

IPSEC/VPN.
<http://nassih.com>
© MOHAMED NASSIH.

1. Introduction.

Il arrive souvent que les entreprises éprouvent le besoin de communiquer avec des filiales, des fournisseurs, des clients ou même du personnel géographiquement éloignées. Le grand problème pour répondre à ce besoin est la sécurité des données qui vont être transitées dans le réseau de transport. Une des solutions consiste à relier les réseaux distants à l'aide de liaisons spécialisées privées. Toutefois la plupart de ces liaisons génèrent des coûts supplémentaires souvent élevés pour les entreprises.

Puisque les réseaux d'entreprises sont souvent reliés à Internet, une deuxième solution s'impose, c'est l'utilisation de l'Internet comme un réseau de transport. Pour sécuriser cet échange de l'information via Internet, on utilise des protocoles d'encapsulation (tunneling), ces protocoles chiffrent les données à l'entrée du réseau et les déchiffrent à la sortie, on parle dans ce cas d'un réseau VPN pour (Virtual Private Network). Il existe plusieurs protocoles qui permettent de faire cette encapsulation, mais le protocole de référence et le plus utilisé est Ipsec.

Ipsec est un ensemble de protocoles développés par l'IETF (Internet Engineering Task Force), qui a pour objectif d'établir des canaux de communications sécurisés garantissant la confidentialité et l'intégrité de la communication, c'est une extension de sécurité pour la version 4 du protocole de l'Internet, Permettant de sécuriser les échanges au niveau réseau.

2. L'architecture d'Ipsec.

L'emplacement de Ipsec au niveau trois présente l'avantage de le rendre exploitable par les couches supérieurs, Ipsec offre donc un moyen de protection unique pour toutes les applications, et à n'importe quel trafic transmis via le protocole IP, et pas seulement pour une application particulière.

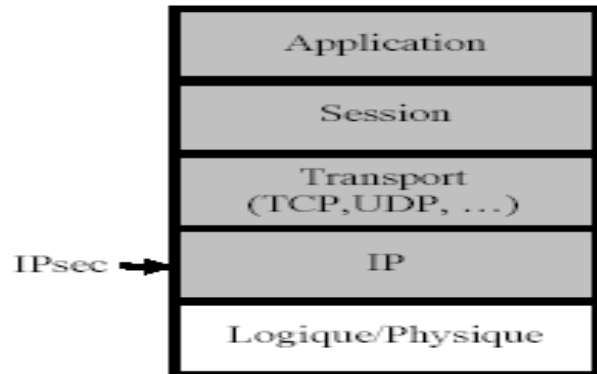


Figure 2.1 : l'emplacement d'IPsec dans l'architecture TCP/IP.

Ipsec utilise principalement deux protocoles, AH (Authentication Header protocol) et ESP (Encapsulating Security Payload). AH est utilisé pour l'authentification et le protocole ESP pour le chiffrement. Ipsec utilise aussi le protocole IKE (Internet Key Exchange) pour la négociation des paramètres de la connexion (les clés par exemple).

Ipsec pourra fonctionner en deux modes, le mode transport et le mode tunnel. Dans le mode transport, seulement la charge utile du paquet IP est chiffrée, l'entête est transmis en clair. Le mode tunnel sécurise tout le paquet IP, dans ce cas Ipsec encapsule le paquet entier dans un nouveau paquet, c'est le mode utilisé pour construire des VPNs. (Voir figure 2.2). Les VPNs à base d'Ipsec sont des connexions sécurisées à base d'un chiffrement à clé publique. Chaque message envoyé par un utilisateur sur le réseau doit être signé en utilisant la clé privée. Le récepteur utilise la clé publique de l'émetteur pour déchiffrer ce message.

Mode transport



Mode tunnel



Non chiffré chiffré

Figure 2.2 : encapsulation de ESP dans le mode transport et tunnel.

3. La configuration du réseau.

La figure 3.1 représente le réseau que nous allons utiliser pour faire la mise en place de notre VPN. Les deux réseaux 194.153.205.0 et 194.153.204.0 représentent deux sites d'une entreprise. L'objectif est de sécuriser l'échange entre ces deux sites.

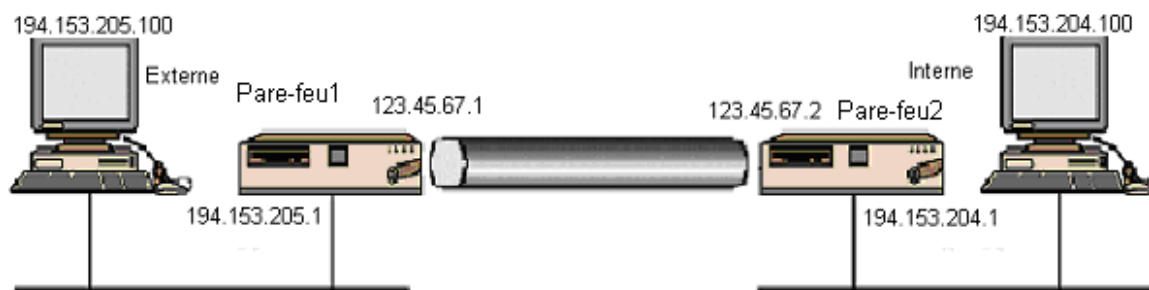


Figure 3.1 : le VPN entre les deux sites.

Le premier site 194.153.205.0 est protégé par le Pare-feu1 et le deuxième site 194.153.204.0 par Pare-feu2. Les deux machines Interne et Externe simulent les deux réseaux internes et vont servir comme des machines de test.

On va supposer que la configuration IP est déjà faite.. Les deux réseaux sont capables de communiquer. (Voir figure 3.2).

```
[root@Interne root]# ping 194.168.205.100
PING 194.168.205.100 (194.168.205.100) 56(84) bytes of data.
64 bytes from 194.168.205.100: icmp_seq=1 ttl=62 time=54.7 ms
64 bytes from 194.168.205.100: icmp_seq=2 ttl=62 time=1.52 ms
64 bytes from 194.168.205.100: icmp_seq=3 ttl=62 time=1.21 ms
64 bytes from 194.168.205.100: icmp_seq=4 ttl=62 time=1.01 ms

--- 194.168.205.100 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3047ms
rtt min/avg/max/mdev = 1.019/14.622/54.732/23.158 ms
[root@Interne root]# _
```

Figure 3.2 : la communication avant la configuration de Ipsec.

Dans notre configuration, les passerelles Linux sont connectées directement au réseau Internet, mais dans la réalité, ces machines sont connectées aux routeurs. L'existence des routeurs n'influence pas notre configuration, il suffit de s'assurer que les deux routeurs sont bien connectés à Internet.

4. FreeS/WAN.

FreeS/WAN est l'implémentation officielle du protocole Isec sous Linux. Le projet FreeS/WAN sera prochainement intégré dans la majorité des distributions Linux et il est disponible au site <http://www.freeswan.org>.

FreeS/WAN est composé de trois grandes parties, KLIPS qui représente le noyau IPsec, et implémente les protocoles AH et ESP, Pluto, qu'est l'implémentation du protocole IKE, et une variété de scripts qui fournies les interfaces d'administration. La configuration de FreeS/WAN se fait via le fichier `/etc/ipsec.conf`. Ce dernier est organisé en trois sections. La première section est «`config setup`», elle contient des lignes de configuration à exécuter au démarrage d'Isec. La deuxième section est la section «`conn nom_connexion`», elle identifie une connexion, et elle contient les paramètres et les clés de la connexion. La troisième section est la section par défaut «`conn %default`». Chaque paramètre qui n'est pas défini dans la deuxième section sera pris de la section par défaut. (Voir figure 4.1)

```
config setup
# À exécuter au démarrage de Isec.
conn nom_connexion
# Clés de la connexion VPN.
# paramètres de la connexion.
conn %default
# paramètres par défaut.
```

Figure 4.1 : format du fichier `/etc/ipsec.conf`.

5. L'installation et la configuration d'Ipsec.

Étape 1 : le téléchargement et l'installation de FreeS/WAN.

Il faut télécharger les packages qui correspondent à notre version de noyau Linux. On pourra utiliser la commande «uname -r» pour avoir la version exacte. Dans notre cas c'est la version 2.4.20-8. Les rpms à télécharger sont donc FreeS/WAN-module-2.06_2.4.20_8-0.i386 et FreeS/WAN-userland-2.06_2.4.20_8-0.i386. La commande `rpm -ivh FreeS/WAN*.rpm` permet d'installer ces deux packages.

Étape 2 : génération des clés.

Le fichier `/etc/ipsec.secrets` est le fichier d'authentification qui va contenir les clés. Nous allons générer deux clés de longueur 2048 bits pour les deux passerelles (pare-feu) en utilisant la commande `ipsec`. La sortie de cette commande doit être dans le fichier `/etc/ipsec.secrets`.

```
ipsec newhostkey -bits 2048 -output /etc/ipsec.secrets
```

Figure 5.1 : génération des clés.

Le système génère deux clés dans le fichier `/etc/ipsec.secrets`. Une clé publique et une autre privée. (La dernière partie du fichier qui se trouve après la phrase «everything after this point is secret» représente la clé privée).

Étape 3 : L'échange des clés.

Souvent on nomme la passerelle gauche (left gateway) la passerelle qui initialise la création du tunnel, et l'autre est nommée la passerelle droite (right gateway). C'est juste une convention. Dans notre cas, nous allons nommer le Pare-feu1, la passerelle gauche et le Pare-feu2, la passerelle droite.

Pour que la passerelle Pare-feu1 puisse être capable de déchiffrer les informations envoyées par Pare-feu2, elle doit posséder sa clé publique. De même pour la passerelle Pare-feu2, elle doit posséder la clé publique de la passerelle Pare-feu1. Le fichier de configuration ipsec.conf sur les deux machines doit contenir donc les deux clés publiques des deux machines. La commande «`ipsec showhostkey --left`» permet d'afficher la clé publique de la passerelle gauche.

Nous utilisons la commande «`ipsec showhostkey --left >> /etc/ipsec.conf`» pour ajouter la clé publique du Pare-feu1 au fichier ipsec.conf. De même sur la passerelle droite, on utilise la commande «`ipsec showhostkey --right >> /etc/ipsec.conf`» pour ajouter la clé publique de la passerelle droite Pare-feu2 au fichier ipsec.conf.

Reste à échanger les clés publiques entre les deux passerelles. Pour se faire on a copié ces clés dans des fichiers sur une disquette et on a fait le transfert. Les figures 5.2 et 5.3 montrent les fichiers de configuration ipsec.conf sur les deux passerelles Pare-feu1 et Pare-feu2. Le nom **f1-f2** identifie la connexion VPN entre les deux passerelles.

```

# version 2.0      # conforms to second version of ipsec.conf specification

# basic configuration
config setup
    interfaces="ipsec0=eth1"
    # Debug-logging controls: "none" for (almost) none, "all" for lots.
    klipsdebug=none
    plutodebug=none

conn %default
    keyingtries=0
    authby=rsasig
    auto=add

conn f1-f2
    right=123.45.67.2
    rightsubnet=194.153.204.0/24
    rightrsasigkey=0sAQ0gLoZxQL0lsQFUrB8TGX/Pgk jF/LURMEbXALwrCsgHBR6OKS/pYp0
wiGZJyG5AE1wbEJmCP9Tjcw+Fsl7oRqg00Z/5C9x9s/6NCbzXpUEcvwEUdQ/NUhrcGoo/kdk+HW4PJDU
YFggMczapuIYNZAqZA413vmhZupC8m4P0EySSYkJ8SX0mJRBWY IBipWQFAoG7fq23s4ou1IFDYTxKjnY
QBtQxZ6TMxMY7j7Fz20Q/OCPSou99beS5pzmYi jAszHb iPF5 izof eT5 j jmfk1vL2xs/HfA3J5FVLpvd j
Sm5mcROaQffleUKt1ZJm/68g.jy00NIS03Sm9LANLkbRZLM+YH
    left=123.45.67.1
    leftsubnet=194.153.205.0/24
    # RSA 2048 bits   Pare-feu1   Fri Jul  8 04:30:30 2005
    leftrsasigkey=0sAQFPQb6G1wXGa2qEMOiyUD/GxzyACGkk41hdhZrz7K4VTdf1ww72mygQZ
q2UsADBryb9U2/4rN1UenUbf8xcP0EiUqFs+KUopUT1XjUs9a i/oav57foq6BtaJqSnX1RQX0xThHFYU
o/LwU55zW532HWvuITnstTFLUv0obAma66DyGs3Uk/W12cXQWPCqvC9S7BRFmNqU6QLXczC+f0nEg ind
oYjg6Kd1Ghj18UnKeUcaeHthfLnesde9Zpy096wmb+U81+J4RwnY/REv69NArX730Es1cKxAfOp5vPJU
XD i7lWLu iA/ossYugMgf6PPAniHp4+h6ytm dpJ3 i bE10Kqv

```

Figure 5.2 : le fichier ipsec.conf de la passerelle Pare-feu1.

```

Version 2.0      # conforms to second version of ipsec.conf specification

# basic configuration
config setup
    interfaces="ipsec0=eth0"
    # Debug-logging controls: "none" for (almost) none, "all" for lots.
    klipsdebug=none
    plutodebug=none

conn %default
    keyingtries=0
    authby=rsasig
    auto=add

conn f1-f2
    right=123.45.67.2
    rightsubnet=194.153.204.0/24
    rightrsasigkey=0sAQ0gLoZxQL0lsQFURb8TGX/Pgk jF/LURMEbXALwrCsgHBR6OKS/pYp0
wiGZJyG5AEIwbEJmCP9TjcW+Fs17oRqg002/5C9x9s/6NCbzXpUEcvwEUdQ/MUhrCgOO/kdk+HW4PJDU
YFggMczapuIYNZAqZA413vmhZupC8m4P0EySSYkJ8SX0mJR8wyIBipWQFAoG7fq23s4ou1IFDYTxKjnY
QBtQxZ6TMxMY7j7Fz20Q/OCPSou99beS5pzmYi jAszHb iPF5 izofeT5 jjmFklvL2xs/HfA3J5FULpvdJ
Sm5mcR0aQffleUKt1ZJm/68g jy00NIS03Sm9LANLkbRZLM+YH
    left=123.45.67.1
    leftsubnet=194.153.205.0/24
    # RSA 2048 bits Firewall1 Fri Jul 8 04:30:30 2005
    _leftrsasigkey=0sAQPPQb6G1wXGa2qEMOiyUD/GxzyACGkk41hdhZrz7K4VTdf1ww72mygQZ
q2UsADBryb9U2/4rN1UenUbf8xcP0EiUqFs+KUopUT1XjUs9ai/oaov57foq6BtaJqSnX1RQX0xThHFYU
o/LwU55zW532HWvuITnstTFLUv0obAma66DyGs3Uk/W12cXQWPCqvC9S7BRFmNqU6QLXczC+f0nEg ind
oYjg6KdlGhj18UnKeUcaeHthfLnesde9Zpy096wmb+U81+J4RwnY/REv69NArX730Es1cKxAf0p5vPJU
XD171WLuia/ossYugMgf6PPAniHp4+h6ytmDpJ3ibE10Kqv

```

Figure 5.3 : le fichier ipsec.conf de la passerelle Pare-feu2.

Étape 4 : le test de la configuration.

Pour redémarrer Ipsec il suffit d'exécuter la commande "ipsec setup --restart"

```

[root@Pare-feu2 root]# ipsec setup --restart
ipsec_setup: Stopping FreeS/WAN IPsec...
IPSEC EVENT: KLIPS device ipsec0 shut down.

ipsec_setup: Starting FreeS/WAN IPsec 2.06...
ipsec_setup: Using /lib/modules/2.4.20-8/kernel/net/ipsec/ipsec.o

[root@Pare-feu2 root]# _

```

Figure 5.4 : le démarrage de Ipsec.

Lorsqu'on installe Ipsec, une interface ipsec0 s'ajoute. Cet interface va être utiliser par Ipsec pour la communication sécurisée. Nous pourrons bien voir cet interface en utilisant la

commande ifconfig (Voir la figure 5.5). Nous remarquons que le nombre de paquet envoyé et reçu est à 0 (on n'a pas encore envoyé du trafic via cette interface).

```
ipsec0 Link encap:Ethernet HWaddr 00:0C:29:64:CE:C6
inet addr:123.45.67.1 Mask:255.0.0.0
UP RUNNING NOARP MTU:16260 Metric:1
RX packets:0 errors:0 dropped:0 overruns:0 frame:0
TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:10
RX bytes:0 (0.0 b) TX bytes:0 (0.0 b)
```

Figure 5.5 : l'interface Ipsec0 sur la passerelle Pare-feu1.

La commande «ipsec auto –up f1-f2» permet de démarrer la connexion VPN f1-f2, (Voir la figure 5.6).

```
[root@Pare-feu1 root]# ipsec auto --up f1-f2
104 "f1-f2" #1: STATE_MAIN_I1: initiate
106 "f1-f2" #1: STATE_MAIN_I2: sent MI2, expecting MR2
108 "f1-f2" #1: STATE_MAIN_I3: sent MI3, expecting MR3
004 "f1-f2" #1: STATE_MAIN_I4: ISAKMP SA established
112 "f1-f2" #2: STATE_QUICK_I1: initiate
004 "f1-f2" #2: STATE_QUICK_I2: sent QI2, IPsec SA established {ESP=>0xaf78af88
<0x0812ead4}
[root@Pare-feu1 root]# _
```

Figure 5.6 : démarrage de la connexion VPN.

La ligne «Interfaces ipsec0=eth0» dans le fichier de configuration, attache l'interface virtuel ipsec0 à une interface physique. La commande «ipsec tncfg» permet de voir à quel interface physique ipsec0 est attaché effectivement.

```
[root@Pare-feu1 root]# ipsec tncfg
ipsec0 -> eth1 mtu=16260(1500) -> 1500
ipsec1 -> NULL mtu=0(0) -> 0
ipsec2 -> NULL mtu=0(0) -> 0
ipsec3 -> NULL mtu=0(0) -> 0
[root@Pare-feu1 root]# _
```

Figure 5.7 : attachement de l'interface ipsec0 à un interface physique.

Lorsque la connexion VPN est établie, la commande «ipsec eroute» permet d'afficher les tunnels actifs.

```
[root@Pare-feu1 root]# ipsec eroute
0          194.153.205.0/24  -> 194.153.204.0/24  => tun0x10020123.45.67.2
[root@Pare-feu1 root]# _
```

Figure 5.8 : affichage des tunnels actifs.

La remarque la plus important à faire est que, le VPN est établie entre les deux réseaux et pas entre les deux passerelles. Donc les informations qui sont envoyées entre les deux passerelles ne sont pas chiffrées. C'est la communication entre les deux réseaux 194.153.204.0 et 194.153.205.0, qu'est sécurisé.

Pour s'assurer que l'échange entre les deux réseaux est bien chiffré, nous allons envoyer un Ping de la machine Interne vers Externe et nous allons capturer le trafic via l'interface externe de la passerelle Pare-feu1. La figure 5.9 montre les paquets ESP échangés.

```
[root@Pare-feu1 root]# tcpdump -i eth1
tcpdump: listening on eth1
11:52:00.915205 123.45.67.1 > 123.45.67.2: ESP (spi=0x73b2fa46, seq=0x1)
11:52:00.953364 123.45.67.2 > 123.45.67.1: ESP (spi=0x40ed90de, seq=0x1)
11:52:01.935107 123.45.67.1 > 123.45.67.2: ESP (spi=0x73b2fa46, seq=0x2)
11:52:01.936500 123.45.67.2 > 123.45.67.1: ESP (spi=0x40ed90de, seq=0x2)
11:52:03.100126 123.45.67.1 > 123.45.67.2: ESP (spi=0x73b2fa46, seq=0x3)
11:52:03.102612 123.45.67.2 > 123.45.67.1: ESP (spi=0x40ed90de, seq=0x3)
11:52:04.250054 123.45.67.1 > 123.45.67.2: ESP (spi=0x73b2fa46, seq=0x4)
11:52:04.250997 123.45.67.2 > 123.45.67.1: ESP (spi=0x40ed90de, seq=0x4)
11:52:05.264831 123.45.67.1 > 123.45.67.2: ESP (spi=0x73b2fa46, seq=0x5)
11:52:05.273372 123.45.67.2 > 123.45.67.1: ESP (spi=0x40ed90de, seq=0x5)
```

Figure 5.9 : capture d'une communication Ipcsec.

Une autre façon de confirmer que le trafic passe bien par le tunnel Ipcsec, est d'exécuter la commande «ifconfig ipsec0».

```

[root@Pare-feu1 root]# ifconfig ipsec0
ipsec0   Link encap:Ethernet  HWaddr 00:0C:29:64:CE:C6
         inet addr:123.45.67.1  Mask:255.0.0.0
         UP RUNNING NOARP  MTU:16260  Metric:1
         RX packets:286 errors:0 dropped:0 overruns:0 frame:0
         TX packets:286 errors:0 dropped:0 overruns:0 carrier:0
         collisions:0 txqueuelen:10
         RX bytes:24024 (23.4 Kb)  TX bytes:42900 (41.8 Kb)

[root@Pare-feu1 root]# _

```

Figure 5.10 : le nombre de paquet envoyé et reçu via l'interface ipsec0.

D'après la figure 5.10, on voit bien que le nombre de paquet envoyé et reçu via l'interface ipsec0 est différent de 0. Nous pourrions obtenir la configuration complète de Ipsec sur une machine en utilisant la commande «ipsec look». La commande «ipsec look» affiche les réseaux liés par le VPN, les protocoles de chiffrement utilisés, les tunnels actifs et la table routage. (Voir la figure 5.11).

```

[root@Pare-feu1 root]# ipsec look
Pare-feu1 Fri Sep  2 12:00:15 EDT 2005
194.153.205.0/24  -> 194.153.204.0/24  => tun0x10020123.45.67.2 esp0x73b2fa460
123.45.67.2 (483)
ipsec0->eth1 mtu=16260(1443)->1500
esp0x40ed90de@123.45.67.1 ESP_3DES_HMAC_MD5: dir=in src=123.45.67.2 iv_bits=64b
its iv=0xbcb9ea70b212f9d ooowin=64 seq=483 bit=0xffffffff alen=128 akle
n=128 eklen=192 life(c,s,h)=bytes(50232,0,0)addtime(526,0,0)usetime(494,0,0)pack
ets(483,0,0) idle=0 refcount=487 ref=7
esp0x73b2fa46@123.45.67.2 ESP_3DES_HMAC_MD5: dir=out src=123.45.67.1 iv_bits=64b
its iv=0xb8120f9804992f2b ooowin=64 seq=483 alen=128 aklen=128 eklen=192 life(c,
s,h)=bytes(65688,0,0)addtime(525,0,0)usetime(494,0,0)packets(483,0,0) idle=0 ref
count=4 ref=12
tun0x10010123.45.67.1 IP/IP: dir=in src=123.45.67.2 policy=194.153.204.0/24->194
.153.205.0/24 flags=0x8<> life(c,s,h)=bytes(50232,0,0)addtime(526,0,0)usetime(49
4,0,0)packets(483,0,0) idle=0 refcount=4 ref=6
tun0x10020123.45.67.2 IP/IP: dir=out src=123.45.67.1 life(c,s,h)=bytes(50232,0,0)
addtime(525,0,0)usetime(494,0,0)packets(483,0,0) idle=0 refcount=4 ref=11

```

Destination	Gateway	Genmask	Flags	MSS	Window	irrt	Iface
0.0.0.0	123.45.67.2	0.0.0.0	UG	0	0	0	eth1
123.0.0.0	0.0.0.0	255.0.0.0	U	0	0	0	eth1
123.0.0.0	0.0.0.0	255.0.0.0	U	0	0	0	ipsec0
169.254.0.0	0.0.0.0	255.255.0.0	U	0	0	0	eth1
194.153.204.0	123.45.67.2	255.255.255.0	UG	0	0	0	ipsec0

```

[root@Pare-feu1 root]# _

```

Figure 5.11 : la configuration complète de ipsec sur firewall1.

6. Ipv4 et le pare-feu.

Nous allons utiliser les passerelles Ipv4 comme des pare-feu. Pour s'assurer que ces deux pare-feu passent proprement le trafic, il faut savoir les ports utilisés par les deux protocoles IKE et ESP.

IKE utilise le protocole 50 pour la négociation de la connexion et le protocole ESP utilise le port 500 pour l'authentification et le chiffrement. Il faut donc accepter le trafic entrant et sortant à travers le port 500, ainsi que le trafic utilisant le protocole 50.

```
Iptables -A INPUT -p udp --sport 500 --dport 500 -j ACCEPT
Iptables -A OUTPUT -p udp --sport 500 --dport 500 -j ACCEPT
Iptables -A INPUT -p 50 -j ACCEPT
Iptables -A OUTPUT -p 50 -j ACCEPT
```

Figure 6.1 : permettre le trafic associé au protocole AH et ESP.

7. Ipv4 et la performance.

Comme rien n'est gratuit dans ce monde, l'utilisation d'Ipv4 ou d'un mécanisme de chiffrement en général impose des ressources et des coûts en matière de temps de calcul et de mémoire, ce qui pourra augmenter considérablement le temps de latence. Le tableau 7.1 montre comment le temps de téléchargement augmente en fonction de la taille du fichier transféré lorsqu'Ipv4 est activé.

Tableau 7.1 : le temps de transfert avec et sans Ipv4.

	Fichier3	Fichier4	Fichier5	Fichier6	Fichier7	Fichier8
Taille (Mo)	1.067	1.961	5.117	10.054	22.004	32.516
Sans Ipv4 (sec)	1.13	1.63	4.05	7.18	10.3	15.3
Avec Ipv4 (sec)	2.41	3.94	7.96	13.7	27.6	30.2
Différence (sec)	1.28	2.31	3.91	6.52	17.3	14.9

On remarque bien que pour les grands fichiers (7^{ème} et 8^{ème}) la différence devient beaucoup plus importante.