procédure pour mettre en place un proxy OPNsens

Téléchargement de OPNsens

Download - OPNsense

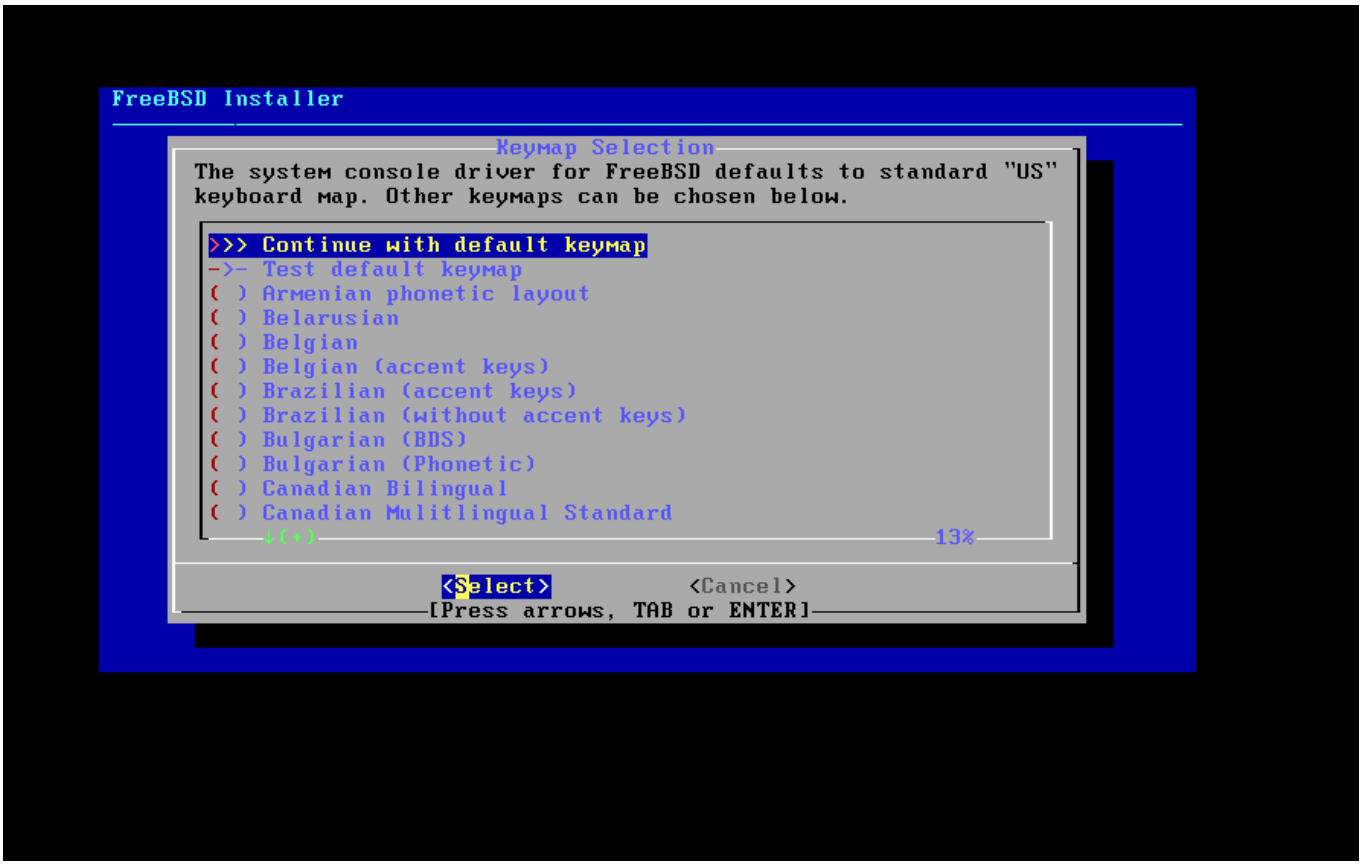
Mise en place d'OPNsens

bien prendre le format DVD

Extraire le dossier téléchargé

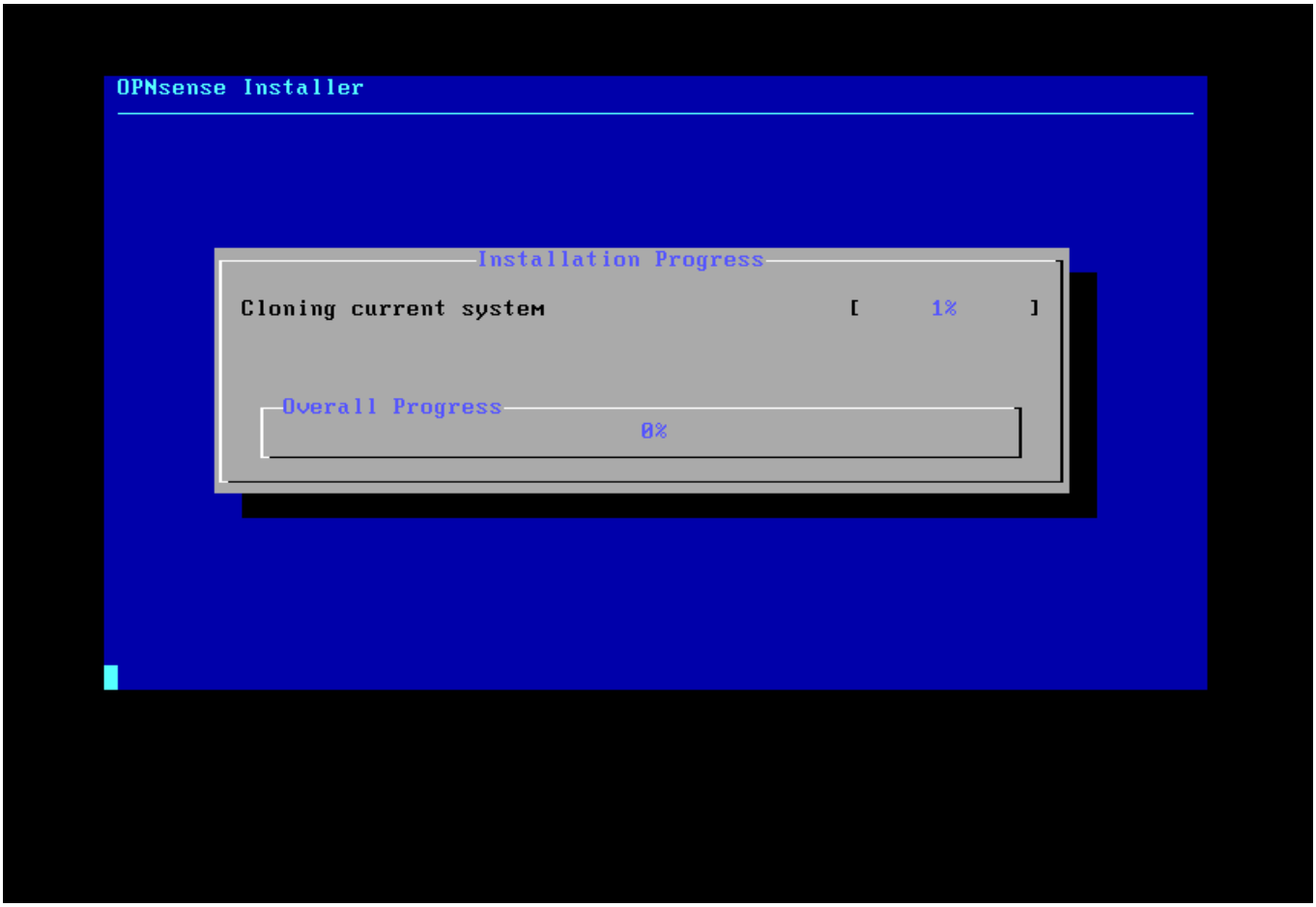
Faire une VM

les login de base OPNsense Installer opnsense



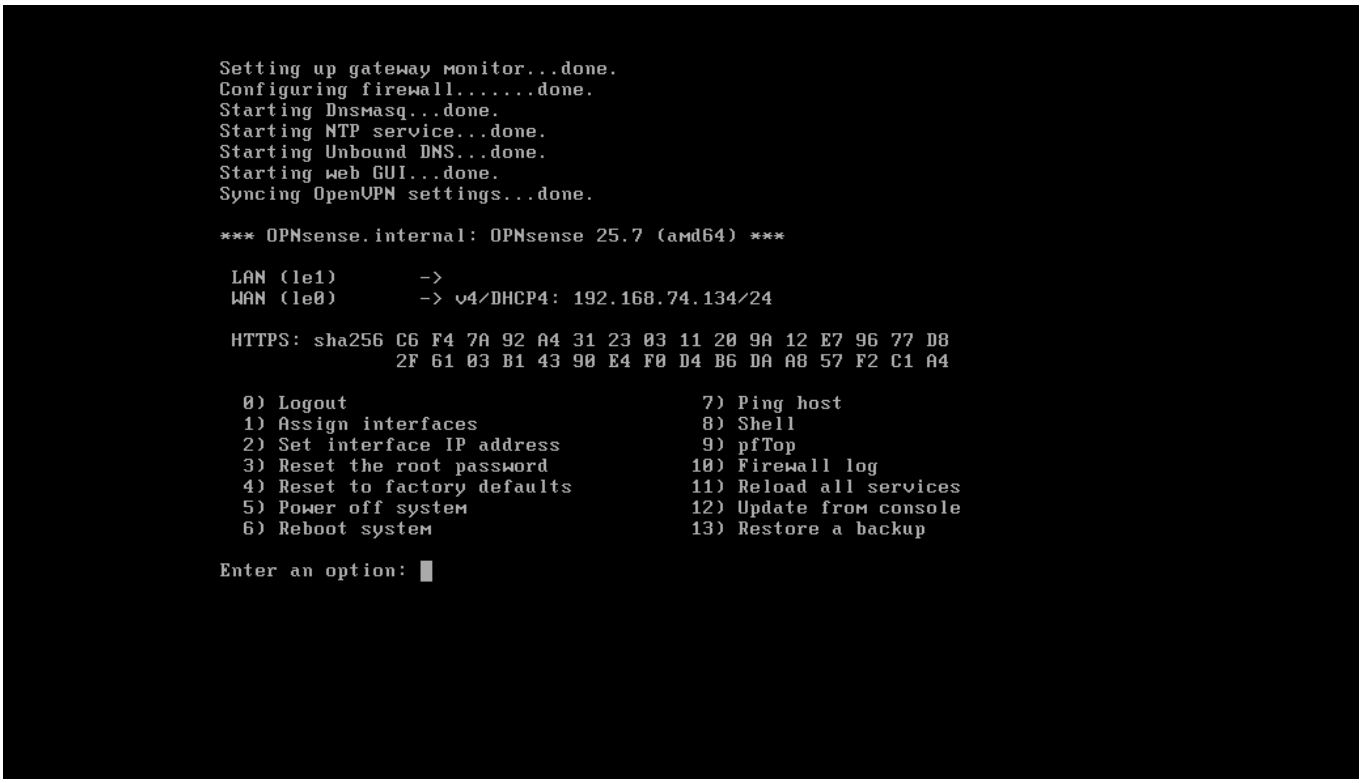
Tout mettre en ok

sélectionner le disque dur virtuel



choisir l'option 1 poour configurer les carte réseaux LAN et WAN

Puis l'option 2 pour configurer le LAN



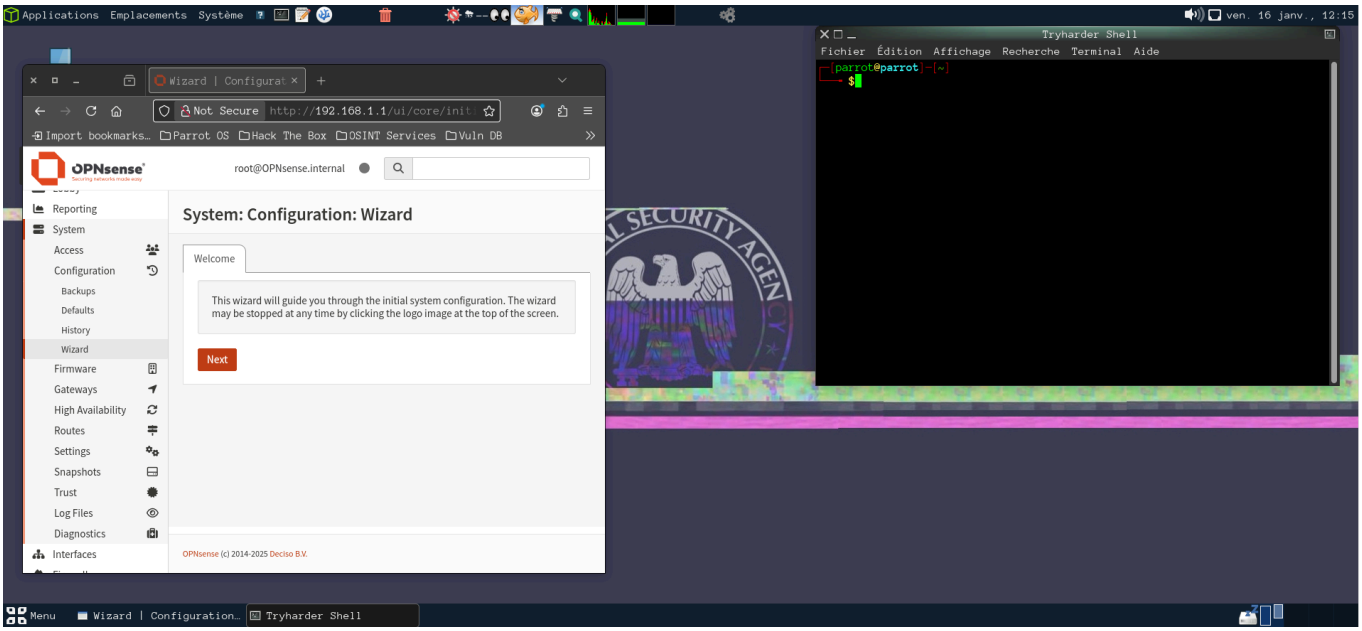
```
Enter an option: 2

Available interfaces:

1 - LAN (le1 - dhcp)
2 - WAN (le0 - dhcp, dhcp6)

Enter the number of the interface to configure: 1

Configure IPv4 address LAN interface via DHCP? [y/N] y

Configure IPv6 address LAN interface via WAN tracking? [Y/n] n
Configure IPv6 address LAN interface via DHCP6? [y/N] n

Enter the new LAN IPv6 address. Press <ENTER> for none:
>

Do you want to change the web GUI protocol from HTTPS to HTTP? [y/N] y
Restore web GUI access defaults? [y/N] n

Writing configuration...done.
Generating /etc/resolv.conf...done.
Generating /etc/hosts...done.
Configuring LAN interface...
```

Finalement il faut pas mettre sur le DHCP l'IP LAN

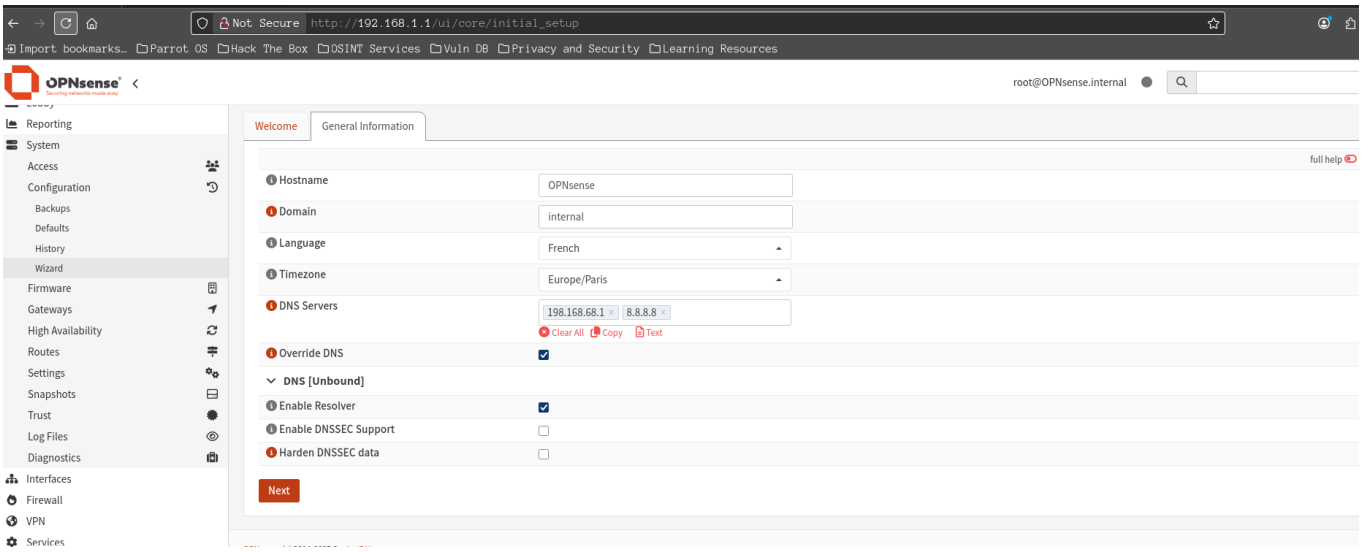
```
Starting Dnsmasq...done.
Starting Unbound DNS...done.
Configuring firewall.......done.
Starting Dnsmasq...done.
Starting Unbound DNS...done.

You can now access the web GUI by opening
the following URL in your web browser:

    http://192.168.1.1

*** OPNsense.internal: OPNsense 25.7 (amd64) ***

 LAN (le1)       -> v4: 192.168.1.1/24
 WAN (le0)       -> v4/DHCP4: 192.168.74.134/24

  0) Logout                              7) Ping host
  1) Assign interfaces                   8) Shell
  2) Set interface IP address            9) pfTop
  3) Reset the root password            10) Firewall log
  4) Reset to factory defaults          11) Reload all services
  5) Power off system                   12) Update from console
  6) Reboot system                      13) Restore a backup

Enter an option:
```

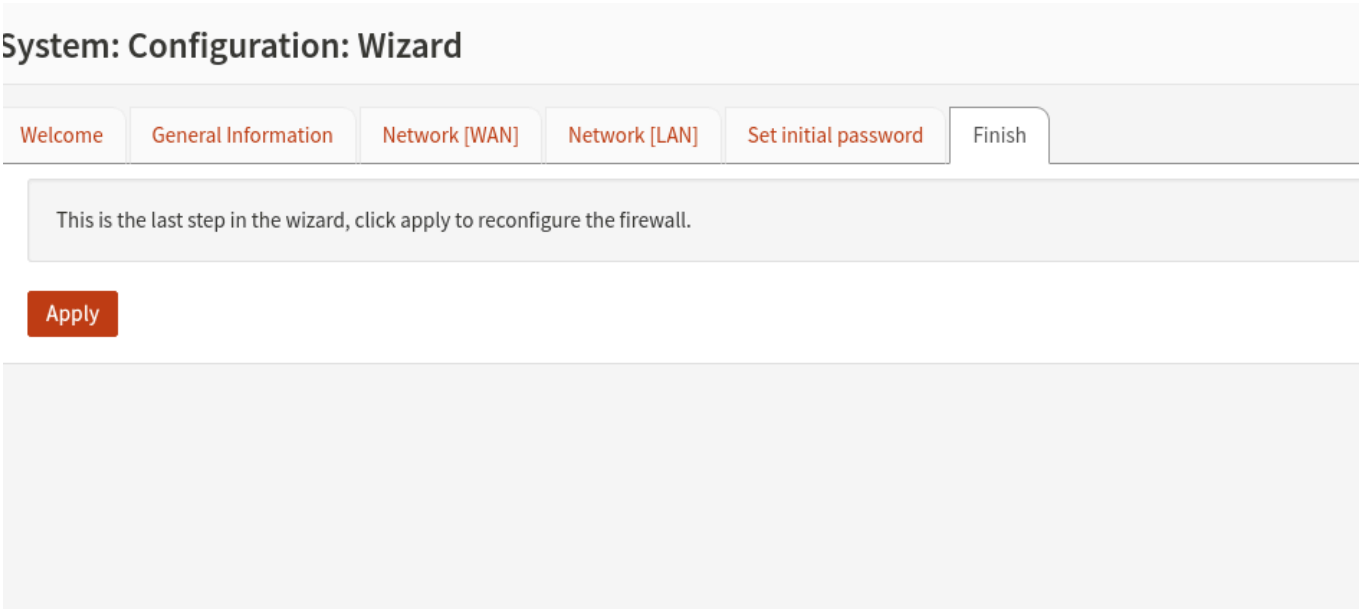
Mettre sur l'autre VM sur lequel on va configurer OPNsense ici LAN segment 1

Se connecter à l'IP LAN sur l'autre VM se connecter en root

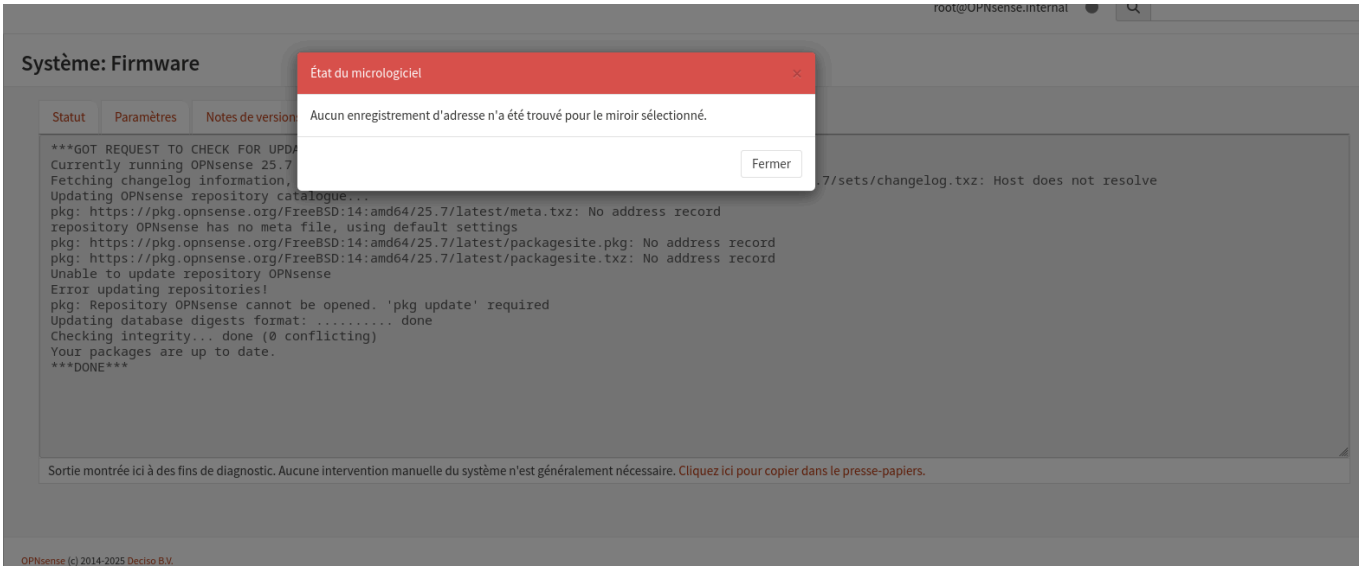


Mise à jour d'OPNsens en ligne de commande `opnsense-update` avec le shell (option 8)
faire next sur l'autre machine





On va vérifier les mises à jour quand même normalement tout est bon



Création d'un certificat SSL sur Linux parrot Sec

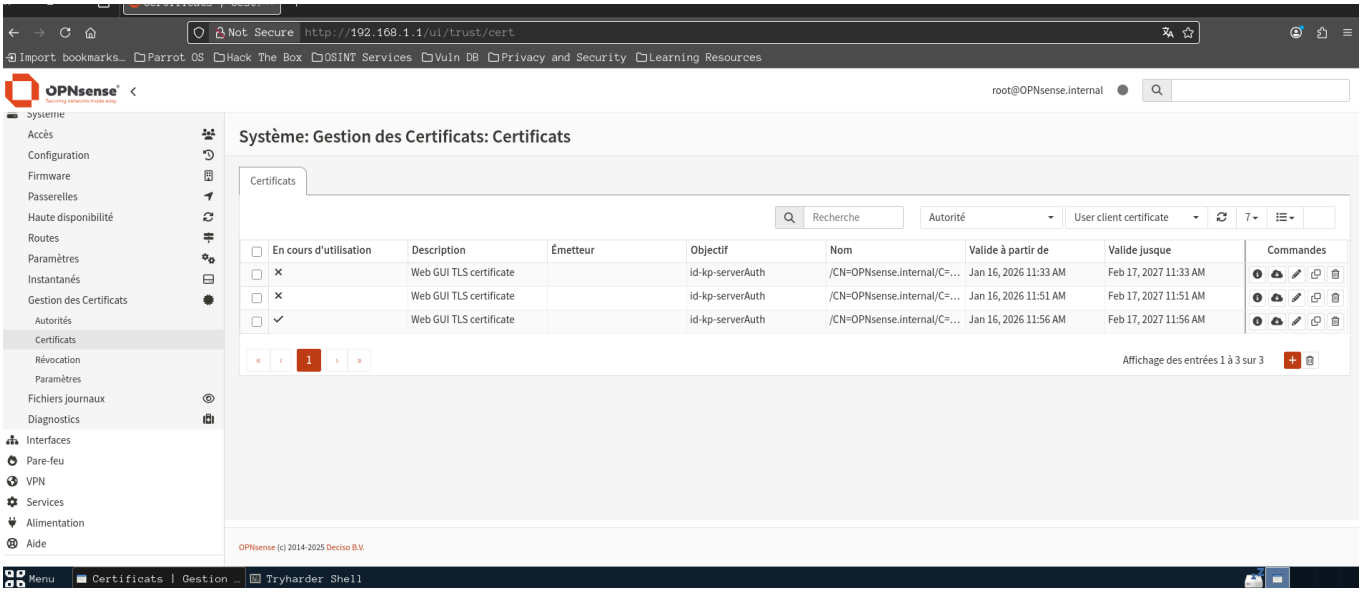
```
#raccourcis clavier pour faire apparaître un shell ctrl+alt+t
#création d'un dossier
mkdir ~/certs-opnsense
#aller dans ce dossier
cd ~/certs-opnsense
#génération de private key
openssl genrsa -out opnsense.key 4096
#généré le certificat auto signé pour une durée de 365 jours
openssl req -new -x509 -sha256 -days 365 -key opnsense.key -out opnsense.crt
#afficher la private key
cat opnsense.key
#afficher le certificat
cat opnsense.crt
```

```
┌─[parrot@parrot]─[~]
└──╼ $mkdir home/cert-opnsense
┌─[parrot@parrot]─[~]
└──╼ $cd home/cert-opnsense
┌─[parrot@parrot]─[~/home/cert-opnsense]
└──╼ $openssl genrsa -out opnsense.key 4096
┌─[parrot@parrot]─[~/home/cert-opnsense]
└──╼ $openssl req -new -x509 -sha256 -days 365 opnsense.key -out opnsense.crt
req: Use -help for summary.
┌─[✗]─[parrot@parrot]─[~/home/cert-opnsense]
└──╼ $openssl req -new -x509 -sha256 -days 365 -key opnsense.key -out opnsense.crt
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:FR
State or Province Name (full name) [Some-State]:
Locality Name (eg, city) []:
Organization Name (eg, company) [Internet Widgits Pty Ltd]:
Organizational Unit Name (eg, section) []:
Common Name (e.g. server FQDN or YOUR name) []:
Email Address []:
┌─[parrot@parrot]─[~/home/cert-opnsense]
└──╼ $cat opnsense.key
-----BEGIN PRIVATE KEY-----
MIIJQgIBADANBgkqhkiG9w0BAQEFAASCCSwwggkoAgEAAoICAQCnKVdaBiFhT933
IXam96DEUJeLbdL3cpTBOFAoj/BC6aOjTfFBvb1BH5n3JxHzSWM7uyCaICsxJvyN
iQSV5JLZYIkkADOGpqBpyzfypFy+/fI0s+/LMF0y7LM2F/Dj/ixJn65qlyl6Onc+
Ya46su3DGO4w2IXyjLKv+ZIS6IzTnmFdxsibmekxgoAh/GZuJIxUovhku1+BPyrV
38fUJoIqZXe/wGlVaMaVtu2egcUHOM+OL2nTxkvlwVWkHAFAUk9PiZIAynlAxqw4
Yk8y4cRsU9nFU9xDB4Fx03+9fl/SozObhZOSzJqqWNe02w93pz7tC7k8Ong+WrIz
gSg1VviLoiTiD1R++ISjdUL8lb/CdzXyurs5YynJKpEZqWdO3thgnv/8gYhIdPOs
3UdREbUm7HXXlBEqv/yLQuCUFi3Gqq8z1xk9oegX/NOZMkvkCgNzhwkQwJqydSbQ
hMfYFYdw8zLJru/bjwbj5fI+mvrDMC5Xwxa7NJsi/hLa6lyP1d5uQBQUDRrhue3r
Pdjq484JSZe3pFUQuQjkI+R5UfEK0OAGbJxbxr/OCWcpDAKD9ki+veHG0op9jv07
```

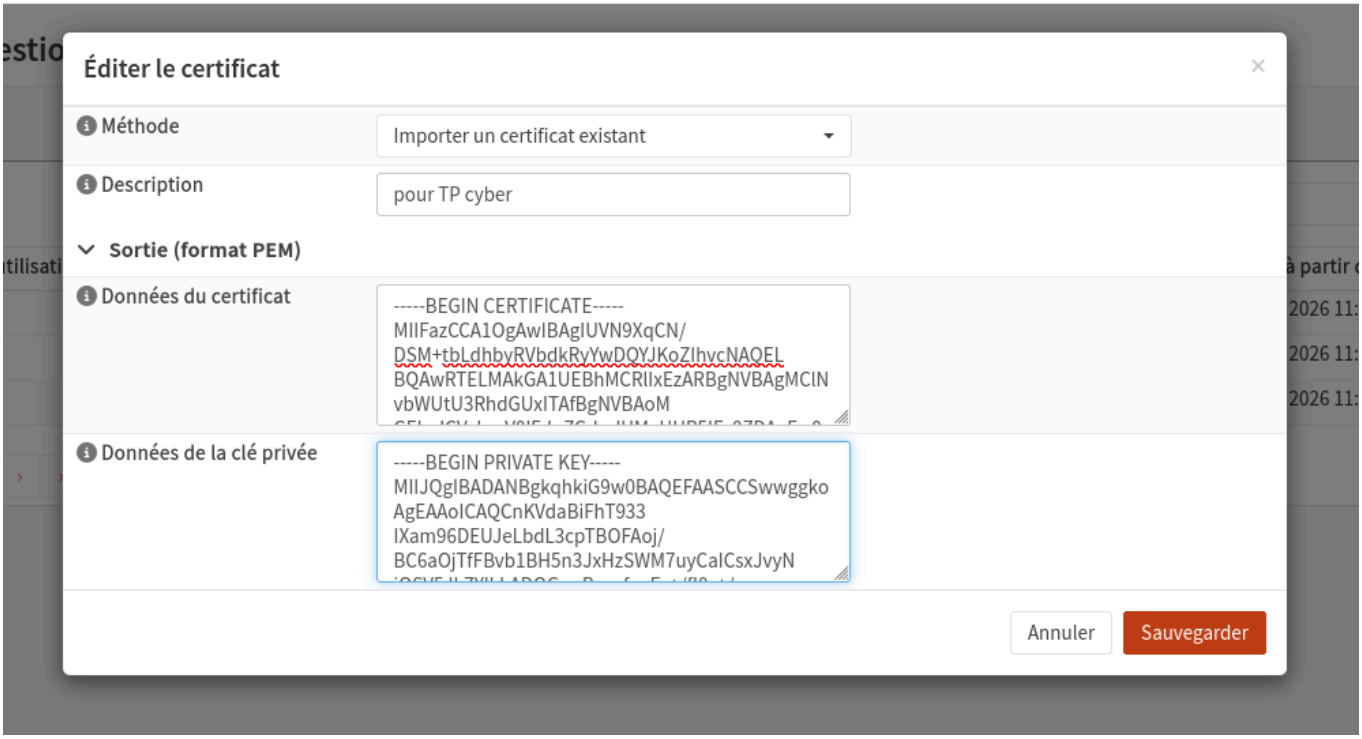
```
2H4qxhWU63gpE12sVw+y3fhVHRf5tK9XSLw3XzjjAmCK7ggam9tKOrqEUOzmE9XZ
Pd1afMz5dIQk/fOIT3A8pn7rWRYp73RRiIhFFCPO8nZra3dDuBjZurw1iBwR91Pi
+LlytWqiGdHVGn9oXRPXZnNXpFgdTw==
-----END PRIVATE KEY-----
┌─[parrot@parrot]─[~/home/cert-opnsense]
└──╼ $cat opnsense.crt
-----BEGIN CERTIFICATE-----
MIIFazCCA1OgAwIBAgIUVN9XqCN/DSM+tbLdhbyRVbdkRyYwDQYJKoZIhvcNAQEL
BQAwRTELMAkGA1UEBhMCRlIxEzARBgNVBAgMClNvbWUtU3RhdGUxITAfBgNVBAoM
GEludGVybmV0IFdpZGdpdHMgUHR5IEx0ZDAeFw0yNjAxMTYxMTQyMzJaFw0yNzAx
MTYxMTQyMzJaMEUxCzAJBgNVBAYTAkZSMRMwEQYDVQQIDApTb211LVN0YXR1MSEw
HwYDVQQKDBhJbnRlcm5ldCBXaWRnaXRzIFB0eSBMdGQwggIiMA0GCSqGSIb3DQEB
AQUAA4ICDwAwggIKAoICAQCnKVdaBiFhT933IXam96DEUJeLbdL3cpTBOFAoj/BC
6aOjTfFBvb1BH5n3JxHzSWM7uyCaICsxJvyNiQSV5JLZYIkkADOGpqBpyzfypFy+
/fI0s+/LMF0y7LM2F/Dj/ixJn65qlyl6Onc+Ya46su3DGO4w2IXyjLKv+ZIS6IzT
nmFdxsibmekxgoAh/GZuJIxUovhku1+BPyrV38fUJoIqZXe/wGlVaMaVtu2egcUH
OM+OL2nTxkvlwVWkHAFAUk9PiZIAynlAxqw4Yk8y4cRsU9nFU9xDB4Fx03+9fl/S
ozObhZOSzJqqWNe02w93pz7tC7k8Ong+WrIzgSg1VviLoiTiD1R++ISjdUL8lb/C
dzXyurs5YynJKpEZqWdO3thgnv/8gYhIdPOs3UdREbUm7HXXlBEqv/yLQuCUFi3G
qq8z1xk9oegX/NOZMkvkCgNzhwkQwJqydSbQhMfYFYdw8zLJru/bjwbj5fI+mvrD
MC5Xwxa7NJsi/hLa6lyP1d5uQBQUDRrhue3rPdjq484JSZe3pFUQuQjkI+R5UfEK
0OAGbJxbxr/OCWcpDAKD9ki+veHG0op9jv07OuDuEnZWix+wjGa5HTl80x7IpTw2
Q9X2luRFsQHbPsXZ3FKyOmVLdXk52nEpo7QEVB1puoF73lCWq666VG8utoTjLlJu
tQIDAQABo1MwUTAdBgNVHQ4EFgQUD9JIvsgSoAcG8b3jFLts5DK2ktEwHwYDVR0j
BBgwFoAUD9JIvsgSoAcG8b3jFLts5DK2ktEwDwYDVR0TAQH/BAUwAwEB/zANBgkq
hkiG9w0BAQsFAAOCAgEAZqvaEJny0EZ4ZF63jlYrsU4oOxHNWqxN0Mf3hUnTtmNo
QKawRVEco9OYXNfv4TGNek8aSY/XetaIDm8goYR/INO/I1pccuqUv2UEI572+ruC
pVV7sXCUyc3cJY/M0AOmeYDygvWgFGSxwZm/AETdXse8FpEv8ocxE442Ct8y8Xg7
c4ssyu+tI5R4Lhmg9nS75VDQg+QWz0Kkk/zByaehR5kYsCl1tbWpq7epnTJOqBEr
wPjbLVJwNyqM4gbJPf3kP6UKso1Obdmk2/x1LSB/cFjkHNHx0SbcA42vk929XewO
bngrK8ulGxC+Ebtb34FqRXd8kVp3mneLGvU9nDJwfdIE1HxFbSvbwIu32w+59QM7
tO2mGFECrMfEq5KLpeiunoUxTkB1qpskyuFT3sUM713u5F+ZgnugMtZwylQJme4U
HlluqVA4y/nKn+jJX4Ta6uuuaf+TVVWx81nz/kAA9DESegqo3jQ9cHGjXvkfYjfC
2awO7k2TYt952Q0A5hgTNvk4Cn3Ae39AB1fQj8/LEz8dqCFlYY18D+t8IbsSA6n0
```

Intégration dans opnsense

Dans l'interface web aller dans System (Système)>gestion des certificats>certificats



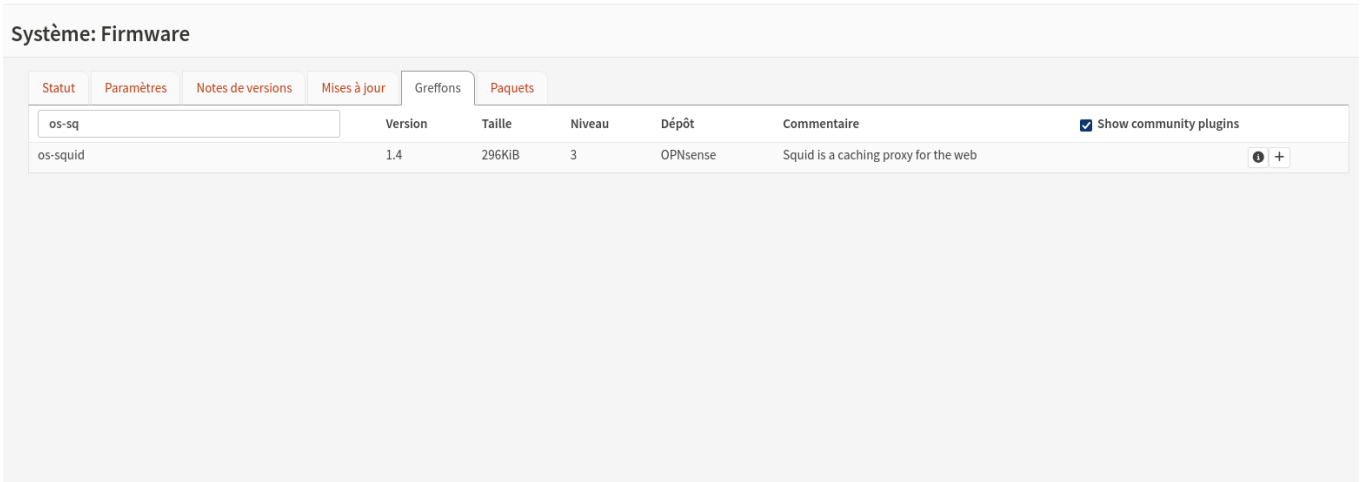
Ilsur la petite croix pour ajouter un certificat> importer un certificat existant copier coller la private key et le certificat au bon endroit



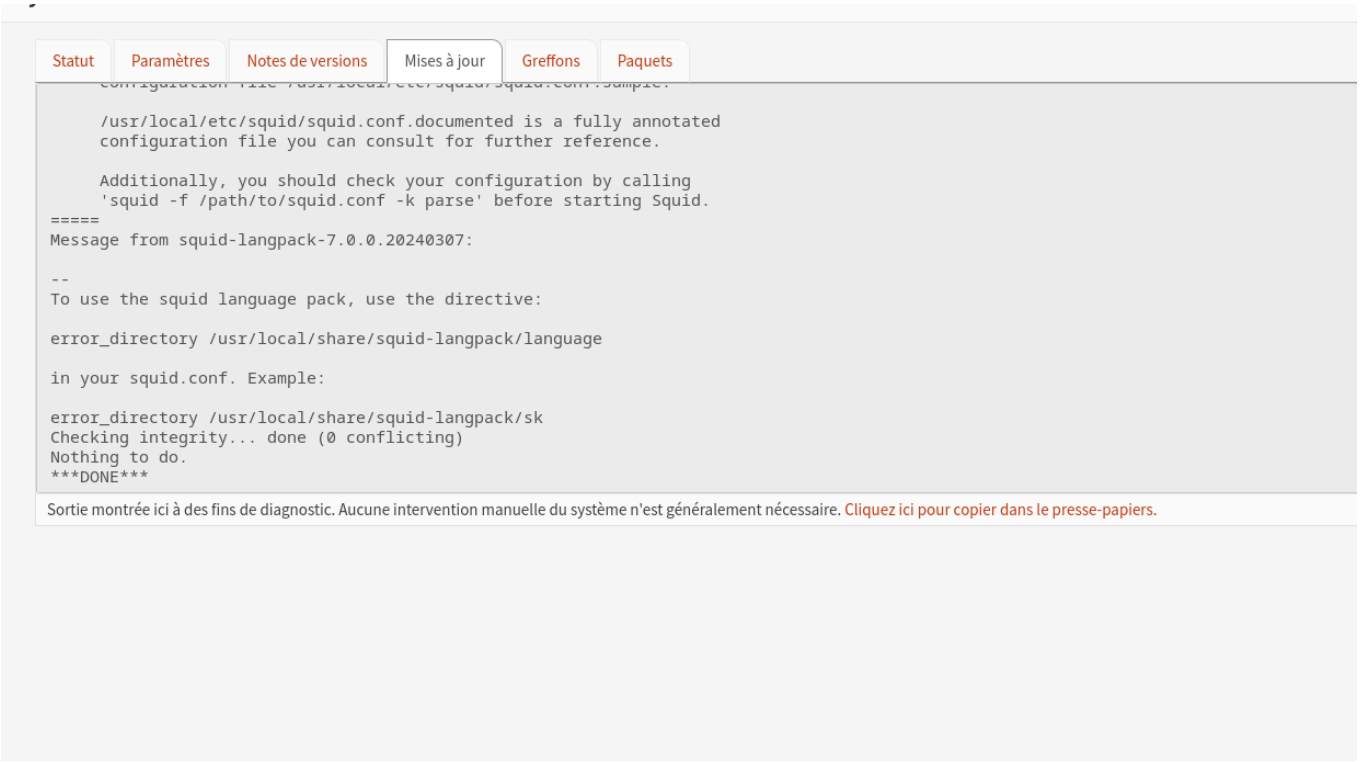
Installation de greffons

os-squid

Aller dans le menu firmware>greffons
coche la case Show community plugins



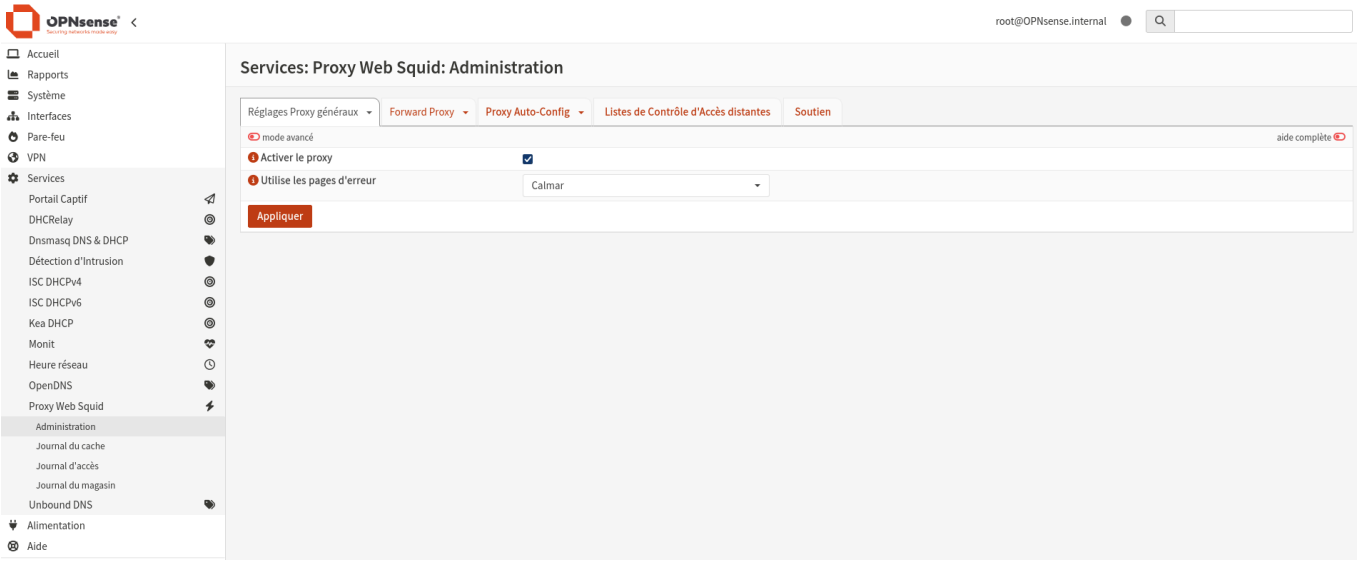
cliquer sur la petit croix installer



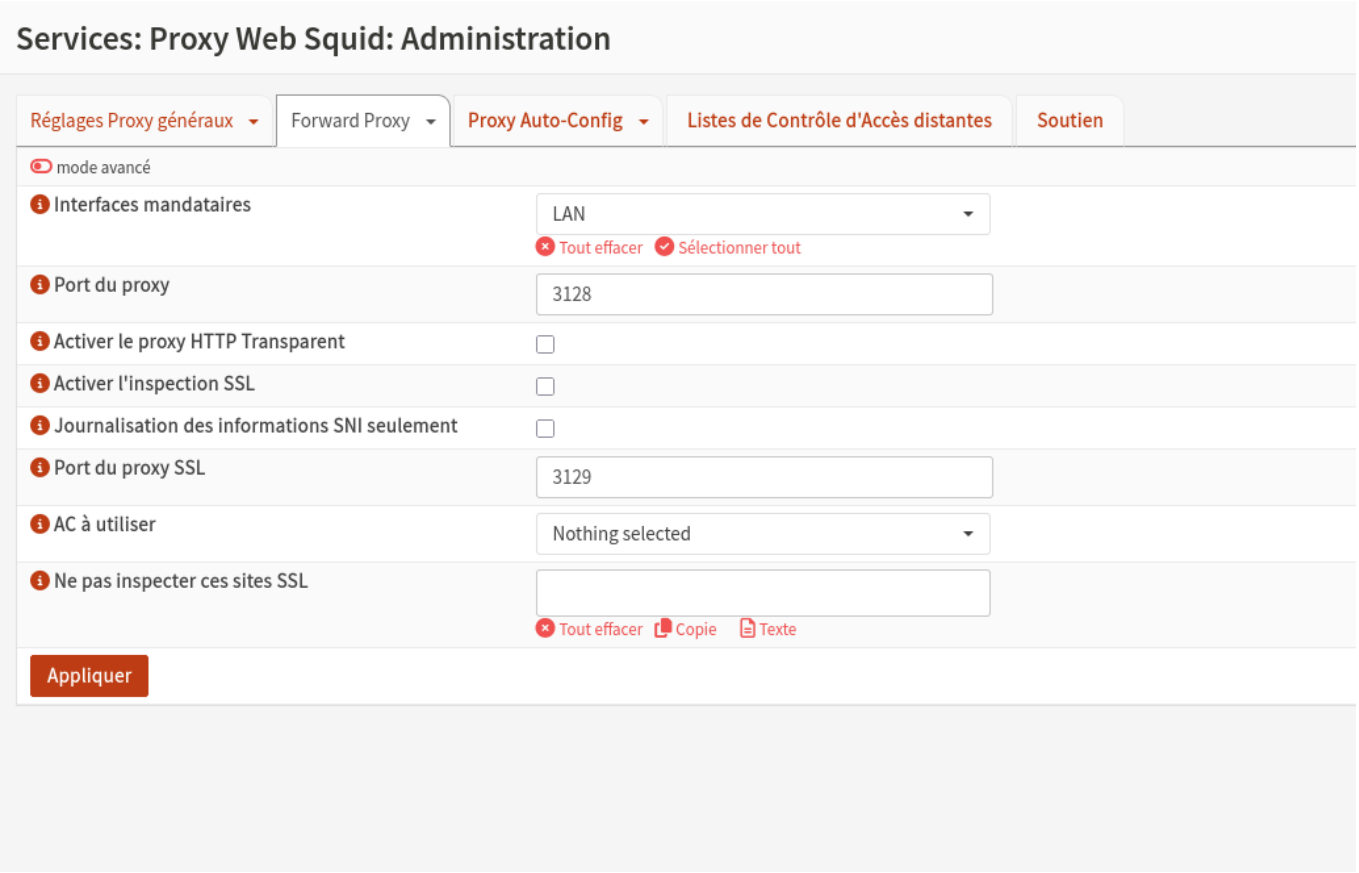
Activer Squid

Aller dans le menu service> ProxyWeb Squid> Administration

cocher la case activer le proxy

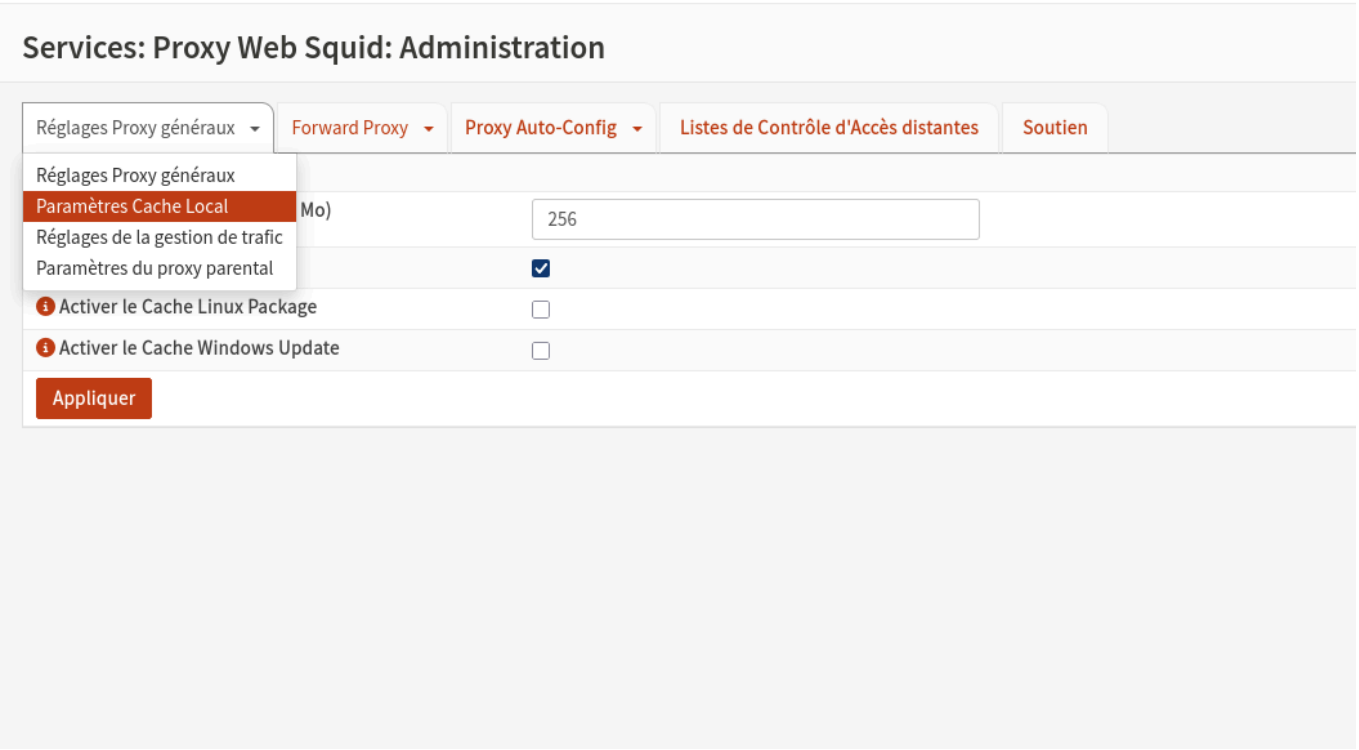


activer le proxy sur le LAN



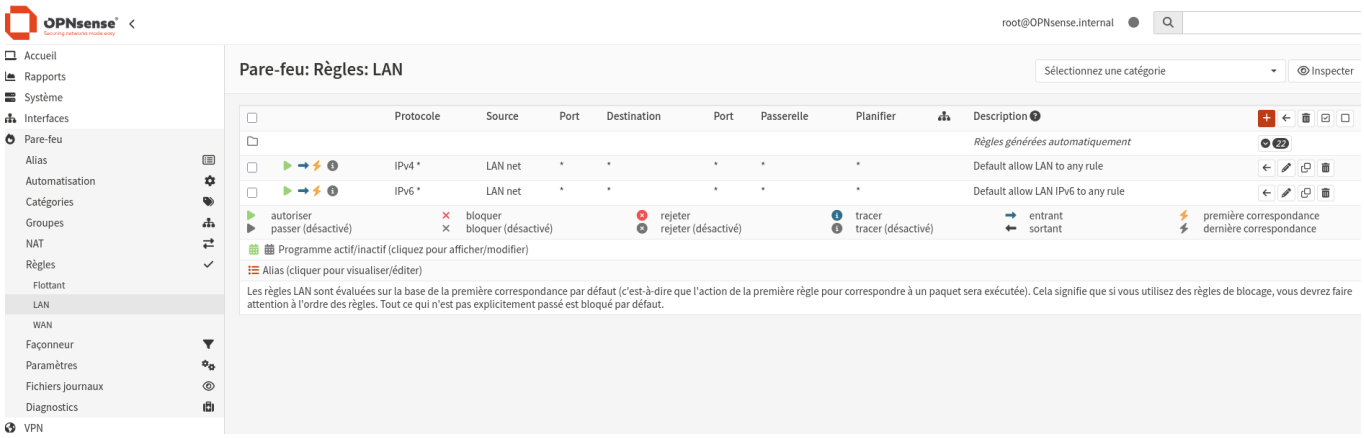
Appliquer

Activer le cache local

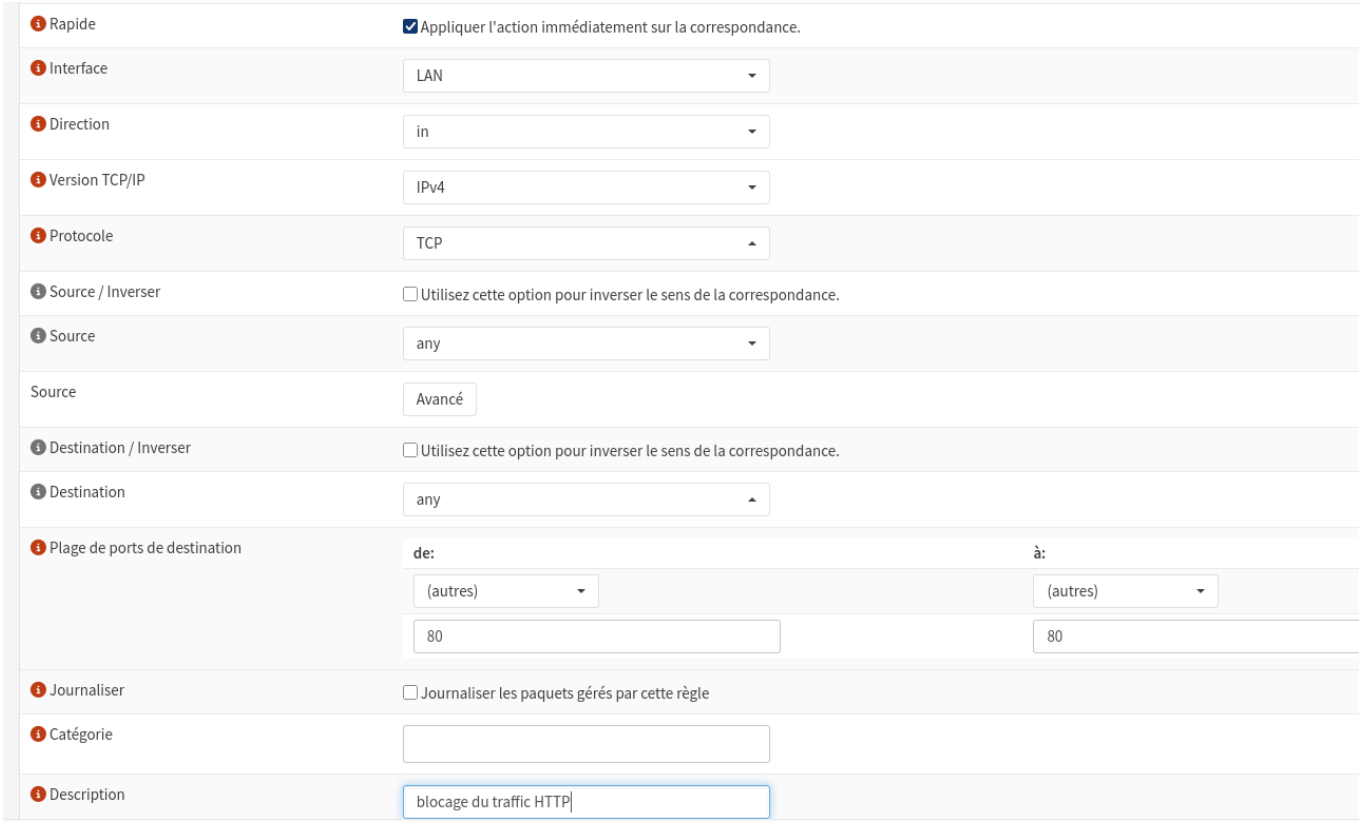


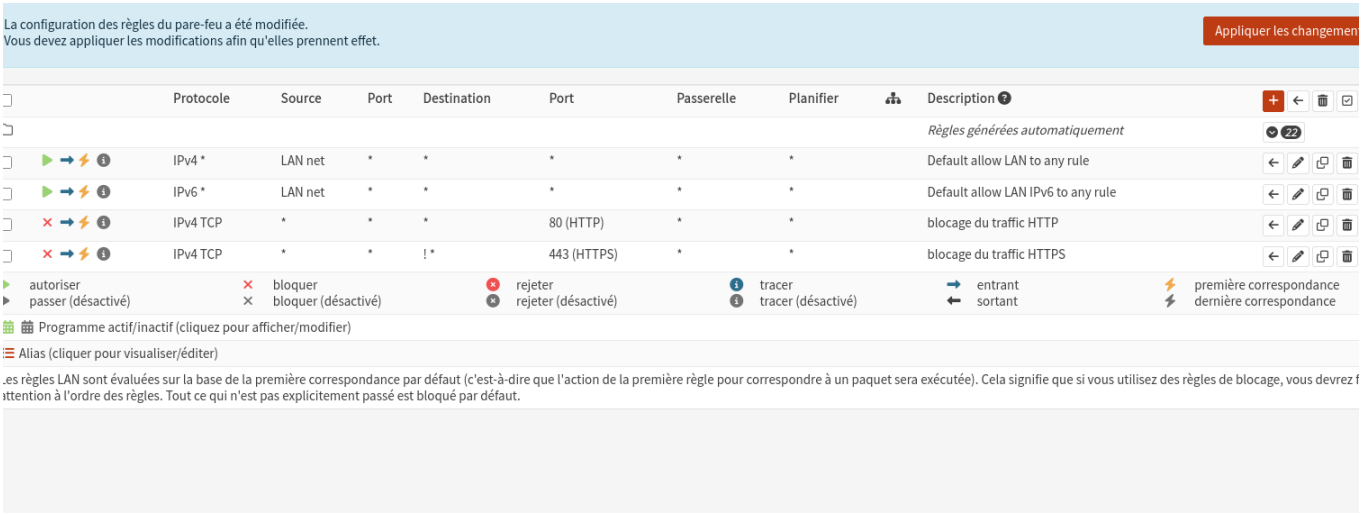
Le cache Linux Package et Windows Update concerne les mise à jour. Cela évite de conservé dans un dossier si on veut retélécharger un programme

Mise en place de règle de blocage



Ajouter une règle

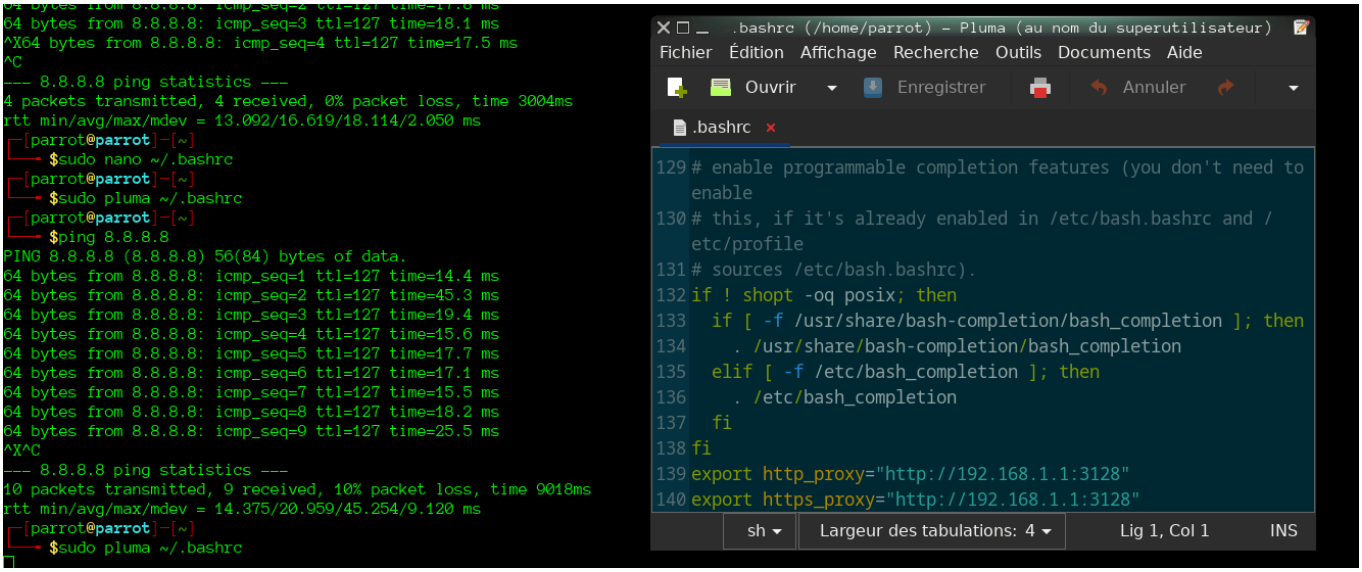




Les monter en haut

Activation du proxy en ligne de commande sur linux

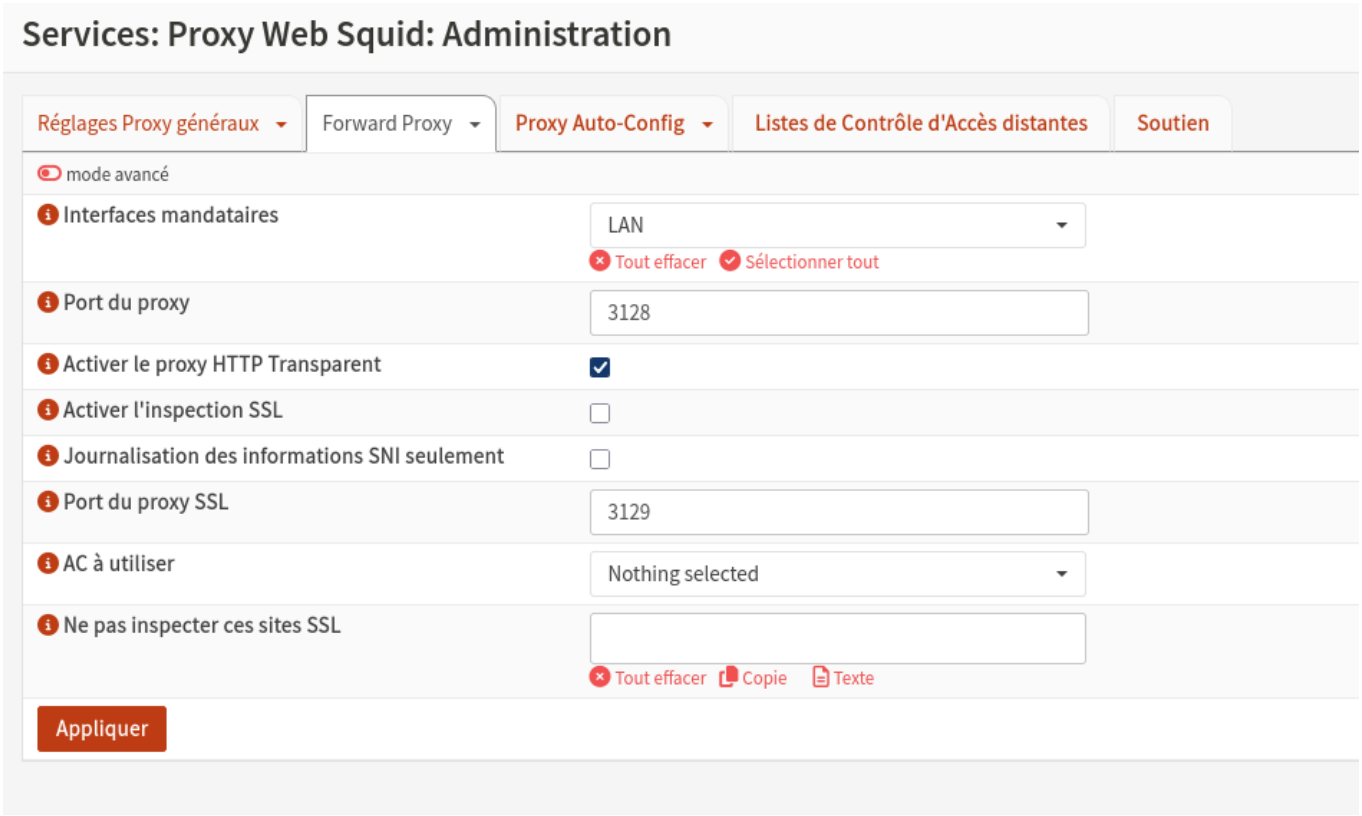
```
#modifier le fichier ~/.bashrc
#sur le protocole TCP 80
export http_proxy="http://192.168.1.1:3128"
#sur le protocole TCP 443
export https_proxy="http://192.168.1.1:3128"
```



L'avantage et l'inconvénian d'un proxy manuelle c'est qu'on peut l'activer et le désactiver quand on veut

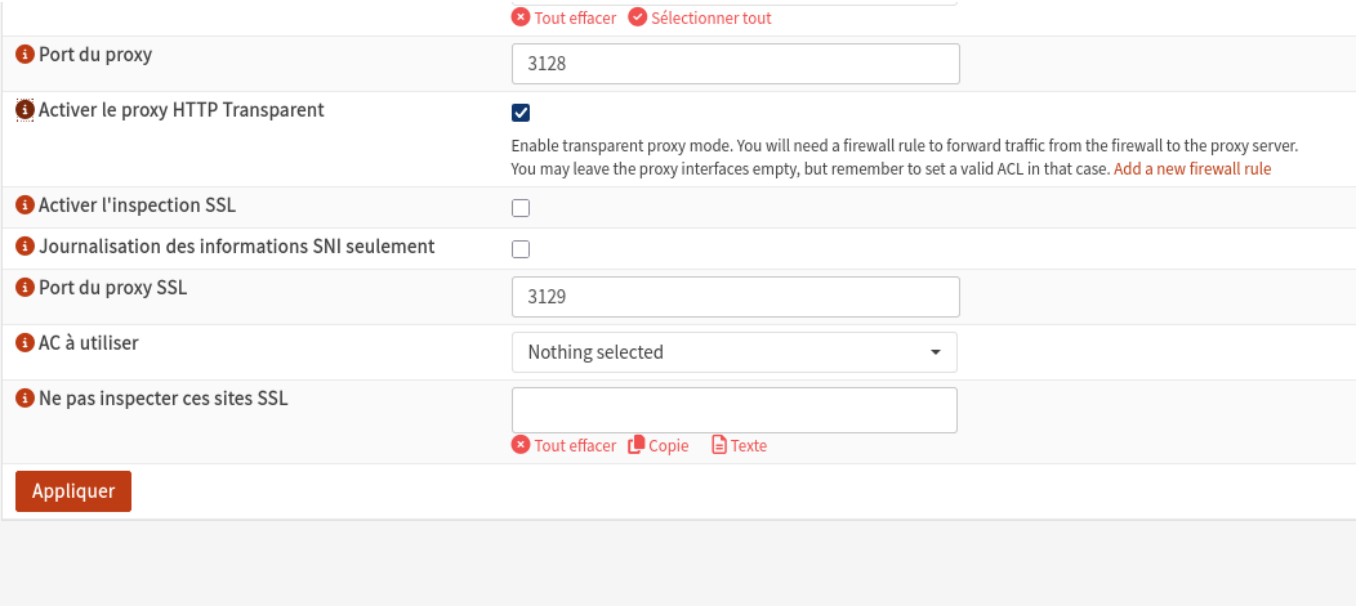
Configuration d'un proxy transparant

Retourner dans le menu Squid Forward Proxy cocher la case Activer le proxy HTTP Transparent

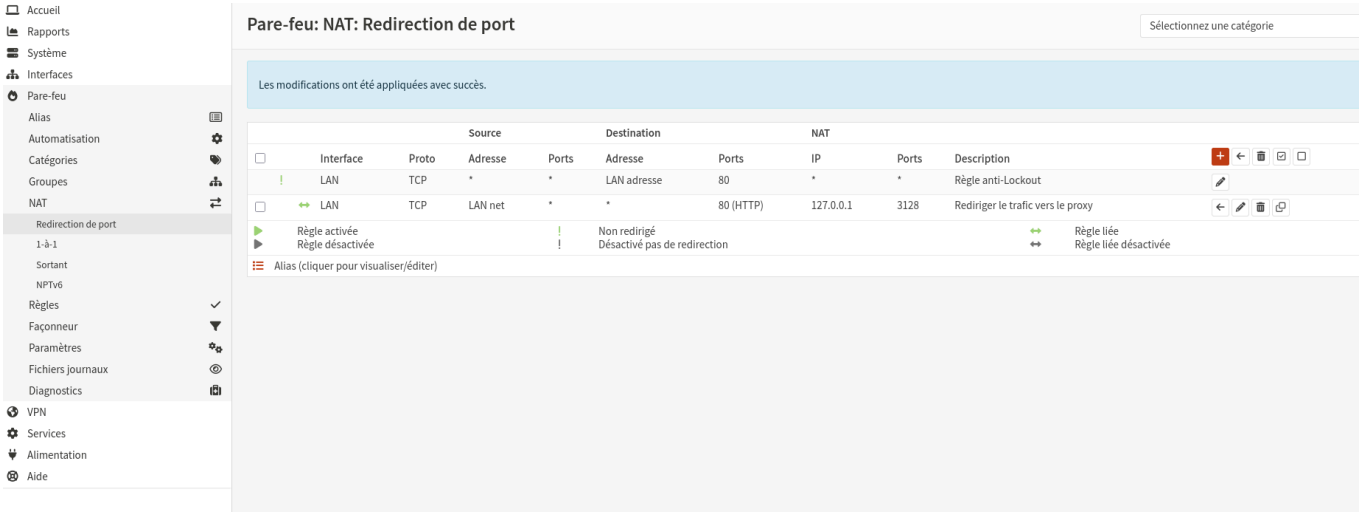


Création de règle de redirection (NAT)

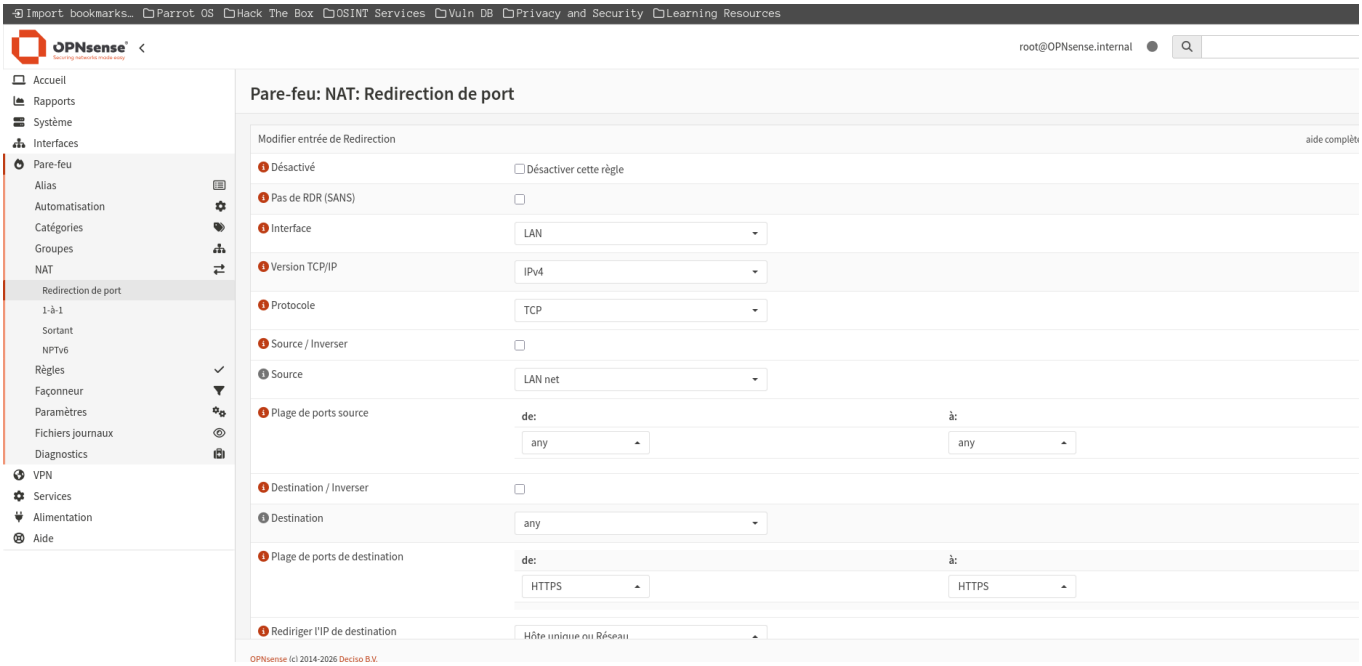
cliquer sur le i de Activer le proxy HTTP Transparent>Add a new firewall rule

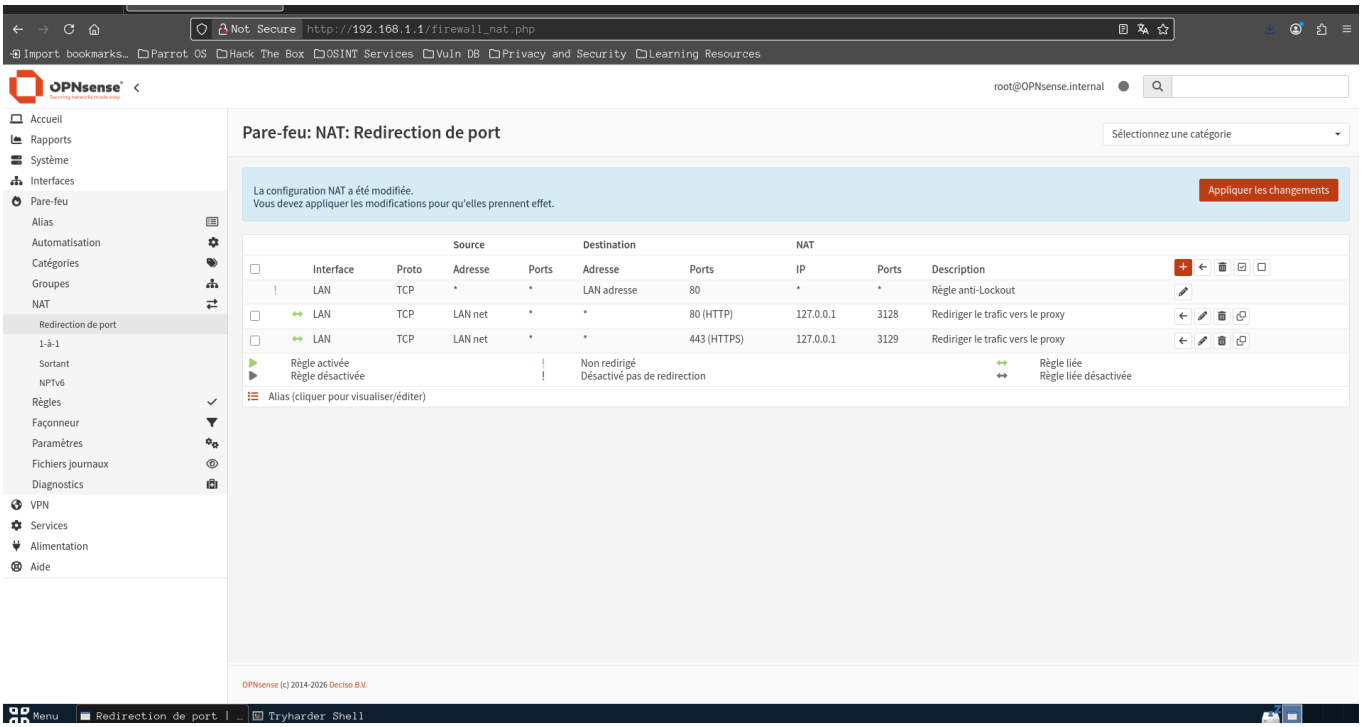


sauvegarder et appliquer ces changement



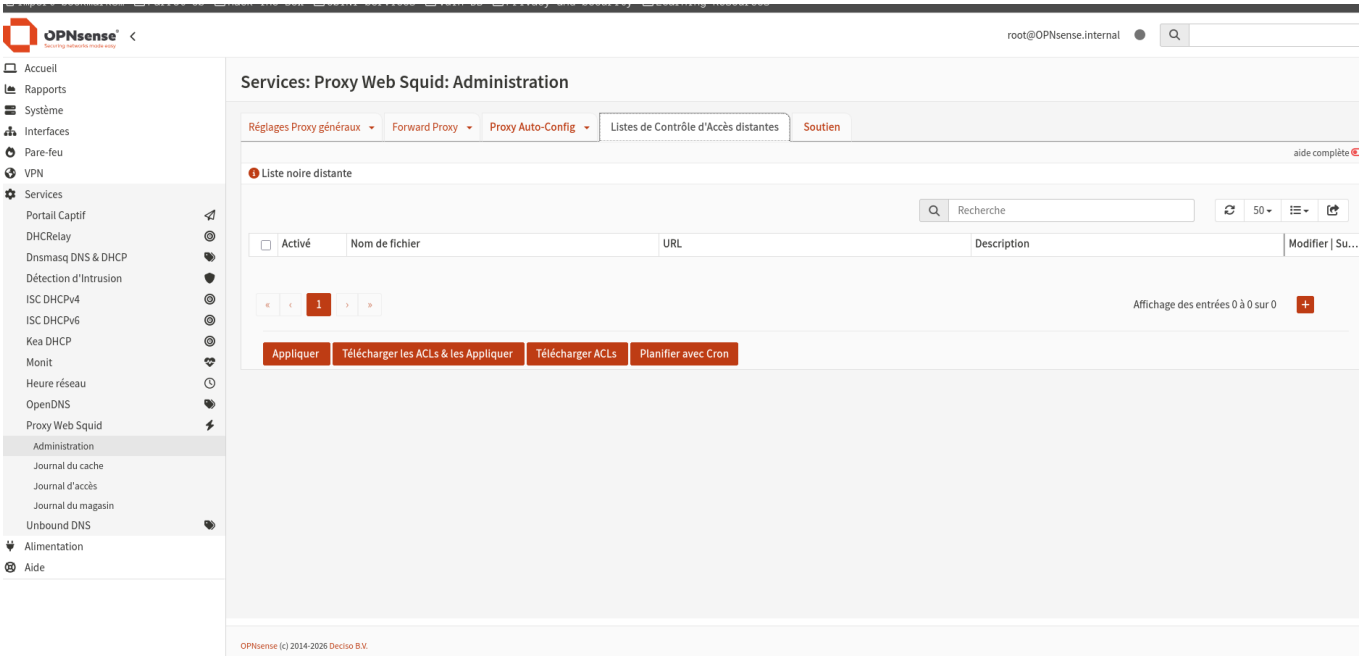
pareil pour Activer l'inspection SSL

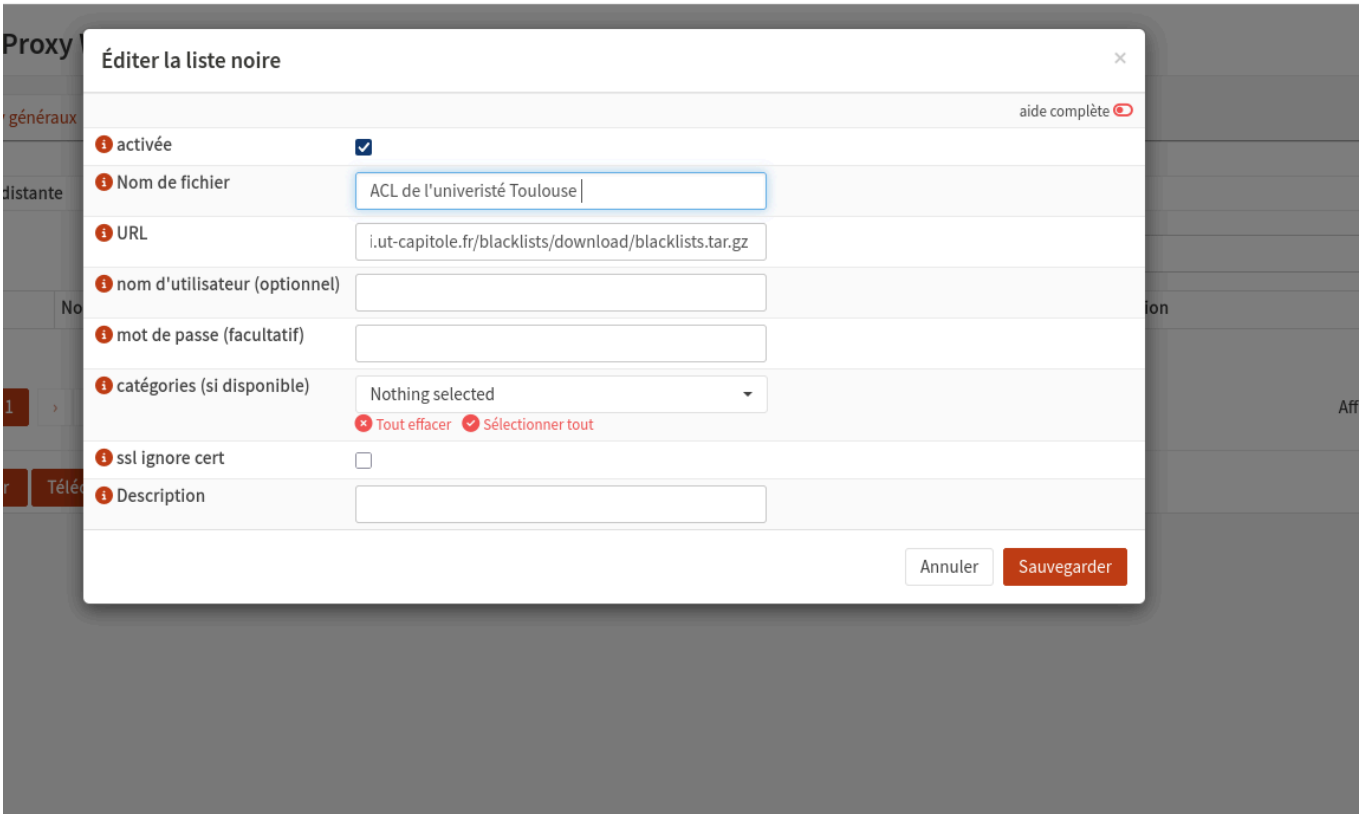




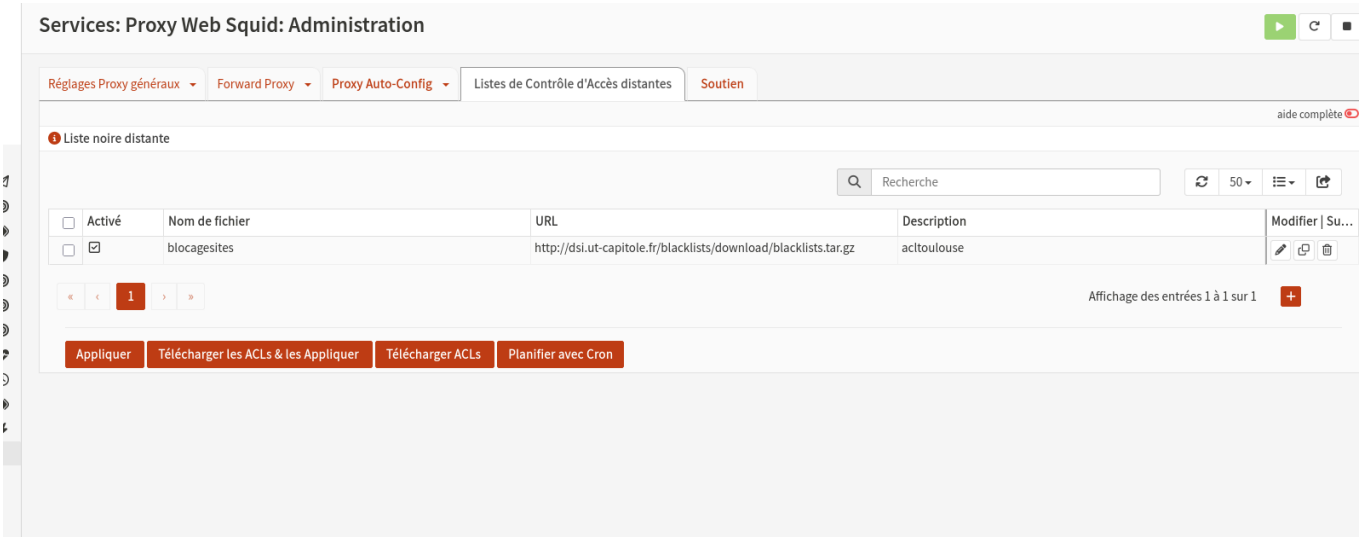
Le proxy transparent est automatique on n'a pas besoin de l'activer et de le désactiver

Ajout de liste de contrôle à distance (ACL)





Le proxy s'est désactivé tout seul je 'arriver plus à rien faire avec l'URL



http://dsi.ut-capitole.fr/blacklists/download/blacklists.tar.gz

Activer le Certificat sur Linux

```
#copie du certificat
sudo cp ~/certs-opnsense/opnsense.crt /usr/local/share/ca-
certificates/epnsense.crt
#mettre à jour la liste des certificats
sudo update-ca-certificates
```

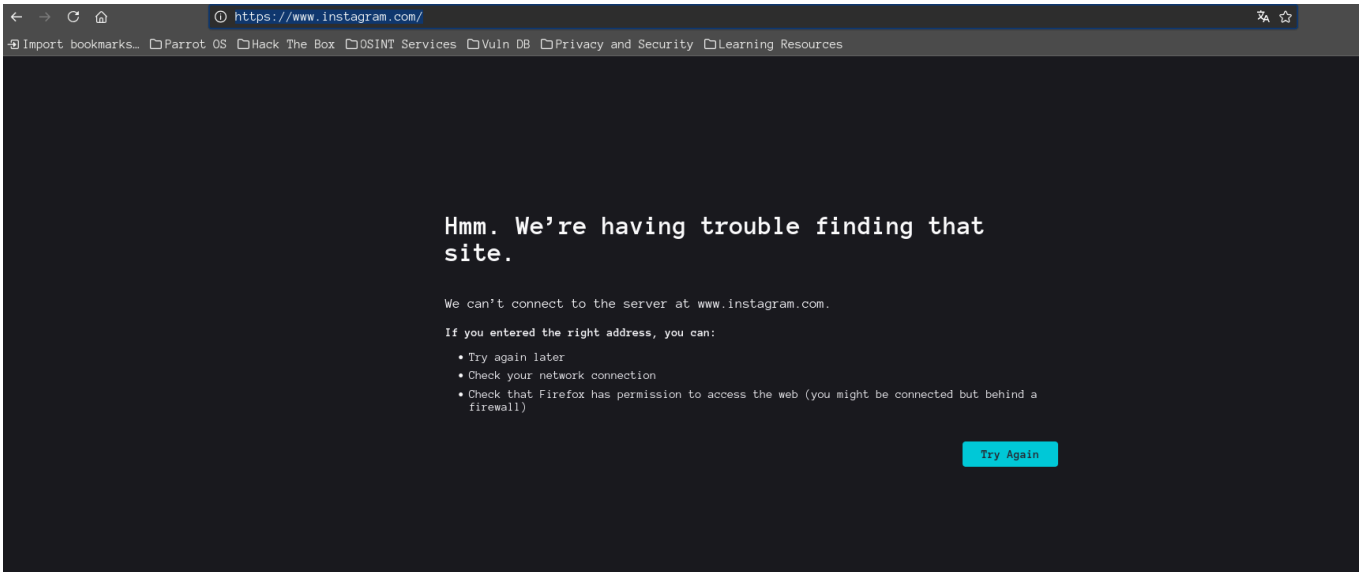
Problème en phase de test

Avec mon proxy transparent j'ai bloqué l'accès au réseaux sociaux mais quand j'essaye d'accéder à instagram et à facebook je peux le faire. Internet est activée et le proxy aussi.

résolution du problème

J'ai commencé par chercher par moi-même. J'ai refait 10 fois tout pour voir si j'ai mal fait une étape quelque part. Puis j'ai cherché sur internet une résolution

Il faut désactiver une règle de pare-feu

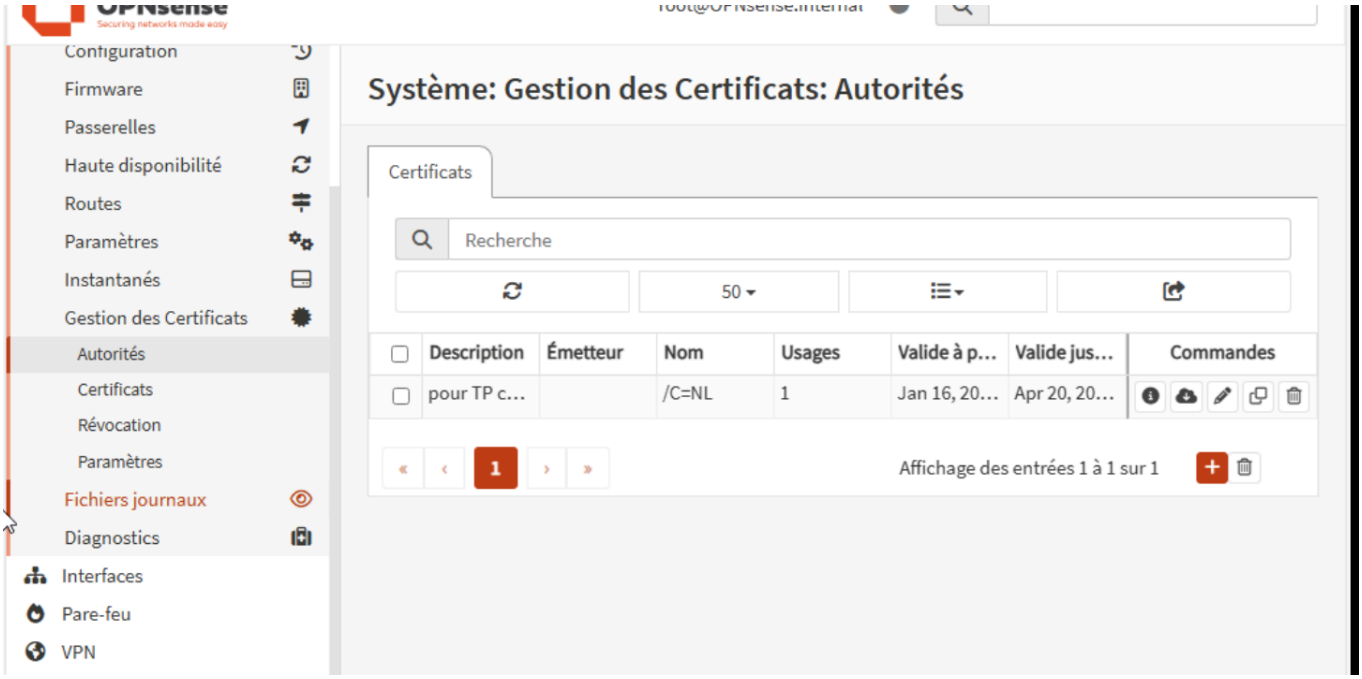


Essai avec windows 11

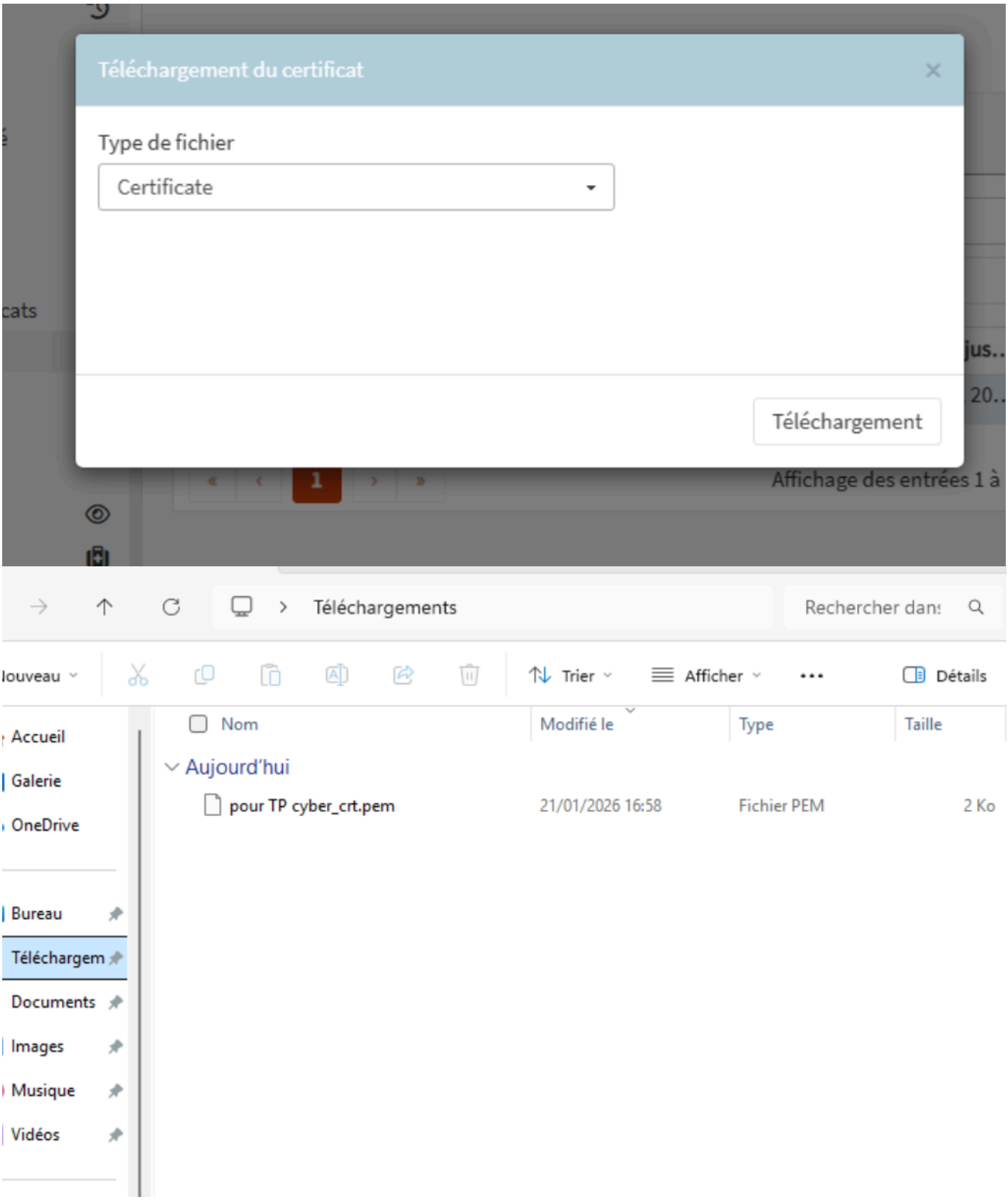
proxy transparent

Installation du certificat

aller dans le menu Système>Gestio des Certificats> Autorités (cliquer sur le plus pour en ajouter un)

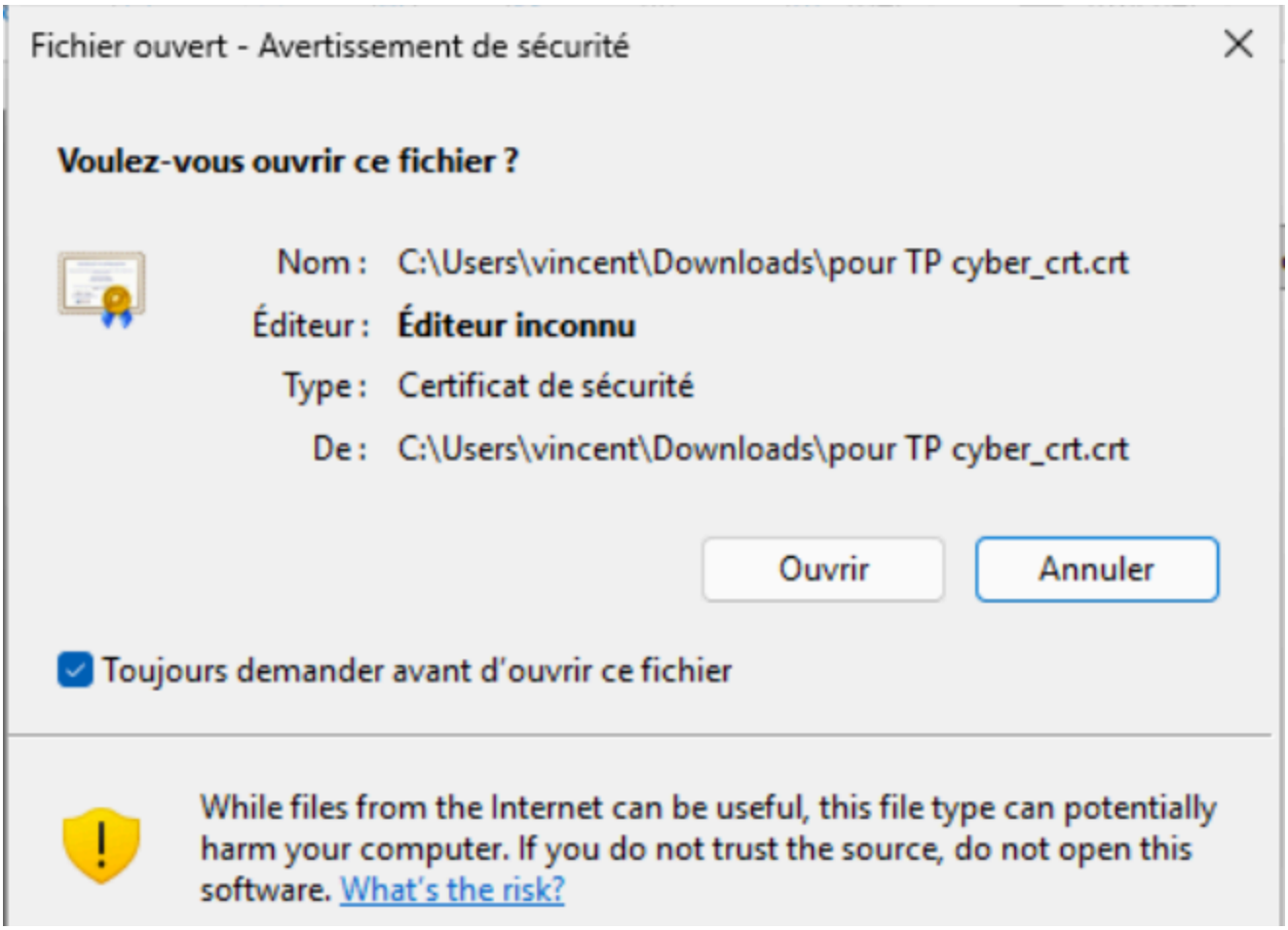


cliquer sur le nuage pour le télécharger

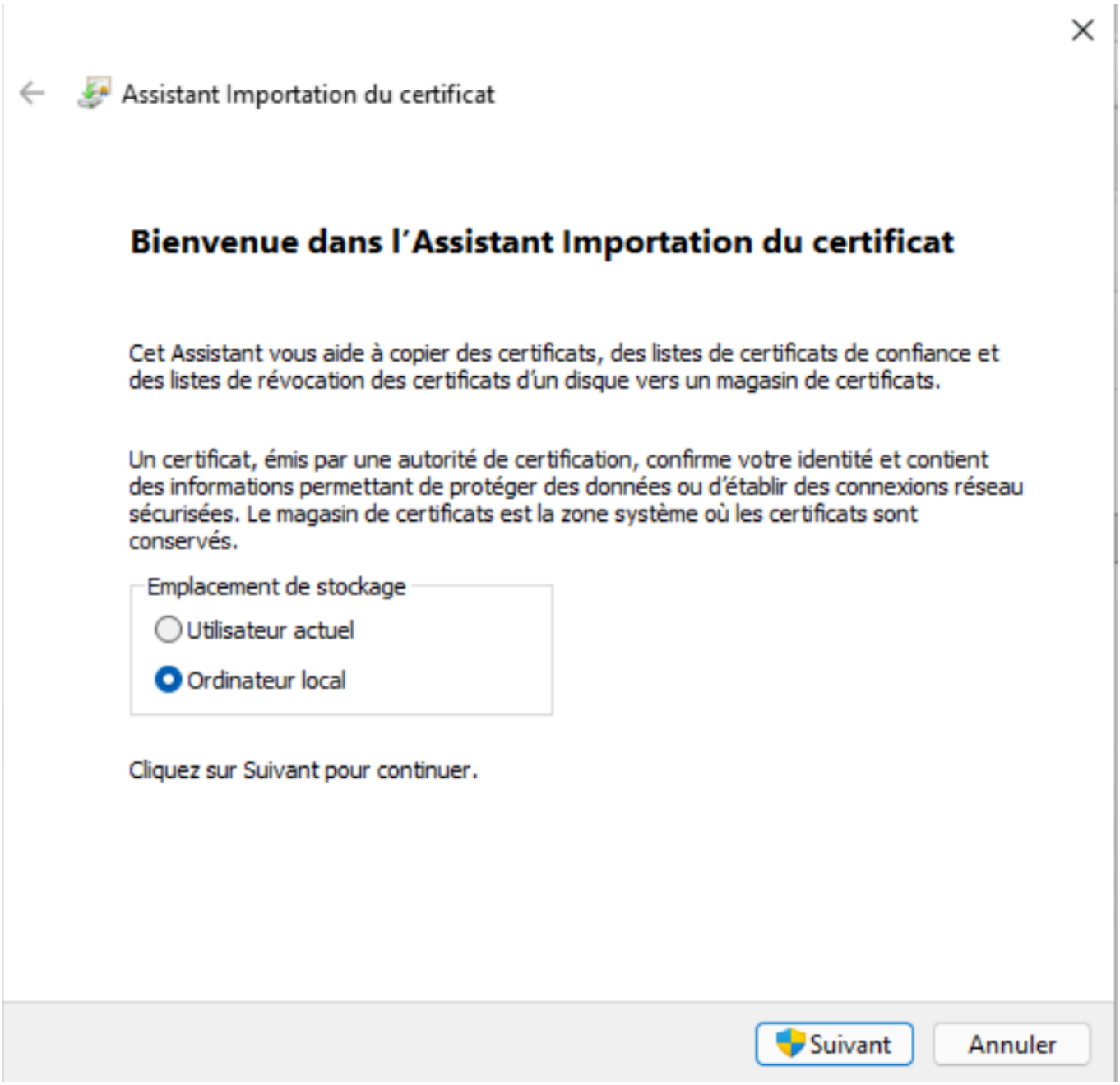

Téléchargement du certificat
Type de fichier
Certificate
Téléchargement
Affichage des entrées 1 à
Téléchargements
Rechercher dans
Trier
Afficher
Détails
Accueil
Galerie
OneDrive
Bureau
Téléchargem
Documents
Images
Musique
Vidéos
Nom
Modifié le
Type
Taille
Aujourd'hui
pour TP cyber_crt.pem
21/01/2026 16:58
Fichier PEM
2 Ko

renomme le en .crt

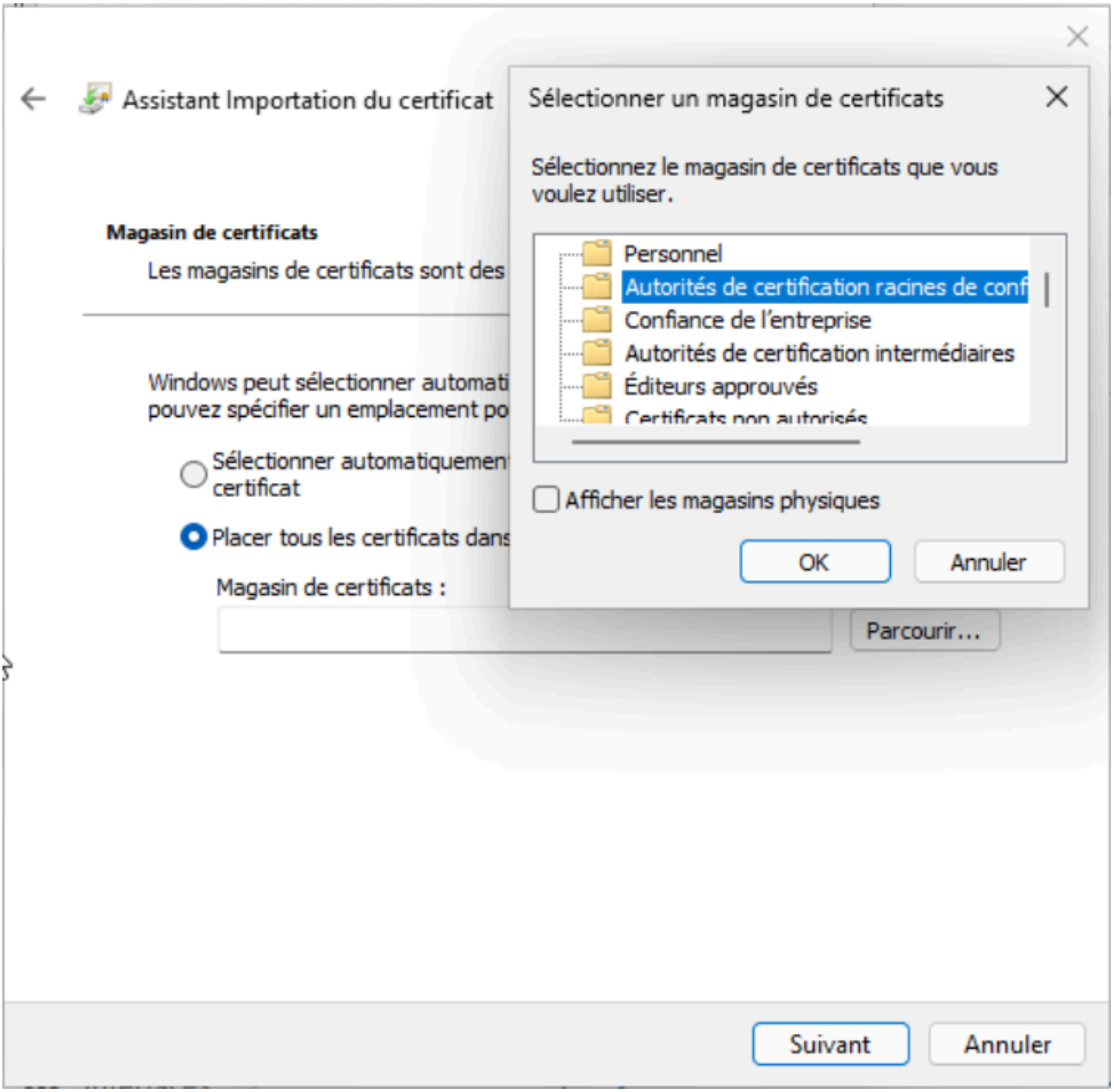
double cliquer dessus



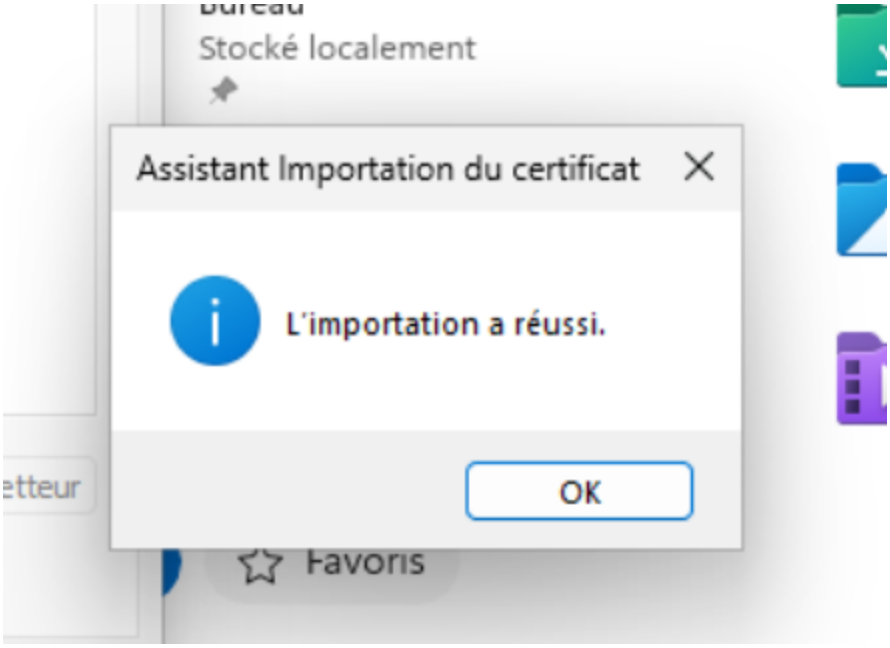
Puis cliquer sur ouvrir et installer ce certificat sélectionner ordinateur local



cliquer sur suivant et oui choisir le bon magasin de certificat



cliquer sur terminé



Test

Le test marche

Réponse au question

Pourquoi est-il préférable d'utiliser OPNsense en mode installé plutôt qu'en live ?

Le mode installé est adapté à la production pour un lab sérieux et un apprentissage réel. Tandis que le mode live est adapté à un test rapide ou pour un dépannage.

Pourquoi avoir besoin de deux interfaces réseau ?

Une interface réseau sera attribué au LAN et l'autre au WAN. Autrement dit l'un sera pour l'accès au configuration via une interface web l'autre sera là pour l'accès réseaux

Quels sont les avantages d’utiliser une configuration DHCP sur l’interface LAN pour les postes clients ?

cela permet des avantages en administration réseau, exploitation quotidienne. Attribue automatiquement des paramètre réseau. Gain de temps. Cela permet une flexibilité des postes.

Pourquoi est-il nécessaire de créer un certificat sur OPNsense pour l'inspection du trafic HTTPS ?

Parce que le trafic HTTPS (trafic HTTP sécurisé) est chiffré de bout en bout. Sans certificats on a accès à des données uniquement chiffré inutilisable. On a besoin de déchiffré les données et les certificats possède cette fonction.

Pourquoi est-il nécessaire d’installer un certificat sur les postes clients pour l’inspection HTTPS ?

Si on installe pas le bon certificat bien concordant c'est un peu comme si on voulait rentrer dans notre maison avec la clé d'une autre serrure. Cela ne pas marcher