

Tunnel IPSec entre 2 routeurs

On entend souvent qu'il est difficile de faire du VPN IPSec entre 2 routeurs. Bon, c'est en partie vrai mais pas tant que ça.

Voici un exemple concret d'une topologie VPN fonctionnel.

N'oubliez pas de faire attention à la sécurité si vous souhaitez vous en inspirer.

Les routeurs Maxime et Jean-Clément vont être configuré pour faire du VPN entre eux, le routeur Stéphane simule un FAI.

Configuration des interfaces

R-Maxime	R-Jean-Clément	R-Stéphane
<pre>hostname Maxime interface g0/0 ip add 70.0.0.1 255.255.255.252 no shut interface g0/1 ip add 192.168.6.254 255.255.255.0 no shut exit</pre>	<pre>hostname JC interface g0/0 ip add 60.0.0.2 255.255.255.252 no shut interface g0/1 ip add 192.168.5.254 255.255.255.0 no shut exit</pre>	<pre>hostname Stephane interface fa0/0 ip address 60.0.0.1 255.255.255.252 no shut interface fa0/1 ip address 70.0.0.2 255.255.255.252 no shut</pre>

Configuration des routes

Une route par défaut pour les routeurs Maxime et Jean-Clément et 2 routes pour le routeur Stéphane

R-Maxime	R-Jean-Clément	R-Stéphane
<pre>ip route 0.0.0.0 0.0.0.0 g0/0</pre>	<pre>ip route 0.0.0.0 0.0.0.0 g0/0</pre>	<pre>ip route 192.168.5.0 255.255.255.0 fa0/0 ip route 192.168.6.0 255.255.255.0 fa0/1</pre>

Configuration VPN

R-Maxime

```
crypto isakmp policy 10
hash md5
authentication pre-share
group 2
lifetime 7200
crypto isakmp key schtroumph address 60.0.0.2 255.255.255.252

crypto ipsec transform-set schtroumph esp-aes esp-sha384-hmac
exit
access-list 101 permit ip 192.168.6.0 0.0.0.255 192.168.5.0 0.0.0.255
crypto map babar 12 ipsec-isakmp
set peer 60.0.0.2
set transform-set schtroumph
match address 101
exit
interface g0/0
crypto map babar
exit
```

R-Jean-Clément

```
crypto isakmp policy 10
hash md5
authentication pre-share
group 2
```

```

lifetime 7200
crypto isakmp key schtroumph address 70.0.0.1 255.255.255.252

crypto ipsec transform-set schtroumph esp-aes esp-sha384-hmac
exit
access-list 101 permit ip 192.168.5.0 0.0.0.255 192.168.6.0 0.0.0.255
crypto map babar 12 ipsec-isakmp
set peer 70.0.0.1
set transform-set schtroumph
match address 101
exit
interface g0/0
crypto map babar
exit

```

Il faut peut être quelques explications.

Configuration du ISAKMP (IKE)

- **crypto isakmp policy X** permet d'initier une règle de connexion avec un autre routeur. Le X peut être ce que vous voulez comme nombre.
- Ensuite, on configure le type de **hash** (faite ? après **hash** pour connaître les options). Ici ce sera en md5
- **authentication pre-share** permet d'indiquer l'utilisation d'un mot de passe partagé entre les 2 routeur pour l'initialisation de la connexion.
- **group 2** C'est le type de groupe pour Diffie-Hellman.

Les groupes Diffie-Hellman déterminent la force de la clé utilisée dans le processus d'échange de clés. Les groupes portant un numéro supérieur sont plus sûrs, mais il faut plus de temps pour créer la clé.

- Groupe Diffie-Hellman 1 : groupe 768 bits
- Groupe Diffie-Hellman 2 : groupe 1024 bits
- Groupe Diffie-Hellman 5 : groupe 1536 bits
- Groupe Diffie-Hellman 14 : groupe 2 048 bits
- Groupe Diffie-Hellman 15 : groupe 3 072 bits
- Groupe Diffie-Hellman 19 : groupe de courbe elliptique 256 bits
- Groupe Diffie-Hellman 20 : groupe de courbe elliptique 384 bits

Les deux pairs d'un échange VPN doivent utiliser le même groupe, qui est négocié pendant la phase 1 du processus de négociation IPsec. Lorsque vous définissez un tunnel BOVPN manuel, vous spécifiez le groupe Diffie-Hellman pendant la phase de création d'une connexion IPsec. Cette phase désigne le stade où deux pairs créent un canal sécurisé et authentifié pour communiquer.

Attention à votre débit, si c'est en local (si si, c'est faisable dans certains cas), choisissez ce que vous voulez, si c'est distant et faible en débit, attention à la

taille de la clef !

- `lifetime 7200` Durée de vie de la clé de session
- `crypto isakmp key schtroumph address 70.0.0.1` C'est **LA** commande qui définit le mot de passe et l'adresse **PUBLIC** du routeur destinataire.

Configuration et Application de l'IPSec

- `access-list 101 permit ip 192.168.6.0 0.0.0.255 192.168.5.0 0.0.0.255` Création d'une ACL permettant au réseau de Maxime d'atteindre le réseau LAN de Jean-Clément
- `crypto ipsec transform-set schtroumph esp-aes esp-sha384-hmac` Création d'une transformation IPSec et utilisation du mot de passe défini avant et de la méthode de chiffrement. Il y a plusieurs choix pour la méthode de chiffrement et son option. Pensez à utiliser le ?
- `crypto map babar X ipsec-isakmp`
`set peer 70.0.0.1`
`set transform-set schtroumph`
`match address 101` Ces commandes permettent la création de la Crypto Map (et son nom babar) et de définir le destinataire de ce VPN, le mot de passe d'initialisation de connexion et l'ACL à utiliser.
- `interface g0/0`
`crypto map babar` Maintenant, on applique la Crypto Map (via son nom) à l'interface de sortie WAN du routeur.

Il est possible d'avoir plusieurs map à appliquer en fonction du nombre de site que vous souhaitez interconnecter.

La condition de fonctionnement est l'utilisation des mêmes options et mots de passe sur le routeur distant.

Et normalement, ça ping :)

Vous voyez, c'est pas trop difficile.

Revision #3

Created 2024-03-25 23:01:03 UTC by Nicolas

Updated 2025-02-04 23:20:55 UTC by Nicolas