OPNsense - Mise en place d'un Proxy Squid et Liste de Filtrage

Guide de Procédure Technique

Yassine Dinar

Objectif de la Procédure

Cette procédure détaille la mise en place complète d'un serveur proxy Squid sur OPNsense, incluant la configuration des certificats SSL pour l'inspection HTTPS et l'implémentation de listes de contrôle d'accès (ACL) pour le filtrage web.

L'environnement cible est une infrastructure virtualisée sous VMware Workstation, simulant un réseau d'entreprise avec séparation WAN/LAN et contrôle du trafic Internet des utilisateurs.

Principe : Un proxy agit comme intermédiaire entre les clients et Internet. En mode transparent avec inspection SSL, il intercepte automatiquement tout le trafic web, permettant le filtrage, la journalisation et le contrôle d'accès sans configuration côté client.

Prérequis Techniques

Élément	Description	Status Requis
VMware Workstation	Hyperviseur de virtualisation version 15 ou supérieure	Installé et fonctionnel
ISO OPNsense	Image au format DVD (et non VGA) téléchargée depuis opnsense.org	Téléchargé et décompressé (.bz2 vers .iso)
VM Windows 10/11	Machine cliente pour les tests et l'accès à l'interface web	Prête à configurer
Ressources matérielles	Minimum 2 Go RAM et 20 Go disque pour la VM OPNsense	Disponibles
Réseaux virtuels VMware	VMnet8 (NAT) pour le WAN et VMnet1 (Host-only) pour le LAN	Configurables dans Virtual Network Editor

Concepts Techniques Fondamentaux

Terme	Définition	Application dans la Procédure
Proxy Transparent	Proxy interceptant le trafic sans configuration client, via redirection NAT	Capture automatique du trafic HTTP/HTTPS sur les ports 80/443 vers Squid
Inspection SSL (MitM)	Technique de déchiffrement du trafic HTTPS pour analyse puis rechiffrement vers le client	Permet le filtrage du contenu des sites sécurisés grâce au certificat CA interne
ACL (Access Control List)	Liste définissant les règles d'autorisation ou de blocage d'accès	Filtrage par catégories (réseaux sociaux, streaming) via la blacklist de Toulouse
NAT (Network Address Translation)	Translation d'adresses permettant la redirection du trafic	Redirection des ports 80/443 vers les ports d'écoute du proxy (3128/3129)
Autorité de Certification (CA)	Entité émettant des certificats numériques de confiance	Création d'une CA interne pour signer les certificats d'interception SSL

Phase 1 : Préparation de l'environnement VMware

Étape 1.1 : Configuration des réseaux virtuels

1. Accès au Virtual Network Editor

- Lancer VMware Workstation avec les droits administrateur
- Accéder au menu "Edit" puis sélectionner "Virtual Network Editor"
- Cliquer sur "Change Settings" pour obtenir les privilèges de modification

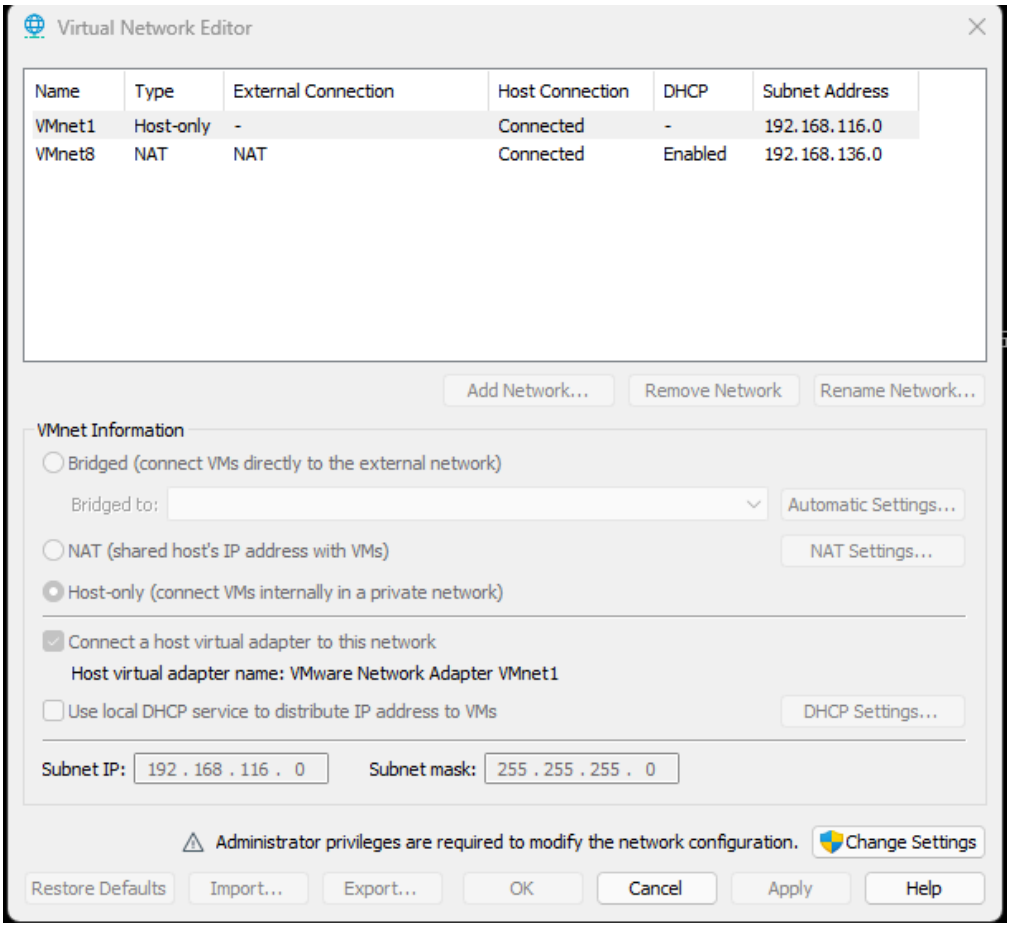
2. Configuration du réseau WAN (VMnet8 - NAT)

- Sélectionner la ligne VMnet8 dans la liste des réseaux
- Vérifier que le type est bien défini sur "NAT"
- S'assurer que l'option "Use local DHCP service" est cochée (VMware fournira une IP au WAN d'OPNsense)
- Noter la plage d'adresses (généralement 192.168.x.0/24)

3. Configuration du réseau LAN (VMnet1 - Host-only)

- Sélectionner la ligne VMnet1 dans la liste des réseaux
- Vérifier que le type est défini sur "Host-only"
- Décocher impérativement l'option "Use local DHCP service to distribute IP address to VMs"
- Cliquer sur "Apply" puis "OK" pour valider

Capture d'écran : Virtual Network Editor avec VMnet8 en NAT (DHCP activé) et VMnet1 en Host-only (DHCP désactivé)



Important : La désactivation du DHCP sur VMnet1 est cruciale. Si deux serveurs DHCP sont actifs sur le même réseau (VMware et OPNsense), des conflits d'adresses IP surviendront et les clients n'utiliseront pas OPNsense comme passerelle.

Étape 1.2 : Création de la machine virtuelle OPNsense

1. Lancement de l'assistant de création

- Dans VMware Workstation, cliquer sur "File" puis "New Virtual Machine"
- Sélectionner "Typical (recommended)" et cliquer sur "Next"
- Choisir "I will install the operating system later" pour éviter une détection automatique erronée

2. Sélection du système d'exploitation

- Guest Operating System : sélectionner "Other"
- Version : choisir "FreeBSD 13 64-bit" (OPNsense est basé sur FreeBSD)
- Nommer la machine virtuelle (exemple : "OPNsense-TP-Proxy")

3. Configuration du stockage

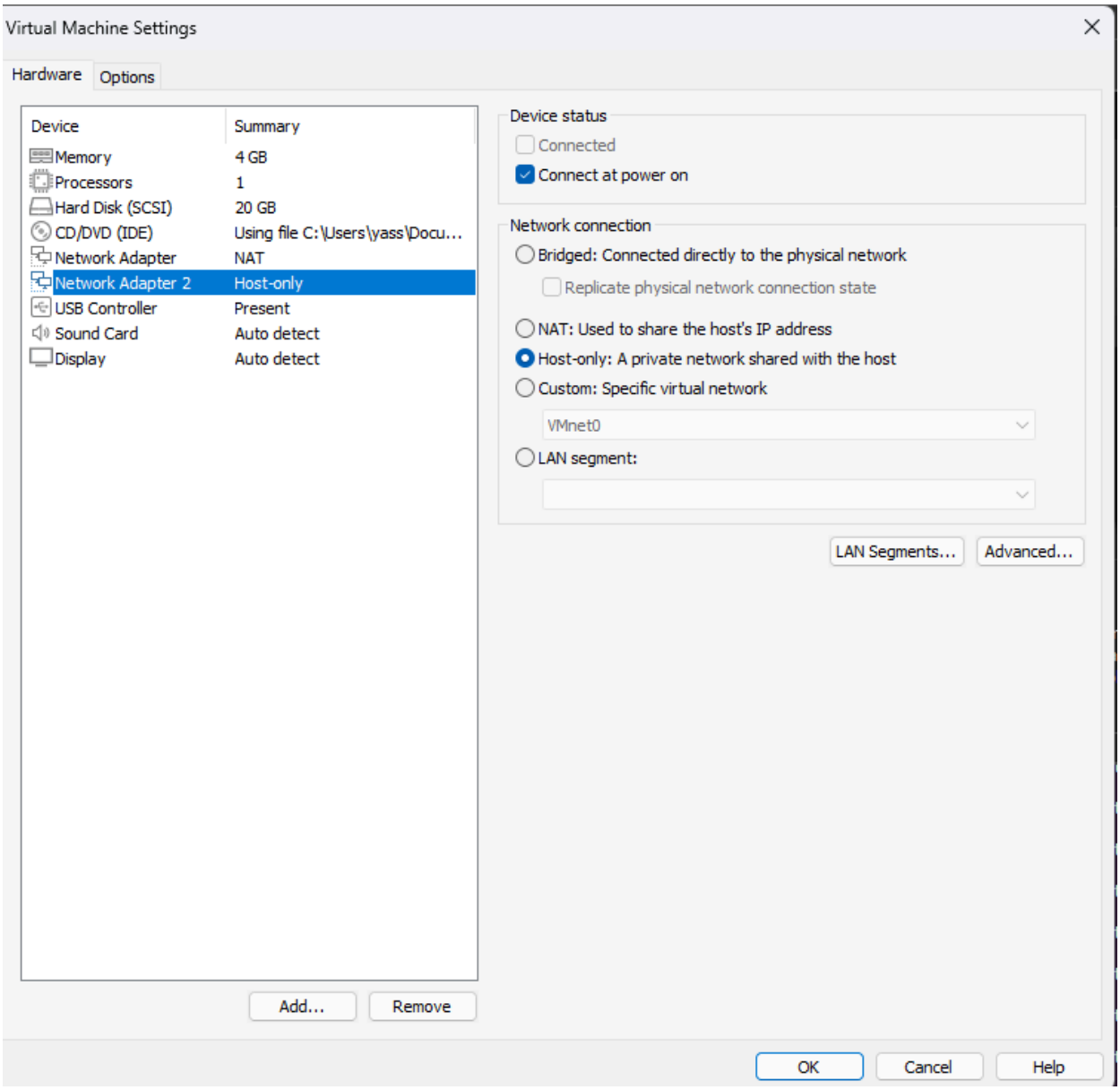
- Définir la taille du disque à 20 Go (suffisant pour OPNsense et les logs)
- Sélectionner "Store virtual disk as a single file"
- Terminer l'assistant

4. Ajout de la seconde carte réseau et insertion de l'ISO

- Faire un clic droit sur la VM créée puis "Settings"
- Sélectionner "CD/DVD (SATA)" et cocher "Use ISO image file"

- Parcourir et sélectionner le fichier ISO OPNsense décompressé
- Cocher impérativement "Connect at power on"
- Cliquer sur "Add" puis "Network Adapter" pour ajouter une seconde carte réseau
- Configurer Network Adapter 1 sur "Custom: VMnet8 (NAT)"
- Configurer Network Adapter 2 sur "Custom: VMnet1 (Host-only)"

Capture d'écran : Paramètres de la VM avec deux cartes réseau configurées (NAT et Host-only)



Phase 2 : Installation d'OPNsense

Étape 2.1 : Processus d'installation

1. Démarrage sur l'ISO

- Démarrer la machine virtuelle
- OPNsense démarre en mode live et affiche un écran de login
- Au prompt "login:", saisir : `installer`
- Au prompt "Password:", saisir : `opnsense`

2. Configuration du clavier et de l'installation

- Keymap Selection : sélectionner un clavier selon votre configuration
- Guided Installation : sélectionner "Install (ZFS)" pour un système de fichiers moderne
- ZFS Configuration : choisir "Stripe - No Redundancy" (un seul disque virtuel)
- Disk Selection : sélectionner le disque VMware avec la barre d'espace puis valider avec Entrée
- Confirmer l'effacement du disque en sélectionnant "YES"

3. Finalisation et redémarrage

- Attendre la fin de l'installation (copie des fichiers système)
- À l'invite de changement de mot de passe root, définir un mot de passe sécurisé
- Sélectionner "Complete Install" puis "Reboot"
- La VM redémarre sur le système installé

Important : Le sujet du TP précise explicitement d'installer OPNsense et de ne pas rester en mode live. Le mode live ne conserve aucune configuration après redémarrage.

Étape 2.2 : Assignation des interfaces réseau

1. Connexion à la console

- Au prompt de login, saisir : `root`
- Saisir le mot de passe défini lors de l'installation
- Le menu principal d'OPNsense s'affiche avec les options numérotées de 0 à 13

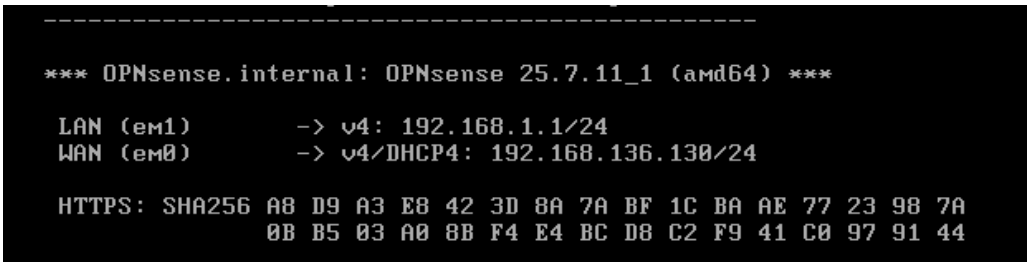
2. Assignation des interfaces (Option 1)

- Taper `1` et appuyer sur Entrée pour "Assign interfaces"
- À la question "Do you want to configure LAGGs now?" : taper `n`
- À la question "Do you want to configure VLANs now?" : taper `n`
- "Enter the WAN interface name" : taper `em0` (carte NAT)
- "Enter the LAN interface name" : taper `em1` (carte Host-only)
- "Enter the Optional interface" : appuyer sur Entrée (laisser vide)
- "Do you want to proceed?" : taper `y`

3. Configuration de l'adresse IP du LAN (Option 2)

- Taper `2` et appuyer sur Entrée pour "Set interface IP address"
- Sélectionner l'interface LAN (généralement option 2)
- "Configure IPv4 via DHCP?" : taper `n`
- "Enter the new LAN IPv4 address" : taper `192.168.1.1`
- "Enter the new LAN IPv4 subnet bit count" : taper `24`
- "Enter the IPv4 upstream gateway" : appuyer sur Entrée (pas de passerelle pour le LAN)
- "Configure IPv6?" : taper `n`
- "Do you want to enable the DHCP server on LAN?" : taper `y`
- "Enter the start address" : taper `192.168.1.100`
- "Enter the end address" : taper `192.168.1.200`

Capture d'écran : Console OPNsense affichant WAN (em0) avec IP DHCP et LAN (em1) en 192.168.1.1



Résultat attendu : L'écran doit afficher deux lignes : WAN (em0) avec une adresse IP fournie par VMware (ex: 192.168.136.x) et LAN (em1) avec l'adresse 192.168.1.1.

Phase 3 : Configuration initiale via l'interface web

Étape 3.1 : Accès à l'interface d'administration

1. Préparation de la machine cliente

- Sur la VM Windows cliente, configurer la carte réseau sur "Custom: VMnet1 (Host-only)"
- Démarrer la VM Windows
- Vérifier que Windows a obtenu une adresse IP automatiquement (ex: 192.168.1.100) via le DHCP d'OPNsense

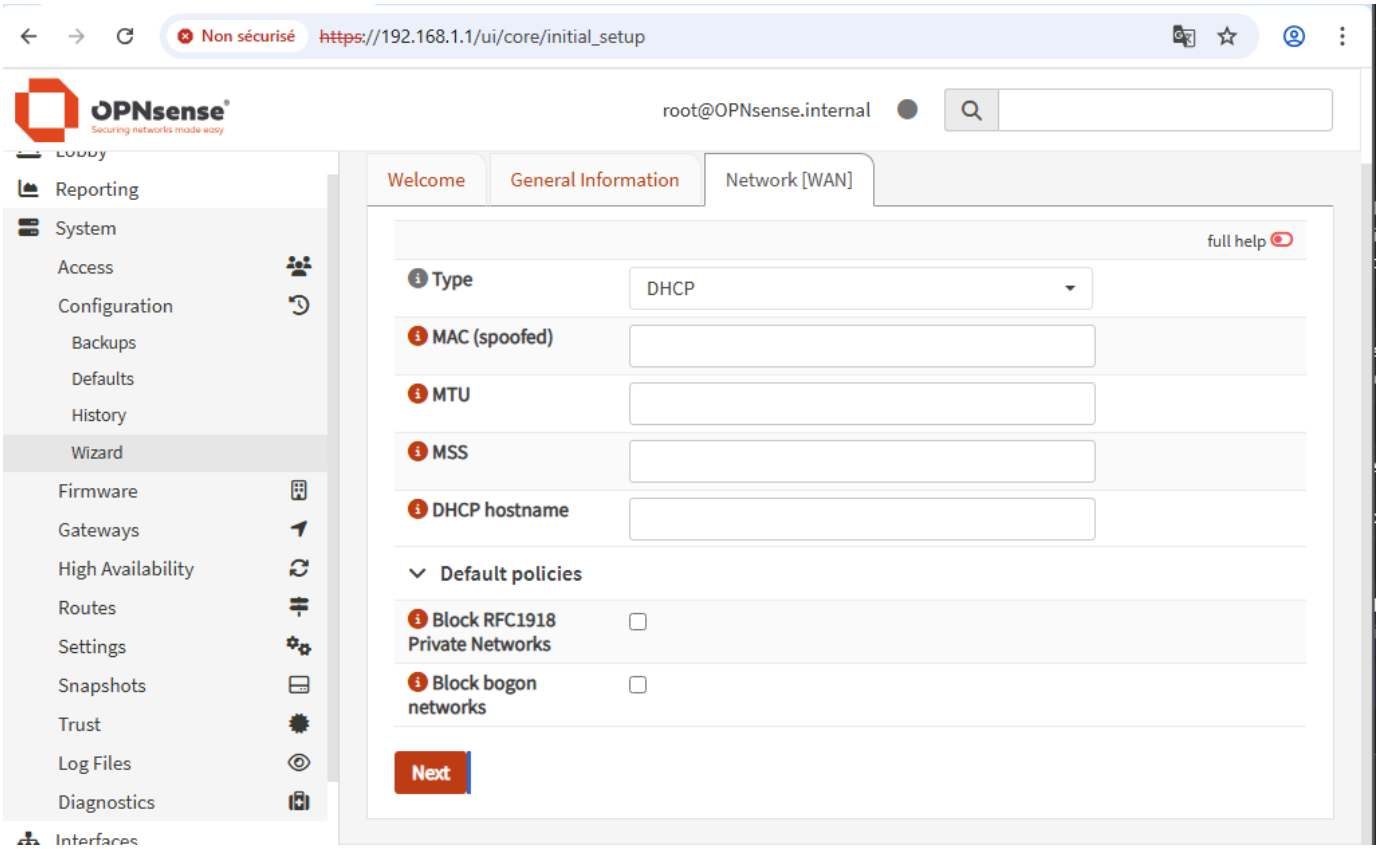
2. Connexion à l'interface web

- Ouvrir un navigateur web (Edge, Chrome ou Firefox)
- Accéder à l'adresse : `https://192.168.1.1`
- Un avertissement de sécurité apparaît (certificat auto-signé) : cliquer sur "Avancé" puis "Continuer vers le site"
- Saisir les identifiants : Utilisateur `root` et le mot de passe défini à l'installation

3. Assistant de configuration initiale (Wizard)

- L'assistant démarre automatiquement à la première connexion
- General Information : configurer le hostname et les serveurs DNS (exemple : 8.8.8.8)
- Time Server : conserver les paramètres par défaut
- Configure WAN Interface : laisser en DHCP
- Descendre en bas de la page WAN et décocher "Block private networks" et "Block bogon networks"
- Configure LAN Interface : vérifier que l'IP est bien 192.168.1.1
- Set Root Password : modifier ou conserver le mot de passe actuel
- Cliquer sur "Reload" pour appliquer la configuration

Capture d'écran : Page de configuration WAN avec les cases "Block private networks" et "Block bogon networks" décochées



Important : Le déblocage des réseaux privés sur le WAN est indispensable dans un environnement VMware. L'interface WAN reçoit une adresse IP privée (192.168.x.x) du NAT VMware. Si ces cases restent cochées, OPNsense bloquera sa propre connexion Internet.

Étape 3.2 : Mise à jour du système

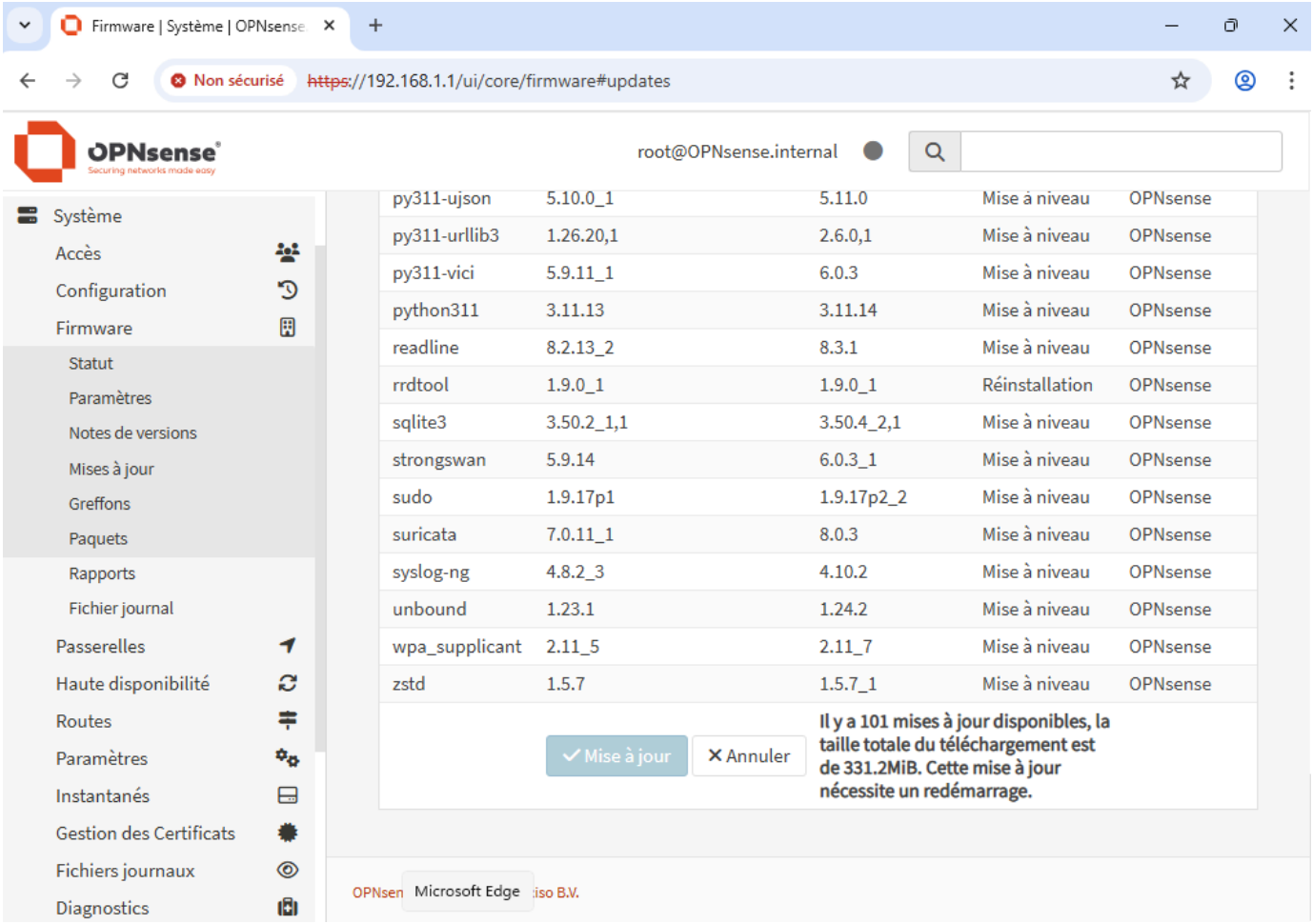
1. Accès au gestionnaire de mises à jour

- Dans le menu latéral, naviguer vers "System" puis "Firmware" puis "Status"
- Cliquer sur le bouton "Check for updates"
- Attendre que la vérification se termine

2. Application des mises à jour

- Si des mises à jour sont disponibles, une liste de paquets s'affiche
- Cliquer sur le bouton "Update" en bas de la page
- Confirmer le lancement de la mise à jour
- Le système télécharge et installe les paquets puis redémarre automatiquement
- Attendre le redémarrage complet et se reconnecter à l'interface web

Capture d'écran : Page Firmware Status avec liste des mises à jour disponibles



Important : Cette étape est essentielle pour garantir la compatibilité avec Squid et bénéficier des derniers correctifs de sécurité.

Phase 4 : Création et déploiement du certificat SSL

Étape 4.1 : Création de l'Autorité de Certification interne

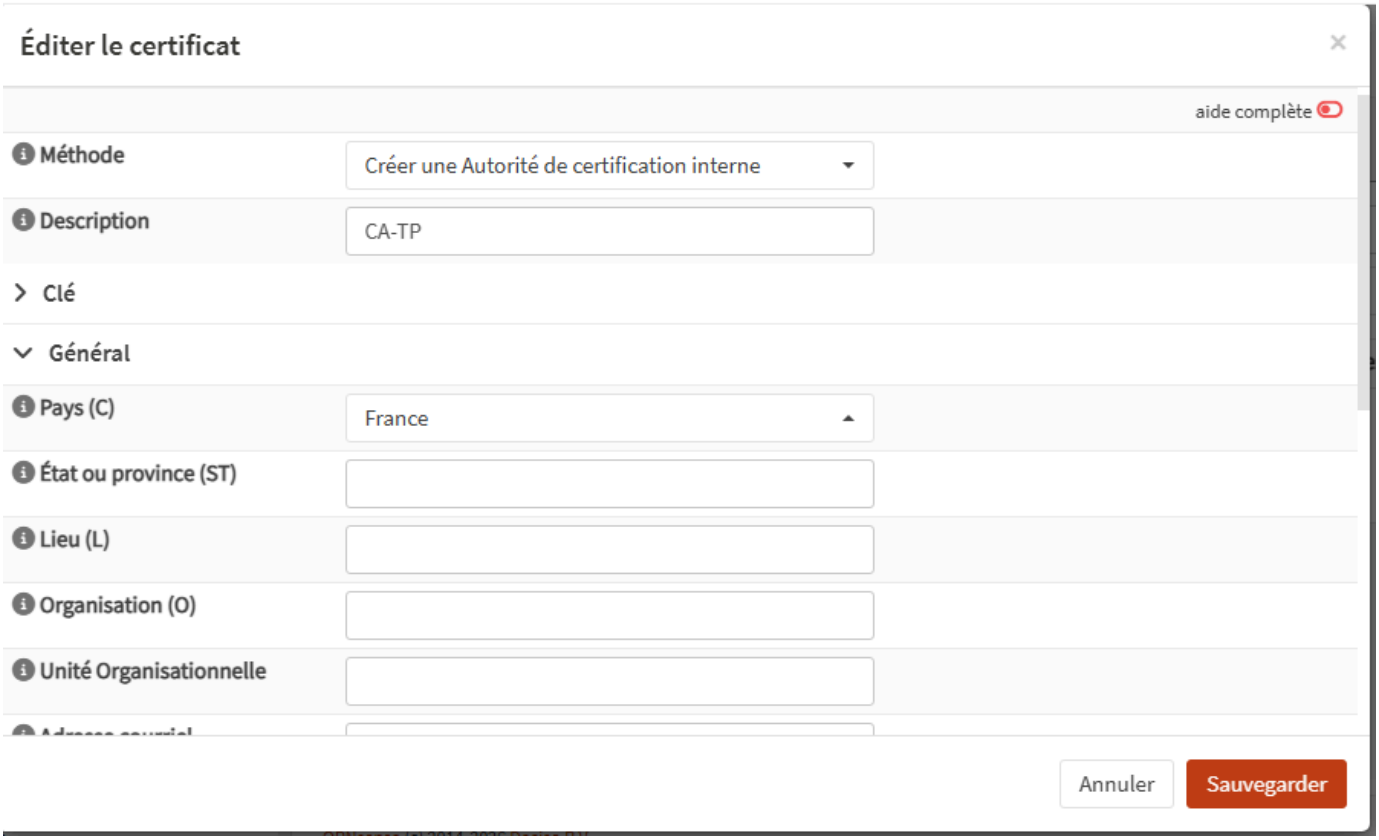
1. Accès à la gestion des certificats

- Dans le menu latéral, naviguer vers "System" puis "Trust" puis "Authorities"
- Cliquer sur le bouton "+" pour ajouter une nouvelle autorité

2. Configuration de l'autorité de certification

- Descriptive name : saisir un nom explicite (exemple : "CA-TP-Proxy")
- Method : sélectionner "Create an internal Certificate Authority"
- Key Type : conserver "RSA" avec une longueur de 2048 ou 4096 bits
- Digest Algorithm : conserver "SHA256"
- Common Name : saisir un nom identifiant (exemple : "opnsense-ca-interne")
- Les champs Country, State, City, Organization sont optionnels mais recommandés
- Cliquer sur "Save" pour créer l'autorité

Capture d'écran : Formulaire de création de l'autorité de certification avec les champs remplis



Résultat attendu : L'autorité de certification apparaît dans la liste avec son nom et sa date de validité.

Étape 4.2 : Installation du certificat sur le poste client Windows

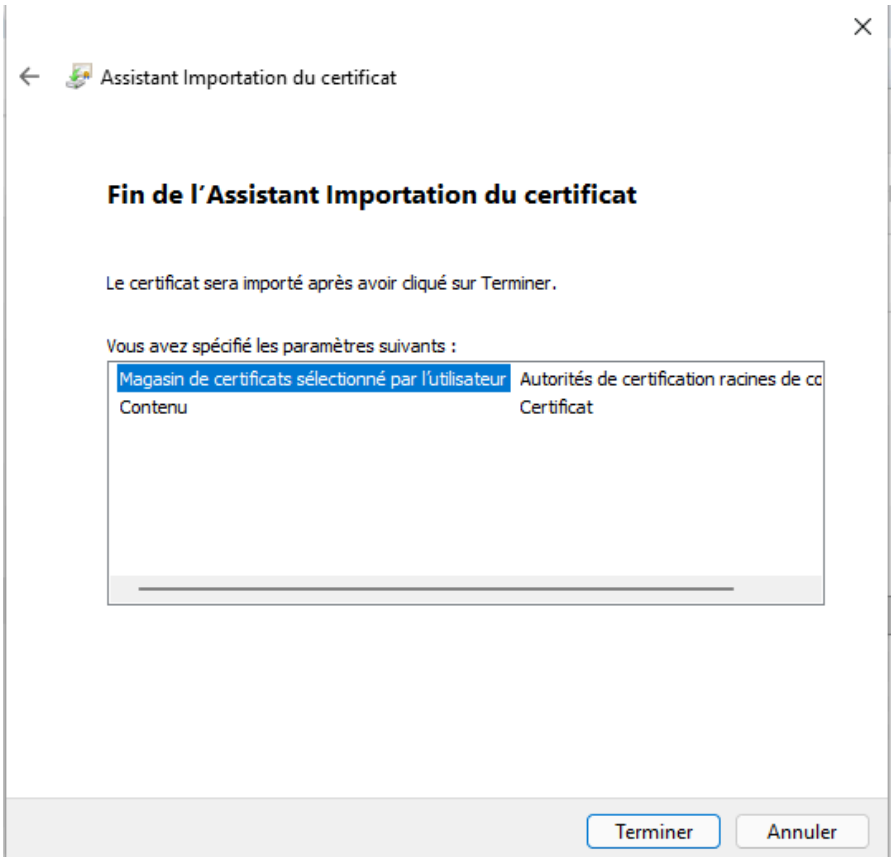
1. Export du certificat depuis OPNsense

- Dans la liste des autorités, repérer la ligne du certificat créé
- Cliquer sur l'icône d'export (nuage avec flèche vers le bas) intitulée "Export CA certificate"
- Le fichier .crt ou .pem est téléchargé sur la machine cliente

2. Installation dans le magasin de certificats Windows

- Si le fichier est au format .pem, le renommer avec l'extension .crt
- Ouvrir le gestionnaire de certificats : taper `certlm.msc` dans la barre de recherche Windows et exécuter en tant qu'administrateur
- Développer "Trusted Root Certification Authorities" (Autorités de certification racines de confiance)
- Faire un clic droit sur "Certificates" puis "All Tasks" puis "Import"
- L'assistant d'importation s'ouvre : cliquer sur "Next"
- Cliquer sur "Browse" et sélectionner le fichier certificat (changer le filtre sur "All Files" si nécessaire)
- Cliquer sur "Next", s'assurer que le magasin de destination est bien "Trusted Root Certification Authorities"
- Cliquer sur "Finish"
- Un message confirme l'importation réussie

Capture d'écran : Gestionnaire de certificats Windows avec le certificat CA-TP-Proxy importé dans les autorités racines de confiance



Important : Sans cette installation, les navigateurs afficheront des erreurs de sécurité à chaque connexion HTTPS car ils ne reconnaîtront pas l'autorité de certification d'OPNsense.

Phase 5 : Installation et configuration de Squid

Étape 5.1 : Installation du plugin Squid

1. Accès au gestionnaire de plugins

- Dans le menu latéral, naviguer vers "System" puis "Firmware" puis "Plugins"
- Cocher la case "Show Community plugins"
- Utiliser la barre de recherche pour filtrer avec le terme "squid"

2. Installation du plugin

- Repérer le paquet "os-squid" dans la liste des résultats
- Cliquer sur le bouton "+" à droite de la ligne pour lancer l'installation
- Attendre la fin de l'installation (environ 1 à 2 minutes)
- Actualiser la page avec F5 pour voir apparaître le nouveau menu

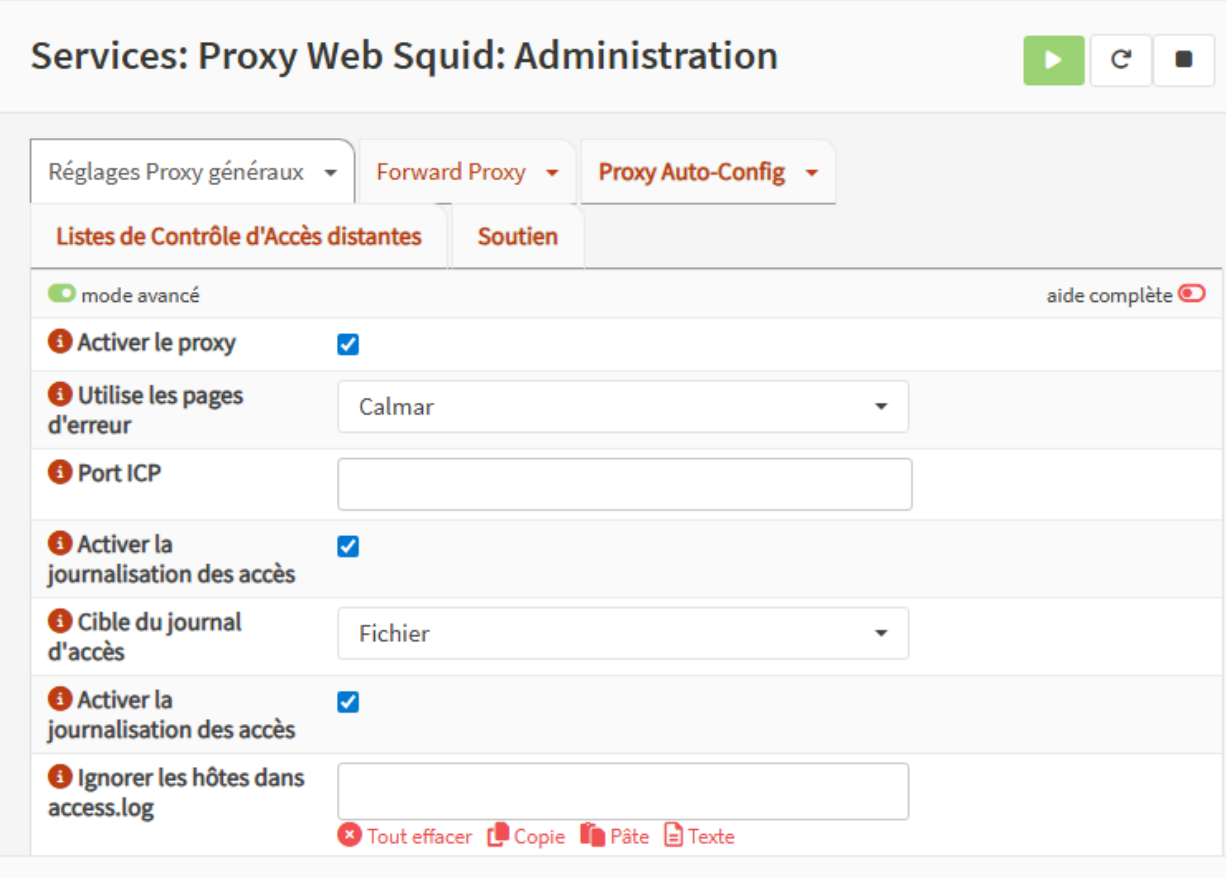
Étape 5.2 : Configuration du proxy manuel

1. Activation du service Squid

- Dans le menu latéral, naviguer vers "Services" puis "Web Proxy" puis "Administration"
- Dans l'onglet "General Proxy Settings" :
- Cocher "Enable proxy"
- Cocher "Enable access logging" (utile pour les tests et le diagnostic)

- Cocher "Enable local cache"
- Cliquer sur "Apply" pour sauvegarder

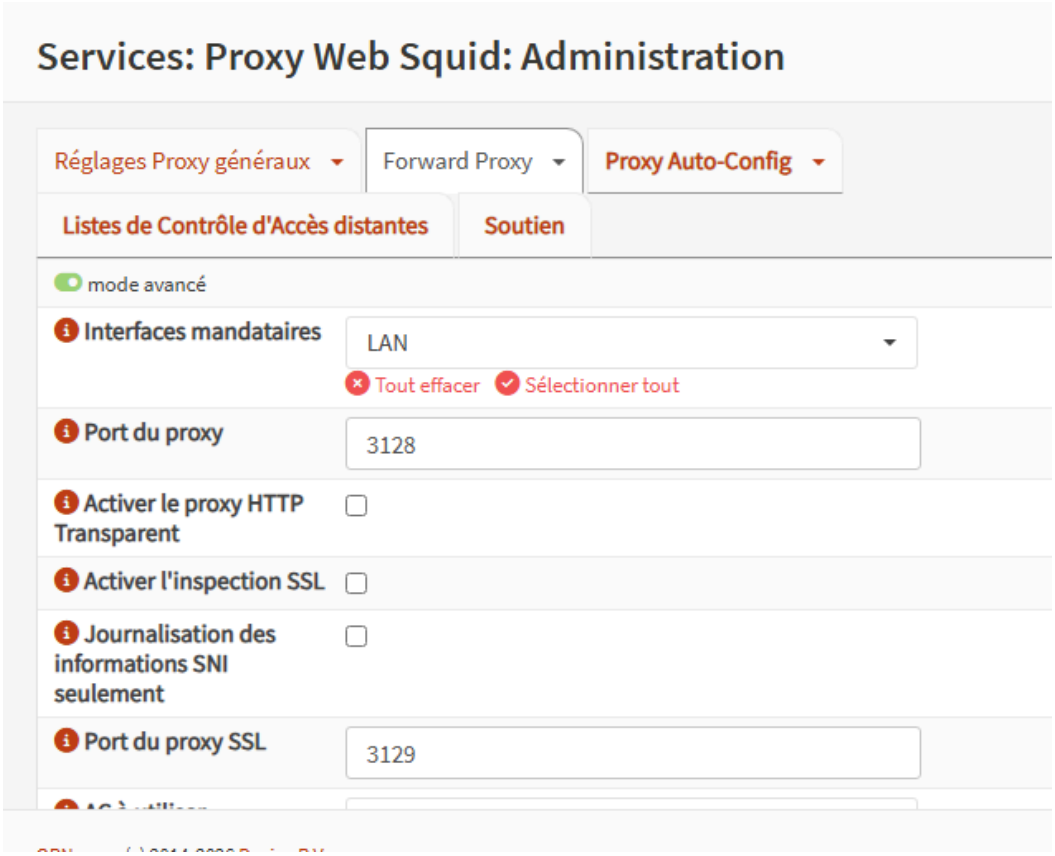
Capture d'écran : Page Administration du proxy avec les options Enable proxy, Enable access logging et Enable local cache cochées



2. Configuration de l'onglet Forward Proxy

- Cliquer sur l'onglet "Forward Proxy"
- Dans le champ "Proxy interfaces" : sélectionner "LAN"
- Vérifier que "Proxy port" est défini sur 3128
- Laisser "Transparent HTTP proxy" décoché pour l'instant (mode manuel d'abord)
- Cliquer sur "Apply" pour sauvegarder

Capture d'écran : Configuration Forward Proxy avec interface LAN sélectionnée et port 3128



Étape 5.3 : Création des règles de pare-feu pour le proxy manuel

1. Accès aux règles du pare-feu LAN

- Dans le menu latéral, naviguer vers "Firewall" puis "Rules" puis "LAN"
- Les règles par défaut autorisent tout le trafic sortant

2. Création de la règle d'autorisation du port proxy

- Cliquer sur "+" pour ajouter une nouvelle règle
- Action : sélectionner "Pass"
- Interface : LAN
- Protocol : TCP
- Source : sélectionner "LAN net"
- Destination : sélectionner "LAN address" ou "Any"
- Destination port range : saisir "3128" dans les champs "from" et "to" (sélectionner "other" si nécessaire)
- Description : saisir "Autoriser acces Proxy"
- Cliquer sur "Save"

3. Création des règles de blocage de l'accès direct

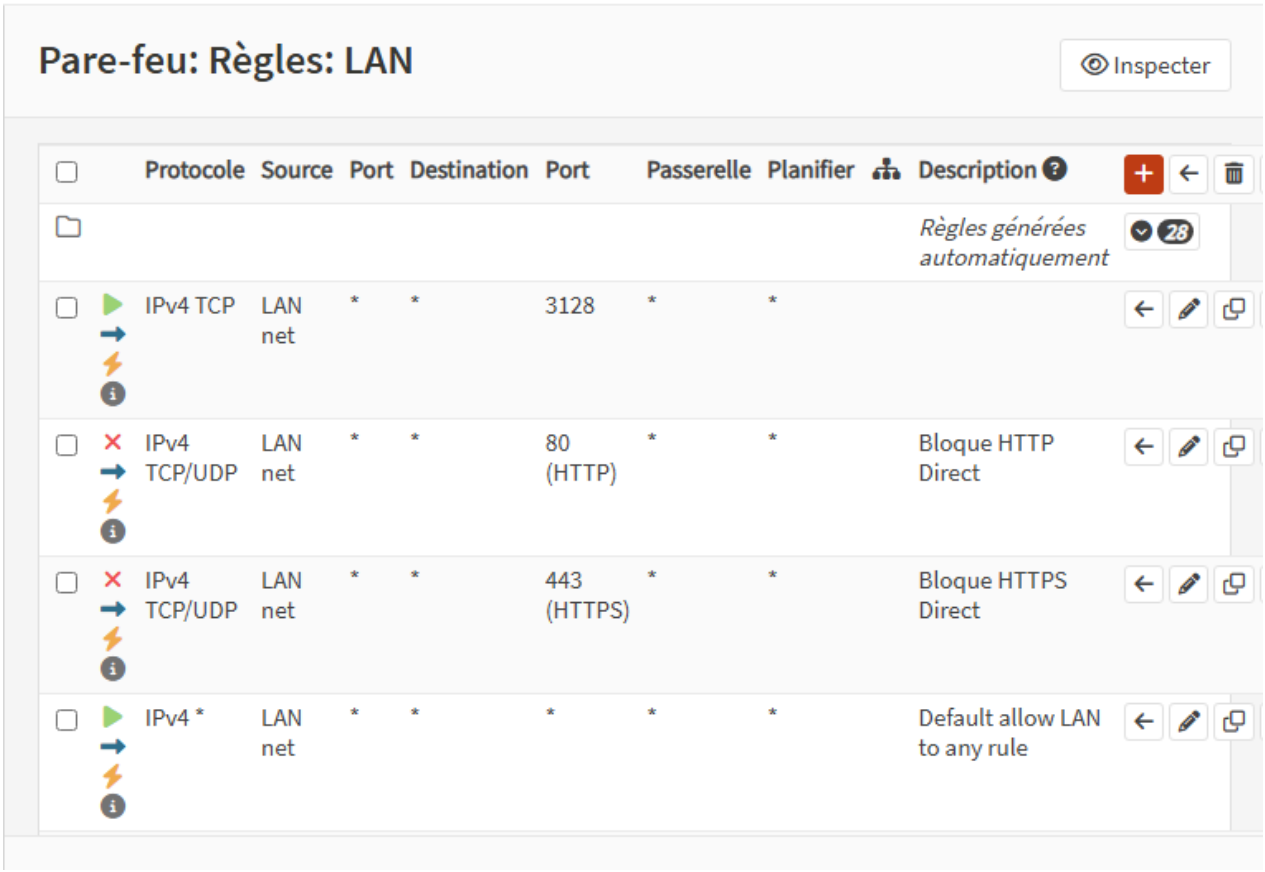
- Cliquer sur "+" pour ajouter une nouvelle règle
- Action : sélectionner "Block"
- Interface : LAN
- Protocol : TCP/UDP
- Source : sélectionner "LAN net"

- Destination port range : sélectionner "HTTP" (port 80)
- Description : saisir "Bloquer HTTP direct"
- Cliquer sur "Save"
- Répéter l'opération pour le HTTPS :
- Action : Block
- Protocol : TCP/UDP
- Source : LAN net
- Destination port range : sélectionner "HTTPS" (port 443)
- Description : saisir "Bloquer HTTPS direct"
- Cliquer sur "Save"

4. Ordonnancement des règles

- L'ordre des règles est crucial : les règles sont évaluées de haut en bas
- Utiliser les flèches ou le glisser-déposer pour positionner les règles dans cet ordre :
  i. Autoriser acces Proxy (Pass, port 3128) - en premier
  ii. Bloquer HTTP direct (Block, port 80)
  iii. Bloquer HTTPS direct (Block, port 443)
  iv. Default allow LAN to any rule - en dernier
- Cliquer sur "Apply Changes" pour activer les règles

Capture d'écran : Liste des règles pare-feu LAN avec l'ordre correct (autorisation 3128 en haut, puis blocages 80 et 443)



Important : Si la règle d'autorisation du port 3128 n'est pas placée avant les règles de blocage, le proxy sera inaccessible et les clients n'auront plus aucun accès Internet.

Étape 5.4 : Configuration du proxy sur le client Windows

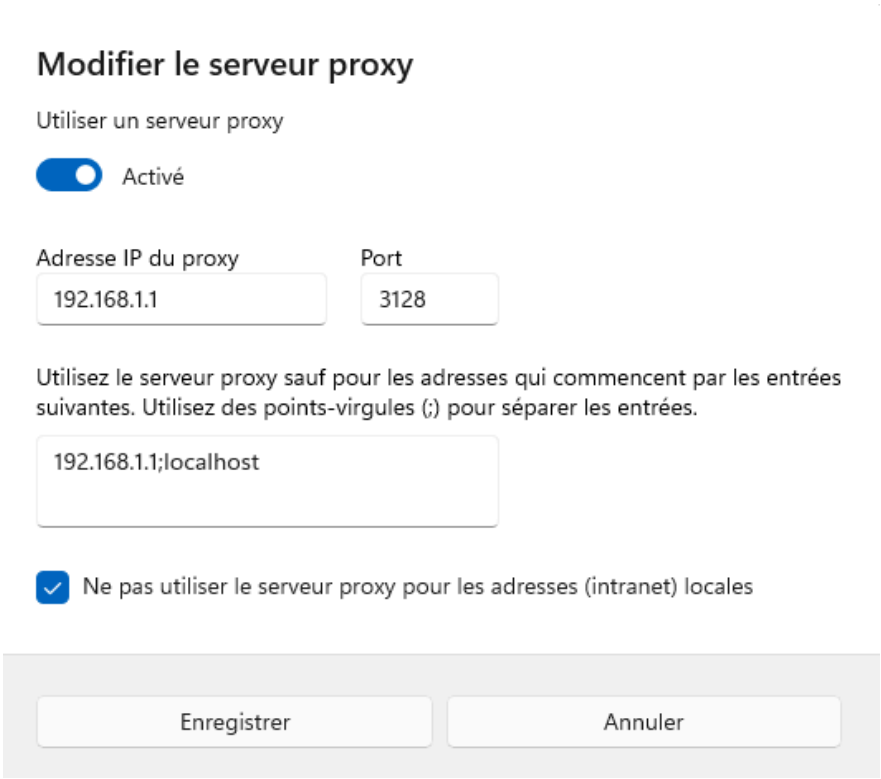
1. Accès aux paramètres proxy de Windows

- Sur le poste client Windows, ouvrir les Paramètres (Windows + I)
- Naviguer vers "Network & Internet" puis "Proxy"
- Dans la section "Manual proxy setup", cliquer sur "Set up"

2. Configuration des paramètres

- Activer "Use a proxy server"
- Address : saisir `192.168.1.1`
- Port : saisir `3128`
- Dans le champ des exceptions, ajouter : `192.168.1.1;localhost`
- Cocher "Don't use the proxy server for local (intranet) addresses"
- Cliquer sur "Save"

Capture d'écran : Paramètres proxy Windows avec adresse 192.168.1.1 et port 3128 configurés



3. Test de fonctionnement

- Ouvrir un navigateur et accéder à un site web (exemple : wikipedia.org)
- La navigation doit fonctionner normalement
- Pour vérifier le passage par le proxy : dans OPNsense, aller dans "Services" puis "Web Proxy" puis "Log File" puis "Access Log"
- Les connexions du client doivent apparaître dans les journaux

Phase 6 : Configuration du proxy transparent

Étape 6.1 : Activation du mode transparent et de l'inspection SSL

1. Configuration du proxy transparent

- Retourner dans "Services" puis "Web Proxy" puis "Administration"
- Cliquer sur l'onglet "Forward Proxy"
- Cocher "Enable Transparent HTTP proxy"
- Cocher "Enable SSL inspection"
- Dans le champ "CA to use" qui apparaît, sélectionner le certificat créé précédemment (CA-TP-Proxy)
- Cliquer sur "Apply"

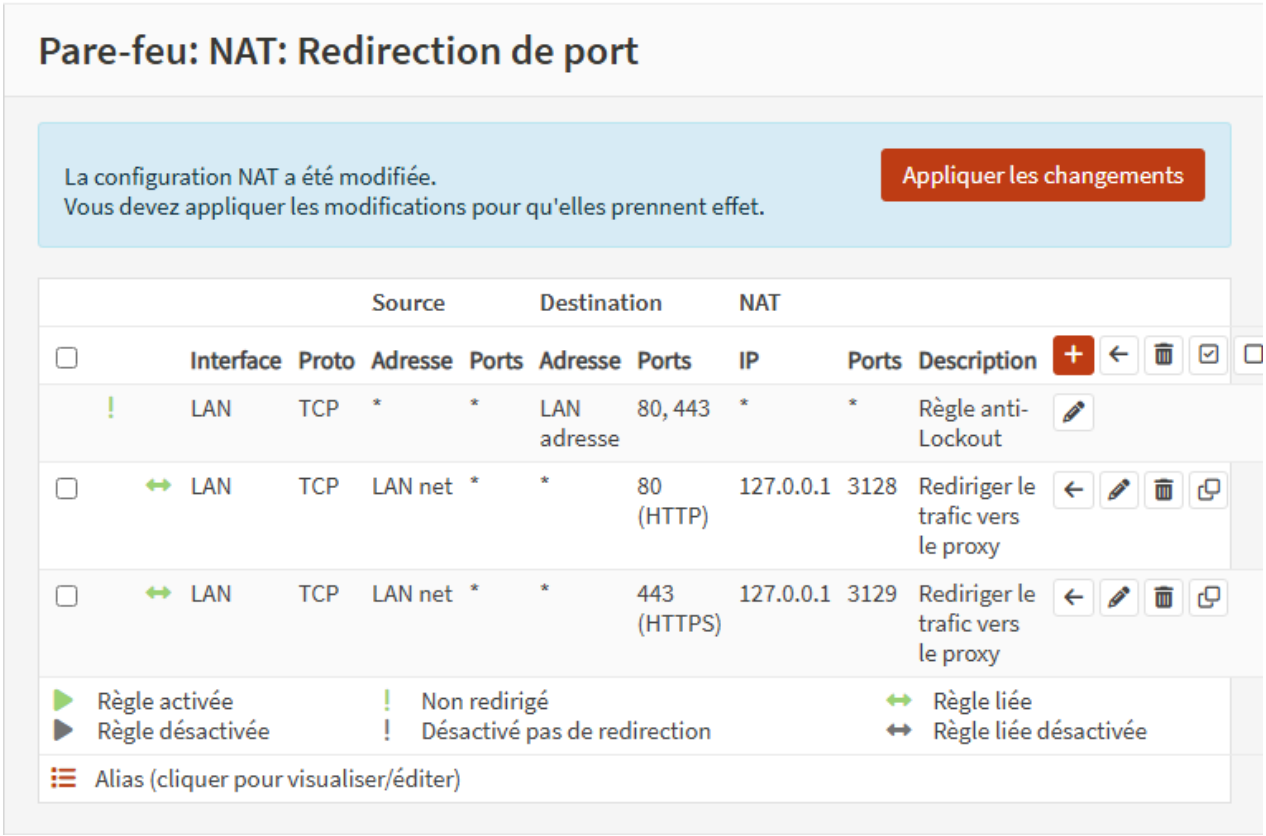
2. Création automatique des règles NAT

- À côté de l'option "Enable Transparent HTTP proxy", cliquer sur l'icône "i" (information)
- Un lien "Add a new firewall rule" apparaît : cliquer dessus
- La page de création de règle NAT s'ouvre avec les paramètres pré-remplis
- Descendre en bas de la page et cliquer sur "Save" sans modification
- Retourner dans l'onglet "Forward Proxy"
- À côté de l'option "Enable SSL inspection", cliquer sur l'icône "i"
- Cliquer sur "Add a new firewall rule"
- Sauvegarder la règle sans modification

3. Application des règles NAT

- Naviguer vers "Firewall" puis "NAT" puis "Port Forward"
- Deux règles de redirection doivent apparaître (HTTP vers 3128 et HTTPS vers 3129)
- Cliquer sur "Apply Changes" pour activer les redirections

Capture d'écran : Page NAT Port Forward avec les deux règles de redirection HTTP (80 vers 3128) et HTTPS (443 vers 3129)



Important : L'oubli de cliquer sur "Apply Changes" dans la page NAT est une erreur fréquente. Les règles créées par l'assistant restent en attente jusqu'à cette validation.

Étape 6.2 : Désactivation du proxy manuel sur le client

1. Suppression de la configuration proxy Windows

- Sur le poste client Windows, retourner dans Paramètres puis "Network & Internet" puis "Proxy"
- Désactiver "Use a proxy server"
- Cliquer sur "Save"

2. Réinitialisation des états du pare-feu

- Dans OPNsense, naviguer vers "Firewall" puis "Diagnostics" puis "States"
- Cliquer sur l'onglet "Reset States"
- Cocher la case de réinitialisation et confirmer
- Fermer et rouvrir le navigateur sur le client

3. Vérification du fonctionnement transparent

- Sans aucune configuration proxy sur Windows, ouvrir le navigateur
- Accéder à un site web (exemple : google.fr)
- La navigation doit fonctionner automatiquement grâce à l'interception transparente

Phase 7 : Configuration du filtrage par liste noire (ACL)

Étape 7.1 : Ajout de la liste de filtrage de l'Université de Toulouse

1. Accès aux listes de contrôle d'accès distantes

- Dans le menu latéral, naviguer vers "Services" puis "Web Proxy" puis "Administration"
- Cliquer sur l'onglet "Remote Access Control Lists"
- Cliquer sur "+" pour ajouter une nouvelle liste

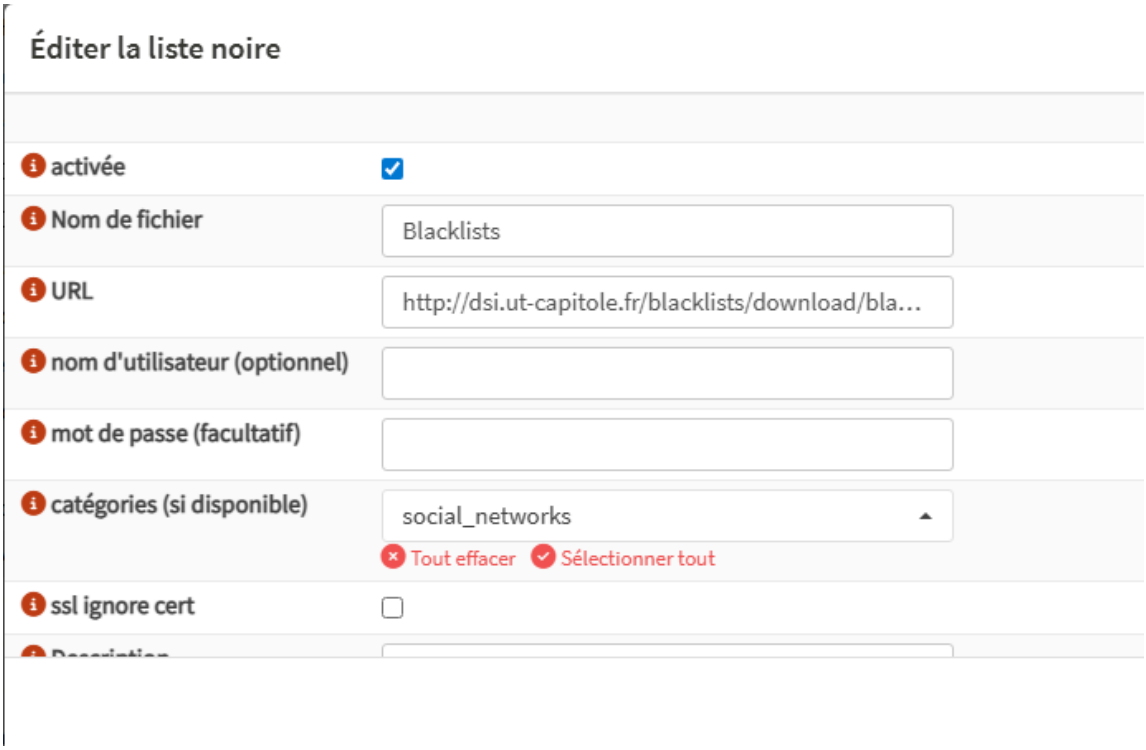
2. Configuration de la liste

- Enabled : cocher la case pour activer
- Filename : saisir "Toulouse" ou "Blacklist"
- URL : saisir `http://dsi.ut-capitole.fr/blacklists/download/blacklists.tar.gz`
- Description : saisir "Liste de filtrage Universite de Toulouse"
- Cliquer sur "Save"

3. Téléchargement et sélection des catégories

- Cliquer sur le bouton "Download ACLs and Apply" en bas de la page
- Attendre le téléchargement complet (peut prendre plusieurs minutes selon la connexion)
- Une fois terminé, cliquer sur l'icône "crayon" pour modifier la liste
- Dans le champ "Categories", sélectionner "social_networks"
- Cliquer sur "Save"
- Cliquer à nouveau sur "Download ACLs and Apply" pour activer le filtrage

Capture d'écran : Configuration de l'ACL avec URL de la blacklist Toulouse et catégorie social_networks sélectionnée



Important : À chaque modification des catégories sélectionnées, il est nécessaire de re-télécharger et appliquer les ACLs pour que les changements prennent effet.

Phase 8 : Tests et Validation

Étape 8.1 : Préparation des tests

1. Réinitialisation complète des connexions

- Dans OPNsense, naviguer vers "Firewall" puis "Diagnostics" puis "States"
- Cliquer sur "Reset States" et confirmer
- Sur le client Windows, fermer complètement le navigateur
- Vider le cache du navigateur ou ouvrir une fenêtre de navigation privée

2. Vérification de l'état des services

- Dans OPNsense, vérifier que le service Squid est actif (icône verte dans le dashboard)
- Vérifier que les règles NAT sont bien appliquées

Étape 8.2 : Validation du filtrage

1. Test d'accès aux sites bloqués

- Sur le poste client Windows, ouvrir le navigateur
- Tenter d'accéder à facebook.com
- Tenter d'accéder à instagram.com
- Tenter d'accéder à twitter.com (x.com)

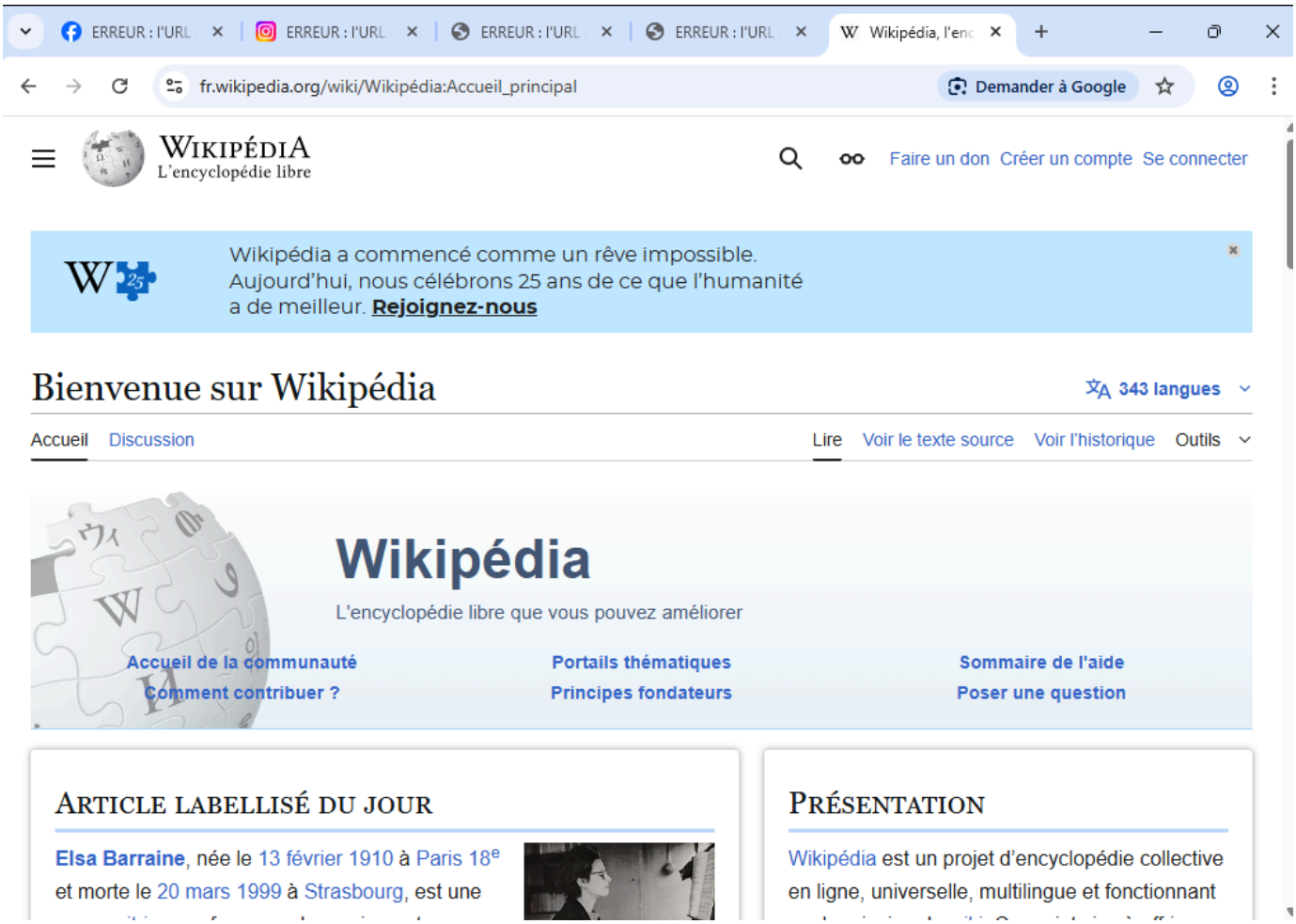
Résultat attendu : Une erreur de connexion ou une page de blocage s'affiche pour chaque tentative.

2. Test d'accès aux sites autorisés

- Accéder à wikipedia.org
- Accéder à google.fr
- Accéder à un site d'actualités quelconque

Résultat attendu : Les sites s'affichent normalement sans erreur.

Capture d'écran : Navigateur montrant Wikipedia accessible et Facebook/Instagram en erreur (onglets multiples)

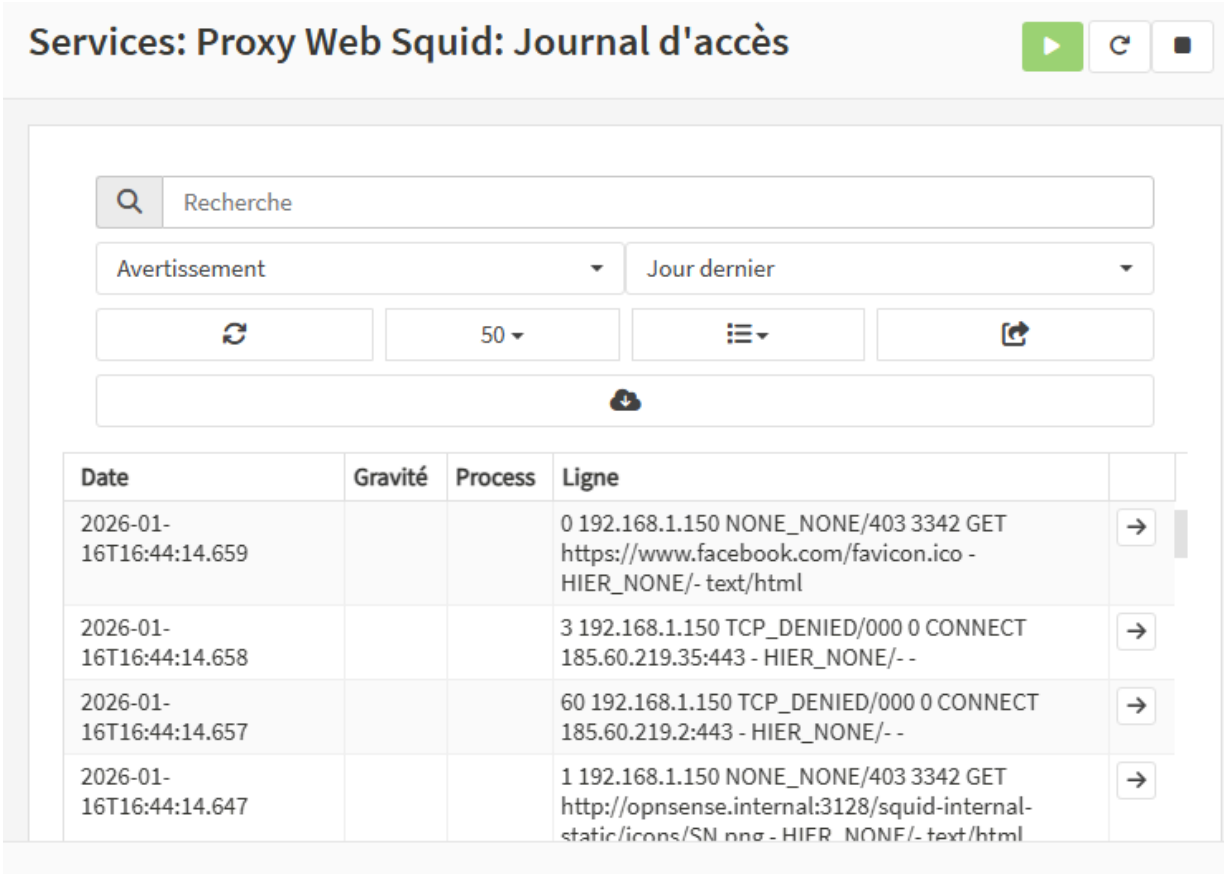


Étape 8.3 : Vérification des journaux

1. Consultation des logs d'accès

- Dans OPNsense, naviguer vers "Services" puis "Web Proxy" puis "Log File"
- Sélectionner "Access Log"
- Cliquer sur le bouton de rafraîchissement
- Les connexions autorisées et bloquées doivent apparaître avec leurs timestamps

Capture d'écran : Journal d'accès Squid montrant les connexions et les blocages



Résultat attendu : Les lignes de log affichent les requêtes avec les codes de statut (TCP_DENIED pour les blocages, TCP_TUNNEL pour les connexions HTTPS autorisées).

Diagnostic et Résolution de Problèmes

Problèmes Courants

Problème	Cause Probable	Solution Recommandée
VM ne démarre pas sur l'ISO	Mauvais type d'image (VGA au lieu de DVD)	Télécharger l'image DVD depuis opnsense.org
"Operating System not found" au boot	ISO non connecté ou mauvais chemin	Vérifier "Connect at power on" dans les paramètres CD/DVD
Une seule interface détectée (em0)	Seconde carte réseau non ajoutée	Ajouter Network Adapter 2 dans les paramètres VM
Pas d'accès Internet sur OPNsense	"Block private networks" coché sur le WAN	Décocher cette option dans la configuration WAN
Client n'obtient pas d'IP	DHCP VMware actif sur VMnet1	Désactiver le DHCP VMware sur le réseau Host-only
Proxy manuel ne fonctionne pas	Service Squid non activé	Vérifier que "Enable proxy" est coché
Erreur certificat sur sites HTTPS	Certificat CA non installé sur le client	Importer le certificat dans les autorités racines de confiance
Filtrage ne s'applique pas	ACLs non téléchargées après modification	Cliquer sur "Download ACLs and Apply"
Sites bloqués toujours accessibles	États du pare-feu non réinitialisés	Reset States dans Firewall Diagnostics puis redémarrer le navigateur
Proxy transparent ne fonctionne pas	Règles NAT non appliquées	Vérifier et cliquer sur "Apply Changes" dans NAT Port Forward

Commandes de Diagnostic

```
# Test de connectivité depuis OPNsense (via l'option 7 du menu console)
ping 8.8.8.8

# Test de résolution DNS
ping google.com

# Vérification du statut du service Squid (via SSH ou console)
service squid status

# Consultation des logs Squid en temps réel
tail -f /var/log/squid/access.log
```

Résultats et Bénéfices

La mise en place du proxy Squid sur OPNsense apporte :

Bénéfices organisationnels :

- **Contrôle du trafic web** : Visibilité complète sur les sites visités par les utilisateurs grâce à la journalisation
- **Sécurité renforcée** : Inspection du trafic HTTPS permettant de détecter les menaces dans le contenu chiffré
- **Politique d'accès** : Application de règles de filtrage par catégories pour bloquer les sites non productifs ou dangereux
- **Économie de bande passante** : Le cache local réduit le trafic Internet pour les contenus fréquemment consultés

Évolutivité assurée :

- Possibilité d'ajouter des catégories de filtrage supplémentaires (adult, gambling, malware, etc.)
- Intégration possible avec l'authentification Active Directory pour des règles par utilisateur
- Extension vers un cluster haute disponibilité pour les environnements critiques

Recommandations d'Extension

1. **Authentification utilisateur** : Configurer l'intégration LDAP/Active Directory pour identifier les utilisateurs et appliquer des politiques personnalisées
2. **Rapports et statistiques** : Installer le plugin LightSquid pour générer des rapports graphiques d'utilisation
3. **Filtrage antivirus** : Activer ClamAV avec Squid pour scanner le contenu téléchargé
4. **Liste blanche** : Créer des exceptions pour les sites métier légitimes qui pourraient être bloqués par erreur

Note d'évolution : Pour un déploiement en production, envisager la mise en place d'un certificat SSL signé par une autorité reconnue pour l'interface web d'administration, ainsi qu'une politique de sauvegarde automatique de la configuration OPNsense.

Questions et Réponses du TP

Question 1 : Pourquoi est-il préférable d'utiliser OPNsense en mode installé plutôt qu'en live ?

Le mode live charge le système entièrement en mémoire RAM sans l'écrire sur le disque dur. Toutes les configurations effectuées (interfaces réseau, règles de pare-feu, certificats, configuration du proxy) sont perdues au redémarrage. Le mode installé permet la persistance des données, la sauvegarde des configurations, l'application des mises à jour système et le fonctionnement normal des services qui nécessitent un stockage permanent comme les journaux Squid.

Question 2 : Pourquoi avoir besoin de deux interfaces réseau ?

Un pare-feu/routeur nécessite au minimum deux interfaces pour séparer les zones de sécurité. L'interface WAN (Wide Area Network) se connecte au réseau externe non fiable (Internet ou réseau de l'entreprise dans notre cas VMware NAT). L'interface LAN (Local Area Network) se connecte au réseau interne à protéger (les postes clients). Cette séparation permet au pare-feu de contrôler, filtrer et journaliser tout le trafic passant d'une zone à l'autre.

Question 3 : Quels sont les avantages d'utiliser une configuration DHCP sur l'interface LAN ?

Le protocole DHCP (Dynamic Host Configuration Protocol) automatise l'attribution des paramètres réseau aux clients : adresse IP, masque de sous-réseau, passerelle par défaut et serveurs DNS. Les avantages sont : simplification de l'administration réseau (pas de configuration manuelle sur chaque poste), élimination des erreurs de saisie et des conflits d'adresses IP, gestion centralisée des paramètres, possibilité de modifier facilement la configuration de tous les clients depuis un point unique.

Question 4 : Peut-on mettre à jour OPNsense sans l'interface graphique ?

Oui, OPNsense peut être mis à jour via la console texte en utilisant l'option 12 du menu principal ou en exécutant la commande `opnsense-update` en ligne de commande via SSH. Cependant, l'interface graphique offre une vue plus détaillée des paquets à mettre à jour, affiche les notes de version, permet de voir la progression du téléchargement et facilite le diagnostic en cas d'erreur.

Question 5 : Pourquoi est-il nécessaire de créer un certificat sur OPNsense pour l'inspection du trafic HTTPS ?

L'inspection HTTPS (aussi appelée SSL/TLS interception ou Man-in-the-Middle légitime) nécessite que le proxy déchiffre le trafic pour l'analyser, puis le rechiffre avant de l'envoyer au client. Pour ce faire, le proxy doit présenter un certificat au client pour chaque site visité. Sans une autorité de certification de confiance, les navigateurs afficheraient des erreurs de sécurité car ils ne pourraient pas vérifier l'authenticité des certificats présentés par le proxy.

Question 6 : Sommes-nous obligés d'installer le certificat manuellement sur chaque poste en environnement d'entreprise ?

Non, dans un environnement Active Directory, le certificat peut être déployé automatiquement via les stratégies de groupe (GPO - Group Policy Objects). Il suffit de placer le certificat CA dans le conteneur approprié du contrôleur de domaine (Configuration Ordinateur > Paramètres Windows > Paramètres de sécurité > Stratégies de clé publique > Autorités de certification racines de confiance) et tous les postes membres du domaine recevront automatiquement le certificat lors de l'application des stratégies.

Question 7 : Quels sont les avantages et les inconvénients d'utiliser un proxy en mode manuel ?

Avantages : Contrôle précis sur quels appareils utilisent le proxy, facilité de diagnostic car la configuration est explicite, pas besoin d'installer de certificat SSL pour le trafic HTTPS de base (sans inspection), compatibilité avec tous les types d'applications qui supportent la configuration proxy.

Inconvénients : Configuration manuelle nécessaire sur chaque appareil (chronophage à grande échelle), les utilisateurs peuvent potentiellement désactiver le proxy dans leurs paramètres si les règles de pare-feu ne bloquent pas l'accès direct, maintenance plus lourde lors des changements d'infrastructure (nouvelle adresse IP du proxy par exemple).

Question 8 : Pourquoi le mode proxy transparent est-il souvent préféré dans des environnements avec de nombreux clients ?

Le proxy transparent élimine totalement le besoin de configurer manuellement chaque poste client. Les utilisateurs ne peuvent pas contourner le proxy en modifiant leurs paramètres réseau car l'interception se fait au niveau du réseau via les règles NAT. Cela simplifie grandement l'administration, garantit que 100% du trafic web passe par le proxy, et permet l'application uniforme des politiques de filtrage et de journalisation sans dépendre de la coopération des utilisateurs.

Document technique rédigé par Yassine Dinar