**Projet de fin d'année**

Thème

# Mise en place d'une architecture réseau avec des fonctionnalités avancées et de haute disponibilité

Résultats des tests

**Spécialité** : Infrastructure et système d'information & cybersécurité


## Présenté par :

- TAGUEMOUNT Kamelia
- N'GORAN Sonia
- BENTO HATCHA Alvan Jetser

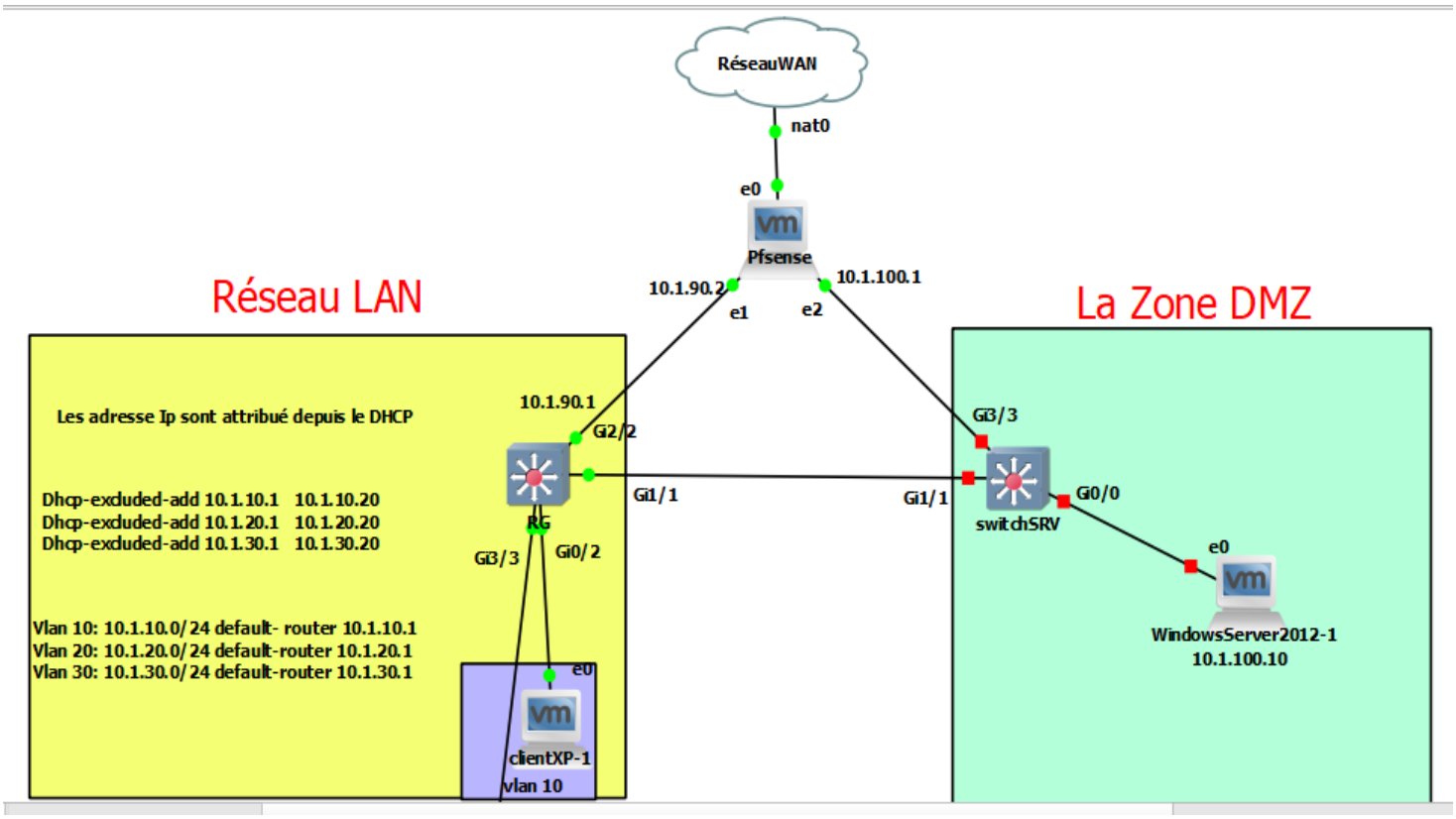

Année : 2020/2021

# Table des matières

1.1 La mise en place des Vlans : ..... 2
1.1.1 Le routage inter-Vlans : ..... 2
1.2 La mise en place de firewall : ..... 4
1.3 La mise en place de la DMZ : ..... 6
1.4 Mise en place des règles de filtrage : ..... 7
1.4.1 La zone DMZ : ..... 7
1.4.2 La Zone LAN : ..... 7
1.4.3 La zone WAN : ..... 8
1.5 Mise en place de portail captif sur le réseau LAN : ..... 8
1.6 Installation et configuration de honeypot : ..... 10
1.7 Mise en place de la stratégie de sauvegarde de la configuration réseau : 12
1.8 Mise en place du système de détection d'intrusion : ..... 14
1.9 Mise en place du SOC : ..... 16
1.10 Mise en place de la redondance réseau : ..... 16
1.10.1 Redondance pfsense : ..... 17
1.10.2 Redondance des serveurs : ..... 18

# 1 Maquette réseau GNS3 :

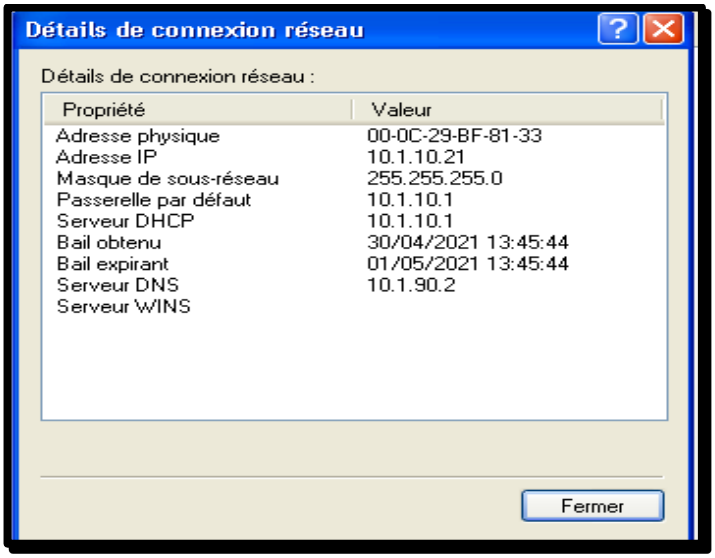
Cette image c'est notre maquette GNS3 sur le quelle on a travaillé et ou on a réaliser notre differents configuration.




# 2 La mise en place des VLANs :

## 2.1 Le routage inter-VLANs :

Après la mise en place des VLANs sur les switches et d'activer les DHCP sur le Switch RG (Répartiteur générale) on remarque les adresse IP du client sont attribué automatique avec le DHCP ci-dessous des captures d'écran :




La machine virtuelle client XP : appartient au vlan 10

```
PC2> show ip

NAME        : PC2[1]
IP/MASK     : 0.0.0.0/0
GATEWAY     : 0.0.0.0
DNS         :
MAC         : 00:50:79:66:68:01
LPORT       : 20111
RHOST:PORT  : 127.0.0.1:20112
MTU         : 1500
```

```
PC2> ip dhcp
DDORA IP 10.1.20.21/24 GW 10.1.20.1

PC2> show ip

NAME        : PC2[1]
IP/MASK     : 10.1.20.21/24
GATEWAY     : 10.1.20.1
DNS         : 10.1.90.2
DHCP SERVER : 10.1.20.1
DHCP LEASE  : 86391, 86400/43200/75600
```

Client Vlan 20

```
PC1> show ip

NAME        : PC1[1]
IP/MASK     : 10.1.10.22/24
GATEWAY     : 10.1.10.1
DNS         : 10.1.90.2
DHCP SERVER : 10.1.10.1
DHCP LEASE  : 86395, 86400/43200/75600
DOMAIN NAME : ens.isetsf.tn
MAC         : 00:50:79:66:68:00
LPORT       : 20113
RHOST:PORT  : 127.0.0.1:20114
MTU         : 1500
```

Pc client Vlan 10

```
PC3> show ip

NAME        : PC3[1]
IP/MASK     : 10.1.30.21/24
GATEWAY     : 10.1.30.1
DNS         : 10.1.90.2
DHCP SERVER : 10.1.30.1
DHCP LEASE  : 86362, 86400/43200/75600
DOMAIN NAME : sco.isetsf.tn
MAC         : 00:50:79:66:68:02
LPORT       : 20115
RHOST:PORT  : 127.0.0.1:20116
MTU         : 1500
```

Pc client Vlan 30

Après avoir effectué les différentes configurations sur les switches pour mettre en place le routage inter-vlan dans notre réseau pour que deux ordinateurs dans des diffèrent vlans peuvent se communiquer entre eux :

```
PC1> ping 10.1.20.21

84 bytes from 10.1.20.21 icmp_seq=1 ttl=63 time=342.731 ms
84 bytes from 10.1.20.21 icmp_seq=2 ttl=63 time=108.942 ms
84 bytes from 10.1.20.21 icmp_seq=3 ttl=63 time=198.170 ms
^C
PC1> ping 10.1.30.21

84 bytes from 10.1.30.21 icmp_seq=1 ttl=63 time=255.587 ms
84 bytes from 10.1.30.21 icmp_seq=2 ttl=63 time=163.143 ms
84 bytes from 10.1.30.21 icmp_seq=3 ttl=63 time=139.517 ms
^C
```

Les Ping de Vlan 10 vers les autre Pc client

```
PC2> ping 10.1.10.22

84 bytes from 10.1.10.22 icmp_seq=1 ttl=63 time=245.632 ms
84 bytes from 10.1.10.22 icmp_seq=2 ttl=63 time=321.309 ms
^C
PC2> ping 10.1.30.21

84 bytes from 10.1.30.21 icmp_seq=1 ttl=63 time=430.250 ms
84 bytes from 10.1.30.21 icmp_seq=2 ttl=63 time=117.124 ms
84 bytes from 10.1.30.21 icmp_seq=3 ttl=63 time=206.677 ms
^C
```

Ping de client Vlan 20 vers les autres clients

```
PC3> ping 10.1.10.22

84 bytes from 10.1.10.22 icmp_seq=1 ttl=63 time=164.729 ms
84 bytes from 10.1.10.22 icmp_seq=2 ttl=63 time=289.984 ms
^C
PC3> ping 10.1.20.21

84 bytes from 10.1.20.21 icmp_seq=1 ttl=63 time=225.839 ms
84 bytes from 10.1.20.21 icmp_seq=2 ttl=63 time=147.906 ms
84 bytes from 10.1.20.21 icmp_seq=3 ttl=63 time=172.667 ms
```

Ping client Vlan 30 vers les autres machines

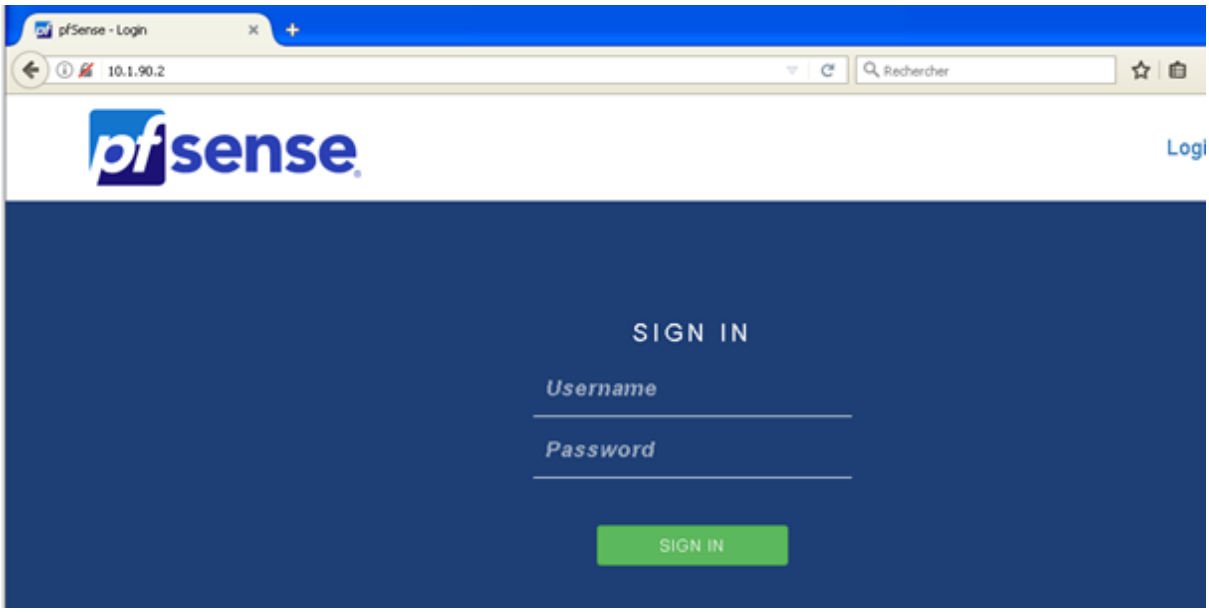
# 3 La mise en place de firewall :

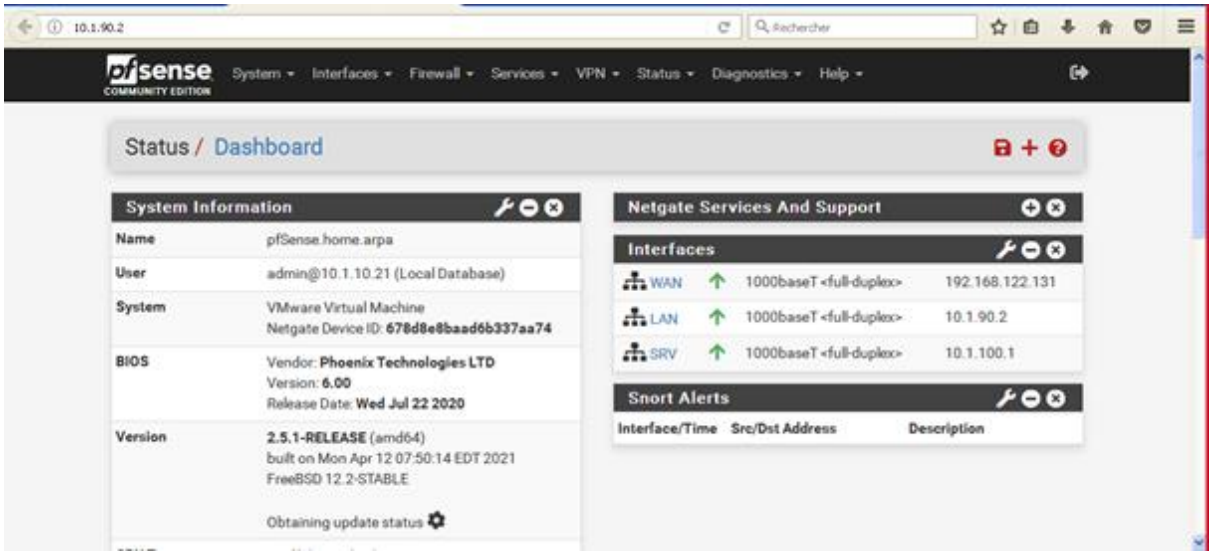
Dans cette partie on a choisi de travailler avec le firewall Pfsense, après les différentes configurations on peut accéder au Pfsense via la zone DMZ et le réseau LAN.

Ci-dessous des images qui illustre :

- Entre LAN et Pfsense :

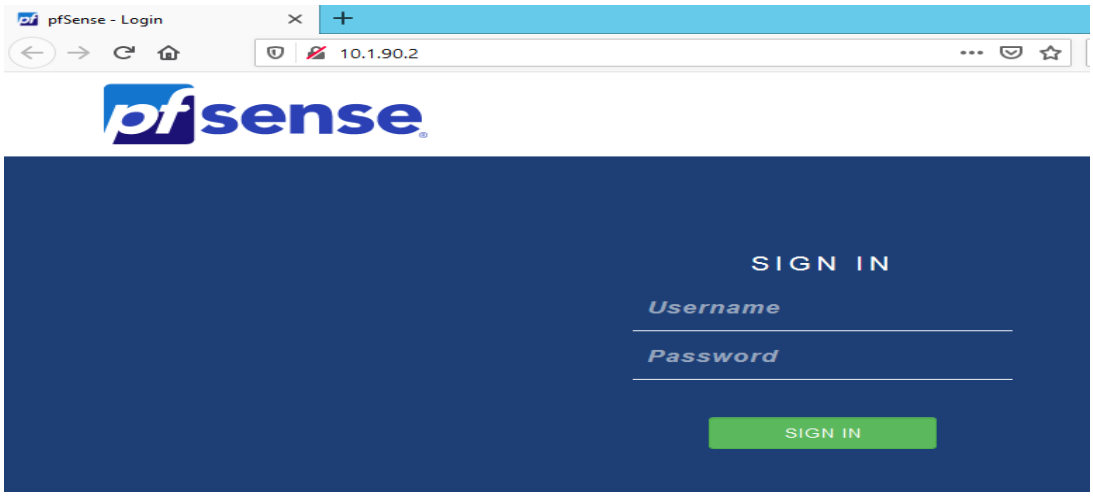
```
C:\Documents and Settings\Administrateur>ping 10.1.90.2

Envoi d'une requête 'ping' sur 10.1.90.2 avec 32 octets de données :

Réponse de 10.1.90.2 : octets=32 temps=85 ms TTL=63
Réponse de 10.1.90.2 : octets=32 temps=125 ms TTL=63
Réponse de 10.1.90.2 : octets=32 temps=100 ms TTL=63
Réponse de 10.1.90.2 : octets=32 temps=46 ms TTL=63

Statistiques Ping pour 10.1.90.2:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 46ms, Maximum = 125ms, Moyenne = 89ms

C:\Documents and Settings\Administrateur>_
```




- Entre la DMZ et le pfsense :

```
C:\Users\Administrateur>ping 10.1.90.2

Envoi d'une requête 'Ping'  10.1.90.2 avec 32 octets de données :
Réponse de 10.1.90.2 : octets=32 temps=80 ms TTL=64
Réponse de 10.1.90.2 : octets=32 temps=33 ms TTL=64
Réponse de 10.1.90.2 : octets=32 temps=38 ms TTL=64
Réponse de 10.1.90.2 : octets=32 temps=38 ms TTL=64

Statistiques Ping pour 10.1.90.2:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 33ms, Maximum = 80ms, Moyenne = 47ms
```



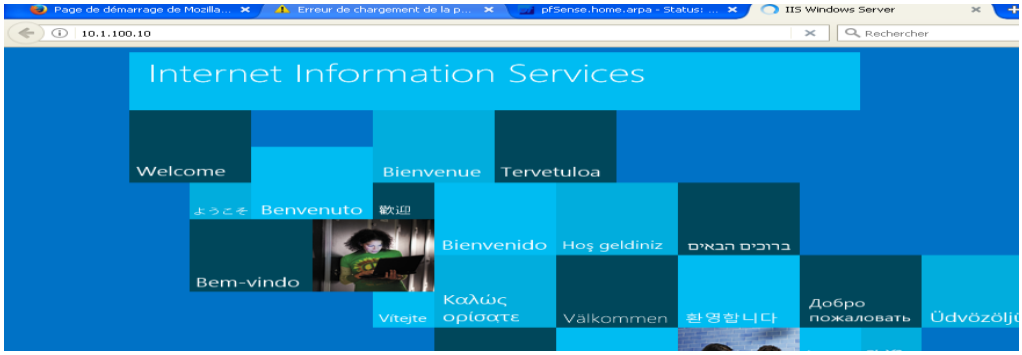

# 4 La mise en place de la DMZ :

Après la configuration de la zone sur le pfsense et la création des différents serveurs on peut accéder vers cette zone là depuis le Lan.

Ci-dessous une image qui illustrer cette partie-là :

```
C:\Documents and Settings\Administrateur>ping 10.1.100.1

Envoi d'une requête 'ping' sur 10.1.100.1 avec 32 octets de données :

Réponse de 10.1.100.1 : octets=32 temps=146 ms TTL=63
Réponse de 10.1.100.1 : octets=32 temps=75 ms TTL=63
Réponse de 10.1.100.1 : octets=32 temps=84 ms TTL=63
Réponse de 10.1.100.1 : octets=32 temps=52 ms TTL=63

Statistiques Ping pour 10.1.100.1:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 52ms, Maximum = 146ms, Moyenne = 89ms

C:\Documents and Settings\Administrateur>ping 10.1.100.10

Envoi d'une requête 'ping' sur 10.1.100.10 avec 32 octets de données :

Réponse de 10.1.100.10 : octets=32 temps=128 ms TTL=126
Réponse de 10.1.100.10 : octets=32 temps=77 ms TTL=126
Réponse de 10.1.100.10 : octets=32 temps=173 ms TTL=126
Réponse de 10.1.100.10 : octets=32 temps=89 ms TTL=126

Statistiques Ping pour 10.1.100.10:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 77ms, Maximum = 173ms, Moyenne = 116ms
```

Et on peut accéder vers la page web de notre serveur web depuis les pc client:



## 4.1 Mise en place des règles de filtrage :

Après la création des différentes zones sur notre pfsense, nous avons mis en place des règles de filtrage sur notre réseau.

### 4.1.1 La zone DMZ :

Dans la Zone DMZ on interdit l'accès vers le pfsense, et laisse passer tous vers cette zone.

- De la DMZ vers le pfsense

```
C:\Users\Administrateur>ping 10.1.90.2

Envoi d'une requête 'Ping'  10.1.90.2 avec 32 octets de données :
Délai d'attente de la demande dépassé.
Délai d'attente de la demande dépassé.
Délai d'attente de la demande dépassé.
Délai d'attente de la demande dépassé.

Statistiques Ping pour 10.1.90.2:
    Paquets : envoyés = 4, reçus = 0, perdus = 4 (perte 100%),
```

- De lan vers la DMZ :

```
C:\Documents and Settings\Administrateur>ping 10.1.100.10

Envoi d'une requête 'ping' sur 10.1.100.10 avec 32 octets de données :

Réponse de 10.1.100.10 : octets=32 temps=141 ms TTL=126
Réponse de 10.1.100.10 : octets=32 temps=82 ms TTL=126
Réponse de 10.1.100.10 : octets=32 temps=102 ms TTL=126
Réponse de 10.1.100.10 : octets=32 temps=84 ms TTL=126

Statistiques Ping pour 10.1.100.10:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 82ms, Maximum = 141ms, Moyenne = 102ms
```

### 4.1.2 La Zone LAN :

Dans cette zone on interdit l'accès depuis internet. Nous avons mis en place des règles pour que cette zone puisse accéder vers tous les réseaux.

- De WAN vers LAN :

```
C:\Users\PC>ping 10.1.90.2

Envoi d'une requête 'Ping'  10.1.90.2 avec 32 octets de données :
Délai d'attente de la demande dépassé.
Délai d'attente de la demande dépassé.
Délai d'attente de la demande dépassé.
Délai d'attente de la demande dépassé.

Statistiques Ping pour 10.1.90.2:
    Paquets : envoyés = 4, reçus = 0, perdus = 4 (perte 100%),
```

- De LAN vers tous les réseaux :

```
C:\Documents and Settings\Administrateur>ping 10.1.90.2

Envoi d'une requête 'ping' sur 10.1.90.2 avec 32 octets de données :

Réponse de 10.1.90.2 : octets=32 temps=1261 ms TTL=63
Réponse de 10.1.90.2 : octets=32 temps=887 ms TTL=63
Réponse de 10.1.90.2 : octets=32 temps=2210 ms TTL=63
Réponse de 10.1.90.2 : octets=32 temps=1031 ms TTL=63

Statistiques Ping pour 10.1.90.2:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 887ms, Maximum = 2210ms, Moyenne = 1347ms

C:\Documents and Settings\Administrateur>ping google.fr

Envoi d'une requête 'ping' sur google.fr [216.58.204.99] avec 32 octets de donné
es :

Réponse de 216.58.204.99 : octets=32 temps=205 ms TTL=111
Réponse de 216.58.204.99 : octets=32 temps=1483 ms TTL=111
Réponse de 216.58.204.99 : octets=32 temps=204 ms TTL=111
Réponse de 216.58.204.99 : octets=32 temps=1638 ms TTL=111

Statistiques Ping pour 216.58.204.99:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 204ms, Maximum = 1638ms, Moyenne = 882ms

C:\Documents and Settings\Administrateur>ping 8.8.8.8

Envoi d'une requête 'ping' sur 8.8.8.8 avec 32 octets de données :

Réponse de 8.8.8.8 : octets=32 temps=1449 ms TTL=111
Réponse de 8.8.8.8 : octets=32 temps=104 ms TTL=111
Réponse de 8.8.8.8 : octets=32 temps=75 ms TTL=111
Réponse de 8.8.8.8 : octets=32 temps=150 ms TTL=111

Statistiques Ping pour 8.8.8.8:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 75ms, Maximum = 1449ms, Moyenne = 444ms
```

### 4.1.3 La zone WAN :

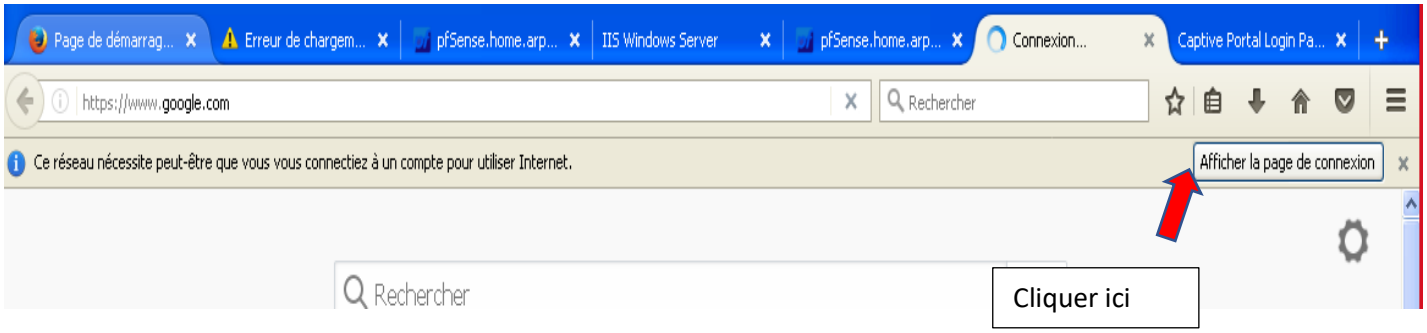
Pour l'interface WAN on n'a pas mis de règles.

# 5 Mise en place de portail captif sur le réseau LAN :

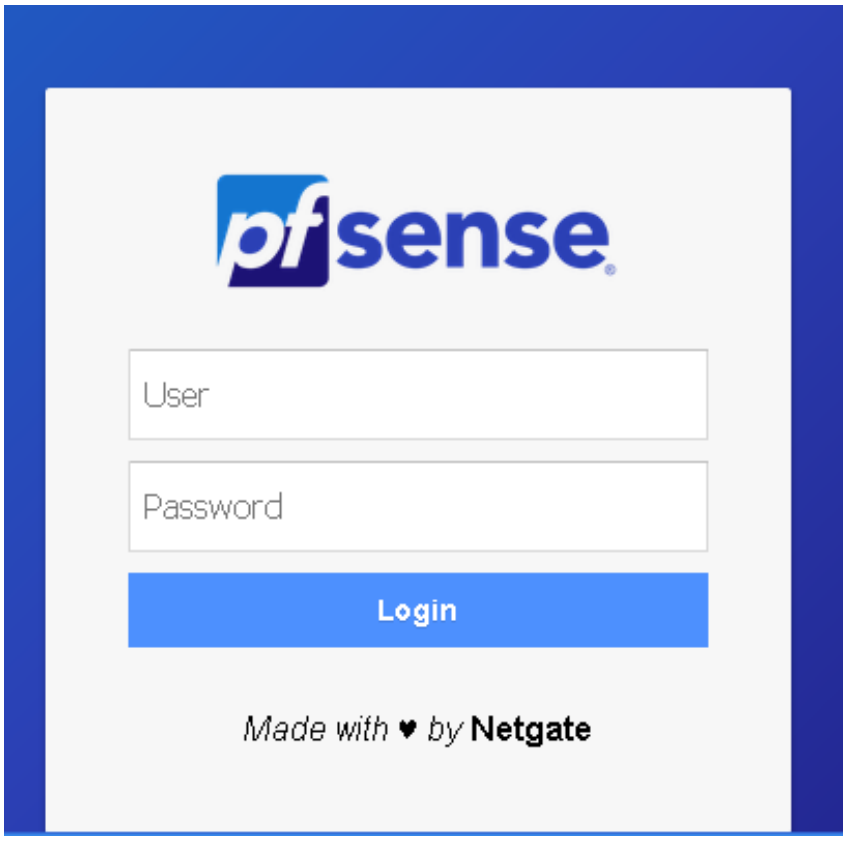
Nous avons configuré un portail captif sur le pfsense pour contrôler les accès du réseau LAN.

Ci-dessous des photos qui illustrant cette configuration :

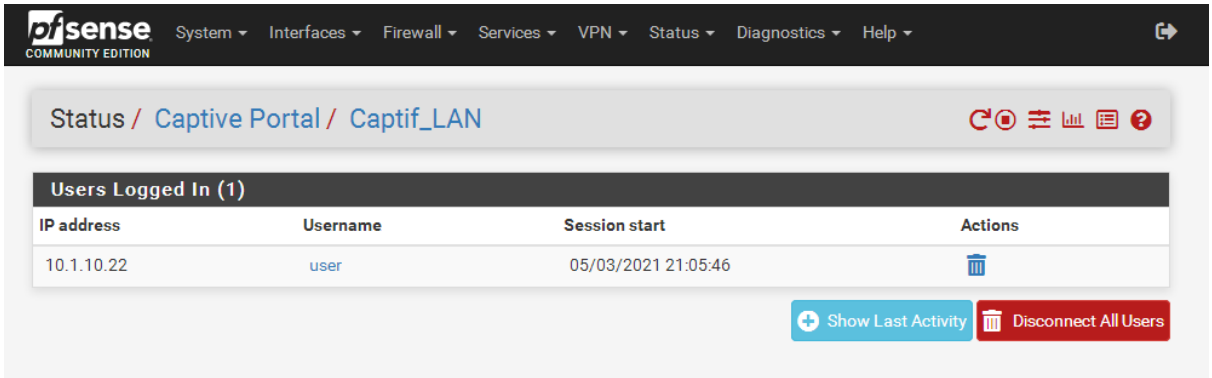
- On a fait une recherche www.google.com on remarque que y a un bottons afficher la page de connexion qui appris.



- En cliquant sur le botton on accède à la page d'authentification :

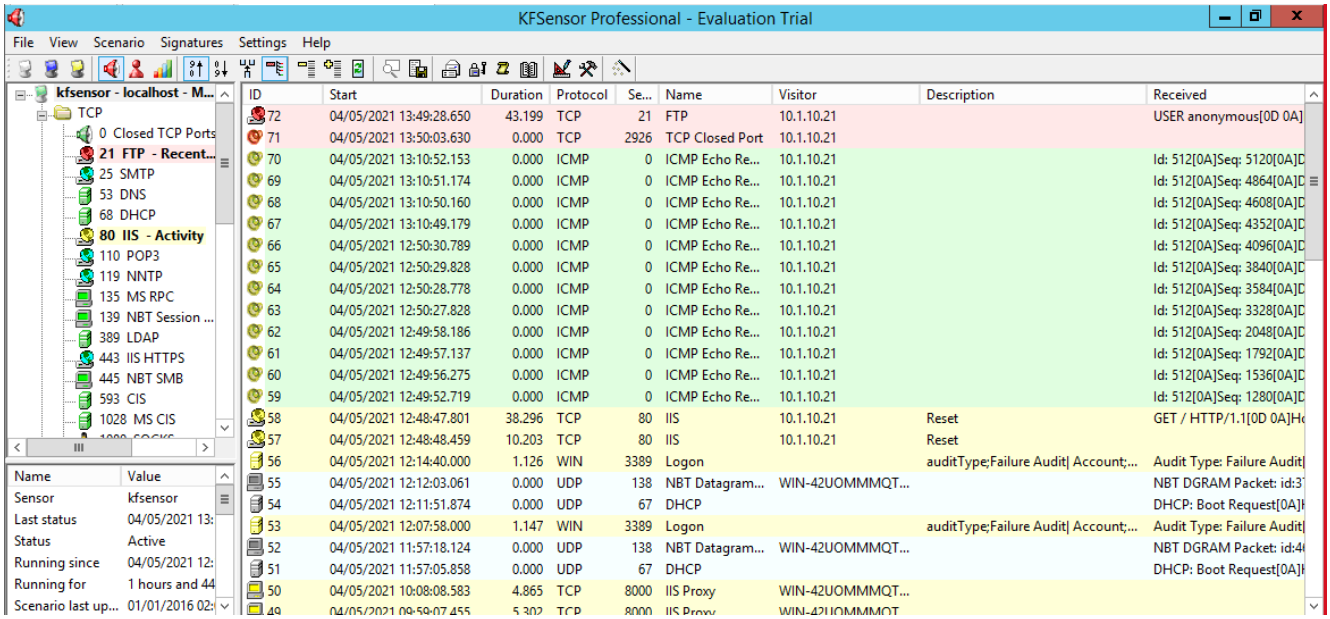


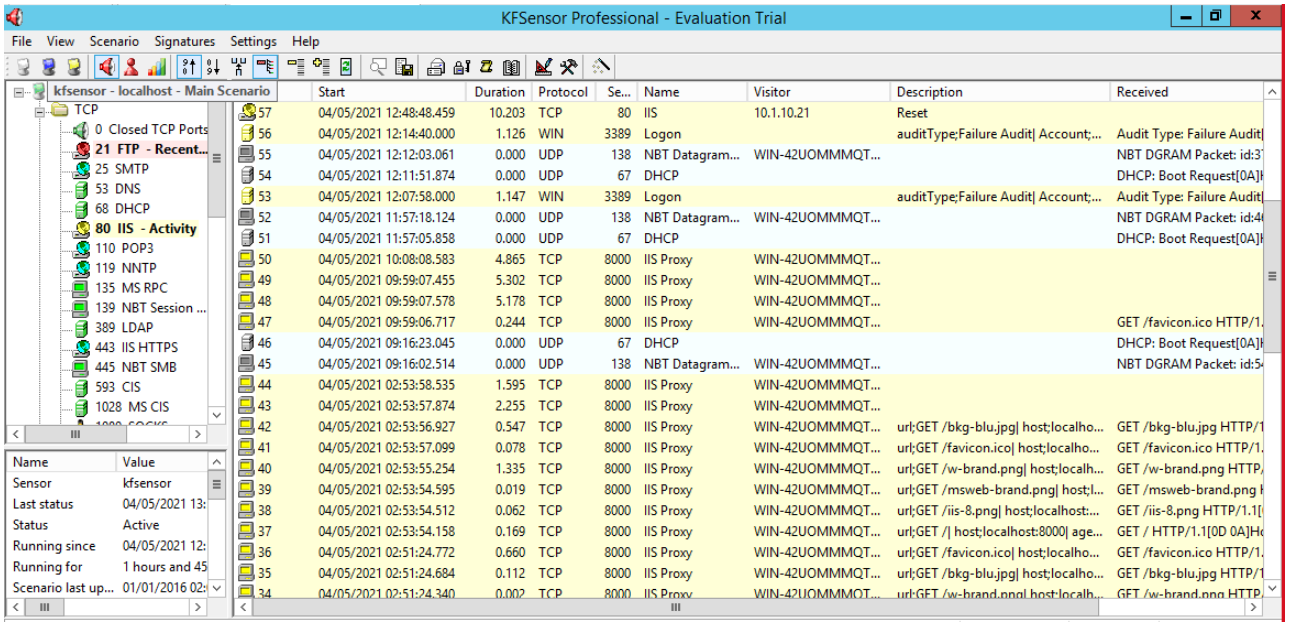

Après avoir accéder à la page on peut voir ça depuis les logs du portail captif :

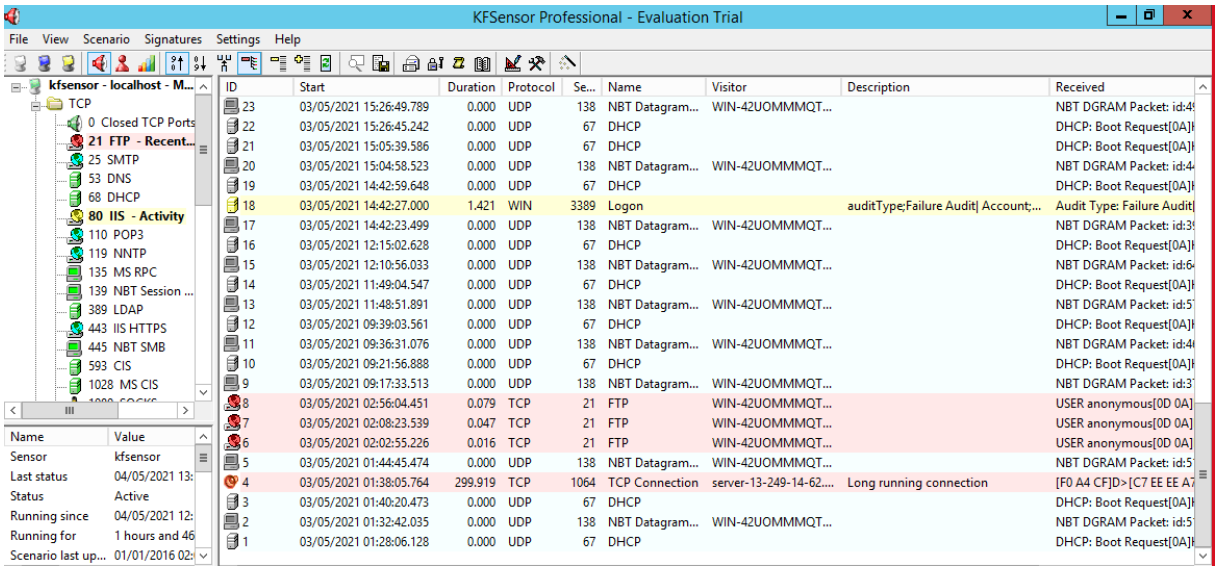


# 6 Installation et configuration de honeypot :

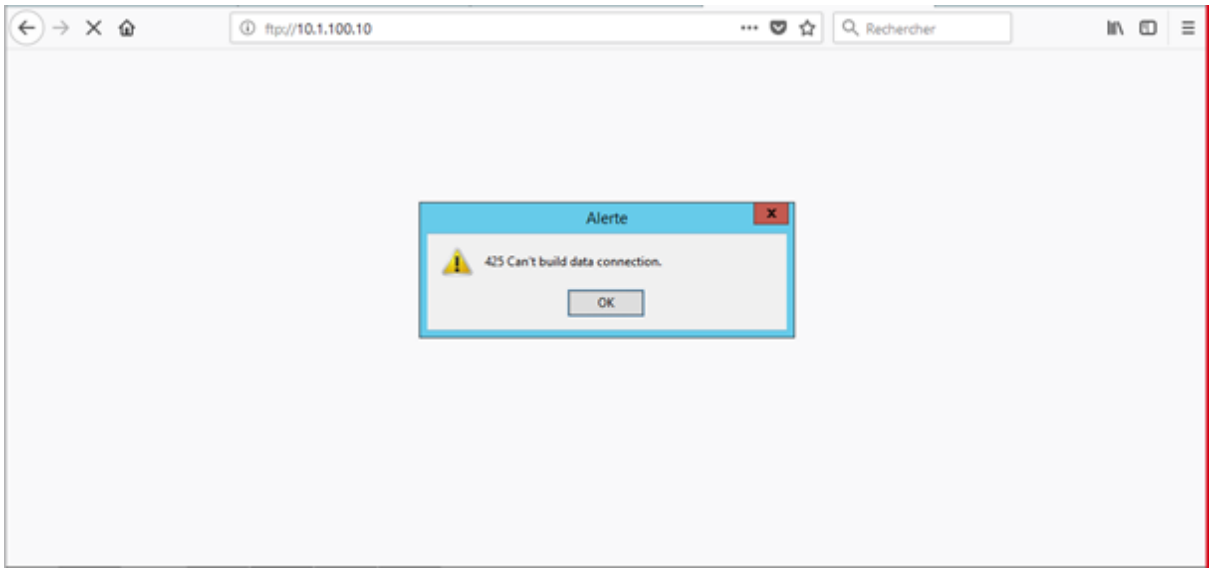
Apres l'installation de l'application de honeypot sur le serveur pour renforcer la sécurité, nous avons les résultats suivants :

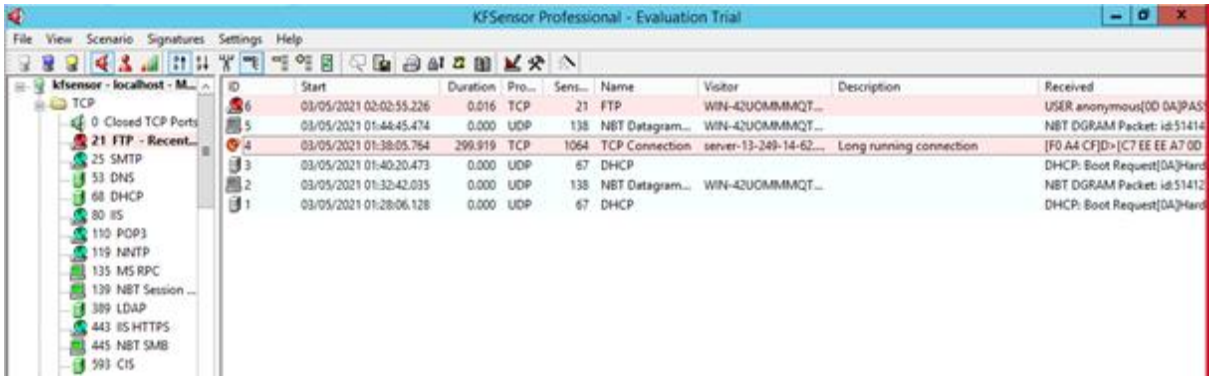


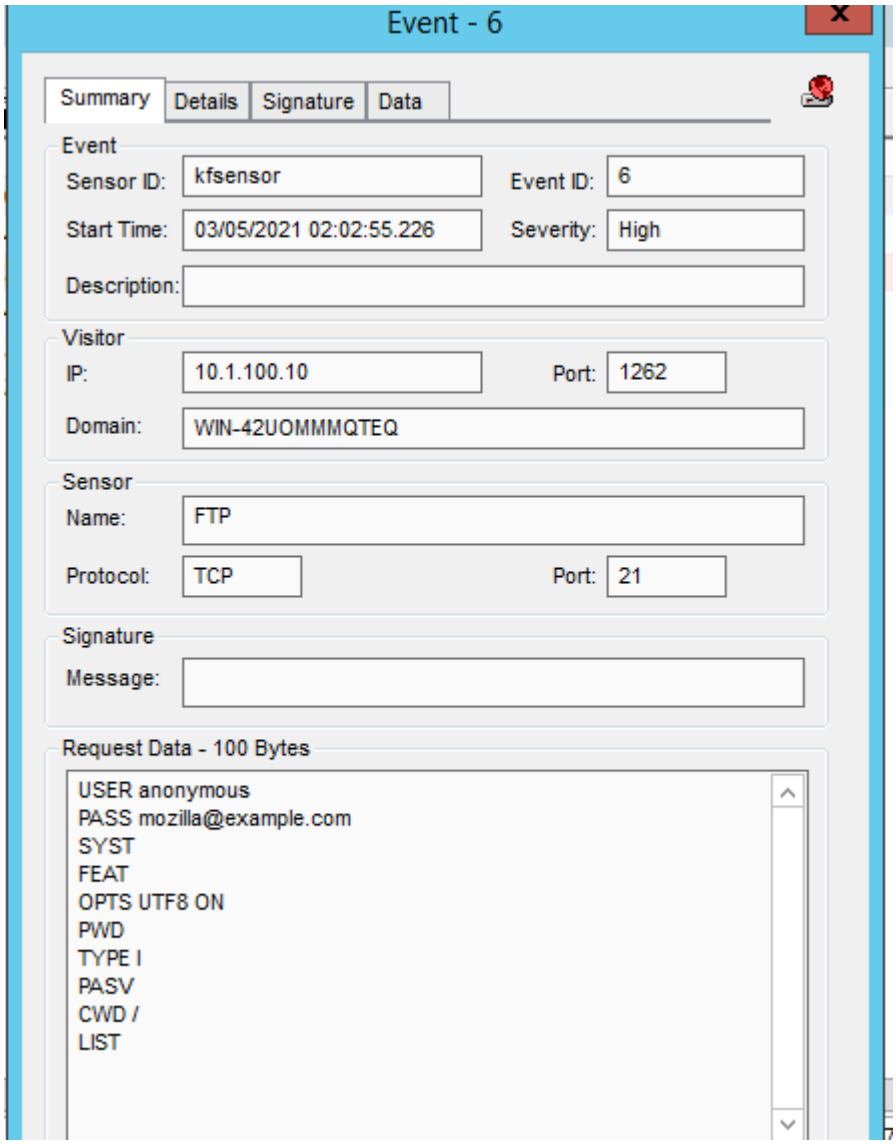






Si on veut accéder a une serveur FTP on reçoit une alerte :





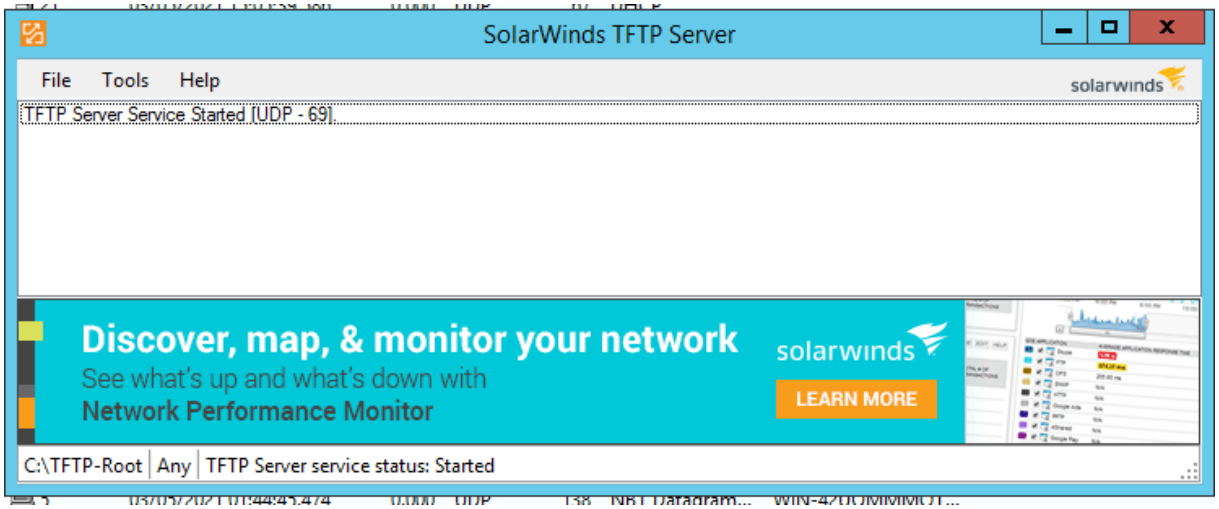

On n'a pas installé le honeypot sur le réseau LAN a cause de manque de ressource sur nous pc.

# 7 Mise en place de la stratégie de sauvegarde de la configuration réseau :

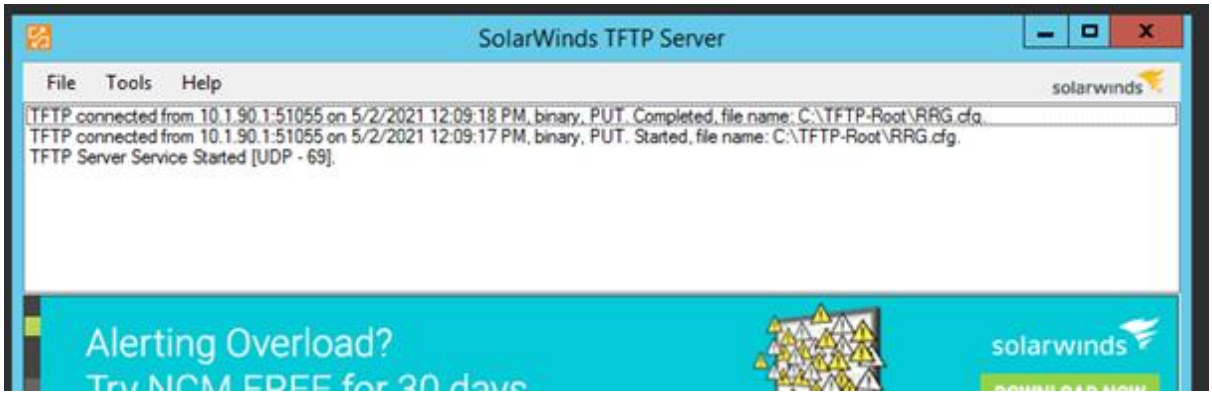
Dans notre entreprise on aura besoin d'un outil pour la sauvegarde des différents équipements réseaux. Après le choisi de l'outil TFTP Server qui joue le rôle de la sauvegarde et la restauration de notre configuration.

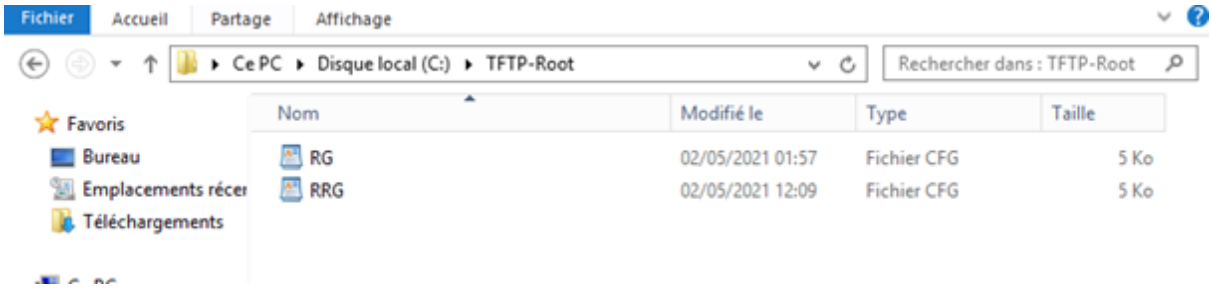
Ci-dessous des captures d'écran qui la sauvegarde est bien mis en place :

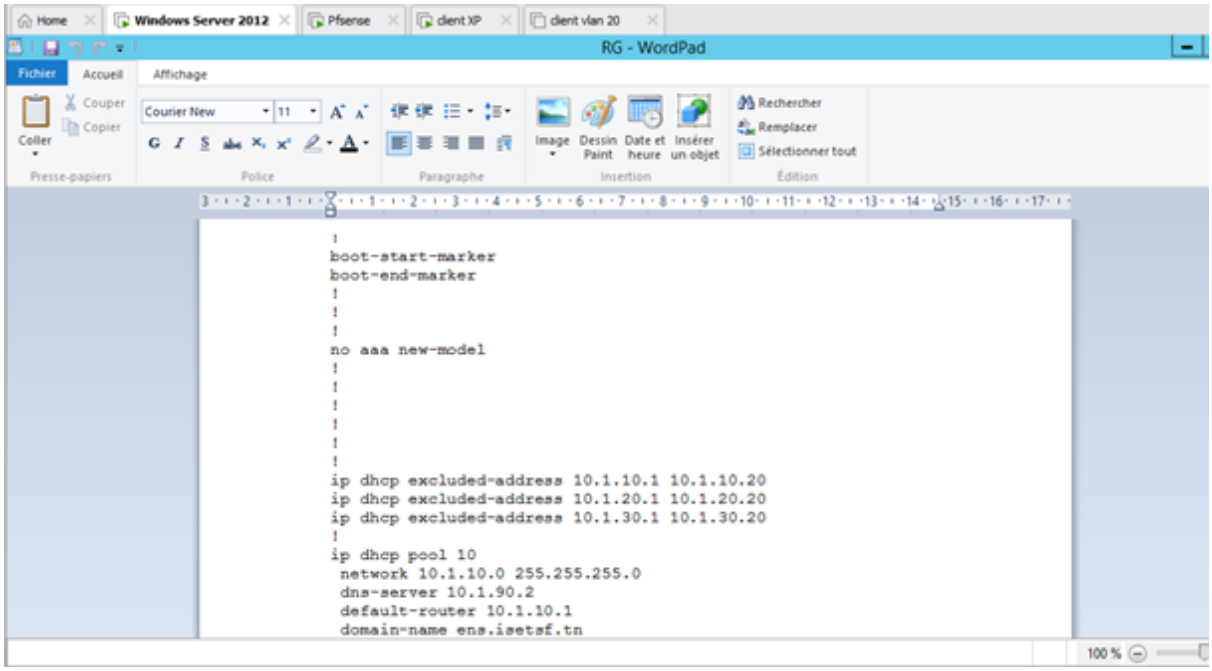
Dans l'exemple de s'sauvegarder la configuration de switch RG :




```
RG#ping 10.1.100.10
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.100.10, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 32/35/39 ms
RG#copy run tftp://10.1.100.10/RRG.cfg
Address or name of remote host [10.1.100.10]?
Destination filename [RRG.cfg]?

-Traceback= 1DBB7C8z 8DBFE5z 90522Ez 904F50z 904D5Dz 900F45z 901B7Bz 901B0Fz 8E76A0z 8E
760Ez 7E4E93z 108617Bz 10879ADz F7080Dz F6DFB6z F6D9EEz - Process "Spanning Tree", CPU
hog, PC 0x008FD5B5

*May  2 09:48:11.598: %SYS-3-CPUHOG: Task is running for (1999)msecs, more than (2000)m
secs (0/0),process = Spanning Tree.!!
4421 bytes copied in 184.817 secs (24 bytes/sec)
RG#
-Traceback= 1DBB7C8z 8DBFE5z 90522Ez 904F50z 904D5Dz 900F45z 901B7Bz 901B0Fz 8E76A0z 8E
760Ez 8CE7DAz 7E4E93z 22B2F97z 22B1BC1z 22D2911z 22B98BFz - Process "IP Input", CPU hog
, PC 0x008FD5B5

*May  2 09:49:05.942: %SYS-3-CPUHOG: Task is running for (2000)msecs, more than (2000)m
secs (0/0),process = IP Input.
```

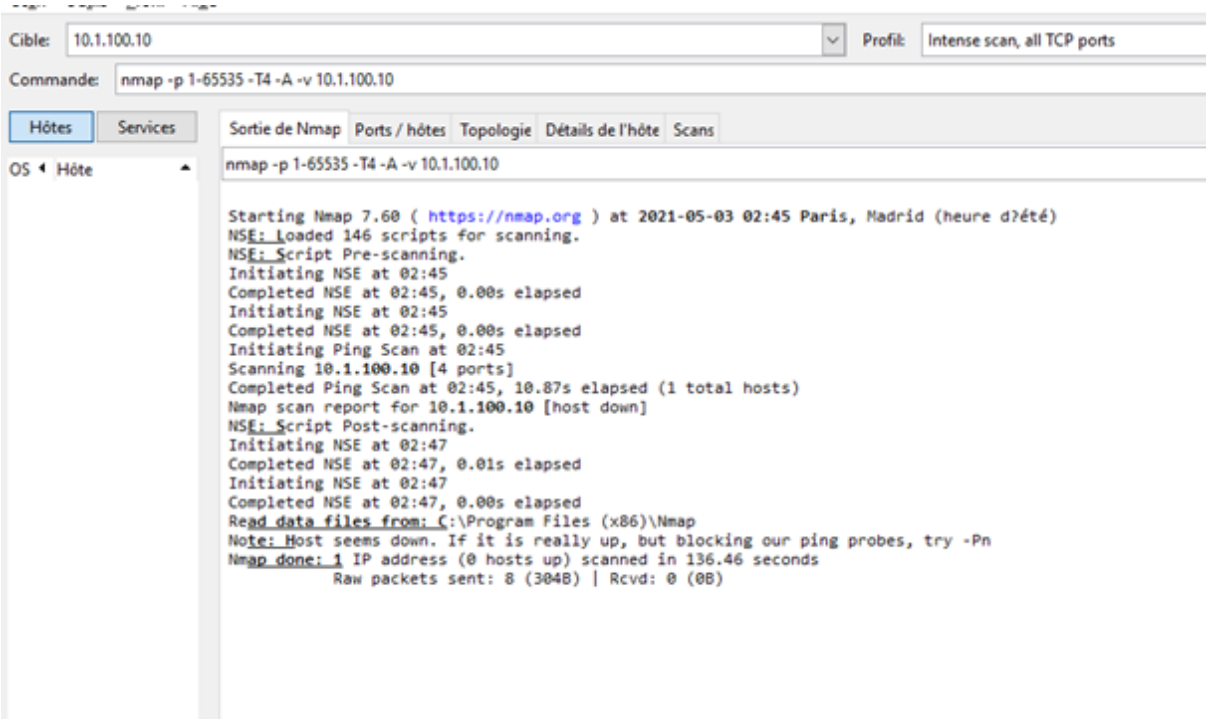




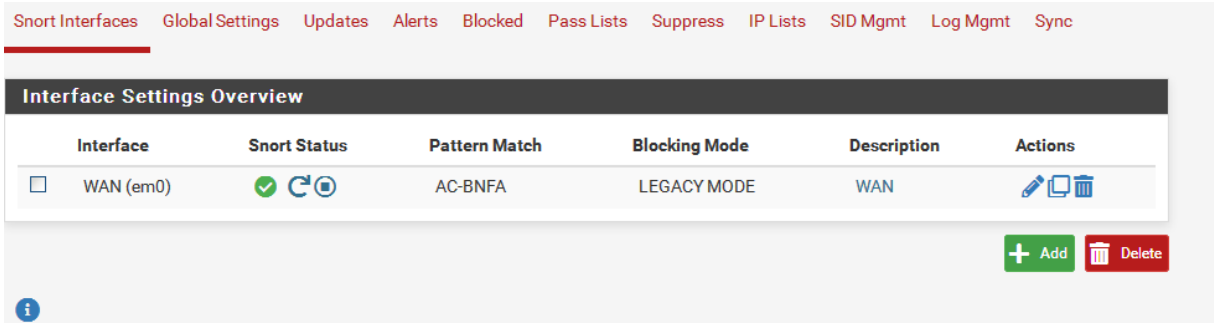



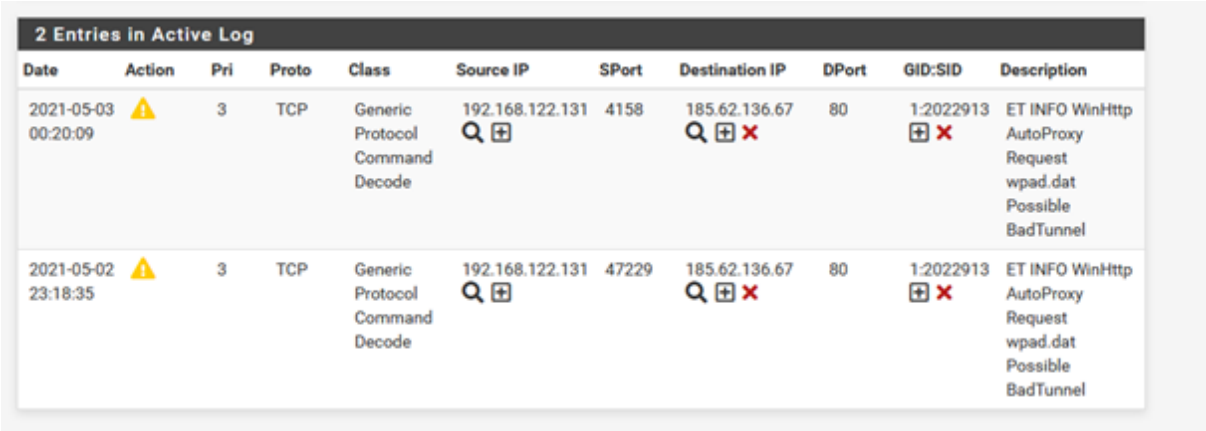

# 8 Mise en place du système de détection d'intrusion :

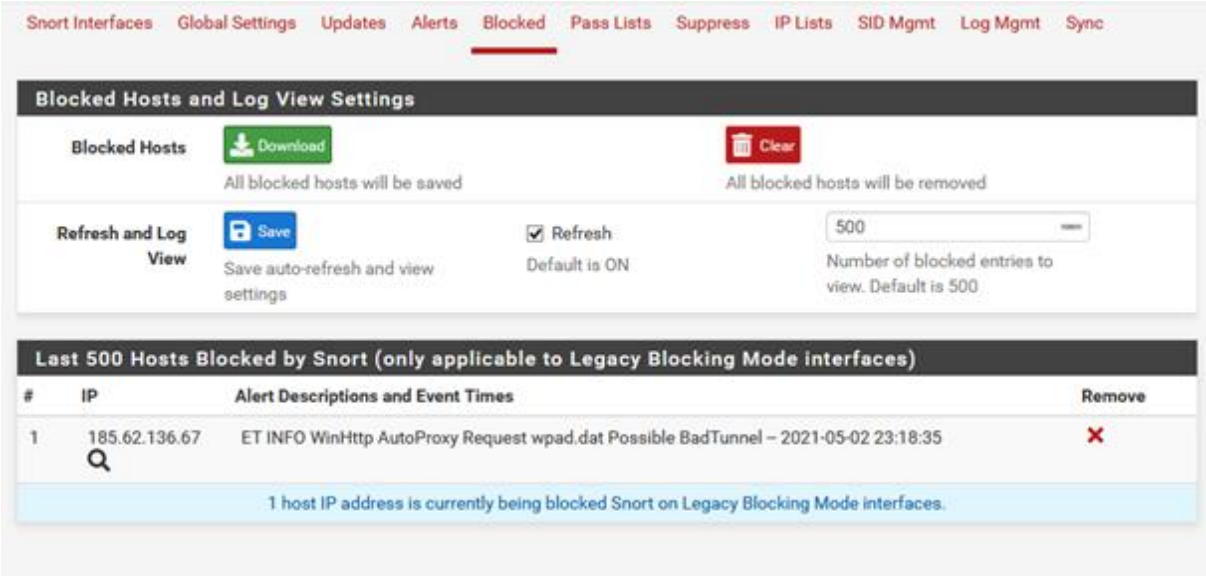
Après l'installation et la configuration de l'outil pour la détection des intrusions. On a fait des teste d'intrusion depuis une machine WAN comme le montre l'image ci-dessous :




Après avoir fait le test on remarque que l'outil nous signale qu'il a eu une intrusion comme le montre l'image ci-dessous :

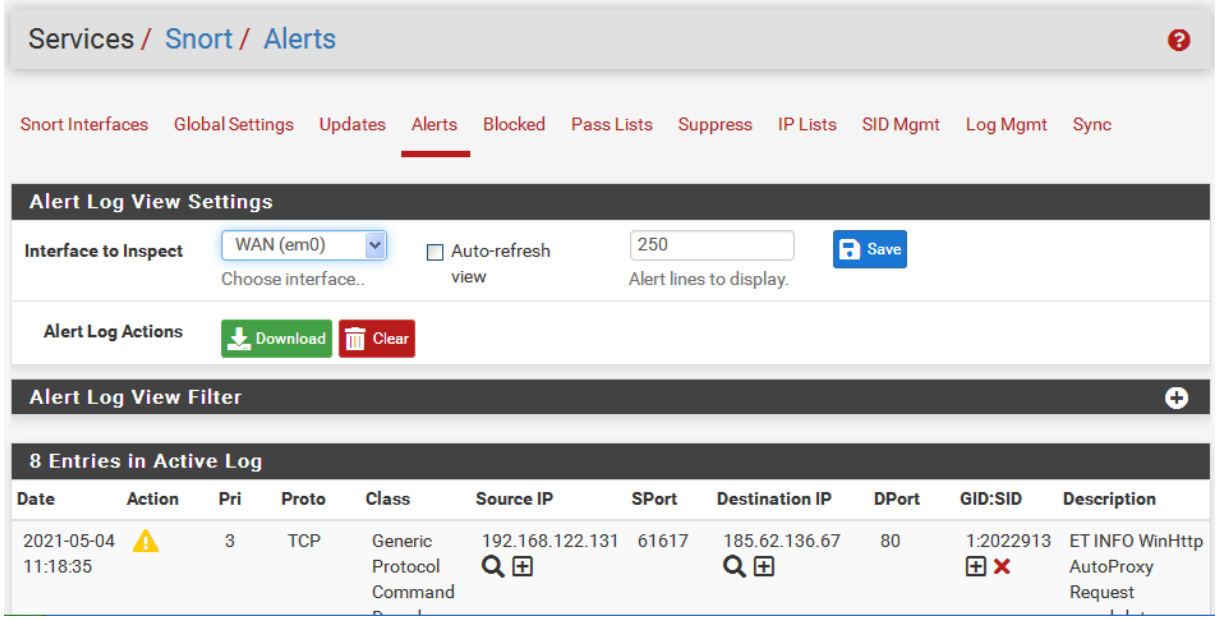





# 9 Mise en place du SOC :

Pour la mise en place du soc on à utiliser le snort pour surveiller le trafic de notre réseau comme la montre l'image :



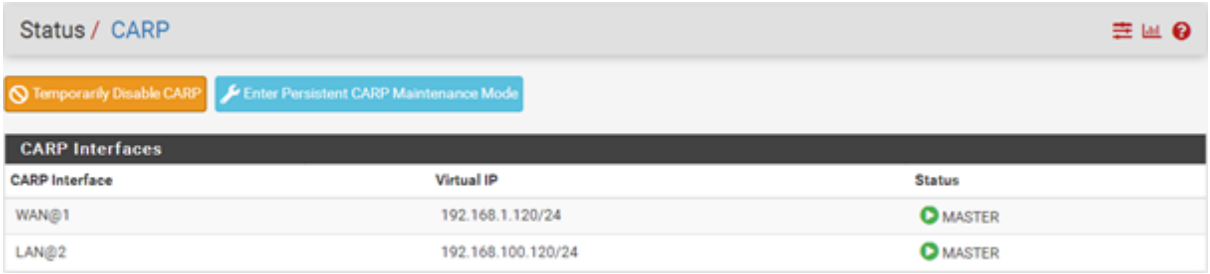

# 10 Mise en place de la redondance réseau :

Pour la mise en place de la redondance dans notre architecteur réseau, nous n'avons pas des ressources suffisantes pour la mettre en place, cependant nous expliquerons le processus à suivre.

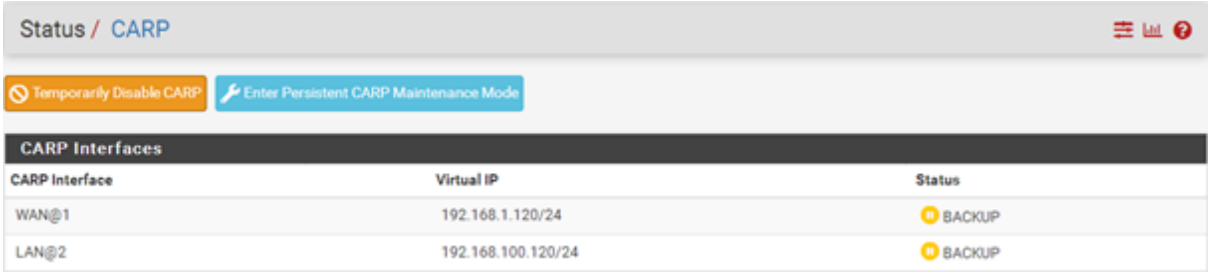
# 10.1 Redondance pfsense :

Pour cela rendons nous dans “***status***“ > “***failover***“

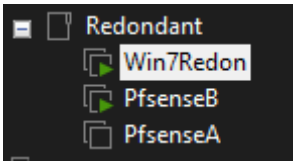
- Pfsense A :



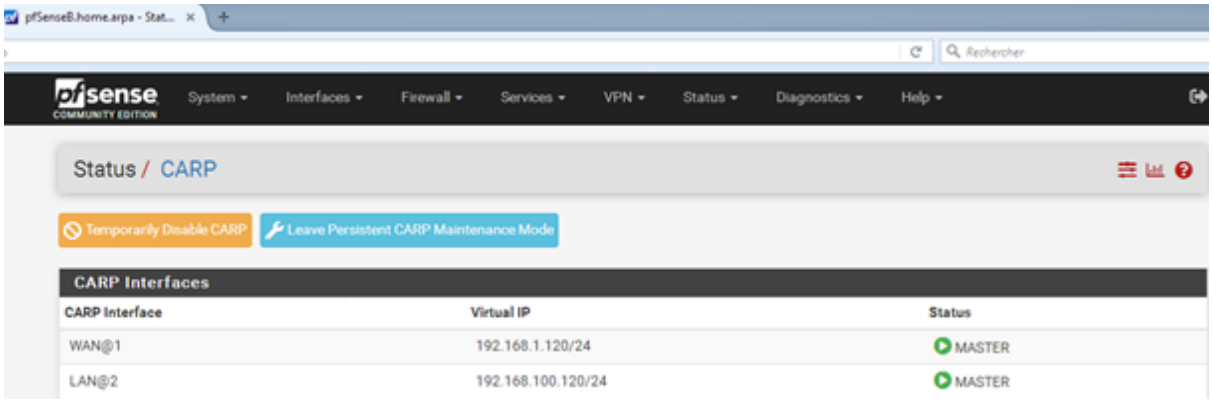

- Pfsense B :




Après arrêt du pfsenseA qui était en master,



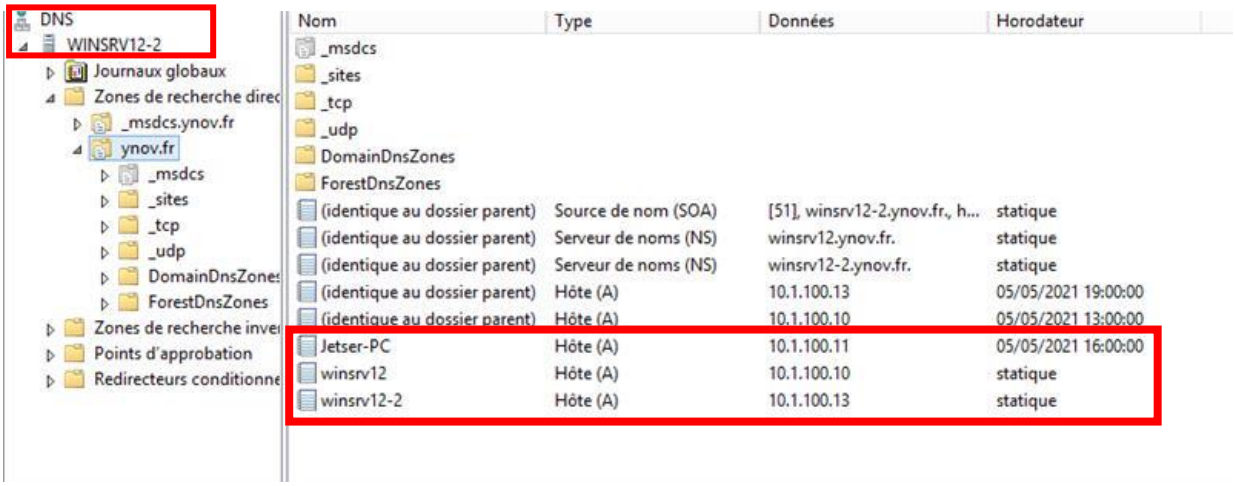

Le pfsenseB passe immédiatement en master comme le montre la figure suivante :




- Teste de l’adresse routage VIP et IP pfsense :

La commande **tracert** nous permet voir que notre requête passe bien par l’adresse ip physique de notre pfsense bien que nous ayons configuré l’adresse sur le VIP

```
C:\Windows\system32\cmd.exe
Réponse de 142.250.178.132 : octets=32 temps=4 ms TTL=118
Réponse de 142.250.178.132 : octets=32 temps=38 ms TTL=118
Réponse de 142.250.178.132 : octets=32 temps=7 ms TTL=118
Réponse de 142.250.178.132 : octets=32 temps=4 ms TTL=118

Statistiques Ping pour 142.250.178.132:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 4ms, Maximum = 38ms, Moyenne = 13ms

C:\Users\Jetser>tracer www.google.com
'tracer' n'est pas reconnu en tant que commande interne
ou externe, un programme exécutable ou un fichier de commandes.

C:\Users\Jetser>tracert www.google.com

Détermination de l'itinéraire vers www.google.com [142.250.178.132]
avec un maximum de 30 sauts :

  1    <1 ms    <1 ms     1 ms  pfSenseB.home.arpa [192.168.100.153]
  2     3 ms     2 ms     1 ms  FREEBOX [192.168.1.254]
  3     8 ms    14 ms     4 ms  194.149.169.93
  4     6 ms     6 ms     5 ms  194.149.166.54
  5    10 ms    36 ms    18 ms  72.14.220.92
  6     7 ms     7 ms     6 ms  108.170.231.111
  7     5 ms     5 ms     5 ms  142.251.64.131
  8     5 ms     6 ms     5 ms  par21s22-in-f4.1e100.net [142.250.178.132]
```

### 10.1.1 Redondance des serveurs :

Dans le test on constate que sur le deuxième serveur on a la réplication du serveur primaire :