

MASTER 2 INFORMATIQUE - CYBERSÉCURITÉ

---

## TP Cisco attaque architecture

---

**Abdel-Malik FOFANA**

**ID: 22218511**

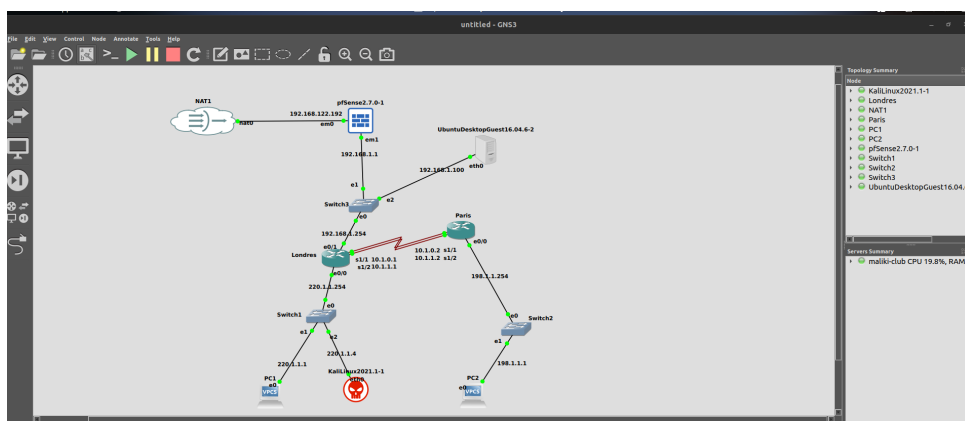
November 1, 2024

## Contents

|          |                                                    |          |
|----------|----------------------------------------------------|----------|
| <b>1</b> | <b>Architecture du reseau</b>                      | <b>2</b> |
| <b>2</b> | <b>Configuration des Routeurs pour l'InterVLAN</b> | <b>2</b> |
| 2.1      | Routeur Londres . . . . .                          | 2        |
| 2.2      | Routeur Paris . . . . .                            | 3        |
| 2.3      | Configuration des Postes de Travail . . . . .      | 4        |
| <b>3</b> | <b>Configuration du firewall PFsense</b>           | <b>5</b> |
| <b>4</b> | <b>Attaque ddos</b>                                | <b>6</b> |
| <b>5</b> | <b>Installation ids/ips snort</b>                  | <b>8</b> |

# 1 Architecture du reseau

Voici l'architecture du reseau



| Device         | Interface                 | IP Address / Connection Details                                                          |
|----------------|---------------------------|------------------------------------------------------------------------------------------|
| pfSense        | WAN (em0)<br>LAN (em1)    | 192.168.122.192<br>192.168.1.1                                                           |
| Ubuntu         | e2                        | 192.168.1.100 (Connected to switch with connection to Londres via e0/1 at 192.168.1.254) |
| Switch 1       | Connected to Londres      | e0/1, IP: 192.168.1.254                                                                  |
| Switch 2       | Connected to Londres      | e0/0, IP: 220.1.1.254                                                                    |
| PC1            | Connected to Switch 2     | 220.1.1.1                                                                                |
| Kali           | Connected to Switch 2     | 220.1.1.4                                                                                |
| Router Londres | Serial Interfaces         | s1/1: 10.1.0.1 to 10.1.0.2 (Paris); s1/2: 10.1.1.1 to 10.1.1.2 (Paris)                   |
| Router Paris   | Serial Interfaces         | s1/1: 10.1.0.2 to 10.1.0.1 (Londres); s1/2: 10.1.1.2 to 10.1.1.1 (Londres)               |
| Switch 3       | Connected to Router Paris | e0/0, IP: 198.1.1.254                                                                    |
| PC2            | Connected to Switch 3     | 198.1.1.1                                                                                |

## 2 Configuration des Routeurs pour l'InterVLAN

### 2.1 Routeur Londres

Pour le routeur Londres, nous configurons les interfaces série et Ethernet. Les interfaces série connectent Londres à Paris et aux autres réseaux, tandis que l'interface Ethernet connecte Londres aux appareils du réseau local (LAN) 220.1.1.0/24.

#### conf terminal

```
\! Interface serie 1/1 : Connexion vers Paris
interface serial 1/1
ip address 10.1.0.1 255.255.255.0
clock rate 19000
```

```
description vers DEC
no shutdown
exit

\! Interface serie 1/2 : Autre connexion serie
interface serial 1/2
ip address 10.1.1.1 255.255.255.0
clock rate 19000
description vers DEC
no shutdown
exit

\! Interface Ethernet0/0 : Connexion LAN de Londres
interface Ethernet0/0
ip address 220.1.1.254 255.255.255.0
no shutdown
exit

\! Route statique pour atteindre le reseau distant de Paris
ip route 198.1.1.0 255.255.255.0 10.1.0.2
exit

\! Sauvegarde de la configuration active
copy running-config startup-config

\! Affiche l'etat des interfaces pour verifier la configuration
show ip interface brief
```

## 2.2 Routeur Paris

Sur le routeur Paris, nous configurons également deux interfaces série et une interface Ethernet. Les interfaces série relient Paris à Londres et aux autres réseaux, et l'interface Ethernet connecte Paris au réseau local 198.1.1.0/24.

```
conf terminal
\! Interface serie 1/1 : Connexion vers Londres
interface serial 1/1
ip address 10.1.0.2 255.255.255.0
clock rate 19000
description vers DEC
no shutdown
```

**exit**

```
\! Interface serie 1/2 : Autre connexion srrie
```

**interface** serial 1/2

**ip** address 10.1.1.2 255.255.255.0

**clock rate** 19000

description vers DEC

**no shutdown**

**exit**

```
\! Interface Ethernet0/0 : Connexion LAN de Paris
```

**interface** Ethernet0/0

**ip** address 198.1.1.254 255.255.255.0

**no shutdown**

**exit**

```
\! Route statique pour atteindre le reseau distant de Londres
```

**ip route** 220.1.1.0 255.255.255.0 10.1.0.1

**exit**

```
\! Sauvegarde de la configuration active
```

**copy** running-config startup-config

## 2.3 Configuration des Postes de Travail

Chaque poste de travail est configuré avec une adresse IP dans son réseau respectif et une passerelle par défaut, qui pointe vers l'interface Ethernet de son routeur.

- **PC1 (réseau de Londres)** : Ce PC utilise une adresse IP dans le sous-réseau 220.1.1.0/24 avec la passerelle configurée sur le routeur Londres.

**ip** 220.1.1.1/24

**gateway** 220.1.1.254

- **PC2 (réseau de Paris)** : Ce PC utilise une adresse IP dans le sous-réseau 198.1.1.0/24 avec la passerelle configurée sur le routeur Paris.

**ip** 198.1.1.1/24

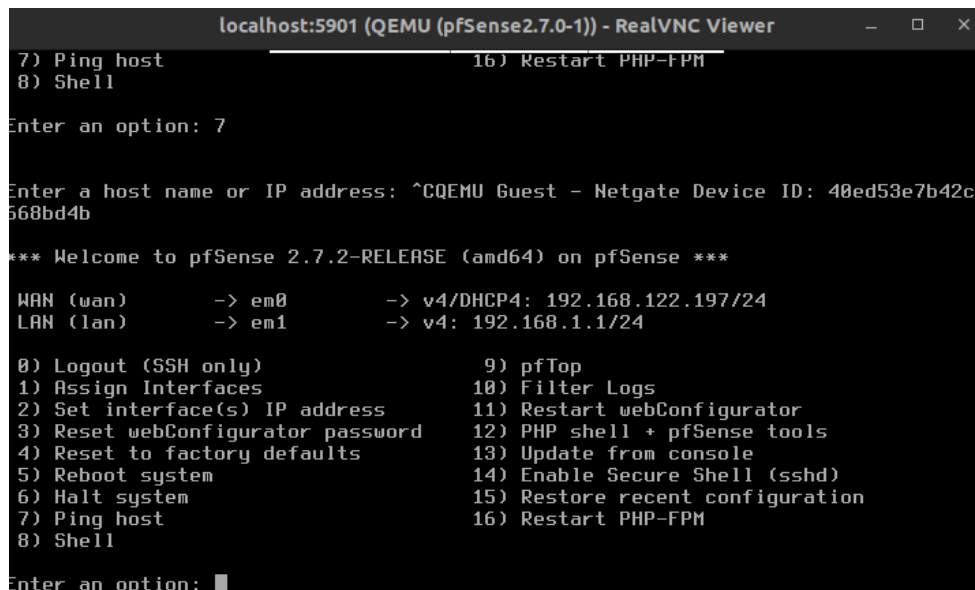
**gateway** 198.1.1.254

- **kali (réseau de Londres)** : les commandes Linux ajoutent une adresse IP et une route par défaut pour la connexion au réseau de Paris.

**sudo ip addr add** 220.1.1.4/24 **dev** eth0

```
sudo ip route add default via 220.1.1.254 dev eth0
```

### 3 Configuration du firewall PfSense



```
localhost:5901 (QEMU (pfSense2.7.0-1)) - RealVNC Viewer
7) Ping host
8) Shell

Enter an option: 7

Enter a host name or IP address: ^CQEMU Guest - Netgate Device ID: 40ed53e7b42c
568bd4b

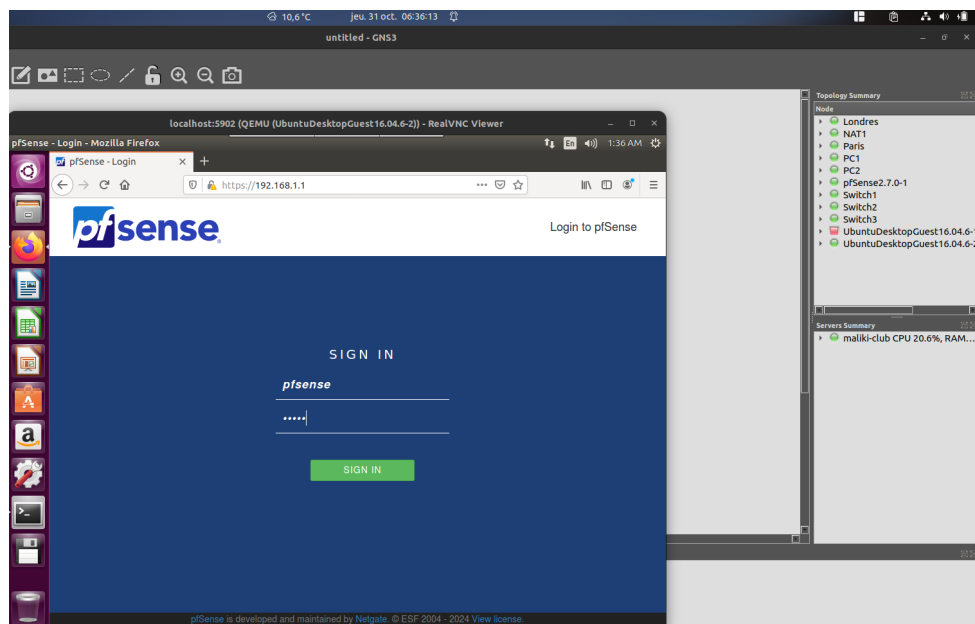
*** Welcome to pfSense 2.7.2-RELEASE (amd64) on pfSense ***

WAN (wan)      -> em0      -> v4/DHCP4: 192.168.122.197/24
LAN (lan)      -> em1      -> v4: 192.168.1.1/24

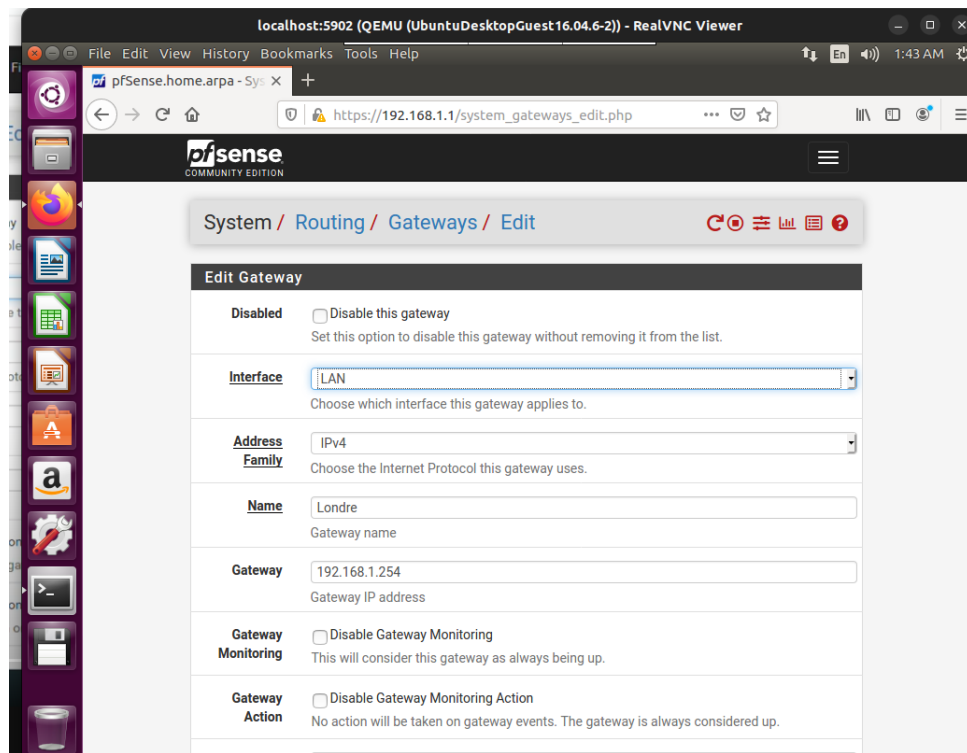
0) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults  13) Update from console
5) Reboot system              14) Enable Secure Shell (sshd)
6) Halt system                 15) Restore recent configuration
7) Ping host                   16) Restart PHP-FPM
8) Shell

Enter an option: 
```

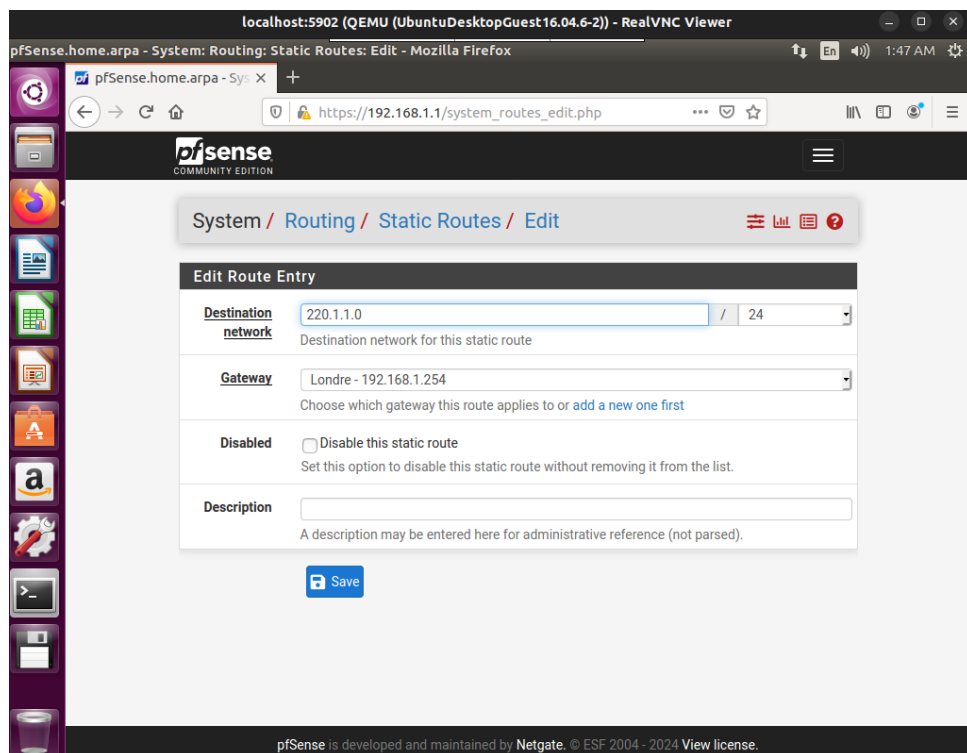
On installe pfsense



On se connecte au panel admin



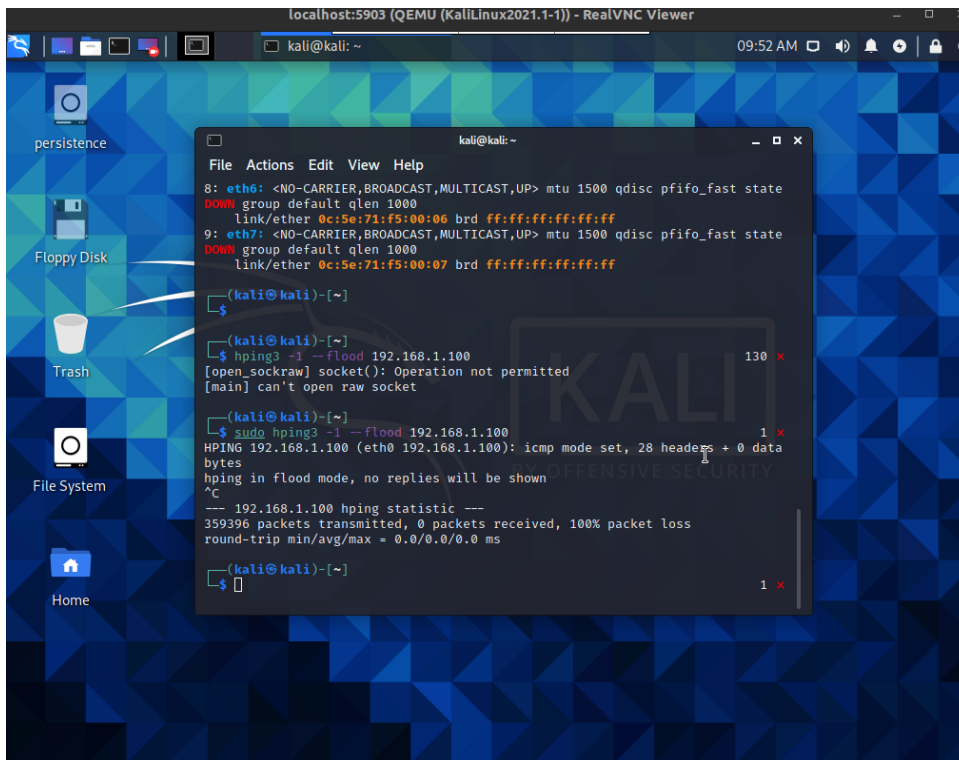
On configure la gateways 192.168.1.254



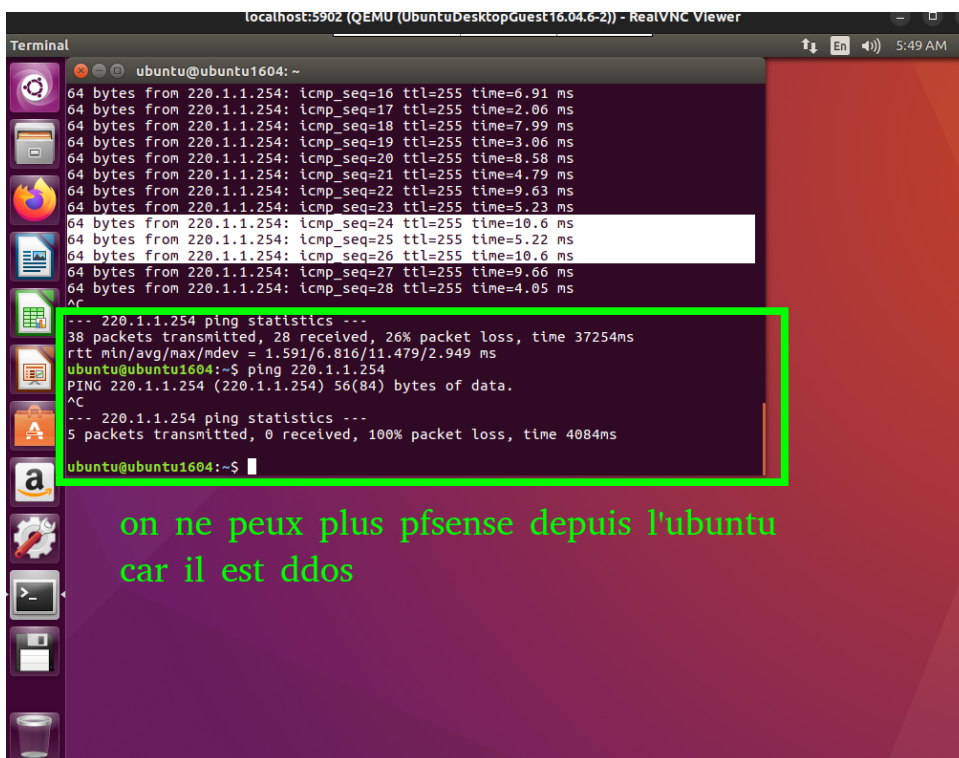
Et on ajoute la route statique vers le pc1 (vers Londres)

## 4 Attaque ddos

On fait le ddos via kali linux (londre 220.1.1.4)



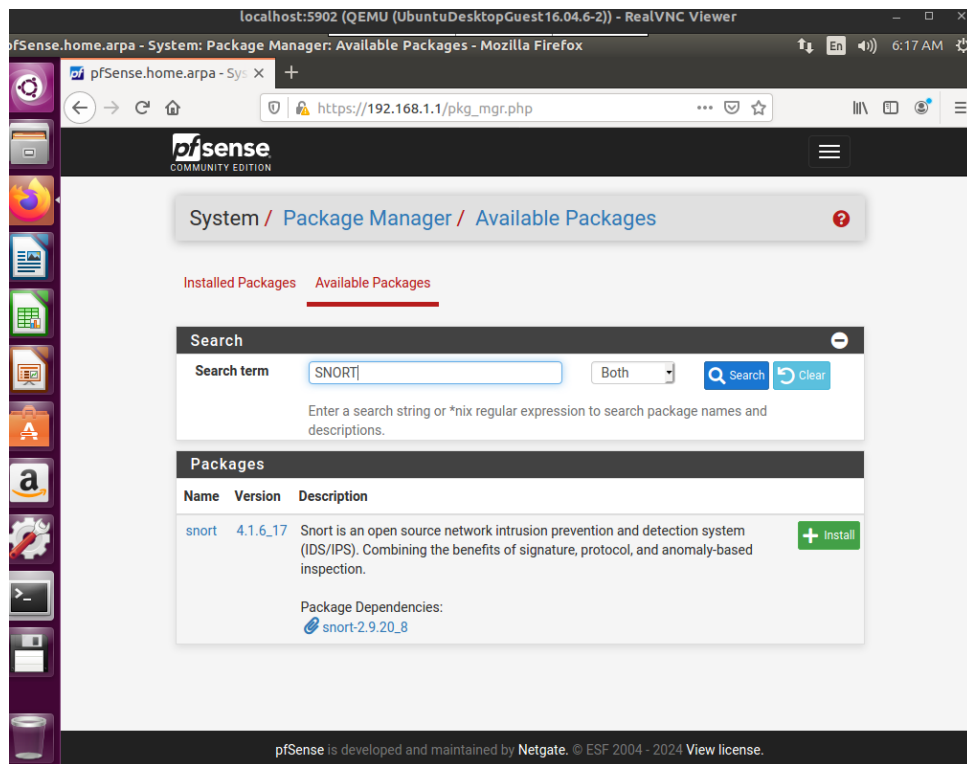
résultat après ddos



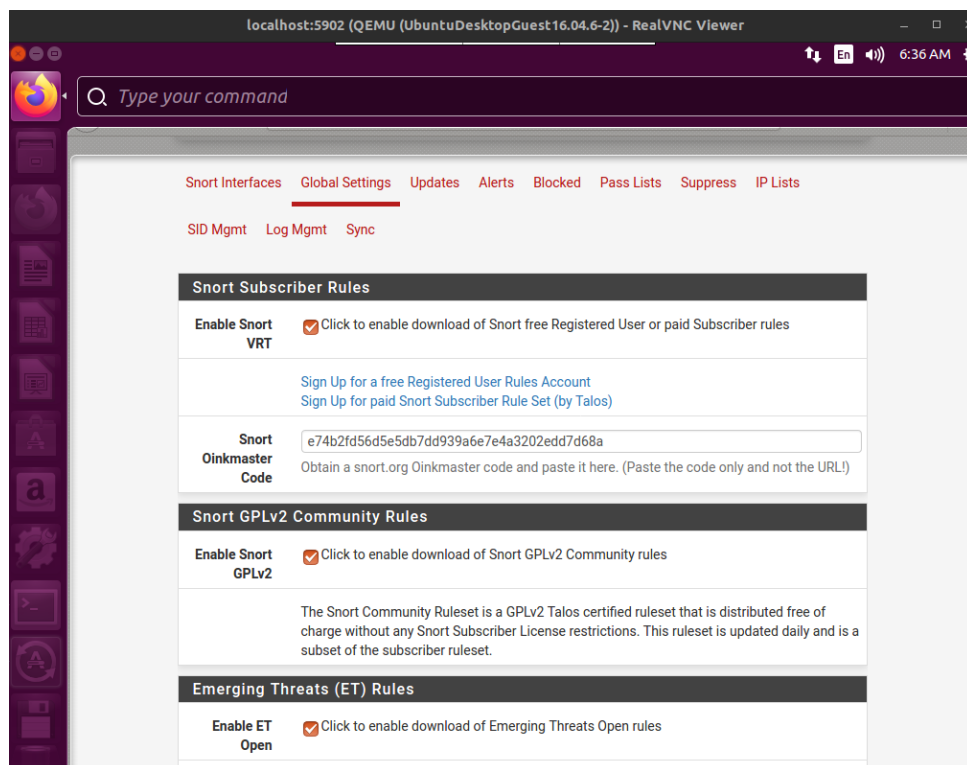
On ne peut plus ping pfsense (192.168.1.1) depuis l'ubuntu car il est ddos



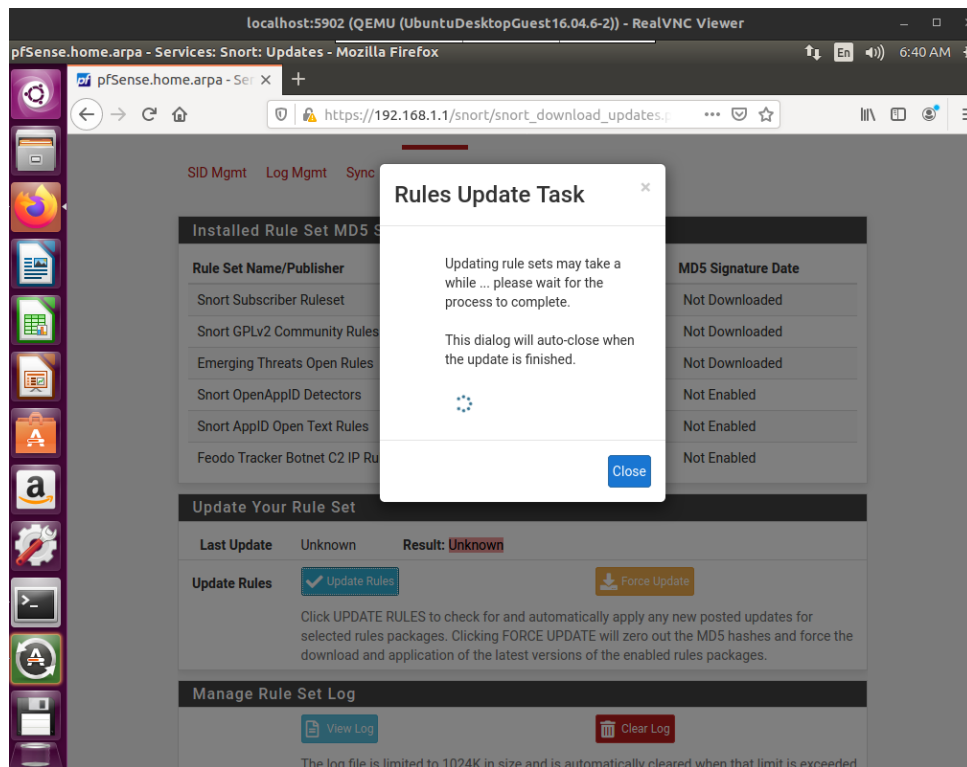
## 5 Installation ids/ips snort



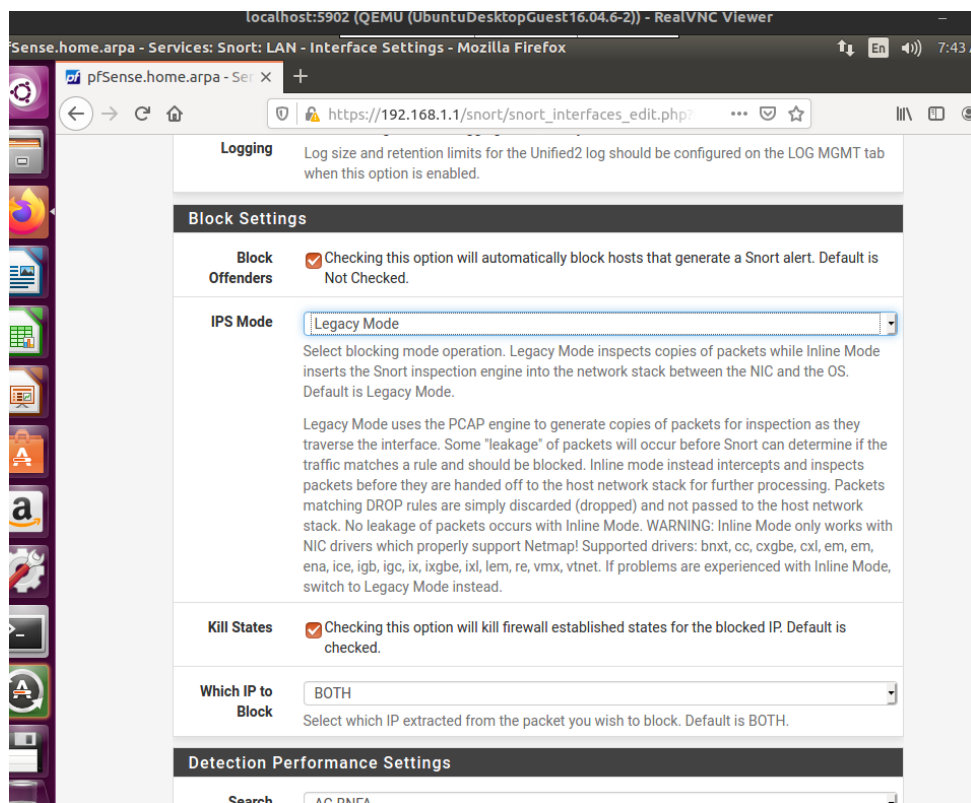
On initialise snort



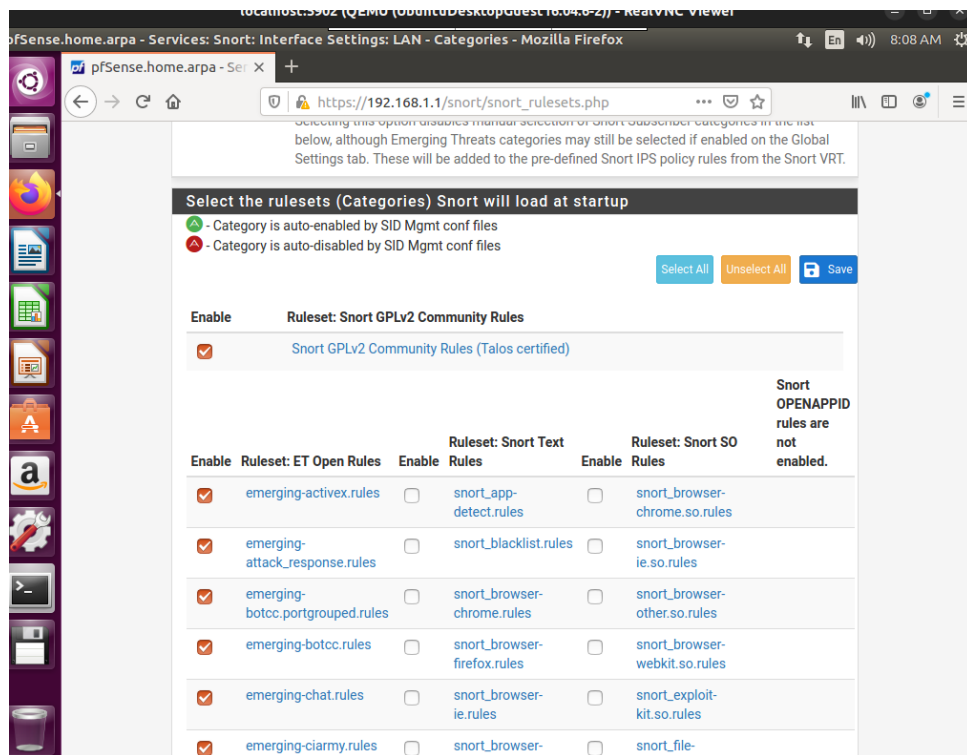
On ajoute la code snort



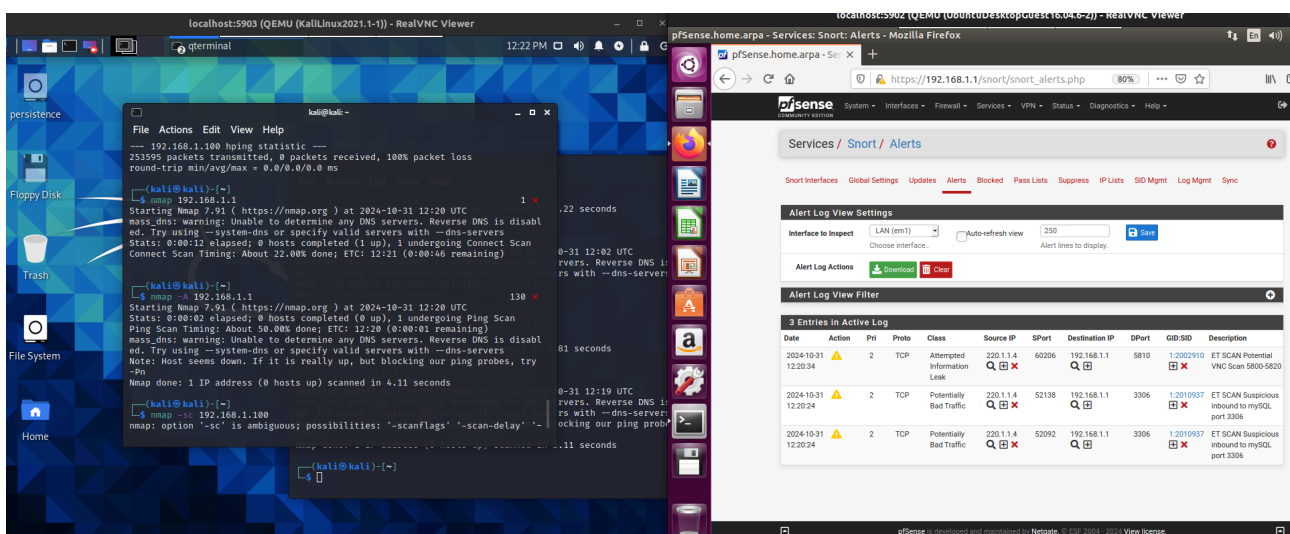
On fait une update



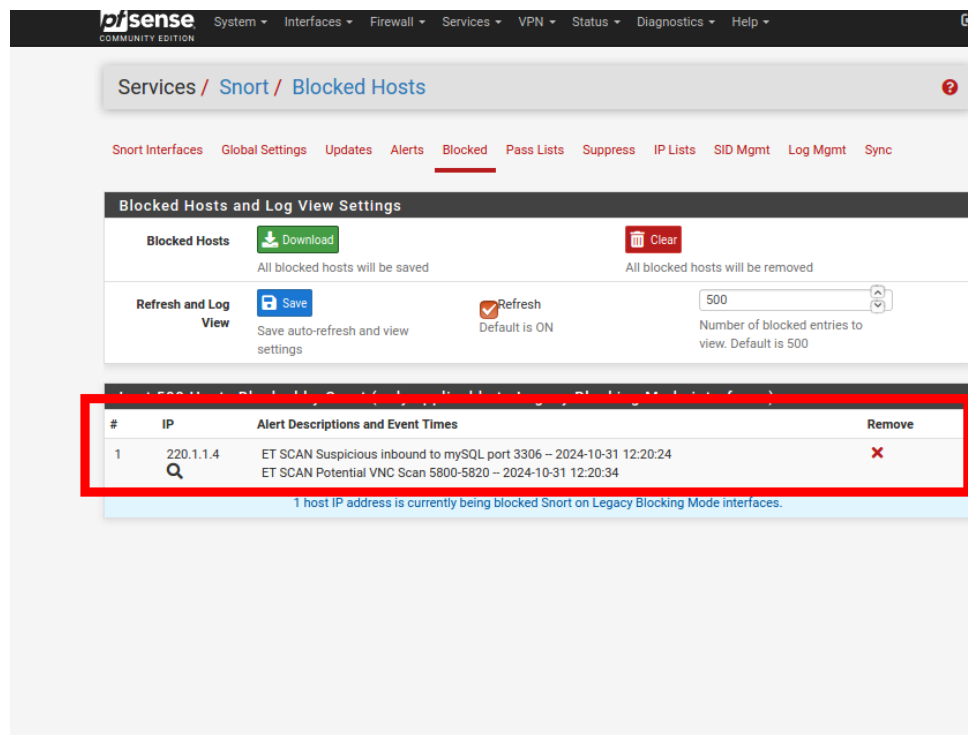
On active l'ids sur l'interface LAN et en prime on active un ips en plus de l'ids



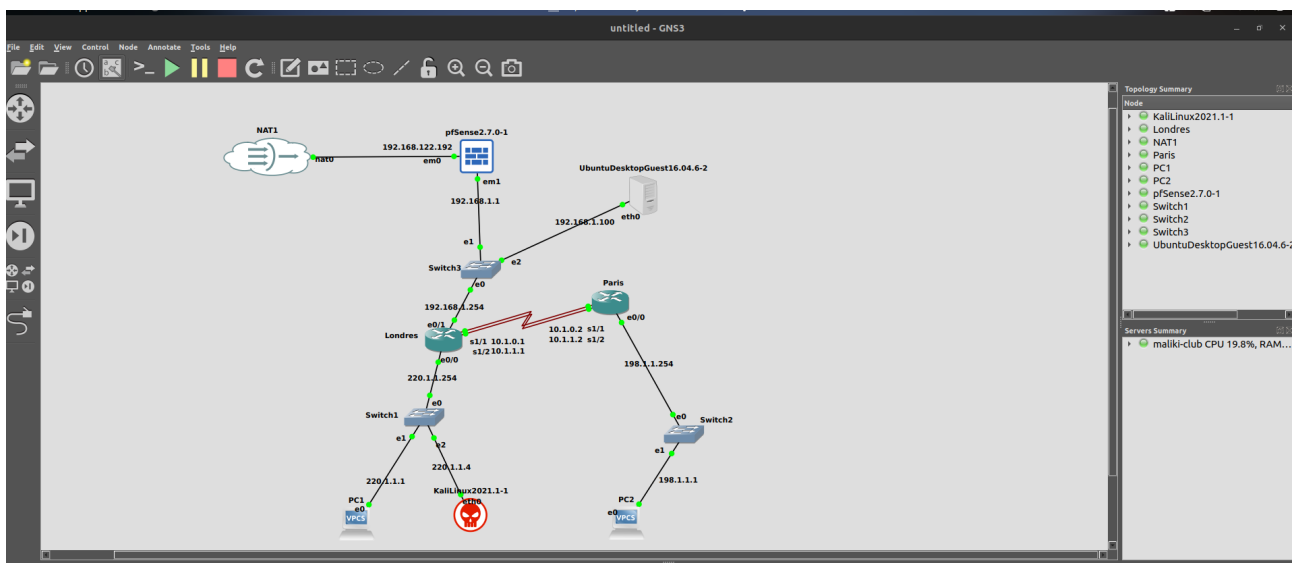
On ajoute des regles



On re-attaque et on voit que snort a reperer l'attaque nmap et que l'utilisateur ne peut plus faire de nmap car il est bloquer automatiquement par snort



Et l'ip de notre attaquant 220.1.1.4 est banni



Voila notre architecture intervlan + ids /ips fonctionne