PLOUZENNEC Eliaz BTS SIO 2

Preuve de compétence

Épreuve E6

pfSense

20/03/2025

Sommaire :

Concevoir une solution d’infrastructure réseau

1. Analyser un besoin exprimé et son contexte juridique

Le besoin exprimé était de mettre en place une infrastructure réseau sécurisée, intégrant une zone DMZ pour héberger un serveur web/FTP et un serveur messagerie accessibles depuis Internet, tout en protégeant le réseau interne de l’entreprise. Cette configuration répond à des enjeux de sécurité en séparant les services exposés du réseau local, ce qui est une bonne pratique conforme aux exigences RGPD (sécurisation des données internes).

2. Étudier l’impact d’une évolution d’un élément d’infrastructure sur le système informatique

La mise en place d’une DMZ dans l’infrastructure existante implique de revoir le plan d’adressage, le routage et les règles de filtrage entre les zones. Cela a nécessité de vérifier que l’ajout du sous-réseau 10.4.9.0/24 n'interférait pas avec les règles existantes et que les accès entre DMZ et réseau interne étaient bien contrôlés.

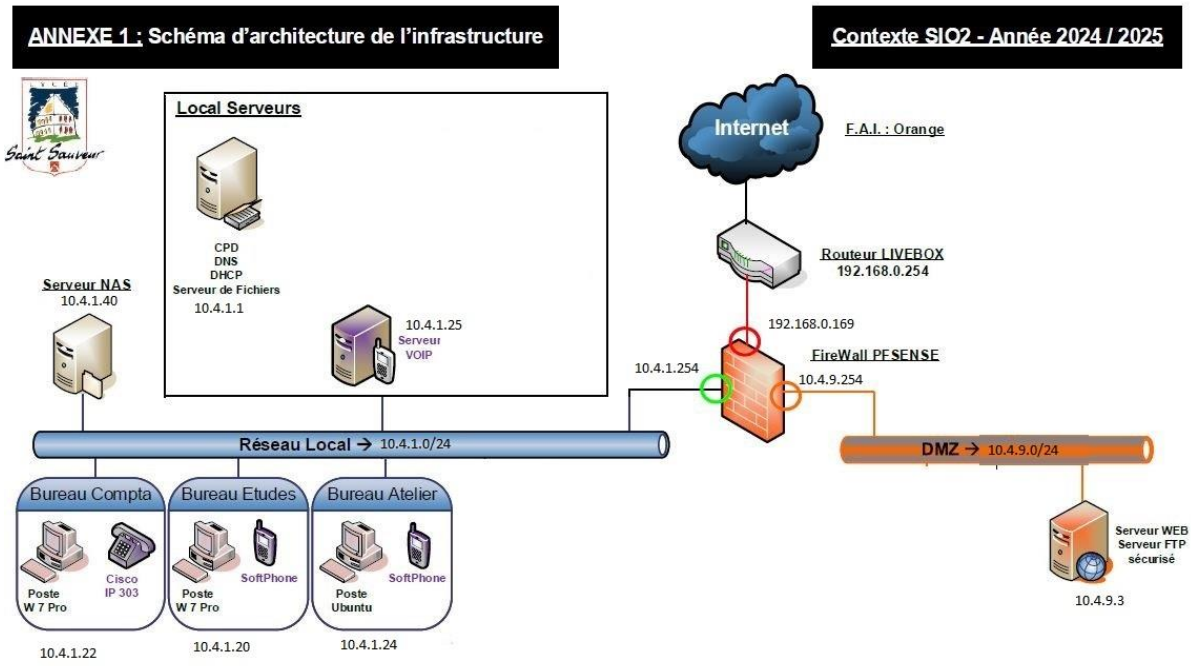
3. Élaborer un dossier de choix d’une solution d’infrastructure et rédiger les spécifications techniques

Le choix de pfSense a été motivé par sa puissance, sa flexibilité et sa compatibilité avec une DMZ multi-services. Une documentation des interfaces, du schéma réseau et firewall a été produite pour appuyer les choix techniques. Le plan d’adressage a été détaillé pour intégrer les réseaux LAN, WAN et DMZ.

4. Maquetter et prototyper une solution d'infrastructure permettant d'atteindre la qualité de service attendue

Une maquette a été réalisée dans l'environnement VMware ESXi du lycée. Elle repose sur :

- Une machine virtuelle dédiée à pfSense, avec 3 interfaces réseau configurées (WAN, LAN, OPT1/DMZ),
- Un serveur web placé dans le réseau DMZ (10.4.9.0/24),
- Des machines clientes dans le réseau LAN (10.4.1.0/24),
- Une connexion au réseau pédagogique via l'interface WAN (192.168.0.0/24).



5. Déterminer et préparer les tests nécessaires à la validation de la solution d'infrastructure retenue

Des tests ont été réalisés pour valider la séparation logique des réseaux via pfSense. Le pare-feu a été configuré avec trois interfaces distinctes (WAN, LAN et DMZ), permettant une circulation isolée entre chaque zone. pfSense agit comme point de passage entre le réseau interne, la DMZ et l'extérieur.

Une **blacklist** a été mise en place afin de bloquer l'accès à certains sites ou adresses IP depuis le réseau LAN.
Les tests effectués ont permis de vérifier :

- la connectivité de base entre les zones,
- le bon fonctionnement de l'accès à Internet depuis le LAN,
- et l'application correcte de la blacklist configurée dans l'interface de filtrage de pfSense.

Installer, tester et déployer une solution d'infrastructure réseau

1. Installer et configurer des éléments d'infrastructure

Le firewall pfSense a été installé et configuré avec trois interfaces :

- WAN (192.168.0.169),
- LAN (10.4.1.254),
- OPT1/DMZ (10.4.9.254).
  Les adresses IP ont été attribuées, le routage activé, et les services DNS, NAT et firewall ont été configurés.

Installer et configurer le Firewall pfSense

Suivre l'installation et au moment de reboot, il faut éjécter virttuellement le disque pour ne pas redémarrer la configuration.
On arrive sur cette page:

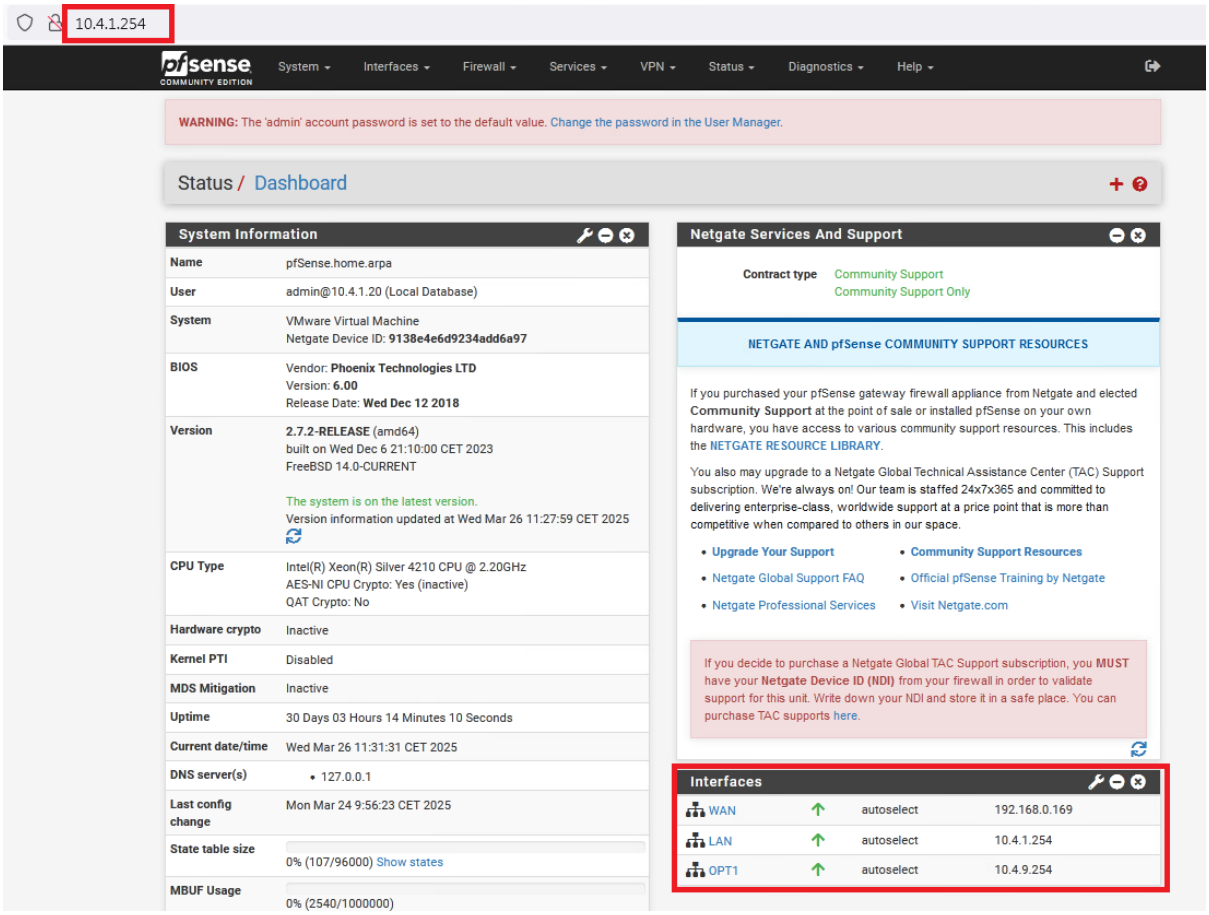
```
WAN (wan)       -> vmx1       -> v4: 192.168.0.169/24
LAN (lan)       -> vmx0       -> v4: 10.4.1.254/24
OPT1 (opt1)     -> vmx2       -> v4: 10.4.9.254/24
```

Où on configure l'entrée WAN, en accès par pont vers le réseau de la salle, ici en avec 192.168.0.168.

Puis on ajoute un LAN, qui mènera vers les machines du réseau Littoral 10.4.1.0/24, on le met en 10.4.1.254/24, qui sera le gateway des machines dans ce réseau.

Puis on ajoute un OPT1, qui mènera vers le réseau de 10.4.9.0/24, qui sera le réseau de la DMZ, avec l'ip 10.4.9.254, qui sera leur gateway.

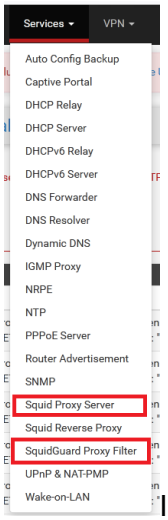
Interface pfSense



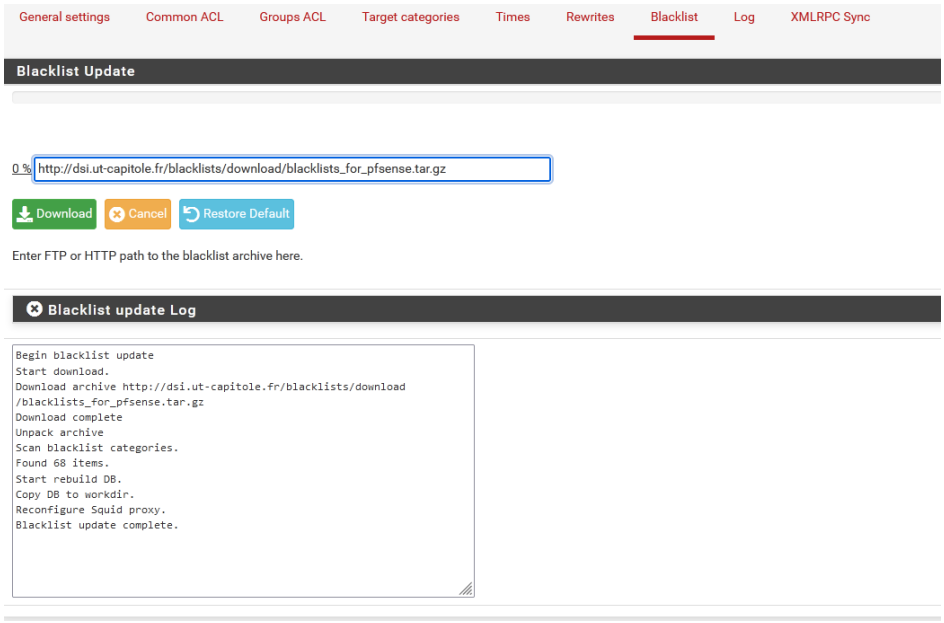
Ainsi on arrive sur cette interface, si on rentre l'ip du gateway pour le réseau 10.4.1.0 (on peut faire pareil du coté OPT1 ou WAN avec leurs interfaces respectives)

On retrouve en bas à droite toutes les interfaces du pfSense.

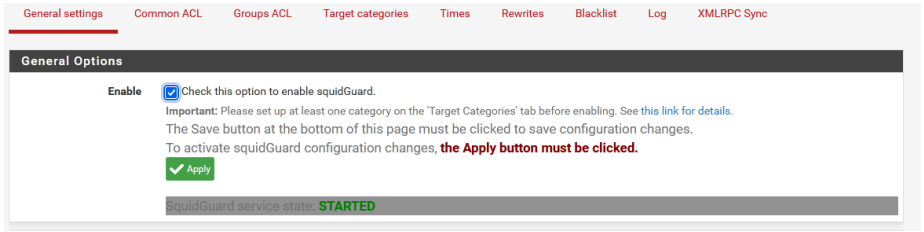
Activer la black list



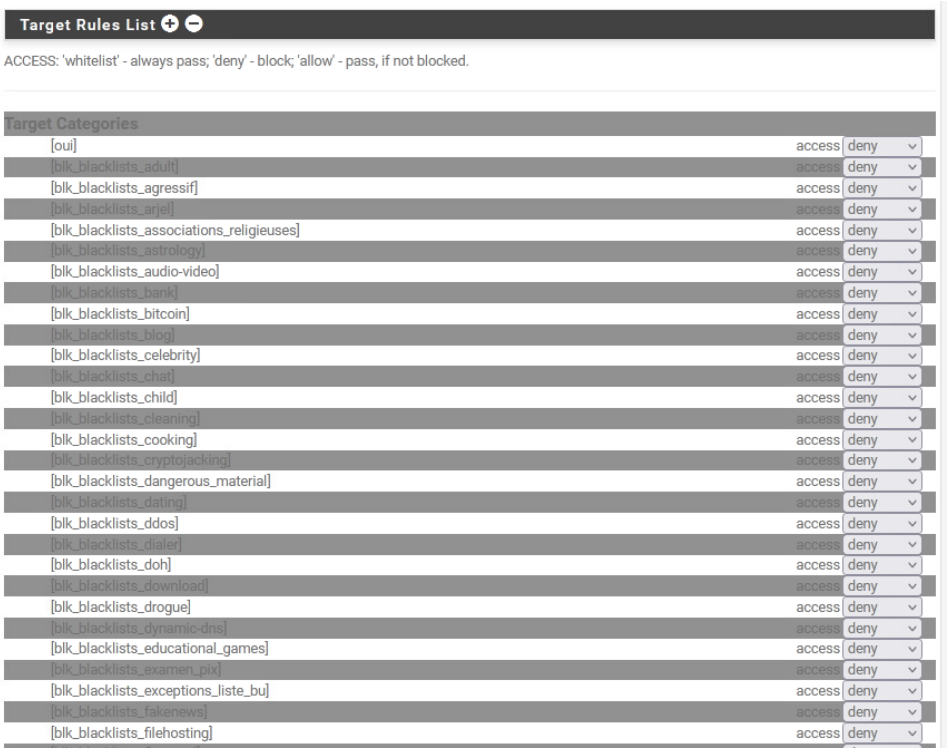
Il faut aller dans les options de Squidguard



Ensuite importer la black list de l'université de Toulouse.



Activer Squidguard

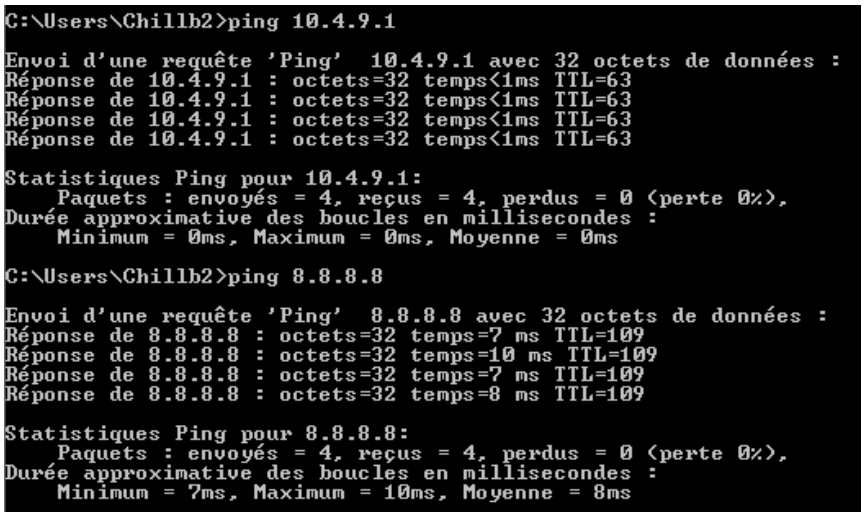


Puis refuser tous les termes de la black list.

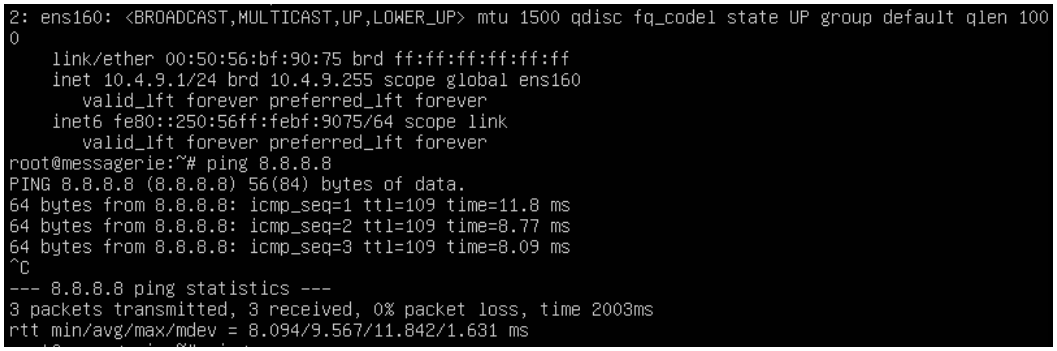
2. Tester l’intégration et l’acceptation d’une solution d’infrastructure

Des tests de connexion ont été réalisés depuis :

- Le reseau Littoral (10.4.1.0/24) à la DMZ (10.4.9.0/24) et de Littoral à internet :



- DMZ vers internet :



3. Déployer une solution d’infrastructure

La solution a été déployée sur une machine virtuelle dédiée au firewall pfSense, intégrée à l’environnement ESXi. Le serveur web/FTP a été mis en ligne dans la DMZ , et l’ensemble a été documenté pour permettre un déploiement fiable et reproductible.