**/etc/ipsec.conf file**

```
config setup
conn %default
    ikelifetime=120m                #IKE Lifetime
    keylife=70m                     #ESP Lifetime
    rekeymargin=5m
    keyingtries=1
    keyexchange=ikev1               #Ike version
    authby=secret                   #IPSec Authentication method. “secret” means we are authenticating using pre-shared key.
    mobike=no                       #Disable MOBIKE feature
    type=tunnel                     #IPSec mode. Specify tunnel mode.
#IKE encryption algorithm, hash algorithm and DH group
    ike=aes-sha1-modp1024
#ESP encryption algorithm, hash algorithm and DH group
    esp=aes-sha1-modp1024
#NetScaler provides a common parameter for specifying IKE and ESP hash algorithm, a common parameter for specifying IKE and ESP encryption algorithm, and a common parameter for specifying IKE and ESP DH group. Therefore, in this file, ike and esp paramters must be set to the same option for an IPsec connection between a StrongSwan appliance and a NetScaler appliance.
conn conn1
    left=203.0.113.200              # Local IPSec endpoint IP address (on StrongSwan appliance)
    leftsubnet=10.20.20.0/24        # StrongSwan side protected network
    right= 198.51.100.100           # Remote IPSec endpoint IP address (on the NetScaler appliance)
    rightsubnet=10.102.147.0/24     # NetScaler side protected network
    leftfirewall=yes                # Add exception to iptables in linux
    auto=add
```