# Prosit : SECURITE

## Contexte :

Sécuriser le réseau des menaces informatiques extérieures

## Mot clés :

* ACL : « Access control list » Ensemble de règles qui définissent les opérations (lire, écrire, exécuter…) que pourra réaliser un utilisateur sur une ressource (un fichier, le plus souvent, mais aussi une adresse ou un port réseau).
* Proxy : Serveur relais qui, sur Internet, stocke les données en vue de faciliter leur accès.
* Filtrage :
* Bac à sable : environnement virtuel ou physique de test qui permet de travailler sans perturber les machines ou serveurs en production.
* UTM
* DMZ: En informatique, une zone démilitarisée est un sous-réseau séparé du réseau local et isolé de celui-ci ainsi que d'Internet par un pare-feu.
* IPS/IDS: “Système Prevention d’intrusion » ; « Système de détection intrusion »

La détection d'intrusion est le processus de surveillance de votre trafic réseau et d'analyse de celui-ci pour détecter des signes d'éventuelles intrusions, telles que des tentatives d'exploitation et des incidents pouvant constituer des menaces imminentes pour votre réseau. Pour sa part, la prévention des intrusions consiste à effectuer une détection des intrusions puis à arrêter les incidents détectés, généralement en supprimant des paquets ou en mettant fin à des sessions.

* NAT/PAT: (NAT) adresses réseau qui relie deux réseaux et mappe les adresses privées en adresses publiques. (PAT) adresse de port est un type de NAT dynamique grâce auquel la traduction d’adresse peut être configurée au niveau du port, et l’utilisation de l’adresse IP est optimisée.
* Firewall: est un programme informatique dont l'objectif est de filtrer les éléments arrivant sur un réseau interne
* SOC (Security Operation Center):  installation abritant une unité de sécurité chargée de surveiller et d’analyser en permanence le dispositif de sécurité d’une entreprise.
* SIEM(Security Information and Event Management): solution de sécurité qui permet aux organisations de détecter les menaces avant qu'elles ne perturbent leurs activités.
* PFsense : système d'exploitation open source ayant pour but la mise en place de routeur/pare-feu basé sur le système d'exploitation FreeBSD.
* Malwares : terme générique utilisé pour désigner une variété de logiciels hostiles ou intrusifs

## Problématique :

Comment sécuriser le réseau des menaces informatique extérieure ?

## Contraintes :

RAS

## Généralisation :

Mettre en place un filtrage firewall

Sécuriser un réseau

## Livrables :

VMs configurées pour la sécurité

Schéma adapter à nos VMs

## Pistes de solution :

Utiliser une VM comme firewall (PFsense ?)

ACL pour filtrage ?

## Plan d’action :

Comprendre la théorie (faire le point vendredi)

Adapter le schéma aux VM

## Réalisation du plan d’action :

Création du firewall via Pfsense :

Dans un premier temps nous avons besoin d’une machine externe pouvant accueillir le Firewall,

On crée pour cela un nouvelle Vm avec l’ISO de Pfsense sous FreeBSD.

Pour configurer Pfsense on suis le tuto ci-contre : <https://www.it-connect.fr/comment-installer-pfsense-dans-virtualbox-pour-creer-un-lab-virtuel/>

On créer ensuite 3 interfaces correspondant au : WAN, LAN, DMZ.

Sur le pfsense commande (ou graphique) on attribue des adresses à chaque interface

Une image contenant texte, capture d’écran, Police, noir

Description générée automatiquement

Via l’option 2.

On choisi de config le Wan par DhcpIpv4, on configure l’IP du Lan et de la DMZ en statique

Une image contenant diagramme, capture d’écran, texte, conception

Description générée automatiquement

Figure :Schéma du réseau

Pour créer un filtre sur Pfsense il nous suffit de créer une nouvelle règle dans le pare-feu pour l’interface voulu :

Une image contenant texte, capture d’écran, logiciel, Page web

Description générée automatiquement

Cette interface permet de créer les règles qui régiront l’interface sur laquelle elle s’applique.

On peut par exemple ouvrir ou restreindre certain port ou certaines plage d’IP.