StrongSwan

Implémentation d'un VPN IPsec

Effectué par :

BOU SABA Elie

William Staël KAYO

Sous la direction de : M. MBAREK Nader

Table de matières

Liste de figures

I- Introduction

L'exploitation de l'outil StrongSwan a été faite pour la mise en place d'un VPN IPsec qui pourra donner lieu à une solution d'accès à distance au réseau d'une entreprise par exemple d'une manière sécurisée. En utilisant une technique sécurisée, on peut offrir un ou plusieurs critères de sécurité (Authentification, confidentialité, intégrité). C'est le cas d'un télétravailleur qui utilise le tunnel VPN pour accéder à ses ressources dans l'entreprise.

Nous avons décrit en détails un tutoriel d'installation du tunnel VPN entre 2 machines en exploitant l'outil StrongSwan. La 1ère machine serve en tant que machine client et la 2ème fait le rôle du serveur IPsec qui nous permet d'accéder aux autres entités du réseau local de l'entreprise.

II- StrongSwan

StrongSwan est une solution IPsec. Vue que c'est basé sur IPsec, plusieurs protocoles peuvent être utilisés (ESP, AH, IKE). Cette solution fournit des algorithmes de chiffrement, de hachage et l'authentification aux serveurs et aux clients. Effectivement, StrongSwan peut être implémenter sur les différents systèmes d'exploitation ce qui lui rend plus efficace à utiliser.

III- Architecture proposée

Notre architecture se base sur les 2 machines qu'on a présenté dans l'introduction. Une 3ème machine sera utilisée à la fin après l'installation du VPN pour tester la connexion vers le réseau local du serveur IPsec (exemple d'un serveur web au sein du réseau local d'une entreprise). On illustre l'architecture dans la figure 1 où on trouve bien les 2 machines. La machine à gauche c'est le travailleur ayant un système d'exploitation Ubuntu et le serveur IPsec qui est aussi une machine Ubuntu et qui est connecté au réseau local de la salle de TP qui est considéré comme le réseau local de l'entreprise. On relie la machine du télétravailleur et du serveur IPsec par un câble Ethernet pour les connecter entre eux (Dans la vie réelle c'est plutôt un réseau WAN) et le serveur IPsec est relié en LAN au réseau de la salle de TP.

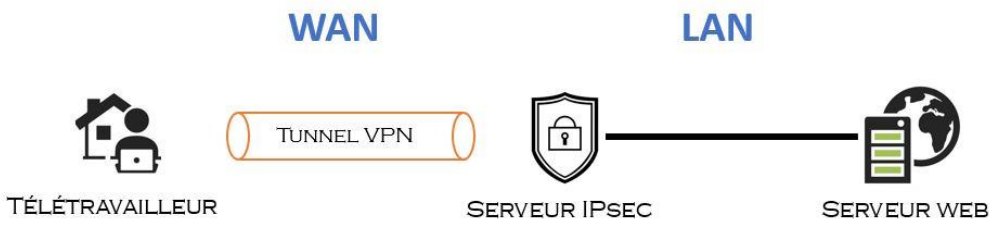


Figure 1 : Architecture proposée

IV- Travail réalisé

1. Configuration d'adressage du serveur IPsec et du client

La configuration de l'adresse ip de l'interface sur le serveur IPsec connectée à la machine du client est faite dans cette première partie. Pour ce faire, on passe aux paramètres IPV4 de réseaux d'Ubuntu. La figure 2 nous montre l'adresse IP que nous avons choisis avec le masque de réseau correspondant.

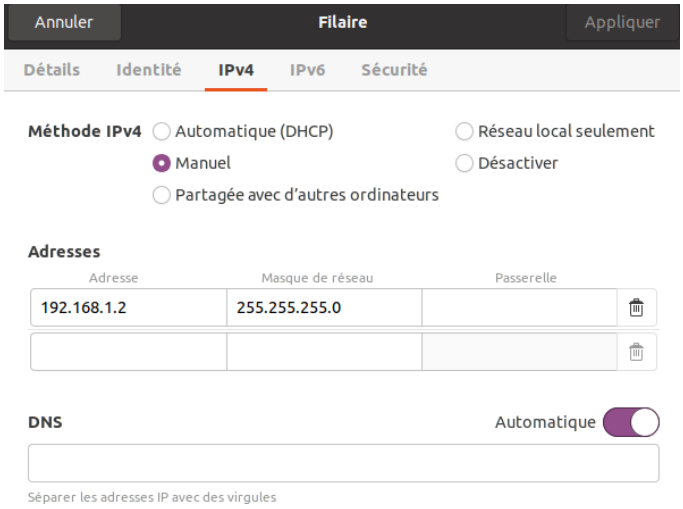


Figure 2 : Configuration de l'interface du serveur IPsec

Nous avons configuré aussi l'adresse ip de la machine du client avec le même masque de réseau pour que les 2 machines puissent communiquer entre eux. La figure 3 nous montre la configuration faite dans les paramètres IP de réseaux du client.

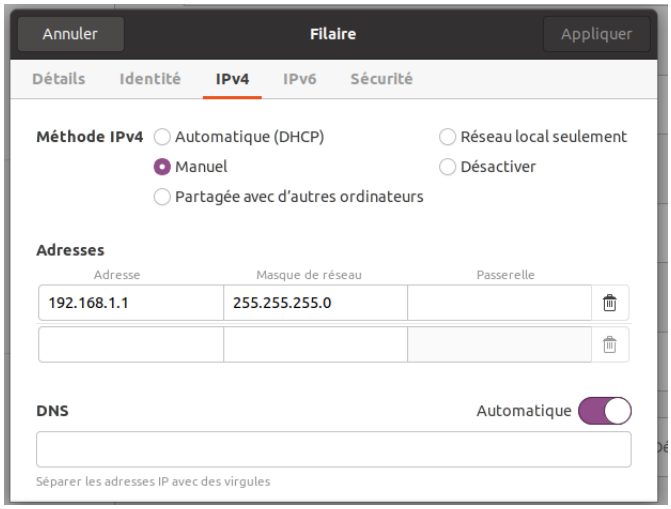


Figure 3 : Configuration de l'interface du télétravailleur

2. Activation du ip forwarding sur le serveur IPsec

Nous avons l'obligation d'activer l'IP forwarding sur le serveur IPsec pour que cette machine puisse acheminer les paquets reçus par le télétravailleur vers le réseau local de destination. Pour achever cela, la commande de la figure 4 est exécuté au niveau du serveur.

N.B : La commande à utiliser ne peut pas être exécuter juste avec sudo et ça va rendre un message d'erreur. Il faut basculer en tant que root pour pouvoir exécuter la commande. On passe au root en utilisant la commande 'sudo -s'.

```
root@eliesaba-Precision-Tower-3620:/home/eliesaba# echo 1 > /proc/sys/net/ipv4/ip_forward
```

Figure 4 : Activation du ip forwarding sur le serveur IPsec

3. Installation de StrongSwan

Au niveau de cette partie, l'installation de l'outil StrongSwan doit être faite sur la machine télétravailleur et sur le serveur IPsec. La figure 5 et 6 nous montre la commande qui nous permet de télécharger et installer le package StrongSwan sur les différentes machines.

```
root@eliesaba-Precision-Tower-3620:/home/eliesaba# apt install -y strongswan
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances
Lecture des informations d'état... Fait
Les paquets suivants ont été installés automatiquement et ne sont plus nécessaires :
  chromium-codecs-ffmpeg-extra gstreamer1.0-vaapi libgstreamer-plugins-bad1.0-0 libva-wayla
Veuillez utiliser « apt autoremove » pour les supprimer.
Les paquets supplémentaires suivants seront installés :
  libcharon-extauth-plugins libstrongswan libstrongswan-standard-plugins strongswan-charon
  strongswan-libcharon strongswan-starter
Paquets suggérés :
  libstrongswan-extra-plugins libcharon-extra-plugins
Les NOUVEAUX paquets suivants seront installés :
  libcharon-extauth-plugins libstrongswan libstrongswan-standard-plugins strongswan
  strongswan-charon strongswan-libcharon strongswan-starter
0 mis à jour, 7 nouvellement installés, 0 à enlever et 91 non mis à jour.
Il est nécessaire de prendre 876 ko dans les archives.
```

Figure 5 : Installation de StrongSwan sur le serveur IPsec

```
williamkayo@williamkayo-Precision-3630-Tower:~$ sudo apt install -y strongswan
[sudo] Mot de passe de williamkayo :
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances
Lecture des informations d'état... Fait
Les paquets suivants ont été installés automatiquement et ne sont plus nécessaires :
  chromium-codecs-ffmpeg-extra gstreamer1.0-vaapi
  libgstreamer-plugins-bad1.0-0 libva-wayland2
Veuillez utiliser « sudo apt autoremove » pour les supprimer.
Les paquets supplémentaires suivants seront installés :
  libcharon-extauth-plugins libstrongswan libstrongswan-standard-plugins
  strongswan-charon strongswan-libcharon strongswan-starter
Paquets suggérés :
  libstrongswan-extra-plugins libcharon-extra-plugins
Les NOUVEAUX paquets suivants seront installés :
```

Figure 6 : Installation de StrongSwan sur la machine du télétravailleur

4. Configuration de StrongSwan sur le serveur IPsec

Dans cette partie, nous avons configuré la connexion IPsec en utilisant la technique d'un secret partagé et en faisant l'échange en se basant sur IKE pour réaliser les négociations. Nous avons passé au niveau du fichier ' /etc/ipsec.conf ' pour configurer le tunnel VPN avec les différents paramètres nécessaires pour la mise en place. La figure 7 illustre la configuration que nous avons fait au niveau du serveur IPsec.

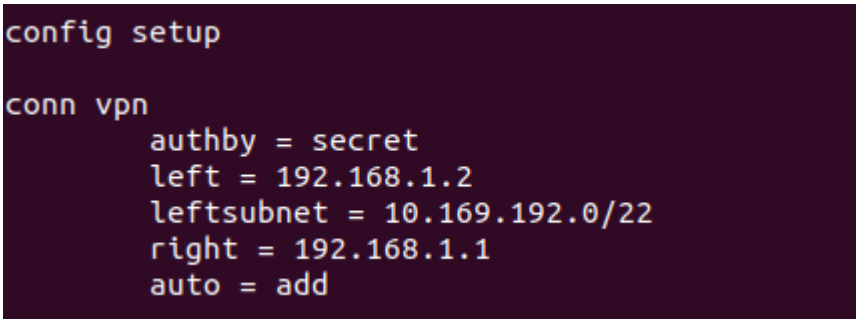


Figure 7 : Configuration du tunnel VPN sur le serveur IPsec

Dans la figure 7, nous avons ajouté plusieurs paramètres qu'on a défini pour le succès du VPN qu'on doit mettre en place. Avec StrongSwan, le protocole utilisé par défaut est le protocole ESP. En fait, 'conn vpn' définit une SA (Security association) ayant le nom 'vpn'. Ensuite, nous avons donné la valeur 'secret' pour authby qui désigne la technique d'authentification utilisée et donc ici c'est un secret partagé. Après, nous avons définit l'ip du server IPsec pour la variable 'left'. Effectivement, dans StrongSwan, 'left' désigne toujours notre machine donc la machine là où on effectue notre configuration et 'right' l'autre côté de la communication. Donc nous avons mis l'adresse ip de l'interface de la machine courant qui est le serveur IPsec et 'right' sera l'adresse ip de l'interface de la machine du télétravailleur connecté au serveur IPsec. 'leftsubnet' c'est le réseau de destination à atteindre par le travailleur donc dans la vie réelle, c'est le réseau local de l'entreprise. Dans notre cas, c'est le réseau local de la salle de TP. Puis, auto est nécessaire pour l'initialisation de la connexion entre les deux entités de communication.

Après avoir bien configuré le fichier ' /etc/ipsec.conf ' pour la création du tunnel VPN, une configuration de la clé secrète partagé est primordiale à faire au niveau du fichier '/etc/ipsec.secrets '. Nous remarquons dans la figure 8 l'adresse IP du télétravailleur avec la valeur de PSK : 'secret1key' qui indique le secret partagé qui sera sollicité lors de l'authentification et la négociation avec IKE entre les 2 machines.

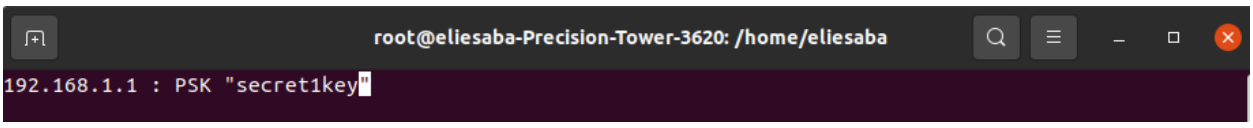


Figure 8 : Configuration du secret partagé sur le serveur IPsec

5. Configuration de StrongSwan sur la machine du télétravailleur

Nous avons configuré les mêmes fichiers sur la machine du télétravailleur mais avec des valeurs différentes pour chaque paramètre qu'on définit dans la figure 9. Au niveau de la configuration le 'left' dans ce cas sera la machine du télétravailleur et le 'right' sera le serveur IPsec. La valeur du 'rightsubnet' désigne le réseau local sur lequel le 'right' est connecté donc le réseau de la salle du TP.

```
root@williamkayo-Precision-3630-Tower:/home/williamkayo# cat /etc/ipsec.conf
# ipsec.conf - strongSwan IPsec configuration file


config setup

conn vpn
        authby = secret
        left = 192.168.1.1
        right = 192.168.1.2
        rightsubnet = 10.169.192.0/22
        auto = add
```

Figure 9 : Configuration du tunnel VPN sur la machine client

Au niveau du clé secret on met l'adresse ip du serveur IPsec avec la même clé secrète que nous avons mis dans la configuration du serveur IPsec.

```
192.168.1.2 : PSK "secret1key"
```

Figure 10 : Configuration du secret partagé sur la machine du télétravailleur

5. Redémarrage du service IPsec sur les 2 machines

Après bien configurer les 2 parties de la communication, un redémarrage de StrongSwan est nécessaire sur les différentes machines concernées. Cela est fait avec la commande 'ipsec restart' qu'il faut exécuter dans la ligne de commande sur chacune des machines.

6. Activation de la connexion VPN et visualisation du status

L'activation du service IPsec sur l'association de sécurité qu'on a défini sur les 2 machines (nommée 'tp') doit être appliquée avec la commande suivante : 'ipsec up tp'. Après l'activation de ce service, la négociation IKE va se lancer en comparant les clés secrètes sur les machines et les algorithmes de chiffrement et de hachage vont être exécuté aussi au niveau de cette

communication. Après, nous avons vérifié le statut de notre connexion qui s'établit en créant le tunnel VPN IPsec. La figure 11 nous montre le statut de la connexion avec la commande qu'on a appliqué sur le serveur IPsec. Nous remarquons dans la dernière ligne le tunnel VPN qui est établit et qui permet à la machine ayant comme ip adresse '192.168.1.1' qui est le télétravailleur de passer par une connexion VPN sécurisé en passant au réseau local de destination. Si on applique la même commande sur la machine du client on va trouver la même dernière ligne de la figure 11.

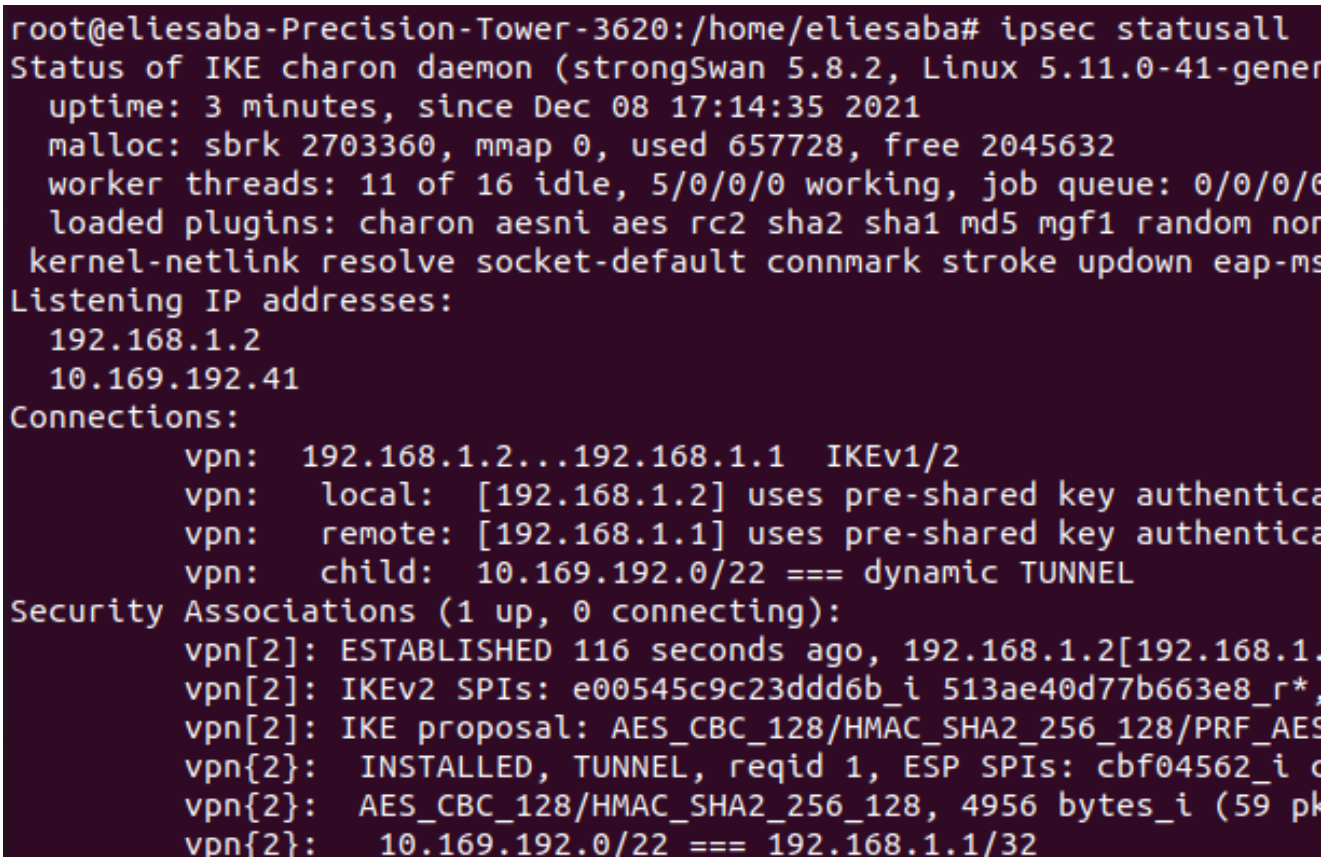


Figure 11 : Vérification du statut de la connexion

N.B : Si la connexion ne fonctionne pas suite au tunnel ou le tunnel n'est pas établit, il faut vérifier les ports qui sont admissibles par le pare-feu. Par la suite, on doit ajouter le port 500 UDP (figure 12) pour que les paquets qui ont pour rôle la négociation en se basant sur IKE puissent être transmises entre les 2 entités concernés.

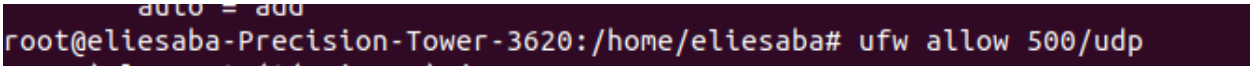


Figure 12 : Ajout du port UDP 500 sur le serveur IPsec

7. Ajout d'une route de la machine du télétravailleur

Maintenant, nous devons ajouter une route de la machine du télétravailleur vers le réseau local de la salle du TP. Pour ce faire, nous avons ajouté le réseau local de la salle du TP qui est le réseau '10.169.192.0' en passant par l'interface de serveur IPsec relié au réseau local et qui est l'interface '10.169.192.41' (Figure 13).

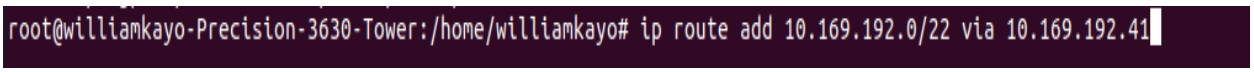


Figure 13 : Ajout d'une route vers un PC du réseau local

Après l'ajout de la route, on vérifie avec la commande 'ip route' qui nous montre le tableau de routage au niveau de la machine du télétravailleur et on voit bien le réseau local de la salle du TP qui est ajouté à la table. On test la connexion en premier temps avec un ping pour voir si les paquets arrivent à leur destination.

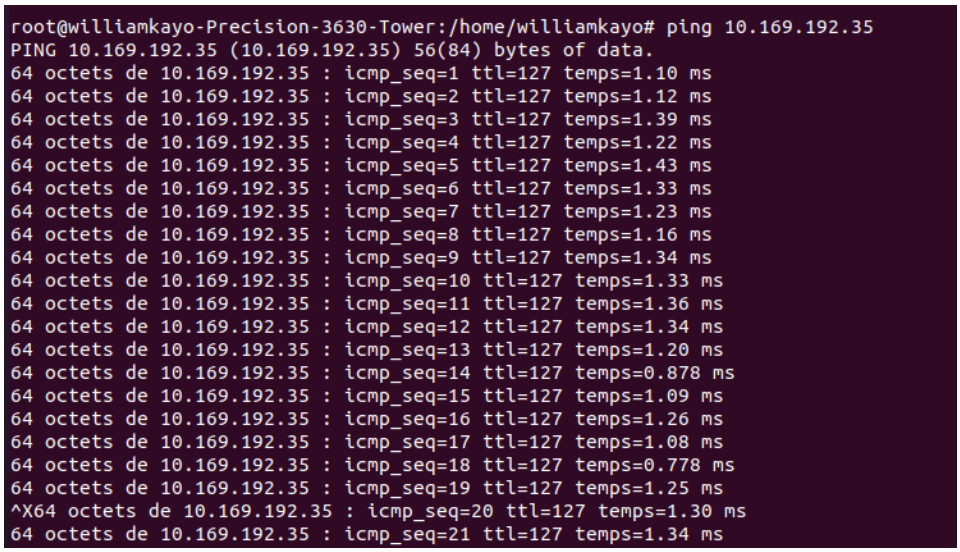
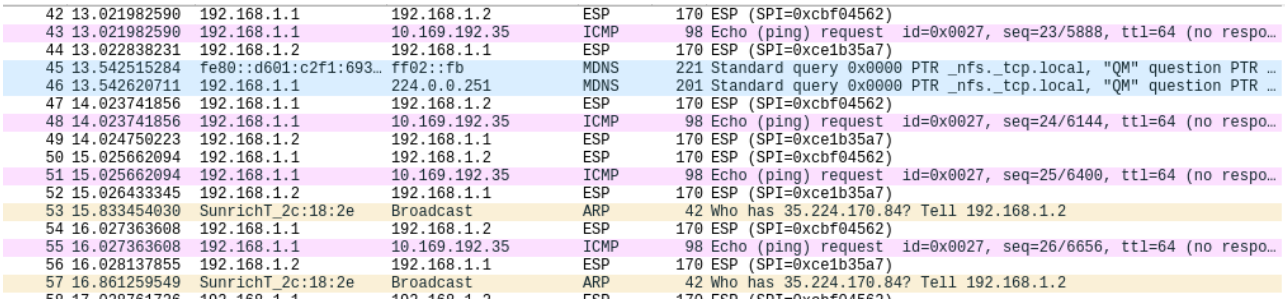


Figure 14 : Test de la connexion

8. Vérification du passage du traffic par le tunnel VPN

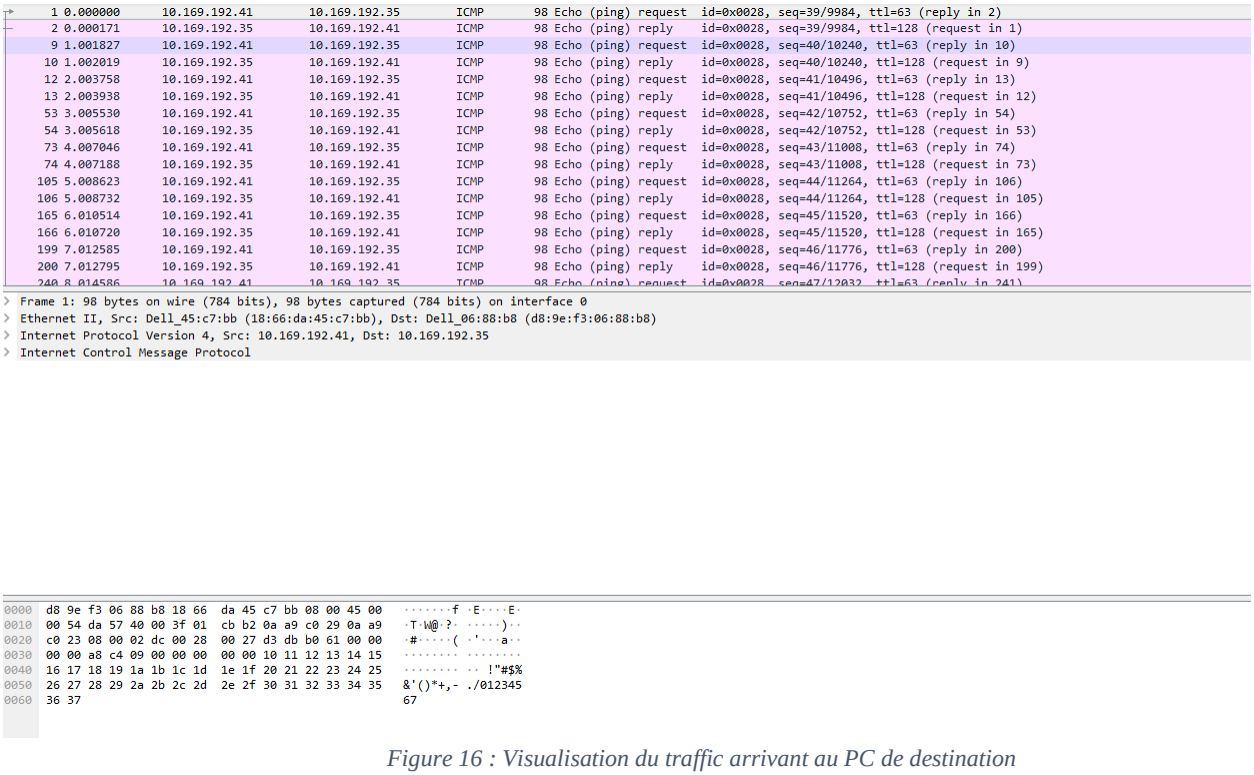
Une connexion qui fonctionne entre le télétravailleur et le PC de destination ne suffit pas pour vérifier que le tunnel VPN est utilisé. C'est pour cette raison, nous avons téléchargé le logiciel 'WireShark' pour capturer le traffic tout au long du chemin et sur les différentes machines. Premièrement, nous avons capturé le traffic qui est généré par la machine du télétravailleur en faisant un 'ping' de la machine du télétravailleur vers le PC de la salle de TP et on remarque que le traffic est encapsulé par le protocole 'ESP' ce qui vérifie bien que le traffic passe par le tunnel VPN que nous avons créé (Figure 15).



42	13.021982590	192.168.1.1	192.168.1.2	ESP	170	ESP (SPI=0xcbf04562)
43	13.021982590	192.168.1.1	10.169.192.35	ICMP	98	Echo (ping) request id=0x0027, seq=23/5888, ttl=64 (no respo…
44	13.022838231	192.168.1.2	192.168.1.1	ESP	170	ESP (SPI=0xce1b35a7)
45	13.542515284	fe80::d601:c2f1:693…	ff02::fb	MDNS	221	Standard query 0x0000 PTR _nfs._tcp.local, "QM" question PTR …
46	13.542620711	192.168.1.1	224.0.0.251	MDNS	201	Standard query 0x0000 PTR _nfs._tcp.local, "QM" question PTR …
47	14.023741856	192.168.1.1	192.168.1.2	ESP	170	ESP (SPI=0xcbf04562)
48	14.023741856	192.168.1.1	10.169.192.35	ICMP	98	Echo (ping) request id=0x0027, seq=24/6144, ttl=64 (no respo…
49	14.024750223	192.168.1.2	192.168.1.1	ESP	170	ESP (SPI=0xce1b35a7)
50	15.025662094	192.168.1.1	192.168.1.2	ESP	170	ESP (SPI=0xcbf04562)
51	15.025662094	192.168.1.1	10.169.192.35	ICMP	98	Echo (ping) request id=0x0027, seq=25/6400, ttl=64 (no respo…
52	15.026433345	192.168.1.2	192.168.1.1	ESP	170	ESP (SPI=0xce1b35a7)
53	15.833454030	SunrichT_2c:18:2e	Broadcast	ARP	42	Who has 35.224.170.84? Tell 192.168.1.2
54	16.027363608	192.168.1.1	192.168.1.2	ESP	170	ESP (SPI=0xcbf04562)
55	16.027363608	192.168.1.1	10.169.192.35	ICMP	98	Echo (ping) request id=0x0027, seq=26/6656, ttl=64 (no respo…
56	16.028137855	192.168.1.2	192.168.1.1	ESP	170	ESP (SPI=0xce1b35a7)
57	16.861259549	SunrichT_2c:18:2e	Broadcast	ARP	42	Who has 35.224.170.84? Tell 192.168.1.2

Figure 15 : Capture du traffic entre le télétravailleur et le serveur IPsec

Ensuite, nous avons capturé le traffic entre le serveur IPsec et la machine de la salle du TP pour voir si les paquets ont été bien décapsulés par le protocole ‘ESP’. Nous remarquons les paquets qui traversent le lien vers le PC de destination et qui sont des paquets ‘ICMP’ (Figure 16).



1	0.000000	10.169.192.41	10.169.192.35	ICMP	98	Echo (ping) request id=0x0028, seq=39/9984, ttl=63 (reply in 2)
2	0.000171	10.169.192.35	10.169.192.41	ICMP	98	Echo (ping) reply id=0x0028, seq=39/9984, ttl=128 (request in 1)
9	1.001827	10.169.192.41	10.169.192.35	ICMP	98	Echo (ping) request id=0x0028, seq=40/10240, ttl=63 (reply in 10)
10	1.002019	10.169.192.35	10.169.192.41	ICMP	98	Echo (ping) reply id=0x0028, seq=40/10240, ttl=128 (request in 9)
12	2.003758	10.169.192.41	10.169.192.35	ICMP	98	Echo (ping) request id=0x0028, seq=41/10496, ttl=63 (reply in 13)
13	2.003938	10.169.192.35	10.169.192.41	ICMP	98	Echo (ping) reply id=0x0028, seq=41/10496, ttl=128 (request in 12)
53	3.005530	10.169.192.41	10.169.192.35	ICMP	98	Echo (ping) request id=0x0028, seq=42/10752, ttl=63 (reply in 54)
54	3.005618	10.169.192.35	10.169.192.41	ICMP	98	Echo (ping) reply id=0x0028, seq=42/10752, ttl=128 (request in 53)
73	4.007046	10.169.192.41	10.169.192.35	ICMP	98	Echo (ping) request id=0x0028, seq=43/11008, ttl=63 (reply in 74)
74	4.007188	10.169.192.35	10.169.192.41	ICMP	98	Echo (ping) reply id=0x0028, seq=43/11008, ttl=128 (request in 73)
105	5.008623	10.169.192.41	10.169.192.35	ICMP	98	Echo (ping) request id=0x0028, seq=44/11264, ttl=63 (reply in 106)
106	5.008732	10.169.192.35	10.169.192.41	ICMP	98	Echo (ping) reply id=0x0028, seq=44/11264, ttl=128 (request in 105)
165	6.010514	10.169.192.41	10.169.192.35	ICMP	98	Echo (ping) request id=0x0028, seq=45/11520, ttl=63 (reply in 166)
166	6.010720	10.169.192.35	10.169.192.41	ICMP	98	Echo (ping) reply id=0x0028, seq=45/11520, ttl=128 (request in 165)
199	7.012585	10.169.192.41	10.169.192.35	ICMP	98	Echo (ping) request id=0x0028, seq=46/11776, ttl=63 (reply in 200)
200	7.012795	10.169.192.35	10.169.192.41	ICMP	98	Echo (ping) reply id=0x0028, seq=46/11776, ttl=128 (request in 199)

```
> Frame 1: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface 0
> Ethernet II, Src: Dell_45:c7:bb (18:66:da:45:c7:bb), Dst: Dell_06:88:b8 (d8:9e:f3:06:88:b8)
> Internet Protocol Version 4, Src: 10.169.192.41, Dst: 10.169.192.35
> Internet Control Message Protocol
```

```
0000  d8 9e f3 06 88 b8 18 66  da 45 c7 bb 08 00 45 00   ·······f ·E····E·
0010  00 54 da 57 40 00 3f 01  cb b2 0a a9 c0 29 0a a9   ·T·W@·?· ·····)··
0020  c0 23 08 00 02 dc 00 28  00 27 d3 db b0 61 00 00   ·#·····( ·'···a··
0030  00 00 a8 c4 09 00 00 00  00 00 10 11 12 13 14 15   ········ ········
0040  16 17 18 19 1a 1b 1c 1d  1e 1f 20 21 22 23 24 25   ········ ·· !"#$%
0050  26 27 28 29 2a 2b 2c 2d  2e 2f 30 31 32 33 34 35   &'()*+,- ./012345
0060  36 37                                             67
```

Figure 16 : Visualisation du traffic arrivant au PC de destination

V- Conclusion

Pour finir, nous avons bien crée un tunnel VPN basé sur IPsec en exploitant l’outil StrongSwan qui nous donne la liberté de configurer les différents paramètres nécessaires pour cette implémentation. Le traffic est maintenant bien sécurisé entre le télétravailleur et le réseau local de l’entreprise.