L'Internet Rapide et Permanent

Virtual Private Network

Par Christian Caleca

Date de publication : 3 mars 2009

Vous disposez d'une connexion permanente et rapide… et maintenant, vous êtes perdu dans la technique…

Cette série « L'Internet Rapide et Permanent », que Christian Caleca nous a aimablement autorisé à reproduire, est là pour répondre à quelques-unes de ces questions. Cet article parlera des réseaux privés virtuels (Virtual Private Network en littérature anglaise ou encore VPN).

N'hésitez pas à commenter cet article !

1 - Introduction

1-1 - Les tunnels

Grâce à un tunnel, il est possible de passer directement d'un point à un autre, sans devoir subir les affres de la circulation à la surface. Les tunnels informatiques s'en rapprochent fortement, en proposant un moyen de relier « directement » deux réseaux privés distants, à travers un interréseau aussi complexe que l'internet.

Il existe une grande quantité de moyens pour réaliser des tunnels informatiques. PPP peut être considéré comme un tunnel dans des configurations comme PPPoE ou PPPoA. L2TP (Layer 2 Tunneling Protocol), est utilisé sur les réseaux des opérateurs, par exemple dans les connexions ADSL non dégroupées.

PPTP (Point to Point Tunneling Protocol), utilisé par Microsoft, ou encore les tunnels sur IPSec sont d'autres solutions. L'objectif de ce chapitre est de montrer le fonctionnement d'un tunnel sur IP à travers une implémentation standardisée : le tunnel GRE, puis à travers une solution plus sécurisée : OpenVPN.

Merci à _SebF, créateur du site **frameip.com**, pour son aimable collaboration.

1-2 - Le principe

Imaginons que nous ayons à intervenir sur deux réseaux privés différents, géographiquement éloignés, les réseaux A et B. Si nous voulons interconnecter ces deux réseaux, nous avons a priori deux possibilités :

- l'une cher, qui consiste à utiliser une liaison spécialisée, proposée par tout bon opérateur de télécoms. Les technologies utilisées par ces opérateurs afin de créer notre réseau privé sont principalement du type ATM (1) , MPLS (2) et, plus anciennement, Frame Relay.
  Les avantages apportés sont la garantie d'un SLA (3) et d'une étanchéité renforcée ;
- l'autre, moins chère, qui consiste à interconnecter ces deux réseaux via de l'internet public.

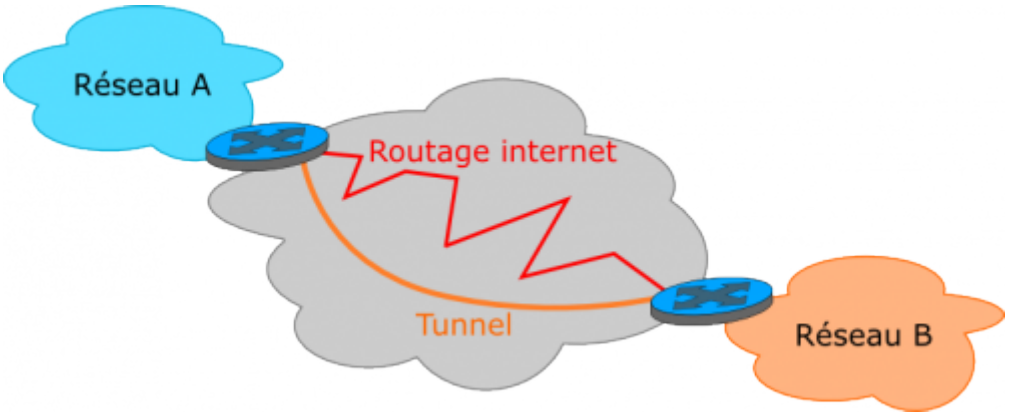
Oui, mais la seconde solution, a priori moins chère, sera plus limitative :

- soit, comme c'est le plus souvent le cas, nous ne disposerons que d'une seule adresse IP publique pour accéder à chaque réseau et dans ce cas, nous ne pourrons pas faire facilement communiquer n'importe quelle machine du réseau A avec n'importe quelle machine du réseau B, puisque ces LAN seront montés avec des adresses IP privées (voyez le **Partage de connexion**, mis en œuvre dans de telles configurations) ;
- soit nous disposons de suffisamment d'adresses IP publiques pour monter nos réseaux avec ces adresses, mais alors, toutes nos machines seront directement exposées sur le Net. Cher et difficile (il n'est pas simple, et encore moins gratuit d'obtenir des plages, même petites, d'adresses IPv4 publiques, encore qu'avec IPv6, ce sera tout à fait réalisable) et pour le moins dangereux.

Comment faire alors ?

Créer une ligne spécialisée virtuelle, qui passera par l'internet, mais qui fonctionnera presque comme une liaison spécialisée. Bien sûr, pour ce faire, un tunnel est nécessaire afin de créer l'interconnexion, de garantir l'étanchéité. L'avantage est de ne pas être dépendant d'un opérateur et ainsi, de pouvoir choisir la sortie internet de chaque site indépendamment les unes des autres. Rien en effet n'interdit de construire plusieurs tunnels, éventuellement sur des connexions internet différentes. Nous disposons de plusieurs technologies telles que PPtP, IPSec et celles qui nous intéressent dans cette documentation : le tunnel GRE et OpenVPN.

Au niveau IP, un tunnel se présente comme ceci :



Et nous aurons l'impression d'avoir à peu près cela :

Bien que la première couche IP circule normalement sur l'internet, en suivant les routes définies par les opérateurs, celle-ci transporte une seconde couche IP et sur cette couche, tout va se passer comme si les deux routeurs communiquaient directement, par l'intermédiaire d'un réseau IP ne comportant que deux nœuds : les deux routeurs.

Grâce à ce tunnel, tout nœud du réseau A pourra communiquer avec tout nœud du réseau B, les deux réseaux étant construits avec des adresses IP **privées**.

Super non ?

Oui, mais souvenez-vous que IPv4 est un protocole qui n'est pas sécurisé, que nous allons l'utiliser et qui plus est, sur un réseau plutôt mal famé. L'opération n'est donc pas sans risques.

1-3 - Comment ça marche

Toujours le même principe, l'encapsulation d'un protocole dans un autre protocole de même niveau. Le plus souvent, nous encapsulerons de l'IP dans de l'IP. Mais pour mieux comprendre, il nous faut poser le problème de façon plus précise.

	Réseau A	**Réseau B**
Adresses :	172.16.0.0	192.168.0.0
Masque :	255.255.0.0	255.255.255.0
Routeur côté LAN :	172.16.254.1	192.168.0.252
Routeur côté internet :	81.248.152.18	80.8.147.232

Les routeurs A et B peuvent discuter entre eux à travers l'internet, puisqu'ils disposent tous deux d'une adresse IP publique. Au niveau IP, le transfert de données est donc réalisable.

Sur cette couche IP, nous encapsulons une seconde couche IP, qui va faire de telle sorte que l'ensemble des routeurs A et B avec le tunnel entre les deux, apparaisse comme un unique routeur, directement connecté aux réseaux A et B, et qui aura :

- 172.16.254.1 dans le réseau A ;
- 192.168.0.252 dans le réseau B.

Nous sommes entre deux réseaux privés, interconnectés par un routeur, rien que de bien classique.

1-4 - Démonstration

Peu importe pour l'instant, la façon dont le tunnel est créé. Depuis un hôte de réseau B d'IP 192.168.0.10, nous faisons un traceroute vers l'hôte du réseau A d'IP 172.16.252.2 :

```
C:\>tracert -d 172.16.252.2
Détermination de l'itinéraire vers 172.16.254.2 avec un maximum de 30 sauts.
  1    <1 ms    <1 ms    <1 ms  192.168.0.252
  2    60 ms    63 ms    59 ms  172.16.254.1
  3    75 ms    63 ms    61 ms  172.16.252.2

Itinéraire déterminé.
```

Et pourtant, si l'on cherche la « vraie route », celle qui est réellement empruntée par le tunnel, nous aurons quelque chose de cette forme entre les deux routeurs :

```
gw2:~# traceroute -n -I 81.248.152.18
traceroute to 81.248.152.18, 30 hops max, 38 byte packets
1 80.8.160.1 49.763 ms 32.095 ms 8.960 ms
2 172.19.46.65 10.883 ms 8.700 ms 11.688 ms
3 193.252.227.82 17.019 ms 23.244 ms 22.403 ms
4 80.10.209.233 38.494 ms 12.467 ms 12.732 ms
5 81.248.152.18 58.968 ms 60.676 ms 60.891 ms
```

Bien entendu, le « vrai » chemin peut être beaucoup plus long, si les deux réseaux A et B sont plus éloignés, mais le chemin par le tunnel gardera sa simplicité dans tous les cas.

1-5 - Mise en œuvre

Pour démontrer le fonctionnement des tunnels, nous verrons deux outils possibles :

- **Le tunnel GRE** ;
- **Open VPN**.

2 - Le tunnel GRE

2-1 - Avertissements

Il existe avec Linux un type de tunnel qui encapsule de l'IP sur IP. Cette solution n'existe, semble-t-il, que sous Linux et reste assez limitative. Nous allons plutôt utiliser une méthode normalisée, à peine plus complexe : le tunnel GRE. Ne confondez donc pas ces deux possibilités.

Le tunnel GRE (Generic Routine Encapsulation) fonctionne parfaitement. C'est un protocole ouvert, initialement développé par CISCO, et qui peut donc se mettre en place sur des plates-formes différentes. Il est défini par le **RFC 2784** :

- il est possible d'ouvrir plusieurs tunnels depuis un hôte donné ;
- il est conçu pour pouvoir encapsuler n'importe quel protocole de niveau 3 dans IP. Pratiquement, le plus souvent, de l'IP dans de l'IP.

Malheureusement, ce n'est pas un protocole sécurisé. Si vous l'utilisez sur l'internet, mesurez les risques que vous prenez !

Faites une recherche sur les façons de prendre possession d'un réseau utilisant un tel tunnel et vous serez fixé. Ce n'est pas facile à faire, mais c'est tout à fait réalisable. Vous êtes prévenu :

- GRE ne prévoit pas de chiffrement des données qui passent dans le tunnel, il n'est pas étanche ;
- GRE ne prévoit pas l'authentification des extrémités du tunnel, vous n'êtes sûr que de l'authenticité de votre bout de tunnel.

(Je l'ai peut-être déjà dit…)

2-2 - Construction

Juste pour voir comme c'est simple à monter, et comme un tunnel peut rendre des services, nous allons tout de même en réaliser un, le temps de faire la manip.

Reprenons la topologie utilisée.

2-2-1 - Les deux réseaux

Les deux réseaux A et B sont les mêmes que définis sur la page « **Virtual Private Network** ».

Les deux routeurs sont des machines sous Linux, avec un noyau 2.4.x. Il nous faut disposer d'iproute2. Toutes les distributions le proposent, mais ne l'installent pas forcément par défaut.

2-2-2 - On creuse

Un tunnel, ça se creuse des deux côtés à la fois. Il faut donc intervenir sur les deux routeurs.

2-2-2-1 - Réseau A

- Amener les outils. Il faut charger le module nécessaire à la construction du tunnel :
  modprobe ip_gre.
- Construire le tunnel :
  ip tunnel add netb mode gre remote 80.8.147.232 local 81.248.152.18 ttl 255.
- netb est le nom de la nouvelle interface réseau qui va conduire au réseau B.
- L'adresse IP de l'autre bout du tunnel (remote) est 80.8.147.232.
- L'adresse IP de ce bout-ci du tunnel (local) est 81.248.152.18.
- On indique un ttl (time to live) maximum (255).
- Monter l'interface réseau :
  ip link set netb up.
- Lui donner une adresse IP qui sera la même que celle de l'interface qui supporte le tunnel dans le réseau local :
  ip addr add 172.16.254.1 dev netb.
- Ici il s'agit de 172.16.254.1.
- Baliser la route vers le réseau B :
  ip route add 192.168.0.0/24 dev netb.

Et voilà. Le tunnel est creusé du côté A. Reste à refaire la même chose du côté B (aux adresses IP près).

2-2-2-2 - Réseau B

- Amener les outils. Il faut charger le module nécessaire à la construction du tunnel :
  modprobe ip_gre.

- Construire le tunnel :
  ip tunnel add neta mode gre remote 81.248.152.18 local 80.8.147.232 ttl 255.
- neta est le nom de la nouvelle interface réseau qui va conduire au réseau A.
- L'adresse IP de l'autre bout du tunnel (remote) est 81.248.152.18 ;
- L'adresse IP de ce bout-ci du tunnel (local) est 80.8.147.232.
- On indique un ttl (time to live) maximum (255).
- Monter l'interface réseau :
  ip link set neta up.
- Lui donner une IP qui sera la même que celle de l'interface qui supporte le tunnel dans le réseau local :
  ip addr add 192.168.0.252 dev neta.
- Ici il s'agit de 192.168.0.252.
- Baliser la route vers le réseau A :
  ip route add 172.16.0.0/16 dev neta.

Et le tunnel est entièrement creusé et opérationnel. Bien entendu, il vous faudra ajouter dans les règles IPtables, ce qui est nécessaire pour que ça fonctionne. C'est à vous de voir en fonction de vos règles en place. On peut imaginer que ces choses du genre :

```
iptables -A FORWARD -i netb -j ACCEPT
iptables -A FORWARD -o netb -j ACCEPT
```

dans le réseau A, et

```
iptables -A FORWARD -i neta -j ACCEPT
iptables -A FORWARD -o neta -j ACCEPT
```

dans le réseau B permettront de laisser passer le trafic dans le tunnel, mais il peut être utile, voire nécessaire, de faire des choses moins permissives.

La notation de type 172.16.0.0/16 maintenant souvent utilisée pour identifier un réseau. Le « /16 » indique que les 16 bits les plus lourds, les plus à gauche, sont les seuls bits à considérer pour identifier le réseau. Autrement dit, que le masque de sous-réseau est 255.255.0.0.

2-2-3 - Vérifications

2-2-3-1 - Les interfaces

Utilisons iproute2, puisque nous l'avons :

```
gw2:~# ip link list
1: lo: <LOOPBACK,UP> mtu 16436 qdisc noqueue
link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
2: eth0: <BROADCAST,MULTICAST,ALLMULTI,UP> mtu 1500 qdisc pfifo_fast qlen 100
link/ether 52:54:05:fc:ad:0c brd ff:ff:ff:ff:ff:ff
3: eth1: <BROADCAST,MULTICAST,ALLMULTI,UP> mtu 1500 qdisc pfifo_fast qlen 100
link/ether 00:20:af:2f:5d:16 brd ff:ff:ff:ff:ff:ff
25: ppp0: <POINTOPOINT,MULTICAST,NOARP,UP> mtu 1492 qdisc pfifo_fast qlen 3
link/ppp
26: gre0@NONE: <NOARP> mtu 1476 qdisc noop
link/gre 0.0.0.0 brd 0.0.0.0
27: neta@NONE: <POINTOPOINT,NOARP,UP> mtu 1468 qdisc noqueue
link/gre 80.8.147.132 peer 81.248.152.18
```

- 25: ppp0 est le lien PPP vers le réseau du fournisseur d'accès internet ;
- 26: gre@NONE est le tunnel lui-même ;
- 27: neta@NONE est l'interface virtuelle, qui correspond à l'extrémité du tunnel.

Notez le MTU qui diminue à chaque niveau, ce qui est normal. Dans cette situation, nous avons sur Ethernet (niveau 2) :

- une couche PPP (PPPoE) ;
  - une couche IP sur ce lien PPP ;
    - un tunnel GRE sur cette couche IP ;
      - une couche IP dans le tunnel.

Les encapsulations successives entrainent à chaque étape, une diminution de la charge utile des paquets (« payload »), donc le MTU diminue.

Notez bien la particularité de GRE : ce n'est pas à proprement parler de l'IP sur IP, mais de l'IP dans GRE dans de l'IP. GRE apparaît comme un protocole intermédiaire, nous le reverrons plus pratiquement sur une analyse de trames.

2-2-3-2 - Snif d'un ping

Nous allons faire un petit ping depuis une machine du réseau B (192.168.0.10) vers une machine du réseau A (172.16.252.2).

Nous observons les trames au niveau du routeur B sur l'interface neta (donc au niveau de l'extrémité du tunnel) :

```
Frame 1 (76 bytes on wire, 76 bytes captured)
    Arrival Time: Mar  3, 2004 16:05:17.050838000
    Time delta from previous packet: 0.000000000 seconds
    Time since reference or first frame: 0.000000000 seconds
    Frame Number: 1
    Packet Length: 76 bytes
    Capture Length: 76 bytes
Linux cooked capture
    Packet type: Sent by us (4)
    Link-layer address type: 778
    Link-layer address length: 0
    Source: <MISSING>
    Protocol: IP (0x0800)


      Comme c'est finalement assez logique, nous ne trouvons pas sur cette interface
      de couche  Ethernet.
      Il nous faudrait étudier de façon plus précise le protocole GRE, mais ce n'est
      pas l'objet de ce chapitre.

Internet Protocol, Src Addr: 192.168.0.10, Dst Addr: 172.16.252.2
   Version: 4
   Header length: 20 bytes
   Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
       0000 00.. = Differentiated Services Codepoint: Default (0x00)
       .... ..0. = ECN-Capable Transport (ECT): 0
       .... ...0 = ECN-CE: 0
   Total Length: 60
   Identification: 0x1b61 (7009)
   Flags: 0x00
       .0.. = Don't fragment: Not set
       ..0. = More fragments: Not set
   Fragment offset: 0
   Time to live: 127
   Protocol: ICMP (0x01)
   Header checksum: 0x9d0c (correct)
   Source: 192.168.0.10 (192.168.0.10)
   Destination: 172.16.252.2 (172.16.252.2)
Internet Control Message Protocol
   Type: 8 (Echo (ping) request)
   Code: 0
   Checksum: 0x2d5c (correct)
   Identifier: 0x0200
   Sequence number: 0x1e00
```

```
    Data (32 bytes)

0000  61 62 63 64 65 66 67 68 69 6a 6b 6c 6d 6e 6f 70   abcdefghijklmnop
0010  71 72 73 74 75 76 77 61 62 63 64 65 66 67 68 69   qrstuvwabcdefghi
Et la réponse :
Frame 2 (76 bytes on wire, 76 bytes captured)
    Arrival Time: Mar  3, 2004 16:05:17.177500000
    Time delta from previous packet: 0.126662000 seconds
    Time since reference or first frame: 0.126662000 seconds
    Frame Number: 2
    Packet Length: 76 bytes
    Capture Length: 76 bytes
Linux cooked capture
    Packet type: Unicast to us (0)
    Link-layer address type: 778
    Link-layer address length: 0
    Source: <MISSING>
    Protocol: IP (0x0800)
Internet Protocol, Src Addr: 172.16.252.2, Dst Addr: 192.168.0.10
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 60
    Identification: 0x067e (1662)
    Flags: 0x00
        .0.. = Don't fragment: Not set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 127
    Protocol: ICMP (0x01)
    Header checksum: 0xb1ef (correct)
    Source: 172.16.252.2 (172.16.252.2)
    Destination: 192.168.0.10 (192.168.0.10)
Internet Control Message Protocol
    Type: 0 (Echo (ping) reply)
    Code: 0
    Checksum: 0x355c (correct)
    Identifier: 0x0200
    Sequence number: 0x1e00
    Data (32 bytes)

0000  61 62 63 64 65 66 67 68 69 6a 6b 6c 6d 6e 6f 70   abcdefghijklmnop
0010  71 72 73 74 75 76 77 61 62 63 64 65 66 67 68 69   qrstuvwabcdefghi
```

Ça marche. Vu au niveau de l'interface neta, tout se passe comme nous avons l'habitude de le voir sur un réseau IP. Notez toutefois que le sniffeur ne reconnaît pas la couche de niveau 2 (ce qui est surligné en bleu pâle).

2-2-4 - Conclusions

Mesurez bien la portée de ce que nous venons de faire…

Au travers de l'internet, nous avons créé une liaison spécialisée virtuelle qui permet de relier entre eux deux réseaux IP. Ces deux réseaux sont constitués avec des IP **privées**, et semblent simplement interconnectés par un routeur. Une adresse IP privée du réseau A dialogue sans problème avec une autre adresse IP privée du réseau B, et réciproquement. Pourtant, le lien entre ces deux réseaux est bel et bien bâti sur l'internet, où ces adresses IP privées sont bannies.

En d'autres termes, si le réseau B est le réseau de votre lieu de travail et le réseau A celui de votre domicile, vous pouvez par exemple :

- depuis chez vous sous Windows, accéder à votre répertoire partagé sur votre lieu de travail par le voisinage réseau Microsoft ;

- en utilisant la connexion du bureau à distance, vous pouvez depuis chez vous travailler sur votre poste de travail professionnel ;
- et d'une manière générale, depuis chez vous, vous pouvez faire tout ce que vous faites sur votre lieu de travail.

Bien entendu, vous êtes tout de même limité par le débit de votre connexion. Vous aurez un tuyau d'environ 128 kbps dans le cas le plus courant d'une connexion de type ADSL, rien de comparable, donc, avec un réseau local qui sera au minimum de 10 Mbps.

2-2-5 - Mais encore une fois attention !!!

Ce type de tunnel n'est absolument pas sécurisé, vous l'ai-je déjà dit ?

- Les données ne sont pas chiffrées dans le tunnel.
- Les deux extrémités du tunnel ne disposent d'aucun processus d'authentification.

Donc, si ce tunnel est en théorie magnifique, en pratique, il l'est beaucoup moins.

Dommage…

Heureusement, d'autres solutions plus sécurisées existent, qui permettent d'aboutir au même résultat sans prendre autant de risques. Ces solutions ne sont pas abordées pour l'instant dans ce chapitre, basées sur le chiffrement et l'authentification.

2-3 - GRE en détail

2-3-1 - Que disent les RFC ?

Elles le disent en anglais dans le **RFC2784**. Désolé, mais personne n'a eu l'idée (même pas moi) de traduire ça en français.

En réalité, pour comprendre comment ça fonctionne, il suffit de voir que :

- GRE est considéré comme un protocole de niveau supérieur, qui sera transporté par IP. Pour IP, GRE est donc quelque chose à transporter, au même titre que TCP, UDP, ICMP… ;
- GRE va transporter des paquets de niveau 3 (IP, IPX…), ce sera de l'IP le plus souvent.

La capture de trames qui suit montre encore une fois un simple ping, mais observé cette fois-ci sur l'interface ppp0, c'est-à-dire l'interface qui sert de support au tunnel dans notre exemple. On y observe clairement les deux couches IP l'une dans l'autre :

```
Frame 5 (108 bytes on wire, 108 bytes captured)
    Arrival Time: May 11, 2004 10:09:55.596430000
    Time delta from previous packet: 1.731613000 seconds
    Time since reference or first frame: 1.731613000 seconds
    Frame Number: 5
    Packet Length: 108 bytes
    Capture Length: 108 bytes
Raw packet data
    No link information available
Internet Protocol, Src Addr: 80.8.147.232 (80.8.147.232), Dst Addr: 81.248.157.2 (81.248.157.2)

    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
```

```
        .... ...0 = ECN-CE: 0
    Total Length: 108
    Identification: 0x0000 (0)
    Flags: 0x04
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 255
    Protocol: GRE (0x2f)
          Vient ensuite GRE sur cette première couche IP
          Notez que pour cette couche IP, GRE est vu comme un protocole de niveau supérieur
          (code de protocole 0x2F) au même titre que TCP (code proto 0x06),
          UDP (code proto 0x11)//// ou ICMP (code proto 0x01)
    Header checksum: 0xa877 (correct)
    Source: 80.8.147.232 (80.8.147.232)
    Destination: 81.248.157.2 (81.248.157.2)
Generic Routing Encapsulation (IP)
    Flags and version: 0000
        0... .... .... .... = No checksum
        .0.. .... .... .... = No routing
        ..0. .... .... .... = No key
        ...0 .... .... .... = No sequence number
        .... 0... .... .... = No strict source route
        .... .000 .... .... = Recursion control: 0
        .... .... 0000 0... = Flags: 0
        .... .... .... .000 = Version: 0
    Protocol Type: IP (0x0800)
Internet Protocol, Src Addr: 192.168.0.15 (192.168.0.15), Dst Addr: 172.16.254.2 (172.16.254.2)
          Vient enfin la seconde couche IP, encapsulée dans GRE. Observez les adresses IP source
          et destination : Ce sont celles des passerelles dans les deux réseaux privés.
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 84
    Identification: 0x0000 (0)
    Flags: 0x04
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 63
    Protocol: ICMP (0x01)
    Header checksum: 0xd0de (correct)
    Source: 192.168.0.15 (192.168.0.15)
    Destination: 172.16.254.2 (172.16.254.2)
Internet Control Message Protocol
          Enfin, ICMP (niveau 4), pour le ping.
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0xaf0c (correct)
    Identifier: 0xa30d
    Sequence number: 0x0001
    Data (56 bytes)

0000  45 00 00 6c 00 00 40 00 ff 2f a8 77 50 08 93 e8   E..l..@../.wP...
0010  51 f8 9d 02 00 00 08 00 45 00 00 54 00 00 40 00   Q.......E..T..@.
0020  3f 01 d0 de c0 a8 00 0f ac 10 fe 02 08 00 af 0c   ?...............
0030  a3 0d 00 01 53 8a a0 40 be 16 09 00 08 09 0a 0b   ....S..@........
0040  0c 0d 0e 0f 10 11 12 13 14 15 16 17 18 19 1a 1b   ................
0050  1c 1d 1e 1f 20 21 22 23 24 25 26 27 28 29 2a 2b   .... !"#$%&'()*+
0060  2c 2d 2e 2f 30 31 32 33 34 35 36 37               ,-./01234567
```

Et nous retrouvons la même structure dans la trame de retour :

```
Frame 6 (108 bytes on wire, 108 bytes captured)
    Arrival Time: May 11, 2004 10:09:55.659309000
    Time delta from previous packet: 0.062879000 seconds
    Time since reference or first frame: 1.794492000 seconds
    Frame Number: 6
```

```
    Packet Length: 108 bytes
    Capture Length: 108 bytes
Raw packet data
    No link information available
Internet Protocol, Src Addr: 81.248.157.2 (81.248.157.2), Dst Addr: 80.8.147.232 (80.8.147.232)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 108
    Identification: 0x0000 (0)
    Flags: 0x04
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 251
    Protocol: GRE (0x2f)
    Header checksum: 0xac77 (correct)
    Source: 81.248.157.2 (81.248.157.2)
    Destination: 80.8.147.232 (80.8.147.232)
Generic Routing Encapsulation (IP)
    Flags and version: 0000
        0... .... .... .... = No checksum
        .0.. .... .... .... = No routing
        ..0. .... .... .... = No key
        ...0 .... .... .... = No sequence number
        .... 0... .... .... = No strict source route
        .... .000 .... .... = Recursion control: 0
        .... .... 0000 0... = Flags: 0
        .... .... .... .000 = Version: 0
    Protocol Type: IP (0x0800)
Internet Protocol, Src Addr: 172.16.254.2 (172.16.254.2), Dst Addr: 192.168.0.15 (192.168.0.15)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 84
    Identification: 0xa541 (42305)
    Flags: 0x00
        .0.. = Don't fragment: Not set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 254
    Protocol: ICMP (0x01)
    Header checksum: 0xac9c (correct)
    Source: 172.16.254.2 (172.16.254.2)
    Destination: 192.168.0.15 (192.168.0.15)
Internet Control Message Protocol
    Type: 0 (Echo (ping) reply)
    Code: 0
    Checksum: 0xb70c (correct)
    Identifier: 0xa30d
    Sequence number: 0x0001
    Data (56 bytes)

0000  45 00 00 6c 00 00 40 00 fb 2f ac 77 51 f8 9d 02   E..l..@../.wQ...
0010  50 08 93 e8 00 00 08 00 45 00 00 54 a5 41 00 00   P.......E..T.A..
0020  fe 01 ac 9c ac 10 fe 02 c0 a8 00 0f 00 00 b7 0c   ................
0030  a3 0d 00 01 53 8a a0 40 be 16 09 00 08 09 0a 0b   ....S..@........
0040  0c 0d 0e 0f 10 11 12 13 14 15 16 17 18 19 1a 1b   ................
0050  1c 1d 1e 1f 20 21 22 23 24 25 26 27 28 29 2a 2b   .... !"#$%&'()*+
0060  2c 2d 2e 2f 30 31 32 33 34 35 36 37               ,-./01234567
```

Notez tout de même ici la remarquable organisation des couches d'un réseau. En réalité, au sens strict, nous avons un tunnel dans un tunnel, puisque notre tunnel GRE est creusé dans une couche IP elle-même « tunnelisée » par PPPoE sur Ethernet du moins, jusqu'à votre modem. Au-delà, nous ne savons pas exactement comment ça se passe,

ce qui n'a d'ailleurs que peu d'importance, du moment que nous avons une couche IP cohérente et fonctionnelle de bout en bout.

- GRE n'a pas besoin de savoir comment est transportée la couche IP sur laquelle il opère, ici, il fonctionne sur une couche IP portée par PPP.
- PPP n'a pas besoin de savoir ce qu'il y a dans la couche IP qu'il transporte.

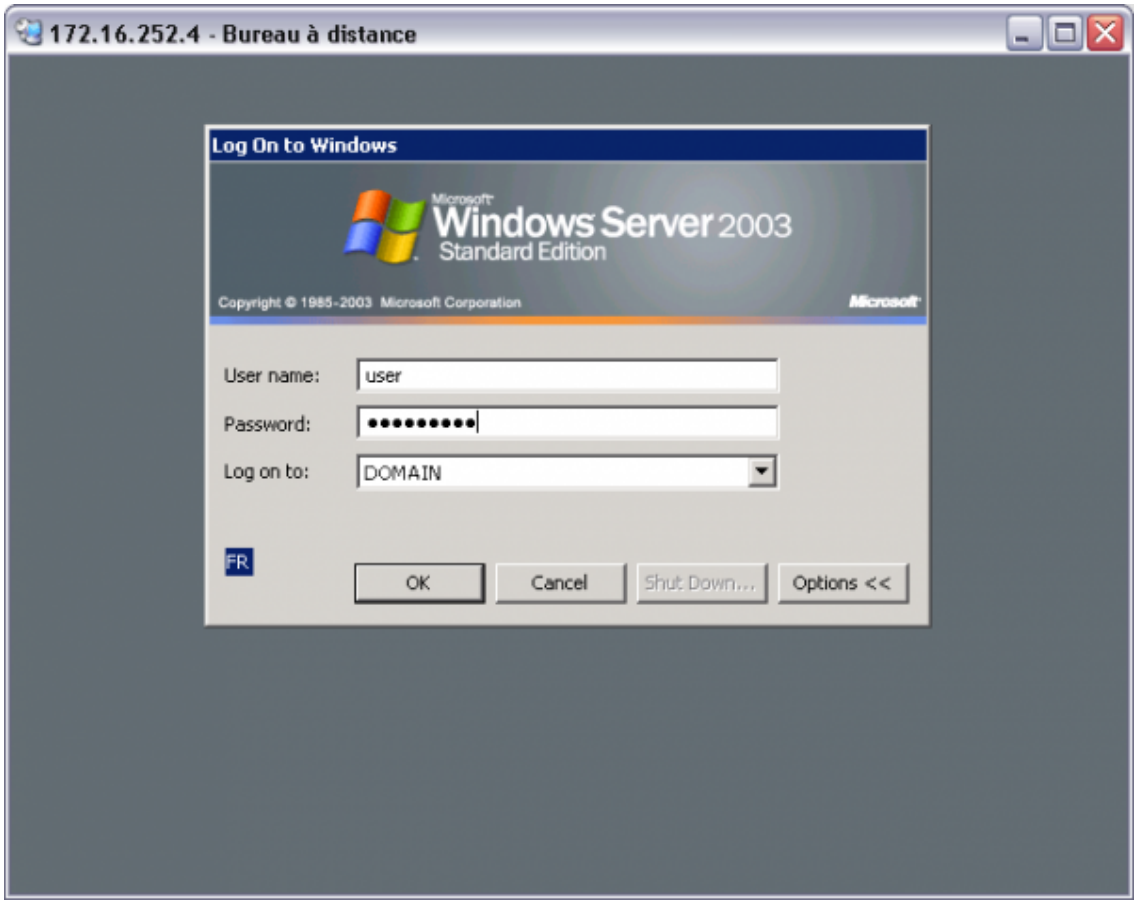
Chacun fait son travail et tout se passe bien. C'est ça la répartition intelligente des tâches.

2-4 - Utilisation

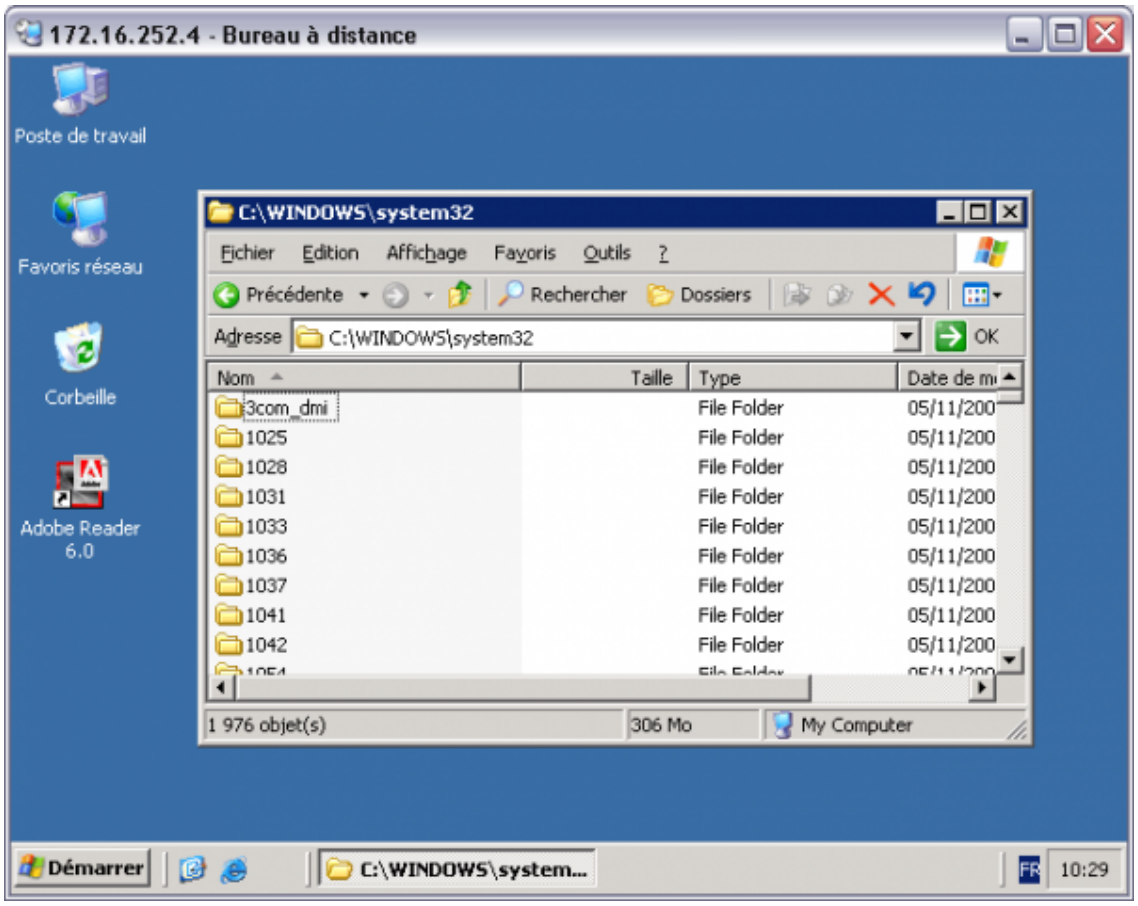
Vous l'avez compris, une fois le tunnel réalisé entre vos deux réseaux, tout se passe comme si ces derniers étaient interconnectés par un routeur, vous êtes chez vous (enfin, tant qu'un intrus ne creuse pas une galerie qui débouche dans votre beau tunnel).

2-4-1 - Premier exemple

Dans votre réseau B depuis un poste Windows, vous ouvrez le bureau à distance d'un serveur Windows situé dans le réseau A exactement comme si votre poste de travail était dans le même réseau A. (Pour être tout à fait dans ce cas, il vous faudra éventuellement, régler quelques problèmes de DNS, mais ce n'est pas l'objet de ce chapitre.) Dans l'exemple, nous utilisons directement l'adresse IP du serveur :

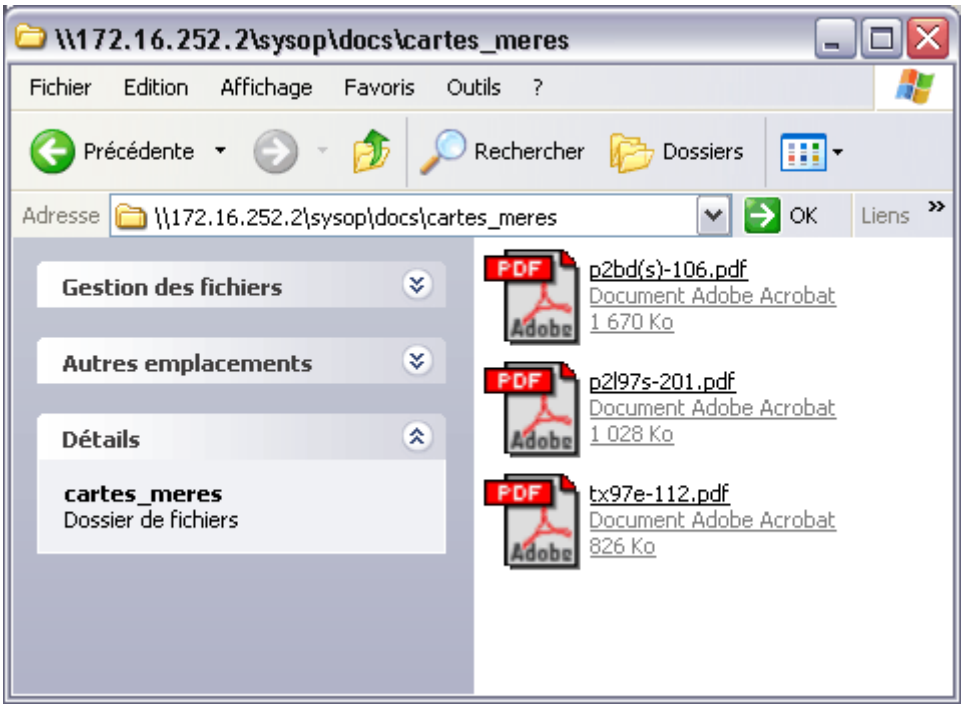


Et après connexion, nous avons un joli terminal :



2-4-2 - Deuxième exemple

Mais ce n'est pas tout, si votre domaine Windows est correctement configuré, que le DNS Active Directory sait résoudre dans les deux réseaux A et B, alors, le tunnel deviendra complètement transparent, vous pourrez, depuis le réseau B ouvrir une session dans le domaine dont le contrôleur se trouve dans le réseau A et votre voisinage réseau vous permettra d'accéder depuis B à des ressources partagées dans le réseau A :



C'est valable, non seulement pour les répertoires partagés, mais aussi pour les imprimantes, bien sûr.

Mais encore une fois, si c'est techniquement possible, c'est tout de même prendre de gros risques de sécurité…

Pour être un peu plus tranquille, il faudrait utiliser un tunnel un peu plus sécurisé, qui chiffre les données et qui assure l'authentification mutuelle pour les deux bouts du tunnel, avec IPSec, par exemple. Mais ça, c'est une autre histoire…

2-4-3 - Troisième exemple

Plus techniquement, GRE est souvent utilisé pour faire communiquer deux réseaux IPv6 (adresses IP de 128 bits, soit 16 octets) à travers un réseau IPv4.

IPv6 est le successeur d'IPv4 (voir le chapitre **IP v6**). Beaucoup de problèmes liés à « l'Internet Protocol » actuel seront résolus, principalement la pénurie d'adresses IP et la gestion laborieuse des tables de routage qui s'allongent démesurément avec le fractionnement des classes IP, mais aussi, la sécurité, la qualité de services seront nativement prises en compte. Malheureusement, la mise à niveau d'un réseau planétaire IPv4 en IPv6 va demander beaucoup de temps et d'investissements en matériel. Des solutions de transition seront donc nécessaires.

2-5 - Limites

Juste un exemple pour montrer au moins qu'un tel tunnel GRE n'offre pas de confidentialité. Nous allons, par l'intermédiaire du « voisinage réseau », utiliser le tunnel pour copier un fichier local sur un hôte distant, à l'autre bout du tunnel.

Ce fichier texte, tout simple, contient le texte : « transfert d'un document par un tunnel GRE ».

Le sniffer, mis en service sur l'un des bouts du tunnel, observe ce qu'il passe sur l'interface ppp0. Je ne vous laisse que la trame importante et vous constaterez que les données sont parfaitement lisibles…

```
Frame 48 (175 bytes on wire, 175 bytes captured)
    Arrival Time: May 13, 2004 10:51:47.184526000
    Time delta from previous packet: 0.000812000 seconds
    Time since reference or first frame: 11.459164000 seconds
```

```
    Frame Number: 48
    Packet Length: 175 bytes
    Capture Length: 175 bytes
Raw packet data
    No link information available
Internet Protocol, Src Addr: 80.8.147.132 (80.8.147.132), Dst Addr: 81.248.152.18 (81.248.152.18)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 175
    Identification: 0x0000 (0)
    Flags: 0x04
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 255
    Protocol: GRE (0x2f)
    Header checksum: 0xa5dd (correct)
    Source: 80.8.147.132 (80.8.147.132)
    Destination: 81.248.152.18 (81.248.152.18)
Generic Routing Encapsulation (IP)
    Flags and version: 0000
        0... .... .... .... = No checksum
        .0.. .... .... .... = No routing
        ..0. .... .... .... = No key
        ...0 .... .... .... = No sequence number
        .... 0... .... .... = No strict source route
        .... .000 .... .... = Recursion control: 0
        .... .... 0000 0... = Flags: 0
        .... .... .... .000 = Version: 0
    Protocol Type: IP (0x0800)
Internet Protocol, Src Addr: 192.168.0.10 (192.168.0.10), Dst Addr: 172.16.254.6 (172.16.254.6)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 151
    Identification: 0xc0db (49371)
    Flags: 0x04
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 127
    Protocol: TCP (0x06)
    Header checksum: 0xcfbb (correct)
    Source: 192.168.0.10 (192.168.0.10)
    Destination: 172.16.254.6 (172.16.254.6)
Transmission Control Protocol, Src Port: 1450 (1450), Dst Port: microsoft-ds (445), Seq: 525021426,
 Ack: 4108893321, Len: 111
    Source port: 1450 (1450)
    Destination port: microsoft-ds (445)
    Sequence number: 525021426
    Next sequence number: 525021537
    Acknowledgement number: 4108893321
    Header length: 20 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 17304
    Checksum: 0xf21a (correct)
NetBIOS Session Service
```

```
    Message Type: Session message
    Length: 107
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response in: 50
        SMB Command: Write AndX (0x2f)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x18
            0... .... = Request/Response: Message is a request to the server
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...1 .... = Canonicalized Pathnames: Pathnames are canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc807
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 1... .... .... = Extended Security Negotiation: Extended security negotiation is
 supported
            .... .... .0.. .... = Long Names Used: Path names in request are not long file names
            .... .... .... .1.. = Security Signatures: Security signatures are supported
            .... .... .... ..1. = Extended Attributes: Extended attributes are supported
            .... .... .... ...1 = Long Names Allowed: Long file names are allowed in the response
        Process ID High: 0
        Signature: EDB2A6ED4322F3CD
        Reserved: 0000
        Tree ID: 32777
        Process ID: 65279
        User ID: 6146
        Multiplex ID: 12417
    Write AndX Request (0x2f)
        Word Count (WCT): 14
        AndXCommand: No further commands (0xff)
        Reserved: 00
        AndXOffset: 57054
        FID: 0x0041
        Offset: 0
        Reserved: FFFFFFFF
        Write Mode: 0x0000
            .... .... .... 0... = Message Start: This is NOT the start of a message (pipe)
            .... .... .... .0.. = Write Raw: DON'T use WriteRawNamedPipe (pipe)
            .... .... .... ..0. = Return Remaining: DON'T return remaining (pipe/dev)
            .... .... .... ...0 = Write Through: Write through not requested
        Remaining: 0
        Data Length High (multiply with 64K): 0
        Data Length Low: 43
        Data Offset: 64
        High Offset: 0
        Byte Count (BCC): 44
        Padding: EE
        File Data: 7472616E7366657274206427756E2064...
0000  45 00 00 af 00 00 40 00 ff 2f a5 dd 50 08 96 3f   E.....@../..P..?
0010  51 f8 9d 02 00 00 08 00 45 00 00 97 c0 db 40 00   Q.......E.....@.
0020  7f 06 cf bb c0 a8 00 0a ac 10 fe 06 05 aa 01 bd   ................
0030  1f 4b 30 f2 f4 e8 bc 89 50 18 43 98 f2 1a 00 00   .K0.....P.C.....
0040  00 00 00 6b ff 53 4d 42 2f 00 00 00 00 18 07 c8   ...k.SMB/.......
0050  00 00 ed b2 a6 ed 43 22 f3 cd 00 00 09 80 ff fe   ......C"........
0060  02 18 81 30 0e ff 00 de de 41 00 00 00 00 00 ff   ...0.....A......
0070  ff ff ff 00 00 00 00 00 00 2b 00 40 00 00 00 00   .........+.@....
0080  00 2c 00 ee 74 72 61 6e 73 66 65 72 74 20 64 27   .,..transfert d'
0090  75 6e 20 64 6f 63 75 6d 65 6e 74 20 70 61 72 20   un document par
00a0  75 6e 20 74 75 6e 6e 65 6c 20 47 52 45 0d 0a      un tunnel GRE..
```

Au minimum, il faudra donc chiffrer au préalable ses données avant de les faire transiter dans ce tunnel, si l'on ne veut pas qu'un indiscret puisse les lire au passage.

2-6 - Conclusion

GRE, techniquement est un excellent tunnel, il est possible d'ouvrir depuis un hôte donné autant de tunnels que l'on désire, vers différents réseaux distants. C'est une solution fort souple, malheureusement trop peu sécurisée pour être utilisée sans risques.

IPSec propose d'autres solutions, plus sécurisées, mais plus délicates à mettre en œuvre.

3 - Open VPN

OpenVPN est un logiciel libre, capable de créer des tunnels sécurisés (ou non) le plus souvent entre deux réseaux distants.

Nous allons nous intéresser particulièrement au cas suivant : deux réseaux IP différents, tous deux connectés à l'internet par l'intermédiaire d'un routeur « nat » vont être reliés par un tunnel. Il s'agira ici d'un tunnel « routé » (tunnel sur IP). Pour information, OpenVPN sait aussi réaliser des tunnels en mode « bridgé » (tunnel sur Ethernet), mais nous n'aborderons pas ici cette façon de faire.

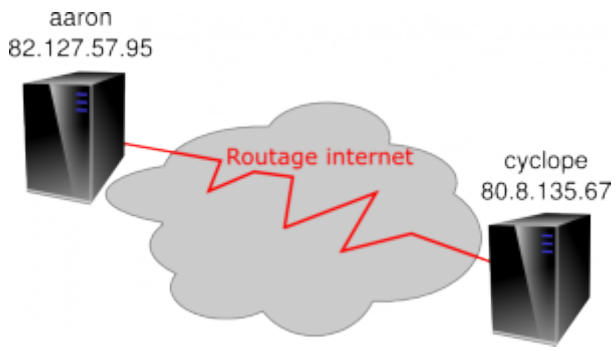
OpenVPN peut utiliser SSL pour la sécurité, ce qui est probablement moins efficace qu'IPsec, mais certainement plus facile à mettre en œuvre.

OpenVPN adopte une architecture client/serveur. Comprenons par là qu'une des extrémités du tunnel doit être configurée en mode serveur. Cette extrémité devra disposer de préférence d'une adresse IP fixe. L'autre extrémité sera configurée en mode client et une adresse IP dynamique fera parfaitement l'affaire.

OpenVPN va créer une interface réseau virtuelle en espace utilisateur à chaque extrémité du réseau. Il nous faudra donc configurer cette interface à chaque bout et également positionner une route pour atteindre le réseau distant, mais tout ceci est pris en charge par OpenVPN lui-même.

3-1 - OpenVPN simple

La plate-forme de tests :



Deux machines disposent d'une connexion internet.

L'une s'appelle AARON, elle dispose d'une adresse IP publique fixe : 82.127.57.95.

L'autre s'appelle CYCLOPE, et dispose d'une adresse IP dynamique : 80.8.135.67, au moment de ce premier test.

Les deux machines sont des Debian Etch, avec un kernel 2.6.24 et la version 2.0.9 d'OpenVPN.

```
aaron:~# apt-get install openvpn
```

```
Reading Package Lists... Done
Building Dependency Tree... Done
The following NEW packages will be installed:
  openvpn
...
Stopping openvpn:.
Starting openvpn:.
```

Le script d'installation vous pose deux questions :

- la première est relative à la création du « device » virtuel nécessaire pour TUN, répondez « yes » ;
- la seconde n'a d'intérêt que si vous faites une mise à jour d'OpenVPN, à travers un tunnel OpenVPN. À mon avis, il vaut mieux, chaque fois que c'est possible, éviter de se mettre dans des situations aussi hasardeuses. Pour ce genre d'opérations, SSH fera parfaitement l'affaire.

Tant qu'on y est, vérifions la présence de la bibliothèque de compression LZO, qui va nous permettre d'optimiser le débit du tunnel :

```
aaron:~# dpkg -l | grep lzo
ii  liblzo1        1.08-1         A real-time data compression library
aaron:~#
```

Elle y est. Sinon, un apt-get install liblzo1 y remédiera.

Comme nous n'avons pour l'instant aucune configuration d'OpenVPN, bien que l'installation ait indiqué :

```
Starting openvpn:.
```

Rien n'a démarré. Pour l'instant, nous faisons des choses simples, nous allons monter un tunnel « à la main », juste pour voir.

3-1-1 - Démarrage du serveur

Sur AARON, qui dispose d'une adresse IP fixe, nous démarrons le serveur :

```
aaron:~# openvpn --port 8147 --dev tun1 --ifconfig 192.168.25.1 192.168.25.2 --comp-lzo --verb 5
```

Quelques mots d'explication sur cette ligne de commande :

- - port 8147, c'est le port qui sera utilisé pour supporter le tunnel ;
- -dev tun1, l'interface réseau virtuelle qui constitue en quelque sorte le bout du tunnel côté serveur ;
- -ifconfig 192.168.25.1 192.168.25.2, va permettre d'attribuer les adresses IP à chaque bout du tunnel :
  - 192.168.25.1 côté local,
  - 192.168.25.2 côté distant ;
- -comp-lzo pour indiquer que l'on utilise la compression en temps réel LZO ;
- -verb 5, c'est le niveau de bavardage que l'on souhaite pour OpenVPN. Le niveau 5 est relativement bavard, comme l'indique la suite :

```
Sat Nov 15 16:12:35 2008 us=919505 Current Parameter Settings:
Sat Nov 15 16:12:35 2008 us=920394   config = '[UNDEF]'
Sat Nov 15 16:12:35 2008 us=920759   mode = 0
Sat Nov 15 16:12:35 2008 us=920997   persist_config = DISABLED
Sat Nov 15 16:12:35 2008 us=921227   persist_mode = 1
Sat Nov 15 16:12:35 2008 us=921453   show_ciphers = DISABLED
Sat Nov 15 16:12:35 2008 us=921679   show_digests = DISABLED
Sat Nov 15 16:12:35 2008 us=921905   show_engines = DISABLED
Sat Nov 15 16:12:35 2008 us=922131   genkey = DISABLED
Sat Nov 15 16:12:35 2008 us=922360   key_pass_file = '[UNDEF]'
Sat Nov 15 16:12:35 2008 us=922590   show_tls_ciphers = DISABLED
```

```
Sat Nov 15 16:12:35 2008 us=922822   proto = 0
Sat Nov 15 16:12:35 2008 us=923050   local = '[UNDEF]'
Sat Nov 15 16:12:35 2008 us=923275   remote_list = NULL
Sat Nov 15 16:12:35 2008 us=923503   remote_random = DISABLED
Sat Nov 15 16:12:35 2008 us=923733   local_port = 8147
Sat Nov 15 16:12:35 2008 us=923960   remote_port = 8147
Sat Nov 15 16:12:35 2008 us=924193   remote_float = DISABLED
Sat Nov 15 16:12:35 2008 us=924456   ipchange = '[UNDEF]'
Sat Nov 15 16:12:35 2008 us=924739   bind_local = ENABLED
Sat Nov 15 16:12:35 2008 us=924967   dev = 'tun1'
Sat Nov 15 16:12:35 2008 us=925195   dev_type = '[UNDEF]'
Sat Nov 15 16:12:35 2008 us=925422   dev_node = '[UNDEF]'
Sat Nov 15 16:12:35 2008 us=925649   tun_ipv6 = DISABLED
Sat Nov 15 16:12:35 2008 us=925875   ifconfig_local = '192.168.25.1'
Sat Nov 15 16:12:35 2008 us=926181   ifconfig_remote_netmask = '192.168.25.2'
Sat Nov 15 16:12:35 2008 us=926417   ifconfig_noexec = DISABLED
Sat Nov 15 16:12:35 2008 us=926646   ifconfig_nowarn = DISABLED
Sat Nov 15 16:12:35 2008 us=926876   shaper = 0
Sat Nov 15 16:12:35 2008 us=927103   tun_mtu = 1500
Sat Nov 15 16:12:35 2008 us=927328   tun_mtu_defined = ENABLED
Sat Nov 15 16:12:35 2008 us=927565   link_mtu = 1500
Sat Nov 15 16:12:35 2008 us=927764   link_mtu_defined = DISABLED
Sat Nov 15 16:12:35 2008 us=927967   tun_mtu_extra = 0
Sat Nov 15 16:12:35 2008 us=928166   tun_mtu_extra_defined = DISABLED
Sat Nov 15 16:12:35 2008 us=928368   fragment = 0
Sat Nov 15 16:12:35 2008 us=928568   mtu_discover_type = -1
Sat Nov 15 16:12:35 2008 us=928812   mtu_test = 0
Sat Nov 15 16:12:35 2008 us=929010   mlock = DISABLED
Sat Nov 15 16:12:35 2008 us=929211   keepalive_ping = 0
Sat Nov 15 16:12:35 2008 us=929411   keepalive_timeout = 0
Sat Nov 15 16:12:35 2008 us=929612   inactivity_timeout = 0
Sat Nov 15 16:12:35 2008 us=929811   ping_send_timeout = 0
Sat Nov 15 16:12:35 2008 us=930010   ping_rec_timeout = 0
Sat Nov 15 16:12:35 2008 us=930209   ping_rec_timeout_action = 0
Sat Nov 15 16:12:35 2008 us=930409   ping_timer_remote = DISABLED
Sat Nov 15 16:12:35 2008 us=930612   remap_sigusr1 = 0
Sat Nov 15 16:12:35 2008 us=930812   explicit_exit_notification = 0
Sat Nov 15 16:12:35 2008 us=931012   persist_tun = DISABLED
Sat Nov 15 16:12:35 2008 us=931211   persist_local_ip = DISABLED
Sat Nov 15 16:12:35 2008 us=931413   persist_remote_ip = DISABLED
Sat Nov 15 16:12:35 2008 us=931615   persist_key = DISABLED
Sat Nov 15 16:12:35 2008 us=931815   mssfix = 1450
Sat Nov 15 16:12:35 2008 us=932014   passtos = DISABLED

Sat Nov 15 16:12:35 2008 us=932216   resolve_retry_seconds = 1000000000
Sat Nov 15 16:12:35 2008 us=932418   connect_retry_seconds = 5
Sat Nov 15 16:12:35 2008 us=932659   username = '[UNDEF]'
Sat Nov 15 16:12:35 2008 us=932859   groupname = '[UNDEF]'
Sat Nov 15 16:12:35 2008 us=933059   chroot_dir = '[UNDEF]'
Sat Nov 15 16:12:35 2008 us=933257   cd_dir = '[UNDEF]'
Sat Nov 15 16:12:35 2008 us=933457   writepid = '[UNDEF]'
Sat Nov 15 16:12:35 2008 us=933657   up_script = '[UNDEF]'
Sat Nov 15 16:12:35 2008 us=933857   down_script = '[UNDEF]'
Sat Nov 15 16:12:35 2008 us=934055   down_pre = DISABLED
Sat Nov 15 16:12:35 2008 us=934254   up_restart = DISABLED
Sat Nov 15 16:12:35 2008 us=934453   up_delay = DISABLED
Sat Nov 15 16:12:35 2008 us=934652   daemon = DISABLED
Sat Nov 15 16:12:35 2008 us=934852   inetd = 0
Sat Nov 15 16:12:35 2008 us=935050   log = DISABLED
Sat Nov 15 16:12:35 2008 us=935250   suppress_timestamps = DISABLED
Sat Nov 15 16:12:35 2008 us=935451   nice = 0
Sat Nov 15 16:12:35 2008 us=935650   verbosity = 5
Sat Nov 15 16:12:35 2008 us=935974   mute = 0
Sat Nov 15 16:12:35 2008 us=936179   gremlin = 0
Sat Nov 15 16:12:35 2008 us=936379   status_file = '[UNDEF]'
Sat Nov 15 16:12:35 2008 us=936620   status_file_version = 1
Sat Nov 15 16:12:35 2008 us=936822   status_file_update_freq = 60
Sat Nov 15 16:12:35 2008 us=937022   occ = ENABLED
Sat Nov 15 16:12:35 2008 us=937223   rcvbuf = 65536
Sat Nov 15 16:12:35 2008 us=937422   sndbuf = 65536
Sat Nov 15 16:12:35 2008 us=937622   socks_proxy_server = '[UNDEF]'
Sat Nov 15 16:12:35 2008 us=937825   socks_proxy_port = 0
```

```
Sat Nov 15 16:12:35 2008 us=938024   socks_proxy_retry = DISABLED
Sat Nov 15 16:12:35 2008 us=938263   fast_io = DISABLED
Sat Nov 15 16:12:35 2008 us=938466   comp_lzo = ENABLED
Sat Nov 15 16:12:35 2008 us=938667   comp_lzo_adaptive = ENABLED
Sat Nov 15 16:12:35 2008 us=938869   route_script = '[UNDEF]'
Sat Nov 15 16:12:35 2008 us=939071   route_default_gateway = '[UNDEF]'
Sat Nov 15 16:12:35 2008 us=939272   route_noexec = DISABLED
Sat Nov 15 16:12:35 2008 us=939471   route_delay = 0
Sat Nov 15 16:12:35 2008 us=939670   route_delay_window = 30
Sat Nov 15 16:12:35 2008 us=939868   route_delay_defined = DISABLED
Sat Nov 15 16:12:35 2008 us=940070   management_addr = '[UNDEF]'
Sat Nov 15 16:12:35 2008 us=940274   management_port = 0
Sat Nov 15 16:12:35 2008 us=940473   management_user_pass = '[UNDEF]'
Sat Nov 15 16:12:35 2008 us=940717   management_log_history_cache = 250
Sat Nov 15 16:12:35 2008 us=940919   management_echo_buffer_size = 100
Sat Nov 15 16:12:35 2008 us=941120   management_query_passwords = DISABLED
Sat Nov 15 16:12:35 2008 us=941321   management_hold = DISABLED
Sat Nov 15 16:12:35 2008 us=941524   shared_secret_file = '[UNDEF]'
Sat Nov 15 16:12:35 2008 us=941727   key_direction = 0
Sat Nov 15 16:12:35 2008 us=941928   ciphername_defined = ENABLED
Sat Nov 15 16:12:35 2008 us=942132   ciphername = 'BF-CBC'
Sat Nov 15 16:12:35 2008 us=942333   authname_defined = ENABLED
Sat Nov 15 16:12:35 2008 us=942535   authname = 'SHA1'
Sat Nov 15 16:12:35 2008 us=942736   keysize = 0
Sat Nov 15 16:12:35 2008 us=942936   engine = DISABLED
Sat Nov 15 16:12:35 2008 us=943136   replay = ENABLED
Sat Nov 15 16:12:35 2008 us=943337   mute_replay_warnings = DISABLED
Sat Nov 15 16:12:35 2008 us=943541   replay_window = 64
Sat Nov 15 16:12:35 2008 us=943741   replay_time = 15
Sat Nov 15 16:12:35 2008 us=943941   packet_id_file = '[UNDEF]'
Sat Nov 15 16:12:35 2008 us=944143   use_iv = ENABLED
Sat Nov 15 16:12:35 2008 us=944344   test_crypto = DISABLED
Sat Nov 15 16:12:35 2008 us=944905   tls_server = DISABLED
Sat Nov 15 16:12:35 2008 us=945125   tls_client = DISABLED
Sat Nov 15 16:12:35 2008 us=945326   key_method = 2
Sat Nov 15 16:12:35 2008 us=945525   ca_file = '[UNDEF]'
Sat Nov 15 16:12:35 2008 us=945725   dh_file = '[UNDEF]'
Sat Nov 15 16:12:35 2008 us=945925   cert_file = '[UNDEF]'
Sat Nov 15 16:12:35 2008 us=946125   priv_key_file = '[UNDEF]'
Sat Nov 15 16:12:35 2008 us=946328   pkcs12_file = '[UNDEF]'
Sat Nov 15 16:12:35 2008 us=946528   cipher_list = '[UNDEF]'
Sat Nov 15 16:12:35 2008 us=946766   tls_verify = '[UNDEF]'
Sat Nov 15 16:12:35 2008 us=946970   tls_remote = '[UNDEF]'
Sat Nov 15 16:12:35 2008 us=947172   crl_file = '[UNDEF]'
Sat Nov 15 16:12:35 2008 us=947375   ns_cert_type = 0
Sat Nov 15 16:12:35 2008 us=947577   tls_timeout = 2
Sat Nov 15 16:12:35 2008 us=947779   renegotiate_bytes = 0
Sat Nov 15 16:12:35 2008 us=947981   renegotiate_packets = 0
Sat Nov 15 16:12:35 2008 us=948183   renegotiate_seconds = 3600
Sat Nov 15 16:12:35 2008 us=948388   handshake_window = 60
Sat Nov 15 16:12:35 2008 us=948627   transition_window = 3600
Sat Nov 15 16:12:35 2008 us=948830   single_session = DISABLED
Sat Nov 15 16:12:35 2008 us=949035   tls_exit = DISABLED
Sat Nov 15 16:12:35 2008 us=949236   tls_auth_file = '[UNDEF]'
Sat Nov 15 16:12:35 2008 us=949522   server_network = 0.0.0.0
Sat Nov 15 16:12:35 2008 us=949737   server_netmask = 0.0.0.0
Sat Nov 15 16:12:35 2008 us=949949   server_bridge_ip = 0.0.0.0
Sat Nov 15 16:12:35 2008 us=950160   server_bridge_netmask = 0.0.0.0
Sat Nov 15 16:12:35 2008 us=950371   server_bridge_pool_start = 0.0.0.0
Sat Nov 15 16:12:35 2008 us=950582   server_bridge_pool_end = 0.0.0.0
Sat Nov 15 16:12:35 2008 us=950785   ifconfig_pool_defined = DISABLED
Sat Nov 15 16:12:35 2008 us=950998   ifconfig_pool_start = 0.0.0.0
Sat Nov 15 16:12:35 2008 us=951209   ifconfig_pool_end = 0.0.0.0
Sat Nov 15 16:12:35 2008 us=951419   ifconfig_pool_netmask = 0.0.0.0
Sat Nov 15 16:12:35 2008 us=951622   ifconfig_pool_persist_filename = '[UNDEF]'
Sat Nov 15 16:12:35 2008 us=951829   ifconfig_pool_persist_refresh_freq = 600
Sat Nov 15 16:12:35 2008 us=952034   ifconfig_pool_linear = DISABLED
Sat Nov 15 16:12:35 2008 us=952238   n_bcast_buf = 256
Sat Nov 15 16:12:35 2008 us=952440   tcp_queue_limit = 64
Sat Nov 15 16:12:35 2008 us=952681   real_hash_size = 256
Sat Nov 15 16:12:35 2008 us=952882   virtual_hash_size = 256
Sat Nov 15 16:12:35 2008 us=953082   client_connect_script = '[UNDEF]'
```

```
Sat Nov 15 16:12:35 2008 us=953285   learn_address_script = '[UNDEF]'
Sat Nov 15 16:12:35 2008 us=953489   client_disconnect_script = '[UNDEF]'
Sat Nov 15 16:12:35 2008 us=953693   client_config_dir = '[UNDEF]'
Sat Nov 15 16:12:35 2008 us=953896   ccd_exclusive = DISABLED
Sat Nov 15 16:12:35 2008 us=954097   tmp_dir = '[UNDEF]'
Sat Nov 15 16:12:35 2008 us=954297   push_ifconfig_defined = DISABLED
Sat Nov 15 16:12:35 2008 us=954509   push_ifconfig_local = 0.0.0.0
Sat Nov 15 16:12:35 2008 us=954759   push_ifconfig_remote_netmask = 0.0.0.0
Sat Nov 15 16:12:35 2008 us=954965   enable_c2c = DISABLED
Sat Nov 15 16:12:35 2008 us=955165   duplicate_cn = DISABLED
Sat Nov 15 16:12:35 2008 us=955365   cf_max = 0
Sat Nov 15 16:12:35 2008 us=955565   cf_per = 0
Sat Nov 15 16:12:35 2008 us=955767   max_clients = 1024
Sat Nov 15 16:12:35 2008 us=955968   max_routes_per_client = 256
Sat Nov 15 16:12:35 2008 us=956170   client_cert_not_required = DISABLED
Sat Nov 15 16:12:35 2008 us=956372   username_as_common_name = DISABLED
Sat Nov 15 16:12:35 2008 us=956614   auth_user_pass_verify_script = '[UNDEF]'
Sat Nov 15 16:12:35 2008 us=956823   auth_user_pass_verify_script_via_file = DISABLED
Sat Nov 15 16:12:35 2008 us=957028   client = DISABLED
Sat Nov 15 16:12:35 2008 us=957228   pull = DISABLED
Sat Nov 15 16:12:35 2008 us=957431   auth_user_pass_file = '[UNDEF]'
Sat Nov 15 16:12:35 2008 us=957639 OpenVPN 2.0.9 i486-pc-linux-gnu [SSL] [LZO] [EPOLL] built on Sep 20
 2007
Sat Nov 15 16:12:35 2008 us=958082 ******* WARNING *******: all encryption and authentication features
 disabled -- all data will be tunnelled as cleartext
Sat Nov 15 16:12:35 2008 us=958372 LZO compression initialized
Sat Nov 15 16:12:36 2008 us=8893 TUN/TAP device tun1 opened
Sat Nov 15 16:12:36 2008 us=9719 TUN/TAP TX queue length set to 100
Sat Nov 15 16:12:36 2008 us=10023 ifconfig tun1 192.168.25.1 pointopoint 192.168.25.2 mtu 1500
Sat Nov 15 16:12:36 2008 us=24915 Data Channel MTU parms [ L:1501 D:1450 EF:1 EB:135 ET:0 EL:0
 AF:14/1 ]
Sat Nov 15 16:12:36 2008 us=25336 Local Options String: 'V4,dev-type tun,link-mtu 1501,tun-mtu
 1500,proto UDPv4,ifconfig 192.168.25.2 192.168.25.1,comp-lzo'
Sat Nov 15 16:12:36 2008 us=25547 Expected Remote Options String: 'V4,dev-type tun,link-mtu 1501,tun-
mtu 1500,proto UDPv4,ifconfig 192.168.25.1 192.168.25.2,comp-lzo'
Sat Nov 15 16:12:36 2008 us=25855 Local Options hash (VER=V4): 'c50ab9ee'
Sat Nov 15 16:12:36 2008 us=26106 Expected Remote Options hash (VER=V4): '932cd9e7'
Sat Nov 15 16:12:36 2008 us=26394 Socket Buffers: R=[110592->131072] S=[110592->131072]
Sat Nov 15 16:12:36 2008 us=26622 UDPv4 link local (bound): [undef]:8147
Sat Nov 15 16:12:36 2008 us=26822 UDPv4 link remote: [undef]
```

Tout ceci n'a pour but que de montrer que nous sommes loin d'utiliser tous les paramètres proposés par OpenVPN. Le but est tout de même d'arriver le plus rapidement possible à une solution sécurisée, plutôt que d'explorer toutes les ressources d'OpenVPN. Toutefois, il n'est pas inutile de lire avec un peu d'attention le listing ci-dessus, qui peut donner pas mal d'idées sur tout ce que peut faire OpenVPN.

Ce qui est surligné montre les principales options définies dans le démarrage d'OpenVPN.

Vérifications :

```
aaron:~# ifconfig
...
ppp0      Link encap:Point-to-Point Protocol
          inet addr:82.127.57.95  P-t-P:193.253.160.3  Mask:255.255.255.255
          UP POINTOPOINT RUNNING NOARP MULTICAST  MTU:1492  Metric:1
          RX packets:342756 errors:0 dropped:0 overruns:0 frame:0
          TX packets:290200 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:3
          RX bytes:426707207 (406.9 MiB)  TX bytes:26657415 (25.4 MiB)

tun1      Lien encap:UNSPEC  HWaddr 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00
          inet adr:192.168.25.1  P-t-P:192.168.25.2  Masque:255.255.255.255
          UP POINTOPOINT RUNNING NOARP MULTICAST  MTU:1500  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 lg file transmission:100
          RX bytes:0 (0.0 b)  TX bytes:0 (0.0 b)
```

Nous avons, en plus de ppp0 qui est la connexion à l'internet, une interface tun1 qui apparaît elle aussi comme une liaison point à point entre 192.168.25.1 (local) et 192.168.25.2 (distant).

```
Table de routage IP du noyau
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
192.168.25.2    0.0.0.0         255.255.255.255 UH    0      0        0 tun1
...
0.0.0.0         193.253.160.3   0.0.0.0         UG    0      0        0 ppp0
```

et nous avons bien la route vers 192.168.25.2 qui passe par tun1

3-1-2 - Démarrage du client

Sur CYCLOPE, nous allons faire quelque chose de très similaire :

```
cyclope:~# openvpn --remote 82.127.57.95 --port 8147 --dev tun1 --ifconfig 192.168.25.2 192.168.25.1 --
comp-lzo --verb 5
```

Notez qu'ici, comme nous sommes client, nous indiquons en plus l'adresse IP distante qui supporte le tunnel (-remote 82.127.57.95).

```
Sat Nov 15 16:34:36 2008 us=173490 Current Parameter Settings:
Sat Nov 15 16:34:36 2008 us=174921   config = '[UNDEF]'
Sat Nov 15 16:34:36 2008 us=175726   mode = 0
Sat Nov 15 16:34:36 2008 us=176424   persist_config = DISABLED
Sat Nov 15 16:34:36 2008 us=177123   persist_mode = 1
Sat Nov 15 16:34:36 2008 us=177812   show_ciphers = DISABLED
Sat Nov 15 16:34:36 2008 us=178498   show_digests = DISABLED
Sat Nov 15 16:34:36 2008 us=179278   show_engines = DISABLED
Sat Nov 15 16:34:36 2008 us=179941   genkey = DISABLED
Sat Nov 15 16:34:36 2008 us=180637   key_pass_file = '[UNDEF]'
Sat Nov 15 16:34:36 2008 us=181333   show_tls_ciphers = DISABLED
Sat Nov 15 16:34:36 2008 us=182030   proto = 0
Sat Nov 15 16:34:36 2008 us=182719   local = '[UNDEF]'
Sat Nov 15 16:34:36 2008 us=183491   remote_list[0] = {'82.127.57.95', 8147}
Sat Nov 15 16:34:36 2008 us=184189   remote_random = DISABLED
Sat Nov 15 16:34:36 2008 us=184887   local_port = 8147
Sat Nov 15 16:34:36 2008 us=185581   remote_port = 8147
Sat Nov 15 16:34:36 2008 us=186272   remote_float = DISABLED
Sat Nov 15 16:34:36 2008 us=186962   ipchange = '[UNDEF]'
Sat Nov 15 16:34:36 2008 us=187543   bind_local = ENABLED
Sat Nov 15 16:34:36 2008 us=188219   dev = 'tun1'
Sat Nov 15 16:34:36 2008 us=188918   dev_type = '[UNDEF]'
Sat Nov 15 16:34:36 2008 us=189610   dev_node = '[UNDEF]'
Sat Nov 15 16:34:36 2008 us=190298   tun_ipv6 = DISABLED
Sat Nov 15 16:34:36 2008 us=190814   ifconfig_local = '192.168.25.2'
Sat Nov 15 16:34:36 2008 us=191576   ifconfig_remote_netmask = '192.168.25.1'
Sat Nov 15 16:34:36 2008 us=192110   ifconfig_noexec = DISABLED
Sat Nov 15 16:34:36 2008 us=192626   ifconfig_nowarn = DISABLED
Sat Nov 15 16:34:36 2008 us=193144   shaper = 0
Sat Nov 15 16:34:36 2008 us=193524   tun_mtu = 1500
Sat Nov 15 16:34:36 2008 us=194325   tun_mtu_defined = ENABLED
Sat Nov 15 16:34:36 2008 us=195256   link_mtu = 1500
Sat Nov 15 16:34:36 2008 us=195933   link_mtu_defined = DISABLED
Sat Nov 15 16:34:36 2008 us=196634   tun_mtu_extra = 0
Sat Nov 15 16:34:36 2008 us=197319   tun_mtu_extra_defined = DISABLED
Sat Nov 15 16:34:36 2008 us=198018   fragment = 0
Sat Nov 15 16:34:36 2008 us=198173   mtu_discover_type = -1
Sat Nov 15 16:34:36 2008 us=198277   mtu_test = 0
Sat Nov 15 16:34:36 2008 us=198565   mlock = DISABLED
Sat Nov 15 16:34:36 2008 us=198674   keepalive_ping = 0
Sat Nov 15 16:34:36 2008 us=198777   keepalive_timeout = 0
Sat Nov 15 16:34:36 2008 us=198879   inactivity_timeout = 0
Sat Nov 15 16:34:36 2008 us=198980   ping_send_timeout = 0
Sat Nov 15 16:34:36 2008 us=199082   ping_rec_timeout = 0
Sat Nov 15 16:34:36 2008 us=199240   ping_rec_timeout_action = 0
```

```
Sat Nov 15 16:34:36 2008 us=199351   ping_timer_remote = DISABLED
Sat Nov 15 16:34:36 2008 us=199454   remap_sigusr1 = 0
Sat Nov 15 16:34:36 2008 us=199556   explicit_exit_notification = 0
Sat Nov 15 16:34:36 2008 us=199657   persist_tun = DISABLED
Sat Nov 15 16:34:36 2008 us=199758   persist_local_ip = DISABLED
Sat Nov 15 16:34:36 2008 us=199861   persist_remote_ip = DISABLED
Sat Nov 15 16:34:36 2008 us=199963   persist_key = DISABLED
Sat Nov 15 16:34:36 2008 us=200065   mssfix = 1450
Sat Nov 15 16:34:36 2008 us=200164   passtos = DISABLED
Sat Nov 15 16:34:36 2008 us=200268   resolve_retry_seconds = 1000000000
Sat Nov 15 16:34:36 2008 us=200371   connect_retry_seconds = 5
Sat Nov 15 16:34:36 2008 us=200472   username = '[UNDEF]'
Sat Nov 15 16:34:36 2008 us=200574   groupname = '[UNDEF]'
Sat Nov 15 16:34:36 2008 us=200676   chroot_dir = '[UNDEF]'
Sat Nov 15 16:34:36 2008 us=200777   cd_dir = '[UNDEF]'
Sat Nov 15 16:34:36 2008 us=200879   writepid = '[UNDEF]'
Sat Nov 15 16:34:36 2008 us=201342   up_script = '[UNDEF]'
Sat Nov 15 16:34:36 2008 us=201449   down_script = '[UNDEF]'
Sat Nov 15 16:34:36 2008 us=201552   down_pre = DISABLED
Sat Nov 15 16:34:36 2008 us=201653   up_restart = DISABLED
Sat Nov 15 16:34:36 2008 us=201754   up_delay = DISABLED
Sat Nov 15 16:34:36 2008 us=201854   daemon = DISABLED
Sat Nov 15 16:34:36 2008 us=201956   inetd = 0
Sat Nov 15 16:34:36 2008 us=202055   log = DISABLED
Sat Nov 15 16:34:36 2008 us=202187   suppress_timestamps = DISABLED
Sat Nov 15 16:34:36 2008 us=202293   nice = 0
Sat Nov 15 16:34:36 2008 us=202395   verbosity = 5
Sat Nov 15 16:34:36 2008 us=202495   mute = 0
Sat Nov 15 16:34:36 2008 us=202594   gremlin = 0
Sat Nov 15 16:34:36 2008 us=202694   status_file = '[UNDEF]'
Sat Nov 15 16:34:36 2008 us=202797   status_file_version = 1
Sat Nov 15 16:34:36 2008 us=202899   status_file_update_freq = 60
Sat Nov 15 16:34:36 2008 us=202998   occ = ENABLED
Sat Nov 15 16:34:36 2008 us=203099   rcvbuf = 65536
Sat Nov 15 16:34:36 2008 us=203257   sndbuf = 65536
Sat Nov 15 16:34:36 2008 us=203364   socks_proxy_server = '[UNDEF]'
Sat Nov 15 16:34:36 2008 us=203467   socks_proxy_port = 0
Sat Nov 15 16:34:36 2008 us=203567   socks_proxy_retry = DISABLED
Sat Nov 15 16:34:36 2008 us=203668   fast_io = DISABLED
Sat Nov 15 16:34:36 2008 us=203768   comp_lzo = ENABLED
Sat Nov 15 16:34:36 2008 us=203870   comp_lzo_adaptive = ENABLED
Sat Nov 15 16:34:36 2008 us=203972   route_script = '[UNDEF]'
Sat Nov 15 16:34:36 2008 us=204075   route_default_gateway = '[UNDEF]'
Sat Nov 15 16:34:36 2008 us=204178   route_noexec = DISABLED
Sat Nov 15 16:34:36 2008 us=204280   route_delay = 0
Sat Nov 15 16:34:36 2008 us=204381   route_delay_window = 30
Sat Nov 15 16:34:36 2008 us=204482   route_delay_defined = DISABLED
Sat Nov 15 16:34:36 2008 us=204584   management_addr = '[UNDEF]'
Sat Nov 15 16:34:36 2008 us=204687   management_port = 0
Sat Nov 15 16:34:36 2008 us=204787   management_user_pass = '[UNDEF]'
Sat Nov 15 16:34:36 2008 us=204892   management_log_history_cache = 250
Sat Nov 15 16:34:36 2008 us=204995   management_echo_buffer_size = 100
Sat Nov 15 16:34:36 2008 us=205096   management_query_passwords = DISABLED
Sat Nov 15 16:34:36 2008 us=205198   management_hold = DISABLED
Sat Nov 15 16:34:36 2008 us=205301   shared_secret_file = '[UNDEF]'
Sat Nov 15 16:34:36 2008 us=205406   key_direction = 0
Sat Nov 15 16:34:36 2008 us=205511   ciphername_defined = ENABLED
Sat Nov 15 16:34:36 2008 us=205617   ciphername = 'BF-CBC'
Sat Nov 15 16:34:36 2008 us=207738   authname_defined = ENABLED
Sat Nov 15 16:34:36 2008 us=208446   authname = 'SHA1'
Sat Nov 15 16:34:36 2008 us=208797   keysize = 0
Sat Nov 15 16:34:36 2008 us=209136   engine = DISABLED
Sat Nov 15 16:34:36 2008 us=209596   replay = ENABLED
Sat Nov 15 16:34:36 2008 us=209938   mute_replay_warnings = DISABLED
Sat Nov 15 16:34:36 2008 us=210281   replay_window = 64
Sat Nov 15 16:34:36 2008 us=211657   replay_time = 15
Sat Nov 15 16:34:36 2008 us=212493   packet_id_file = '[UNDEF]'
Sat Nov 15 16:34:36 2008 us=213188   use_iv = ENABLED
Sat Nov 15 16:34:36 2008 us=213880   test_crypto = DISABLED
Sat Nov 15 16:34:36 2008 us=214576   tls_server = DISABLED
Sat Nov 15 16:34:36 2008 us=215350   tls_client = DISABLED
Sat Nov 15 16:34:36 2008 us=216024   key_method = 2
```

```
Sat Nov 15 16:34:36 2008 us=216707   ca_file = '[UNDEF]'
Sat Nov 15 16:34:36 2008 us=217400   dh_file = '[UNDEF]'
Sat Nov 15 16:34:36 2008 us=218080   cert_file = '[UNDEF]'
Sat Nov 15 16:34:36 2008 us=218775   priv_key_file = '[UNDEF]'
Sat Nov 15 16:34:36 2008 us=219533   pkcs12_file = '[UNDEF]'
Sat Nov 15 16:34:36 2008 us=220223   cipher_list = '[UNDEF]'
Sat Nov 15 16:34:36 2008 us=220918   tls_verify = '[UNDEF]'
Sat Nov 15 16:34:36 2008 us=221613   tls_remote = '[UNDEF]'
Sat Nov 15 16:34:36 2008 us=222309   crl_file = '[UNDEF]'
Sat Nov 15 16:34:36 2008 us=223007   ns_cert_type = 0
Sat Nov 15 16:34:36 2008 us=223760   tls_timeout = 2
Sat Nov 15 16:34:36 2008 us=224460   renegotiate_bytes = 0
Sat Nov 15 16:34:36 2008 us=225159   renegotiate_packets = 0
Sat Nov 15 16:34:36 2008 us=225858   renegotiate_seconds = 3600
Sat Nov 15 16:34:36 2008 us=226428   handshake_window = 60
Sat Nov 15 16:34:36 2008 us=226544   transition_window = 3600
Sat Nov 15 16:34:36 2008 us=226648   single_session = DISABLED
Sat Nov 15 16:34:36 2008 us=226753   tls_exit = DISABLED
Sat Nov 15 16:34:36 2008 us=226858   tls_auth_file = '[UNDEF]'
Sat Nov 15 16:34:36 2008 us=227094   server_network = 0.0.0.0
Sat Nov 15 16:34:36 2008 us=227279   server_netmask = 0.0.0.0
Sat Nov 15 16:34:36 2008 us=227402   server_bridge_ip = 0.0.0.0
Sat Nov 15 16:34:36 2008 us=227522   server_bridge_netmask = 0.0.0.0
Sat Nov 15 16:34:36 2008 us=227675   server_bridge_pool_start = 0.0.0.0
Sat Nov 15 16:34:36 2008 us=227795   server_bridge_pool_end = 0.0.0.0
Sat Nov 15 16:34:36 2008 us=227902   ifconfig_pool_defined = DISABLED
Sat Nov 15 16:34:36 2008 us=228204   ifconfig_pool_start = 0.0.0.0
Sat Nov 15 16:34:36 2008 us=228332   ifconfig_pool_end = 0.0.0.0
Sat Nov 15 16:34:36 2008 us=228450   ifconfig_pool_netmask = 0.0.0.0
Sat Nov 15 16:34:36 2008 us=228592   ifconfig_pool_persist_filename = '[UNDEF]'
Sat Nov 15 16:34:36 2008 us=228713   ifconfig_pool_persist_refresh_freq = 600
Sat Nov 15 16:34:36 2008 us=228819   ifconfig_pool_linear = DISABLED
Sat Nov 15 16:34:36 2008 us=228926   n_bcast_buf = 256
Sat Nov 15 16:34:36 2008 us=229032   tcp_queue_limit = 64
Sat Nov 15 16:34:36 2008 us=229135   real_hash_size = 256
Sat Nov 15 16:34:36 2008 us=229240   virtual_hash_size = 256
Sat Nov 15 16:34:36 2008 us=229344   client_connect_script = '[UNDEF]'
Sat Nov 15 16:34:36 2008 us=229450   learn_address_script = '[UNDEF]'
Sat Nov 15 16:34:36 2008 us=229556   client_disconnect_script = '[UNDEF]'
Sat Nov 15 16:34:36 2008 us=229663   client_config_dir = '[UNDEF]'
Sat Nov 15 16:34:36 2008 us=229767   ccd_exclusive = DISABLED
Sat Nov 15 16:34:36 2008 us=229870   tmp_dir = '[UNDEF]'
Sat Nov 15 16:34:36 2008 us=229972   push_ifconfig_defined = DISABLED
Sat Nov 15 16:34:36 2008 us=230091   push_ifconfig_local = 0.0.0.0
Sat Nov 15 16:34:36 2008 us=230210   push_ifconfig_remote_netmask = 0.0.0.0
Sat Nov 15 16:34:36 2008 us=230315   enable_c2c = DISABLED
Sat Nov 15 16:34:36 2008 us=230417   duplicate_cn = DISABLED
Sat Nov 15 16:34:36 2008 us=230521   cf_max = 0
Sat Nov 15 16:34:36 2008 us=230623   cf_per = 0
Sat Nov 15 16:34:36 2008 us=230726   max_clients = 1024
Sat Nov 15 16:34:36 2008 us=230832   max_routes_per_client = 256
Sat Nov 15 16:34:36 2008 us=230936   client_cert_not_required = DISABLED
Sat Nov 15 16:34:36 2008 us=231040   username_as_common_name = DISABLED
Sat Nov 15 16:34:36 2008 us=231147   auth_user_pass_verify_script = '[UNDEF]'
Sat Nov 15 16:34:36 2008 us=231317   auth_user_pass_verify_script_via_file = DISABLED
Sat Nov 15 16:34:36 2008 us=231425   client = DISABLED
Sat Nov 15 16:34:36 2008 us=231527   pull = DISABLED
Sat Nov 15 16:34:36 2008 us=231630   auth_user_pass_file = '[UNDEF]'
Sat Nov 15 16:34:36 2008 us=231742 OpenVPN 2.0.9 i486-pc-linux-gnu [SSL] [LZO] [EPOLL] built on Sep 20
 2007
Sat Nov 15 16:34:36 2008 us=232260 ******* WARNING *******: all encryption and authentication features
 disabled -- all data will be tunnelled as cleartext
Sat Nov 15 16:34:36 2008 us=232487 LZO compression initialized
Sat Nov 15 16:34:36 2008 us=291858 TUN/TAP device tun1 opened
Sat Nov 15 16:34:36 2008 us=292762 TUN/TAP TX queue length set to 100
Sat Nov 15 16:34:36 2008 us=293672 ifconfig tun1 192.168.25.2 pointopoint 192.168.25.1 mtu 1500
Sat Nov 15 16:34:36 2008 us=316511 Data Channel MTU parms [ L:1501 D:1450 EF:1 EB:135 ET:0 EL:0
 AF:14/1 ]
Sat Nov 15 16:34:36 2008 us=318237 Local Options String: 'V4,dev-type tun,link-mtu 1501,tun-mtu
 1500,proto UDPv4,ifconfig 192.168.25.1 192.168.25.2,comp-lzo'
Sat Nov 15 16:34:36 2008 us=318785 Expected Remote Options String: 'V4,dev-type tun,link-mtu 1501,tun-
mtu 1500,proto UDPv4,ifconfig 192.168.25.2 192.168.25.1,comp-lzo'
```

```
Sat Nov 15 16:34:36 2008 us=319679 Local Options hash (VER=V4): '932cd9e7'
Sat Nov 15 16:34:36 2008 us=320671 Expected Remote Options hash (VER=V4): 'c50ab9ee'
Sat Nov 15 16:34:36 2008 us=321508 Socket Buffers: R=[110592->131072] S=[110592->131072]
Sat Nov 15 16:34:36 2008 us=322223 UDPv4 link local (bound): [undef]:8147
Sat Nov 15 16:34:36 2008 us=322935 UDPv4 link remote: 82.127.57.95:8147
```

Vérification des interfaces virtuelles :

```
cyclope:~# ifconfig
...
ppp0      Link encap:Point-to-Point Protocol
          inet addr:80.8.135.67  P-t-P:80.8.128.1  Mask:255.255.255.255
          UP POINTOPOINT RUNNING NOARP MULTICAST  MTU:1492  Metric:1
          RX packets:5197 errors:0 dropped:0 overruns:0 frame:0
          TX packets:133 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:3
          RX bytes:295907 (288.9 KiB)  TX bytes:9499 (9.2 KiB)

tun1      Link encap:Point-to-Point Protocol
          inet addr:192.168.25.2  P-t-P:192.168.25.1  Mask:255.255.255.255
          UP POINTOPOINT RUNNING NOARP MULTICAST  MTU:1299  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)
```

Vérification des routes :

```
cyclope:~# route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
192.168.25.1    0.0.0.0         255.255.255.255 UH    0      0        0 tun1
...
0.0.0.0         80.8.128.1      0.0.0.0         UG    0      0        0 ppp0
```

3-1-3 - Contrôle du tunnel

Depuis CYCLOPE (192.168.25.2), un petit ping sur AARON (192.168.25.1) :

```
cyclope:~# ping -c 4 192.168.25.1
PING 192.168.25.1 (192.168.25.1): 56 data bytes

--- 192.168.25.1 ping statistics ---
4 packets transmitted, 0 packets received, 100% packet loss
```

Ah ! Ça ne fonctionne pas…

Et c'est bon signe !

Si ça fonctionnait, ça voudrait dire que les deux machines sont connectées à l'internet sans firewall, ce qui serait très **mal !**

Réfléchissons. Nous avons sur les deux hôtes des règles IPtables du genre :

```
iptables -P INPUT DROP
iptables -A INPUT -i ppp0 -m state --state RELATED,ESTABLISHED -j ACCEPT
```

Donc, les paquets « NEW » n'entrent pas, c'est normal. Ajoutons ceci de chaque côté :

```
iptables -A INPUT -i ppp0 -p UDP --dport 8147 -j ACCEPT
```

Rappelons-nous en effet qu'OpenVPN utilise ici UDP et que nous avons établi le tunnel sur le port 8147.

Deuxième essai :

```
cyclope:~# ping -c 4 192.168.25.1
PING 192.168.25.1 (192.168.25.1): 56 data bytes

--- 192.168.25.1 ping statistics ---
4 packets transmitted, 0 packets received, 100% packet loss
```

Ça, c'est ce qui arrive quand on ne réfléchit pas assez… On a dit quelque chose au firewall, à propos de tun1 ? Non ? Alors, c'est normal que ça ne fonctionne toujours pas (iptables -P INPUT DROP).

```
iptables -A INPUT -i tun1 -j ACCEPT
iptables -A OUTPUT -o tun1 -j ACCEPT
```

Ceci afin d'éviter les ennuis, mais par la suite, ce sera peut-être une bonne chose d'affiner un peu plus ces règles de filtrage.

Troisième essai :

```
cyclope:~# ping -c 4 192.168.25.1
PING 192.168.25.1 (192.168.25.1): 56 data bytes
64 bytes from 192.168.25.1: icmp_seq=0 ttl=64 time=89.0 ms
64 bytes from 192.168.25.1: icmp_seq=1 ttl=64 time=65.3 ms
64 bytes from 192.168.25.1: icmp_seq=2 ttl=64 time=71.4 ms
64 bytes from 192.168.25.1: icmp_seq=3 ttl=64 time=74.9 ms

--- 192.168.25.1 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 65.3/75.1/89.0 ms
```

Bon. On y est arrivé, et tout ça pour pas grand-chose, à part que l'on a vérifié que le tunnel fonctionne.

Attention tout de même que ça pourrait encore ne pas fonctionner, en fonction des règles en vigueur sur FORWARD.

Mais réfléchissons encore un peu…

Lorsque nous avons établi le tunnel, en lançant OpenVPN de chaque côté, nous n'avons rien établi du tout, puisque les firewalls ne laissaient pas passer. Pourtant, ça a fonctionné quand même, après modification des règles, ce qui prouve qu'OpenVPN est très efficace sur des liaisons difficiles.

3-1-4 - Un petit coup de sniffeur

Nous sommes sur CYCLOPE. On sniffe le ping sur tun 1 :

```
No.     Time        Source          Destination     Protocol Info
      1 0.000000    192.168.25.2    192.168.25.1    ICMP     Echo (ping) request
      2 0.077503    192.168.25.1    192.168.25.2    ICMP     Echo (ping) reply
      3 1.007802    192.168.25.2    192.168.25.1    ICMP     Echo (ping) request
      4 1.095914    192.168.25.1    192.168.25.2    ICMP     Echo (ping) reply
      5 2.018634    192.168.25.2    192.168.25.1    ICMP     Echo (ping) request
      6 2.083968    192.168.25.1    192.168.25.2    ICMP     Echo (ping) reply
      7 3.019537    192.168.25.2    192.168.25.1    ICMP     Echo (ping) request
      8 3.087613    192.168.25.1    192.168.25.2    ICMP     Echo (ping) reply
```

Pas besoin d'entrer dans les détails, nous voyons bien ICMP qui circule entre 192.168.25.1 et 192.168.25.2.

Puis on le resniffe sur ppp0 :

```
No.     Time        Source          Destination     Protocol Info
      1 0.000000    80.8.135.67     82.127.57.95    UDP      Source port: 8147  Destination port: 8147
      2 0.067128    82.127.57.95    80.8.135.67     UDP      Source port: 8147  Destination port: 8147
      3 1.011132    80.8.135.67     82.127.57.95    UDP      Source port: 8147  Destination port: 8147
      4 1.074716    82.127.57.95    80.8.135.67     UDP      Source port: 8147  Destination port: 8147
      5 2.027369    80.8.135.67     82.127.57.95    UDP      Source port: 8147  Destination port: 8147
      6 2.096456    82.127.57.95    80.8.135.67     UDP      Source port: 8147  Destination port: 8147
      7 3.041653    80.8.135.67     82.127.57.95    UDP      Source port: 8147  Destination port: 8147
      8 3.105374    82.127.57.95    80.8.135.67     UDP      Source port: 8147  Destination port: 8147
```

À ce niveau, nous ne voyons que de l'UDP, bien sûr. Si nous regardons en détail l'une des trames :

```
Frame 1 (129 bytes on wire, 129 bytes captured)
    Arrival Time: Jun 26, 2004 16:22:50.261813000
    Time delta from previous packet: 0.000000000 seconds
    Time since reference or first frame: 0.000000000 seconds
    Frame Number: 1
    Packet Length: 129 bytes
    Capture Length: 129 bytes
Linux cooked capture
    Packet type: Sent by us (4)
    Link-layer address type: 512
    Link-layer address length: 0
    Source: <MISSING>
    Protocol: IP (0x0800)
Internet Protocol, Src Addr: 80.8.135.67, Dst Addr: 82.127.57.95
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 113
    Identification: 0x0200 (512)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: UDP (0x11)
    Header checksum: 0xd552 (correct)
    Source: 80.8.135.67 (80.8.135.67)
    Destination: 82.127.57.95 (82.127.57.95)
User Datagram Protocol, Src Port: 8147 (8147), Dst Port: 8147 (8147)
    Source port: 8147 (8147)
    Destination port: 8147 (8147)
    Length: 93
    Checksum: 0x6263 (correct)
Data (85 bytes)
0000  fa 45 00 00 54 00 00 40 00 40 01 87 55 c0 a8 19   .E..T..@.@..U...
0010  02 c0 a8 19 01 08 00 5c 4c ee 0a 00 00 40 dd 86   .......\L....@..
0020  ba 00 03 fb 0a 08 09 0a 0b 0c 0d 0e 0f 10 11 12   ................
0030  13 14 15 16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 22   ............. !"
0040  23 24 25 26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 32   #$%&'()*+,-./012
0050  33 34 35 36 37                                    34567
```

Et que nous savons décoder les données transportées, nous trouverons le paquet ICMP compressé par LZO. Un simple sniff ne suffira déjà pas à lire les données qui circulent.

3-1-5 - Premières conclusions

Nous avons réussi à monter un tunnel tout simple, qui relie point à point deux hôtes distants, tous deux connectés à l'internet.

À l'intérieur de ce tunnel, tout se passe comme si les deux hôtes étaient reliés par une liaison série, par exemple avec PPP.

Nous n'avons pas réuni deux réseaux, juste deux machines. Mais si ces machines sont des routeurs, en réfléchissant (encore) un peu, nous trouverons bien des règles de routages intelligentes qui permettront aux réseaux qui sont derrière ces routeurs de communiquer entre eux.

Il n'y a pas d'authentification, il n'y a pas de confidentialité, il y a juste une compression des données.

Bien sûr, nous allons faire mieux, en mettant en œuvre du chiffrement.

3-2 - OpenVPN avec une clé partagée

Cette méthode consiste à créer une clé de chiffrement symétrique, que l'on va communiquer aux deux bouts du tunnel. Simple, efficace et relativement sécurisé.

En effet, il va y avoir ici :

- un chiffrement des données dans le tunnel ;
- une (pseudo) authentification des extrémités, si l'on suppose que le secret partagé ne l'est bien qu'entre les deux extrémités souhaitées.

3-2-1 - Création du secret

C'est openvpn qui se charge lui-même de l'opération. Créons ce secret sur cyclope :

```
cyclope:~# openvpn --genkey --secret shared.key
```

Ce qui nous donne dans le répertoire de root (mais nous aurions pu la créer ailleurs) :

```
cyclope:~# cat shared.key
#
# 2048 bit OpenVPN static key
#
-----BEGIN OpenVPN Static key V1-----
f7257a2e6711515f6599d18748910696
7cd9ed0fbd09060e936a0a96584c5c29
1b1ba87ac953aa6f09d5e03e4d9b815c
2b849998f8fede8394edfa965d58d5eb
bd811c44df8d4b2fee59e2ca1d300942
79cc16e2da898b3c5d81ac8dd595c276
1517d3893178924e4b8b79b9add4efcd
e65685b2f813808b0852f9f283588762
3c544069b06e45a00ea799d4ddbd3916
925d71f4577ea4693fe380fd7d534ff0
5a6cb5048ce4f7d62c996d545d6f92ae
a59d828dbb7c5e16d8ce2ebf8238cbfb
0dccf02e0dafed1442ef8e11cb452c93
2c9691ee67ffafd1bce0c6c89736944b
8977756470622841278ad45e924f9bff
74004f2850fd8c72efd8de48b628d0c3
-----END OpenVPN Static key V1-----
```

Il ne nous reste plus qu'à copier un exemplaire de ce secret sur aaron par un moyen sécurisé, scp par exemple, et de tester le tunnel en ajoutant l'appel à ce secret.

3-2-2 - Sur aaron

La commande :

```
aaron:~# openvpn --port 8147 --dev tun1 --ifconfig 192.168.25.1 192.168.25.2 --comp-lzo --verb 5 --
secret /root/shared.key
```

Et la réponse :

```
Sat Nov 15 17:42:06 2008 us=754964 Current Parameter Settings:
Sat Nov 15 17:42:06 2008 us=755921   config = '[UNDEF]'
Sat Nov 15 17:42:06 2008 us=756229   mode = 0
Sat Nov 15 17:42:06 2008 us=756485   persist_config = DISABLED
Sat Nov 15 17:42:06 2008 us=756784   persist_mode = 1
Sat Nov 15 17:42:06 2008 us=757012   show_ciphers = DISABLED
Sat Nov 15 17:42:06 2008 us=757239   show_digests = DISABLED
Sat Nov 15 17:42:06 2008 us=757466   show_engines = DISABLED
Sat Nov 15 17:42:06 2008 us=757693   genkey = DISABLED
Sat Nov 15 17:42:06 2008 us=757923   key_pass_file = '[UNDEF]'
Sat Nov 15 17:42:06 2008 us=758153   show_tls_ciphers = DISABLED
Sat Nov 15 17:42:06 2008 us=758384   proto = 0
Sat Nov 15 17:42:06 2008 us=758611   local = '[UNDEF]'
Sat Nov 15 17:42:06 2008 us=758838   remote_list = NULL
Sat Nov 15 17:42:06 2008 us=759066   remote_random = DISABLED
Sat Nov 15 17:42:06 2008 us=759297   local_port = 8147
Sat Nov 15 17:42:06 2008 us=759526   remote_port = 8147
Sat Nov 15 17:42:06 2008 us=759760   remote_float = DISABLED
Sat Nov 15 17:42:06 2008 us=760023   ipchange = '[UNDEF]'
Sat Nov 15 17:42:06 2008 us=760259   bind_local = ENABLED
Sat Nov 15 17:42:06 2008 us=760488   dev = 'tun1'
Sat Nov 15 17:42:06 2008 us=760762   dev_type = '[UNDEF]'
Sat Nov 15 17:42:06 2008 us=760991   dev_node = '[UNDEF]'
Sat Nov 15 17:42:06 2008 us=761218   tun_ipv6 = DISABLED
Sat Nov 15 17:42:06 2008 us=761445   ifconfig_local = '192.168.25.1'
Sat Nov 15 17:42:06 2008 us=761686   ifconfig_remote_netmask = '192.168.25.2'
Sat Nov 15 17:42:06 2008 us=761919   ifconfig_noexec = DISABLED
Sat Nov 15 17:42:06 2008 us=762150   ifconfig_nowarn = DISABLED
Sat Nov 15 17:42:06 2008 us=762380   shaper = 0
Sat Nov 15 17:42:06 2008 us=762610   tun_mtu = 1500
Sat Nov 15 17:42:06 2008 us=762836   tun_mtu_defined = ENABLED
Sat Nov 15 17:42:06 2008 us=763079   link_mtu = 1500
Sat Nov 15 17:42:06 2008 us=763307   link_mtu_defined = DISABLED
Sat Nov 15 17:42:06 2008 us=763538   tun_mtu_extra = 0
Sat Nov 15 17:42:06 2008 us=763765   tun_mtu_extra_defined = DISABLED
Sat Nov 15 17:42:06 2008 us=763996   fragment = 0
Sat Nov 15 17:42:06 2008 us=764224   mtu_discover_type = -1
Sat Nov 15 17:42:06 2008 us=764452   mtu_test = 0
Sat Nov 15 17:42:06 2008 us=764769   mlock = DISABLED
Sat Nov 15 17:42:06 2008 us=765002   keepalive_ping = 0
Sat Nov 15 17:42:06 2008 us=765230   keepalive_timeout = 0
Sat Nov 15 17:42:06 2008 us=765458   inactivity_timeout = 0
Sat Nov 15 17:42:06 2008 us=765685   ping_send_timeout = 0
Sat Nov 15 17:42:06 2008 us=765913   ping_rec_timeout = 0
Sat Nov 15 17:42:06 2008 us=766141   ping_rec_timeout_action = 0
Sat Nov 15 17:42:06 2008 us=766372   ping_timer_remote = DISABLED
Sat Nov 15 17:42:06 2008 us=766607   remap_sigusr1 = 0
Sat Nov 15 17:42:06 2008 us=766836   explicit_exit_notification = 0
Sat Nov 15 17:42:06 2008 us=767066   persist_tun = DISABLED
Sat Nov 15 17:42:06 2008 us=767294   persist_local_ip = DISABLED
Sat Nov 15 17:42:06 2008 us=767524   persist_remote_ip = DISABLED
Sat Nov 15 17:42:06 2008 us=767754   persist_key = DISABLED
Sat Nov 15 17:42:06 2008 us=767982   mssfix = 1450
Sat Nov 15 17:42:06 2008 us=768208   passtos = DISABLED
Sat Nov 15 17:42:06 2008 us=768437   resolve_retry_seconds = 1000000000
Sat Nov 15 17:42:06 2008 us=768714   connect_retry_seconds = 5
Sat Nov 15 17:42:06 2008 us=768945   username = '[UNDEF]'
Sat Nov 15 17:42:06 2008 us=769174   groupname = '[UNDEF]'
Sat Nov 15 17:42:06 2008 us=769401   chroot_dir = '[UNDEF]'
Sat Nov 15 17:42:06 2008 us=769628   cd_dir = '[UNDEF]'
Sat Nov 15 17:42:06 2008 us=769869   writepid = '[UNDEF]'
Sat Nov 15 17:42:06 2008 us=770099   up_script = '[UNDEF]'
Sat Nov 15 17:42:06 2008 us=770327   down_script = '[UNDEF]'
Sat Nov 15 17:42:06 2008 us=770554   down_pre = DISABLED
Sat Nov 15 17:42:06 2008 us=770781   up_restart = DISABLED
Sat Nov 15 17:42:06 2008 us=771008   up_delay = DISABLED
```

```
Sat Nov 15 17:42:06 2008 us=771235   daemon = DISABLED
Sat Nov 15 17:42:06 2008 us=771463   inetd = 0
Sat Nov 15 17:42:06 2008 us=771689   log = DISABLED
Sat Nov 15 17:42:06 2008 us=771916   suppress_timestamps = DISABLED
Sat Nov 15 17:42:06 2008 us=772146   nice = 0
Sat Nov 15 17:42:06 2008 us=772374   verbosity = 5
Sat Nov 15 17:42:06 2008 us=772641   mute = 0
Sat Nov 15 17:42:06 2008 us=772871   gremlin = 0
Sat Nov 15 17:42:06 2008 us=773098   status_file = '[UNDEF]'
Sat Nov 15 17:42:06 2008 us=773332   status_file_version = 1
Sat Nov 15 17:42:06 2008 us=773560   status_file_update_freq = 60
Sat Nov 15 17:42:06 2008 us=773788   occ = ENABLED
Sat Nov 15 17:42:06 2008 us=774017   rcvbuf = 65536
Sat Nov 15 17:42:06 2008 us=774245   sndbuf = 65536
Sat Nov 15 17:42:06 2008 us=774474   socks_proxy_server = '[UNDEF]'
Sat Nov 15 17:42:06 2008 us=774705   socks_proxy_port = 0
Sat Nov 15 17:42:06 2008 us=774933   socks_proxy_retry = DISABLED
Sat Nov 15 17:42:06 2008 us=775163   fast_io = DISABLED
Sat Nov 15 17:42:06 2008 us=775391   comp_lzo = ENABLED
Sat Nov 15 17:42:06 2008 us=775620   comp_lzo_adaptive = ENABLED
Sat Nov 15 17:42:06 2008 us=775851   route_script = '[UNDEF]'
Sat Nov 15 17:42:06 2008 us=776082   route_default_gateway = '[UNDEF]'
Sat Nov 15 17:42:06 2008 us=776311   route_noexec = DISABLED
Sat Nov 15 17:42:06 2008 us=776552   route_delay = 0
Sat Nov 15 17:42:06 2008 us=776823   route_delay_window = 30
Sat Nov 15 17:42:06 2008 us=777051   route_delay_defined = DISABLED
Sat Nov 15 17:42:06 2008 us=777282   management_addr = '[UNDEF]'
Sat Nov 15 17:42:06 2008 us=777514   management_port = 0
Sat Nov 15 17:42:06 2008 us=777742   management_user_pass = '[UNDEF]'
Sat Nov 15 17:42:06 2008 us=777974   management_log_history_cache = 250
Sat Nov 15 17:42:06 2008 us=778205   management_echo_buffer_size = 100
Sat Nov 15 17:42:06 2008 us=778434   management_query_passwords = DISABLED
Sat Nov 15 17:42:06 2008 us=778664   management_hold = DISABLED
Sat Nov 15 17:42:06 2008 us=778895   shared_secret_file = '/root/shared.key'
Sat Nov 15 17:42:06 2008 us=779127   key_direction = 0
Sat Nov 15 17:42:06 2008 us=779357   ciphername_defined = ENABLED
Sat Nov 15 17:42:06 2008 us=779603   ciphername = 'BF-CBC'
Sat Nov 15 17:42:06 2008 us=779833   authname_defined = ENABLED
Sat Nov 15 17:42:06 2008 us=780064   authname = 'SHA1'
Sat Nov 15 17:42:06 2008 us=780293   keysize = 0
Sat Nov 15 17:42:06 2008 us=780521   engine = DISABLED
Sat Nov 15 17:42:06 2008 us=780792   replay = ENABLED
Sat Nov 15 17:42:06 2008 us=781022   mute_replay_warnings = DISABLED
Sat Nov 15 17:42:06 2008 us=781485   replay_window = 64
Sat Nov 15 17:42:06 2008 us=781733   replay_time = 15
Sat Nov 15 17:42:06 2008 us=781962   packet_id_file = '[UNDEF]'
Sat Nov 15 17:42:06 2008 us=782193   use_iv = ENABLED
Sat Nov 15 17:42:06 2008 us=782422   test_crypto = DISABLED
Sat Nov 15 17:42:06 2008 us=782651   tls_server = DISABLED
Sat Nov 15 17:42:06 2008 us=782879   tls_client = DISABLED
Sat Nov 15 17:42:06 2008 us=783109   key_method = 2
Sat Nov 15 17:42:06 2008 us=783340   ca_file = '[UNDEF]'
Sat Nov 15 17:42:06 2008 us=783570   dh_file = '[UNDEF]'
Sat Nov 15 17:42:06 2008 us=783798   cert_file = '[UNDEF]'
Sat Nov 15 17:42:06 2008 us=784027   priv_key_file = '[UNDEF]'
Sat Nov 15 17:42:06 2008 us=784258   pkcs12_file = '[UNDEF]'
Sat Nov 15 17:42:06 2008 us=784486   cipher_list = '[UNDEF]'
Sat Nov 15 17:42:06 2008 us=784757   tls_verify = '[UNDEF]'
Sat Nov 15 17:42:06 2008 us=784986   tls_remote = '[UNDEF]'
Sat Nov 15 17:42:06 2008 us=785215   crl_file = '[UNDEF]'
Sat Nov 15 17:42:06 2008 us=785445   ns_cert_type = 0
Sat Nov 15 17:42:06 2008 us=785675   tls_timeout = 2
Sat Nov 15 17:42:06 2008 us=785905   renegotiate_bytes = 0
Sat Nov 15 17:42:06 2008 us=786136   renegotiate_packets = 0
Sat Nov 15 17:42:06 2008 us=786366   renegotiate_seconds = 3600
Sat Nov 15 17:42:06 2008 us=786599   handshake_window = 60
Sat Nov 15 17:42:06 2008 us=786842   transition_window = 3600
Sat Nov 15 17:42:06 2008 us=787075   single_session = DISABLED
Sat Nov 15 17:42:06 2008 us=787307   tls_exit = DISABLED
Sat Nov 15 17:42:06 2008 us=787535   tls_auth_file = '[UNDEF]'
Sat Nov 15 17:42:06 2008 us=787850   server_network = 0.0.0.0
Sat Nov 15 17:42:06 2008 us=788097   server_netmask = 0.0.0.0
```

```
Sat Nov 15 17:42:06 2008 us=788337   server_bridge_ip = 0.0.0.0
Sat Nov 15 17:42:06 2008 us=788616   server_bridge_netmask = 0.0.0.0
Sat Nov 15 17:42:06 2008 us=788861   server_bridge_pool_start = 0.0.0.0
Sat Nov 15 17:42:06 2008 us=789101   server_bridge_pool_end = 0.0.0.0
Sat Nov 15 17:42:06 2008 us=789333   ifconfig_pool_defined = DISABLED
Sat Nov 15 17:42:06 2008 us=789575   ifconfig_pool_start = 0.0.0.0
Sat Nov 15 17:42:06 2008 us=789817   ifconfig_pool_end = 0.0.0.0
Sat Nov 15 17:42:06 2008 us=790060   ifconfig_pool_netmask = 0.0.0.0
Sat Nov 15 17:42:06 2008 us=790291   ifconfig_pool_persist_filename = '[UNDEF]'
Sat Nov 15 17:42:06 2008 us=790527   ifconfig_pool_persist_refresh_freq = 600
Sat Nov 15 17:42:06 2008 us=790761   ifconfig_pool_linear = DISABLED
Sat Nov 15 17:42:06 2008 us=790994   n_bcast_buf = 256
Sat Nov 15 17:42:06 2008 us=791225   tcp_queue_limit = 64
Sat Nov 15 17:42:06 2008 us=791454   real_hash_size = 256
Sat Nov 15 17:42:06 2008 us=791684   virtual_hash_size = 256
Sat Nov 15 17:42:06 2008 us=791914   client_connect_script = '[UNDEF]'
Sat Nov 15 17:42:06 2008 us=792147   learn_address_script = '[UNDEF]'
Sat Nov 15 17:42:06 2008 us=792380   client_disconnect_script = '[UNDEF]'
Sat Nov 15 17:42:06 2008 us=792652   client_config_dir = '[UNDEF]'
Sat Nov 15 17:42:06 2008 us=792887   ccd_exclusive = DISABLED
Sat Nov 15 17:42:06 2008 us=793131   tmp_dir = '[UNDEF]'
Sat Nov 15 17:42:06 2008 us=793334   push_ifconfig_defined = DISABLED
Sat Nov 15 17:42:06 2008 us=793548   push_ifconfig_local = 0.0.0.0
Sat Nov 15 17:42:06 2008 us=793761   push_ifconfig_remote_netmask = 0.0.0.0
Sat Nov 15 17:42:06 2008 us=793965   enable_c2c = DISABLED
Sat Nov 15 17:42:06 2008 us=794166   duplicate_cn = DISABLED
Sat Nov 15 17:42:06 2008 us=794369   cf_max = 0
Sat Nov 15 17:42:06 2008 us=794572   cf_per = 0
Sat Nov 15 17:42:06 2008 us=794774   max_clients = 1024
Sat Nov 15 17:42:06 2008 us=794977   max_routes_per_client = 256
Sat Nov 15 17:42:06 2008 us=795182   client_cert_not_required = DISABLED
Sat Nov 15 17:42:06 2008 us=795387   username_as_common_name = DISABLED
Sat Nov 15 17:42:06 2008 us=795592   auth_user_pass_verify_script = '[UNDEF]'
Sat Nov 15 17:42:06 2008 us=795799   auth_user_pass_verify_script_via_file = DISABLED
Sat Nov 15 17:42:06 2008 us=796006   client = DISABLED
Sat Nov 15 17:42:06 2008 us=796207   pull = DISABLED
Sat Nov 15 17:42:06 2008 us=796410   auth_user_pass_file = '[UNDEF]'
Sat Nov 15 17:42:06 2008 us=796661 OpenVPN 2.0.9 i486-pc-linux-gnu [SSL] [LZO] [EPOLL] built on Sep 20
 2007
Sat Nov 15 17:42:06 2008 us=798465 Static Encrypt: Cipher 'BF-CBC' initialized with 128 bit key
Sat Nov 15 17:42:06 2008 us=798743 Static Encrypt: Using 160 bit message hash 'SHA1' for HMAC
 authentication
Sat Nov 15 17:42:06 2008 us=799255 Static Decrypt: Cipher 'BF-CBC' initialized with 128 bit key
Sat Nov 15 17:42:06 2008 us=799485 Static Decrypt: Using 160 bit message hash 'SHA1' for HMAC
 authentication
Sat Nov 15 17:42:06 2008 us=799753 LZO compression initialized
Sat Nov 15 17:42:06 2008 us=850486 TUN/TAP device tun1 opened
Sat Nov 15 17:42:06 2008 us=850907 TUN/TAP TX queue length set to 100
Sat Nov 15 17:42:06 2008 us=851230 ifconfig tun1 192.168.25.1 pointopoint 192.168.25.2 mtu 1500
Sat Nov 15 17:42:06 2008 us=865884 Data Channel MTU parms [ L:1545 D:1450 EF:45 EB:135 ET:0 EL:0
 AF:3/1 ]
Sat Nov 15 17:42:06 2008 us=866409 Local Options String: 'V4,dev-type tun,link-mtu 1545,tun-mtu
 1500,proto UDPv4,ifconfig 192.168.25.2 192.168.25.1,comp-lzo,cipher BF-CBC,auth SHA1,keysize
 128,secret'
Sat Nov 15 17:42:06 2008 us=866663 Expected Remote Options String: 'V4,dev-type tun,link-mtu 1545,tun-
mtu 1500,proto UDPv4,ifconfig 192.168.25.1 192.168.25.2,comp-lzo,cipher BF-CBC,auth SHA1,keysize
 128,secret'
Sat Nov 15 17:42:06 2008 us=867004 Local Options hash (VER=V4): '6963813b'
Sat Nov 15 17:42:06 2008 us=867286 Expected Remote Options hash (VER=V4): '3210d11a'
Sat Nov 15 17:42:06 2008 us=867602 Socket Buffers: R=[110592->131072] S=[110592->131072]
Sat Nov 15 17:42:06 2008 us=867859 UDPv4 link local (bound): [undef]:8147
Sat Nov 15 17:42:06 2008 us=868086 UDPv4 link remote: [undef]
```

Nous n'avons plus de vilain « warning » nous signalant que les données circulent en clair, nous avons à la place les informations sur la méthode de chiffrement.

3-2-3 - Sur cyclope

La commande :

```
cyclope:/etc/openvpn# openvpn --remote 82.127.57.95  --port 8147 --dev tun1 --ifconfig 192.168.25.2
 192.168.25.1 --comp-lzo --verb 5 --secret /root/shared.key
```

Et la réponse :

```
Sat Nov 15 17:48:47 2008 us=847763 Current Parameter Settings:
Sat Nov 15 17:48:47 2008 us=849252   config = '[UNDEF]'
Sat Nov 15 17:48:47 2008 us=850003   mode = 0
Sat Nov 15 17:48:47 2008 us=850695   persist_config = DISABLED
Sat Nov 15 17:48:47 2008 us=851472   persist_mode = 1
Sat Nov 15 17:48:47 2008 us=852164   show_ciphers = DISABLED
Sat Nov 15 17:48:47 2008 us=852859   show_digests = DISABLED
Sat Nov 15 17:48:47 2008 us=853550   show_engines = DISABLED
Sat Nov 15 17:48:47 2008 us=854244   genkey = DISABLED
Sat Nov 15 17:48:47 2008 us=854939   key_pass_file = '[UNDEF]'
Sat Nov 15 17:48:47 2008 us=855703   show_tls_ciphers = DISABLED
Sat Nov 15 17:48:47 2008 us=856406   proto = 0
Sat Nov 15 17:48:47 2008 us=857097   local = '[UNDEF]'
Sat Nov 15 17:48:47 2008 us=857794   remote_list[0] = {'82.127.57.95', 8147}
Sat Nov 15 17:48:47 2008 us=858488   remote_random = DISABLED
Sat Nov 15 17:48:47 2008 us=860129   local_port = 8147
Sat Nov 15 17:48:47 2008 us=860657   remote_port = 8147
Sat Nov 15 17:48:47 2008 us=861336   remote_float = DISABLED
Sat Nov 15 17:48:47 2008 us=862029   ipchange = '[UNDEF]'
Sat Nov 15 17:48:47 2008 us=862720   bind_local = ENABLED
Sat Nov 15 17:48:47 2008 us=864281   dev = 'tun1'
Sat Nov 15 17:48:47 2008 us=864789   dev_type = '[UNDEF]'
Sat Nov 15 17:48:47 2008 us=865482   dev_node = '[UNDEF]'
Sat Nov 15 17:48:47 2008 us=866171   tun_ipv6 = DISABLED
Sat Nov 15 17:48:47 2008 us=866860   ifconfig_local = '192.168.25.2'
Sat Nov 15 17:48:47 2008 us=867794   ifconfig_remote_netmask = '192.168.25.1'
Sat Nov 15 17:48:47 2008 us=868492   ifconfig_noexec = DISABLED
Sat Nov 15 17:48:47 2008 us=869183   ifconfig_nowarn = DISABLED
Sat Nov 15 17:48:47 2008 us=869875   shaper = 0
Sat Nov 15 17:48:47 2008 us=870569   tun_mtu = 1500
Sat Nov 15 17:48:47 2008 us=871472   tun_mtu_defined = ENABLED
Sat Nov 15 17:48:47 2008 us=871991   link_mtu = 1500
Sat Nov 15 17:48:47 2008 us=872506   link_mtu_defined = DISABLED
Sat Nov 15 17:48:47 2008 us=872892   tun_mtu_extra = 0
Sat Nov 15 17:48:47 2008 us=873233   tun_mtu_extra_defined = DISABLED
Sat Nov 15 17:48:47 2008 us=873575   fragment = 0
Sat Nov 15 17:48:47 2008 us=873914   mtu_discover_type = -1
Sat Nov 15 17:48:47 2008 us=874253   mtu_test = 0
Sat Nov 15 17:48:47 2008 us=874588   mlock = DISABLED
Sat Nov 15 17:48:47 2008 us=874710   keepalive_ping = 0
Sat Nov 15 17:48:47 2008 us=874814   keepalive_timeout = 0
Sat Nov 15 17:48:47 2008 us=874918   inactivity_timeout = 0
Sat Nov 15 17:48:47 2008 us=875021   ping_send_timeout = 0
Sat Nov 15 17:48:47 2008 us=875124   ping_rec_timeout = 0
Sat Nov 15 17:48:47 2008 us=875674   ping_rec_timeout_action = 0
Sat Nov 15 17:48:47 2008 us=875793   ping_timer_remote = DISABLED
Sat Nov 15 17:48:47 2008 us=875899   remap_sigusr1 = 0
Sat Nov 15 17:48:47 2008 us=876002   explicit_exit_notification = 0
Sat Nov 15 17:48:47 2008 us=876104   persist_tun = DISABLED
Sat Nov 15 17:48:47 2008 us=876238   persist_local_ip = DISABLED
Sat Nov 15 17:48:47 2008 us=876344   persist_remote_ip = DISABLED
Sat Nov 15 17:48:47 2008 us=876618   persist_key = DISABLED
Sat Nov 15 17:48:47 2008 us=876735   mssfix = 1450
Sat Nov 15 17:48:47 2008 us=876836   passtos = DISABLED
Sat Nov 15 17:48:47 2008 us=876943   resolve_retry_seconds = 1000000000
Sat Nov 15 17:48:47 2008 us=877046   connect_retry_seconds = 5
Sat Nov 15 17:48:47 2008 us=877148   username = '[UNDEF]'
Sat Nov 15 17:48:47 2008 us=877251   groupname = '[UNDEF]'
Sat Nov 15 17:48:47 2008 us=877354   chroot_dir = '[UNDEF]'
Sat Nov 15 17:48:47 2008 us=877456   cd_dir = '[UNDEF]'
Sat Nov 15 17:48:47 2008 us=877559   writepid = '[UNDEF]'
Sat Nov 15 17:48:47 2008 us=877661   up_script = '[UNDEF]'
Sat Nov 15 17:48:47 2008 us=877763   down_script = '[UNDEF]'
Sat Nov 15 17:48:47 2008 us=877865   down_pre = DISABLED
Sat Nov 15 17:48:47 2008 us=877966   up_restart = DISABLED
Sat Nov 15 17:48:47 2008 us=878068   up_delay = DISABLED
```

```
Sat Nov 15 17:48:47 2008 us=878168   daemon = DISABLED
Sat Nov 15 17:48:47 2008 us=878270   inetd = 0
Sat Nov 15 17:48:47 2008 us=878370   log = DISABLED
Sat Nov 15 17:48:47 2008 us=878471   suppress_timestamps = DISABLED
Sat Nov 15 17:48:47 2008 us=878574   nice = 0
Sat Nov 15 17:48:47 2008 us=878675   verbosity = 5
Sat Nov 15 17:48:47 2008 us=878777   mute = 0
Sat Nov 15 17:48:47 2008 us=878877   gremlin = 0
Sat Nov 15 17:48:47 2008 us=878978   status_file = '[UNDEF]'
Sat Nov 15 17:48:47 2008 us=879082   status_file_version = 1
Sat Nov 15 17:48:47 2008 us=880451   status_file_update_freq = 60
Sat Nov 15 17:48:47 2008 us=880862   occ = ENABLED
Sat Nov 15 17:48:47 2008 us=881262   rcvbuf = 65536
Sat Nov 15 17:48:47 2008 us=881733   sndbuf = 65536
Sat Nov 15 17:48:47 2008 us=882075   socks_proxy_server = '[UNDEF]'
Sat Nov 15 17:48:47 2008 us=883751   socks_proxy_port = 0
Sat Nov 15 17:48:47 2008 us=884239   socks_proxy_retry = DISABLED
Sat Nov 15 17:48:47 2008 us=884935   fast_io = DISABLED
Sat Nov 15 17:48:47 2008 us=885449   comp_lzo = ENABLED
Sat Nov 15 17:48:47 2008 us=886142   comp_lzo_adaptive = ENABLED
Sat Nov 15 17:48:47 2008 us=886661   route_script = '[UNDEF]'
Sat Nov 15 17:48:47 2008 us=887423   route_default_gateway = '[UNDEF]'
Sat Nov 15 17:48:47 2008 us=887945   route_noexec = DISABLED
Sat Nov 15 17:48:47 2008 us=888634   route_delay = 0
Sat Nov 15 17:48:47 2008 us=889152   route_delay_window = 30
Sat Nov 15 17:48:47 2008 us=889305   route_delay_defined = DISABLED
Sat Nov 15 17:48:47 2008 us=889595   management_addr = '[UNDEF]'
Sat Nov 15 17:48:47 2008 us=889709   management_port = 0
Sat Nov 15 17:48:47 2008 us=889812   management_user_pass = '[UNDEF]'
Sat Nov 15 17:48:47 2008 us=889917   management_log_history_cache = 250
Sat Nov 15 17:48:47 2008 us=890021   management_echo_buffer_size = 100
Sat Nov 15 17:48:47 2008 us=890124   management_query_passwords = DISABLED
Sat Nov 15 17:48:47 2008 us=890228   management_hold = DISABLED

Sat Nov 15 17:48:47 2008 us=890332   shared_secret_file = '/root/shared.key
Sat Nov 15 17:48:47 2008 us=890439   key_direction = 0
Sat Nov 15 17:48:47 2008 us=890545   ciphername_defined = ENABLED
Sat Nov 15 17:48:47 2008 us=890651   ciphername = 'BF-CBC'
Sat Nov 15 17:48:47 2008 us=890756   authname_defined = ENABLED
Sat Nov 15 17:48:47 2008 us=890861   authname = 'SHA1'
Sat Nov 15 17:48:47 2008 us=890965   keysize = 0'
Sat Nov 15 17:48:47 2008 us=891068   engine = DISABLED
Sat Nov 15 17:48:47 2008 us=891230   replay = ENABLED
Sat Nov 15 17:48:47 2008 us=891348   mute_replay_warnings = DISABLED
Sat Nov 15 17:48:47 2008 us=891456   replay_window = 64
Sat Nov 15 17:48:47 2008 us=891561   replay_time = 15
Sat Nov 15 17:48:47 2008 us=891665   packet_id_file = '[UNDEF]'
Sat Nov 15 17:48:47 2008 us=891768   use_iv = ENABLED
Sat Nov 15 17:48:47 2008 us=891871   test_crypto = DISABLED
Sat Nov 15 17:48:47 2008 us=891975   tls_server = DISABLED
Sat Nov 15 17:48:47 2008 us=892078   tls_client = DISABLED
Sat Nov 15 17:48:47 2008 us=892184   key_method = 2
Sat Nov 15 17:48:47 2008 us=892286   ca_file = '[UNDEF]'
Sat Nov 15 17:48:47 2008 us=892390   dh_file = '[UNDEF]'
Sat Nov 15 17:48:47 2008 us=892493   cert_file = '[UNDEF]'
Sat Nov 15 17:48:47 2008 us=892597   priv_key_file = '[UNDEF]'
Sat Nov 15 17:48:47 2008 us=892701   pkcs12_file = '[UNDEF]'
Sat Nov 15 17:48:47 2008 us=892807   cipher_list = '[UNDEF]'
Sat Nov 15 17:48:47 2008 us=892912   tls_verify = '[UNDEF]'
Sat Nov 15 17:48:47 2008 us=893019   tls_remote = '[UNDEF]'
Sat Nov 15 17:48:47 2008 us=893125   crl_file = '[UNDEF]'
Sat Nov 15 17:48:47 2008 us=893231   ns_cert_type = 0
Sat Nov 15 17:48:47 2008 us=893338   tls_timeout = 2
Sat Nov 15 17:48:47 2008 us=893445   renegotiate_bytes = 0
Sat Nov 15 17:48:47 2008 us=893552   renegotiate_packets = 0
Sat Nov 15 17:48:47 2008 us=893659   renegotiate_seconds = 3600
Sat Nov 15 17:48:47 2008 us=893766   handshake_window = 60
Sat Nov 15 17:48:47 2008 us=893873   transition_window = 3600
Sat Nov 15 17:48:47 2008 us=893977   single_session = DISABLED
Sat Nov 15 17:48:47 2008 us=894083   tls_exit = DISABLED
Sat Nov 15 17:48:47 2008 us=894189   tls_auth_file = '[UNDEF]'
Sat Nov 15 17:48:47 2008 us=894428   server_network = 0.0.0.0
```

```
Sat Nov 15 17:48:47 2008 us=894555   server_netmask = 0.0.0.0
Sat Nov 15 17:48:47 2008 us=894673   server_bridge_ip = 0.0.0.0
Sat Nov 15 17:48:47 2008 us=894792   server_bridge_netmask = 0.0.0.0
Sat Nov 15 17:48:47 2008 us=894912   server_bridge_pool_start = 0.0.0.0
Sat Nov 15 17:48:47 2008 us=895031   server_bridge_pool_end = 0.0.0.0
Sat Nov 15 17:48:47 2008 us=895140   ifconfig_pool_defined = DISABLED
Sat Nov 15 17:48:47 2008 us=897711   ifconfig_pool_start = 0.0.0.0
Sat Nov 15 17:48:47 2008 us=898297   ifconfig_pool_end = 0.0.0.0
Sat Nov 15 17:48:47 2008 us=898672   ifconfig_pool_netmask = 0.0.0.0
Sat Nov 15 17:48:47 2008 us=899060   ifconfig_pool_persist_filename = '[UNDEF]'
Sat Nov 15 17:48:47 2008 us=899615   ifconfig_pool_persist_refresh_freq = 600
Sat Nov 15 17:48:47 2008 us=900676   ifconfig_pool_linear = DISABLED
Sat Nov 15 17:48:47 2008 us=901202   n_bcast_buf = 256
Sat Nov 15 17:48:47 2008 us=901590   tcp_queue_limit = 64
Sat Nov 15 17:48:47 2008 us=901932   real_hash_size = 256
Sat Nov 15 17:48:47 2008 us=902271   virtual_hash_size = 256
Sat Nov 15 17:48:47 2008 us=902609   client_connect_script = '[UNDEF]'
Sat Nov 15 17:48:47 2008 us=902954   learn_address_script = '[UNDEF]'
Sat Nov 15 17:48:47 2008 us=903360   client_disconnect_script = '[UNDEF]'
Sat Nov 15 17:48:47 2008 us=903706   client_config_dir = '[UNDEF]'
Sat Nov 15 17:48:47 2008 us=904047   ccd_exclusive = DISABLED
Sat Nov 15 17:48:47 2008 us=904388   tmp_dir = '[UNDEF]'
Sat Nov 15 17:48:47 2008 us=904728   push_ifconfig_defined = DISABLED
Sat Nov 15 17:48:47 2008 us=905084   push_ifconfig_local = 0.0.0.0
Sat Nov 15 17:48:47 2008 us=905442   push_ifconfig_remote_netmask = 0.0.0.0
Sat Nov 15 17:48:47 2008 us=905783   enable_c2c = DISABLED
Sat Nov 15 17:48:47 2008 us=906129   duplicate_cn = DISABLED
Sat Nov 15 17:48:47 2008 us=906469   cf_max = 0
Sat Nov 15 17:48:47 2008 us=906809   cf_per = 0
Sat Nov 15 17:48:47 2008 us=907150   max_clients = 1024
Sat Nov 15 17:48:47 2008 us=907550   max_routes_per_client = 256
Sat Nov 15 17:48:47 2008 us=907895   client_cert_not_required = DISABLED
Sat Nov 15 17:48:47 2008 us=908239   username_as_common_name = DISABLED
Sat Nov 15 17:48:47 2008 us=908584   auth_user_pass_verify_script = '[UNDEF]'
Sat Nov 15 17:48:47 2008 us=909652   auth_user_pass_verify_script_via_file = DISABLED
Sat Nov 15 17:48:47 2008 us=910080   client = DISABLED
Sat Nov 15 17:48:47 2008 us=910480   pull = DISABLED
Sat Nov 15 17:48:47 2008 us=911004   auth_user_pass_file = '[UNDEF]'
Sat Nov 15 17:48:47 2008 us=911590 OpenVPN 2.0.9 i486-pc-linux-gnu [SSL] [LZO] [EPOLL] built on Sep 20
 2007
Sat Nov 15 17:48:47 2008 us=930468 Static Encrypt: Cipher 'BF-CBC' initialized with 128 bit key
Sat Nov 15 17:48:47 2008 us=931249 Static Encrypt: Using 160 bit message hash 'SHA1' for HMAC
 authentication
Sat Nov 15 17:48:47 2008 us=932250 Static Decrypt: Cipher 'BF-CBC' initialized with 128 bit key
Sat Nov 15 17:48:47 2008 us=932794 Static Decrypt: Using 160 bit message hash 'SHA1' for HMAC
 authentication
Sat Nov 15 17:48:47 2008 us=933445 LZO compression initialized
Sat Nov 15 17:48:47 2008 us=988633 TUN/TAP device tun1 opened
Sat Nov 15 17:48:47 2008 us=989602 TUN/TAP TX queue length set to 100
Sat Nov 15 17:48:47 2008 us=990265 ifconfig tun1 192.168.25.2 pointopoint 192.168.25.1 mtu 1500
Sat Nov 15 17:48:48 2008 us=16600 Data Channel MTU parms [ L:1545 D:1450 EF:45 EB:135 ET:0 EL:0
 AF:3/1 ]
Sat Nov 15 17:48:48 2008 us=16998 Local Options String: 'V4,dev-type tun,link-mtu 1545,tun-mtu
 1500,proto UDPv4,ifconfig 192.168.25.1 192.168.25.2,comp-lzo,cipher BF-CBC,auth SHA1,keysize
 128,secret'
Sat Nov 15 17:48:48 2008 us=17112 Expected Remote Options String: 'V4,dev-type tun,link-mtu 1545,tun-
mtu 1500,proto UDPv4,ifconfig 192.168.25.2 192.168.25.1,comp-lzo,cipher BF-CBC,auth SHA1,keysize
 128,secret'
Sat Nov 15 17:48:48 2008 us=17383 Local Options hash (VER=V4): '3210d11a'
Sat Nov 15 17:48:48 2008 us=17565 Expected Remote Options hash (VER=V4): '6963813b'
Sat Nov 15 17:48:48 2008 us=17795 Socket Buffers: R=[110592->131072] S=[110592->131072]
Sat Nov 15 17:48:48 2008 us=17940 UDPv4 link local (bound): [undef]:8147
Sat Nov 15 17:48:48 2008 us=18059 UDPv4 link remote: 82.127.57.95:8147
Sat Nov 15 17:48:58 2008 us=894383 Peer Connection Initiated with 82.127.57.95:8147
Sat Nov 15 17:49:00 2008 us=39348 Initialization Sequence Completed
```

Rien à dire de plus.

3-2-4 - Contrôle

Depuis aaron :

```
aaron:~# ping -c 4 192.168.25.2
PING 192.168.25.2 (192.168.25.2) 56(84) bytes of data.
64 bytes from 192.168.25.2: icmp_seq=1 ttl=64 time=53.2 ms
64 bytes from 192.168.25.2: icmp_seq=2 ttl=64 time=52.3 ms
64 bytes from 192.168.25.2: icmp_seq=3 ttl=64 time=49.9 ms
64 bytes from 192.168.25.2: icmp_seq=4 ttl=64 time=50.9 ms

--- 192.168.25.2 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 2998ms
rtt min/avg/max/mdev = 49.942/51.613/53.256/1.309 ms
```

Si ça marche dans un sens, il n'y a pas de raison que ce ne soit pas pareil dans l'autre :

```
cyclope:~# ping -c 4 192.168.25.1
PING 192.168.25.1 (192.168.25.1) 56(84) bytes of data.
64 bytes from 192.168.25.1: icmp_seq=1 ttl=64 time=52.8 ms
64 bytes from 192.168.25.1: icmp_seq=2 ttl=64 time=59.7 ms
64 bytes from 192.168.25.1: icmp_seq=3 ttl=64 time=50.9 ms
64 bytes from 192.168.25.1: icmp_seq=4 ttl=64 time=51.1 ms

--- 192.168.25.1 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3001ms
rtt min/avg/max/mdev = 50.980/53.681/59.734/3.574 ms
```

3-2-5 - Conclusion intermédiaire

Nous disposons ici d'un tunnel relativement sécurisé. Il le sera aussi longtemps que le secret partagé, ne sera pas trop partagé, c'est-à-dire qu'il ne le sera qu'entre aaron et cyclope.

Dans l'étape suivante, en utilisant TLS et des certificats, nous pourrons non seulement chiffrer les données, mais également faire une authentification mutuelle de chaque bout du tunnel.

3-3 - OpenVPN avec TLS

3-3-1 - Les certificats

Puisque nous savons utiliser TinyCA, autant nous en servir. Nous allons créer avec notre CA un certificat pour aaron (serveur) et un autre pour cyclope (client) et allons les placer, ainsi que leur clé privée, sur leurs destinations respectives.

Nous ne détaillons pas la création de ces certificats, reportez-vous à la page **Mise en œuvre avec TinyCA** du chapitre **Notions de cryptographie**.

Nous disposons donc de :

- bts.eme-cacert.pem le certificat de notre CA ;
- cyclope.maison.mrs-key.pem la clé privée de cyclope ;
- cyclope.maison.mrs.pem le certificat de cyclope ;
- aaron.bts.eme-key.pem la clé privée de aaron ;
- aaron.bts.eme.pem le certificat de aaron.

Nous posons, par un moyen sécurisé, bts.eme-cacert.pem, cyclope.maison.mrs-key.pem et cyclope.maison.mrs.pem par exemple dans le répertoire de root de cyclope.

Nous posons, par un moyen sécurisé, bts.eme-cacert.pem, aaron.bts.eme-key.pem et aaron.bts.eme.pem par exemple dans le répertoire de root de aaron.

3-3-2 - Paramètre « Diffie Hellman »

Enfin, nous créons sur aaron (le serveur), un paramètre « Diffie Hellman » au moyen d'OpenSSL, qui servira à générer les clés de session. En effet, la cryptographie « asymétrique », très gourmande en ressources, n'est utilisée que dans la phase d'authentification et d'établissement du tunnel. Par la suite, les données sont chiffrées de manière symétrique avec une clé partagée, communiquée par le serveur au client (à travers un chiffrement asymétrique, bien entendu).

```
aaron:~# openssl dhparam -out dh1024.pem 1024
Generating DH parameters, 1024 bit long safe prime, generator 2
This is going to take a long time
.................................
```

Et quelques (parfois très longues) minutes plus tard, nous avons le fichier :

```
aaron:~# cat dh1024.pem
-----BEGIN DH PARAMETERS-----
MIGHAoGBANcTIW0XcvuNDSgK+KiS0rmo14zHNxnMK3IHjvWCqjJL8F0+nwFKvLql
FBggAoL1Si+4iuVJoZU3T4H/tsGlsayvWF1l4PNVuaenER2bhIDeFNGx1A/WbYmK
1JNOVpyfwC/i1fv1L/8bpzrjGsgl4GIy8sKzJt+PXRcV61fcJIM7AgEC
-----END DH PARAMETERS-----
```

Celui-là, on ne pourra pas dire qu'il a été écrit à la légère.

3-3-3 - Le tunnel final

La ligne de commande va commencer à être longue…

3-3-3-1 - Sur aaron

C'est le serveur.

```
aaron:~# openvpn --port 8147 --dev tun1 --ifconfig 192.168.25.1 192.168.25.2 --comp-lzo --verb 5 --tls-
server --dh dh1024.pem --ca bts.eme-cacert.pem --cert aaron.bts.eme.pem --key aaron.bts.eme-key.pem --
reneg-sec 21600
```

Ce qui nous dit :

```
Sat Nov 15 18:49:41 2008 us=923686 Current Parameter Settings:
Sat Nov 15 18:49:41 2008 us=924704   config = '[UNDEF]'
Sat Nov 15 18:49:41 2008 us=924953   mode = 0
Sat Nov 15 18:49:41 2008 us=925180   persist_config = DISABLED
Sat Nov 15 18:49:41 2008 us=925410   persist_mode = 1
Sat Nov 15 18:49:41 2008 us=925635   show_ciphers = DISABLED
Sat Nov 15 18:49:41 2008 us=925862   show_digests = DISABLED
Sat Nov 15 18:49:41 2008 us=926087   show_engines = DISABLED
Sat Nov 15 18:49:41 2008 us=926314   genkey = DISABLED
Sat Nov 15 18:49:41 2008 us=926542   key_pass_file = '[UNDEF]'
Sat Nov 15 18:49:41 2008 us=926771   show_tls_ciphers = DISABLED
Sat Nov 15 18:49:41 2008 us=927001   proto = 0
Sat Nov 15 18:49:41 2008 us=927226   local = '[UNDEF]'
Sat Nov 15 18:49:41 2008 us=927452   remote_list = NULL
Sat Nov 15 18:49:41 2008 us=927679   remote_random = DISABLED
Sat Nov 15 18:49:41 2008 us=927909   local_port = 8147
Sat Nov 15 18:49:41 2008 us=928155   remote_port = 8147
Sat Nov 15 18:49:41 2008 us=928381   remote_float = DISABLED
Sat Nov 15 18:49:41 2008 us=928688   ipchange = '[UNDEF]'
Sat Nov 15 18:49:41 2008 us=928925   bind_local = ENABLED
```

```
Sat Nov 15 18:49:41 2008 us=929153   dev = 'tun1'
Sat Nov 15 18:49:41 2008 us=929381   dev_type = '[UNDEF]'
Sat Nov 15 18:49:41 2008 us=929608   dev_node = '[UNDEF]'
Sat Nov 15 18:49:41 2008 us=929832   tun_ipv6 = DISABLED
Sat Nov 15 18:49:41 2008 us=930059   ifconfig_local = '192.168.25.1'
Sat Nov 15 18:49:41 2008 us=930303   ifconfig_remote_netmask = '192.168.25.2'
Sat Nov 15 18:49:41 2008 us=930536   ifconfig_noexec = DISABLED
Sat Nov 15 18:49:41 2008 us=930765   ifconfig_nowarn = DISABLED
Sat Nov 15 18:49:41 2008 us=930995   shaper = 0
Sat Nov 15 18:49:41 2008 us=931222   tun_mtu = 1500
Sat Nov 15 18:49:41 2008 us=931452   tun_mtu_defined = ENABLED
Sat Nov 15 18:49:41 2008 us=931683   link_mtu = 1500
Sat Nov 15 18:49:41 2008 us=931909   link_mtu_defined = DISABLED
Sat Nov 15 18:49:41 2008 us=932140   tun_mtu_extra = 0
Sat Nov 15 18:49:41 2008 us=932365   tun_mtu_extra_defined = DISABLED
Sat Nov 15 18:49:41 2008 us=932635   fragment = 0
Sat Nov 15 18:49:41 2008 us=932866   mtu_discover_type = -1
Sat Nov 15 18:49:41 2008 us=933092   mtu_test = 0
Sat Nov 15 18:49:41 2008 us=933317   mlock = DISABLED
Sat Nov 15 18:49:41 2008 us=933545   keepalive_ping = 0
Sat Nov 15 18:49:41 2008 us=933772   keepalive_timeout = 0
Sat Nov 15 18:49:41 2008 us=933999   inactivity_timeout = 0
Sat Nov 15 18:49:41 2008 us=934227   ping_send_timeout = 0
Sat Nov 15 18:49:41 2008 us=934452   ping_rec_timeout = 0
Sat Nov 15 18:49:41 2008 us=934679   ping_rec_timeout_action = 0
Sat Nov 15 18:49:41 2008 us=934921   ping_timer_remote = DISABLED
Sat Nov 15 18:49:41 2008 us=935153   remap_sigusr1 = 0
Sat Nov 15 18:49:41 2008 us=935381   explicit_exit_notification = 0
Sat Nov 15 18:49:41 2008 us=935609   persist_tun = DISABLED
Sat Nov 15 18:49:41 2008 us=935837   persist_local_ip = DISABLED
Sat Nov 15 18:49:41 2008 us=936065   persist_remote_ip = DISABLED
Sat Nov 15 18:49:41 2008 us=936294   persist_key = DISABLED
Sat Nov 15 18:49:41 2008 us=936521   mssfix = 1450
Sat Nov 15 18:49:41 2008 us=936787   passtos = DISABLED
Sat Nov 15 18:49:41 2008 us=937016   resolve_retry_seconds = 1000000000
Sat Nov 15 18:49:41 2008 us=937245   connect_retry_seconds = 5
Sat Nov 15 18:49:41 2008 us=937473   username = '[UNDEF]'
Sat Nov 15 18:49:41 2008 us=937700   groupname = '[UNDEF]'
Sat Nov 15 18:49:41 2008 us=937926   chroot_dir = '[UNDEF]'
Sat Nov 15 18:49:41 2008 us=938157   cd_dir = '[UNDEF]'
Sat Nov 15 18:49:41 2008 us=938385   writepid = '[UNDEF]'
Sat Nov 15 18:49:41 2008 us=938612   up_script = '[UNDEF]'
Sat Nov 15 18:49:41 2008 us=938839   down_script = '[UNDEF]'
Sat Nov 15 18:49:41 2008 us=939065   down_pre = DISABLED
Sat Nov 15 18:49:41 2008 us=939291   up_restart = DISABLED
Sat Nov 15 18:49:41 2008 us=939518   up_delay = DISABLED
Sat Nov 15 18:49:41 2008 us=939743   daemon = DISABLED
Sat Nov 15 18:49:41 2008 us=939970   inetd = 0
Sat Nov 15 18:49:41 2008 us=940195   log = DISABLED
Sat Nov 15 18:49:41 2008 us=940422   suppress_timestamps = DISABLED
Sat Nov 15 18:49:41 2008 us=940692   nice = 0
Sat Nov 15 18:49:41 2008 us=940919   verbosity = 5
Sat Nov 15 18:49:41 2008 us=941146   mute = 0
Sat Nov 15 18:49:41 2008 us=941372   gremlin = 0
Sat Nov 15 18:49:41 2008 us=941611   status_file = '[UNDEF]'
Sat Nov 15 18:49:41 2008 us=941840   status_file_version = 1
Sat Nov 15 18:49:41 2008 us=942066   status_file_update_freq = 60
Sat Nov 15 18:49:41 2008 us=942292   occ = ENABLED
Sat Nov 15 18:49:41 2008 us=942520   rcvbuf = 65536
Sat Nov 15 18:49:41 2008 us=942747   sndbuf = 65536
Sat Nov 15 18:49:41 2008 us=942975   socks_proxy_server = '[UNDEF]'
Sat Nov 15 18:49:41 2008 us=943205   socks_proxy_port = 0
Sat Nov 15 18:49:41 2008 us=943431   socks_proxy_retry = DISABLED
Sat Nov 15 18:49:41 2008 us=943660   fast_io = DISABLED
Sat Nov 15 18:49:41 2008 us=943887   comp_lzo = ENABLED
Sat Nov 15 18:49:41 2008 us=944114   comp_lzo_adaptive = ENABLED
Sat Nov 15 18:49:41 2008 us=944345   route_script = '[UNDEF]'
Sat Nov 15 18:49:41 2008 us=944614   route_default_gateway = '[UNDEF]'
Sat Nov 15 18:49:41 2008 us=944852   route_noexec = DISABLED
Sat Nov 15 18:49:41 2008 us=945081   route_delay = 0
Sat Nov 15 18:49:41 2008 us=945309   route_delay_window = 30
Sat Nov 15 18:49:41 2008 us=945534   route_delay_defined = DISABLED
```

```
Sat Nov 15 18:49:41 2008 us=945764   management_addr = '[UNDEF]'
Sat Nov 15 18:49:41 2008 us=945995   management_port = 0
Sat Nov 15 18:49:41 2008 us=946221   management_user_pass = '[UNDEF]'
Sat Nov 15 18:49:41 2008 us=946452   management_log_history_cache = 250
Sat Nov 15 18:49:41 2008 us=946683   management_echo_buffer_size = 100
Sat Nov 15 18:49:41 2008 us=946911   management_query_passwords = DISABLED
Sat Nov 15 18:49:41 2008 us=947139   management_hold = DISABLED
Sat Nov 15 18:49:41 2008 us=947369   shared_secret_file = '[UNDEF]'
Sat Nov 15 18:49:41 2008 us=947599   key_direction = 0
Sat Nov 15 18:49:41 2008 us=947842   ciphername_defined = ENABLED
Sat Nov 15 18:49:41 2008 us=948074   ciphername = 'BF-CBC'
Sat Nov 15 18:49:41 2008 us=948302   authname_defined = ENABLED
Sat Nov 15 18:49:41 2008 us=948809   authname = 'SHA1'
Sat Nov 15 18:49:41 2008 us=949054   keysize = 0
Sat Nov 15 18:49:41 2008 us=949281   engine = DISABLED
Sat Nov 15 18:49:41 2008 us=949509   replay = ENABLED
Sat Nov 15 18:49:41 2008 us=949738   mute_replay_warnings = DISABLED
Sat Nov 15 18:49:41 2008 us=949970   replay_window = 64
Sat Nov 15 18:49:41 2008 us=950198   replay_time = 15
Sat Nov 15 18:49:41 2008 us=950424   packet_id_file = '[UNDEF]'
Sat Nov 15 18:49:41 2008 us=950654   use_iv = ENABLED
Sat Nov 15 18:49:41 2008 us=950882   test_crypto = DISABLED
Sat Nov 15 18:49:41 2008 us=951109   tls_server = ENABLED
Sat Nov 15 18:49:41 2008 us=951336   tls_client = DISABLED
Sat Nov 15 18:49:41 2008 us=951569   key_method = 2
Sat Nov 15 18:49:41 2008 us=951797   ca_file = 'bts.eme-cacert.pem'
Sat Nov 15 18:49:41 2008 us=952028   dh_file = 'dh1024.pem'
Sat Nov 15 18:49:41 2008 us=952256   cert_file = 'aaron.bts.eme.pem'
Sat Nov 15 18:49:41 2008 us=952485   priv_key_file = 'aaron.bts.eme-key.pem'
Sat Nov 15 18:49:41 2008 us=952760   pkcs12_file = '[UNDEF]'
Sat Nov 15 18:49:41 2008 us=952987   cipher_list = '[UNDEF]'
Sat Nov 15 18:49:41 2008 us=953214   tls_verify = '[UNDEF]'
Sat Nov 15 18:49:41 2008 us=953442   tls_remote = '[UNDEF]'
Sat Nov 15 18:49:41 2008 us=953669   crl_file = '[UNDEF]'
Sat Nov 15 18:49:41 2008 us=953898   ns_cert_type = 0
Sat Nov 15 18:49:41 2008 us=954127   tls_timeout = 2
Sat Nov 15 18:49:41 2008 us=954356   renegotiate_bytes = 0
Sat Nov 15 18:49:41 2008 us=954584   renegotiate_packets = 0
Sat Nov 15 18:49:41 2008 us=954826   renegotiate_seconds = 21600
Sat Nov 15 18:49:41 2008 us=955057   handshake_window = 60
Sat Nov 15 18:49:41 2008 us=955285   transition_window = 3600
Sat Nov 15 18:49:41 2008 us=955513   single_session = DISABLED
Sat Nov 15 18:49:41 2008 us=955743   tls_exit = DISABLED
Sat Nov 15 18:49:41 2008 us=955971   tls_auth_file = '[UNDEF]'
Sat Nov 15 18:49:41 2008 us=956283   server_network = 0.0.0.0
Sat Nov 15 18:49:41 2008 us=956530   server_netmask = 0.0.0.0
Sat Nov 15 18:49:41 2008 us=956810   server_bridge_ip = 0.0.0.0
Sat Nov 15 18:49:41 2008 us=957049   server_bridge_netmask = 0.0.0.0
Sat Nov 15 18:49:41 2008 us=957288   server_bridge_pool_start = 0.0.0.0
Sat Nov 15 18:49:41 2008 us=957527   server_bridge_pool_end = 0.0.0.0
Sat Nov 15 18:49:41 2008 us=957758   ifconfig_pool_defined = DISABLED
Sat Nov 15 18:49:41 2008 us=957997   ifconfig_pool_start = 0.0.0.0
Sat Nov 15 18:49:41 2008 us=958249   ifconfig_pool_end = 0.0.0.0
Sat Nov 15 18:49:41 2008 us=958487   ifconfig_pool_netmask = 0.0.0.0
Sat Nov 15 18:49:41 2008 us=958717   ifconfig_pool_persist_filename = '[UNDEF]'
Sat Nov 15 18:49:41 2008 us=958952   ifconfig_pool_persist_refresh_freq = 600
Sat Nov 15 18:49:41 2008 us=959185   ifconfig_pool_linear = DISABLED
Sat Nov 15 18:49:41 2008 us=959417   n_bcast_buf = 256
Sat Nov 15 18:49:41 2008 us=959647   tcp_queue_limit = 64
Sat Nov 15 18:49:41 2008 us=959875   real_hash_size = 256
Sat Nov 15 18:49:41 2008 us=960104   virtual_hash_size = 256
Sat Nov 15 18:49:41 2008 us=960332   client_connect_script = '[UNDEF]'
Sat Nov 15 18:49:41 2008 us=960565   learn_address_script = '[UNDEF]'
Sat Nov 15 18:49:41 2008 us=960836   client_disconnect_script = '[UNDEF]'
Sat Nov 15 18:49:41 2008 us=961068   client_config_dir = '[UNDEF]'
Sat Nov 15 18:49:41 2008 us=961302   ccd_exclusive = DISABLED
Sat Nov 15 18:49:41 2008 us=961532   tmp_dir = '[UNDEF]'
Sat Nov 15 18:49:41 2008 us=961760   push_ifconfig_defined = DISABLED
Sat Nov 15 18:49:41 2008 us=962000   push_ifconfig_local = 0.0.0.0
Sat Nov 15 18:49:41 2008 us=962238   push_ifconfig_remote_netmask = 0.0.0.0
Sat Nov 15 18:49:41 2008 us=962467   enable_c2c = DISABLED
Sat Nov 15 18:49:41 2008 us=962694   duplicate_cn = DISABLED
```

```
Sat Nov 15 18:49:41 2008 us=962921   cf_max = 0
Sat Nov 15 18:49:41 2008 us=963150   cf_per = 0
Sat Nov 15 18:49:41 2008 us=963379   max_clients = 1024
Sat Nov 15 18:49:41 2008 us=963609   max_routes_per_client = 256
Sat Nov 15 18:49:41 2008 us=963839   client_cert_not_required = DISABLED
Sat Nov 15 18:49:41 2008 us=964069   username_as_common_name = DISABLED
Sat Nov 15 18:49:41 2008 us=964300   auth_user_pass_verify_script = '[UNDEF]'
Sat Nov 15 18:49:41 2008 us=964545   auth_user_pass_verify_script_via_file = DISABLED
Sat Nov 15 18:49:41 2008 us=964847   client = DISABLED
Sat Nov 15 18:49:41 2008 us=965048   pull = DISABLED
Sat Nov 15 18:49:41 2008 us=965250   auth_user_pass_file = '[UNDEF]'
Sat Nov 15 18:49:41 2008 us=965456 OpenVPN 2.0.9 i486-pc-linux-gnu [SSL] [LZO] [EPOLL] built on Sep 20
 2007
Sat Nov 15 18:49:42 2008 us=15536 Diffie-Hellman initialized with 1024 bit key
Sat Nov 15 18:49:42 2008 us=21069 LZO compression initialized
Sat Nov 15 18:49:42 2008 us=21975 Control Channel MTU parms [ L:1542 D:138 EF:38 EB:0 ET:0 EL:0 ]
Sat Nov 15 18:49:42 2008 us=72086 TUN/TAP device tun1 opened
Sat Nov 15 18:49:42 2008 us=72501 TUN/TAP TX queue length set to 100
Sat Nov 15 18:49:42 2008 us=72890 ifconfig tun1 192.168.25.1 pointopoint 192.168.25.2 mtu 1500
Sat Nov 15 18:49:42 2008 us=87489 Data Channel MTU parms [ L:1542 D:1450 EF:42 EB:135 ET:0 EL:0
 AF:3/1 ]
Sat Nov 15 18:49:42 2008 us=88034 Local Options String: 'V4,dev-type tun,link-mtu 1542,tun-mtu
 1500,proto UDPv4,ifconfig 192.168.25.2 192.168.25.1,comp-lzo,cipher BF-CBC,auth SHA1,keysize 128,key-
method 2,tls-server'
Sat Nov 15 18:49:42 2008 us=88289 Expected Remote Options String: 'V4,dev-type tun,link-mtu 1542,tun-
mtu 1500,proto UDPv4,ifconfig 192.168.25.1 192.168.25.2,comp-lzo,cipher BF-CBC,auth SHA1,keysize
 128,key-method 2,tls-client'
Sat Nov 15 18:49:42 2008 us=88685 Local Options hash (VER=V4): '40c5ad26'
Sat Nov 15 18:49:42 2008 us=88966 Expected Remote Options hash (VER=V4): 'b7094d11'
Sat Nov 15 18:49:42 2008 us=89285 Socket Buffers: R=[110592->131072] S=[110592->131072]
Sat Nov 15 18:49:42 2008 us=89823 UDPv4 link local (bound): [undef]:8147
Sat Nov 15 18:49:42 2008 us=90054 UDPv4 link remote: [undef]
```

3-3-3-2 - Sur cyclope

C'est le client

```
cyclope:~# openvpn --remote 82.127.57.95  --port 8147 --dev tun1 --ifconfig 192.168.25.2 192.168.25.1
 --comp-lzo --verb 5 --tls-client --ca bts.eme-cacert.pem --cert cyclope.maison.mrs.pem --key
 cyclope.maison.mrs-key.pem
```

```
Sat Nov 15 18:55:03 2008 us=70505 Current Parameter Settings:
Sat Nov 15 18:55:03 2008 us=72038   config = '[UNDEF]'
Sat Nov 15 18:55:03 2008 us=72781   mode = 0
Sat Nov 15 18:55:03 2008 us=73464   persist_config = DISABLED
Sat Nov 15 18:55:03 2008 us=74166   persist_mode = 1
Sat Nov 15 18:55:03 2008 us=74853   show_ciphers = DISABLED
Sat Nov 15 18:55:03 2008 us=75617   show_digests = DISABLED
Sat Nov 15 18:55:03 2008 us=76425   show_engines = DISABLED
Sat Nov 15 18:55:03 2008 us=77118   genkey = DISABLED
Sat Nov 15 18:55:03 2008 us=77810   key_pass_file = '[UNDEF]'
Sat Nov 15 18:55:03 2008 us=78515   show_tls_ciphers = DISABLED
Sat Nov 15 18:55:03 2008 us=79374   proto = 0
Sat Nov 15 18:55:03 2008 us=80071   local = '[UNDEF]'
Sat Nov 15 18:55:03 2008 us=80886   remote_list[0] = {'82.127.57.95', 8147}
Sat Nov 15 18:55:03 2008 us=81641   remote_random = DISABLED
Sat Nov 15 18:55:03 2008 us=82336   local_port = 8147
Sat Nov 15 18:55:03 2008 us=83033   remote_port = 8147
Sat Nov 15 18:55:03 2008 us=84055   remote_float = DISABLED
Sat Nov 15 18:55:03 2008 us=84570   ipchange = '[UNDEF]'
Sat Nov 15 18:55:03 2008 us=84953   bind_local = ENABLED
Sat Nov 15 18:55:03 2008 us=85293   dev = 'tun1'
Sat Nov 15 18:55:03 2008 us=86334   dev_type = '[UNDEF]'
Sat Nov 15 18:55:03 2008 us=86994   dev_node = '[UNDEF]'
Sat Nov 15 18:55:03 2008 us=87748   tun_ipv6 = DISABLED
Sat Nov 15 18:55:03 2008 us=88442   ifconfig_local = '192.168.25.2'
Sat Nov 15 18:55:03 2008 us=89163   ifconfig_remote_netmask = '192.168.25.1'
Sat Nov 15 18:55:03 2008 us=89688   ifconfig_noexec = DISABLED
Sat Nov 15 18:55:03 2008 us=90204   ifconfig_nowarn = DISABLED
```

```
Sat Nov 15 18:55:03 2008 us=91041   shaper = 0
Sat Nov 15 18:55:03 2008 us=91799   tun_mtu = 1500
Sat Nov 15 18:55:03 2008 us=92494   tun_mtu_defined = ENABLED
Sat Nov 15 18:55:03 2008 us=93193   link_mtu = 1500
Sat Nov 15 18:55:03 2008 us=93887   link_mtu_defined = DISABLED
Sat Nov 15 18:55:03 2008 us=94587   tun_mtu_extra = 0
Sat Nov 15 18:55:03 2008 us=95535   tun_mtu_extra_defined = DISABLED
Sat Nov 15 18:55:03 2008 us=96226   fragment = 0
Sat Nov 15 18:55:03 2008 us=96917   mtu_discover_type = -1
Sat Nov 15 18:55:03 2008 us=97432   mtu_test = 0
Sat Nov 15 18:55:03 2008 us=97944   mlock = DISABLED
Sat Nov 15 18:55:03 2008 us=98458   keepalive_ping = 0
Sat Nov 15 18:55:03 2008 us=98613   keepalive_timeout = 0
Sat Nov 15 18:55:03 2008 us=98719   inactivity_timeout = 0
Sat Nov 15 18:55:03 2008 us=98822   ping_send_timeout = 0
Sat Nov 15 18:55:03 2008 us=98924   ping_rec_timeout = 0
Sat Nov 15 18:55:03 2008 us=99027   ping_rec_timeout_action = 0
Sat Nov 15 18:55:03 2008 us=99128   ping_timer_remote = DISABLED
Sat Nov 15 18:55:03 2008 us=99295   remap_sigusr1 = 0
Sat Nov 15 18:55:03 2008 us=99401   explicit_exit_notification = 0
Sat Nov 15 18:55:03 2008 us=99502   persist_tun = DISABLED
Sat Nov 15 18:55:03 2008 us=99604   persist_local_ip = DISABLED
Sat Nov 15 18:55:03 2008 us=99705   persist_remote_ip = DISABLED
Sat Nov 15 18:55:03 2008 us=99806   persist_key = DISABLED
Sat Nov 15 18:55:03 2008 us=99910   mssfix = 1450
Sat Nov 15 18:55:03 2008 us=100010   passtos = DISABLED
Sat Nov 15 18:55:03 2008 us=100116   resolve_retry_seconds = 1000000000
Sat Nov 15 18:55:03 2008 us=100220   connect_retry_seconds = 5
Sat Nov 15 18:55:03 2008 us=100322   username = '[UNDEF]'
Sat Nov 15 18:55:03 2008 us=100425   groupname = '[UNDEF]'
Sat Nov 15 18:55:03 2008 us=100708   chroot_dir = '[UNDEF]'
Sat Nov 15 18:55:03 2008 us=100831   cd_dir = '[UNDEF]'
Sat Nov 15 18:55:03 2008 us=100937   writepid = '[UNDEF]'
Sat Nov 15 18:55:03 2008 us=101038   up_script = '[UNDEF]'
Sat Nov 15 18:55:03 2008 us=101141   down_script = '[UNDEF]'
Sat Nov 15 18:55:03 2008 us=101243   down_pre = DISABLED
Sat Nov 15 18:55:03 2008 us=101344   up_restart = DISABLED
Sat Nov 15 18:55:03 2008 us=101447   up_delay = DISABLED
Sat Nov 15 18:55:03 2008 us=101548   daemon = DISABLED
Sat Nov 15 18:55:03 2008 us=101650   inetd = 0
Sat Nov 15 18:55:03 2008 us=101750   log = DISABLED
Sat Nov 15 18:55:03 2008 us=101852   suppress_timestamps = DISABLED
Sat Nov 15 18:55:03 2008 us=101955   nice = 0
Sat Nov 15 18:55:03 2008 us=102056   verbosity = 5
Sat Nov 15 18:55:03 2008 us=102158   mute = 0
Sat Nov 15 18:55:03 2008 us=102258   gremlin = 0
Sat Nov 15 18:55:03 2008 us=102358   status_file = '[UNDEF]'
Sat Nov 15 18:55:03 2008 us=102462   status_file_version = 1
Sat Nov 15 18:55:03 2008 us=102566   status_file_update_freq = 60
Sat Nov 15 18:55:03 2008 us=102667   occ = ENABLED
Sat Nov 15 18:55:03 2008 us=102769   rcvbuf = 65536
Sat Nov 15 18:55:03 2008 us=102871   sndbuf = 65536
Sat Nov 15 18:55:03 2008 us=102973   socks_proxy_server = '[UNDEF]'
Sat Nov 15 18:55:03 2008 us=103078   socks_proxy_port = 0
Sat Nov 15 18:55:03 2008 us=103234   socks_proxy_retry = DISABLED
Sat Nov 15 18:55:03 2008 us=103346   fast_io = DISABLED
Sat Nov 15 18:55:03 2008 us=103448   comp_lzo = ENABLED
Sat Nov 15 18:55:03 2008 us=103551   comp_lzo_adaptive = ENABLED
Sat Nov 15 18:55:03 2008 us=103654   route_script = '[UNDEF]'
Sat Nov 15 18:55:03 2008 us=103758   route_default_gateway = '[UNDEF]'
Sat Nov 15 18:55:03 2008 us=103860   route_noexec = DISABLED
Sat Nov 15 18:55:03 2008 us=103964   route_delay = 0
Sat Nov 15 18:55:03 2008 us=104066   route_delay_window = 30
Sat Nov 15 18:55:03 2008 us=104167   route_delay_defined = DISABLED
Sat Nov 15 18:55:03 2008 us=104271   management_addr = '[UNDEF]'
Sat Nov 15 18:55:03 2008 us=104376   management_port = 0
Sat Nov 15 18:55:03 2008 us=104477   management_user_pass = '[UNDEF]'
Sat Nov 15 18:55:03 2008 us=104582   management_log_history_cache = 250
Sat Nov 15 18:55:03 2008 us=104687   management_echo_buffer_size = 100
Sat Nov 15 18:55:03 2008 us=104789   management_query_passwords = DISABLED
Sat Nov 15 18:55:03 2008 us=104892   management_hold = DISABLED
Sat Nov 15 18:55:03 2008 us=104996   shared_secret_file = '[UNDEF]'
```

```
Sat Nov 15 18:55:03 2008 us=105101   key_direction = 0
Sat Nov 15 18:55:03 2008 us=105207   ciphername_defined = ENABLED
Sat Nov 15 18:55:03 2008 us=105313   ciphername = 'BF-CBC'
Sat Nov 15 18:55:03 2008 us=105418   authname_defined = ENABLED
Sat Nov 15 18:55:03 2008 us=105522   authname = 'SHA1'
Sat Nov 15 18:55:03 2008 us=105628   keysize = 0
Sat Nov 15 18:55:03 2008 us=105730   engine = DISABLED
Sat Nov 15 18:55:03 2008 us=109467   replay = ENABLED
Sat Nov 15 18:55:03 2008 us=109904   mute_replay_warnings = DISABLED
Sat Nov 15 18:55:03 2008 us=110259   replay_window = 64
Sat Nov 15 18:55:03 2008 us=111754   replay_time = 15
Sat Nov 15 18:55:03 2008 us=112450   packet_id_file = '[UNDEF]'
Sat Nov 15 18:55:03 2008 us=113148   use_iv = ENABLED
Sat Nov 15 18:55:03 2008 us=113838   test_crypto = DISABLED
Sat Nov 15 18:55:03 2008 us=114529   tls_server = DISABLED
Sat Nov 15 18:55:03 2008 us=115306   tls_client = ENABLED
Sat Nov 15 18:55:03 2008 us=115980   key_method = 2
Sat Nov 15 18:55:03 2008 us=116674   ca_file = 'bts.eme-cacert.pem'
Sat Nov 15 18:55:03 2008 us=117377   dh_file = '[UNDEF]'
Sat Nov 15 18:55:03 2008 us=118067   cert_file = 'cyclope.maison.mrs.pem'
Sat Nov 15 18:55:03 2008 us=118769   priv_key_file = 'cyclope.maison.mrs-key.pem'
Sat Nov 15 18:55:03 2008 us=119534   pkcs12_file = '[UNDEF]'
Sat Nov 15 18:55:03 2008 us=120226   cipher_list = '[UNDEF]'
Sat Nov 15 18:55:03 2008 us=120918   tls_verify = '[UNDEF]'
Sat Nov 15 18:55:03 2008 us=121610   tls_remote = '[UNDEF]'
Sat Nov 15 18:55:03 2008 us=121769   crl_file = '[UNDEF]'
Sat Nov 15 18:55:03 2008 us=122060   ns_cert_type = 0
Sat Nov 15 18:55:03 2008 us=122174   tls_timeout = 2
Sat Nov 15 18:55:03 2008 us=122281   renegotiate_bytes = 0
Sat Nov 15 18:55:03 2008 us=122389   renegotiate_packets = 0
Sat Nov 15 18:55:03 2008 us=122496   renegotiate_seconds = 3600
Sat Nov 15 18:55:03 2008 us=122604   handshake_window = 60
Sat Nov 15 18:55:03 2008 us=122709   transition_window = 3600
Sat Nov 15 18:55:03 2008 us=122813   single_session = DISABLED
Sat Nov 15 18:55:03 2008 us=122918   tls_exit = DISABLED
Sat Nov 15 18:55:03 2008 us=123024   tls_auth_file = '[UNDEF]'
Sat Nov 15 18:55:03 2008 us=123350   server_network = 0.0.0.0
Sat Nov 15 18:55:03 2008 us=123480   server_netmask = 0.0.0.0
Sat Nov 15 18:55:03 2008 us=123599   server_bridge_ip = 0.0.0.0
Sat Nov 15 18:55:03 2008 us=123716   server_bridge_netmask = 0.0.0.0
Sat Nov 15 18:55:03 2008 us=123835   server_bridge_pool_start = 0.0.0.0
Sat Nov 15 18:55:03 2008 us=123954   server_bridge_pool_end = 0.0.0.0
Sat Nov 15 18:55:03 2008 us=124061   ifconfig_pool_defined = DISABLED
Sat Nov 15 18:55:03 2008 us=124180   ifconfig_pool_start = 0.0.0.0
Sat Nov 15 18:55:03 2008 us=124299   ifconfig_pool_end = 0.0.0.0
Sat Nov 15 18:55:03 2008 us=124455   ifconfig_pool_netmask = 0.0.0.0
Sat Nov 15 18:55:03 2008 us=124574   ifconfig_pool_persist_filename = '[UNDEF]'
Sat Nov 15 18:55:03 2008 us=124683   ifconfig_pool_persist_refresh_freq = 600
Sat Nov 15 18:55:03 2008 us=124790   ifconfig_pool_linear = DISABLED
Sat Nov 15 18:55:03 2008 us=124897   n_bcast_buf = 256
Sat Nov 15 18:55:03 2008 us=125005   tcp_queue_limit = 64
Sat Nov 15 18:55:03 2008 us=125109   real_hash_size = 256
Sat Nov 15 18:55:03 2008 us=125214   virtual_hash_size = 256
Sat Nov 15 18:55:03 2008 us=125321   client_connect_script = '[UNDEF]'
Sat Nov 15 18:55:03 2008 us=125429   learn_address_script = '[UNDEF]'
Sat Nov 15 18:55:03 2008 us=125536   client_disconnect_script = '[UNDEF]'
Sat Nov 15 18:55:03 2008 us=125642   client_config_dir = '[UNDEF]'
Sat Nov 15 18:55:03 2008 us=125747   ccd_exclusive = DISABLED
Sat Nov 15 18:55:03 2008 us=125851   tmp_dir = '[UNDEF]'
Sat Nov 15 18:55:03 2008 us=125955   push_ifconfig_defined = DISABLED
Sat Nov 15 18:55:03 2008 us=126075   push_ifconfig_local = 0.0.0.0
Sat Nov 15 18:55:03 2008 us=126193   push_ifconfig_remote_netmask = 0.0.0.0
Sat Nov 15 18:55:03 2008 us=126299   enable_c2c = DISABLED
Sat Nov 15 18:55:03 2008 us=126403   duplicate_cn = DISABLED
Sat Nov 15 18:55:03 2008 us=126509   cf_max = 0
Sat Nov 15 18:55:03 2008 us=126612   cf_per = 0
Sat Nov 15 18:55:03 2008 us=126718   max_clients = 1024
Sat Nov 15 18:55:03 2008 us=126826   max_routes_per_client = 256
Sat Nov 15 18:55:03 2008 us=126931   client_cert_not_required = DISABLED
Sat Nov 15 18:55:03 2008 us=127037   username_as_common_name = DISABLED
Sat Nov 15 18:55:03 2008 us=127144   auth_user_pass_verify_script = '[UNDEF]'
Sat Nov 15 18:55:03 2008 us=127317   auth_user_pass_verify_script_via_file = DISABLED
```

```
Sat Nov 15 18:55:03 2008 us=127426   client = DISABLED
Sat Nov 15 18:55:03 2008 us=127529   pull = DISABLED
Sat Nov 15 18:55:03 2008 us=127633   auth_user_pass_file = '[UNDEF]'
Sat Nov 15 18:55:03 2008 us=127747 OpenVPN 2.0.9 i486-pc-linux-gnu [SSL] [LZO] [EPOLL] built on Sep 20
 2007
Sat Nov 15 18:55:03 2008 us=128224 WARNING: No server certificate verification method has been enabled.
  See http://openvpn.net/howto.html#mitm for more info.
Sat Nov 15 18:55:03 2008 us=193832 LZO compression initialized
Sat Nov 15 18:55:03 2008 us=215986 Control Channel MTU parms [ L:1542 D:138 EF:38 EB:0 ET:0 EL:0 ]
Sat Nov 15 18:55:03 2008 us=274091 TUN/TAP device tun1 opened
Sat Nov 15 18:55:03 2008 us=275033 TUN/TAP TX queue length set to 100
Sat Nov 15 18:55:03 2008 us=275779 ifconfig tun1 192.168.25.2 pointopoint 192.168.25.1 mtu 1500
Sat Nov 15 18:55:03 2008 us=467561 Data Channel MTU parms [ L:1542 D:1450 EF:42 EB:135 ET:0 EL:0
 AF:3/1 ]
Sat Nov 15 18:55:03 2008 us=468607 Local Options String: 'V4,dev-type tun,link-mtu 1542,tun-mtu
 1500,proto UDPv4,ifconfig 192.168.25.1 192.168.25.2,comp-lzo,cipher BF-CBC,auth SHA1,keysize 128,key-
method 2,tls-client'
Sat Nov 15 18:55:03 2008 us=469420 Expected Remote Options String: 'V4,dev-type tun,link-mtu 1542,tun-
mtu 1500,proto UDPv4,ifconfig 192.168.25.2 192.168.25.1,comp-lzo,cipher BF-CBC,auth SHA1,keysize
 128,key-method 2,tls-server'
Sat Nov 15 18:55:03 2008 us=470311 Local Options hash (VER=V4): 'b7094d11'
Sat Nov 15 18:55:03 2008 us=471125 Expected Remote Options hash (VER=V4): '40c5ad26'
Sat Nov 15 18:55:03 2008 us=472024 Socket Buffers: R=[110592->131072] S=[110592->131072]
Sat Nov 15 18:55:03 2008 us=472741 UDPv4 link local (bound): [undef]:8147
Sat Nov 15 18:55:03 2008 us=473457 UDPv4 link remote: 82.127.57.95:8147
Sat Nov 15 18:55:03 2008 us=566989 TLS: Initial packet from 82.127.57.95:8147, sid=fa310697 a7811164
Sat Nov 15 18:55:04 2008 us=947948 VERIFY OK: depth=1, /C=FR/ST=Bouches_du_Rhone/L=Marseille/O=EME/
OU=EME/CN=rootCA.bts.eme/emailAddress=sysop@bts.eme
Sat Nov 15 18:55:04 2008 us=963876 VERIFY OK: depth=0, /C=FR/ST=Bouches_du_Rhone/L=Marseille/O=EME/
OU=EME/CN=aaron.bts.eme/emailAddress=sysop@bts.eme
Sat Nov 15 18:55:07 2008 us=57442 Data Channel Encrypt: Cipher 'BF-CBC' initialized with 128 bit key
Sat Nov 15 18:55:07 2008 us=58073 Data Channel Encrypt: Using 160 bit message hash 'SHA1' for HMAC
 authentication
Sat Nov 15 18:55:07 2008 us=59658 Data Channel Decrypt: Cipher 'BF-CBC' initialized with 128 bit key
Sat Nov 15 18:55:07 2008 us=60217 Data Channel Decrypt: Using 160 bit message hash 'SHA1' for HMAC
 authentication
Sat Nov 15 18:55:07 2008 us=62054 Control Channel: TLSv1, cipher TLSv1/SSLv3 DHE-RSA-AES256-SHA, 4096
 bit RSA
Sat Nov 15 18:55:07 2008 us=62827 [aaron.bts.eme] Peer Connection Initiated with 82.127.57.95:8147
Sat Nov 15 18:55:08 2008 us=235349 Initialization Sequence Completed
```

Sitôt que le client se connecte au serveur, il obtient le certificat de aaron et vérifie qu'il est bien signé par la CA. Il doit se passer aussi des choses sur aaron concernant l'identité de cyclope :

```
Sat Nov 15 18:55:11 2008 us=189661 TLS: Initial packet from 82.229.41.132:8147, sid=66df4f24 9bbda6c9
Sat Nov 15 18:55:14 2008 us=507464 VERIFY OK: depth=1, /C=FR/ST=Bouches_du_Rhone/L=Marseille/O=EME/
OU=EME/CN=rootCA.bts.eme/emailAddress=sysop@bts.eme
Sat Nov 15 18:55:14 2008 us=517805 VERIFY OK: depth=0, /C=FR/ST=Bouches_du_Rhone/L=Marseille/O=EME/
OU=EME/CN=cyclope.maison.mrs/emailAddress=sysop@maison.mrs
Sat Nov 15 18:55:14 2008 us=697312 Data Channel Encrypt: Cipher 'BF-CBC' initialized with 128 bit key
Sat Nov 15 18:55:14 2008 us=697683 Data Channel Encrypt: Using 160 bit message hash 'SHA1' for HMAC
 authentication
Sat Nov 15 18:55:14 2008 us=698267 Data Channel Decrypt: Cipher 'BF-CBC' initialized with 128 bit key
Sat Nov 15 18:55:14 2008 us=698533 Data Channel Decrypt: Using 160 bit message hash 'SHA1' for HMAC
 authentication
Sat Nov 15 18:55:14 2008 us=775185 Control Channel: TLSv1, cipher TLSv1/SSLv3 DHE-RSA-AES256-SHA, 4096
 bit RSA
Sat Nov 15 18:55:14 2008 us=775576 [cyclope.maison.mrs] Peer Connection Initiated with 80.8.135.67:8147
Sat Nov 15 18:55:15 2008 us=812670 Initialization Sequence Completed
```

Effectivement il y a bien authentification mutuelle des deux bouts du tunnel.

3-3-4 - Conclusion presque finale

Nous disposons désormais d'un tunnel chiffré, où chaque extrémité sait authentifier l'autre bout. En réalité, il ne fait que vérifier que le certificat présenté par l'autre bout est bien signé par la CA connue (directive -ca).

Avant de mettre en production, il serait peut-être bon de durcir encore un peu plus ce tunnel, si c'est possible.

3-4 - Mise en production

3-4-1 - Implémentation Debian

Il suffit donc d'installer le paquet openvpn et les dépendances manquantes viendront avec. L'installation, en plus du code et de la documentation dans /usr/share/doc/openvpn (le README.Debian n'est pas une lecture inutile) produit un répertoire /etc/openvpn vide et un fichier /etc/default/openvpn auquel il faudra jeter un coup d'œil. De plus, un script d'init /etc/init.d/openvpn permettra le démarrage et l'arrêt automatique du tunnel. Enfin, des scripts de gestion du réseau permettront de démarrer ou d'arrêter les tunnels suivant l'état des interfaces physiques associées.

Voici la liste complète des fichiers installés par le paquet :

```
:~# dpkg -L openvpn
/.
/etc
/etc/openvpn
/etc/network
/etc/network/if-up.d
/etc/network/if-up.d/openvpn
/etc/network/if-down.d
/etc/network/if-down.d/openvpn
/etc/default
/etc/default/openvpn
/etc/init.d
/etc/init.d/openvpn
/usr
/usr/sbin
/usr/sbin/openvpn
/usr/share
/usr/share/man
/usr/share/man/man8
/usr/share/man/man8/openvpn.8.gz
/usr/share/doc
/usr/share/doc/openvpn
/usr/share/doc/openvpn/README.auth-pam
/usr/share/doc/openvpn/README.down-root
/usr/share/doc/openvpn/AUTHORS
/usr/share/doc/openvpn/PORTS
/usr/share/doc/openvpn/README
/usr/share/doc/openvpn/README.Debian
/usr/share/doc/openvpn/copyright
/usr/share/doc/openvpn/examples
/usr/share/doc/openvpn/examples/sample-config-files
/usr/share/doc/openvpn/examples/sample-config-files/openvpn-startup.sh
/usr/share/doc/openvpn/examples/sample-config-files/firewall.sh
/usr/share/doc/openvpn/examples/sample-config-files/loopback-client
/usr/share/doc/openvpn/examples/sample-config-files/README
/usr/share/doc/openvpn/examples/sample-config-files/xinetd-server-config
/usr/share/doc/openvpn/examples/sample-config-files/loopback-server
/usr/share/doc/openvpn/examples/sample-config-files/office.up
/usr/share/doc/openvpn/examples/sample-config-files/xinetd-client-config
/usr/share/doc/openvpn/examples/sample-config-files/home.up
/usr/share/doc/openvpn/examples/sample-config-files/openvpn-shutdown.sh
/usr/share/doc/openvpn/examples/sample-config-files/static-home.conf
/usr/share/doc/openvpn/examples/sample-config-files/tls-home.conf
/usr/share/doc/openvpn/examples/sample-config-files/tls-office.conf
/usr/share/doc/openvpn/examples/sample-config-files/client.conf
/usr/share/doc/openvpn/examples/sample-config-files/static-office.conf
/usr/share/doc/openvpn/examples/sample-config-files/server.conf.gz
/usr/share/doc/openvpn/examples/sample-keys
/usr/share/doc/openvpn/examples/sample-keys/README
/usr/share/doc/openvpn/examples/sample-keys/dh1024.pem
/usr/share/doc/openvpn/examples/sample-keys/pass.crt
/usr/share/doc/openvpn/examples/sample-keys/pass.key
```

```
/usr/share/doc/openvpn/examples/sample-keys/tmp-ca.crt
/usr/share/doc/openvpn/examples/sample-keys/tmp-ca.key
/usr/share/doc/openvpn/examples/sample-keys/server.crt
/usr/share/doc/openvpn/examples/sample-keys/server.key
/usr/share/doc/openvpn/examples/sample-keys/client.crt
/usr/share/doc/openvpn/examples/sample-keys/client.key
/usr/share/doc/openvpn/examples/sample-keys/pkcs12.p12
/usr/share/doc/openvpn/examples/easy-rsa
/usr/share/doc/openvpn/examples/easy-rsa/2.0
/usr/share/doc/openvpn/examples/easy-rsa/2.0/vars
/usr/share/doc/openvpn/examples/easy-rsa/2.0/list-crl
/usr/share/doc/openvpn/examples/easy-rsa/2.0/clean-all
/usr/share/doc/openvpn/examples/easy-rsa/2.0/Makefile
/usr/share/doc/openvpn/examples/easy-rsa/2.0/openssl.cnf
/usr/share/doc/openvpn/examples/easy-rsa/2.0/sign-req
/usr/share/doc/openvpn/examples/easy-rsa/2.0/build-key-pkcs12
/usr/share/doc/openvpn/examples/easy-rsa/2.0/build-key-server
/usr/share/doc/openvpn/examples/easy-rsa/2.0/build-key-pass
/usr/share/doc/openvpn/examples/easy-rsa/2.0/revoke-full
/usr/share/doc/openvpn/examples/easy-rsa/2.0/build-req-pass
/usr/share/doc/openvpn/examples/easy-rsa/2.0/inherit-inter
/usr/share/doc/openvpn/examples/easy-rsa/2.0/whichopensslcnf
/usr/share/doc/openvpn/examples/easy-rsa/2.0/build-key
/usr/share/doc/openvpn/examples/easy-rsa/2.0/build-req
/usr/share/doc/openvpn/examples/easy-rsa/2.0/build-ca
/usr/share/doc/openvpn/examples/easy-rsa/2.0/build-dh
/usr/share/doc/openvpn/examples/easy-rsa/2.0/build-inter
/usr/share/doc/openvpn/examples/easy-rsa/2.0/pkitool
/usr/share/doc/openvpn/examples/easy-rsa/2.0/README.gz
/usr/share/doc/openvpn/examples/easy-rsa/2.0/openssl-0.9.6.cnf.gz
/usr/share/doc/openvpn/examples/easy-rsa/vars
/usr/share/doc/openvpn/examples/easy-rsa/list-crl
/usr/share/doc/openvpn/examples/easy-rsa/clean-all
/usr/share/doc/openvpn/examples/easy-rsa/openssl.cnf
/usr/share/doc/openvpn/examples/easy-rsa/sign-req
/usr/share/doc/openvpn/examples/easy-rsa/build-key-pkcs12
/usr/share/doc/openvpn/examples/easy-rsa/build-key-server
/usr/share/doc/openvpn/examples/easy-rsa/build-key-pass
/usr/share/doc/openvpn/examples/easy-rsa/revoke-full
/usr/share/doc/openvpn/examples/easy-rsa/.externals
/usr/share/doc/openvpn/examples/easy-rsa/make-crl
/usr/share/doc/openvpn/examples/easy-rsa/build-req-pass
/usr/share/doc/openvpn/examples/easy-rsa/build-key
/usr/share/doc/openvpn/examples/easy-rsa/build-req
/usr/share/doc/openvpn/examples/easy-rsa/build-ca
/usr/share/doc/openvpn/examples/easy-rsa/build-dh
/usr/share/doc/openvpn/examples/easy-rsa/build-inter
/usr/share/doc/openvpn/examples/easy-rsa/revoke-crt
/usr/share/doc/openvpn/examples/easy-rsa/README.gz
/usr/share/doc/openvpn/changelog.Debian.gz
/usr/share/doc/openvpn/changelog.gz
/usr/share/openvpn
/usr/share/openvpn/verify-cn
/usr/lib
/usr/lib/openvpn
/usr/lib/openvpn/openvpn-auth-pam.so
/usr/lib/openvpn/openvpn-down-root.so
/usr/include
/usr/include/openvpn
/usr/include/openvpn/openvpn-plugin.h
```

Il suffira de placer dans le répertoire /etc/openvpn/ autant de fichiers de configuration que l'on souhaitera démarrer de tunnels différents. Ces fichiers de configuration devront contenir les paramètres que nous avons jusqu'ici indiqués en ligne de commande.

3-4-2 - Mise en service

Nous allons donc créer pour chaque extrémité de tunnel un fichier de configuration qui aboutira au même mode de fonctionnement que celui que nous avons vu en page précédente.

3-4-2-1 - Pour aaron

(Le serveur.)

Nous avions la ligne de commande :

```
openvpn --port 8147 --dev tun1 --ifconfig 192.168.25.1 192.168.25.2 --comp-lzo --verb 5 --tls-server --
dh dh1024.pem --ca bts.eme-cacert.pem --cert aaron.bts.eme.pem --key aaron.bts.eme-key.pem --reneg-sec
 21600
```

Ceci va nous donner, avec quelques modifications nécessaires :

```
port 8147
dev tun1
ifconfig 192.168.25.1 192.168.25.2
comp-lzo
verb 5
tls-server
dh /root/dh1024.pem
ca /root/bts.eme-cacert.pem
cert /root/aaron.bts.eme.pem
key /root/aaron.bts.eme-key.pem
reneg-sec 21600
```

Il sera sans doute intéressant de compléter quelque peu ce fichier, et probablement de déplacer les clés, certificats et autres ustensiles de sécurité ailleurs, avant de démarrer le tunnel.

3-4-2-2 - Pour cyclope

(Le client.)

Nous avions :

```
openvpn --remote 82.127.57.95  --port 8147 --dev tun1 --ifconfig 192.168.25.2 192.168.25.1 --comp-lzo
 --verb 5 --tls-client --ca bts.eme-cacert.pem --cert cyclope.maison.mrs.pem --key cyclope.maison.mrs-
key.pem
```

Ce qui nous donne :

```
remote 82.127.57.95
port 8147
dev tun1
ifconfig 192.168.25.2 192.168.25.1
comp-lzo
verb 5
tls-client
ca /root/bts.eme-cacert.pem
cert /root/cyclope.maison.mrs.pem
key /root/cyclope.maison.mrs-key.pem
```

Mêmes remarques.

3-4-3 - Durcissement

Voyons un peu, avant de mettre en production, s'il est possible de prendre quelques mesures susceptibles de rendre notre tunnel plus solide, en termes de sécurité.

3-4-3-1 - Interface d'écoute

Dans la configuration actuelle, openvpn va écouter sur toutes les interfaces de l'hôte. Ce n'est ni nécessaire ni même souhaitable, suivant la configuration de notre hôte. Le paramètre :

```
local <adresse_ip>
```

permettra de n'écouter que sur l'adresse spécifiée. Pratique uniquement en cas d'adresse IP fixe bien entendu.

3-4-3-2 - Mode point à point

OpenVPN, dans ses versions 2.0 et supérieures, sait faire des tunnels multipoints. Si ce n'est pas ce que nous souhaitons, autant le spécifier, même si la documentation dit que le mode par défaut est le mode point à point :

```
mode p2p
```

3-4-3-3 - Gérer les routes

Notre tunnel a pour vocation d'être placé entre deux routeurs, afin d'interconnecter deux réseaux privés distants. Nos routeurs (serveur comme client) ont besoin de connaitre la route vers le réseau distant à atteindre.

Supposons que aaron soit dans le réseau IP 192.168.1.0/24 et que cyclope soit dans 192.168.2.0/24, nous n'aurons pour aaron qu'à rajouter dans la configuration la ligne suivante :

```
route 192.168.2.0 255.255.255.0 192.168.25.2
```

Et pour cyclope :

```
route 192.168.1.0 255.255.255.0 192.168.25.1
```

3-4-3-4 - root

Par défaut, OpenVPN va démarrer sous l'identité root, puis le service restera sous cette identité. Ce n'est sans doute pas une bonne idée et mieux vaudra choisir un utilisateur sans privilèges.

Les paramètres :

```
user nobody
group nogroup
```

arrangeront ça. Mais attention ! Sitôt le tunnel négocié (par root), openvpn va passer en mode « daemon » sans aucun privilège. En cas de rupture du tunnel, il y aura des problèmes, les clés n'étant lisibles que par root. De même pour la manipulation de tun. Il est donc conseillé d'ajouter les paramètres :

```
persistent-key
persistent-tun
```

de manière à ce que nobody ne soit pas amené à faire des choses qu'il n'a pas le droit de faire.

3-4-3-5 - Authentification supplémentaire

La directive tls-auth ajoute une authentification de type HMAC (4) au-dessus du canal TLS « **to protect against DoS attacks »**, dit la documentation.

Nous utilisons une clé partagée, comme celle que nous avons réalisée plus tôt dans ce chapitre, et que nous avions appelée poétiquement shared.key.

Cette mesure présente quelques avantages, surtout s'il n'est pas possible de spécifier les adresses IP de chaque bout (les vraies, pas celles qui sont dans le tunnel). Nous avons vu que le client doit connaitre l'adresse IP du serveur, mais dans notre configuration le serveur ne connait pas celle du client et peut difficilement la connaitre si le client dispose d'une adresse IP dynamique, ce qui est souvent le cas.

La documentation dit :

The tls-auth directive adds an additional HMAC signature to all SSL/TLS handshake packets for integrity verification. Any UDP packet not bearing the correct HMAC signature can be dropped without further processing. The tls-auth HMAC signature provides an additional level of security above and beyond that provided by SSL/TLS. It can protect against:

- **DoS attacks or port flooding on the OpenVPN UDP port.**
- **Port scanning to determine which server UDP ports are in a listening state.**
- **Buffer overflow vulnerabilities in the SSL/TLS implementation.**
- **SSL/TLS handshake initiations from unauthorized machines (while such handshakes would ultimately fail to authenticate, tls-auth can cut them off at a much earlier point).**

Ça fait envie…

La méthode d'utilisation est assez simple :

3-4-3-5-1 - Sur aaron (serveur)

```
tls-auth <chemin_vers_shared.key> 0
```

3-4-3-5-2 - Sur betelgeuse (client)

```
tls-auth <chemin_vers_shared.key> 1
```

3-4-4 - Configuration finale

Dans un cas simple d'un seul tunnel par hôte, nous n'avons rien à modifier dans /etc/default/openvpn. Nous avons juste à créer un fichier de configuration pour chacune des extrémités, que nous appellerons par exemple vpn.conf et à le mettre dans /etc/openvpn.

Nous allons créer un répertoire pour y ranger tous les ustensiles de sécurité (certificats, clés…), par exemple /etc/openvpncerts, y placer pour chaque extrémité :

- le certificat de la CA ;
- le certificat de l'hôte ;
- la clé privée de l'hôte, dont nous prendrons soin de ne la rendre lisible que par root ;
- le secret partagé (clé symétrique) lisible uniquement par root elle aussi.

Voici la version finale des fichiers de configuration.

3-4-4-1 - Pour aaron

```
mode p2p
port 8147
dev tun1
user nobody
group nogroup
persist-key
persist-tun
ifconfig 192.168.25.1 192.168.25.2
tls-server
dh /etc/openvpncerts/dh1024.pem
ca /etc/openvpncerts/bts.eme-cacert.pem
cert /etc/openvpncerts/aaron.bts.eme.pem
key /etc/openvpncerts/aaron.bts.eme-key.pem
tls-auth /etc/openvpncerts/shared.key 0
reneg-sec 900
comp-lzo
verb 1
route 192.168.0.0 255.255.255.0 192.168.25.2
```

3-4-4-2 - Pour cyclope

```
mode p2p
remote 82.127.57.95
port 8147
dev tun1
user nobody
group nogroup
persist-key
persist-tun
ifconfig 192.168.25.2 192.168.25.1
tls-client
ca /etc/openvpncerts/bts.eme-cacert.pem
cert /etc/openvpncerts/cyclope.maison.mrs.pem
key /etc/openvpncerts/cyclope.maison.mrs-key.pem
tls-auth /etc/openvpncerts/shared.key 1
reneg-sec 900
comp-lzo
verb 1
route 192.168.10.0 255.255.255.0 192.168.25.1
```

Cette configuration devrait donner satisfaction dans bien des cas.

3-4-5 - Conclusion

Nous sommes très loin d'avoir vu tout ce qu'il est possible de faire avec OpenVPN. Sa documentation n'est pas toujours très claire, mais elle vous en apprendra sans doute encore beaucoup plus sur ses possibilités.

La solution vue ici permettra de relier simplement deux réseaux IP privés distants à travers l'internet, avec un niveau de sécurité convenable.

4 - Remerciements Developpez

Vous pouvez retrouver l'article original ici : **L'Internet Rapide et Permanent**. Christian Caleca a aimablement autorisé l'équipe « **Réseaux** » de **Developpez.com** à reprendre son article. Retrouvez tous les articles de Christian Caleca **sur cette page**.

Nos remerciements à **ClaudeLeloup** pour sa relecture orthographique.

N'hésitez pas à commenter cet article !

1 : **Asynchronous Transfer Mode** : TTA en français (technologie temporelle asynchrone). Technologie de réseau à haut débit (centaines de Mbit/s, jusqu'à 2.5 Gbit/s) très sérieusement normalisée et présentée comme une solution d'avenir. Les données sont transmises sous forme de paquets de taille fixe (53 octets de long), appelés cellule. Originellement conçu pour la voix et les WAN, l'ATM est en train de passer aux LAN. Cette technologie semble prendre l'ascendant en ce moment sur ses concurrentes. Le principal problème étant la rapidité de commutation, qui doit être élevée vu la taille des cellules. Voir aussi « frame relay ». En plus, c'est Made in France, mais personne ne le sait.
2 : **MultiProtocol Label Switching** : technique conçue par **l'IETF** pour faire remonter des informations de niveau 2 OSI, comme la bande passante ou la latence d'un lien, dans la couche 3 (e.g. IP). Cela permet de gérer un peu mieux les ressources disponibles au sein d'un réseau.
3 : **Service Level Agreement** : Accord entre un client et un fournisseur sur le niveau de qualité de service offert par ce dernier. Le SLA est souvent suivi d'un SLM : Service Level Management. Gestion de la qualité de service, lors de laquelle on s'assure que le fournisseur tient bien ses promesses d'un point de vue qualitatif.
4 : **Keyed-hash message authentication code** : code d'authentification d'une empreinte cryptographique de message avec clé.