

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 transparent](#)
- [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](#)

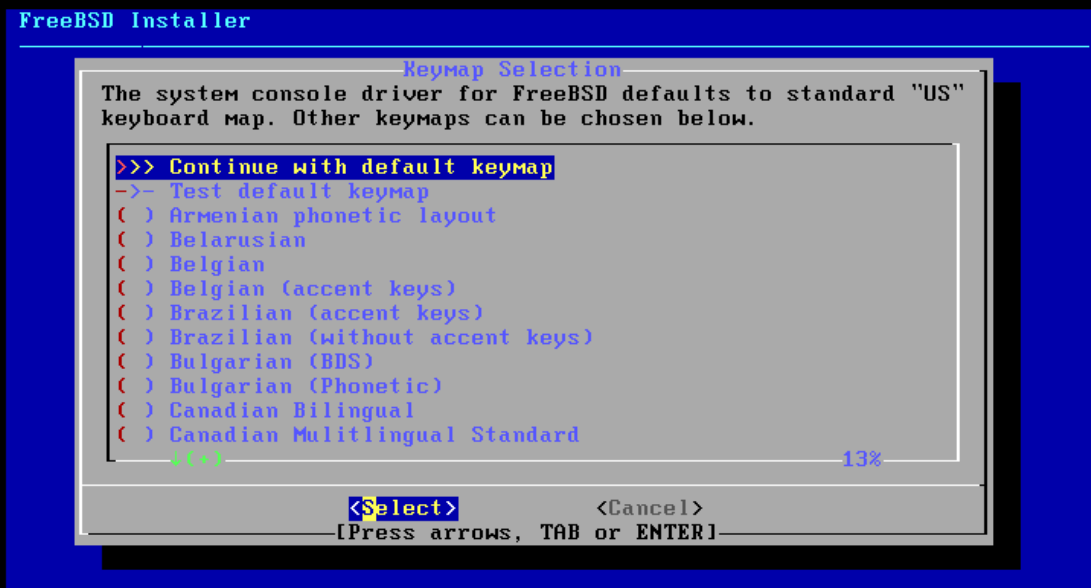
Mise en place d'OPNsens

bien prendre le format DVD

Extraire le dossier téléchargé

Faire une VM

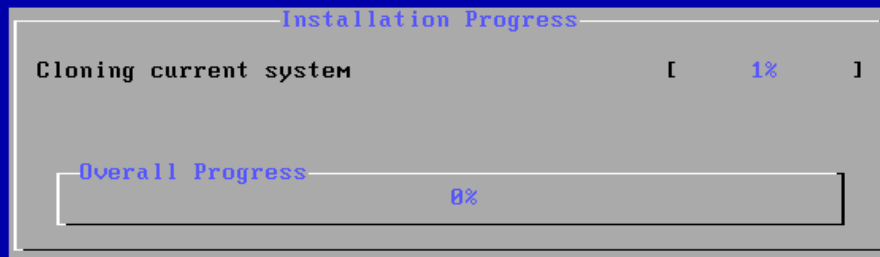
les login de base OPNsense Installer opnsense



Tout mettre en ok

sélectionner le disque dur virtuel

OPNsense Installer



choisir l'option 1 pour configurer les carte réseaux LAN et WAN
Puis l'option 2 pour configurer le LAN

```
Setting up gateway monitor...done.
Configuring firewall.....done.
Starting Dnsmasq...done.
Starting NTP service...done.
Starting Unbound DNS...done.
Starting web GUI...done.
Syncing OpenVPN settings...done.

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

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

HTTPS: sha256 C6 F4 7A 92 A4 31 23 03 11 20 9A 12 E7 96 77 D8
          2F 61 03 B1 43 90 E4 F0 D4 B6 DA A8 57 F2 C1 A4

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: █
```

```

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

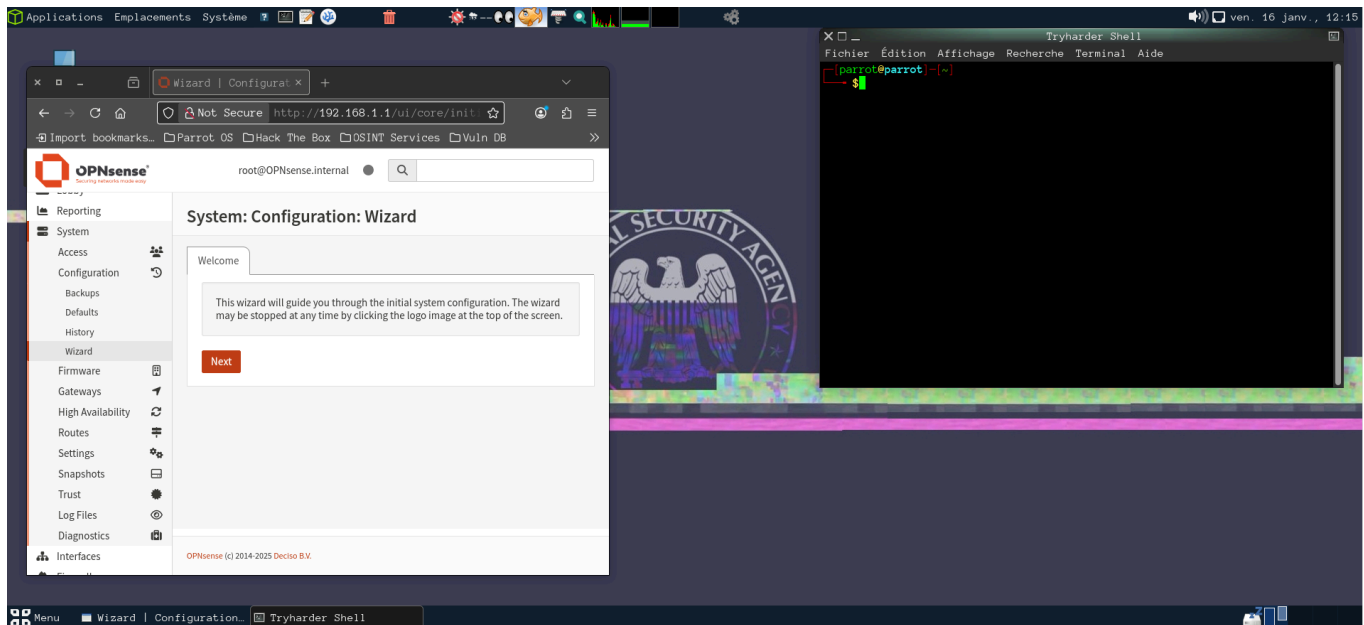
0) Logout
1) Assign interfaces
2) Set interface IP address
3) Reset the root password
4) Reset to factory defaults
5) Power off system
6) Reboot system
7) Ping host
8) Shell
9) pfTop
10) Firewall log
11) Reload all services
12) Update from console
13) Restore a backup

Enter an option:

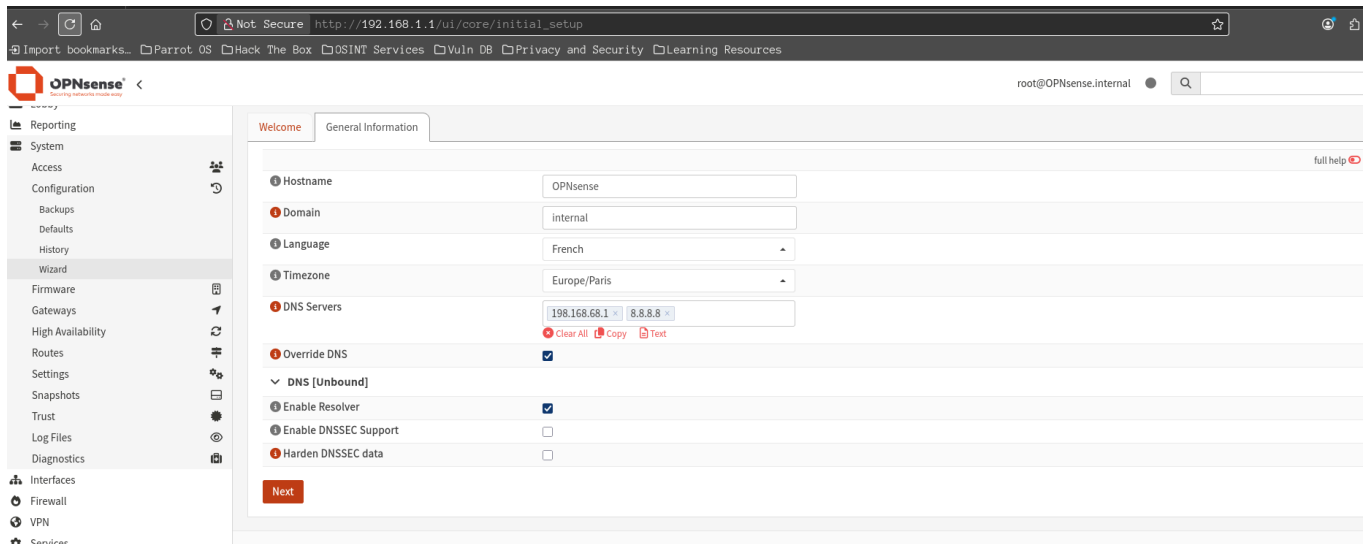
```

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

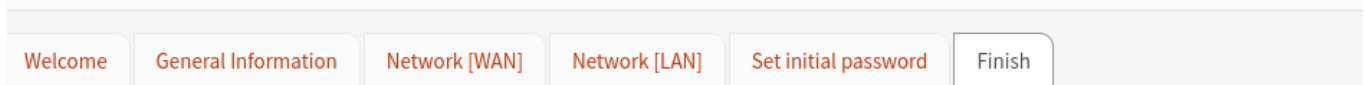
Se connecter à l'IP LAN sur l'autre VM se connecter en root



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



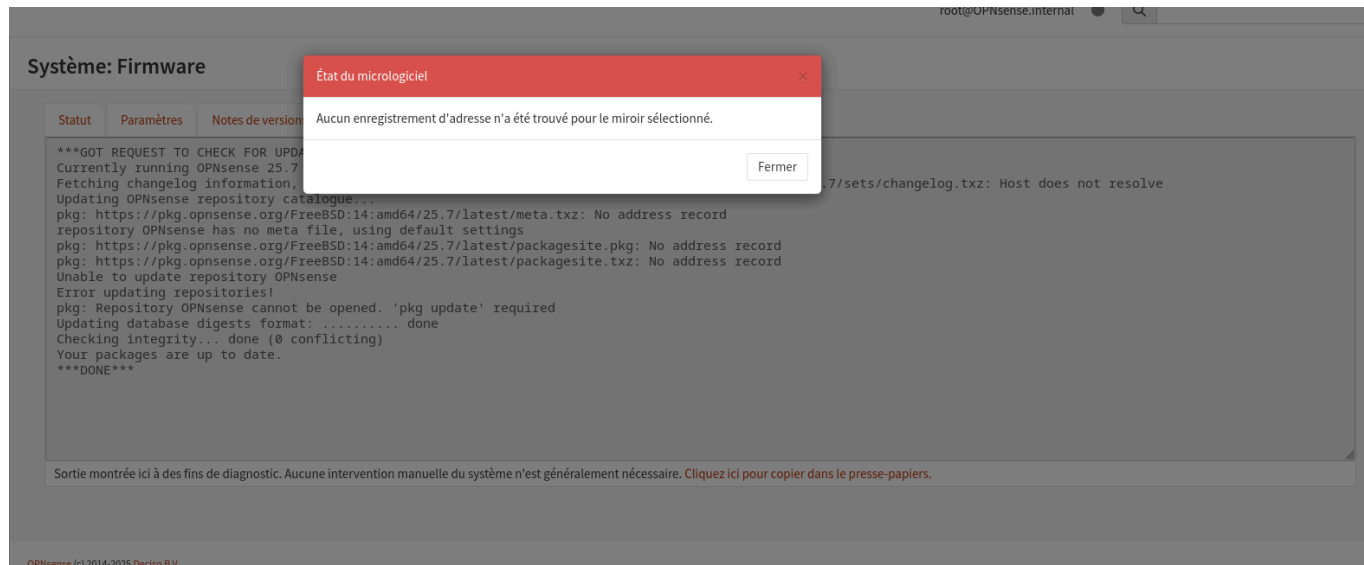
System: Configuration: Wizard



This is the last step in the wizard, click apply to reconfigure the firewall.

Apply

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-----
MIIJQgIBADANBgkqhkiG9w0BAQEFAASCSSwwggkoAgEAAoICAQCnKVdaBiFhT933
IXam96DEUJeLbdL3cpTBOFAoj/BC6a0jTfFBvb1BH5n3JxHzSWM7uyCaICsxJvyN
iQSV5JLZYIkADOGpqBpyzfypFy+/fI0s+/LMF0y7LM2F/Dj/ixJn65qlyl60nc+
Ya46su3DGO4w2IXyjLKv+ZIS6IzTnmFdxsibmekxgoAh/GZuJIxUovhku1+BPyrV
38fUJoIqZXe/wG1VaMaVtu2egcUHOM+OL2nTxkv1wVwkHAFauK9PiZIAynlAxqw4
Yk8y4cRsU9nFU9xDB4Fx03+9f1/Soz0bhZOSzJqqWNe02w93pz7tC7k80ng+WriZ
gSg1VviLoiTid1R++ISjdUL8lb/CdzXyurs5YynJKpEZqWd03thgnv/8gYhIdPOs
3UdREbUm7HXX1BEqv/yLQuCUFi3Gqq8z1xk9oegX/NOZMkvkCgNzhwkQwJqydSbQ
hMfYFYdw8zLJru/bjwbj5fI+mvrDMC5Xwxa7NJsi/hLa6lyP1d5uQBQUDRrhue3r
Pdjq484JSZe3pFUQuQjkI+R5UfEK00AGbJxbxr/OCWcpDAKD9ki+veHG0op9jv07

```

```

2H4qxhWU63gpE12sVw+y3fhVHRf5tK9XSLw3XzjjAmCK7ggam9tK0rqEU0zmE9XZ
Pd1afMz5dIQk/f0IT3A8pn7rWRYp73RRiIhFFCPO8nZra3dDuBjZurw1iBwR91Pi
+LlytWqiGdHVGn9oXRPXZnNXpFgdTw==
-----END PRIVATE KEY-----
[parrot@parrot]--[~/home/cert-opsense]
$cat opsense.crt
-----BEGIN CERTIFICATE-----
MIIFAzCCA10gAwIBAgIUUVN9XqCN/DSM+tbLdhbyRVbdkRyYwDQYJKoZIhvcNAQEL
BQAwRTElMAkGA1UEBhMCRR1IxEzARBgNVBAgMC1NvbWUtU3RhdGUxITAfBgNVBAoM
GE1udGVybWV0IFdpZGdpdHMgUHR5IEEx0ZDAeFw0yNjAxMTYxMTQyMzJaFw0yNzAx
MTYxMTQyMzJaMEUxCzAJBgNVBAYTAkZSMRMwEQYDVQQIDApTb211LVN0YXRIMSEw
HwYDVQQKBDBhJbnRlcm5ldCBXaWRnaXRzIFB0eSBMdGQwggiMA0GCSqGSIb3DQEB
AQUAA4ICDwAwggIKAoICAQCnKVdaBiFhT933IXam96DEUJeLbdL3cpTBOFAoj/BC
6aOjTfFBvb1BH5n3JxHzSWM7uyCaICsxJvyNiQSV5JLZYIkkADOGpqBpyzfypFy+
/fI0s+/LMF0y7LM2F/Dj/ixJn65qlyl60nc+Ya46su3DGO4w2IXyjLKv+ZIS6IzT
nmFdxsibmekxgoAh/GZuJIXUovhku1+BPyrV38fUJoIqZXe/wG1VaMaVtu2egcUH
OM+OL2nTxkv1wVWkHAFauK9PiZIAyn1Axqw4Yk8y4cRsU9nFU9xDB4Fx03+9f1/S
oz0bhZ0SzJqqWNe02w93pz7tC7k80ng+WrIzgSg1VviLoiTiD1R++ISjdUL81b/C
dzXyurs5YynJKpEZqWd03thgnv/8gYhIdP0s3UdREbUm7HXX1BEqv/yLQuCUFi3G
qq8z1xk9oegX/NOZMkvkCgNzhwkQwJqydSbQhMfYFYdw8zLJru/bjwbj5fI+mvrD
MC5Xwxa7NJsi/hLa6lyP1d5uQBQUdRrhue3rPdjq484JSZe3pFUQuQjkI+R5UfEK
00AGbJxbxr/OCwcpDAKD9ki+veHG0op9jv070uDuEnZWix+wjGa5HT180x7IpTw2
Q9X21uRFsQHbPsXZ3FKyOmVLdXk52nEpo7QEVb1puoF731CWq666VG8utoTjL1Ju
tQIDAQABo1MwUTAdBgNVHQ4EFgQUd9JIvsgSoAcG8b3jFLts5DK2ktEwHwYDVR0j
BBgwFoAUD9JIvsgSoAcG8b3jFLts5DK2ktEwDwYDVR0TAQH/BAUwAwEB/zANBgkq
hkiG9w0BAQsFAAOCAGEAZqvaEJny0EZ4ZF63j1YrsU4oOxHNWqxN0Mf3hUnTtmNo
QKawRVEco90YXNfv4TGnek8aSY/XetaIDm8goYR/INO/I1pccuqUv2UEI572+ruC
pV7sXCuyc3cJY/M0A0meYDygvWgFGSxwZm/AETdXse8FpEv8ocxE442Ct8y8Xg7
c4ssyu+tI5R4Lhmg9nS75VDQg+QWz0Kkk/zByaehR5kYsC11tbWpq7epnTJ0qBEr
wPjbLVJwNyqM4gbJPf3kP6UKso1Obdmk2/x1LSB/cFjkHNHx0SbcA42vk929Xew0
bngrK8ulGxC+Ebtt34FqRXd8kVp3mneLGVU9nDJwfdIE1HxFbSvbwIu32w+59QM7
t02mGFECrMfEq5KLpeiunoUxTkB1qpskyuFT3sUM713u5F+ZgnugMtZwy1QJme4U
H1luqVA4y/nKn+jJX4Ta6uuuaf+TVVWx81nz/kAA9DESegqo3jQ9cHGjXvkfyjfc
2aw07k2TYt952Q0A5hgTNvk4Cn3Ae39AB1fQj8/LEz8dqCF1YY18D+t8IbsSA6n0

```

Intégration dans opsense

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

The screenshot shows the OPNsense web interface. The left sidebar contains a menu with options like 'Accès', 'Configuration', 'Firmware', 'Passerelles', 'Haute disponibilité', 'Routes', 'Paramètres', 'Instantanés', 'Gestion des Certificats', 'Autorités', 'Certificats', 'Révocation', 'Paramètres', 'Fichiers journaux', and 'Diagnostics'. The main content area is titled 'Système: Gestion des Certificats: Certificats' and displays a table of certificates.

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

At the bottom of the table, it says 'Affichage des entrées 1 à 3 sur 3'.

cliquer sur la petit croix installer

StatutParamètresNotes de versionsMises à jourGreffonsPaquets

Configuration file /usr/local/etc/squid/squid.conf.example.

```
/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

OPNsense

AccueilRapportsSystèmeInterfacesPare-feuVPNServicesPortail CaptifDHCRelayDnsmasq DNS & DHCPDétection d'IntrusionISC DHCPv4ISC DHCPv6Kea DHCPMonitHeure réseauOpenDNSProxy Web SquidAdministrationJournal du cacheJournal d'accèsJournal du magasinUnbound DNSAlimentationAide

root@OPNsense.internal

Services: Proxy Web Squid: Administration

Réglages Proxy générauxForward ProxyProxy Auto-ConfigListes de Contrôle d'Accès distantesSoutien

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

i

 Interfaces mandataires

LAN

Tout effacer

Sélectionner tout

i

 Port du proxy

3128

i

 Activer le proxy HTTP Transparent

i

 Activer l'inspection SSL

i

 Journalisation des informations SNI seulement

i

 Port du proxy SSL

3129

i

 AC à utiliser

Nothing selected

i

 Ne pas inspecter ces sites SSL

Tout effacer

Copie

Texte

Appliquer

Appliquer

Activer le cache local

Services: Proxy Web Squid: Administration

Réglages Proxy généraux

Forward Proxy

Proxy Auto-Config

Listes de Contrôle d'Accès distantes

Soutien

Réglages Proxy généraux

Paramètres Cache Local

Réglages de la gestion de trafic

Paramètres du proxy parental

Mo)

256

i

 Activer le Cache Linux Package

i

 Activer le Cache Windows Update

Appliquer

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

mode avancé

i Taille du cache mémoire (en Mo)

i Activer le cache local
☒

i Activer le Cache Linux Package
☐

i Activer le Cache Windows Update
☐

Appliquer

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

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
Inspector

	Protocole	Source	Port	Destination	Port	Passerelle	Planifier	Description	
Règles générées automatiquement									
<input type="checkbox"/>	IPv4 *	LAN net	*	*	*	*	*	Default allow LAN to any rule	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
<input type="checkbox"/>	IPv6 *	LAN net	*	*	*	*	*	Default allow LAN IPv6 to any rule	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
<input checked="" type="checkbox"/>	autoriser	<input checked="" type="checkbox"/> bloquer	<input checked="" type="checkbox"/> rejeter	<input checked="" type="checkbox"/> tracer	<input checked="" type="checkbox"/> entrant	<input checked="" type="checkbox"/> première correspondance			
<input checked="" type="checkbox"/>	passer (désactivé)	<input checked="" type="checkbox"/> bloquer (désactivé)	<input checked="" type="checkbox"/> rejeter (désactivé)	<input checked="" type="checkbox"/> tracer (désactivé)	<input checked="" type="checkbox"/> sortant	<input checked="" type="checkbox"/> dernière correspondance			
Programme actif/inactif (cliquez pour afficher/modifier)									
Alias (cliquez 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 ☒ Appliquer l'action immédiatement sur la correspondance.

Interface LAN

Direction in

Version TCP/IP IPv4

Protocole TCP

Source / Inverser ☐ Utilisez cette option pour inverser le sens de la correspondance.

Source any

Source Avancé

Destination / Inverser ☐ Utilisez cette option pour inverser le sens de la correspondance.

Destination any

Plage de ports de destination

de: (autres) à: (autres)

80 80

Journaliser ☐ Journaliser les paquets gérés par cette règle

Catégorie

Description blocage du trafic 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	👤	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 trafic HTTP	←	↻	🗑️	
▶	🔴 ➡ ⚡ ⓘ	IPv4 TCP	*	*	! *	443 (HTTPS)	*	*	blocage du trafic HTTPS	←	↻	🗑️	
▶ autoriser ▶ passer (désactivé)	×	bloquer bloquer (désactivé)	×	rejeter rejeter (désactivé)	ⓘ	tracer tracer (désactivé)	➡ entrant ⚡ sortant	⚡ première correspondance dernière correspondance					

 Programme actif/inactif (cliquez 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
--- 8.8.8.8 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]~$
[parrot@parrot]~$ sudo nano ~/.bashrc
[parrot@parrot]~$
[parrot@parrot]~$ sudo pluma ~/.bashrc
[parrot@parrot]~$
[parrot@parrot]~$ $ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=127 time=14.4 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=127 time=45.3 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=127 time=19.4 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=127 time=15.6 ms
64 bytes from 8.8.8.8: icmp_seq=5 ttl=127 time=17.7 ms
64 bytes from 8.8.8.8: icmp_seq=6 ttl=127 time=17.1 ms
64 bytes from 8.8.8.8: icmp_seq=7 ttl=127 time=15.5 ms
64 bytes from 8.8.8.8: icmp_seq=8 ttl=127 time=18.2 ms
64 bytes from 8.8.8.8: icmp_seq=9 ttl=127 time=25.5 ms
^X^C
--- 8.8.8.8 ping statistics ---
10 packets transmitted, 9 received, 10% packet loss, time 9018ms
rtt min/avg/max/mdev = 14.375/20.959/45.254/9.120 ms
[parrot@parrot]~$
[parrot@parrot]~$ sudo pluma ~/.bashrc
```

```
.bashrc (/home/parrot) - Pluma (au nom du superutilisateur)
Fichier Édition Affichage Recherche Outils Documents Aide
Ouvrir Enregistrer Annuler
.bashrc x
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 manuel 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

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

Création de règle de redirection (NAT)

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

Tout effacer

Sélectionner tout

Port du proxy

3128

Activer le proxy HTTP Transparent

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

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

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							
	Interface	Proto	Adresse	Ports	Adresse	Ports	IP	Ports	Description	
<input type="checkbox"/>	LAN	TCP	*	*	LAN adresse	80	*	*	Règle anti-Lockout	<div><div></div><div></div><div></div><div></div></div>
<input type="checkbox"/>	LAN	TCP	LAN net	*	*	80 (HTTP)	127.0.0.1	3128	Rediriger le trafic vers le proxy	<div><div></div><div></div><div></div><div></div></div>
<div><div></div><div></div></div>	Règle activée / Règle désactivée									
<div><div></div><div></div></div>	Non redirigé / Désactivé pas de redirection									
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

OPNsense

root@OPNsense.internal

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

aide complète

Modifier entrée de Redirection

Désactivé

Désactiver cette règle

Pas de RDR (SANS)

Interface

LAN

Version TCP/IP

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 Firewall configuration interface showing NAT Port Forwarding rules.

La configuration NAT a été modifiée. Vous devez appliquer les modifications pour qu'elles prennent effet. [Appliquer les changements](#)

	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	← → - +
<input checked="" type="checkbox"/>									Règle activée	
<input type="checkbox"/>									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)

OPNsense Services: Proxy Web Squid: Administration interface.

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

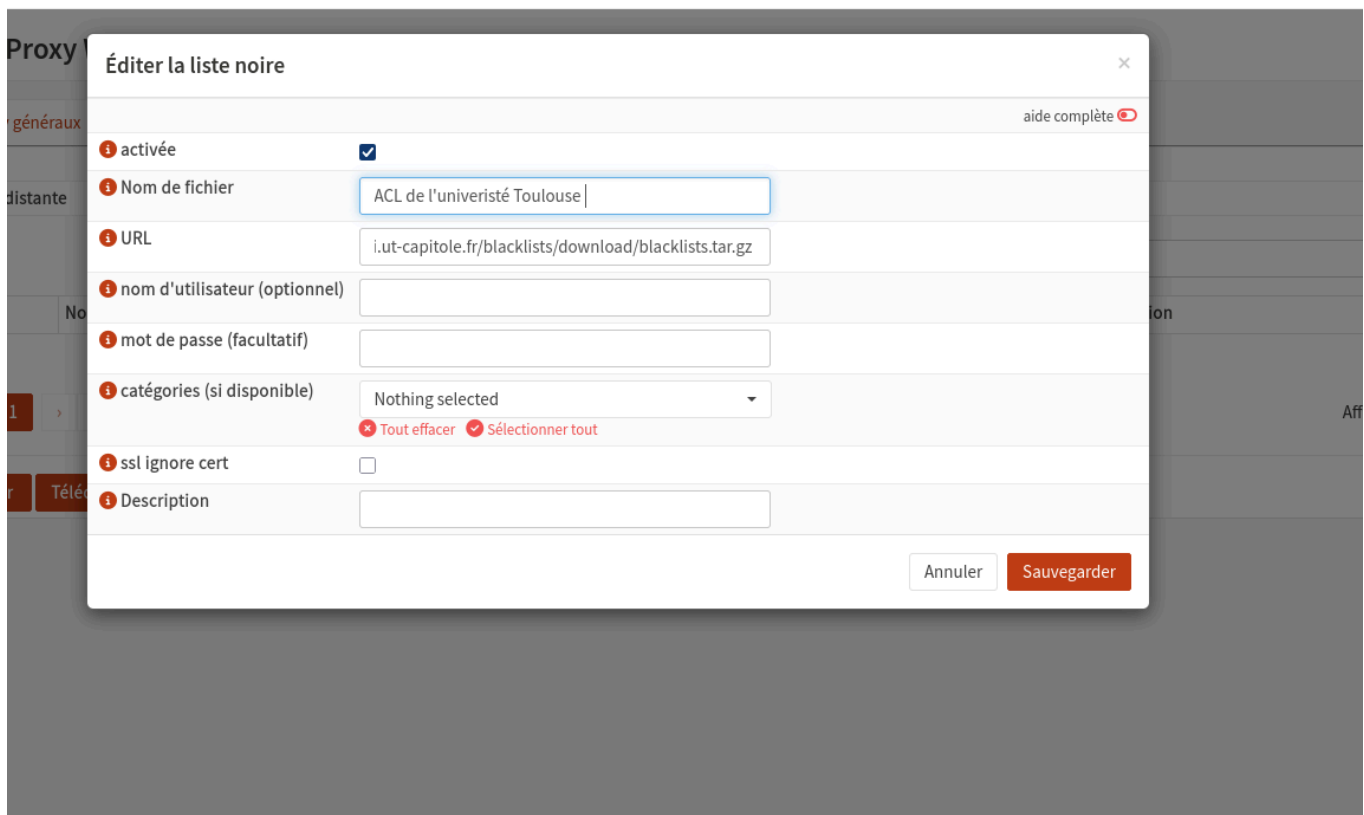
Liste noire distante

Recherche

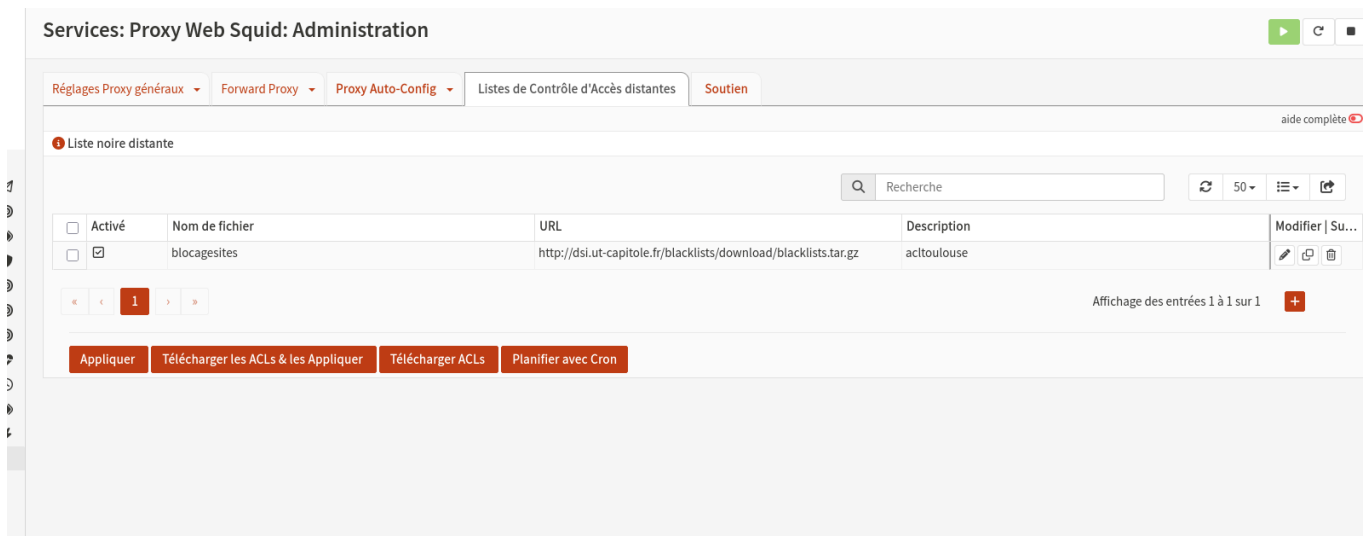
<input type="checkbox"/> Activé	Nom de fichier	URL	Description	Modifier Su...
Affichage des entrées 0 à 0 sur 0				

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



<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/opnsense.crt
#mettre à jour la liste des certificats
sudo update-ca-certificates
```

Problème en phase de test

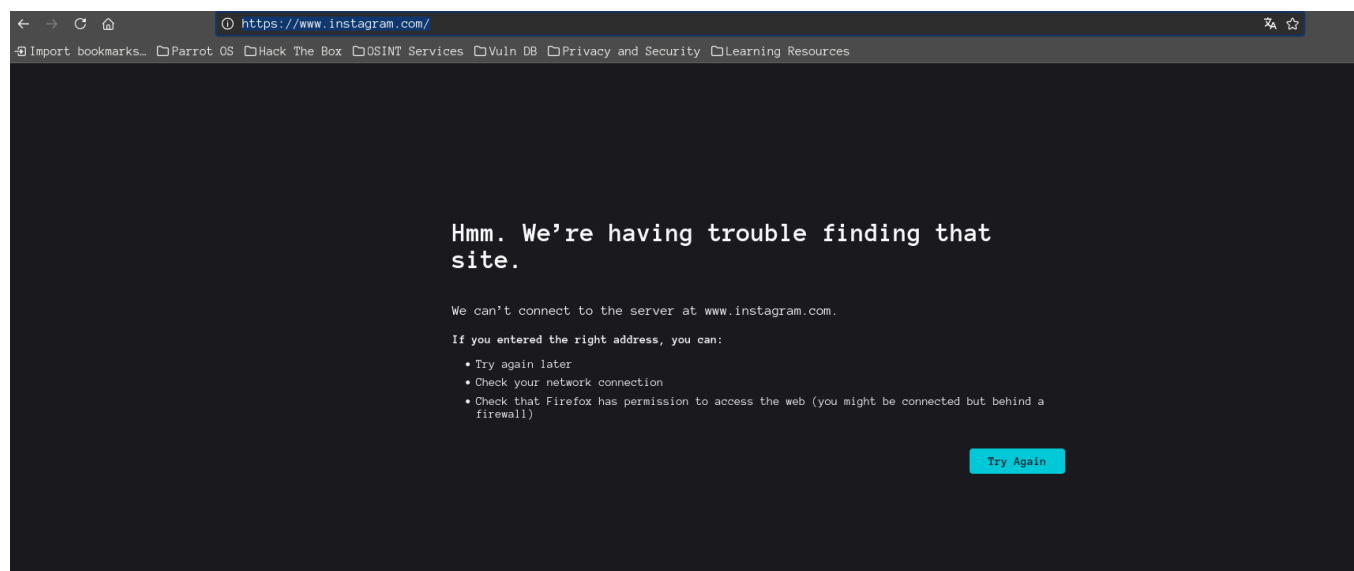
Avec mon proxy transparent j'ai bloqué l'accès au réseaux sociaux mais quand j'essaye d'accéder à instagram et à facebook je peux le faire. Internet est activée et le proxy aussi.

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										22
<input type="checkbox"/>		IPv4 TCP	LAN net	*	127.0.0.1	3128	*	*	Rediriger le trafic vers le proxy	
<input type="checkbox"/>		IPv4 TCP	LAN net	*	127.0.0.1	3129	*	*	Rediriger le trafic vers le proxy	
<input type="checkbox"/>		IPv4 *	LAN net	*	*	*	*	*	Default allow LAN to any rule	
<input type="checkbox"/>		IPv6 *	LAN net	*	*	*	*	*	Default allow LAN IPv6 to any rule	




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)

**OPNsense**
Securing networks made easy

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

root@opnsense.internal

Système: Gestion des Certificats: Autorités

Certificats

Recherche

50

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

1

Affichage des entrées 1 à 1 sur 1

cliquer sur le nuage pour le télécharger

Téléchargement du certificat



Type de fichier

Certificate

Téléchargement



Téléchargements

Rechercher dans:



Nouveau



Trier

Afficher



Détails

Accueil

Galerie

OneDrive

Bureau

Téléchargement

Documents

Images

Musique

Vidéos

Nom

Modifié le

Type

Taille

Aujourd'hui




pour TP cyber.crt.pem

21/01/2026 16:58

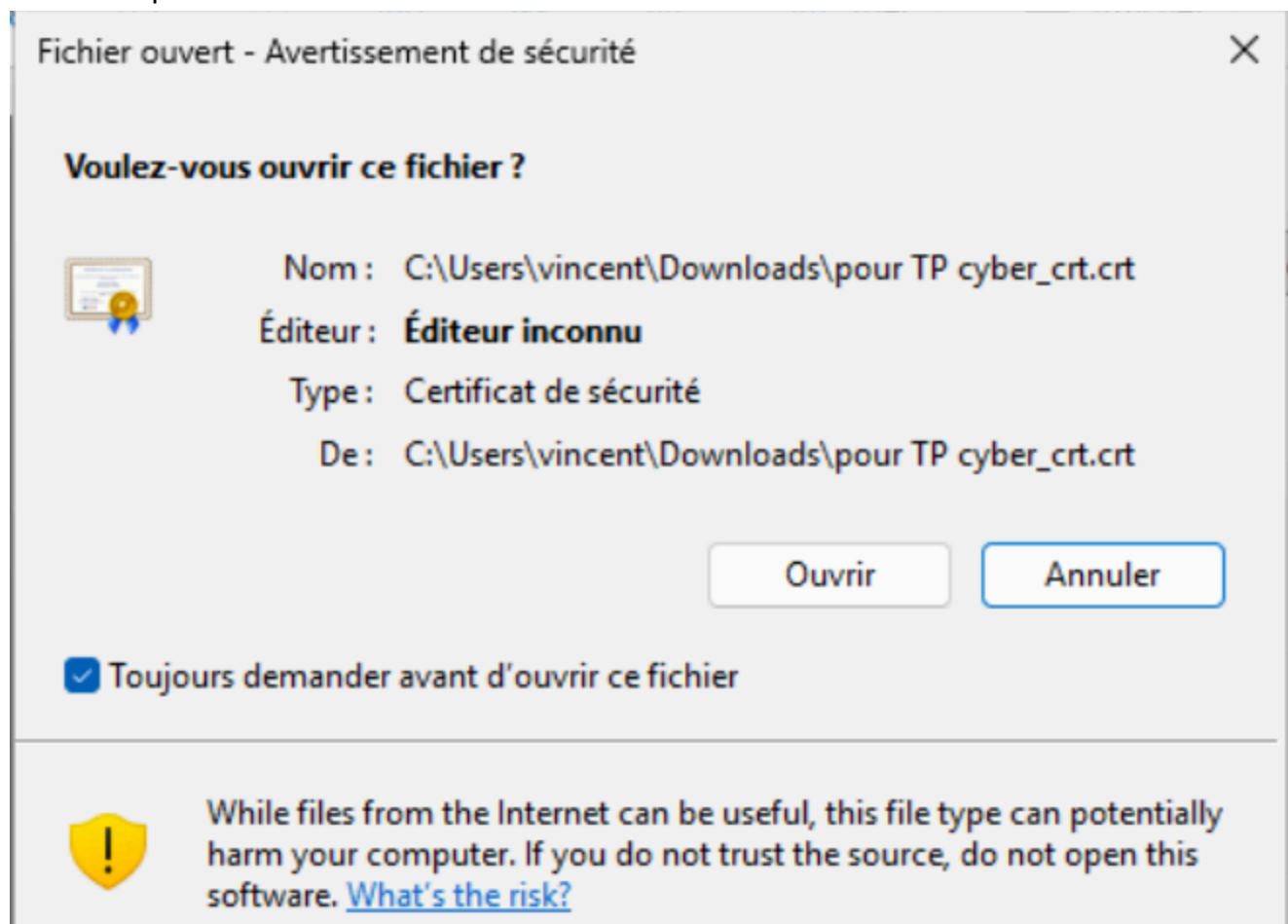
Fichier PEM

2 Ko

renomme le en .crt

Nom	Modifié 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



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

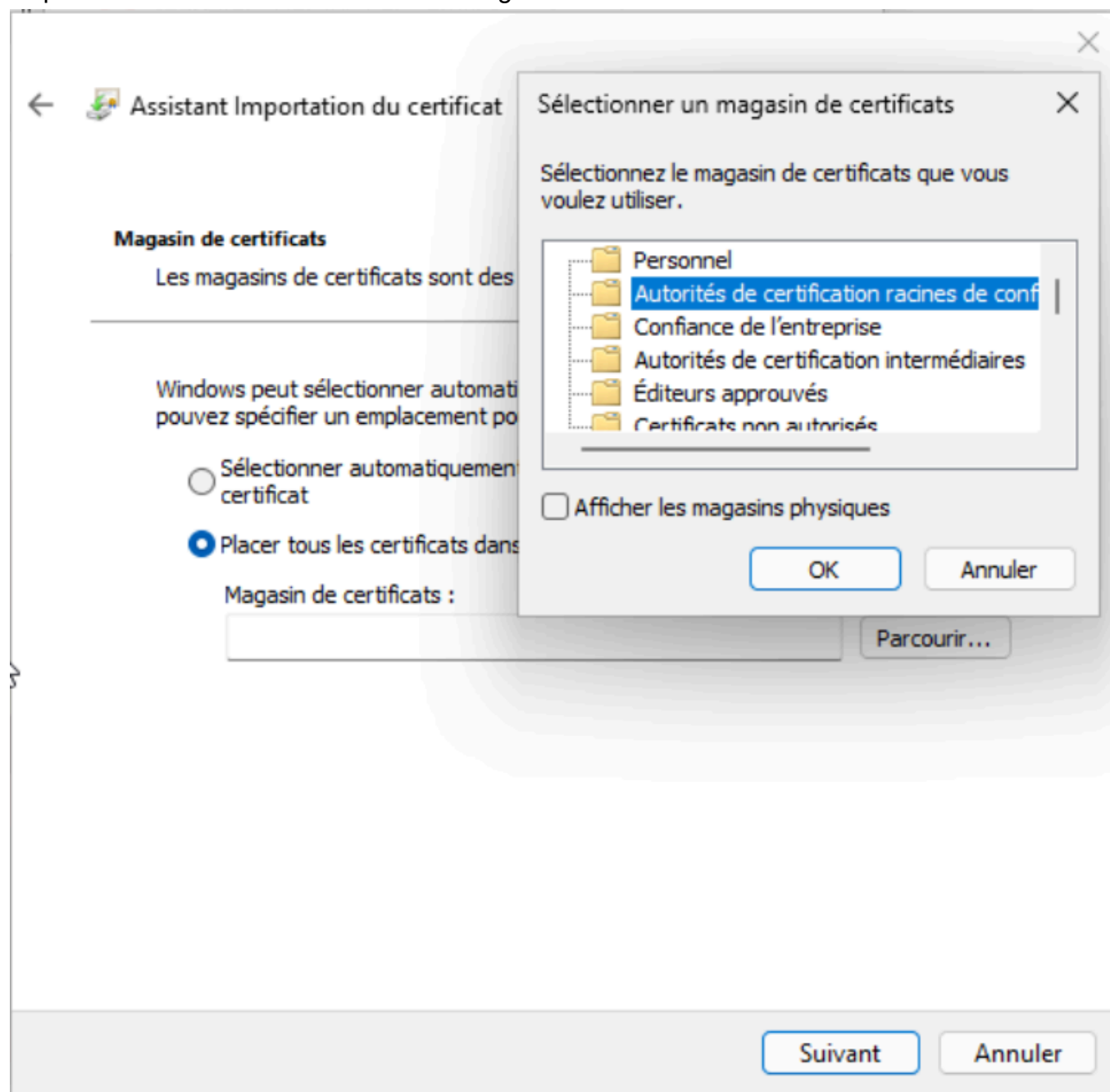
Cliquez sur Suivant pour continuer.



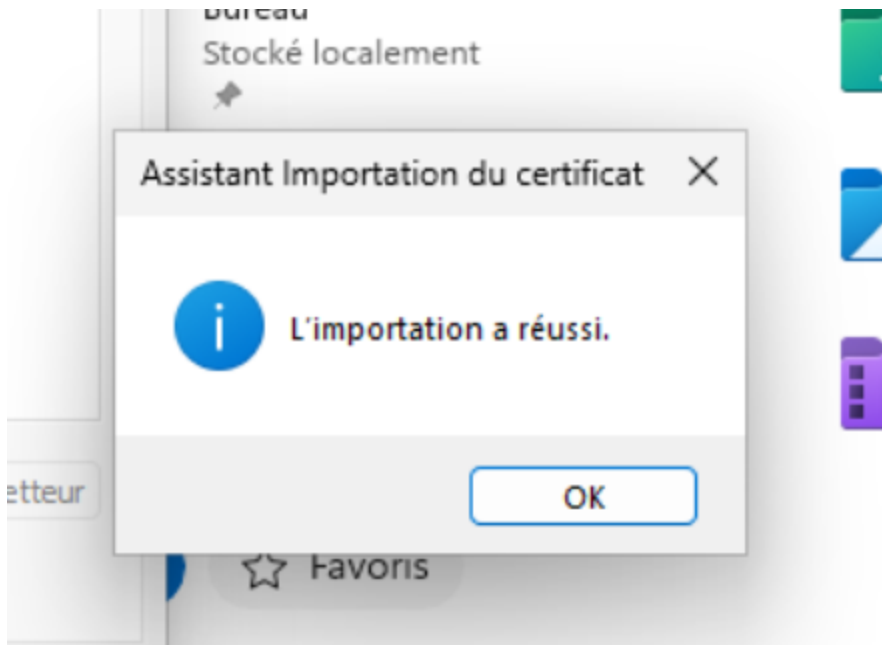
Suivant

Annuler

cliquer sur suivant et oui choisir le bon magasin de certificat

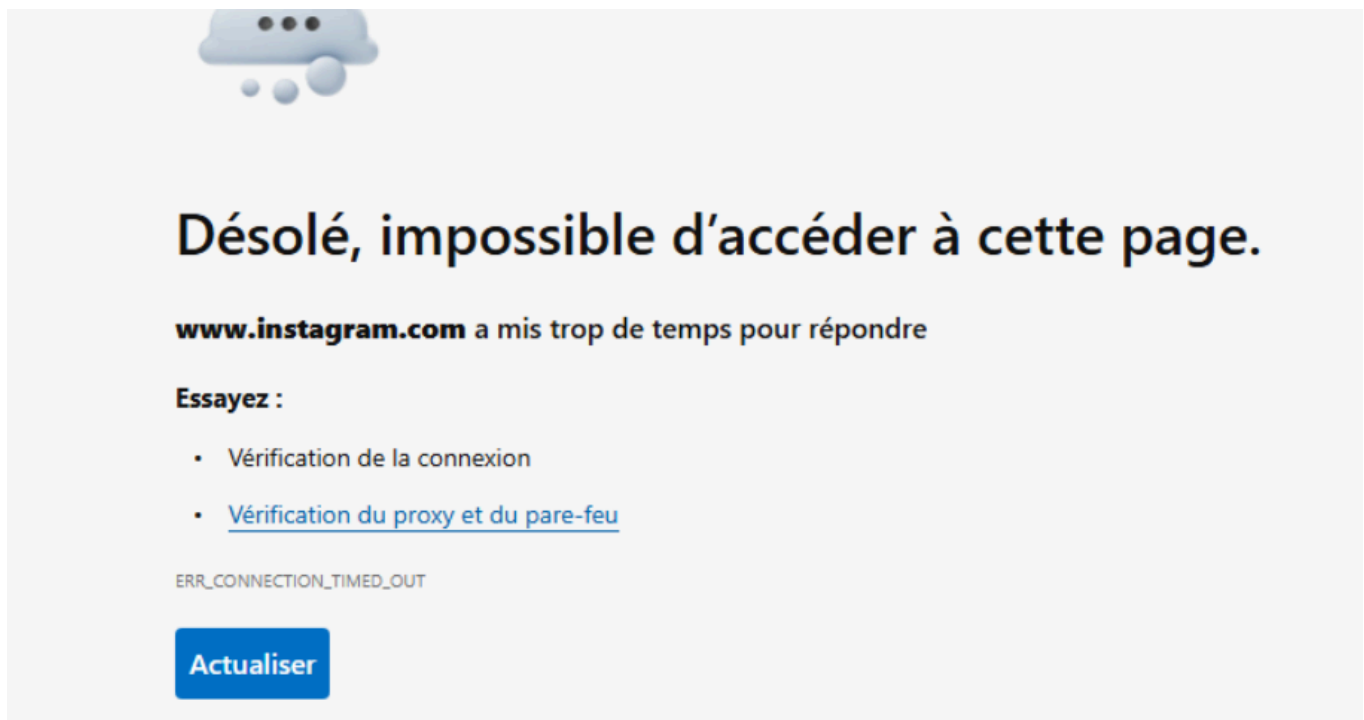


cliquer sur terminé



Test

Le test marche



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