


TP n° 4 — Virtual Private Network par ipsec

F. Butelle

Ce TP est conçu pour fonctionner avec marionnet (voir www.marionnet.org). Il suppose des machines virtuelles Mageia4¹.

1 Mise en place

1.  Si vous êtes à l'IUT dans une nouvelle salle de TP hybride (sauf T206), vous devez ouvrir un terminal et taper :

```
$ source /iutv/Mes_Montages/TP/TPINFO/bashrc
```

(Dans le doute, utilisez la commande `$ ls_b_release -d` : si c'est Ubuntu 20 alors il faut faire la commande précédente)

Nous allons utiliser **uniquement** des Machines Virtuelles de type **Mageia4** avec un noyau linux $\geq 3.2.64$.

2. Pour pouvoir avoir ce type de MV, **avant de lancer marionnet**, tapez dans un terminal de l'hôte :

```
$ mario installMV mageia4
```

...Patientez!

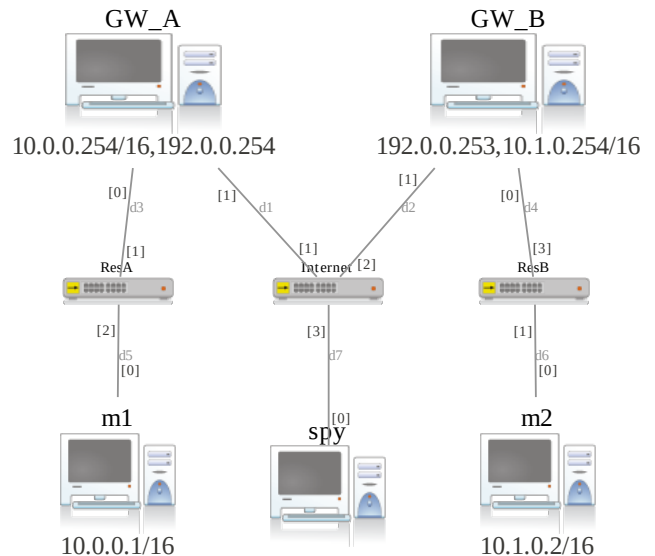
3. démarrez `$ checkMario` et choisissez le projet R4.08/TP4-VPN! Ne lancez l'évaluation que lorsque vous pensez que c'est bon ou pour vous aider à déboguer.


4. Ajoutez les câbles et hubs nécessaires pour faire comme le réseau ci-contre

(Remarque : Les machines GW_A et GW_B sont des «*routeurs du pauvre*» : des PCs avec deux cartes réseaux!)

5. Les adresses IP doivent être fixées par l'onglet Interfaces de marionnet. De même, les routes par défaut sont configurables dans cet onglet par la case "Passerelle IPv4", après avoir cliqué sur la flèche devant le nom des machines (ou sur la loupe avec un +) :

Composants	Documents	Réseau virtuel					
Nom	Type	Adresse MAC	MTU	Adresse IPv4	Passerelle IPv4	Adresse	
GW_A	eth0	02:04:06:54:ae:b0	1500	10.0.0.254/16			
	eth1	02:04:06:7f:1e:bc	1500	192.0.0.254	192.0.0.253		



6. Démarrez toutes les machines
7.  Il faut activer le «forwarding» sur GW_A et GW_B et désactiver les redirections faites par le protocole ICMP : créez un fichier `/etc/sysctl.d/ipsec.conf` sur chacun, avec comme contenu :

```
net.ipv4.ip_forward=1
net.ipv4.conf.all.accept_redirects=0
net.ipv4.conf.default.accept_redirects=0
net.ipv4.conf.all.send_redirects=0
net.ipv4.conf.default.send_redirects=0
```

8. Faire `$ systemctl restart systemd-sysctl` sur les deux GW pour prendre en compte ces valeurs.
9. Pour une première vérification faire : `$ ipsec verify` sur chaque GW. La **première** erreur détectée doit être :

```
| Checking that pluto is running                                     [FAILED]
```

En cas de problème avant cette ligne revoir les étapes précédentes.

Note : *rp_filter* signifie Reverse Path Filtering : à la réception d'un paquet le système vérifie que l'adresse source est une adresse de retour routable, sinon le paquet est détruit.

1. Au besoin téléchargeable ici : <http://www-info.iutv.univ-paris13.fr/~butelle/machine-mageia4.tar.xz>

2 Routage

2.1 Vérifications

- Faire un `$ ping` de m1 à m2.

Si le ping de m1 à m2 ne fonctionne pas, revérifiez toutes les adresses, les tables de routages y compris celles de m1 et m2 (la table donnée par la commande route doit comporter 2 lignes pour m1 et m2, 3 lignes pour GW_A et GW_B). Attention aussi aux branchements des cartes réseaux de GW_A et GW_B (eth1 sur le hub Internet) et aussi vérifiez que le forwarding est bien activé par `$ sysctl net.ipv4.ip_forward`

Rappel : ajouter une route par défaut : `$ route add default gw <adressePasserelle>`, supprimer une route : mettre `del` à la place de `add`.

Tables de routage :

M1				
Destination	GW	Mask	Flags	Interf.
10.0.0.0	-	255.255.0.0	U	eth0
default	10.0.0.254	0.0.0.0	UG	eth0
GW_A				
Destination	GW	Mask	Flags	Interf.
10.0.0.0	-	255.255.0.0	U	eth0
192.0.0.0	-	255.255.255.0	U	eth1
default	192.0.0.253	0.0.0.0	UG	eth1
GW_B				
Destination	GW	Mask	Flags	Interf.
10.1.0.0	-	255.255.0.0	U	eth0
192.0.0.0	-	255.255.255.0	U	eth1
default	192.0.0.254	0.0.0.0	UG	eth1
M2				
Destination	GW	Mask	Flags	Interf.
10.1.0.0	-	255.255.0.0	U	eth0
default	10.1.0.254	0.0.0.0	UG	eth0

2.2 Activez l'espion

Si le ping est ok, activez la carte réseau sur l'espion (spy) par

- `$ ifconfig eth0 up`
- puis démarrez `$ wireshark` sur l'espion (spy) (il est lent, il faut être patient : s'il ne démarre pas dans les 10s, arrêtez tout dans marionnet, sauvez le projet, fermer marionnet et le relancer)
- puis un ping de m1 à m2...
- Que voyez vous passer comme paquets entre les passerelles?

**Des paquets ICMP (pour ping) et aussi des paquets ARP pour l'association adresse IP <=> adresse MAC.
A condition bien sûr d'avoir utilisé un HUB pour "Internet" et non un switch...**

3 Configuration du VPN ipsec

3.1 Authentification

Il faut maintenant configurer ipsec sur GW_A ET GW_B. Pour trouver les fichiers de config : `$ ipsec --confdir`. Normalement c'est dans `/etc/openswan`. Modifier `/etc/openswan/ipsec.conf` (par exemple avec nano) :

```
version 2.0
config setup
    plutodebug="control parsing"
    protostack=auto
    plutostderrlog=/var/log/pluto
```

```
conn maconnexion
  type=tunnel
  phase2=ah
  authby=secret
  left=adresse publique de la passerelle
  leftsubnet=adresse du réseau prive derriere la passerelle
  right=adresse publique de la passerelle d'en face
  rightsubnet=adresse du reseau prive derriere la passerelle d'en face
  auto=start
```

```
#fichier ipsec.conf pour GW_A
version 2.0

config setup
  plutodebug="control parsing"
  protostack=auto
  plutostderrlog=/var/log/pluto

conn maconnexion
  type=tunnel
  phase2=ah
  authby=secret
  left=192.0.0.254
  leftsubnet=10.0.0.0/16
  right=192.0.0.253
  rightsubnet=10.1.0.0/16
  auto=start
```

Notes :

- Supprimez tout le contenu du fichier d'abord pour être sûr de ne pas garder une mauvaise configuration.
- *pluto* est l'implémentation du démon *ipsec*,
- *type=tunnel* indique que l'on veut relier deux passerelles, il existe aussi le mode transport pour faire du VPN direct d'hôte à hôte.
- *phase2=ah* signifie que l'on ne va utiliser que le protocole AH de IPsec, AH=Authentication Header. Donc même quand le tunnel IPsec va être en fonction vous devriez pouvoir voir le contenu des paquets, AH ne fait que rajouter une couche d'authentification.

Créez le fichier `/etc/openswan/ipsec.secrets` sur GW_A ET GW_B :

```
adresse_publique_GW adresse_publique_autre_GW : PSK "le mot de passe"
```

Sur GW_A :

```
192.0.0.254 192.0.0.253: PSK "le mot de passe"
```

On (re)démarré le service *ipsec* : `$ systemctl restart ipsec` (à peu près en même temps sur les 2 GW).

Vous pourrez vérifier que votre tunnel est en place avec `$ ipsec setup status` (en fait il est probable qu'il affiche 2 tunnels).

Vous pouvez consulter les logs de *ipsec* avec `$ systemctl status ipsec -l` et `$ tail /var/log/pluto`.

En particulier, `$ grep === /var/log/pluto` sur GW_A doit vous donner :

```
[root@GW_A ~]# grep === /var/log/pluto
"maconnexion" #3:      us: 10.0.0.0/16===192.0.0.254<192.0.0.254>
"maconnexion" #3:      them: 192.0.0.253<192.0.0.253>===10.1.0.0/16
```

Pour vous aider à déboguer ou à vérifier votre installation, lancez l'évaluation au niveau de checkMario, si tout est ok, vous pouvez passer à la suite.

3.2 Tests et observations

- Faites un ping entre `m1` et `m2`
- Activez le service web sur `m2` par `$ systemctl unmask httpd` puis `$ systemctl start httpd`.

- Au niveau de m1, le navigateur en mode texte est `$ lynx <URL>`.
Regardez les échanges dans wireshark (parfois le premier lancement de wireshark ne passe pas, il faut le relancer).
Quel est l'empilement protocolaire utilisé?

Ethernet,IP,AH,IP,TCP,HTTP

- Sur GW_A, faire `$ ip tunnel show` puis `$ ifconfig tunl0`.
tunl0 est une pseudo carte réseau qui est utilisée pour le tunnel, pourquoi son MTU est de 1480 au lieu de 1500?

La valeur de 1500 est liée au protocole Ethernet : la taille max des données dans Ethernet donne la taille max d'un paquet IP encapsulé dans Ethernet. Ici le tunnel consiste à tout faire passer dans des paquets IP, donc on perd les 20 octets de son entête.

3.3 Confidentialité

On veut maintenant ajouter la confidentialité à l'authentification.

- Dans ipsec.conf il faut mettre `phase2=ah+esp` pour qu'ipsec utilise *Encapsulating Security Payload* en plus de AH (souvent on se contente d'ESP qui apporte confidentialité et intégrité).
- Modifiez les fichiers ipsec.conf des passerelles pour utiliser ah+esp et relancez les services ipsec sur chaque passerelle.
- Essayez à nouveau une communication entre m1 et m2... Comment vérifier que la communication est chiffrée?

Oui dans l'analyseur on ne peut voir que l'encapsulation : Ethernet,IP,AH,ESP et puis c'est tout : même les adresses de l'émetteur et du destinataire dans les réseaux privés ne sont visibles.