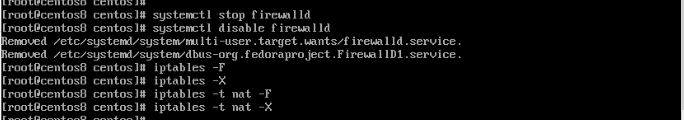
# **Report on VPN (Task 4)**

**Name:** Aravindh JAWAHAR

StrongSwan Ipsec VPN

This lab will be composed of 4 CentOS 8 VM with 1GB of ram and 2vCPUS each. They will need to in same subnet and be able to reach each other.

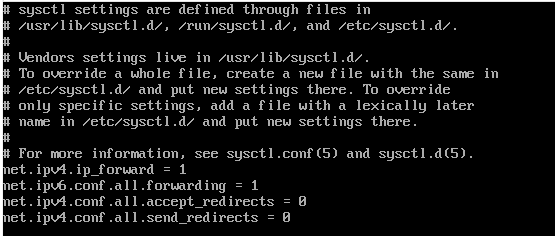
1. Firewall for the VM(1,2) has been disabled and we delete the IP tables by flushing it if any values



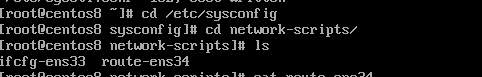
SELinux has been disabled in the VM 1 and 2

1. Enabling routing on both VM’s(VM-1 and VM-2) as follows

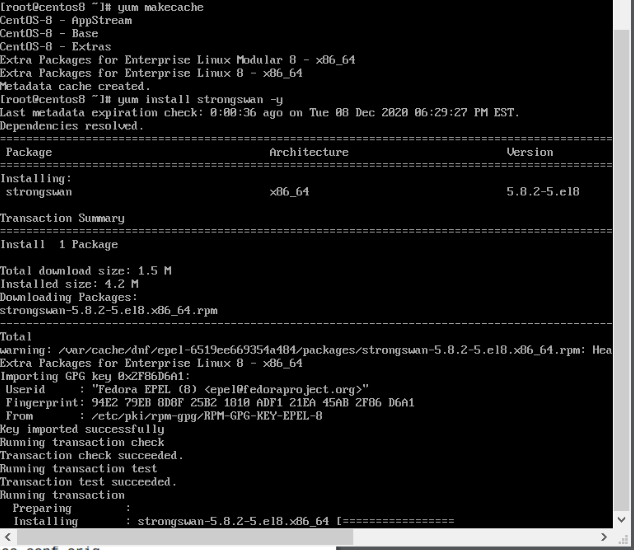
Enabling the kernel IP forwarding functionality in /etc/sysctl.conf



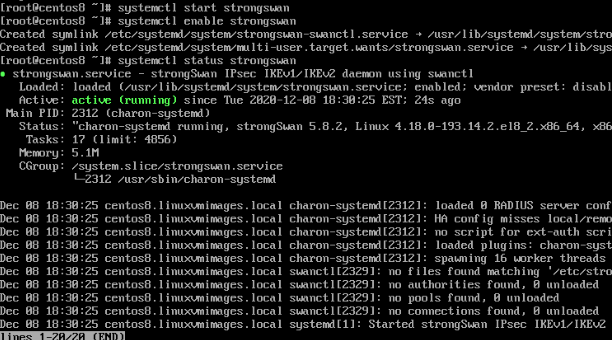
1. Adding routes to the new remote local network by enabling the scripts in /etc/sysconfig/network-scripts/route-ens34



1. Installing **strongswan** on VM-1 and VM-2



1. Enabling the service (strongswan) on VM-1 and VM-2



1. On both VMS we copy the contents of ipsec.conf to ipsec.conf.orig
2. Configure the connection profiles on each security gateways for each site using the **/etc/strongswan/ipsec.conf** strongswan configuration file

**Config setup** - the general configuration information for IPSec which applies to all connections

**charondebug** specifies the amount of charon debug output to be logged

**uniqueids** - participant ID

**conn gateway1-to-gateway2** - setting connection name

**type** - connection type

**auto** - handle connection when ipsec started or restarted

**keyexchange** - version of IKE protocol

**authby** -specifies how peers authenticate each other

**left** - left participant public IP

**leftsubnet** - private subnet of left

**right** - right participant public IP

**rightsubnet** - private subnet behind left

**ike** - declare list of IKE authentication algorithm

**esp** - specify list pf ESP algorithm for connection

**aggressive** - declares to use aggressive or main mode

**keyingtries** - defines attempts t negotiate a connection

**ikelifetime** - pecifies how long the keying channel of a connection should last before being renegotiated

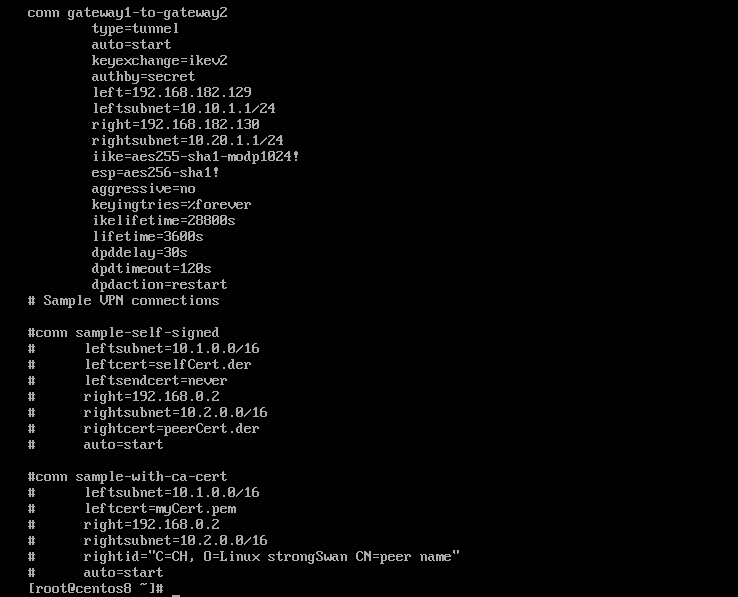
**lifetime** - length of instance of connection

**dpddelat** - declares the time interval of message exchanges sent to the peer

**dpdtimeout** - timeout interval incase the connections are deleted after inactivity

**dpdaction** - uses dead peer connection protocol to manage the connection

VM-1



1. VM-2

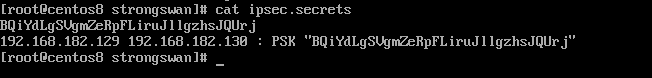


1. Pre-Shared Key (**PSK**) is a client **authentication** method that uses a string of 64 hexadecimal digits, or as a passphrase of 8 to 63 printable ASCII characters, to generate unique encryption keys for each wireless client.

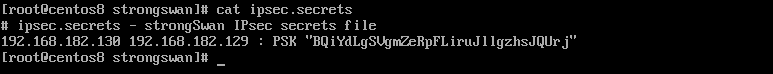
We generate the random key and copy it to /etc/strongswan/ipsec.secrets



On VM-1

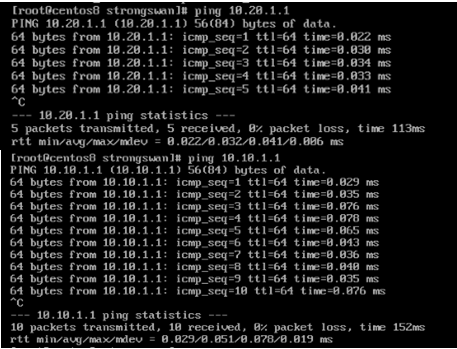


On VM-2

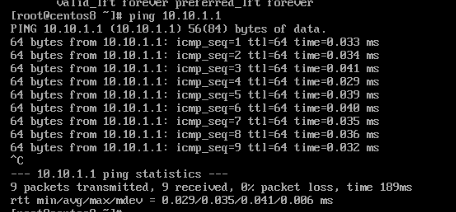
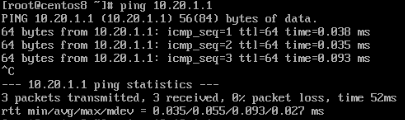


1. We restart the strongswan by rebooting the system and the service
2. Testing the network access via ping for both VM’s(1 and 2)

Ping to tunnel interface from VM-1

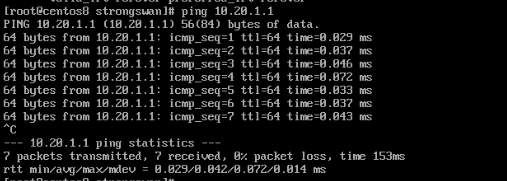


Ping to tunnel interface from VM-2

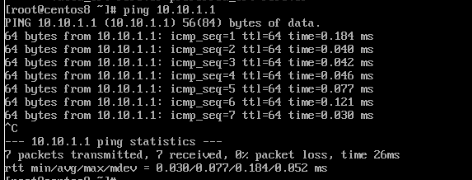


1. Ping to tunnel interface of VM-1 from VM-4 and to VM-2 tunnel interface from VM-3

From VM-3



From VM-4



1. IPsec, also known as the Internet Protocol Security or IP Security protocol, defines the architecture for security services for IP network traffic. It defines the cryptographic algorithms used to encrypt, decrypt, and authenticate packets, as well as the protocols needed for secure key exchange and key management.

It has mechanisms for IP security

1. Encapsulation security payload (ESP)

Method for encrypting the IP packets

1. Internet key exchange (IKE)

Used to manage cryptographic keys used by hosts for Ipsec

1. The IP Authentication Header (AH)

for digital signing the IP packets

Internet key exchange protocol (IEKV2) is defined to allow hosts to specify which services are incorporated in the packets in which algorithms are used to provide services and mechanisms for sharing the keys

IPsec protocol:

Defined for both version of IP’s ipv4 and ipv6

Working of Ipsec protocol:

* When the host recognizes packets should be transmitted using ipsec
* IKE phase 1, allows two hosts using ipsec to negotiate policy to authenticate themselves and initiate channel between hosts
* IKE Phase 2, which itself is conducted over the secure channel setup in IKE Phase 1. It requires the two hosts to negotiate and initiate the security association for the IPsec circuit carrying actual network data
* actual exchange of data across the newly created IPsec encrypted tunnel
* Termination of Ipsec tunnel when the communication is complete or during session time out. Then the hosts discard the keys over security association