TP2
Implémentation d'un réseau sécurisé
Pfsense - OpenVPN - Snort

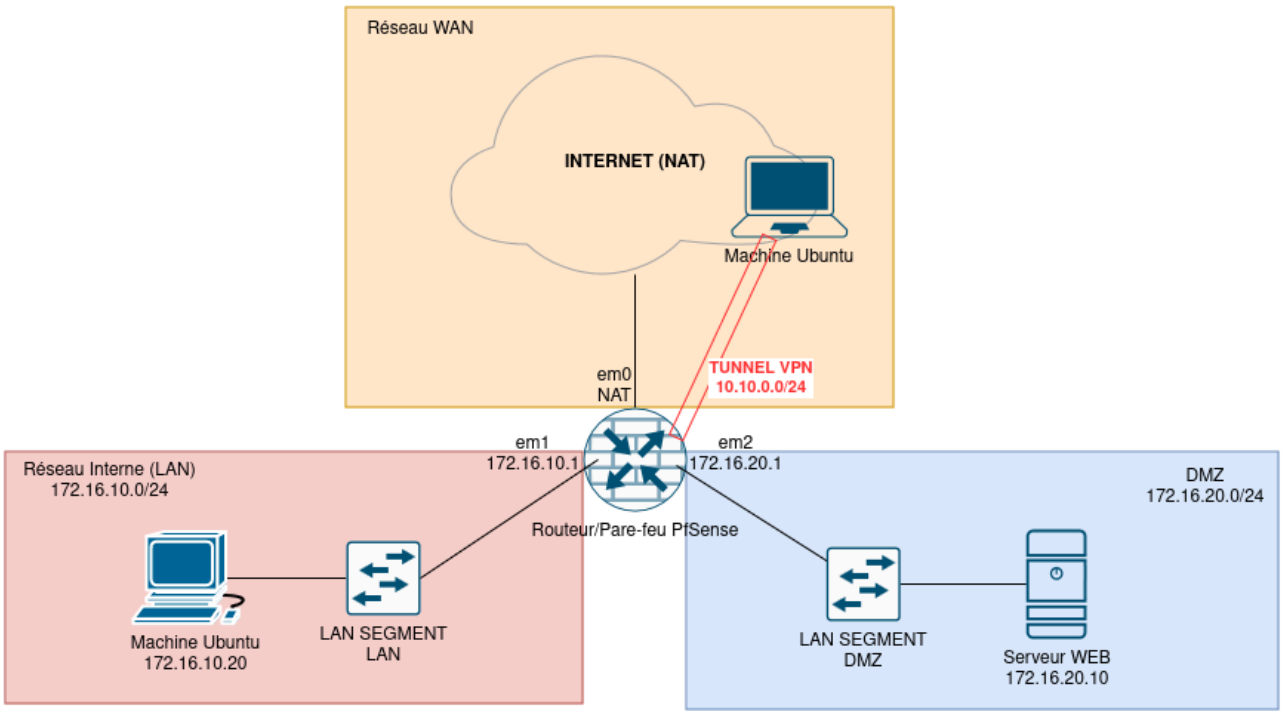
Contexte et objectif

L'entreprise *ABC Logistiques* veut implémenter un réseau sécurisé. Ils possèdent un serveur Web qui expose au public un site web, et une machine qui ne devrait être accessible qu'aux employés, seulement depuis le réseau interne de l'entreprise.

ABC Logistiques veut aussi permettre à ses employés d'accéder au réseau interne à distance afin de leur permettre de faire du télétravail.

On vous demande, en tant qu'administrateur système, d'implémenter une solution VPN qui permettra aux employés d'accéder aux machines du réseau interne à partir d'internet.

Ce travail pratique a pour objectif de vous introduire à l'implémentation d'un réseau d'entreprise sécurisé. Nous utiliserons PfSense, un système d'exploitation open source largement utilisé en entreprise en tant que routeur et pare-feu. Nous allons y implémenter un serveur VPN, certaines règles de pare-feu pour contrôler les flux entre les différents réseaux ainsi que certaines règles et signatures Snort pour filtrer et bloquer l'accès à certaines applications.
La topologie du réseau à implémenter est la suivante :



Composition du réseau

- **Un réseau interne (LAN) - 172.16.10.0/24**
    - Avec une machine Ubuntu (172.16.10.20)
- **Un réseau externe (NAT) -** Considéré comme le WAN, ou Internet,
    - Avec une machine Ubuntu.
- **Une zone démilitarisée, ou DMZ (LAN) - 172.16.20.0/24**
    - Avec un serveur Web (d'adresse IP 172.16.20.10).
- **Un routeur/pare-feu PfSense**, qui permettra de filtrer et router le trafic entre le LAN, le WAN et la DMZ.

Trois VMs vous sont fournies :

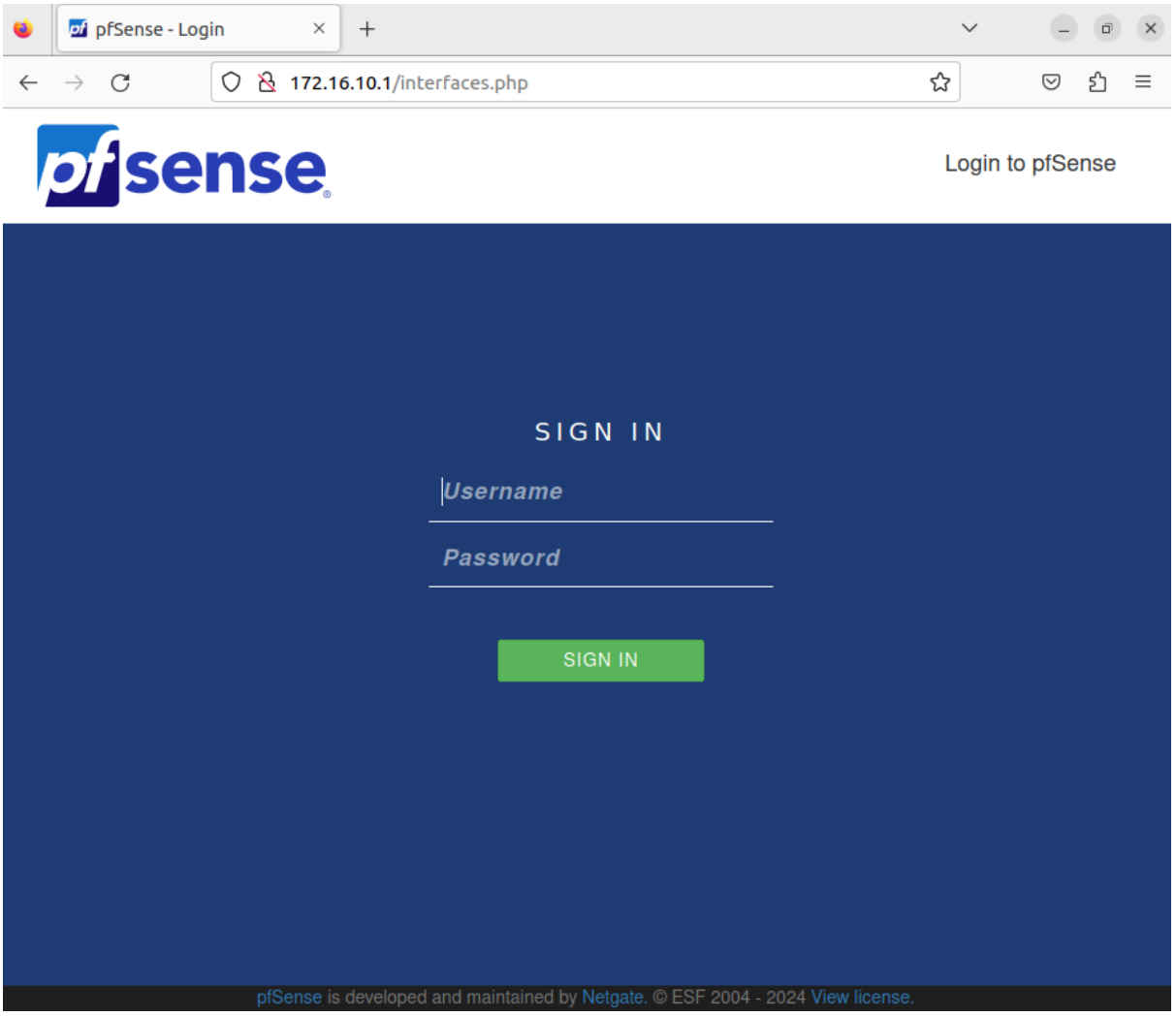
- **Une machine client Ubuntu (*ubuntu-client.ova*) -** Vous devez configurer son adaptateur réseau en NAT ;
- **Une machine Ubuntu dans le réseau interne (*ubuntu-lan.ova*) -** Vous devez configurer son adaptateur réseau en LAN Segment (LAN).
- **Une machine PfSense (*pfsense.ova*) -** Vous devez configurer le premier adaptateur réseau en NAT (WAN), le deuxième en LAN Segment (LAN), le troisième dans un LAN Segment différent (DMZ).
- **Une machine Ubuntu pour le serveur Web (ubuntu-web-server.ova)-**: Vous devez configurer son adaptateur réseau en LAN Segment (DMZ)

Étapes d'implémentation

Configuration de PfSense

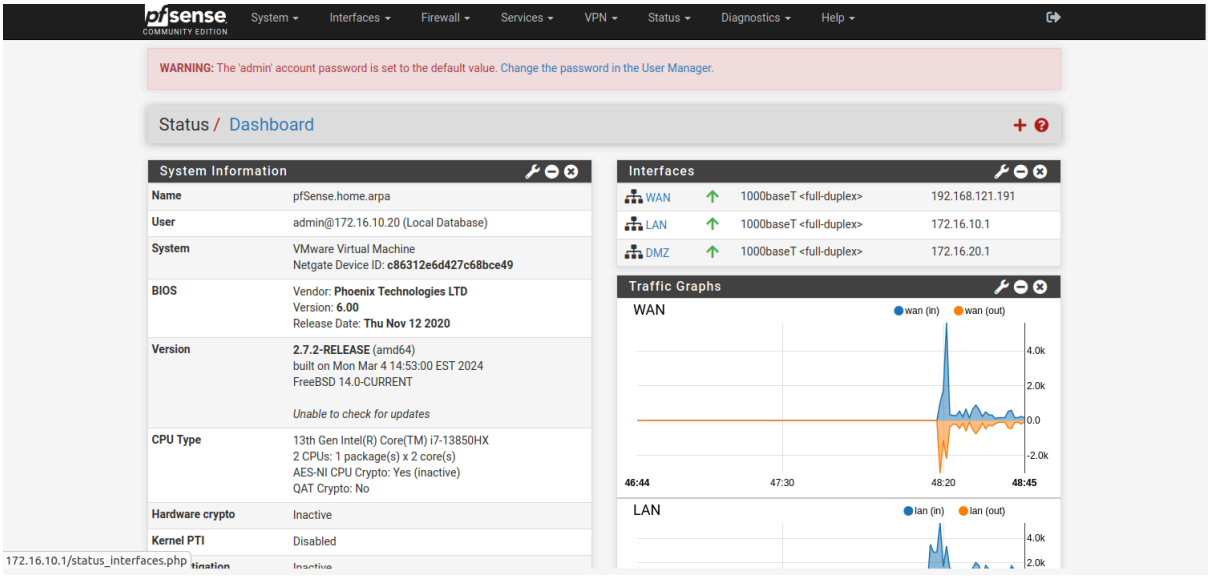
Après avoir configuré correctement vos adaptateurs réseau, allumez la VM PfSense et la machine Ubuntu dans le LAN. PfSense possède une interface accessible sur le navigateur d'une machine du LAN.

Ouvrez un navigateur dans la machine Ubuntu du LAN et entrez l'adresse IP de l'interface de PfSense située dans le LAN (172.16.10.1). Vous verrez une page de connexion apparaître :



- **Identifiant :** admin
- **Mot de passe :** pfsense

Maintenant, vous devrez voir apparaître le tableau de bord de PfSense.



Partie I - Règles de pare-feu

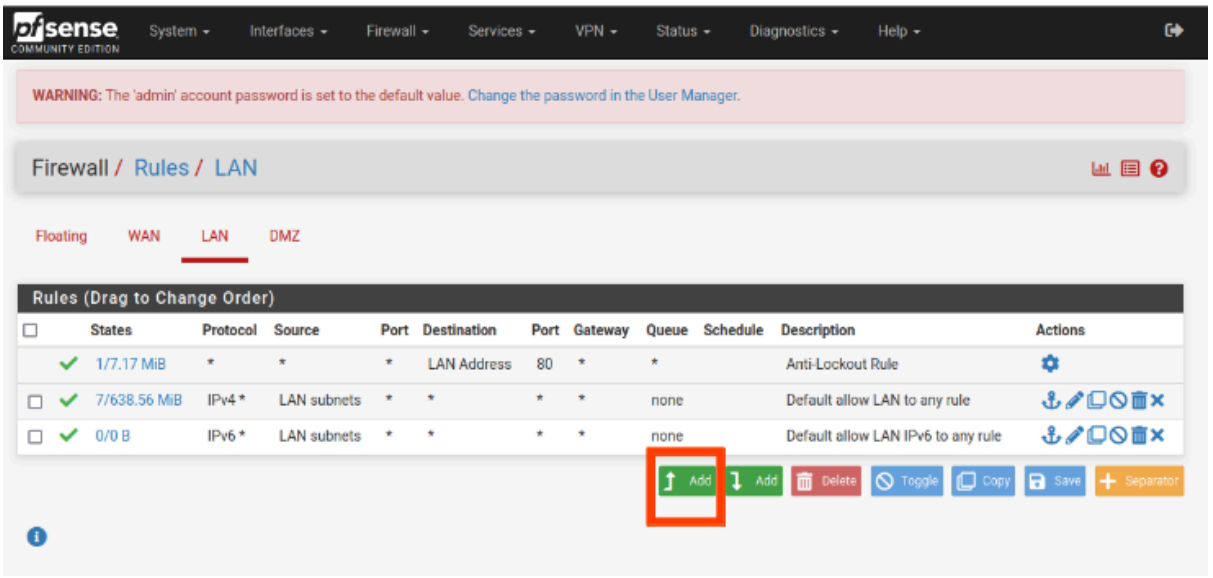
Afin de sécuriser notre réseau, la première étape est de contrôler les flux entrant et sortant du LAN et de la DMZ pour autoriser seulement les flux nécessaires.

Règles pour le flux du LAN

Par défaut, tout trafic est autorisé du LAN vers le WAN, et du LAN vers la DMZ (vous pouvez tester ceci en naviguant sur le site web hébergé sur le serveur web à partir du navigateur de votre client Ubuntu situé dans le LAN).

Nous voudrions changer le trafic autorisé du LAN vers la DMZ pour autoriser seulement le trafic TCP sur les ports 80 (soit http, pour accéder à notre site web), 20 (SSH pour pouvoir se connecter au serveur web en SSH) et les requêtes ping, et ce afin d'assurer un meilleur contrôle des flux du LAN vers la DMZ.

Dans l'onglet *Firewall → Rules*, allez sur l'onglet *LAN*. et cliquez sur le bouton "*Add*" pour ajouter une règle :



Sélectionnez les options suivantes pour bloquer par défaut les flux entre le LAN et la DMZ :

- **Action :** Block,
- **Protocol :** “Any”
- **Source :** LAN Subnets
- **Destination :** DMZ Subnets
- **Description :** “Bloquer les flux entre le LAN et la DMZ par défaut”

Enregistrez, appliquez les changements puis réessayer de naviguer vers votre site web. Vous n’y arriverez plus !

Maintenant créez deux règles :

Règle 1 - Autoriser l’accès au serveur web sur le port 80 HTTP

- **Action :** Pass
- **Protocol :** TCP
- **Source :** LAN Subnets
- **Destination :** Address or Alias puis entrez l’adresse IP du serveur WEB : 172.16.20.10
- **Destination Port Range :** From HTTP (80)
- **Description :** Autoriser l’accès au serveur web sur le port 80 HTTP

Règle 2 : Autoriser l’accès au serveur web sur le port 22 SSH

- **Action -** Pass
- **Protocol -** TCP
- **Source -** LAN Subnets
- **Destination -** Address or Alias puis entrez l’adresse IP du serveur WEB : 172.16.20.10
- **Destination Port Range -** From SSH (22)
- **Description -** Autoriser l’accès au serveur web sur le port 22 SSH

Enregistrez et appliquez les changements. Vous devrez pouvoir aller de nouveau sur le site web du serveur dans la DMZ.

Attention ! L'ordre des règles est important. Si la règle qui bloque le flux est avant les règles d'autorisation, vous ne serez pas capable de communiquer avec votre serveur web sur le port 80 ou 22.

Maintenant, essayez de ping votre serveur web depuis votre machine sur le LAN. Que remarquez-vous ?

Il faut créer une nouvelle règle pour autoriser les requêtes ping, avec les options suivantes :

- **Action :** Pass
- **Protocol :** ICMP
- **ICMP Subtypes :** echo request
- **Source :** LAN Subnets
- **Destination :** Address or Alias puis entrez l'adresse IP du serveur WEB : 172.16.20.10
- **Description :** Autoriser l'accès au serveur web depuis le LAN pour les requêtes ICMP (ping)

Sauvegardez et appliquez les changements, puis réessayez de ping le serveur Web. Bingo!

Règles pour la DMZ

Par défaut, la DMZ n'a aucune règle, mais il serait pratique d'autoriser les serveurs de la DMZ à faire des requêtes HTTP, HTTPS et DNS, ainsi que des requêtes ICMP echo reply. Le reste des flux doivent être bloqués pour assurer un minimum de sécurité ! Allez dans l'onglet *Firewall→Rules*, puis dans l'onglet *DMZ* et ajoutez les règles suivantes :

Règle 1 - Bloquer le flux vers le LAN

- **Action :** block
- **Protocol :** any
- **Source :** DMZ subnets
- **Destination :** LAN subnets
- **Description :** Bloquer flux vers le LAN

Règle 2 - Autoriser le flux pour les requêtes HTTP

- **Action :** pass
- **Protocol :** TCP
- **Source :** DMZ subnets
- **Destination :** any
- **Destination Port Range :** HTTP (80)
- **Description :** Autoriser le flux pour les requêtes HTTP

Règle 3 - Autoriser le flux pour les requêtes HTTPS

- **Action :** pass
- **Protocol :** TCP

- **Source :** DMZ subnets
- **Destination :** any
- **Destination Port Range :** HTTPS (443)
- **Description :** Autoriser le flux pour les requêtes HTTPS

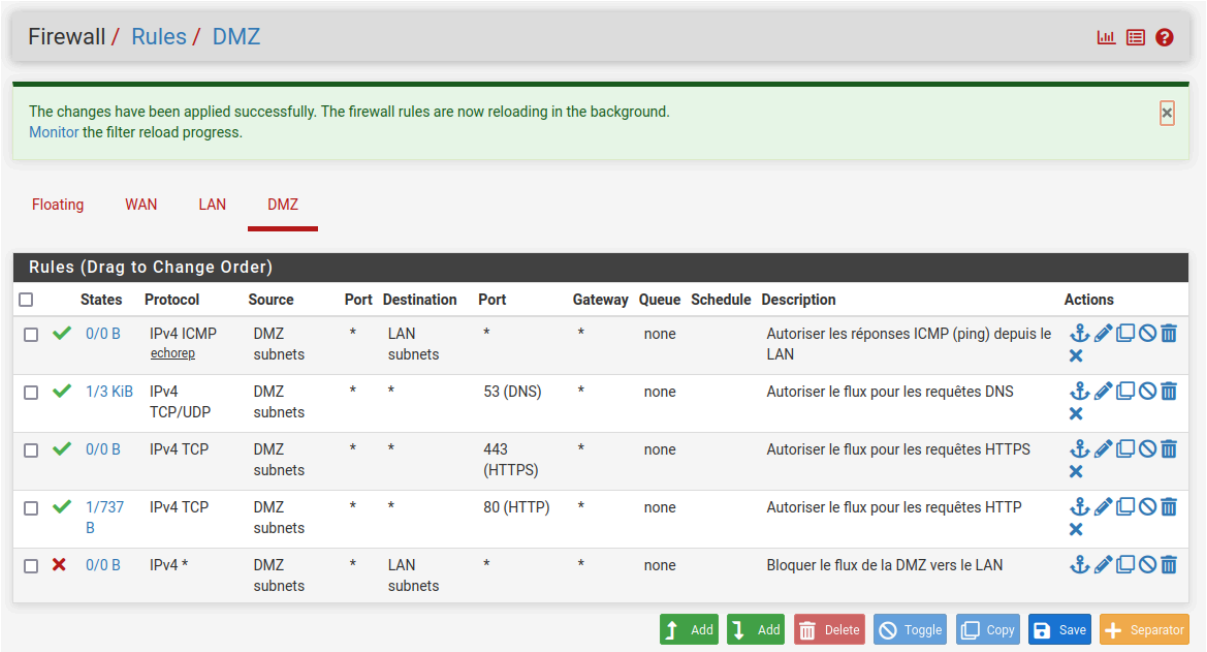
Règle 4 - Autoriser le flux pour les requêtes DNS

- **Action :** pass
- **Protocol :** TCP/UDP
- **Source :** DMZ subnets
- **Destination :** any
- **Destination Port Range :** DNS (53)
- **Description :** Autoriser le flux pour les requêtes DNS

Règle 5 - Autoriser les réponses ICMP (ping) depuis le LAN

- **Action :** pass
- **Protocol :** ICMP
- **ICMP Subtypes :** echo reply
- **Source :** DMZ subnets
- **Destination :** LAN subnets
- **Description :** Autoriser les réponses ICMP (ping) depuis le LAN

Enregistrez et appliquez les changements. Vous devrez avoir l'ensemble de règles suivantes :



Maintenant testez vos règles :

- Essayez de naviguer sur internet depuis votre serveur Web. Vous devrez y arriver.

- Essayez d'envoyer un ping de votre machine Ubuntu sur le LAN vers votre serveur Web. Vous devriez y arriver.
- Essayez d'envoyer un ping de votre serveur Web vers votre machine Ubuntu sur le LAN. Cela devrait échouer.

Règles de NAT pour le serveur Web

Pour avoir accès à notre serveur Web depuis le WAN (internet), la bonne pratique serait de mettre en place un proxy inverse (de type HA Proxy, par exemple) pour publier notre site de façon sécurisée. Une façon plus simple (mais moins sécurisée) est de créer une règle de NAT de "*port forwarding*". Nous n'allons pas rentrer dans les détails de ce que c'est que le port forwarding, si vous voulez en savoir plus, vous pouvez consulter la vidéo suivante :

Sur l'interface PfSense, allez sur *Firewall → NAT* et créez une nouvelle règle avec les options suivantes :

- **Interface -** WAN
- **Protocol -** TCP
- **Destination -** WAN address
- **Destination port range -** HTTP
- **Redirect target IP -** Address or Alias puis entrez l'IP de votre serveur Web (172.16.20.10)
- **Redirect target port -** HTTP

Enregistrez et appliquez les changements.

Allez sur votre machine située sur le WAN (NAT), et essayez d'accéder au site Web de votre serveur Web en entrant l'adresse IP de votre interface PfSense située sur le NAT.
Vous remarquerez que ça ne fonctionne pas.

Pourquoi ?! Nous avons pourtant implémenté la règle de port forwarding !

Ceci est dû au fait que, dans les paramètres de notre interface WAN, l'option *Block private networks and loopback address* est activée. Cette option permet de bloquer les flux qui arrivent sur l'interface WAN et qui ont une adresse IP source privée (*10.x.x.x/8, 172.16.x.x/12, 182.167.x.x/16*). Cette option devrait être activée en production, mais pour le contexte de notre Travail Pratique, nous devons la désactiver pour accéder à notre site web à partir du WAN.

Allez sur l'onglet *Interfaces→WAN*, puis désactiver cette option. Sauvegardez vos changements et appliquez-les. Retourner à votre machine située sur "Internet" et essayez de naviguer sur le site web en entrant l'adresse IP de l'interface WAN de PfSense... Bingo !

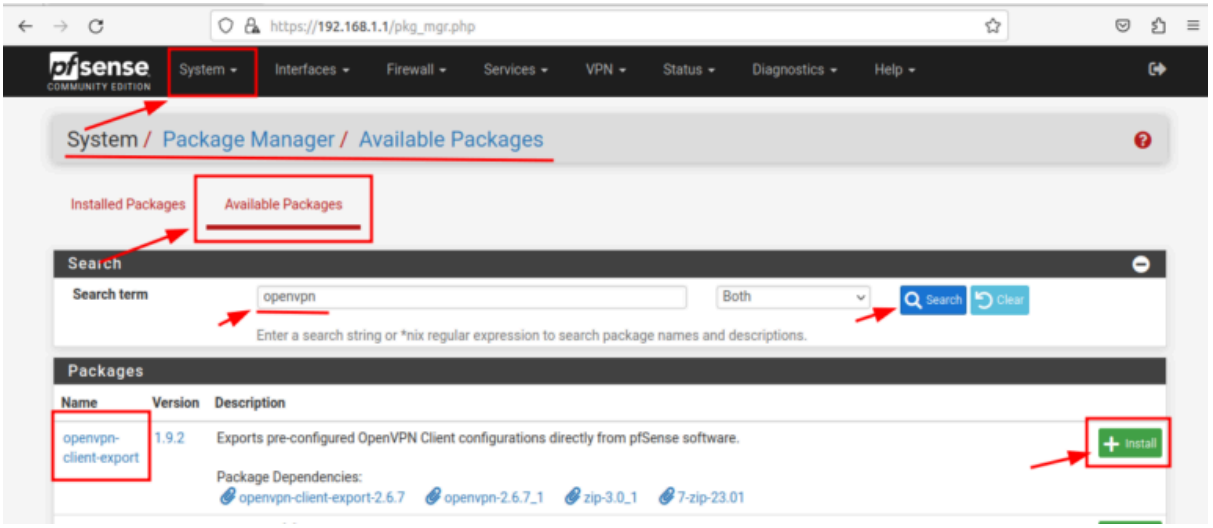
Avant de passer à la partie suivante, appelez votre enseignant pour qu'il vérifie votre implémentation (et vous donne les points de cette partie !)

Partie II - Implémentation d'un serveur OpenVPN

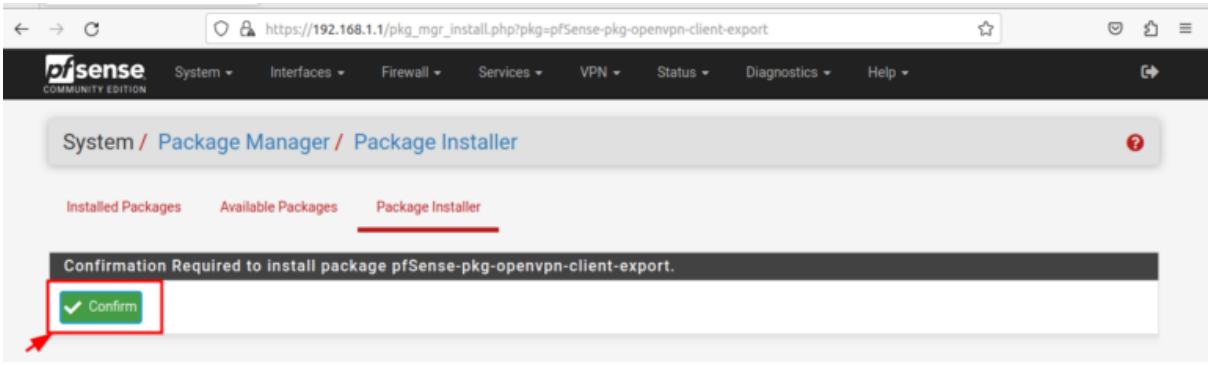
Dans cette partie, nous allons mettre en place un serveur VPN de telle sorte à ce que les employés de l'entreprise puissent se connecter aux machines du réseau interne depuis Internet. Nous allons utiliser OpenVPN, une solution open-source permettant de créer un réseau privé virtuel (VPN).

Étape 1 : Installation de *openvpn-client-export*

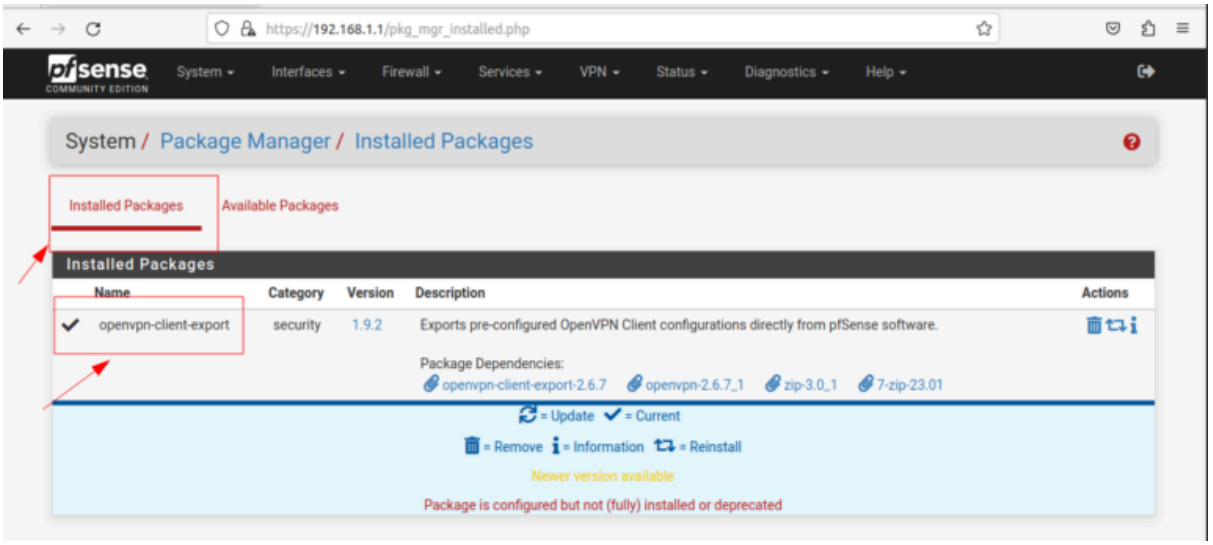
Dans l'interface de PfSense allez sur l'onglet *System→Package Manager→Available Packages* et téléchargez *open-vpn-client-expor*t. Ce paquet permet d'exporter plus facilement tous les paramètres VPN pour le client après avoir configuré le serveur OpenVPN.



Confirmez l'installation :



Une fois l'installation terminée, vous pouvez voir ce package dans la section "*Installed packages*".



Étape 2 : Configuration du serveur OpenVPN

Dans les prochaines étapes, nous allons créer un certificat un utilisateur puis activer OpenVPN.

Naviguez à l'onglet *VPN→OpenVPN* puis l'onglet *Wizar*d.

Pour *Type of Server*, sélectionnez *Local User Access*

Pour *Create a New Certificate Authority (CA) Certificate*, entrez un nom descriptif (par exemple, *openvpn-ca*) puis les options suivantes :

- **Country Code -** CA
- **State or Province -** QC
- **City -** Montreal
- **Organisation -** CMV

À l'étape *Choose a Server Certificate*, cliquez sur le bouton *"Add new Certificate"*

Dans *Server Setup* (étape 9 sur 11) choisissez une description, puis dans les options *Tunnel Settings* sélectionnez les options suivantes :

- ***IPv4 Tunnel Network -*** Choisissez un réseau qui ne rentre pas en conflit avec les réseau du WAN, de la DMZ ou du LAN (par exemple 10.10.10.0/24). C'est le réseau qui sera utilisé pour le tunnel VPN
- ***IPv4 Local Network -*** Choisissez le réseau qui sera accessible par le tunnel, soit le réseau LAN (172.16.10.0/24)

Dans les configurations des règles de pare-feu *(Firewall Rule Configuration*, étape 10 sur 11), cochez les cases *Firewall Rule* et *OpenVPN rule*, qui permettent d'ajouter des règles de pare-feu pour autoriser le flux du VPN vers le LAN.

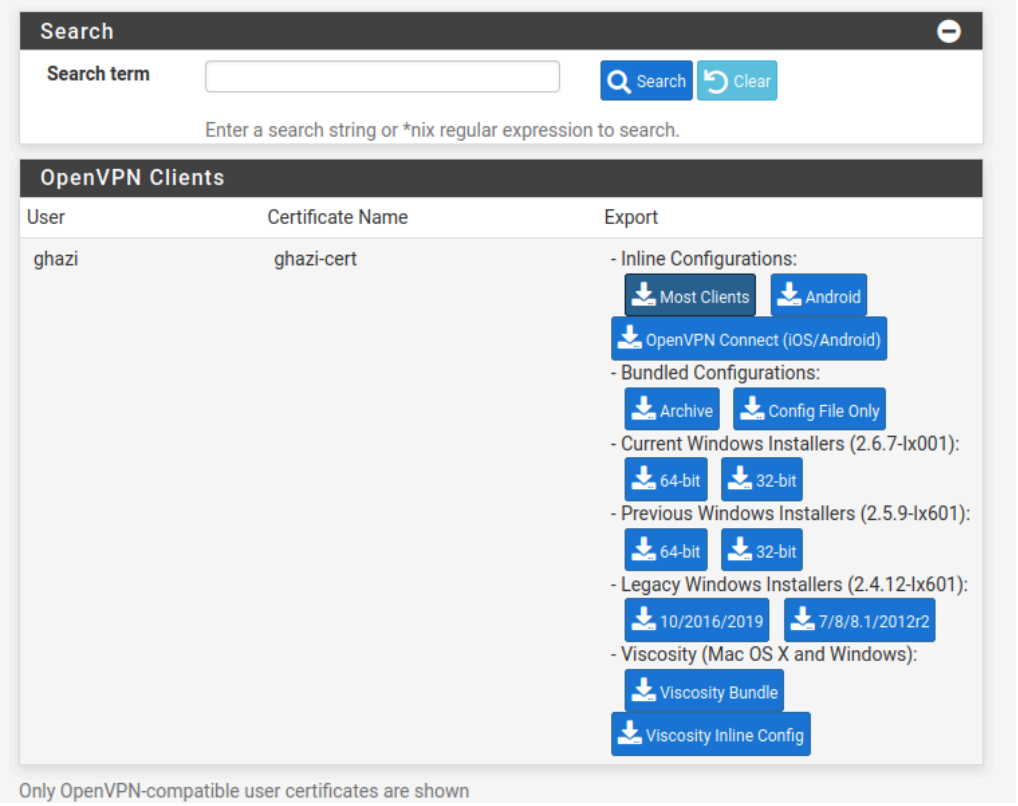
Maintenant, il reste à créer un utilisateur qui utilisera ce VPN.

Naviguez dans l'onglet *System→User Manager*, puis, dans *Users*, cliquez sur le bouton *Add* pour ajouter un nouvel utilisateur.

Ajoutez un nom et un mot de passe de votre choix, puis créez un certificat pour votre utilisateur.

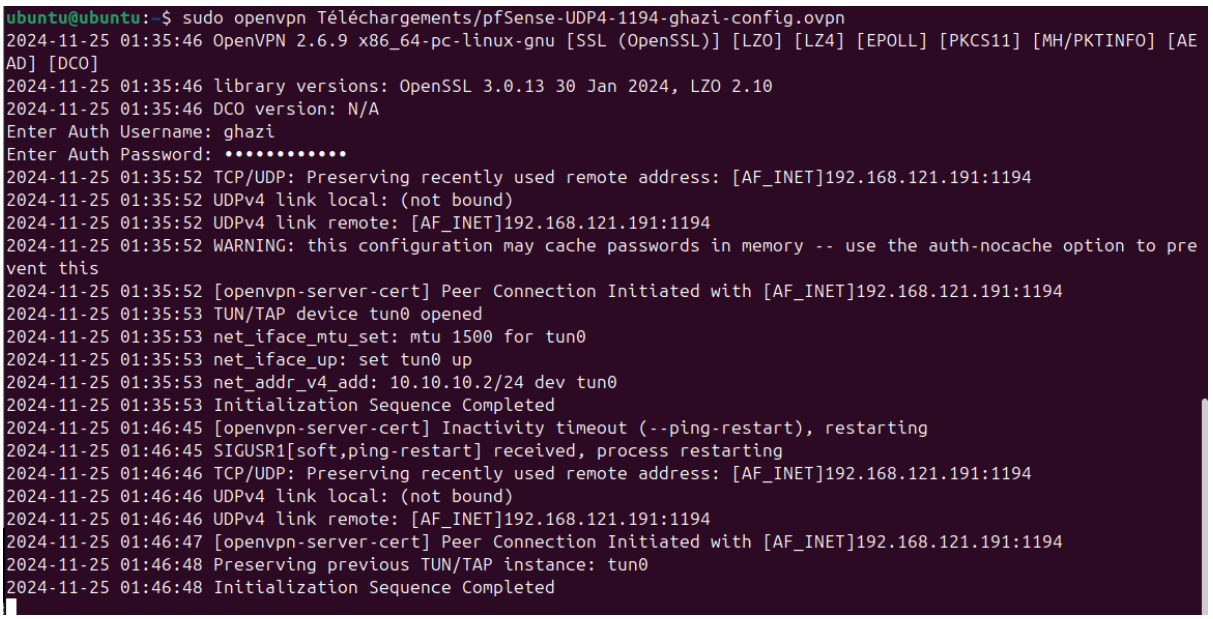
Après avoir créé l'utilisateur, allez sur l'onglet *VPN→OpenVPN* puis sur l'onglet *Client Export*. dans la section *OpenVPN Clients* vous devriez trouver l'utilisateur que vous venez de créer.

Téléchargez le fichier de configuration (*Inline Configurations*, bouton *Most Clients*), puis copiez-le dans la VM Ubuntu située dans le NAT (Internet). L'extension du fichier est *.ovpn*



Maintenant, ouvrez un terminal dans votre machine client connectée au WAN, et activez le tunnel VPN à l'aide de la commande :

```
sudo openvpn <chemin vers le fichier de configuration téléchargé>
```



Vous devriez voir Initialization Sequence Completed !

Ouvrez un nouveau terminal et essayez de faire une connexion SSH vers la machine ubuntu située dans le LAN (172.16.10.20) :

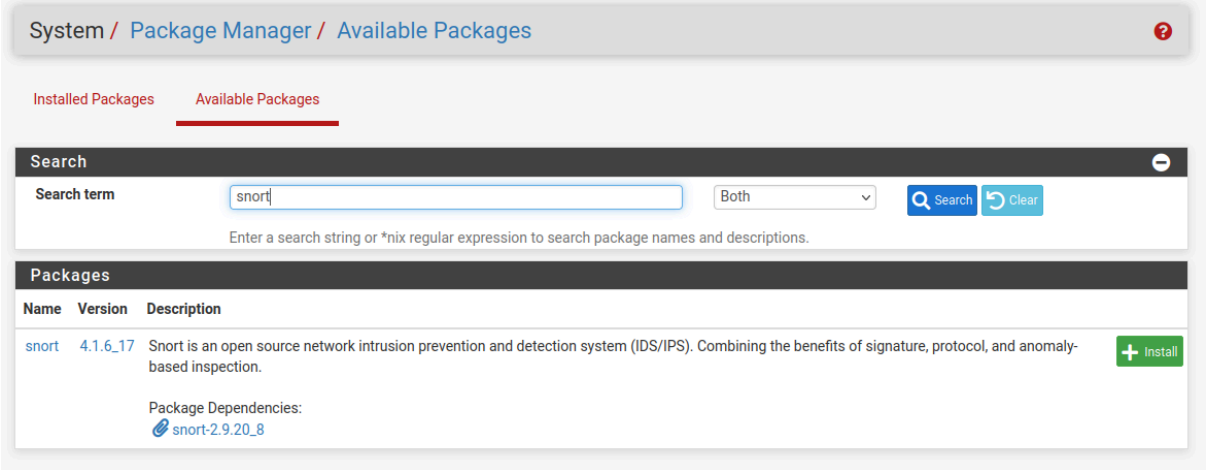
```
ssh infosec@172.16.10.20
```

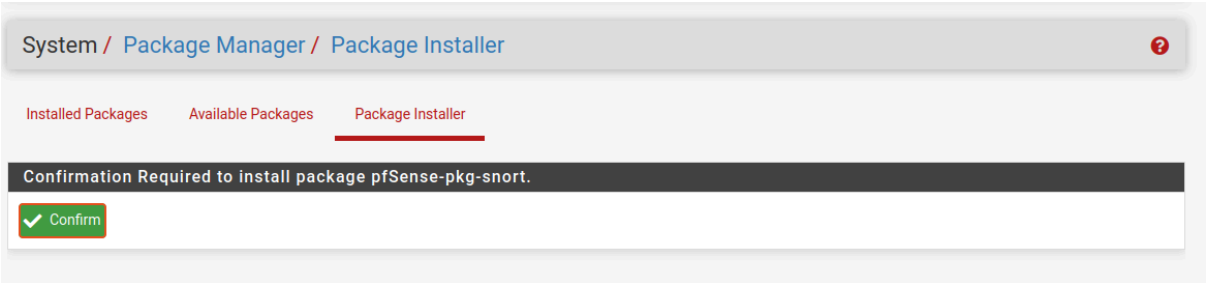
Si vous y êtes arrivés, bravo ! Appelez votre enseignant pour qu'il vous donne les points de cette partie.

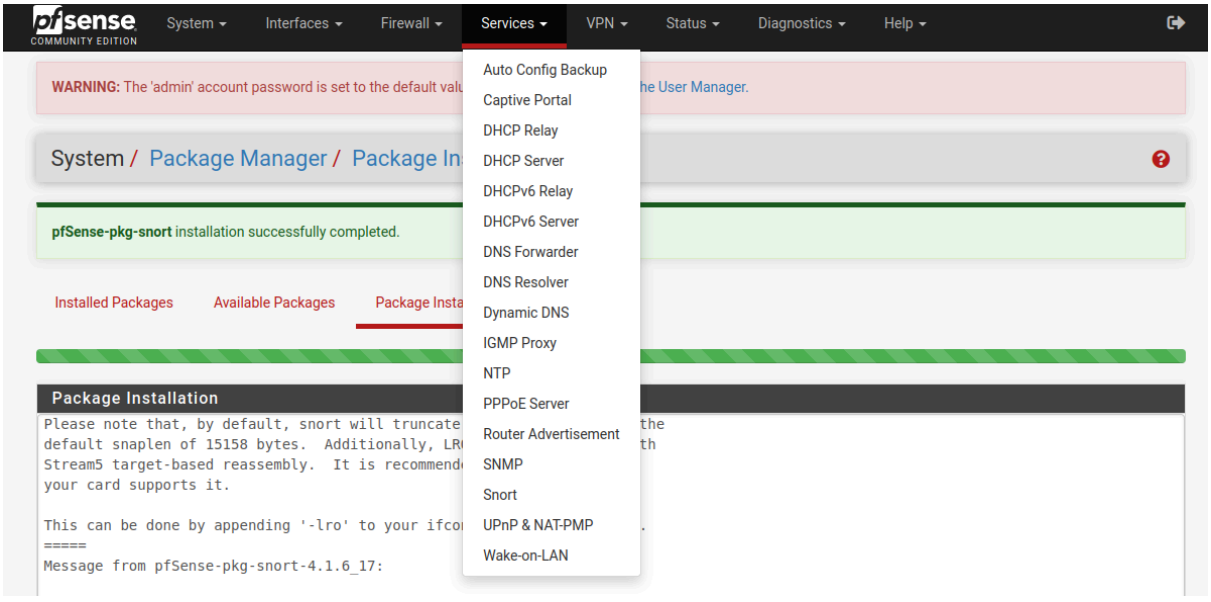
Partie III - Implémentation de règles snort

L'entreprise désire interdire l'accès à Facebook, Netflix et ChatGPT pour ses employés. Pour ce faire, vous décidez d'utiliser snort pour surveiller et bloquer le flux vers cette application.

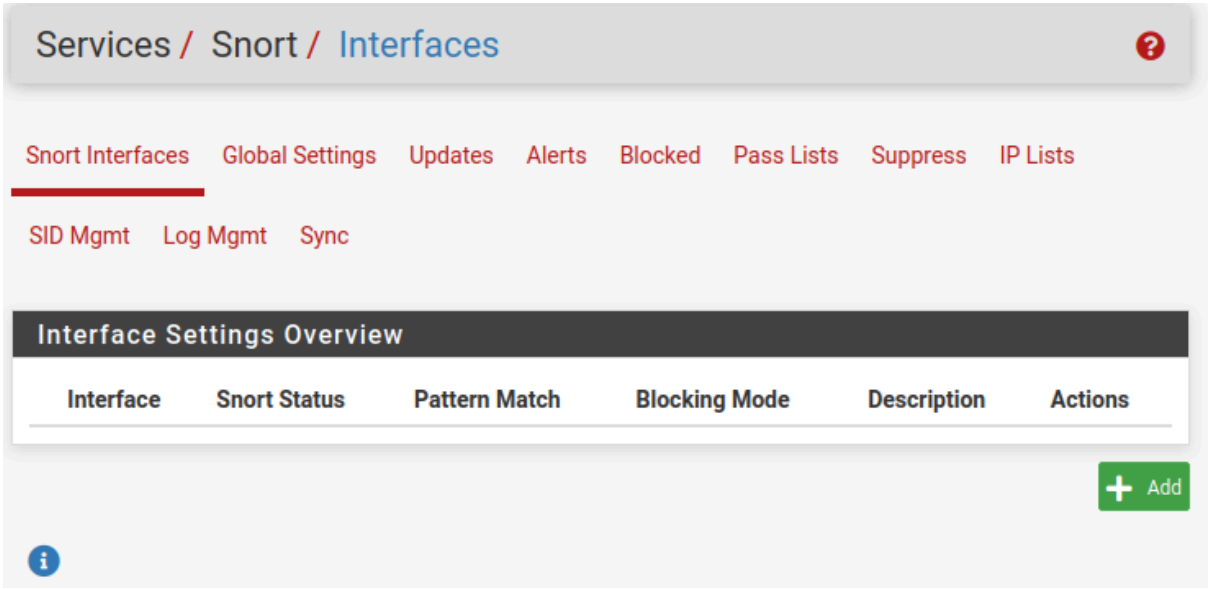
Installez snort (onglet *System→Package Manager→Available Packages*), confirmez l'installation. Une fois l'installation terminée, un nouvel onglet snort est disponible dans l'onglet *Services* de PfSense.

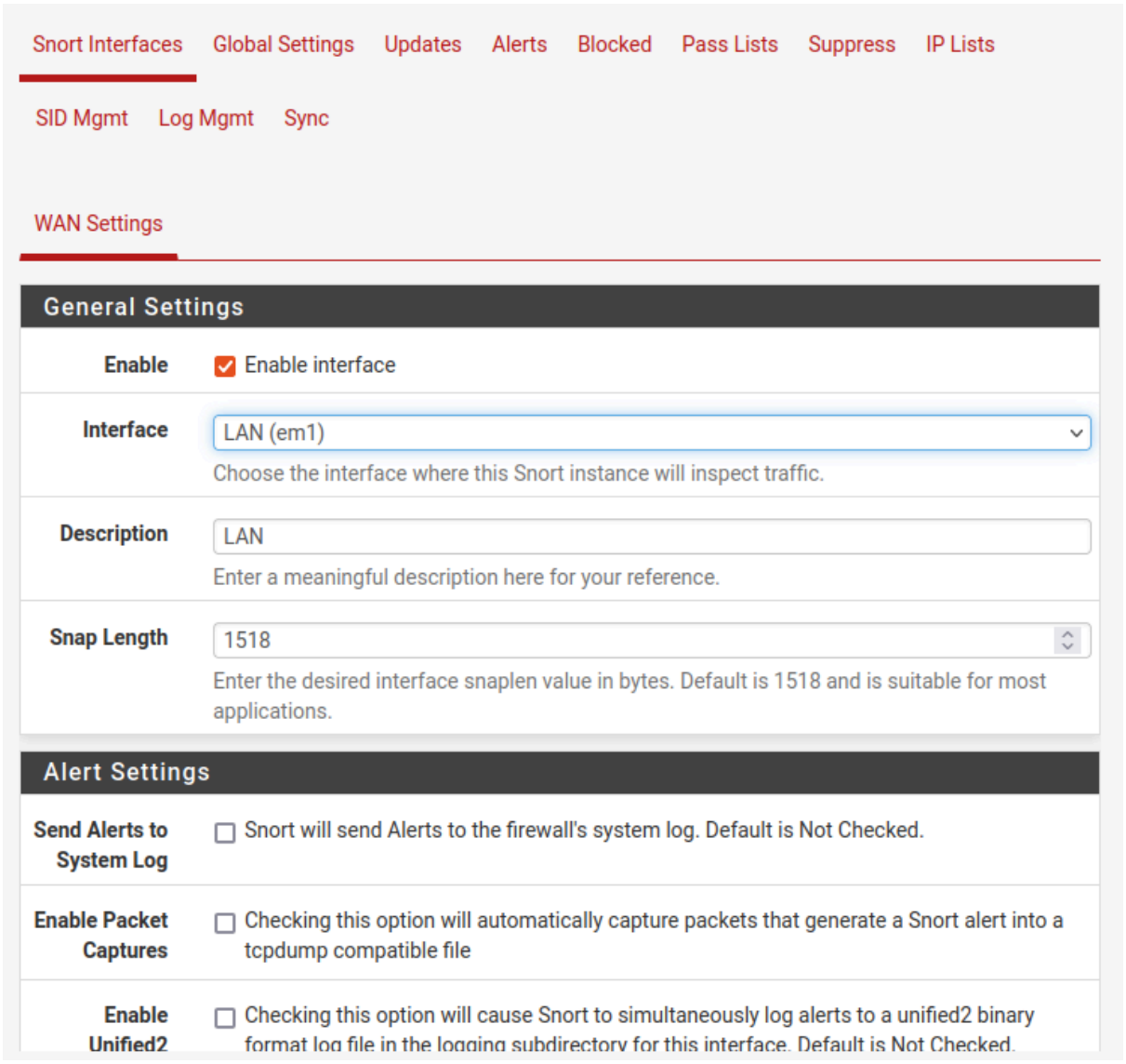

System / Package Manager / Available Packages
Installed Packages
Available Packages
Search
Search term
snort
Both
Search
Clear
Enter a search string or *nix regular expression to search package names and descriptions.
Packages
Name
Version
Description
snort
4.1.6_17
Snort is an open source network intrusion prevention and detection system (IDS/IPS). Combining the benefits of signature, protocol, and anomaly-based inspection.
Package Dependencies:
snort-2.9.20_8
Install


System / Package Manager / Package Installer
Installed Packages
Available Packages
Package Installer
Confirmation Required to install package pfSense-pkg-snort.
Confirm


pfsense
COMMUNITY EDITION
System
Interfaces
Firewall
Services
VPN
Status
Diagnostics
Help
Auto Config Backup
Captive Portal
DHCP Relay
DHCP Server
DHCPv6 Relay
DHCPv6 Server
DNS Forwarder
DNS Resolver
Dynamic DNS
IGMP Proxy
NTP
PPPoE Server
Router Advertisement
SNMP
Snort
UPnP & NAT-PMP
Wake-on-LAN
WARNING: The 'admin' account password is set to the default valu
he User Manager.
System / Package Manager / Package In
pfSense-pkg-snort installation successfully completed.
Installed Packages
Available Packages
Package Insta
Package Installation
Please note that, by default, snort will truncate
the
default snaplen of 15158 bytes. Additionally, LR
th
Stream5 target-based reassembly. It is recommend
your card supports it.
This can be done by appending '-lro' to your ifco
=====
Message from pfSense-pkg-snort-4.1.6_17:

Dans l'onglet Snort, volet Snort Interfaces, ajoutez une interface (bouton *Add*) sur laquelle vous allez analyser les flux. Dans notre cas c'est l'interface LAN.





Block Settings

Block Offenders

☐ Checking this option will automatically block hosts that generate a Snort alert. Default is Not Checked.

Detection Performance Settings

Search Method

AC-BNFA

Choose a fast pattern matcher algorithm. Default is AC-BNFA.

Split ANY-ANY

☐ Enable splitting of ANY-ANY port group. Default is Not Checked.

Search Optimize

☐ Enable search optimization. Default is Not Checked.

Stream Inserts

☐ Do not evaluate stream inserted packets against the detection engine. Default is Not Checked.

Checksum Check Disable

☐ Disable checksum checking within Snort to improve performance. Default is Not Checked.

Choose the Networks Snort Should Inspect and Whitelist

Home Net

default — View List

Choose the Home Net you want this interface to use.

Default Home Net adds only local networks, WAN IPs, Gateways, VPNs and VIPs.
Create an Alias to hold a list of friendly IPs that the firewall cannot see or to customize the default Home Net.

External Net

default — View List

Choose the External Net you want this interface to use.

External Net is networks that are not Home Net. Most users should leave this setting at default.
Create a Pass List and add an Alias to it, and then assign the Pass List here for custom External Net settings.

Choose a Suppression or Filtering List (Optional)

Alert Suppression and Filtering

default — View List

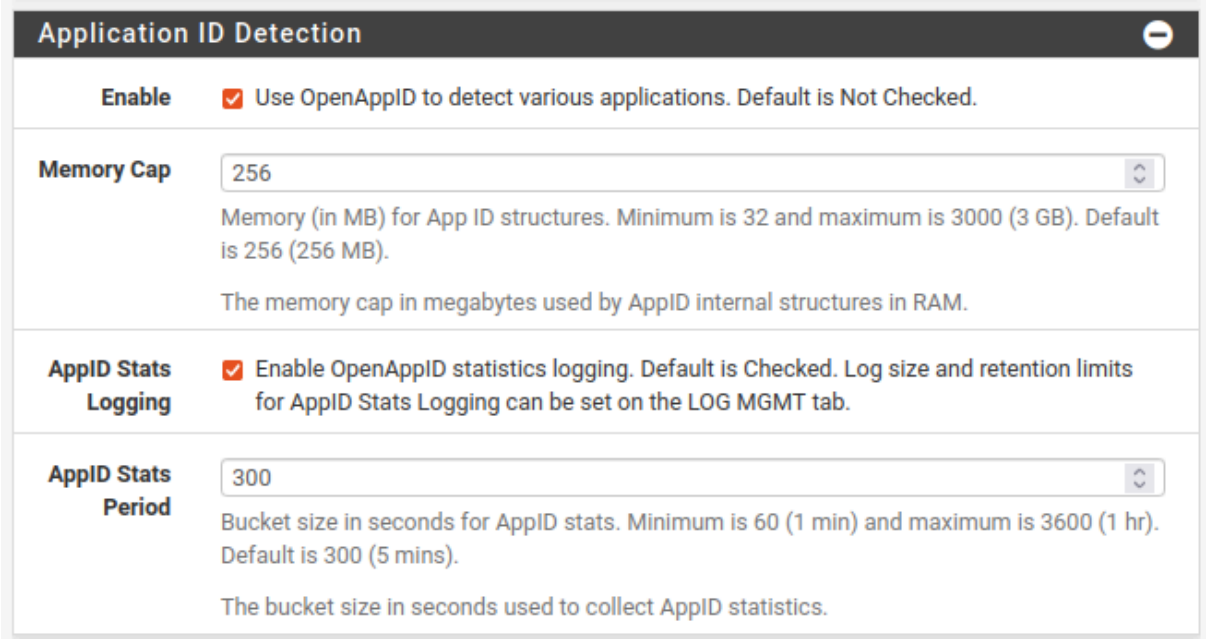
Choose the suppression or filtering file you want this interface to use.

Custom Configuration Options

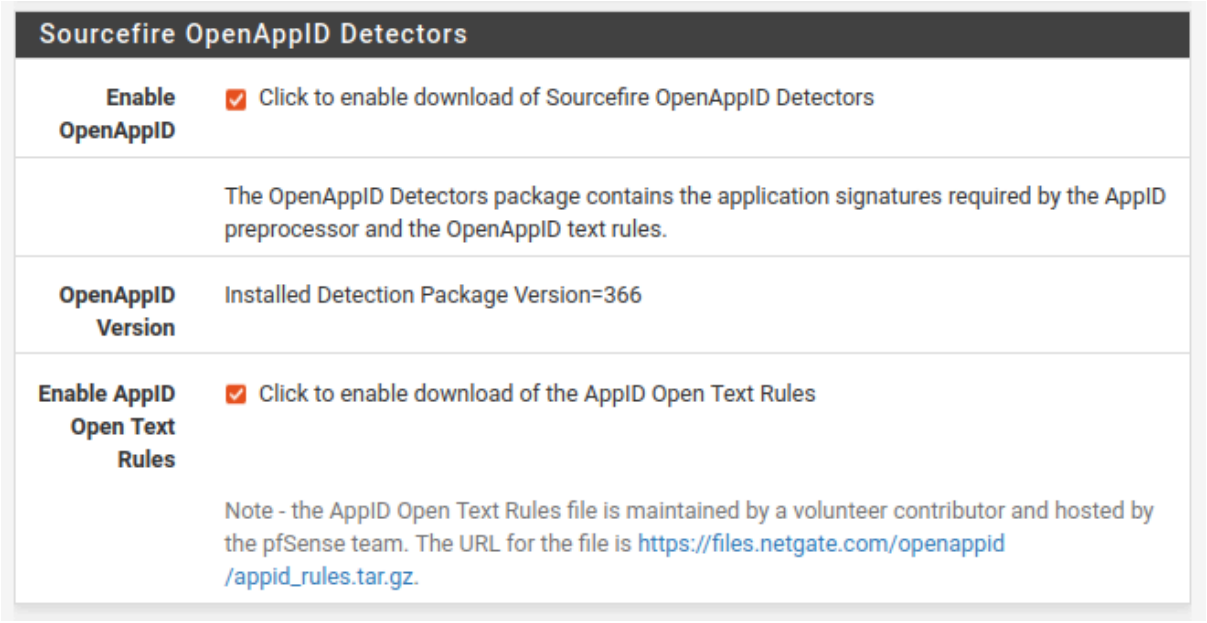
Advanced

Enregistrez les changements puis allez sur l'onglet *LAN Preprocs*.

Dans la section *Application ID Detection*, Activez OpenAppID pour détecter les applications :



Enregistrez les changements, puis allez dans Global Settings.
Dans la section *Sourcefire OpenAppID Detectors* activez *OpenAppId* pour détecter le trafic des applications :



Enfin, repartez dans *Snort Interfaces* et activez l'interface pour commencer à écouter.

Maintenant, votre rôle est de mettre en place quelques règles :

- Une règle pour alerter lorsqu'une requête ping est lancée dans une des machines dans le LAN.
- Une règle pour alerter lorsqu'une machine du LAN se connecte à Facebook,
- Une règle pour alerter lorsqu'une machine du LAN se connecte à Netflix,
- Une règle pour alerter lorsqu'une machine du LAN se connecte à ChatGPT

Vous pouvez vous aider du site suivant (ou demander de l'aide à votre enseignant) :

https://forum.netgate.com/topic/183210/guide-snort-s-appid-custom-rules-quick-guide-to-blocking-example-shows-openai-chatgpt-or-itunes

Après avoir observé les alertes, changez le comportement de snort pour qu'il change du mode Détection d'intrusion (IDS) à prévention d'intrusion (IPS) en bloquant le trafic vers Facebook, Netflix et ChatGPT au lieu de seulement alerter sur ce trafic.

Demandez de l'aide à votre enseignant si jamais vous n'y arrivez pas.

Si vous avez terminé, bravo ! Appelez votre enseignant pour qu'il vous donne les points pour cette partie.

Méthode d'évaluation

Pour chaque points mentionné dans la grille de correction ci-dessous, appelez votre enseignant pour lui montrer votre implémentation. Si votre implémentation fonctionne, il vous donnera les points associés à cette étape.

Grille de correction

	Points
Implémentation des règles de pare-feu - *Pour le LAN* - *Pour la DMZ*	 3 3
Bonne implémentation du port forwarding (le site web est accessible sur le WAN)	2
OpenVPN fonctionne	3
Implémentation de l'alerte Snort (ping)	1
Implémentation du blocage de l'application Facebook , Netflix et ChatGPT	3
TOTAL	**15**