Configuration de strongswan ipsec avec un routeur cisco

###### configuration de base ###############

I-configuration cisco

1-Gateway parameters (Live)

VPN gateway device : Cisco ISR 3845

VPN Gateway device IP (or public ip) :41.191.70.9

Encryption Domain/ Network/ Host (or subnetip) :10.177.64.58 and 10.177.64.131

Local/remote TCP Ports : HTTPS (443)

2 -Tunnel Properties

- Phase 1:

Exchange Mode:Main

Encryption Schema : ikev1

Authentication Method :PRESHARED ( via sms ou appel)

Encryption : AES-256

Hash : SHA-1

Diffie-Hellman Group :5

Lifetime (Seconds) :36000

- Phase 2:

Encryption : AES-256

Hash : SHA-1

Perfect Forward Secrecy (or pfs): YES

Diffie-Hellman Group :5

Lifetime (Seconds) :24000

II- ubuntu 20 configuration

public ip : 160.154.66.19

subnet ip : 192.168.2.110 and 192.168.2.121

###### fin de la configuration de base ################

installation et configuration de strongswan

strongSwan is an open-source, cross-platform, full-featured and widely-used IPsec-based VPN (Virtual Private Network) implementation that runs on Linux, FreeBSD, OS X, Windows, Android, and iOS. It is primarily a keying daemon that supports the Internet Key Exchange protocols (IKEv1 and IKEv2) to establish security associations (SA) between two peers.

This article describes how to set up a site-to-site IPSec VPN gateways using strongSwan on Ubuntu and Debian servers. By site-to-site we mean each security gateway has a sub-net behind it. Besides, the peers will authenticate each other using a pre-shared key (PSK).

### **Step 1: Enabling Kernel Packet Forwarding**

1. First, you need to configure the kernel to enable packet forwarding by adding the appropriate system variables in /etc/sysctl.conf configuration file on both security gateways.

**#- sudo nano /etc/sysctl.com**

Look for the following lines and uncomment them and set their values as shown (read comments in the file for more information).

net.ipv4.ip\_forward = 1

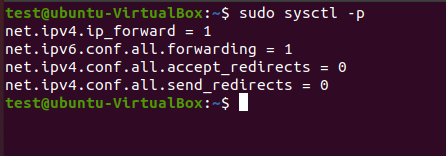
net.ipv6.conf.all.forwarding = 1

net.ipv4.conf.all.accept\_redirects = 0

net.ipv4.conf.all.send\_redirects = 0

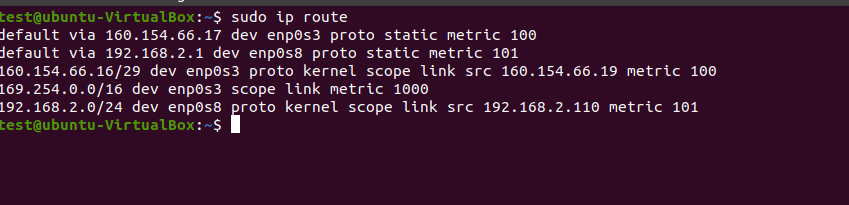
2. Next, load the new settings by running the following command.

#- sudo sysctl -p



3. If you have a UFW firewall service enabled, you need to add the following rules to the /etc/ufw/before.rules configuration file just before the filter rules in either security gate

#-sudo ip route pour voir les routes au niveau de mes adresses



nb : ici on va utiliser notre carte qui se trouve au niveau du dev ( c’est notre passerelle de l’ip public de ubuntu que nous avons communiquer )

Donc on va utiliser la carte **enp0s3**

#- **sudo nano /etc/ufw/before.rules**

avant la ligne ligne **\*règle** ajouter:

**\*nat**

**-A POSTROUTING -s 10.177.64.131/32 -o enp0s3 -m policy --pol ipsec --dir out -j ACCEPT**

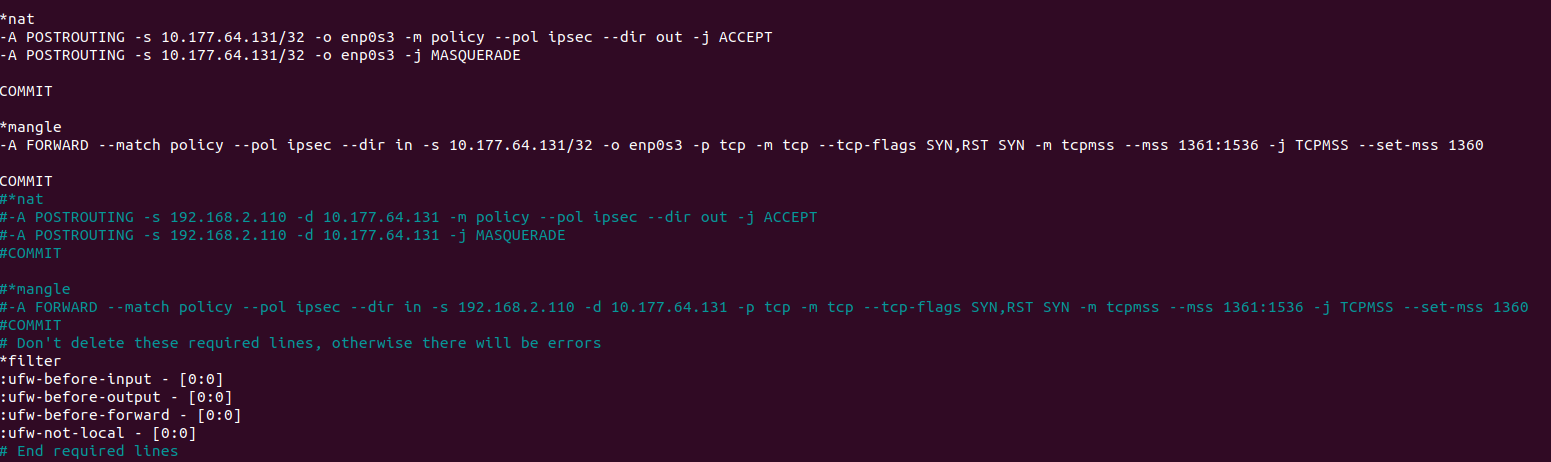
**-A POSTROUTING -s 10.177.64.131/32 -o enp0s3 -j MASQUERADE**

**COMMIT**

**\*mangle**

**-A FORWARD --match policy --pol ipsec --dir in -s 10.177.64.131/32 -o enp0s3 -p tcp -m tcp --tcp-flags SYN,RST SYN -m tcpmss --mss 1361:1536 -j TCPMSS --set-mss 1360**

**COMMIT**

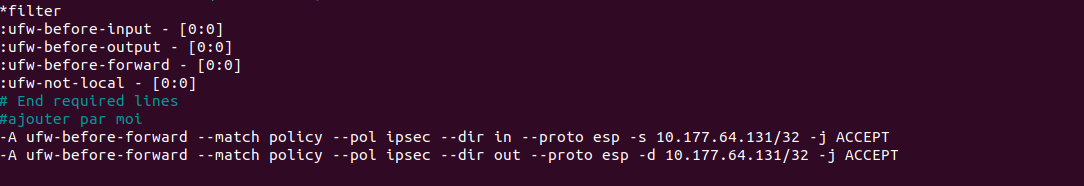


nb : n’oubliez pas de remplacer enps03 par le nom de votre carte reseau

Après la ligne des \*règles , ajouter cette ligne :

**-A ufw-before-forward --match policy --pol ipsec --dir in --proto esp -s 10.177.64.131/32 -j ACCEPT**

**-A ufw-before-forward --match policy --pol ipsec --dir out --proto esp -d 10.177.64.131/32 -j ACCEPT**

****

**4.** Once firewall rules have been added, then apply the new changes by restarting **UFW** as shown.

# - **sudo ufw disable**

# - **sudo ufw enable**

### **Step 2: Installing strongSwan in Debian and Ubuntu**

**5.** Update your package cache on both security gateways and install the **strongswan** package using the [APT package manager](https://www.tecmint.com/apt-advanced-package-command-examples-in-ubuntu/).

# - sudo apt update

# - sudo apt install strongswan

**6.** Once the installation is complete, the installer script will start the **strongswan** service and enable it to automatically start at system boot. You can check its status and whether it is enabled using the following command.

#~ **sudo systemctl status strongswan.service**

#~ **sudo systemctl is-enabled strongswan.service**

### **Step 3: Configuring Security Gateways**

7. Next, you need to configure the security gateways using the **/etc/ipsec.conf** configuration file.

**#~ sudo cp /etc/ipsec.conf /etc/ipsec.conf.orig**

**#~sudo nano /etc/ipsec.conf**

**config setup**

**charondebug="all"**

**uniqueids=yes**

**strictcrlpolicy=no**

**conn cerco-to-moov**

**authby=secret**

**left=%defaultroute**

**leftid=160.154.66.19**

**leftsubnet=192.168.2.110/32**

**right=41.191.70.9**

**rightid=41.191.70.9**

**rightsubnet=10.177.64.131/32**

**ike=aes256-sha1-modp1536!**

**esp=aes256-sha1-modp1536**

**keyingtries=%forever**

**leftauth=psk**

**rightauth=psk**

**keyexchange=ikev1**

**ikelifetime=36000s**

**lifetime=24000s**

**dpddelay=60s**

**dpdtimeout=120s**

**dpdaction=restart**

**auto=add**

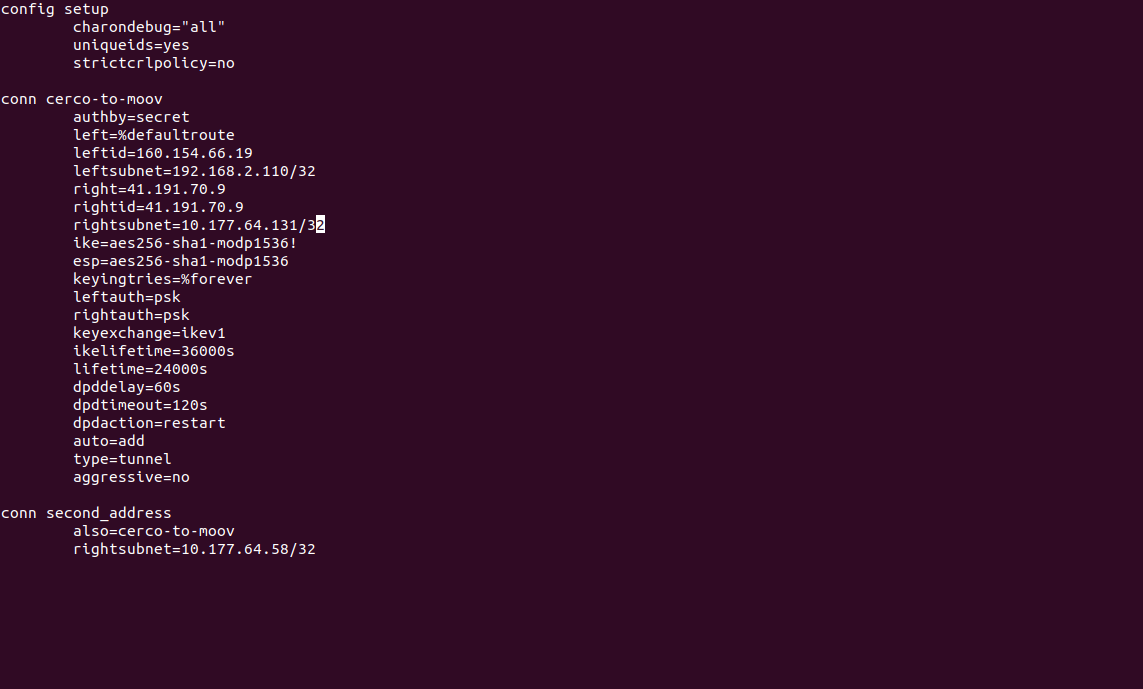
**type=tunnel**

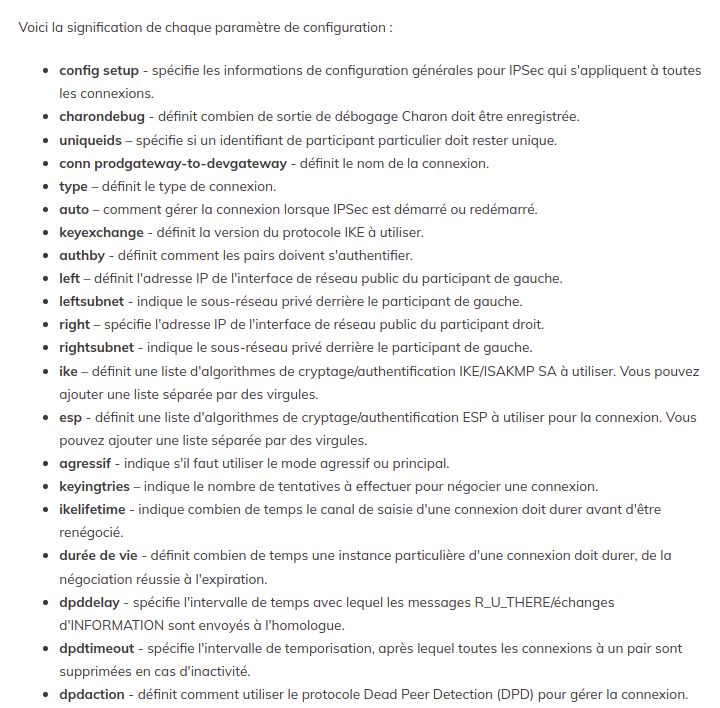
**aggressive=no**

**conn second\_address**

**also=cerco-to-moov**

**rightsubnet=10.177.64.58/32**

****

****

**nb : pour plus d’info sur la commande ipsec : #~ man ipsec.conf**

### 

### 

### 

### **Étape 4 : Configuration de PSK pour l'authentification d'égal à égal**

Ajoutez le **PSK** générer et qui vous a été envoyé dans le fichier **/etc/ipsec.secrets** sur les deux passerelles.

**#~sudo nano /etc/ipsec.secrets**

**structure :**

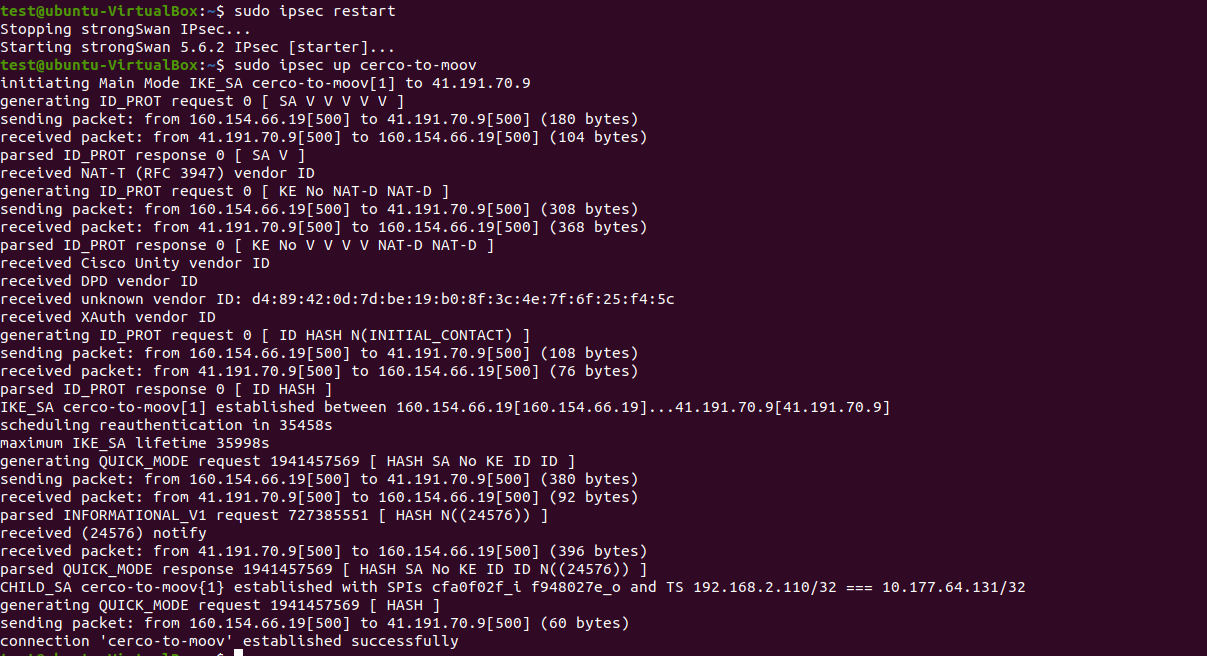
**ubuntu\_public cisco\_public : PSK “key”**

****

Redémarrez le programme IPSec et vérifiez son état pour afficher les connexions.

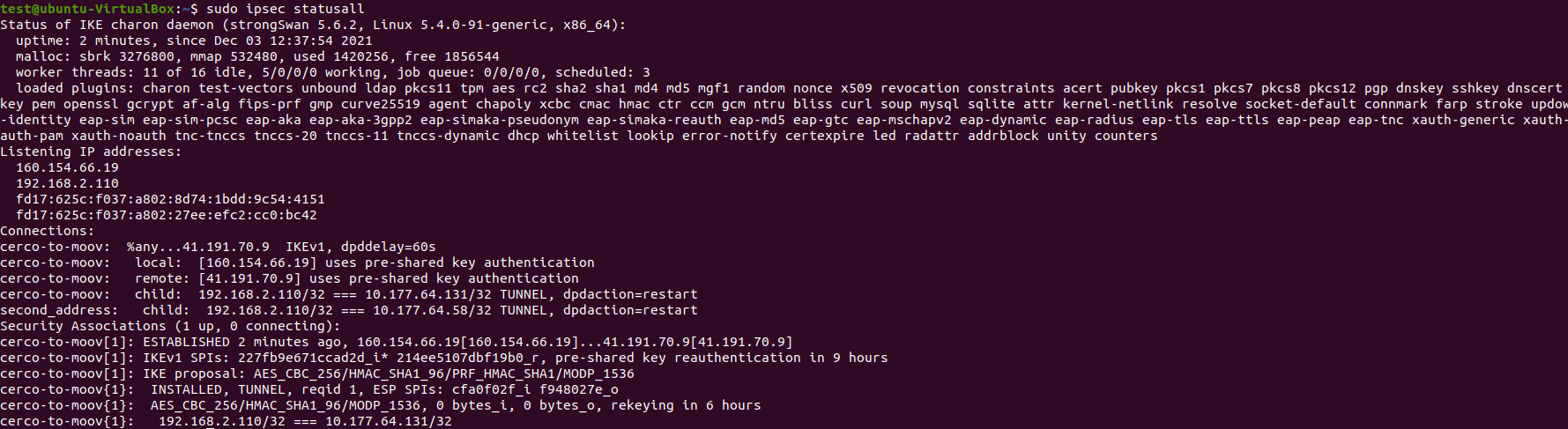
**#~ sudo ipsec restart**

**#~sudo ipsec up ‘ ajouter le nom de la connection configurer dans ipsec.conf’**

****

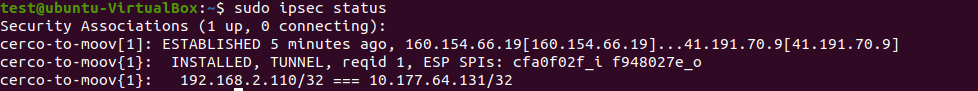
La connection à bien été établie

#~ **sudo ipsec statusall (vérifie le statut de toute vos connections up )**

****

**Nb : dans SA\_CHILD vous voyez que les deux addresse privée sont connectées**

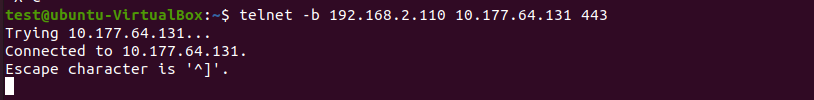
#~ **sudo ipsec status**

****

**Vérifions que les sous-réseaux communiquent :**

**#~ telnet -b 192.168.2.110 10.177.64.131 443**

**-b permet de spécifier l'adresse source**

****

**liens utile :** [**https://www.tecmint.com/setup-ipsec-vpn-with-strongswan-on-debian-ubuntu/**](https://www.tecmint.com/setup-ipsec-vpn-with-strongswan-on-debian-ubuntu/)

[**https://docs.netgate.com/pfsense/en/latest/troubleshooting/ipsec.html**](https://docs.netgate.com/pfsense/en/latest/troubleshooting/ipsec.html)