NOM Prénom : Ethan Georget
BTS SIO SISR - Bloc 3
Compte-Rendu : Mise en œuvre UTM (Squid, SquidGuard, Snort)

COMPTE-RENDU TECHNIQUE : SÉCURISATION UTM SOUS PFSENSE

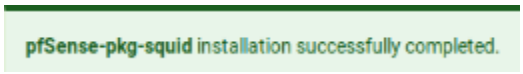
1. Présentation et Objectifs du Projet

L'objectif de ce laboratoire est de transformer une passerelle pfSense en une solution **UTM (Unified Threat Management)** afin de centraliser la sécurité du réseau local. Cette implémentation vise à ajouter des couches de protection applicative au-delà du filtrage de paquets standard.

- **Proxy Cache & Filtrage** : Optimisation des flux et contrôle de la navigation via le service Squid.
- **Filtrage par listes (URL)** : Interdiction d'accès à des catégories de sites spécifiques via SquidGuard.
- **IDS/IPS** : Analyse, détection et prévention d'intrusions réseau en temps réel via Snort.

2. Proxy Mandataire et Filtrage SSL (Squid)

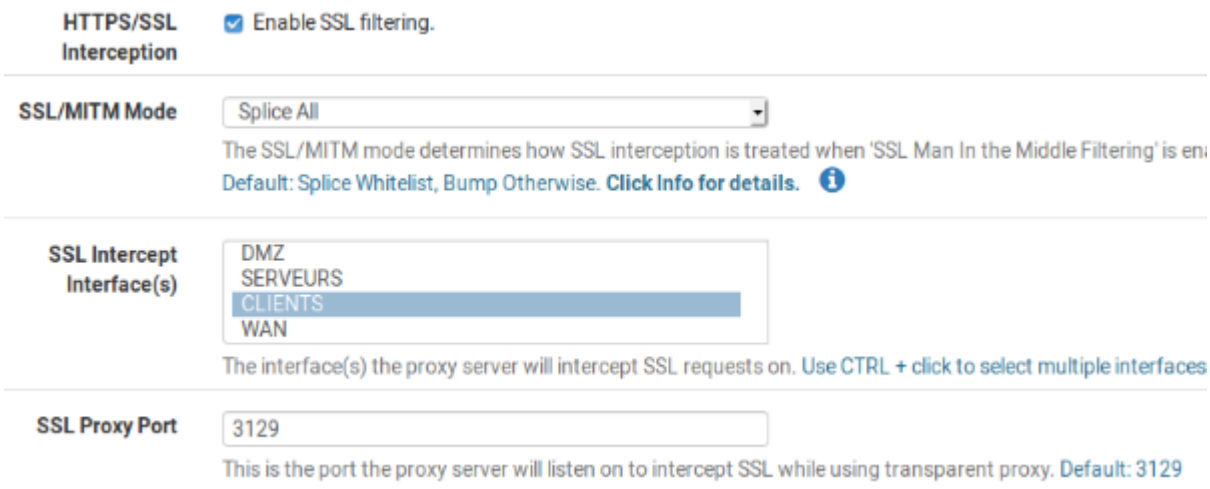
Le service Squid a été installé via le gestionnaire de paquets de pfSense. Il est configuré pour écouter sur l'interface CLIENTS sur le port 3128. Ce service permet de centraliser les requêtes web, de gérer un cache local et d'appliquer une politique de filtrage.

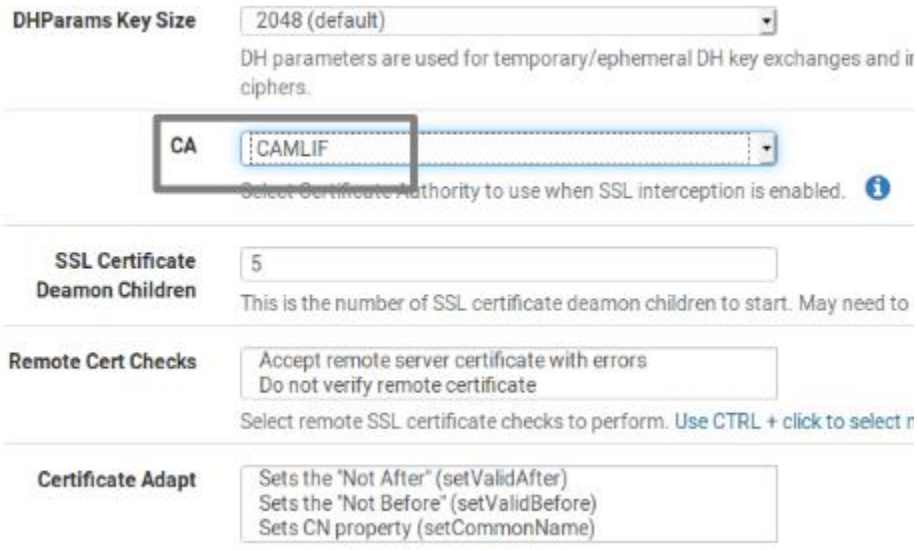


2.1 Infrastructure de clés (PKI) et SSL Intercept

Pour permettre au proxy d'analyser le trafic chiffré (HTTPS), une Autorité de Certification (CA) interne nommée 'CAMLIF' a été générée. Un certificat serveur spécifique (pfsense.mlif.local) de type 'Server Certificate' a ensuite été créé et signé par cette CA. Côté Squid, l'interception SSL a été configurée en mode 'Splice All'. Ce mode permet de récupérer le SNI (Server Name Indication) pour filtrer les domaines sans nécessiter un déchiffrement complet, ce qui limite les alertes de sécurité côté client.

Common Name	internal-ca
	The following certificate authority subject components are optional and
Country Code	FR
State or Province	IDF
City	PARIS
Organization	MLIF





3. Automatisation par WPAD

La méthode WPAD (Web Proxy Auto-Discovery) a été déployée pour éviter une configuration manuelle des navigateurs clients. Nous avons créé trois fichiers (wpad.dat, wpad.da et proxy.pac) contenant le script FindProxyForURL pointant vers l'IP 192.168.50.254.

```
mv /tmp/proxy.pac /usr/local/www
```

Le déploiement est complété par un enregistrement DNS de type A nommé 'wpad' sur le serveur Debian, pointant vers l'interface LAN du pare-feu.

```
wpad            IN      A       192.168.50.254
```

3.1 Vérification du déploiement des services

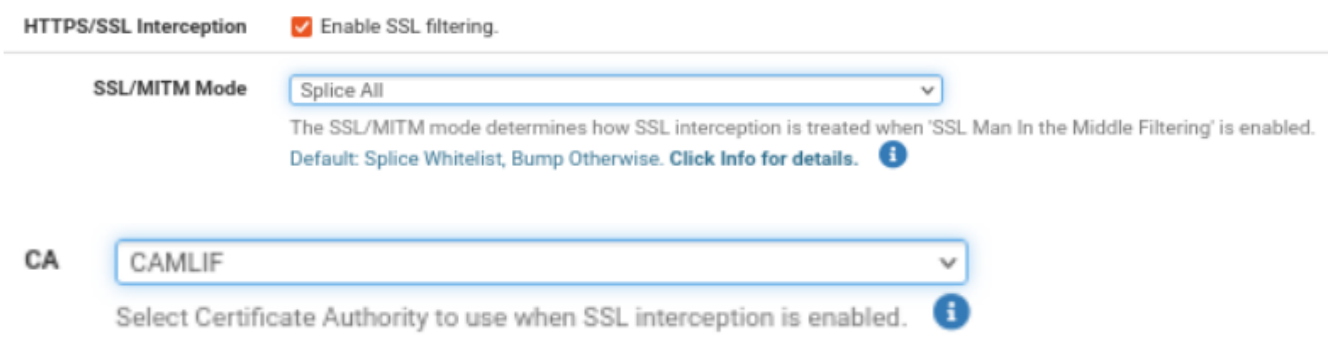
Une fois les packages installés depuis le "Package Manager", j'ai vérifié que Squid et SquidGuard apparaissaient bien comme "déjà installés" dans pfSense. Cela confirme que les binaires sont présents sur le système et que je peux passer à la configuration des services.

4. Filtrage par catégories (SquidGuard)

L'extension SquidGuard exploite les blacklists de l'Université de Toulouse Capitole. Les catégories 'socialnet', 'porn' et 'downloads' ont été configurées sur 'deny'. La validation a été confirmée sur le client Debian : les tentatives de connexion vers des sites comme facebook.com sont désormais interceptées, affichant un message de refus d'accès.

4.1 Mise en place du filtrage SSL (Splice All)

Afin de filtrer les flux sécurisés sans casser la chaîne de confiance, j'ai activé le filtrage SSL dans les options générales de Squid. J'ai configuré le mode « Splice All » en l'associant au certificat de serveur précédemment généré, permettant ainsi au proxy d'analyser le nom de domaine (SNI) des requêtes sur le port 443.



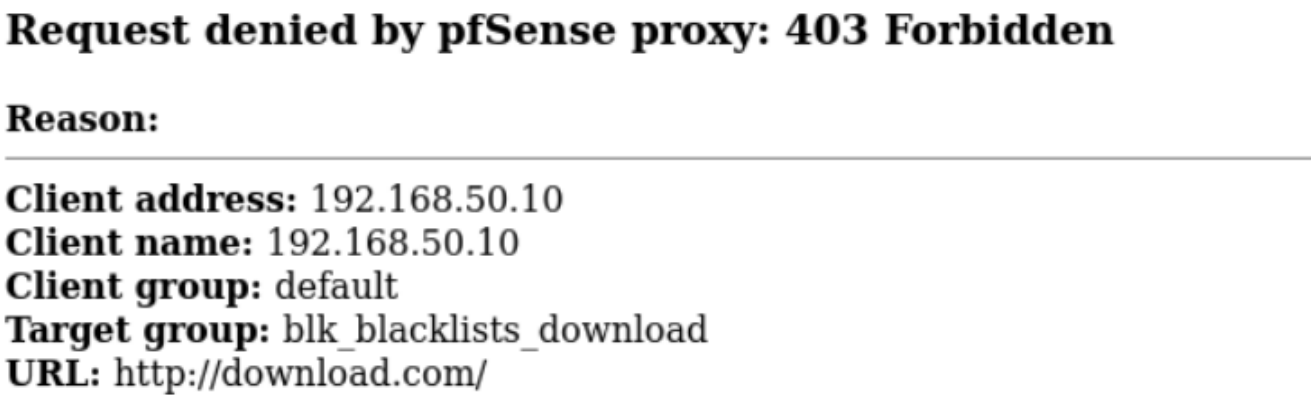
5. Système de Prévention d'Intrusion (Snort)

Snort a été déployé pour assurer une surveillance périmétrique DPI (Deep Packet Inspection). Dans un premier temps, la configuration globale nécessite l'ajout d'un 'Oinkcode'

Ensuite, Snort est activé sur l'interface WAN. Pour transformer le simple IDS (détection) en IPS (prévention), l'option cruciale 'Block Offenders' doit être cochée. Cela instruit le pare-feu de bannir l'IP source de tout paquet correspondant à une signature d'attaque.

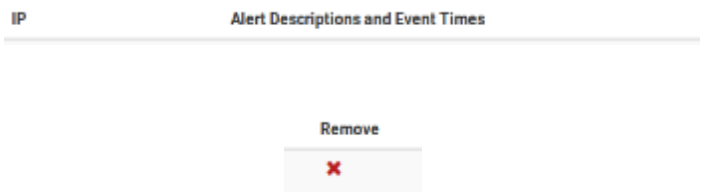
5.1 Paramétrage des ACL et catégories de blocage

Pour rendre le filtrage effectif, j'ai configuré les ACL communes dans SquidGuard. J'ai utilisé l'onglet "Target Categories" pour définir l'action "deny" sur les thématiques sensibles (publicités, malwares, etc.), forçant ainsi le proxy à rejeter toute requête vers ces domaines.



5.2 Test de validation

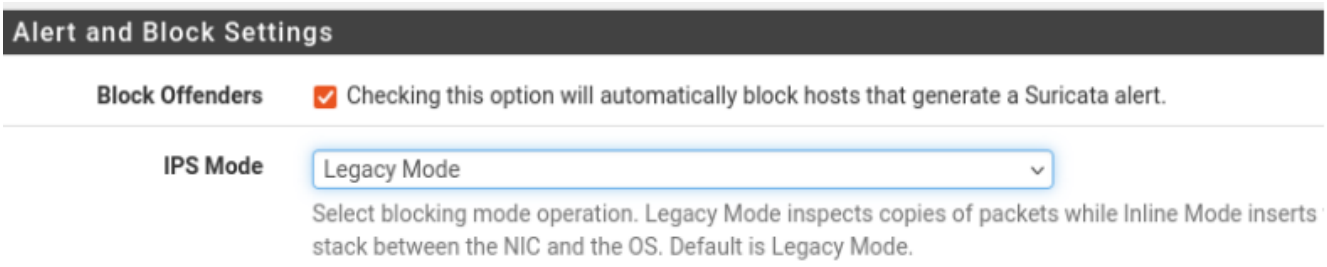
Un scan de ports nmap agressif a été simulé depuis l'extérieur. Snort a instantanément identifié la menace et a ajouté l'IP source à la liste des hôtes bloqués.



6. Détection d'intrusion et mode IPS avec Snort

Pour sécuriser le périmètre, j'ai mis en place Snort sur l'interface WAN. J'ai activé l'option **"Block Offenders"** pour passer en mode IPS, permettant au système de bannir automatiquement toute adresse IP identifiée comme malveillante.

J'ai validé le fonctionnement par un scan de ports externe (nmap -sS -A). Le système a immédiatement détecté l'attaque et banni l'IP source, comme en témoignent les journaux d'alertes.



7. Conclusion

La mise en œuvre de cette solution **UTM** sur pfSense m'a permis de transformer une simple passerelle de réseau en un équipement de sécurité complet et polyvalent. Grâce à l'intégration de **Squid** et **SquidGuard**, j'ai pu centraliser la gestion des flux de navigation, optimiser la bande passante et appliquer une politique de filtrage d'URL rigoureuse par catégories.

L'ajout de **Snort** en mode **IPS (Intrusion Prevention System)** apporte une couche de sécurité supplémentaire indispensable en bloquant automatiquement les tentatives d'attaques identifiées lors de mes phases de tests. Ce projet démontre qu'une solution "Open Source" bien configurée offre un niveau de protection professionnelle, capable de sécuriser efficacement le système d'information de la MLIF contre les menaces modernes