# Site-to-Site VPN configuration-Debian

-Setup

-PSK: Skill39

-Debian

-Private network: 192.168.100.1/24

-Public network: 10.10.10.1/24

-GRE subnet: 10.20.20.1/24

-Windows

-Private network: 192.168.200.1/24

-Public network: 10.10.10.2/24

GRE subnet: 10.20.20.2/24

-Enable packet forwarding by editing the /etc/sysctl.conf file. Look for the following lines and uncomment them

net.ipv4.ip\_forward = 1

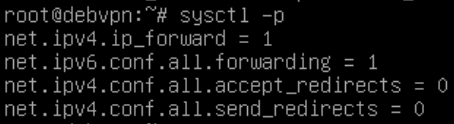
net.ipv6.conf.all.forwarding = 1

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

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

-Load the new settings

sysctl -p



-Load the ip\_gre modul

modprobe ip\_gre

-Create the GRE tunnel interface

ip tunnel add tun0 mode gre remote 10.10.10.2 local 10.10.10.1 ttl 255

ip link set tun0 up

ip addr add 10.20.20.1/24 dev tun0

-To make it persistent after restart edit the /etc/network/interfaces file with the following

auto tun0

iface tun0 inet tunnel

address 10.20.20.1/24

mode gre

endpoint 10.10.10.2

local 10.10.10.1

ttl 255

remote 10.10.10.2

-Install Strongswan

apt install strongswan

-Edit the /etc/ipsec.conf file

config setup

charondebug = ”all”

uniqueids = yes

conn devgateway-to-prodgateway

type = tunnel

auto = add

auto = start

keyexchange = ikev2

authby = secret

left = 10.20.20.1

leftsubnet = 192.168.100.1/24

right = 10.20.20.2

rightsubnet = 192.168.200.1/24

rightsourceip = 192.168.200.1/24

ike = aes128-sha1-modp1024!

esp = aes128-sha1!

aggressive = no

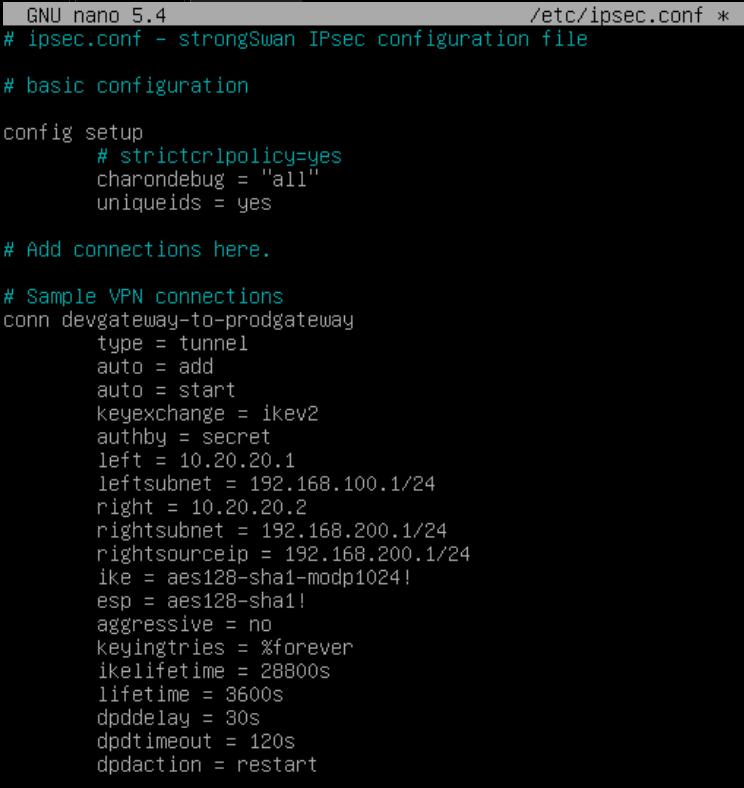
keyingtries = %forever

ikelifetime = 28800s

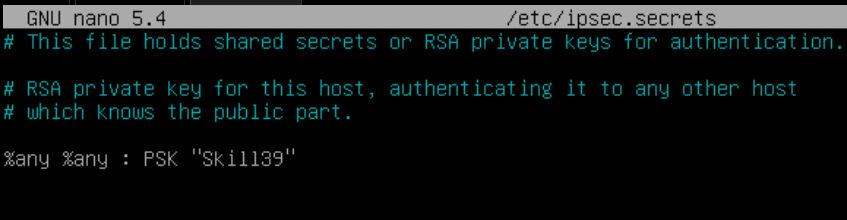
lifetime = 3600s

dpddelay = 30s

dpdtimeout = 120s

dpdaction = restart

-Edit the /etc/ipsec.secrets file

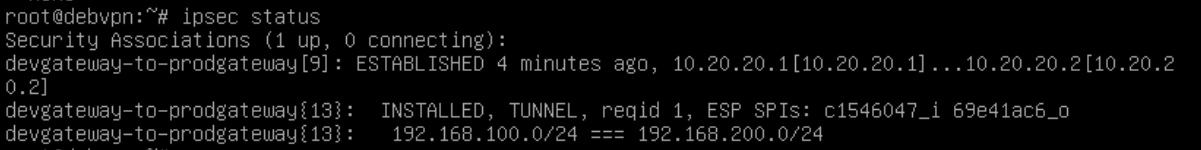
%any %any : PSK „Skill39”

-Restart Strongswan

systemctl restart strongswan-starter

-You can check the status of the VPN connection with:

ipsec status

-If everything works you should see a similar output

-Also you can reset the connection with

ipsec restart