# IPSec site to site

On Red Hat based Systems (CentOS, Fedora or RHEL):

# yum install openswan lsof (or liberswan)

Next, we modify the kernel parameters to allow IP forwarding and disable redirects permanently.

# vim /etc/sysctl.conf

net.ipv4.ip\_forward = 1

Reload /etc/sysctl.conf:

# sysctl -p

We allow necessary ports in the firewall. Please make sure that the rules are not conflicting with existing firewall rules.

# iptables -A INPUT -p udp --dport 500 -j ACCEPT

# iptables -A INPUT -p tcp --dport 4500 -j ACCEPT

# iptables -A INPUT -p udp --dport 4500 -j ACCEPT

Start the IPsec service and enable the service to be started:

systemctl enable ipsec

**for firewalld** : Configure the firewall to allow 500 and 4500/UDP ports for the IKE, ESP, and AH protocols by adding the IPsec service:

# firewall-cmd --add-service="ipsec"

# firewall-cmd --runtime-to-permanent

Finally, we create firewall rules for NAT.

# iptables -t nat -A POSTROUTING -s site-A-private-subnet -d site-B-private-subnet -j SNAT --to site-A-Public-IP

## Preparing Configuration Files

The first configuration file that we will work with is ipsec.conf. Regardless of which server you are configuring, always consider your site as **left** and remote site as **right**. The following configuration is done in siteA's VPN server.

# vim /etc/ipsec.conf

## connection definition in Red Hat ##

conn demo-connection-redhat

authby=secret

auto=start

ike=3des-md5

## phase 1 ##

keyexchange=ike

## phase 2 ##

phase2=esp

phase2alg=3des-md5

compress=no

pfs=yes

type=tunnel

left=<siteA-public-IP>

leftsourceip=<siteA-public-IP>

leftsubnet=<siteA-private-subnet>/netmask

## for direct routing ##

leftsubnet=<siteA-public-IP>/32

leftnexthop=%defaultroute

right=<siteB-public-IP>

rightsubnet=<siteB-private-subnet>/netmask

## connection definition in Debian ##

conn demo-connection-debian

authby=secret

auto=start

## phase 1 ##

keyexchange=ike

## phase 2 ##

esp=3des-md5

pfs=yes

type=tunnel

left=<siteA-public-IP>

leftsourceip=<siteA-public-IP>

leftsubnet=<siteA-private-subnet>/netmask

## for direct routing ##

leftsubnet=<siteA-public-IP>/32

leftnexthop=%defaultroute

right=<siteB-public-IP>

rightsubnet=<siteB-private-subnet>/netmask

Authentication can be done in several different ways. This tutorial will cover the use of pre-shared key, which is added to the file /etc/ipsec.secrets.

# vim /etc/ipsec.secrets

siteA-public-IP siteB-public-IP: PSK "pre-shared-key"

## in case of multiple sites ##

siteA-public-IP siteC-public-IP: PSK "corresponding-pre-shared-key"

## Starting the Service and Troubleshooting

The server should now be ready to create a site-to-site VPN tunnel. If you are managing site-B as well, please make sure that you have configured the site-B's server with necessary parameters. For Red Hat based systems, please make sure that you add the service into startup using chkconfig command.

# systemctl restart ipsec

## Check tunnel status

we can check the status of the tunnel using the following useful commands.

# service ipsec status

# ipsec auto --status