

procédure pour mettre en place un proxy OPNsens

- [Téléchargement de OPNsens](#)
- [Mise en place d'OPNsens](#)
- [Création d'un certificat SSL sur Linux parrot Sec](#)
 - [Intégration dans opnsense](#)
- [Installation de greffons](#)
 - [os-squid](#)
 - [Activer Squid](#)
 - [Activer le cache local](#)
 - [Mise en place de règle de blocage](#)
- [Activation du proxy en ligne de commande sur linux](#)
- [Configuration d'un proxy transparant](#)
- [Création de règle de redirection \(NAT\)](#)
- [Ajout de liste de contrôle à distance \(ACL\)](#)
- [Activer le Certificat sur Linux](#)
- [Problème en phase de test](#)
 - [résolution du problème](#)
- [Essai avec windows 11](#)
 - [proxy transparent](#)
 - [Installation du certificat](#)
- [Test](#)
- [Réponse au question](#)
 - [Pourquoi est-il préférable d'utiliser OPNsense en mode installé plutôt qu'en live ?](#)
 - [Pourquoi avoir besoin de deux interfaces réseau ?](#)
 - [Quels sont les avantages d'utiliser une configuration DHCP sur l'interface LAN pour les postes clients ?](#)
 - [Pourquoi est-il nécessaire de créer un certificat sur OPNsense pour l'inspection du trafic HTTPS ?](#)
 - [Pourquoi est-il nécessaire d'installer un certificat sur les postes clients pour l'inspection HTTPS ?](#)

Téléchargement de OPNsens

[Download - OPNsense](#)

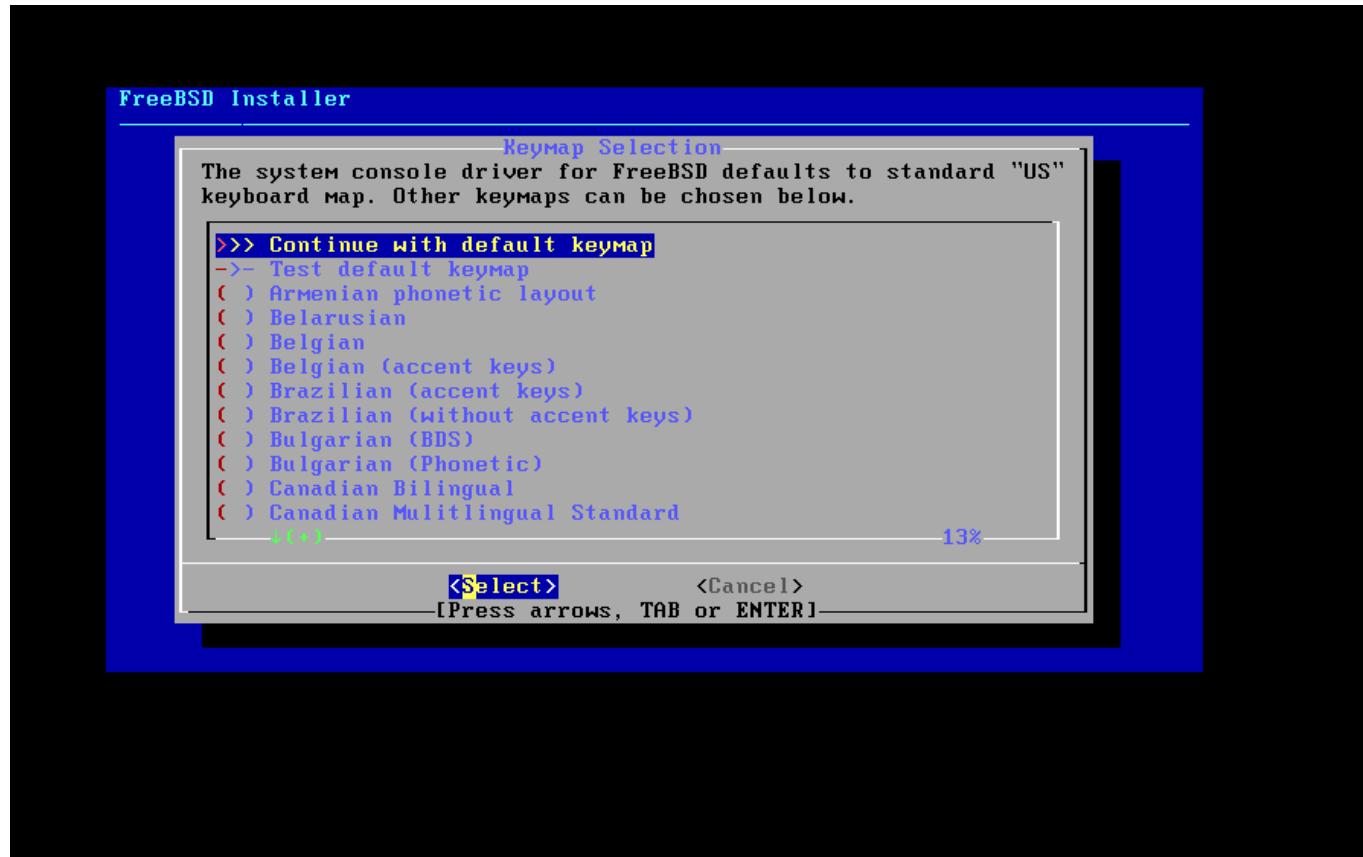
Mise en place d'OPNsens

bien prendre le format DVD

Extraire le dossier téléchargé

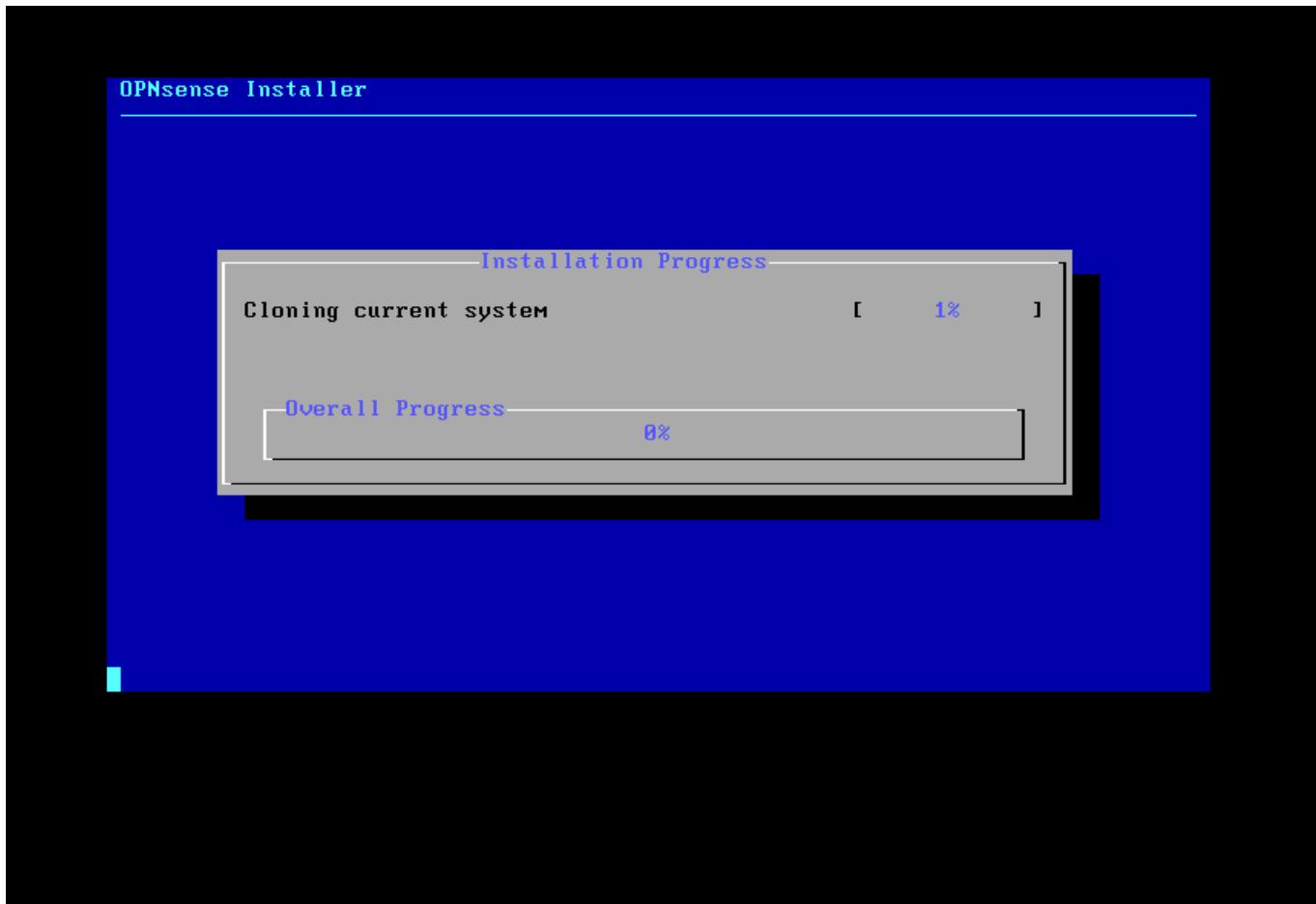
Faire une VM

les login de base OPNsense Installer opnsense



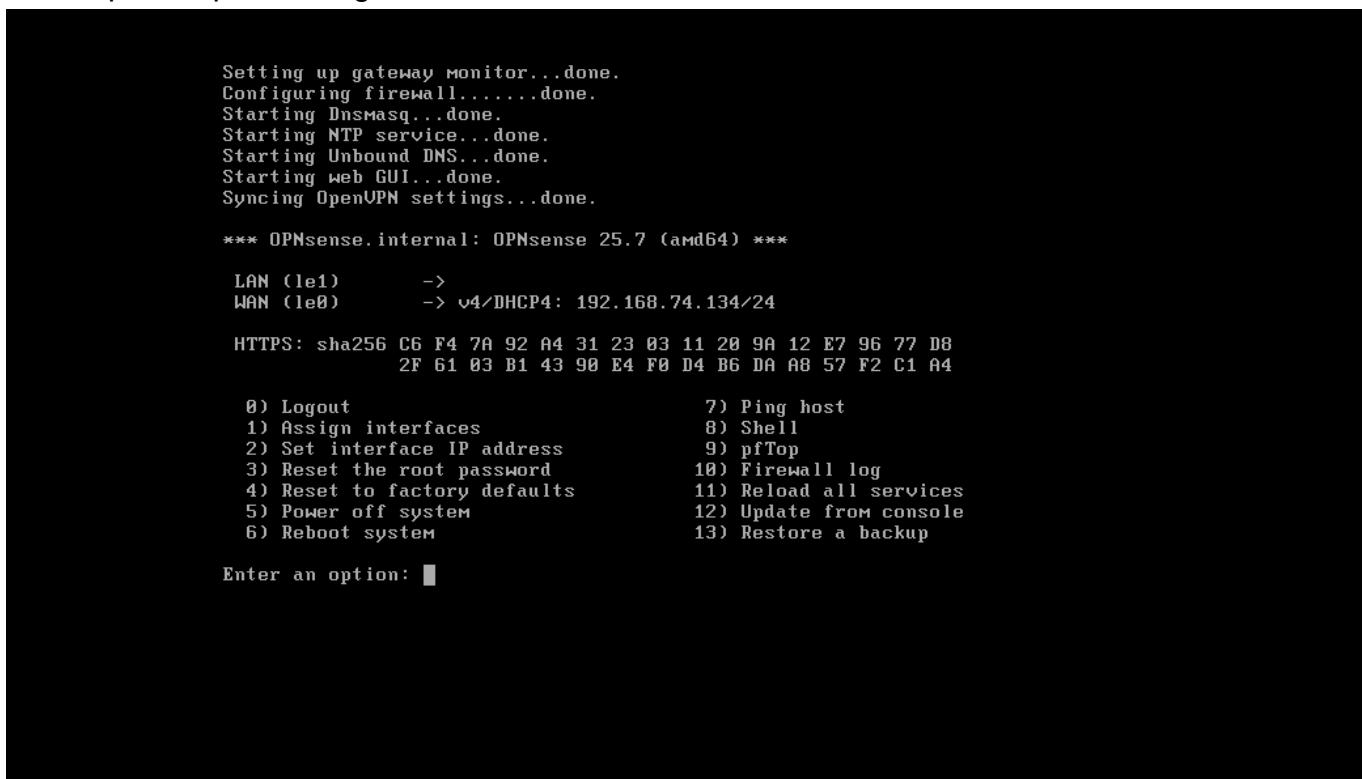
Tout mettre en ok

sélectionner le disque dur virtuel



choisir l'option 1 pour 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) ***

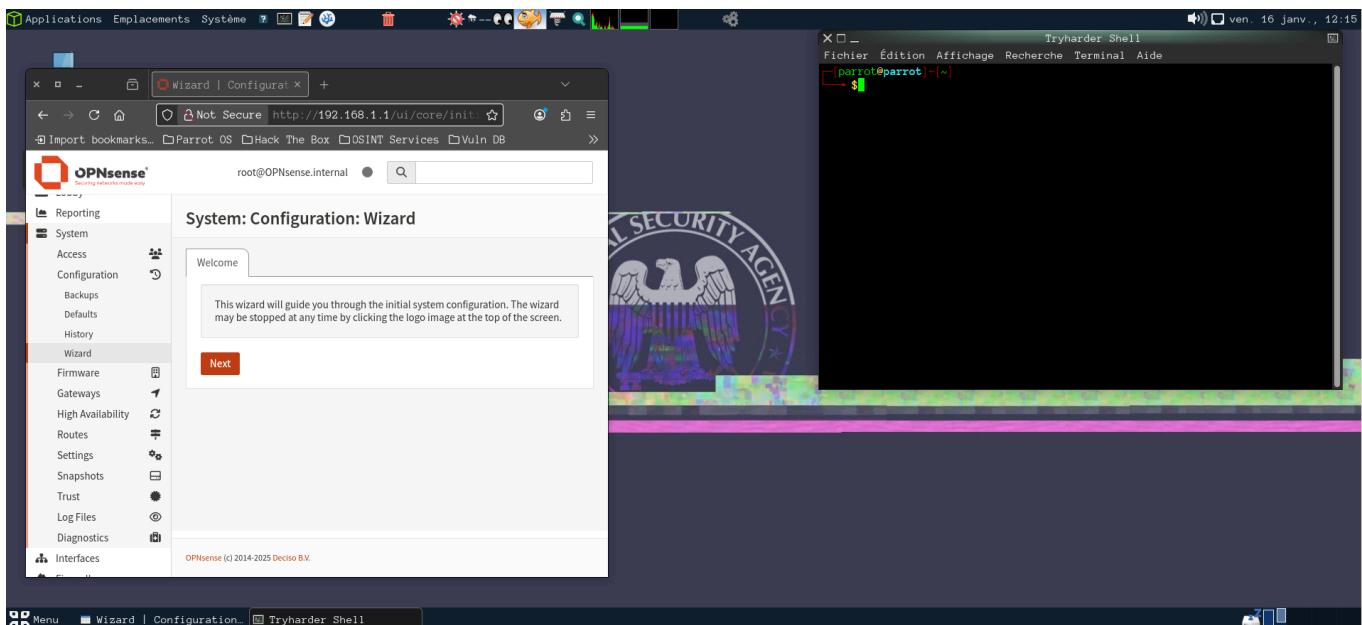
LAN (le1)      -> v4: 192.168.1.1/24
WAN (le0)      -> v4/DHCP4: 192.168.74.134/24

 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

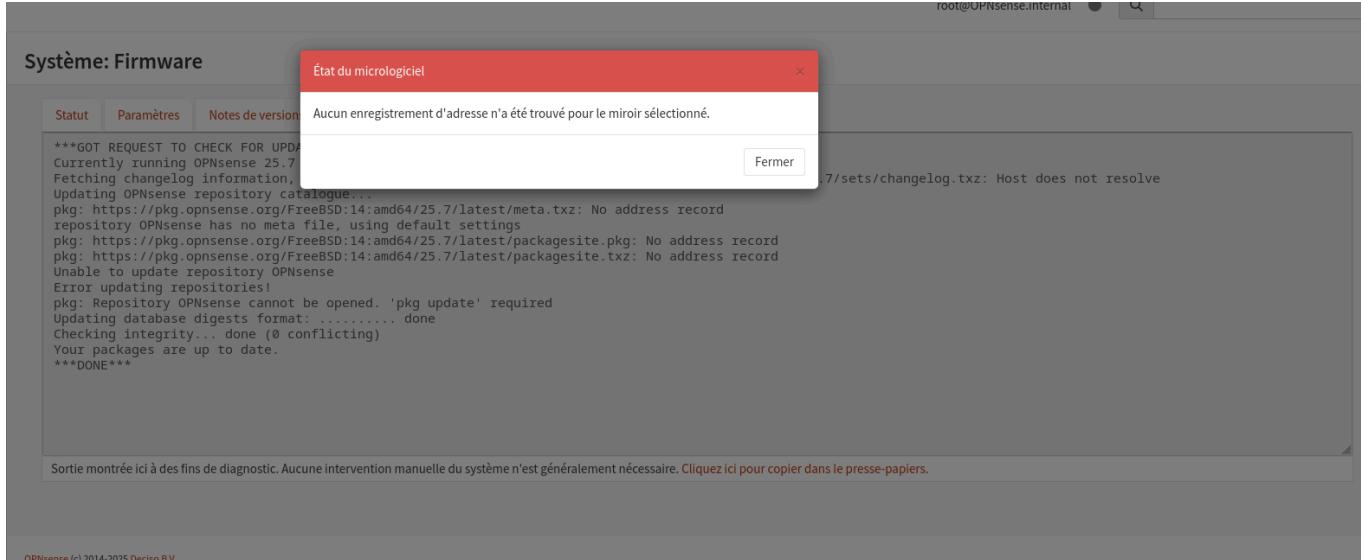
Se connecter à l'IP LAN sur l'autre VM se connecter en root



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

System: Configuration: Wizard

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.
[X] [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-----
MIIJQgIBADANBgkqhkiG9w0BAQEFAASCCSwggkoAgEAAoICAQCnKVdaBiFhT933
IXam96DEUJeLbdL3cpTB0FAoj/BC6a0jTfFBvb1BH5n3JxHzSWM7uyCaICsxJvyN
iQSV5JLZYIkADOGpqBpyzfypFy+/fI0s+/LMF0y7LM2F/Dj/ixJn65qly160nc+
Ya46su3DG04w2IXyjLKv+ZIS6IzThmFdxsibmekxgoAh/GZuJIxUovhku1+BPyrV
38fUJoIqZXe/wG1VaMaVtu2egcUHOM+OL2nTxkv1wVWkHAFAUk9PiZIAynlAxqw4
Yk8y4cRsU9nFU9xDB4Fx03+9f1/Soz0bhZ0SzJqqWNe02w93pz7tC7k80ng+WRIz
gSg1VviLoiTid1R++ISjdUL81b/CdzXyurs5YynJKpEZqWd03thgnv/8gYhIdPOs
3UdREbUm7HXX1BEqv/yLQuCUFi3Gqq8z1xk9oegX/N0ZMkvkCgNzhwkQwJqydSbQ
hMfYFYdw8zLJru/bjwbj5fI+mvrDMC5Xwxax7NJsi/hLa61yP1d5uQBQUDRrhue3r
Pdq484JSZe3pFUQuQjkI+R5UfEK00AGbJxbxr/OCWcpDAKD9ki+veHG0op9jv07
```

```

2H4qxhWU63gpE12sVw+y3fhVHRf5tK9XSLw3XzjjAmCK7ggam9tKOrqEU0zmE9XZ
Pd1afMz5dIQk/fOIT3A8pn7rWRYp73RRiIhFFCP08nZra3dDuBjZurw1iBwR91Pi
+LlytWqiGdHVGN9oXRPXZnNXpFgdTw==
-----END PRIVATE KEY-----
[parrot@parrot] -[~/home/cert-opnsense]
$ cat opnsense.crt
-----BEGIN CERTIFICATE-----
MIIFAzCCA10gAwIBAgIUVN9XqCN/DSM+tbLdhbyRVbdkRyYwDQYJKoZIhvcNAQEL
BQAwRTelMAkGA1UEBhMCR1IxExARBgNVBAgMC1NvbWUtU3RhdGUxITAfBgNVBAoM
GE1udGVybmo0IFdpZGdpdHMgUHR5IE0ZDAeFw0yNjAxMTYxMTQyMzJaFw0yNzAx
MTYxMTQyMzJaMEUxCzAJBgNVBAYTAkZSMRMwEQYDVQQIDA0Tb211LVN0YXR1MSEw
HwYDVQQKDBhJbnR1cm51dCBXaWRnaXRzIFB0eSBMdGQwggIIMA0GCSqGSIb3DQE
BQUAA4ICDwAwggIKAoICAQChVdaBiFhT933IXam96DEUJeLbdL3cpTBOFAoj/BC
6a0jTfFBvb1BH5n3JxHzSWM7uyCaICsxJvyNiQSV5JLZYIkADOGpqBpyzfypFy+
/fI0s+/LMF0y7LM2F/Dj/ixJn65qly160nc+Ya46su3DG04w2IXyjLKv+ZIS6IzT
nmFdxsibmekxgoAh/GZuJIxUovhku1+BPyV38fUJoIqZXe/wG1VaMaVtu2egcUH
OM+OL2nTxkv1wVwkHAFAUk9PiZIAyn1Axqw4Yk8y4cRsU9nFU9xDB4Fx03+9f1/S
oz0bhZ0SzJqqWNe02w93pz7tC7k80ng+WRIzgSg1VviLoiT1D1R++ISjdUL81b/C
dzXyurs5YynJKpEZqWd03thgnv/8gYhIdPOs3UdREbUm7HXX1BEqv/yLQuCUFi3G
qq8z1xk9oeGx/NOZMkvkCgNzhwkQwJqydSbQhMFYFYdw8zLJru/bjwbj5fI+mvrD
MC5Xwxa7NJsi/hLa61yP1d5uQBQUDRrhue3rPdj484JSZe3pFUQuQjkI+R5ufEK
00AGbJxbxr/OCWcpDAKD9ki+veHG0op9jv070uDuEnZWix+wjGa5HT180x7IpTw2
Q9X21uRFsQHbPsXZ3FKyOmVLdXk52nEpo7QEVB1puoF731CWq666VG8utoTjL1Ju
tQIDAQABo1MwUTAdBgNVHQ4EFgQUd9JIVsgSoAcG8b3jFLts5DK2ktEwHwYDVR0j
BBgwFoAUD9JIVsgSoAcG8b3jFLts5DK2ktEwDwYDVR0TAQH/BAUwAwEB/zANBgkq
hkiG9w0BAQsFAAACAgEAZqvaEJny0EZ4ZF63j1YrsU4o0xHNWqxN0Mf3hUnItmNo
QKawRVEco90YXNfv4TGNek8aSY/XetaIDm8goYR/INO/I1pccuqUv2UEI572+ruC
pVV7sXCUyc3cJY/M0A0meYDygvWgFGSxwZm/AETdXse8FpEv8ocxE442Ct8y8Xg7
c4ssyu+tI5R4Lhmg9nS75VDQg+QWzOKkk/zByaeH5kYsC11tbWpq7epnTJ0qBER
wPjbLVJwNyqM4gbJPf3kP6UKso10bdk2/x1LSB/cFjkHNhx0SbcA42vk929Xew0
bngrK8u1Gx+C+Ebtb34FqRXd8kVp3mneLGvU9nDJwdIE1HxFbSvbwIu32w+59QM7
t02mGFECrMfEq5KLpeiunoUxTkB1qpskyuFT3sUM713u5F+ZgnugMtZwy1QJme4U
H11uqVA4y/nKn+jJX4Ta6uuuaaf+TVWx81nz/kAA9DESegqo3jQ9cHGjXvkfYjfC
2aw07k2TYt952Q0A5hgTNvk4Cn3Ae39AB1fQj8/LEz8dqCF1YY18D+t8IbsSA6n0

```

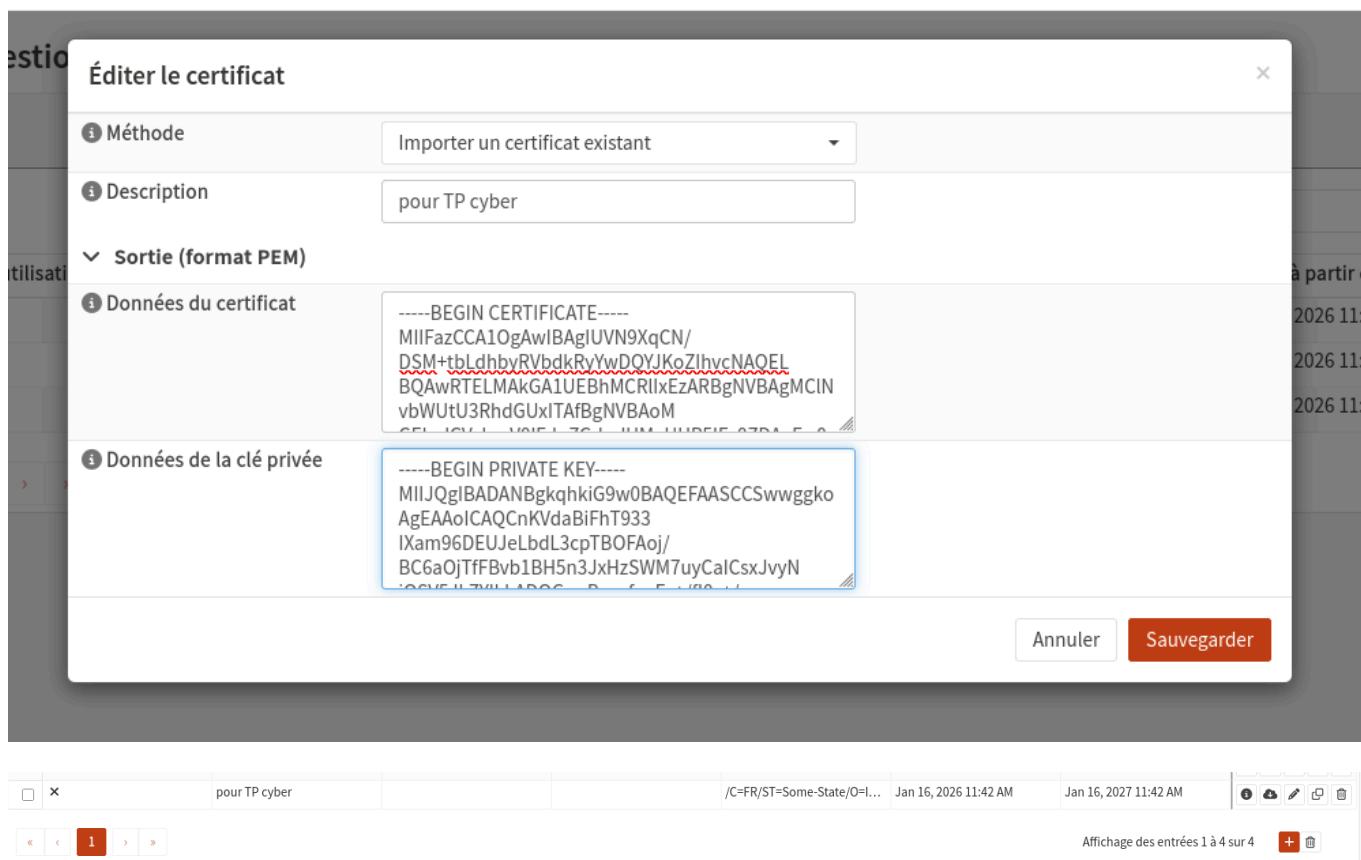
Intégration dans opnsense

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

En cours d'utilisation	Description	Émetteur	Objectif	Nom	Valide à partir de	Valide jusqu'à	Commandes
<input type="checkbox"/>	Web GUI TLS certificate			/CN=OPNsense.internal/C=...	Jan 16, 2026 11:33 AM	Feb 17, 2027 11:33 AM	
<input type="checkbox"/>	Web GUI TLS certificate			/CN=OPNsense.internal/C=...	Jan 16, 2026 11:51 AM	Feb 17, 2027 11:51 AM	
<input checked="" type="checkbox"/>	Web GUI TLS certificate			/CN=OPNsense.internal/C=...	Jan 16, 2026 11:56 AM	Feb 17, 2027 11:56 AM	

Affichage des entrées 1 à 3 sur 3

Il suffit de cliquer sur 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

Système: Firmware					
Statut	Paramètres	Notes de versions	Mises à jour	Greffons	Paquets
os-sq		Version	Taille	Niveau	Dépôt
os-sq		1.4	296KiB	3	OPNsense
Squid is a caching proxy for the web					<input checked="" type="checkbox"/> Show community plugins (i) +

cliquer sur la petit croix installer

```
/usr/local/etc/squid/squid.conf documented is a fully annotated configuration file you can consult for further reference.

Additionally, you should check your configuration by calling
'squid -f /path/to/squid.conf -k parse' before starting Squid.
=====
Message from squid-langpack-7.0.0.20240307:

-- 
To use the squid language pack, use the directive:

error_directory /usr/local/share/squid-langpack/language

in your squid.conf. Example:

error_directory /usr/local/share/squid-langpack/sk
Checking integrity... done (0 conflicting)
Nothing to do.
***DONE***
```

Sortie montrée ici à des fins de diagnostic. Aucune intervention manuelle du système n'est généralement nécessaire. [Cliquez ici pour copier dans le presse-papiers.](#)

Activer Squid

Aller dans le menu service> ProxyWeb Squid> Administration
cocher la case activer le proxy

Services: Proxy Web Squid: Administration

Réglages Proxy généraux Forward Proxy Proxy Auto-Config Listes de Contrôle d'Accès distantes Soutien aide complète

mode avancé

Activer le proxy

Utilise les pages d'erreur Calmar

Appliquer

activer le proxy sur le LAN

Services: Proxy Web Squid: Administration

Réglages Proxy généraux ▾ Forward Proxy ▾ **Proxy Auto-Config** ▾ Listes de Contrôle d'Accès distantes Soutien

mode avancé

Interfaces mandataires LAN
✖ Tout effacer ✓ Sélectionner tout

Port du proxy 3128

Activer le proxy HTTP Transparent

Activer l'inspection SSL

Journalisation des informations SNI seulement

Port du proxy SSL 3129

AC à utiliser Nothing selected

Ne pas inspecter ces sites SSL
✖ Tout effacer ⌂ Copie ⌂ Texte

Appliquer

Appliquer

Activer le cache local

Réglages Proxy généraux ▾ Forward Proxy ▾ **Proxy Auto-Config** ▾ Listes de Contrôle d'Accès distantes Soutien

Réglages Proxy généraux

Paramètres Cache Local Mo) 256

Réglages de la gestion de trafic

Paramètres du proxy parental

Activer le Cache Linux Package

Activer le Cache Windows Update

Appliquer

Réglages Proxy généraux ▾ Forward Proxy ▾ Proxy Auto-Config ▾ Listes de Contrôle d'Accès distantes Soutien

mode avancé

Taille du cache mémoire (en Mo)

Activer le cache local

Activer le Cache Linux Package

Activer le Cache Windows Update

Appliquer

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

Mise en place de règle de blocage

OPNsense® root@OPNsense.internal

Accueil Rapports Système Interfaces Pare-feu Alias Automatisation Catégories Groupes NAT Règles Flottant LAN WAN Façonneur Paramètres Fichiers journaux Diagnostics VPN

Pare-feu: Règles: LAN

Sélectionnez une catégorie Inspecter

	Protocole	Source	Port	Destination	Port	Passerelle	Planifier	Description	Actions
Règles générées automatiquement									+ 22
<input type="checkbox"/>	IPv4 *	LAN net	*	*	*	*	*	Default allow LAN to any rule	edit remove inspect refresh
<input type="checkbox"/>	IPv6 *	LAN net	*	*	*	*	*	Default allow LAN IPv6 to any rule	edit remove inspect refresh
	autoriser		x	bloquer					
	passer (désactivé)		x	bloquer (désactivé)					
								rejeter	
								rejeter (désactivé)	
								tracer	
								tracer (désactivé)	
								entrant	
								sortant	
								première correspondance	
								dernière correspondance	
Alias (cliquer pour visualiser/éditer)									
Les règles LAN sont évaluées sur la base de la première correspondance par défaut (c'est-à-dire que l'action de la première règle pour correspondre à un paquet sera exécutée). Cela signifie que si vous utilisez des règles de blocage, vous devrez faire attention à l'ordre des règles. Tout ce qui n'est pas explicitement passé est bloqué par défaut.									

Ajouter une règle

Rapide	<input checked="" type="checkbox"/> Appliquer l'action immédiatement sur la correspondance.	
Interface	LAN	
Direction	in	
Version TCP/IP	IPv4	
Protocole	TCP	
Source / Inverser	<input type="checkbox"/> Utilisez cette option pour inverser le sens de la correspondance.	
Source	any	
Source	Avancé	
Destination / Inverser	<input type="checkbox"/> Utilisez cette option pour inverser le sens de la correspondance.	
Destination	any	
Plage de ports de destination	de: (autres) 80	à: (autres) 80
Journaliser	<input type="checkbox"/> Journaliser les paquets gérés par cette règle	
Catégorie		
Description	blocage du traffic HTTP	

La configuration des règles du pare-feu a été modifiée.
Vous devez appliquer les modifications afin qu'elles prennent effet.

Appliquer les changements

	Protocole	Source	Port	Destination	Port	Passerelle	Planifier	Actions	Description
Règles générées automatiquement (22)									
✓	IPv4 *	LAN net	*	*	*	*	*		Default allow LAN to any rule
✓	IPv6 *	LAN net	*	*	*	*	*		Default allow LAN IPv6 to any rule
✓	IPv4 TCP	*	*	*	80 (HTTP)	*	*		blocage du traffic HTTP
✓	IPv4 TCP	*	*	!*	443 (HTTPS)	*	*		blocage du traffic HTTPS
► autoriser ► passer (désactivé)	✗ bloquer ✗ bloquer (désactivé)			✗ rejeter ✗ rejeter (désactivé)		✗ tracer ✗ tracer (désactivé)		entrant sortant	première correspondance dernière correspondance
Programme actif/inactif (cliquer pour afficher/modifier)									
Alias (cliquer pour visualiser/éditer)									

Les règles LAN sont évaluées sur la base de la première correspondance par défaut (c'est-à-dire que l'action de la première règle pour correspondre à un paquet sera exécutée). Cela signifie que si vous utilisez des règles de blocage, vous devrez faire attention à l'ordre des règles. Tout ce qui n'est pas explicitement passé est bloqué par défaut.

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"
```

```

64 bytes from 8.8.8.8: icmp_seq=2 ttl=127 time=17.0 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=127 time=18.1 ms
^X64 bytes from 8.8.8.8: icmp_seq=4 ttl=127 time=17.5 ms
^C
--- 8.8.8 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3004ms
rtt min/avg/max/mdev = 13.092/16.619/18.114/2.050 ms
[parrot@parrot] -[~]
└─ $ sudo nano ~/.bashrc
[parrot@parrot] -[~]
└─ $ sudo pluma ~/.bashrc
[parrot@parrot] -[~]
└─ $ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=127 time=14.4 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=127 time=45.3 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=127 time=19.4 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=127 time=15.6 ms
64 bytes from 8.8.8.8: icmp_seq=5 ttl=127 time=17.7 ms
64 bytes from 8.8.8.8: icmp_seq=6 ttl=127 time=17.1 ms
64 bytes from 8.8.8.8: icmp_seq=7 ttl=127 time=15.5 ms
64 bytes from 8.8.8.8: icmp_seq=8 ttl=127 time=18.2 ms
64 bytes from 8.8.8.8: icmp_seq=9 ttl=127 time=25.5 ms
^X^C
--- 8.8.8 ping statistics ---
10 packets transmitted, 9 received, 10% packet loss, time 9018ms
rtt min/avg/max/mdev = 14.375/20.059/45.254/9.120 ms
[parrot@parrot] -[~]
└─ $ sudo pluma ~/.bashrc

```

```

129 # enable programmable completion features (you don't need to
enable
130 # this, if it's already enabled in /etc/bash.bashrc and /
etc/profile
131 # sources /etc/bash.bashrc).
132 if ! shopt -oq posix; then
133   if [ -f /usr/share/bash-completion/bash_completion ]; then
134     . /usr/share/bash-completion/bash_completion
135   elif [ -f /etc/bash_completion ]; then
136     . /etc/bash_completion
137   fi
138 fi
139 export http_proxy="http://192.168.1.1:3128"
140 export https_proxy="http://192.168.1.1:3128"

```

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

Configuration d'un proxy transparent

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

Réglages Proxy généraux	Forward Proxy	Proxy Auto-Config	Listes de Contrôle d'Accès distantes	Soutien
<input checked="" type="radio"/> mode avancé				
Interfaces mandataires	LAN <input type="button" value="Tout effacer"/> <input checked="" type="checkbox"/> Sélectionner tout			
Port du proxy	3128			
Activer le proxy HTTP Transparent	<input checked="" type="checkbox"/>			
Activer l'inspection SSL	<input type="checkbox"/>			
Journalisation des informations SNI seulement	<input type="checkbox"/>			
Port du proxy SSL	3129			
AC à utiliser	Nothing selected			
Ne pas inspecter ces sites SSL	<input type="button" value="Tout effacer"/> <input type="button" value="Copie"/> <input type="button" value="Texte"/>			
<input type="button" value="Appliquer"/>				

Création de règle de redirection (NAT)

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

Sélectionner tout

Port du proxy	3128
Activer le proxy HTTP Transparent	<input checked="" type="checkbox"/>
Enable transparent proxy mode. You will need a firewall rule to forward traffic from the firewall to the proxy server. You may leave the proxy interfaces empty, but remember to set a valid ACL in that case. Add a new firewall rule	
Activer l'inspection SSL	<input type="checkbox"/>
Journalisation des informations SNI seulement	<input type="checkbox"/>
Port du proxy SSL	3129
AC à utiliser	Nothing selected
Ne pas inspecter ces sites SSL	
<input type="button" value="Tout effacer"/> <input type="button" value="Copie"/> <input type="button" value="Texte"/>	
Appliquer	

sauvegarder et appliquer ces changement

Accueil
Rapports
Système
Interfaces
Pare-feu
Alias
Automatisation
Catégories
Groupes
NAT
Redirection de port
1-à-1
Sortant
NPTv6
Règles
Façonneur
Paramètres
Fichiers journaux
Diagnostics
VPN
Services
Alimentation
Aide

Pare-feu: NAT: Redirection de port

Sélectionnez une catégorie

Les modifications ont été appliquées avec succès.

	Source	Destination	NAT				
<input type="checkbox"/> LAN	TCP	*	LAN adresse	80	<input type="checkbox"/> Règle anti-Lockout		
<input type="checkbox"/> LAN	TCP	LAN net	*	80 (HTTP)	127.0.0.1	3128	Rediriger le trafic vers le proxy
<input checked="" type="checkbox"/> Règle activée			Non redirigé				Règle liée
<input checked="" type="checkbox"/> Règle désactivée			Désactivé pas de redirection				Règle liée désactivée
<input type="checkbox"/> Alias (cliquer pour visualiser/éditer)							

pareil pour Activer l'inspection SSL

Import bookmarks... Parrot OS Hack The Box OSINT Services Vuln DB Privacy and Security Learning Resources

root@OPNsense.internal

OPNsense® Securing networks made easy

Accueil
Rapports
Système
Interfaces
Pare-feu
Alias
Automatisation
Catégories
Groupes
NAT
Redirection de port
1-à-1
Sortant
NPTv6
Règles
Façonneur
Paramètres
Fichiers journaux
Diagnostics
VPN
Services
Alimentation
Aide

Pare-feu: NAT: Redirection de port

Modifier entrée de Redirection

Désactivé Désactiver cette règle

Pas de RDR (SANS)

Interface LAN

Version TCP/IPv4

Protocole TCP

Source / Inverser

Source LAN net

Plage de ports source de: any à: any

Destination / Inverser

Destination any

Plage de ports de destination de: HTTPS à: HTTPS

Rediriger l'IP de destination Hôte unique ou Réseau

OPNsense (c) 2014-2026 Deciso B.V.

Pare-feu: NAT: Redirection de port

La configuration NAT a été modifiée.
Vous devez appliquer les modifications pour qu'elles prennent effet.

	Source	Destination	NAT	
	Interface Proto Adresse Ports	Adresse Ports	IP Ports Description	
<input type="checkbox"/>	LAN TCP *	LAN adresse 80	*	Règle anti-Lockout
<input type="checkbox"/>	LAN TCP LAN net *	80 (HTTP)	127.0.0.1 3128	Rediriger le trafic vers le proxy
<input type="checkbox"/>	LAN TCP LAN net *	443 (HTTPS)	127.0.0.1 3129	Rediriger le trafic vers le proxy
	Règle activée Règle désactivée	Non redirigé Désactivé pas de redirection		Règle liée Règle liée désactivée
	Alias (cliquer pour visualiser/éditer)			

OPNsense (c) 2014-2026 Deciso B.V.

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)

Services: Proxy Web Squid: Administration

Réglages Proxy généraux ▾ Forward Proxy ▾ Proxy Auto-Config ▾ Listes de Contrôle d'Accès distantes Soutien aide complète ⓘ

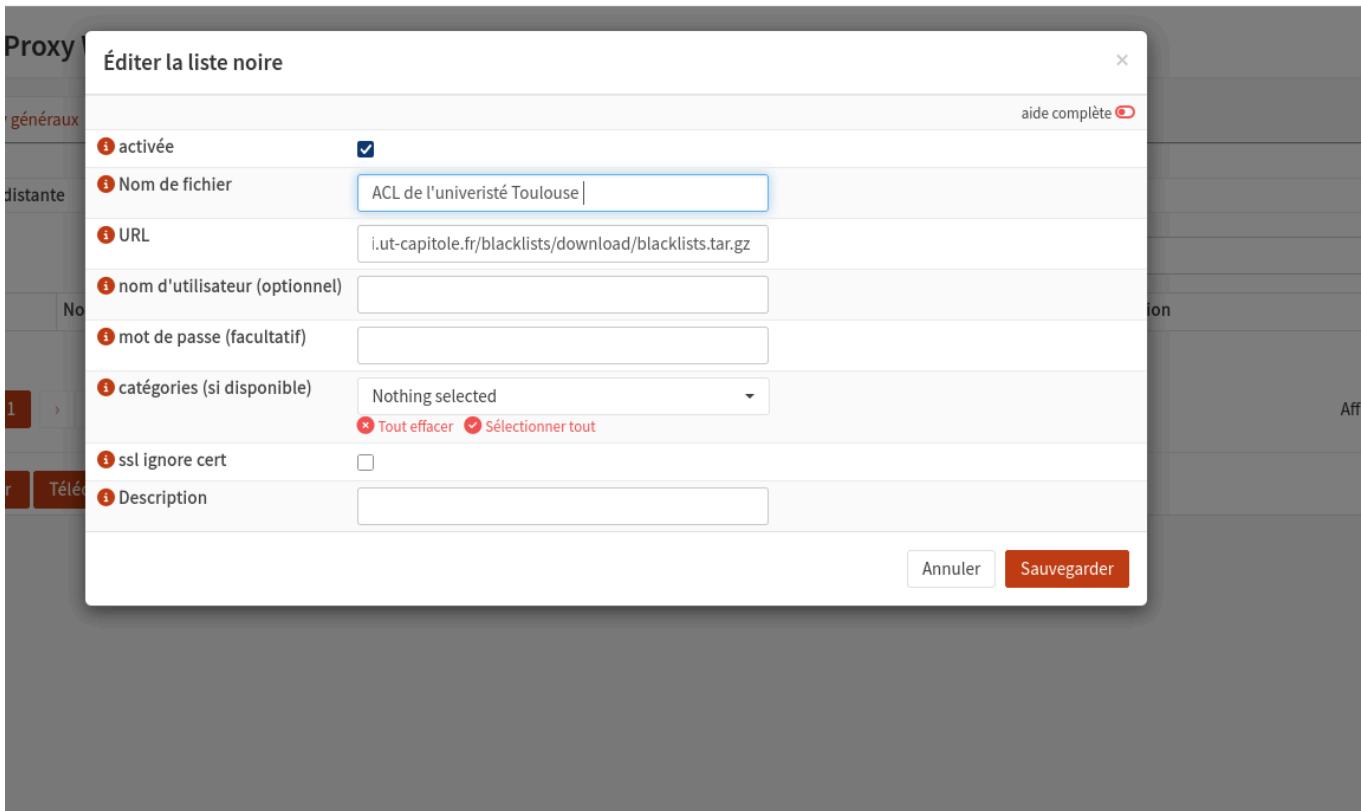
1 Liste noire distante

Activé	Nom de fichier	URL	Description	Modifier Supprimer
<input type="checkbox"/>				

Affichage des entrées 0 à 0 sur 0 +

Appliquer Télécharger les ACLs & les Appliquer Télécharger ACLs Planifier avec Cron

OPNsense (c) 2014-2026 Deciso B.V.



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

Services: Proxy Web Squid: Administration

Réglages Proxy généraux ▾ Forward Proxy ▾ Proxy Auto-Config ▾ Listes de Contrôle d'Accès distantes Soutien aide complète

>Liste noire distante

<input type="checkbox"/> Activé	Nom de fichier	URL	Description	Modifier Su...
<input checked="" type="checkbox"/>	blocagesites	http://dsi.ut-capitole.fr/blacklists/download/blacklists.tar.gz	actltoulouse	

Affichage des entrées 1 à 1 sur 1 [+ Ajouter](#)

[Appliquer](#) [Télécharger les ACLs & les Appliquer](#) [Télécharger ACLs](#) [Planifier avec Cron](#)

<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

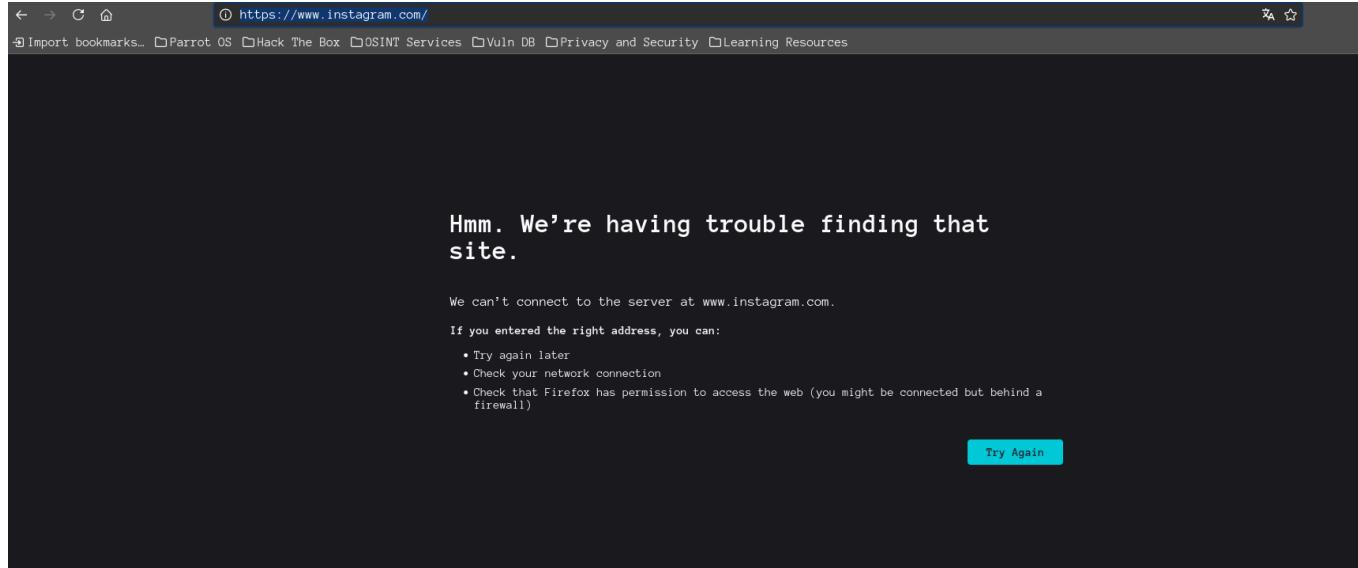
Avec mon proxy transparent j'ai bloqué l'accès au réseaux sociaux mais quand j'essaye d'accéder à instagram et à facebook je peux le faire. Internet est activée et le proxy aussi.

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

Règles générées automatiquement						
<input type="checkbox"/>	▶ ➔ ⚡ ⓘ	IPv4 TCP	LAN net	*	127.0.0.1	3128
<input type="checkbox"/>	▶ ➔ ⚡ ⓘ	IPv4 TCP	LAN net	*	127.0.0.1	3129
<input type="checkbox"/>	▶ ➔ ⚡ ⓘ	IPv4 *	LAN net	*	*	*
<input type="checkbox"/>	▶ ➔ ⚡ ⓘ	IPv6 *	LAN net	*	*	*



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)

- Configuration 
- Firmware 
- Passerelles 
- Haute disponibilité 
- Routes 
- Paramètres 
- Instantanés 
- Gestion des Certificats 
- Autorités 
- Certificats 
- Révocation 
- Paramètres 
- Fichiers journaux 
- Diagnostics 
- Interfaces 
- Pare-feu 
- VPN 

Système: Gestion des Certificats: Autorités

Certificats

 Recherche



50 ▾



<input type="checkbox"/>	Description	Émetteur	Nom	Usages	Validé à p...	Validé jus...	Commandes
<input type="checkbox"/>	pour TP c...		/C=NL	1	Jan 16, 20...	Apr 20, 20...	    

« ‹ › »

Affichage des entrées 1 à 1 sur 1

cliquer sur le nuage pour le télécharger

Téléchargement du certificat

Type de fichier

Certificate

Téléchargement

Affichage des entrées 1 à

→ ↑ ↵ > Téléchargements Rechercher dans: 🔎

Nouveau 🗑️ 📁 📄 📤 🗑️ Trier ⚙️ Afficher ⚙️ ⏮ Détails

☐ Nom	Modifié le	Type	Taille
pour TP cyber_crt.pem	21/01/2026 16:58	Fichier PEM	2 Ko

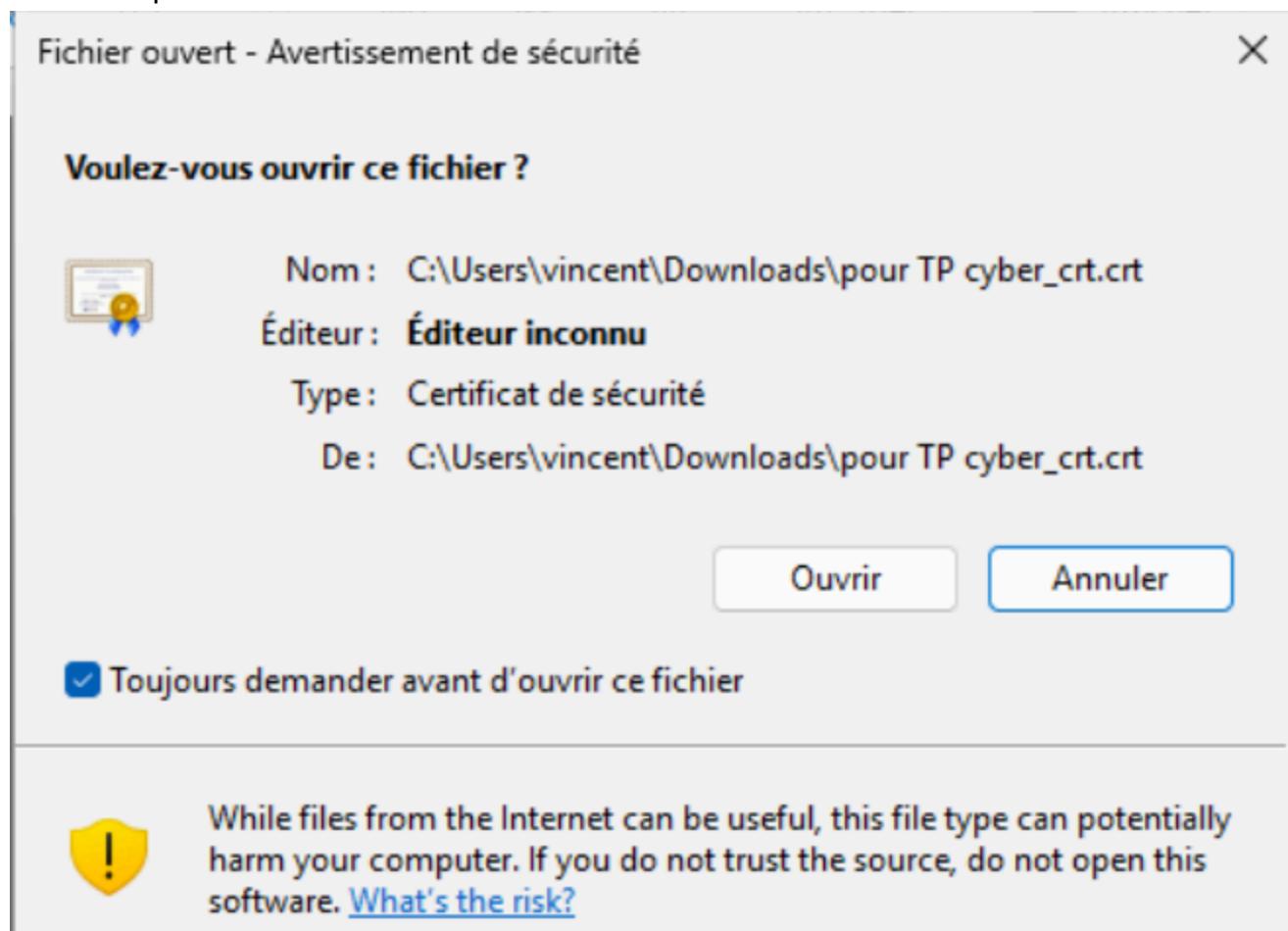
Accueil Galerie OneDrive Bureau Téléchargement Documents Images Musique Vidéos

Detailed description: This image shows a Windows file explorer window with a modal dialog box overlaid. The dialog box is titled 'Téléchargement du certificat' and has a dropdown menu set to 'Certificate'. A large 'Téléchargement' button is at the bottom right. The main file explorer window shows a folder structure on the left with 'Téléchargement' selected. The main pane displays a single file: 'pour TP cyber_crt.pem' (File type: Fichier PEM, Size: 2 Ko). The file was modified on 21/01/2026 at 16:58.

renomme le en .crt

Nom	Modifie le	Type	Taille
▼ Aujourd'hui			
 pour TP cyber_crt	21/01/2026 16:58	Certificat de sécur...	2 Ko

double cliquer dessus



Puis cliquer sur ouvrir et installer ce certificat sélectionner ordinateur local

The screenshot shows the 'Import Certificate Wizard' welcome screen. At the top right is a close button (X). Below it, a back arrow and the title 'Assistant Importation du certificat'. The main heading 'Bienvenue dans l'Assistant Importation du certificat' is bolded. A descriptive text follows: 'Cet Assistant vous aide à copier des certificats, des listes de certificats de confiance et des listes de révocation des certificats d'un disque vers un magasin de certificats.' Below this, another text explains: 'Un certificat, émis par une autorité de certification, confirme votre identité et contient des informations permettant de protéger des données ou d'établir des connexions réseau sécurisées. Le magasin de certificats est la zone système où les certificats sont conservés.' A section titled 'Emplacement de stockage' contains two radio buttons: 'Utilisateur actuel' (unchecked) and 'Ordinateur local' (checked). At the bottom, a note says 'Cliquez sur Suivant pour continuer.' and at the very bottom are 'Suivant' and 'Annuler' buttons.

← Assistant Importation du certificat

Bienvenue dans l'Assistant Importation du certificat

Cet Assistant vous aide à copier des certificats, des listes de certificats de confiance et des listes de révocation des certificats d'un disque vers un magasin de certificats.

Un certificat, émis par une autorité de certification, confirme votre identité et contient des informations permettant de protéger des données ou d'établir des connexions réseau sécurisées. Le magasin de certificats est la zone système où les certificats sont conservés.

Emplacement de stockage

Utilisateur actuel

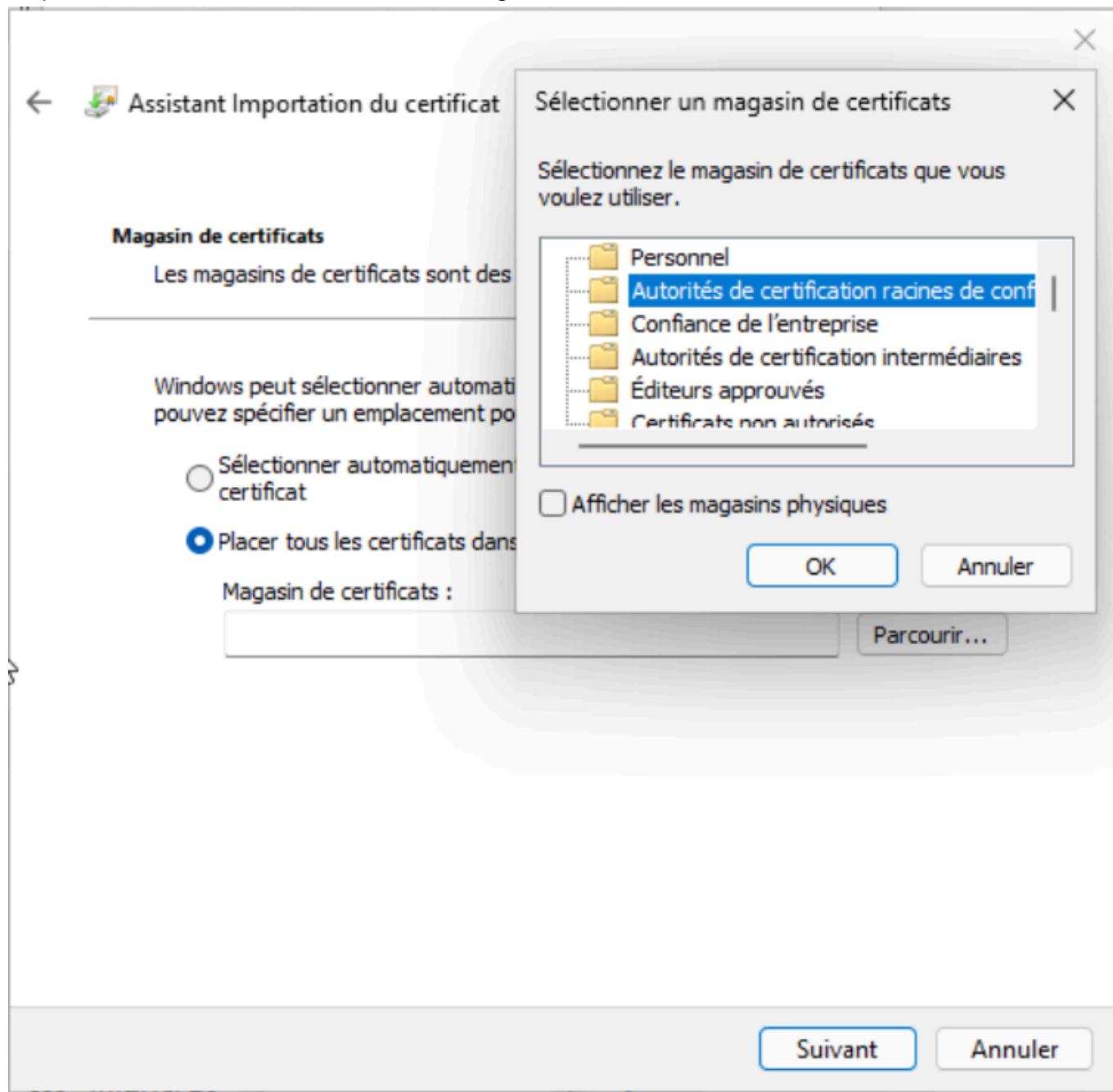
Ordinateur local

Cliquez sur **Suivant** pour continuer.

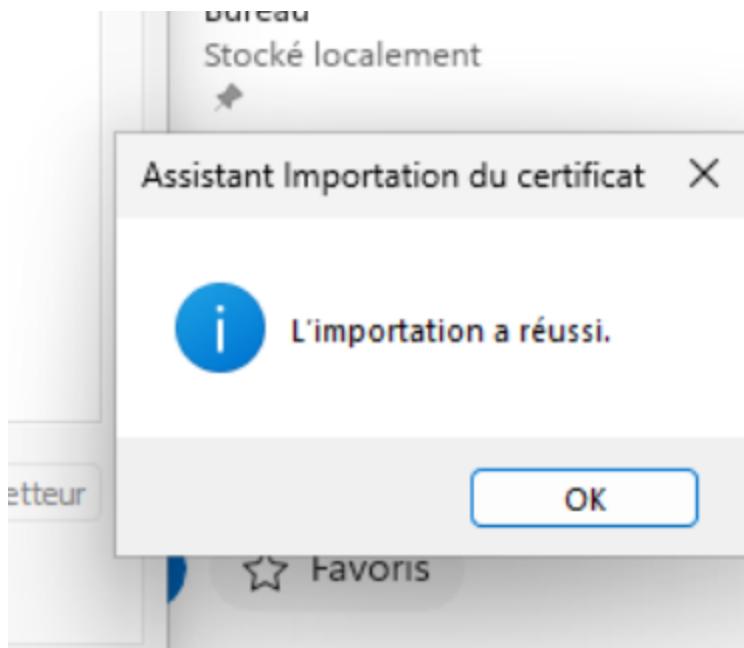
Suivant

Annuler

cliquer sur suivant et oui choisir le bon magasin de certificat



cliquer sur terminé



Test

Le test marche

A screenshot of a browser displaying a connection error page. At the top, there's a small blue cloud icon with three dots. The main content area has a light gray background with the text "Désolé, impossible d'accéder à cette page." (Sorry, unable to reach this page.) in large bold letters. Below it, it says "www.instagram.com a mis trop de temps pour répondre" (www.instagram.com took too long to respond). A section titled "Essayez :" (Try:) lists two items: "Vérification de la connexion" (Connection check) and "Vérification du proxy et du pare-feu" (Proxy and firewall check), with the second item being underlined. At the bottom left, the error code "ERR_CONNECTION_TIMED_OUT" is shown, and at the bottom right, there's a blue "Actualiser" (Refresh) button.

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