

StrongSwan یک open-source, cross-platform VPN است که بر پایه IPsec کار میکند و در حوزه های وسیعی مورد استفاده قرار میگیرد که روی Linux و FreeBSD و OS X و Windows و Android و iOS اجرا می شود.

این VPN پروتکل IKE (Internet Key Exchange) و IKEv1 و IKEv2 را پشتیبانی می کند تا دو peer بتوانند بین هم یک security association (SA) برقرار کنند.

ما برای پروژه خود، یک IPsec VPN site-to-site راه اندازی کردیم. منظور از site-to-site این است که هر security gateway یک subnet در پشت خود دارد و علاوه بر آن هر peer برای authentication دیگری از یک pre-shared key (PSK) استفاده می کند.

1- در گام اول می بایست طوری kernel را پیکره بندی کنیم که packet forwarding فعال شود این کار را با اضافه کردن متغیر مناسب در فایل /etc/sysctl.conf انجام می دهیم.

```
$ sudo vim /etc/sysctl.conf
```

در فایل فوق، خطوط زیر را از حالت comment در می آوریم.

```
net.ipv4.ip_forward = 1

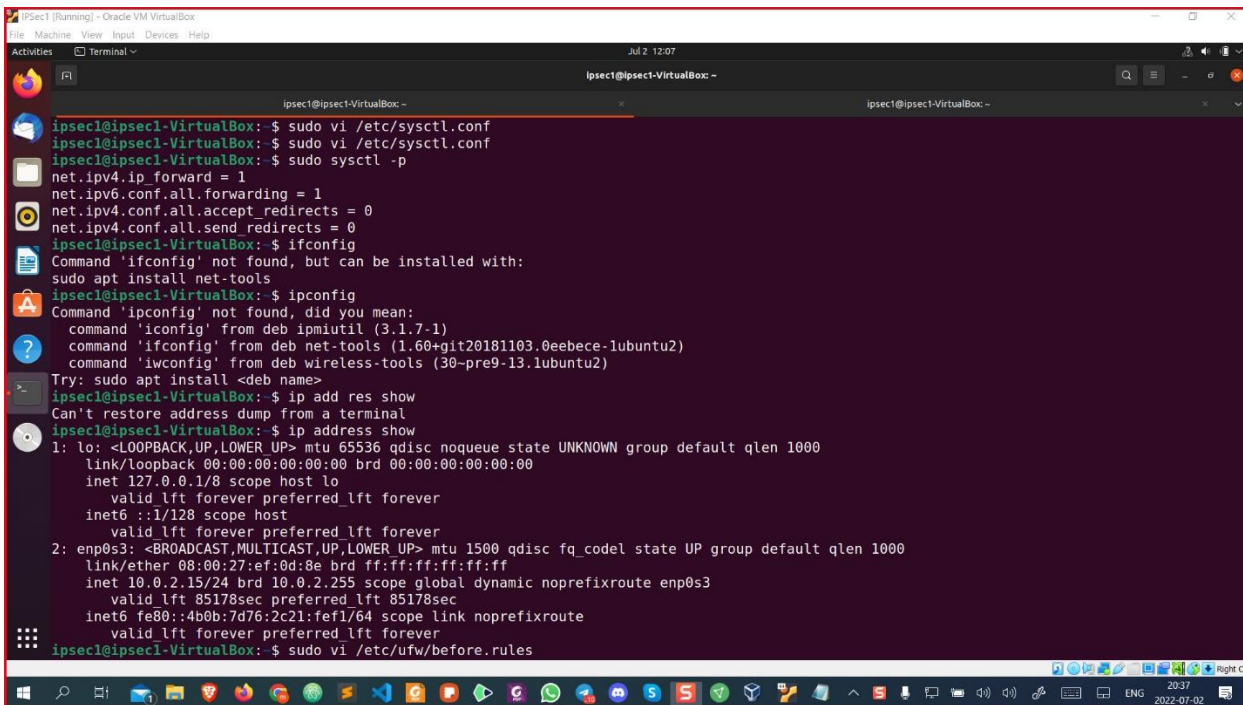
net.ipv6.conf.all.forwarding = 1

net.ipv4.conf.all.accept_redirects = 0

net.ipv4.conf.all.send_redirects = 0
```

2- بعد از آن، setting جدید را با استفاده از دستور زیر، load می کنیم.

```
$ sudo sysctl -p
```



```
ipsec1@ipsec1-VirtualBox: ~  
ipsec1@ipsec1-VirtualBox:~$ sudo vi /etc/sysctl.conf  
ipsec1@ipsec1-VirtualBox:~$ sudo vi /etc/sysctl.conf  
ipsec1@ipsec1-VirtualBox:~$ sudo sysctl -p  
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  
ipsec1@ipsec1-VirtualBox:~$ ifconfig  
Command 'ifconfig' not found, but can be installed with:  
sudo apt install net-tools  
ipsec1@ipsec1-VirtualBox:~$ ipconfig  
Command 'ipconfig' not found, did you mean:  
  command 'ifconfig' from deb ipmiutil (3.1.7-1)  
  command 'ifconfig' from deb net-tools (1.60+git20181103.0eebece-lubuntu2)  
  command 'iwconfig' from deb wireless-tools (30-pre9-13.lubuntu2)  
Try: sudo apt install <deb name>  
ipsec1@ipsec1-VirtualBox:~$ ip add res show  
Can't restore address dump from a terminal  
ipsec1@ipsec1-VirtualBox:~$ ip address show  
1: lo: <LOOPBACK,UP,LOWER UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000  
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00  
    inet 127.0.0.1/8 scope host lo  
        valid lft forever preferred_lft forever  
    inet6 ::1/128 scope host  
        valid lft forever preferred_lft forever  
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000  
    link/ether 08:00:27:ef:0d:8e brd ff:ff:ff:ff:ff:ff  
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic noprefixroute enp0s3  
        valid lft 85178sec preferred_lft 85178sec  
    inet6 fe80::4b0b:7d76:2c21:fe11/64 scope link noprefixroute  
        valid_lft forever preferred_lft forever  
ipsec1@ipsec1-VirtualBox:~$ sudo vi /etc/ufw/before.rules
```

3- در گام بعدی، UFW firewall را غیرفعال می‌کنیم.

```
$ sudo ufw disable
```

4- در گام بعدی، package cache خود را update کرده و پکیج strongswan را نصب می‌کنیم.

```
$ sudo apt update  
  
$ sudo apt install strongswan
```

```
IPSec1 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Terminal Jul 2 12:09
ipsec1@ipsec1-VirtualBox: ~
ipsec1@ipsec1-VirtualBox: ~
valid_lft 85178sec preferred_lft 85178sec
inet6 fe80::4b0b:7d76:2c21:fe1/64 scope link noprefixroute
valid_lft forever preferred_lft forever
ipsec1@ipsec1-VirtualBox: ~$ sudo vi /etc/ufw/before.rules
ipsec1@ipsec1-VirtualBox: ~$ sudo ufw disable
Firewall stopped and disabled on system startup
ipsec1@ipsec1-VirtualBox: ~$ sudo apt update
Hit:1 http://us.archive.ubuntu.com/ubuntu hirsute InRelease
Hit:2 http://us.archive.ubuntu.com/ubuntu hirsute-updates InRelease
Hit:3 http://security.ubuntu.com/ubuntu hirsute-security InRelease
Hit:4 http://us.archive.ubuntu.com/ubuntu hirsute-backports InRelease
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
281 packages can be upgraded. Run 'apt list --upgradable' to see them.
ipsec1@ipsec1-VirtualBox: ~$ sudo apt install strongswan
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  libcharon-extauth-plugins libstrongswan libstrongswan-standard-plugins strongswan-charon strongswan-libcharon strongswan-starter
Suggested packages:
  libstrongswan-extra-plugins libcharon-extra-plugins
The following NEW packages will be installed:
  libcharon-extauth-plugins libstrongswan libstrongswan-standard-plugins strongswan strongswan-charon strongswan-libcharon
  strongswan-starter
0 upgraded, 7 newly installed, 0 to remove and 281 not upgraded.
Need to get 882 kB of archives.
After this operation, 4,188 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://us.archive.ubuntu.com/ubuntu hirsute-updates/main amd64 libstrongswan amd64 5.9.1-lubuntu1.2 [360 kB]
Get:2 http://us.archive.ubuntu.com/ubuntu hirsute-updates/main amd64 strongswan-libcharon amd64 5.9.1-lubuntu1.2 [243 kB]
```

```
Activities Terminal Jul 2 12:11
ipsec2@ipsec2-VirtualBox: ~
ipsec2@ipsec2-VirtualBox: ~
valid_lft forever preferred_lft forever
ipsec2@ipsec2-VirtualBox: ~$ sudo ufw disable
[sudo] password for ipsec2:
Firewall stopped and disabled on system startup
ipsec2@ipsec2-VirtualBox: ~$ sudo apt update
Hit:1 http://us.archive.ubuntu.com/ubuntu hirsute InRelease
Hit:2 http://us.archive.ubuntu.com/ubuntu hirsute-updates InRelease
Hit:3 http://security.ubuntu.com/ubuntu hirsute-security InRelease
Hit:4 http://us.archive.ubuntu.com/ubuntu hirsute-backports InRelease
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
281 packages can be upgraded. Run 'apt list --upgradable' to see them.
ipsec2@ipsec2-VirtualBox: ~$ sudo apt install strongswan
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  libcharon-extauth-plugins libstrongswan libstrongswan-standard-plugins strongswan-charon strongswan-libcharon
  strongswan-starter
Suggested packages:
  libstrongswan-extra-plugins libcharon-extra-plugins
The following NEW packages will be installed:
  libcharon-extauth-plugins libstrongswan libstrongswan-standard-plugins strongswan strongswan-charon strongswan-libcharon
  strongswan-starter
0 upgraded, 7 newly installed, 0 to remove and 281 not upgraded.
Need to get 882 kB of archives.
After this operation, 4,188 kB of additional disk space will be used.
```

5- در گام بعدی سرویس strongswan فعال شده و توسط دستورات زیر، می‌توانیم حالت آنها را چک کنیم.

```
$ sudo systemctl status strongswan-starter

$ sudo systemctl is-enabled strongswan-starter
```

6- در گام بعدی، gateway ها را config می‌کنیم.
در طرف اول داریم:

```
$ sudo cp /etc/ipsec.conf /etc/ipsec.conf.orig  
  
$ sudo nano /etc/ipsec.conf
```

متن های زیر را در این فایل قرار می‌دهیم.

```
config setup  
  
    charondebug="all"  
  
    uniqueids=yes  
  
conn devgateway-to-prodgateway  
  
    type=tunnel  
  
    auto=start  
  
    keyexchange=ikev2  
  
    authby=secret  
  
    left=...  
  
    leftsubnet=...  
  
    right=...  
  
    rightsubnet=...
```

```
ike=aes256-sha1-modp1024!
```

```
esp=aes256-sha1!
```

```
aggressive=no
```

```
keyingtries=%forever
```

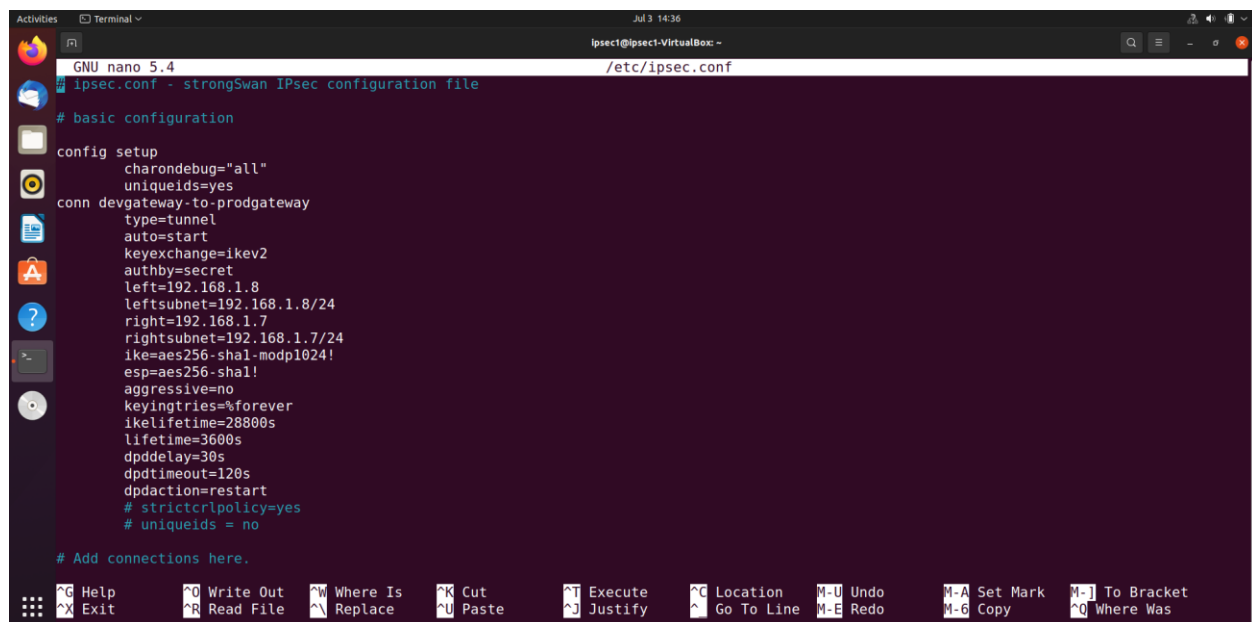
```
ikelifetime=28800s
```

```
lifetime=3600s
```

```
dpddelay=30s
```

```
dpdtimeout=120s
```

```
dpdaction=restart
```



The screenshot shows a terminal window titled "ipsec1@ipsec1-VirtualBox: ~" with the file "/etc/ipsec.conf" open in the "GNU nano 5.4" editor. The file is a strongSwan IPsec configuration file. The configuration includes a basic setup section with debugging, unique IDs, and a connection named "devgateway-to-prodgateway" configured as a tunnel. The connection settings include IP addresses, subnets, IKE and ESP proposals, aggressive mode, keyingtries, lifetimes, delays, timeouts, and actions. The configuration ends with a comment to add connections here. The terminal window also shows a sidebar with application icons and a bottom status bar with various keyboard shortcuts.

```
ipsec1@ipsec1-VirtualBox: ~  
/etc/ipsec.conf  
# basic configuration  
config setup  
    charondebug="all"  
    uniqueids=yes  
conn devgateway-to-prodgateway  
    type=tunnel  
    auto=start  
    keyexchange=ikev2  
    authby=secret  
    left=192.168.1.8  
    leftsubnet=192.168.1.8/24  
    right=192.168.1.7  
    rightsubnet=192.168.1.7/24  
    ike=aes256-sha1-modp1024!  
    esp=aes256-sha1!  
    aggressive=no  
    keyingtries=%forever  
    ikelifetime=28800s  
    lifetime=3600s  
    dpddelay=30s  
    dpdtimeout=120s  
    dpdaction=restart  
    # strictcrpolicy=yes  
    # uniqueids = no  
  
# Add connections here.
```

در طرف دوم داریم:

```
$ sudo cp /etc/ipsec.conf /etc/ipsec.conf.orig  
  
$ sudo nano /etc/ipsec.conf
```

در فایل در طرف دوم داریم:

```
config setup  
  
    charondebug="all"  
  
    uniqueids=yes  
  
conn prodgateway-to-devgateway  
  
    type=tunnel  
  
    auto=start  
  
    keyexchange=ikev2  
  
    authby=secret  
  
    left=...  
  
    leftsubnet=...  
  
    right=...  
  
    rightsubnet=...  
  
    ike=aes256-sha1-modp1024!
```

```
esp=aes256-sha1!
```

```
aggressive=no
```

```
keyingtries=%forever
```

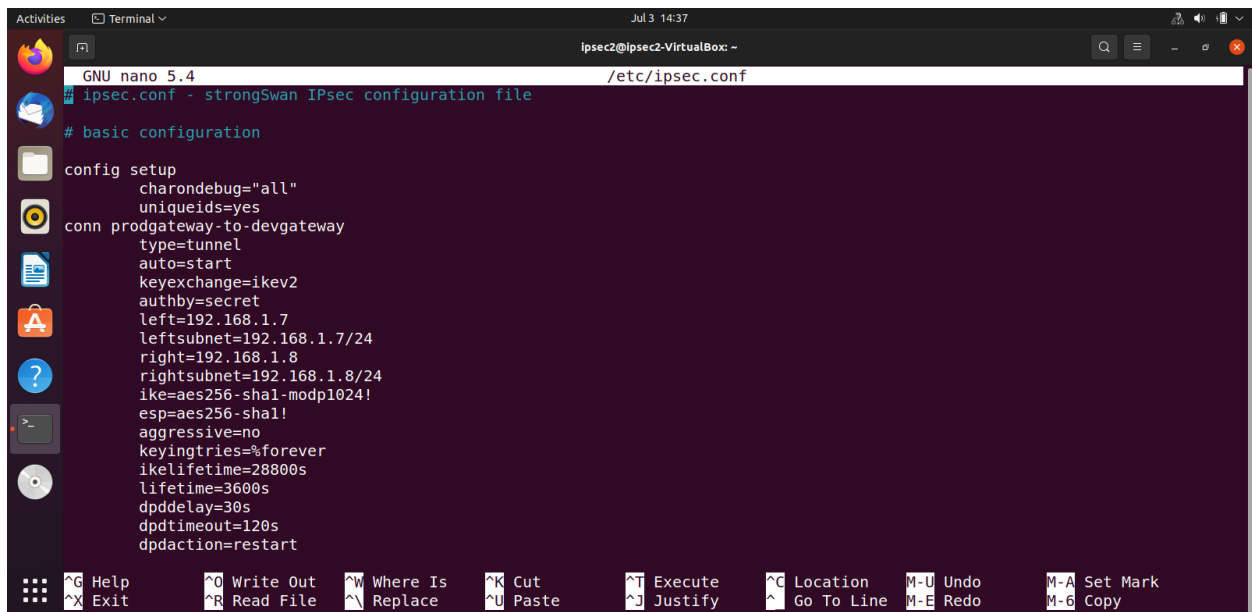
```
ikelifetime=28800s
```

```
lifetime=3600s
```

```
dpddelay=30s
```

```
dpdtimeout=120s
```

```
dpdaction=restart
```



```
GNU nano 5.4 /etc/ipsec.conf
# ipsec.conf - strongSwan IPsec configuration file

# basic configuration

config setup
    charondebug="all"
    uniqueids=yes

conn prodgateway-to-devgateway
    type=tunnel
    auto=start
    keyexchange=ikev2
    authby=secret
    left=192.168.1.7
    leftsubnet=192.168.1.7/24
    right=192.168.1.8
    rightsubnet=192.168.1.8/24
    ike=aes256-sha1-modp1024!
    esp=aes256-sha1!
    aggressive=no
    keyingtries=%forever
    ikelifetime=28800s
    lifetime=3600s
    dpddelay=30s
    dpdtimeout=120s
    dpdaction=restart
```

Activities Terminal Jul 3 14:37 ipsec2@ipsec2-VirtualBox: ~

Help Exit Write Out Read File Where Is Replace Cut Paste Execute Justify Location Go To Line Undo Redo Set Mark Copy

```
Activities Jul 3 14:41 ipsec2@ipsec2-VirtualBox -
# ipsec.conf - strongSwan IPsec configuration file

# basic configuration

config setup
    charondebug="all"
    uniqueids=yes

conn prodgateway-to-devgateway
    type=tunnel
    auto=start
    keyexchange=ikev2
    authby=secret
    left=192.168.1.7
    leftsubnet=192.168.1.7/24
    right=192.168.1.8
    rightsubnet=192.168.1.8/24
    ike=aes256-sha1-modp1024!
    esp=aes256-sha1!
    aggressive=no
    keyingtries=forever
    ikelifetime=28800s
    lifetime=3600s
    dpddelay=30s
    dpdtimeout=120s
    dpdaction=restart
    # strictcrpolicy=yes
    # uniqueids = no

# Add connections here.

# Sample VPN connections

#conn sample-self-signed
#    leftsubnet=10.1.0.0/16
#    leftcert=selfCert.der
```

با استفاده از دستور زیر می‌توانیم، به راهنمای IPsec دست پیدا کنیم.

```
IPSec1 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Jul 2 12:09 ipsec1@ipsec1-VirtualBox -

Setting up strongswan (5.9.1-lubuntu1.2) ...
Processing triggers for man-db (2.9.4-2) ...
ipsec1@ipsec1-VirtualBox: ~$ sudo systemctl status strongswan.service
Unit strongswan.service could not be found.
ipsec1@ipsec1-VirtualBox: ~$ sudo systemctl status strongswan
Unit strongswan.service could not be found.
ipsec1@ipsec1-VirtualBox: ~$ sudo systemctl status strongswan-starter
● strongswan-starter.service - strongSwan IPsec IKEv1/IKEv2 daemon using ipsec.conf
   Loaded: loaded (/lib/systemd/system/strongswan-starter.service; enabled; vendor preset: enabled)
   Active: active (running) since Sat 2022-07-02 11:20:43 EDT; 3min 55s ago
     Main PID: 2962 (starter)
        Tasks: 18 (limit: 4635)
         Memory: 2.5M
          CGroup: /system.slice/strongswan-starter.service
                  └─2962 /usr/lib/ipsec/starter --daemon charon --nofork
                     2971 /usr/lib/ipsec/charon

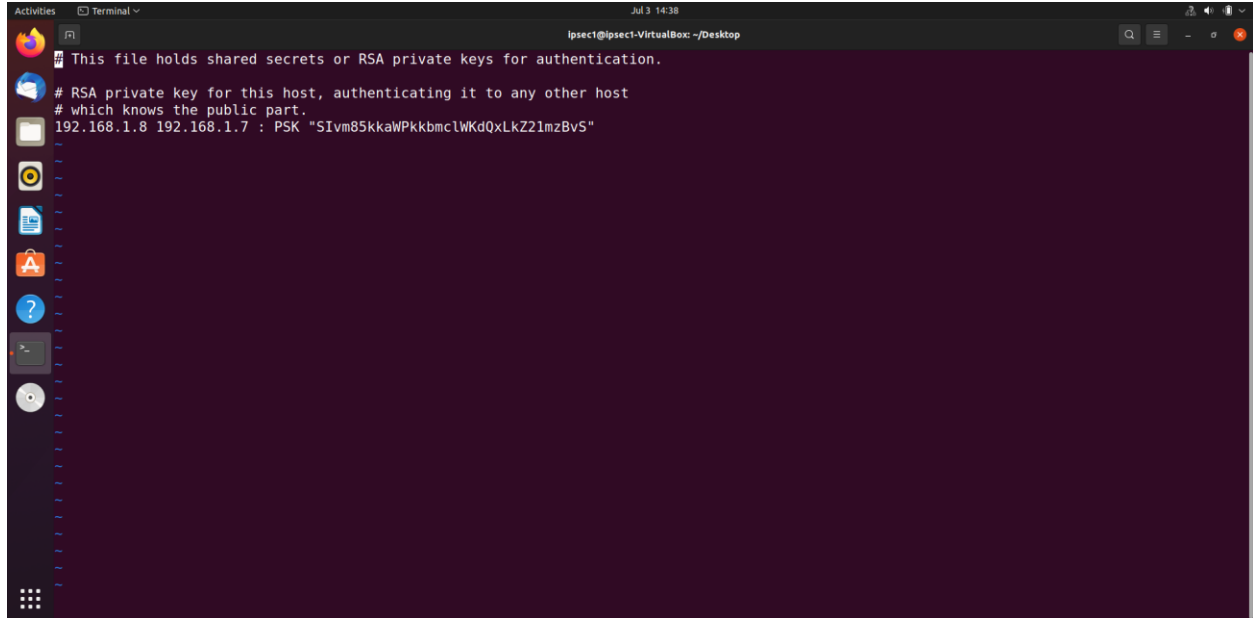
Jul 02 11:20:43 ipsec1-VirtualBox charon[2971]: 00[CFG] loading aa certificates from '/etc/ipsec.d/aacerts'
Jul 02 11:20:43 ipsec1-VirtualBox charon[2971]: 00[CFG] loading ocsig certificates from '/etc/ipsec.d/ocspcerts'
Jul 02 11:20:43 ipsec1-VirtualBox charon[2971]: 00[CFG] loading attribute certificates from '/etc/ipsec.d/acerts'
Jul 02 11:20:43 ipsec1-VirtualBox charon[2971]: 00[CFG] loading crls from '/etc/ipsec.d/crls'
Jul 02 11:20:43 ipsec1-VirtualBox charon[2971]: 00[CFG] loading secrets from '/etc/ipsec.secrets'
Jul 02 11:20:43 ipsec1-VirtualBox charon[2971]: 00[LIB] loaded plugins: charon aes rc2 sha2 sha1 md5 mgf1 random nonce x509 revocation const
Jul 02 11:20:43 ipsec1-VirtualBox charon[2971]: 00[LIB] dropped capabilities, running as uid 0, gid 0
Jul 02 11:20:43 ipsec1-VirtualBox charon[2971]: 00[JOB] spawning 16 worker threads
Jul 02 11:20:43 ipsec1-VirtualBox ipsec[2962]: charon (2971) started after 80 ms
Jul 02 11:20:43 ipsec1-VirtualBox ipsec_starter[2962]: charon (2971) started after 80 ms
ipsec1@ipsec1-VirtualBox: ~$ sudo systemctl is-enabled strongswan-starter
enabled
ipsec1@ipsec1-VirtualBox: ~$ sudo cp /etc/ipsec.conf /etc/ipsec.conf.orig
ipsec1@ipsec1-VirtualBox: ~$ sudo nano /etc/ipsec.conf
ipsec1@ipsec1-VirtualBox: ~$ head -c 24 /dev/urandom | base64
```

7- برای به دست آوردن یک PSK از دستور زیر استفاده می‌کنیم.

```
$ head -c 24 /dev/urandom | base64
```


8- PSK را در فایل `/etc/ipsec.secrets` قرار می‌دهیم.

```
$ sudo vim /etc/ipsec.secrets
```



9- IPsec را restart کرده و وضعیت آن را مشاهده می‌کنیم.

```
$ sudo ipsec restart
```

```
$ sudo ipsec status
```

10- در نهایت، ping می‌کنیم.

```
IPSec1 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Terminal
Jul 2 12:09
ipsec1@ipsec1-VirtualBox: ~
ipsec1@ipsec1-VirtualBox: ~
Jul 02 11:20:43 ipsec1-VirtualBox charon[2971]: 00[JOB] spawning 16 worker threads
Jul 02 11:20:43 ipsec1-VirtualBox ipsec[2962]: charon (2971) started after 80 ms
Jul 02 11:20:43 ipsec1-VirtualBox ipsec starter[2962]: charon (2971) started after 80 ms
ipsec1@ipsec1-VirtualBox:~$ sudo systemctl is-enabled strongswan-starter
enabled
ipsec1@ipsec1-VirtualBox:~$ sudo cp /etc/ipsec.conf /etc/ipsec.conf.orig
ipsec1@ipsec1-VirtualBox:~$ sudo nano /etc/ipsec.conf
ipsec1@ipsec1-VirtualBox:~$ head -c 24 /dev/urandom | base64
S1vmB5kkaWPkbbmclWkdQxLkZ21mzBvS
ipsec1@ipsec1-VirtualBox:~$ sudo vi /etc/ipsec.secrets
[sudo] password for ipsec1:
ipsec1@ipsec1-VirtualBox:~$ sudo gedit /etc/ipsec.secrets
ipsec1@ipsec1-VirtualBox:~$ sudo ipsec restart
Stopping strongSwan IPsec...
Starting strongSwan 5.9.1 IPsec [starter]...
ipsec1@ipsec1-VirtualBox:~$ sudo ipsec status
Security Associations (0 up, 1 connecting):
devgateway-to-prodgateway[1]: CONNECTING, 10.20.20.1[%any]...10.20.20.3[%any]
ipsec1@ipsec1-VirtualBox:~$ sudo nano /etc/ipsec.conf
ipsec1@ipsec1-VirtualBox:~$ sudo gedit /etc/ipsec.conf
ipsec1@ipsec1-VirtualBox:~$ sudo gedit /etc/ipsec.conf
ipsec1@ipsec1-VirtualBox:~$ sudo ipsec restart
Stopping strongSwan IPsec...
Starting strongSwan 5.9.1 IPsec [starter]...
ipsec1@ipsec1-VirtualBox:~$ sudo ipsec status
Security Associations (1 up, 0 connecting):
devgateway-to-prodgateway[2]: ESTABLISHED 5 seconds ago, 192.168.1.8[192.168.1.8]...192.168.1.7[192.168.1.7]
devgateway-to-prodgateway[1]: INSTALLED, TUNNEL, reqid 1, ESP SPIs: c7c3dbld_i caca0f45_o
devgateway-to-prodgateway[1]: 192.168.1.0/24 === 192.168.1.0/24
ipsec1@ipsec1-VirtualBox:~$ ping 192.168.1.7
PING 192.168.1.7 (192.168.1.7) 56(84) bytes of data:
64 bytes from 192.168.1.7: icmp_seq=1 ttl=64 time=0.918 ms
```

```
IPSec1 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Terminal
Jul 2 12:10
ipsec1@ipsec1-VirtualBox: ~
ipsec1@ipsec1-VirtualBox: ~
ipsec1@ipsec1-VirtualBox:~$ --- 192.168.1.7 ping statistics ---
9 packets transmitted, 9 received, 0% packet loss, time 8027ms
rtt min/avg/max/mdev = 0.908/2.169/8.337/2.242 ms
ipsec1@ipsec1-VirtualBox:~$ sudo gedit /etc/ipsec.conf
ipsec1@ipsec1-VirtualBox:~$ sudo gedit /etc/ipsec.secrets
ipsec1@ipsec1-VirtualBox:~$ sudo ipsec restart
Stopping strongSwan IPsec...
Starting strongSwan 5.9.1 IPsec [starter]...
ipsec1@ipsec1-VirtualBox:~$ sudo ipsec status
Security Associations (0 up, 0 connecting):
none
ipsec1@ipsec1-VirtualBox:~$ ping 192.168.1.7
PING 192.168.1.7 (192.168.1.7) 56(84) bytes of data:
64 bytes from 192.168.1.7: icmp_seq=1 ttl=64 time=1.15 ms
64 bytes from 192.168.1.7: icmp_seq=2 ttl=64 time=1.13 ms
64 bytes from 192.168.1.7: icmp_seq=3 ttl=64 time=1.09 ms
64 bytes from 192.168.1.7: icmp_seq=4 ttl=64 time=0.907 ms
64 bytes from 192.168.1.7: icmp_seq=5 ttl=64 time=1.02 ms
ipsec1@ipsec1-VirtualBox:~$ --- 192.168.1.7 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4007ms
rtt min/avg/max/mdev = 0.907/1.060/1.146/0.087 ms
ipsec1@ipsec1-VirtualBox:~$ sudo gedit /etc/ipsec.secrets
ipsec1@ipsec1-VirtualBox:~$ sudo ipsec restart
Stopping strongSwan IPsec...
Starting strongSwan 5.9.1 IPsec [starter]...
ipsec1@ipsec1-VirtualBox:~$ sudo ipsec status
Security Associations (1 up, 0 connecting):
devgateway-to-prodgateway[2]: ESTABLISHED 8 seconds ago, 192.168.1.8[192.168.1.8]...192.168.1.7[192.168.1.7]
devgateway-to-prodgateway[2]: INSTALLED, TUNNEL, reqid 1, ESP SPIs: c7cb5659_i cf3b5086_o
devgateway-to-prodgateway[2]: 192.168.1.0/24 === 192.168.1.0/24
ipsec1@ipsec1-VirtualBox:~$
```