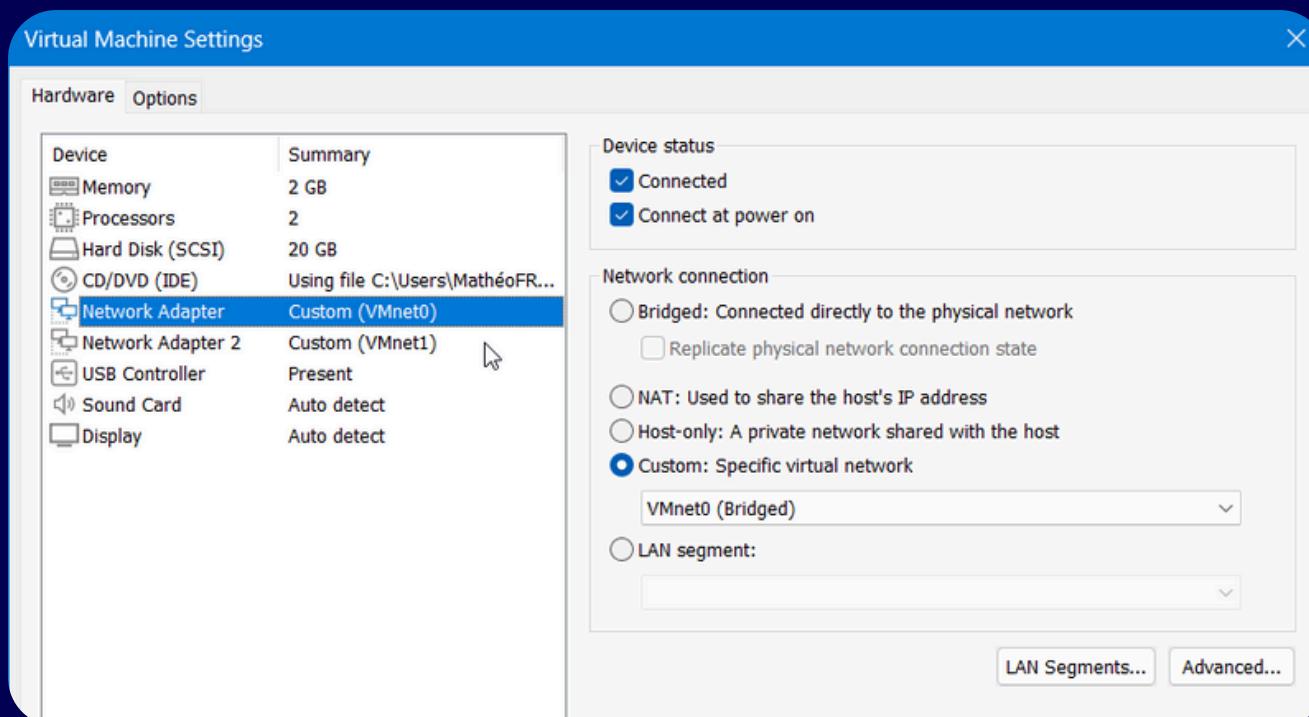
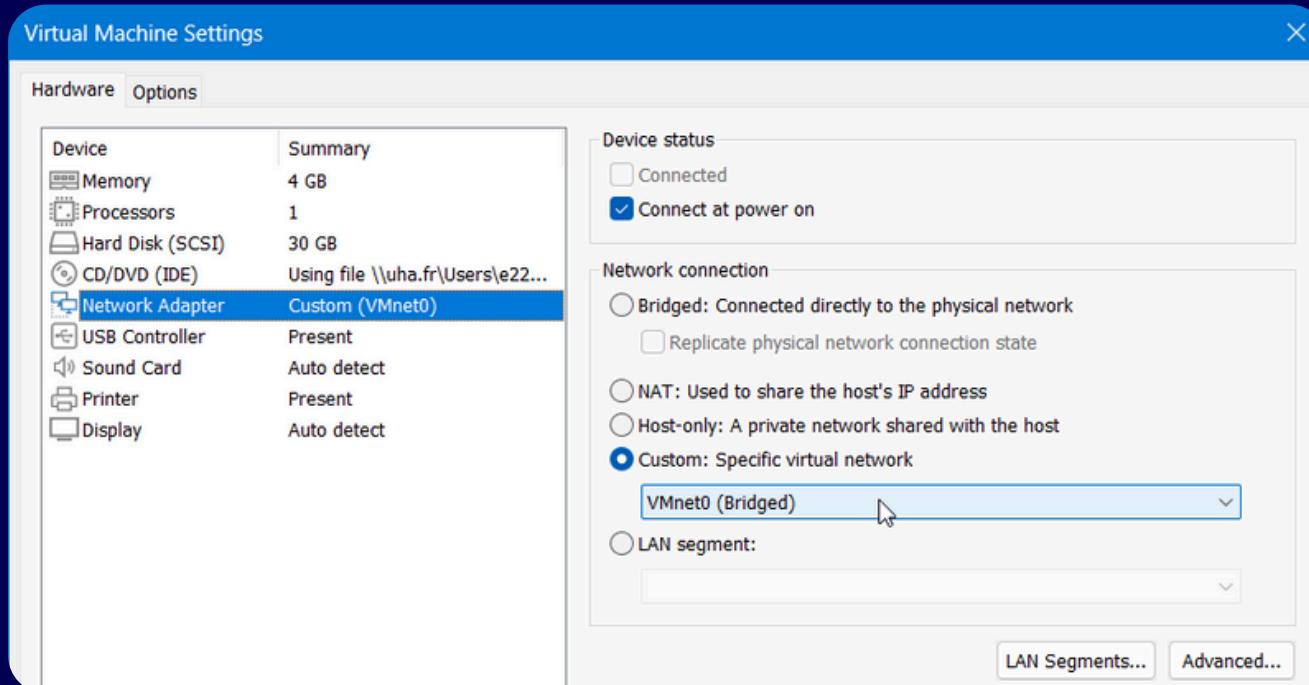


- Environnement virtualisé sous VMware Workstation Pro et Virtualbox.
- Ordinateurs physiquement reliés par câble ethernet
- Parefeu servant de routeur

SERVICES MIS EN PLACE



ADRESSAGE IP



Virtual Network Editor					
Name	Type	External Connection	Host Connection	DHCP	Subnet Address
VMnet0	Bridged	Realtek PCIe GbE Family Contr...	-	-	-
VMnet1	Bridged	ASIX AX88179 USB 3.0 to Giga...	-	-	-

```
WAN -> em0
LAN -> em1

Do you want to proceed [y\?n]? y

Writing configuration...done.
One moment while the settings are reloading... done!
VMware Virtual Machine - Netgate Device ID: 69a00119301924aed678

*** Welcome to pfSense 2.7.2-RELEASE (amd64) on pfSense ***
WAN (wan)      -> em0      -> v4/DHCP4: 10.128.200.15/16
LAN (lan)      -> em1      -> v4: 192.168.1.100/24

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: ■
```

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.

Firewall / Rules / WAN

Floating **WAN** LAN OpenVPN

Rules (Drag to Change Order)

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	IPv4 ICMP	10.128.0.0/16	*	*	*	*	none			
<input checked="" type="checkbox"/>	0/0 B	any								
<input type="checkbox"/>	IPv4 UDP	*	*	*	1194 (OpenVPN)	*	none		Accès distant OpenVPN	
										Add Add

Firewall / Rules / LAN

Floating **LAN** WAN OpenVPN

Rules (Drag to Change Order)

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	2/339 KiB	*	*	*	LAN Address	80	*	*	Anti-Lockout Rule	
<input checked="" type="checkbox"/>	0/0 B	IPv4 ICMP	*	*	*	*	*	*	none	
<input type="checkbox"/>	any									
<input checked="" type="checkbox"/>	1/384 B	IPv4 *	LAN subnets	*	*	*	*	*	Default allow LAN to any rule	
<input checked="" type="checkbox"/>	0/0 B	IPv4 ICMP	*	*	*	*	*	*	none	
<input checked="" type="checkbox"/>	any									
<input checked="" type="checkbox"/>	0/0 B	IPv4 TCP	*	*	LAN address	636 (LDAP/S)	*	*	none	
										Add Add

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 i Valid From: Fri, 06 Jun 2025 07:06:20 +0000 Valid Until: Mon, 04 Jun 2035 07:06:20 +0000	In Use		

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



OPENVPN

PRESENTATION DE LA CONNEXION SECURISEE

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



```
toto@debian:~
```

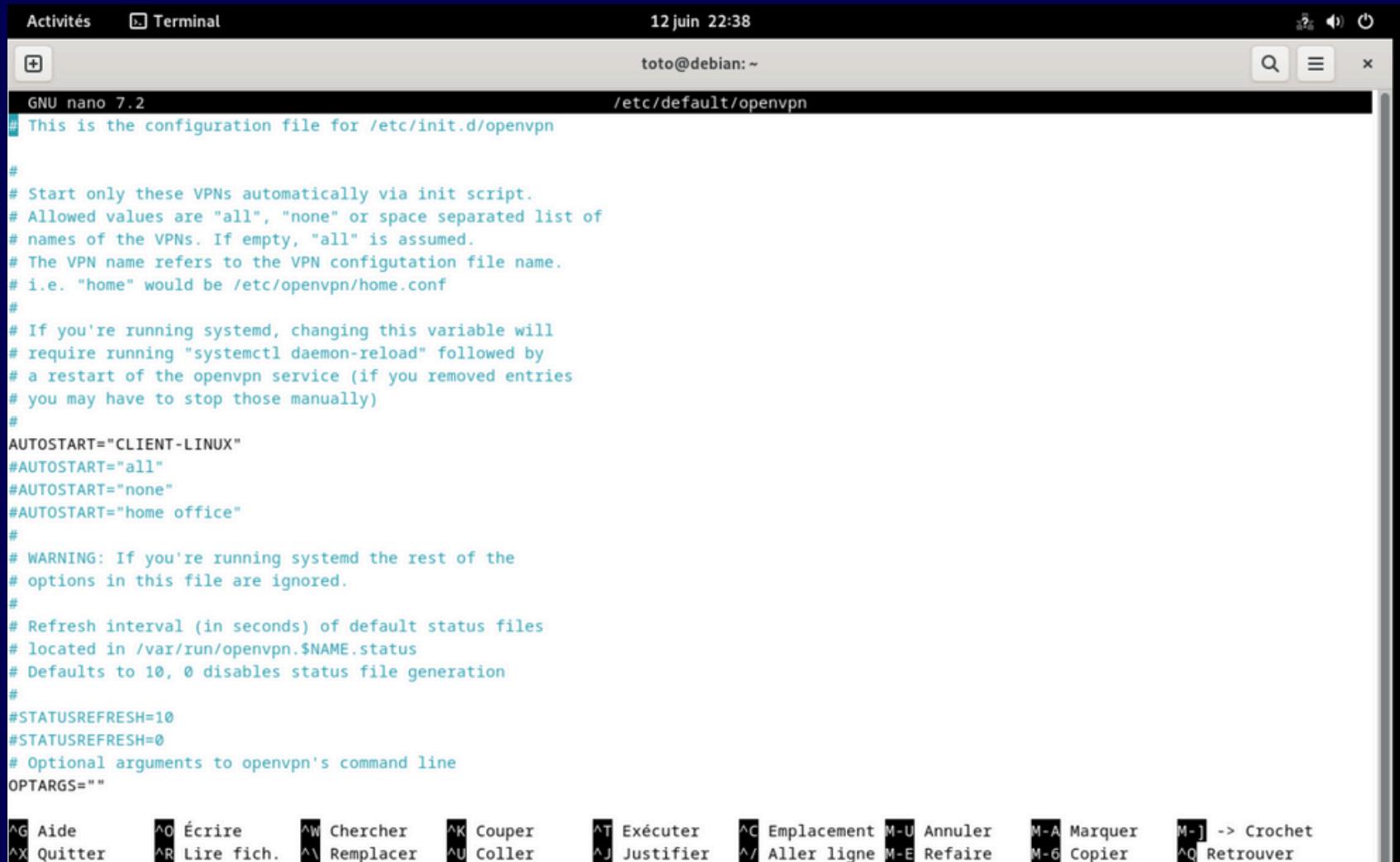
```
GNU nano 7.2          /etc/openvpn/CLIENT-LINUX.conf
dev tun
persist-tun
persist-key
data-ciphers AES-256-GCM:AES-128-GCM:CHACHA20-POLY1305:AES-256-CBC
data-ciphers-fallback AES-256-CBC
auth SHA256
tls-client
client
resolv-retry infinite
remote 10.128.200.15 1194 udp4
nobind
verify-x509-name "cert-firewall" name
auth-user-pass auth.txt
pkcs12 pfSense-UDP4-1194-vpn-user.p12
tls-auth pfSense-UDP4-1194-vpn-user-tls.key 1
remote-cert-tls server
explicit-exit-notify
auth-nocache
```

[Lecture de 18 lignes]

^G Aide ^O Écrire ^W Chercher ^K Couper ^T Exécuter ^C Emplacement M-U Annuler
^X Quitter ^R Lire fich. ^\ Remplacer ^U Coller ^J Justifier ^/ Aller ligne M-E Refaire

MONTAGE DU VPN AU DÉMARRAGE DE LA MACHINE

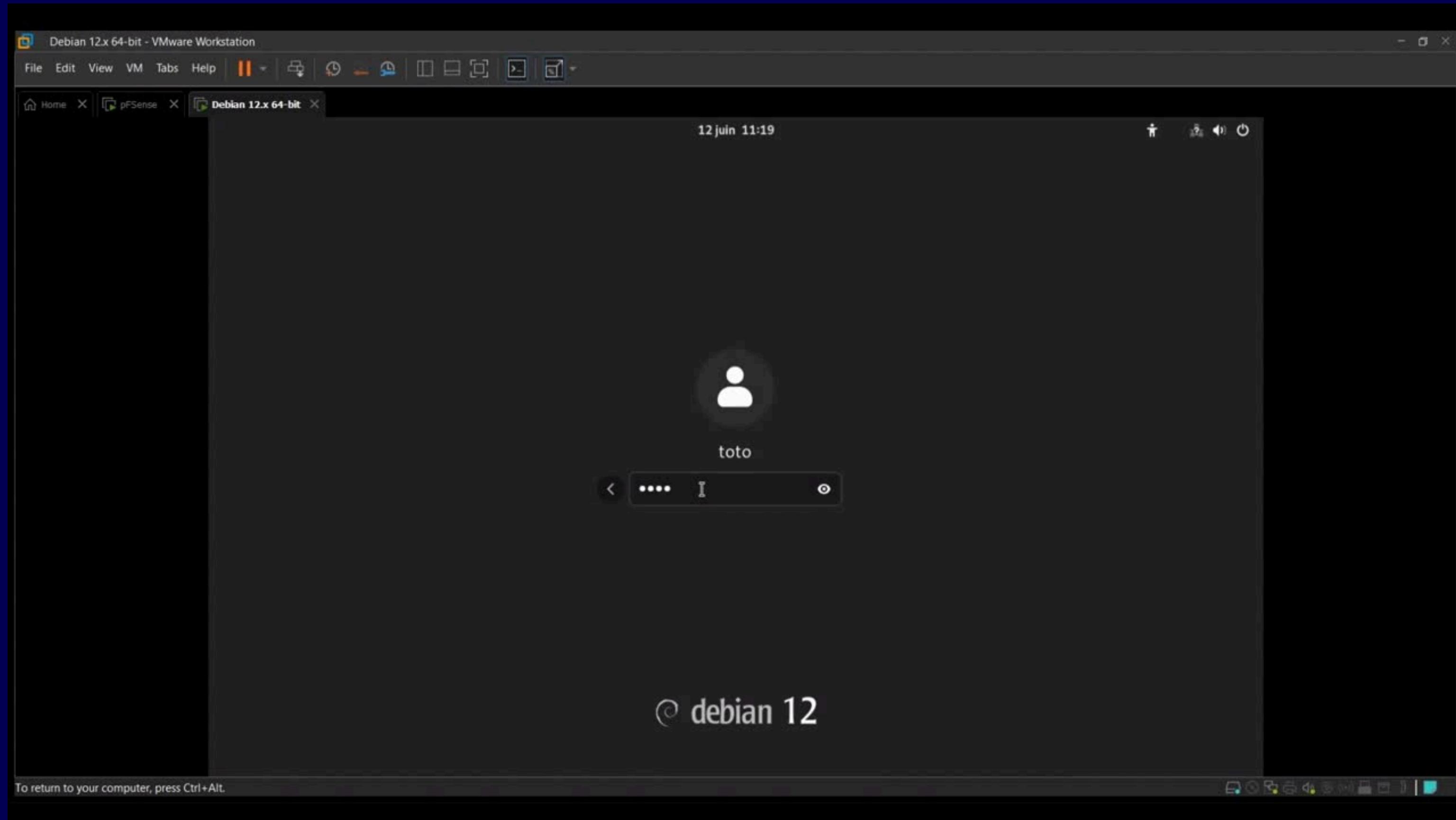
Après l'importation des fichiers dans le dossier openvpn, il suffit de déclarer notre connexion en autostart dans le fichier /etc/default/openvpn.



The screenshot shows a terminal window titled "Activités" with a "Terminal" icon. The window title bar says "toto@debian:~". The terminal window displays the contents of the file "/etc/default/openvpn" using the "GNU nano 7.2" editor. The file contains configuration options for the OpenVPN service, specifically regarding automatic startup. Key lines include "# This is the configuration file for /etc/init.d/openvpn", "# Start only these VPNs automatically via init script.", and "# AUTOSTART="CLIENT-LINUX" which is currently commented out with a '#'. The bottom of the screen shows the standard nano key bindings.

```
GNU nano 7.2          12 juin 22:38
# This is the configuration file for /etc/init.d/openvpn

#
# Start only these VPNs automatically via init script.
# Allowed values are "all", "none" or space separated list of
# names of the VPNs. If empty, "all" is assumed.
# The VPN name refers to the VPN configuration file name.
# i.e. "home" would be /etc/openvpn/home.conf
#
# If you're running systemd, changing this variable will
# require running "systemctl daemon-reload" followed by
# a restart of the openvpn service (if you removed entries
# you may have to stop those manually)
#
AUTOSTART="CLIENT-LINUX"
#AUTOSTART="all"
#AUTOSTART="none"
#AUTOSTART="home office"
#
# WARNING: If you're running systemd the rest of the
# options in this file are ignored.
#
# Refresh interval (in seconds) of default status files
# located in /var/run/openvpn.$NAME.status
# Defaults to 10, 0 disables status file generation
#
#STATUSREFRESH=10
#STATUSREFRESH=0
# Optional arguments to openvpn's command line
OPTARGS=""
```





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
);

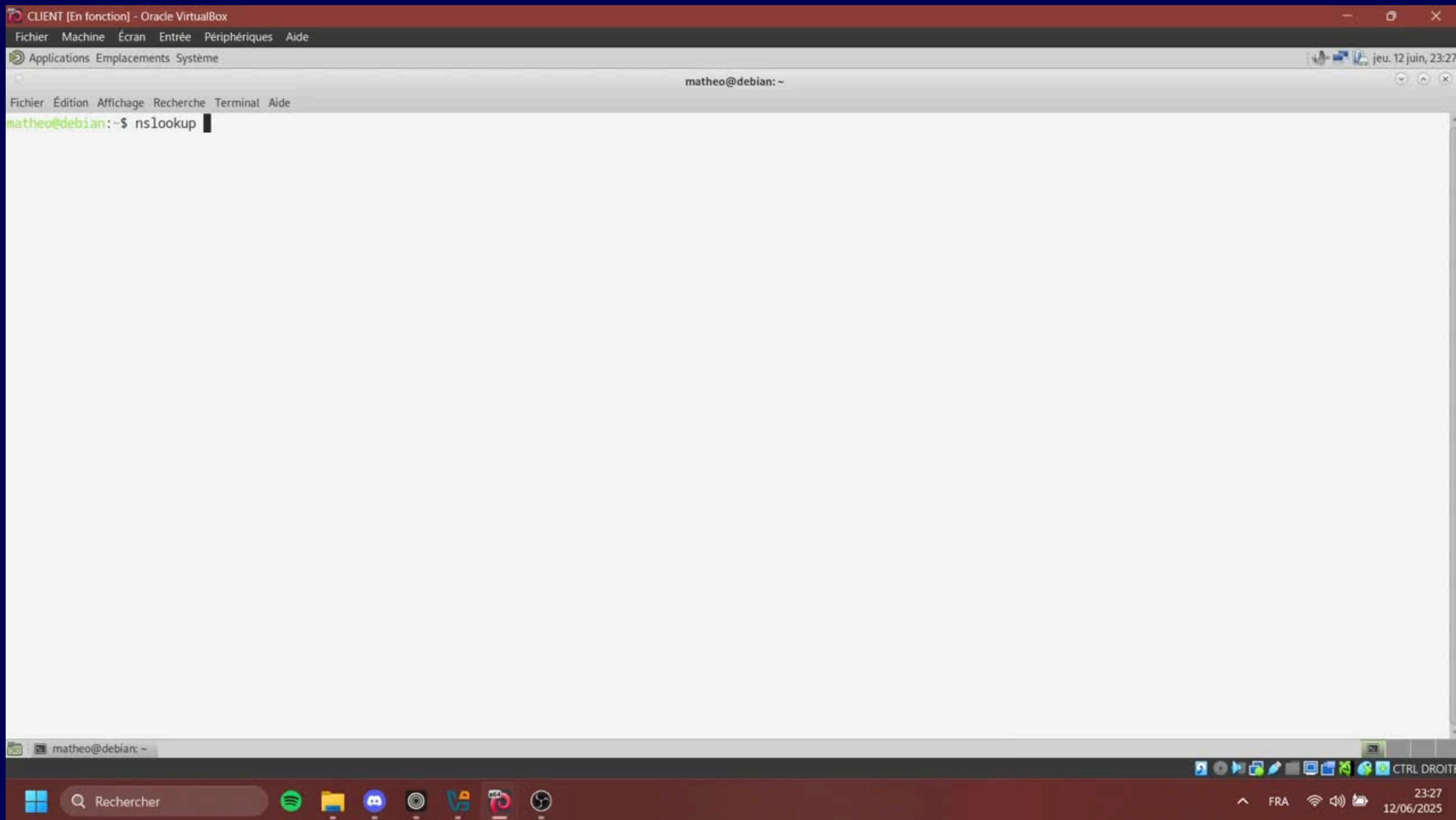
@ IN NS ns.sae.fr.
ns.sae.fr. IN A 192.168.1.112
@ IN A 192.168.1.112
```

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

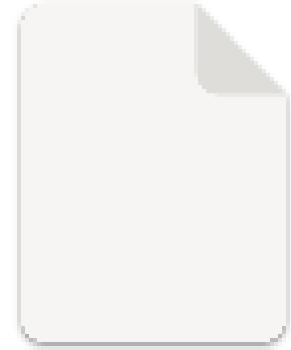
# Group, sae.fr
dn: ou=Group,dc=sae,dc=fr
objectClass: top
objectClass: organizationalUnit
ou: Group
description: Groupes

# 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$1MHl4tF0PI7kp4tY$ZhYXRylMK57.zNRIj48Q8w
uidNumber: 1005
gidNumber: 1005
homeDirectory: /home/matheo
loginShell: /bin/bash
gecos: Matheo LeCrack
```

LDAPS



mycacert.crt



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.

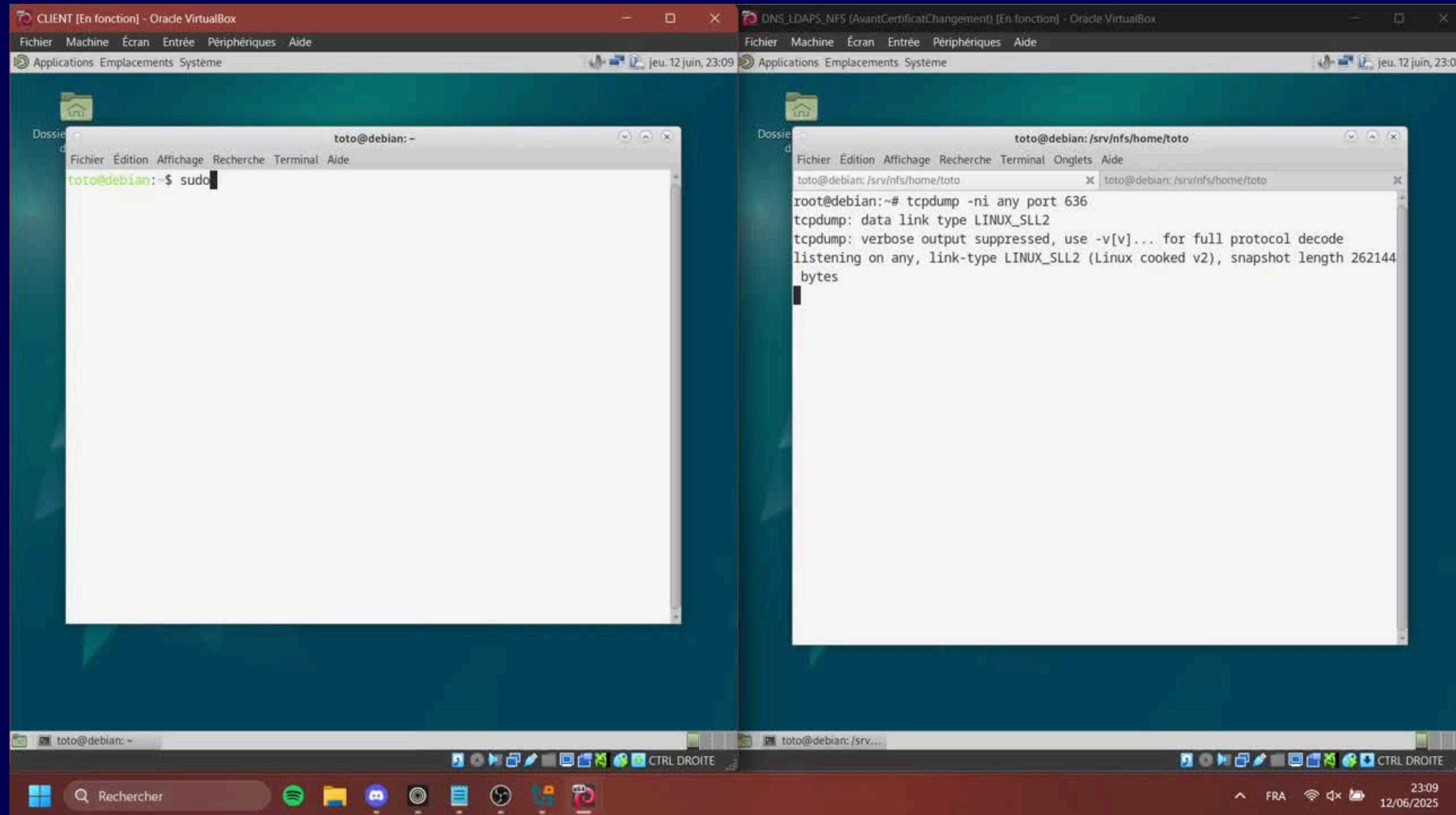
BASE    dc=sae,dc=fr
URI     ldaps://ldap.sae.fr
#ldap://ldap-provider.example.com:666

#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: olcTSLCertificateFile
olcTSLCertificateFile: /etc/ldap/sae_slapd_cert.pem
-
add: olcTSLCertificateKeyFile
olcTSLCertificateKeyFile: /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