# GENERAL INFORMATION ABOUT THE PRACTICE

**Practice name:** Practicing Site-to-Site VPN on Linux

**Number of students working together:** 01

**Score:** 01 point

**Practice location:** Computer room

**Request:**

- Hardware requirements: Each student is provided with 01 computer with minimum configuration: CPU 2.0 GHz, RAM 16GB, HDD 100GB

- Software requirements on the machine:

+ Operating system CentOS7, Ubuntu 14.04

+ VMware Workstation 9.0 or higher

- Practice tools: VMware virtual machine:

+ Windows CentOS7, Ubuntu 14.04

- LAN connection required: yes

- Internet connection required: no

- Requirements: projector, whiteboard, pen/chalk

# PREPARATION FOR PRACTICE

**For instructors:**

Before preparation for practice the lesson, the instructor (practice instructor) needs to check the suitability of the actual conditions of the practice room with the requirements of the practice lesson.

No other requirements.

**For students:**

Before starting the practice, it is necessary to create copies of the virtual machines for use. Also specify the storage location for the tools specified in the requirements section

# PART 1. CONFIGURATION OF VPN NETWORK ACCORDING TO CLIENT MODEL TO-SIDE

## 1.1. Description

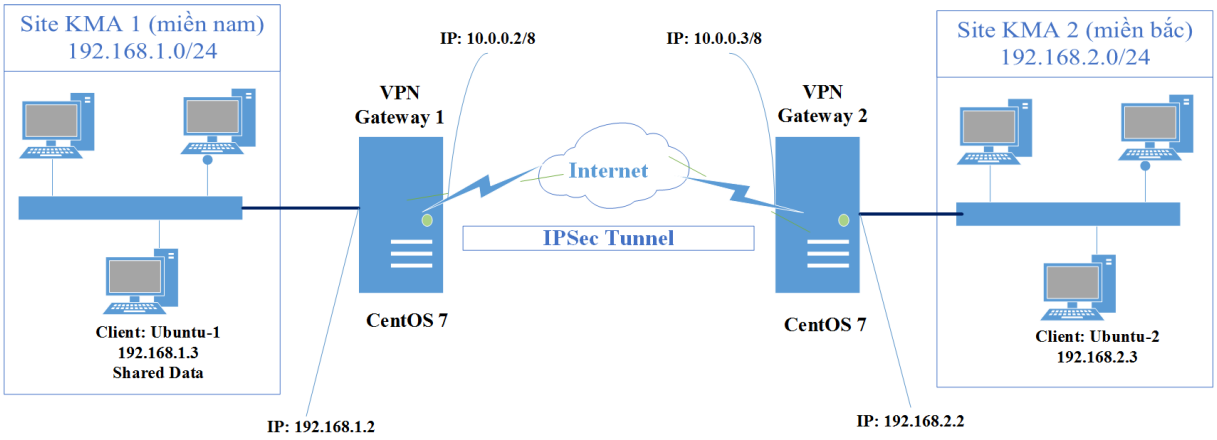
This section guides students to exploit and use VPN tools in Site to Site VPN and Remote Access VPN versions on Linux platform.

## 1.2. Preparation

- 02 virtual machines running CentOS7 operating system.

- 02 virtual machine running Ubuntu operating system.

## 1.3. Deployment model




## 1.4. Description of work to be performed

- Install StrongSwan.

- Configure Site to Site IPSec VPN with StrongSwan.

- Test connectivity between networks in Site to Site VPN

- Share user data with FTP service file sharing via Site to Site VPN

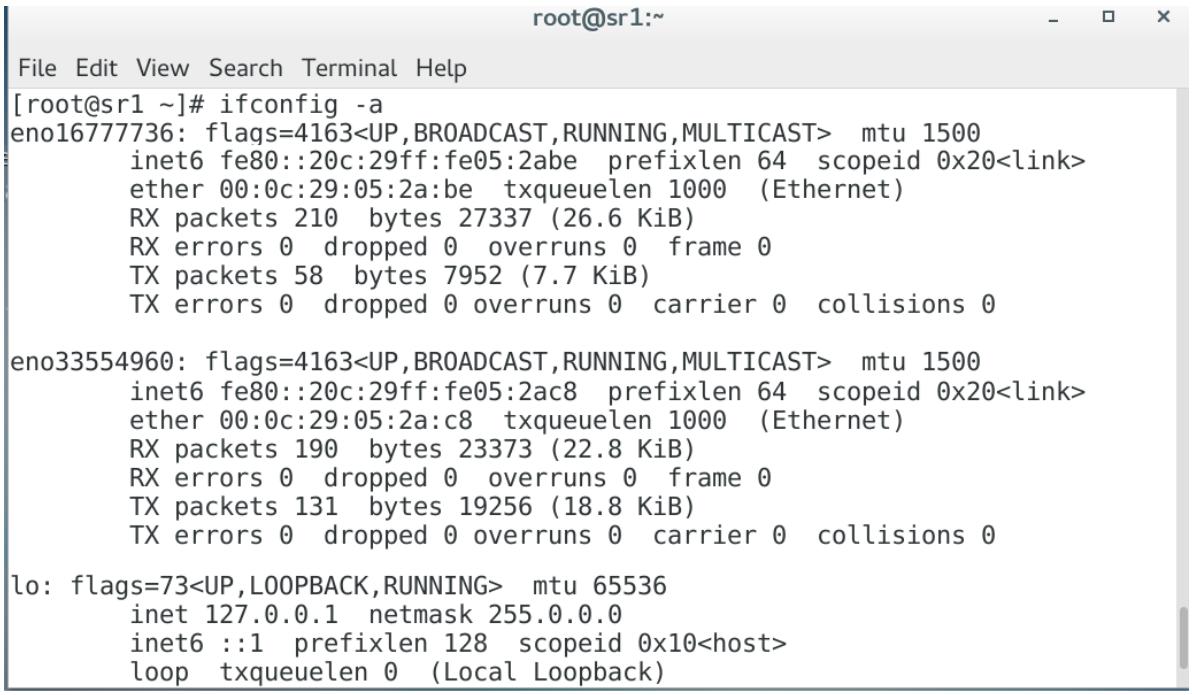
## 1.5. Implementation steps

- Set up IP address

+ On VPN Gateway 1:

• Check the network name tag on the machine with the command:

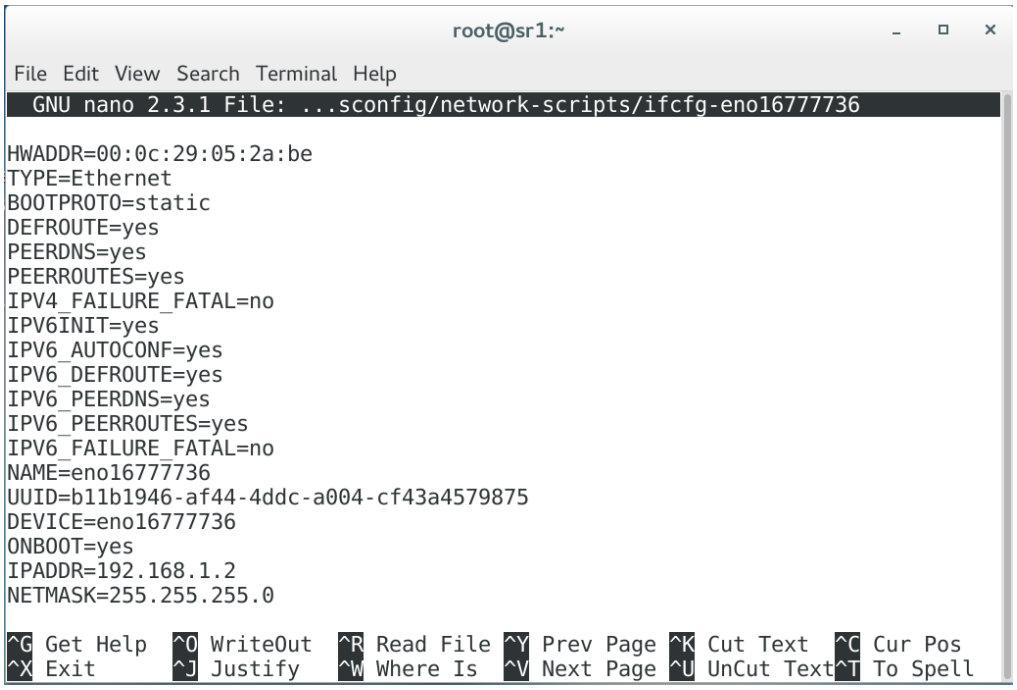
```
#ifconfgi –a
```



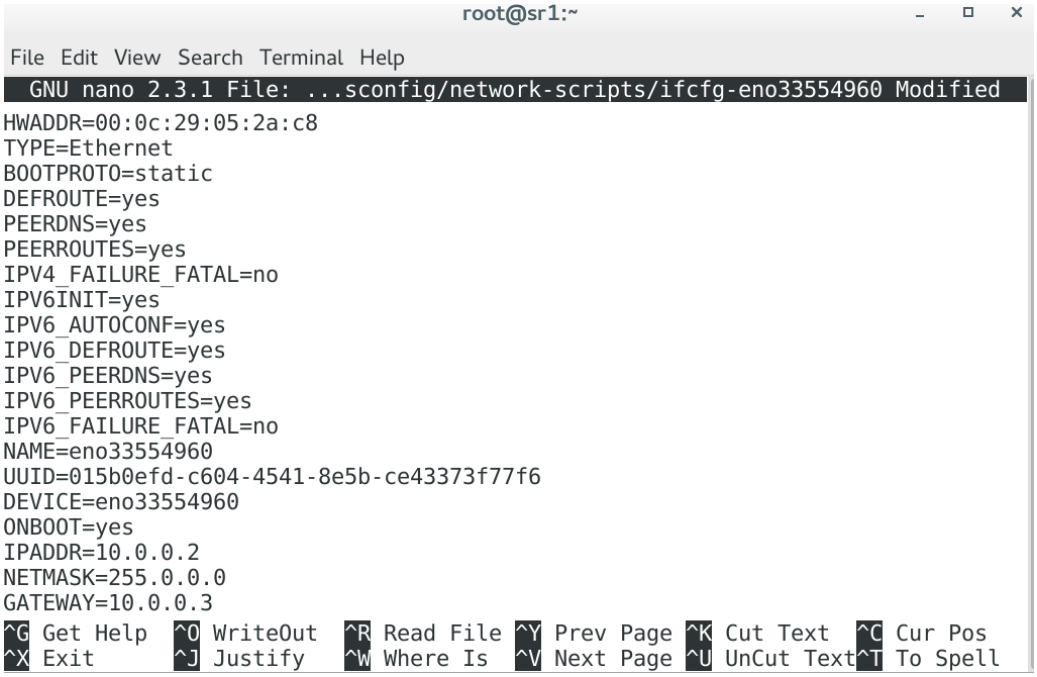

Thus, VPN Gateway 1 has two network cards named: eno16777736 and eno33554960. Similar to these two network cards, these are two configuration files in the /etc/sysconfig/network-scripts directory: ifcfg-eno16777736 and ifcf-eno33554960 . If these files do not exist (configuration in VMware), they need to be created.

Configure the IP address for the card network information edit file as follows:

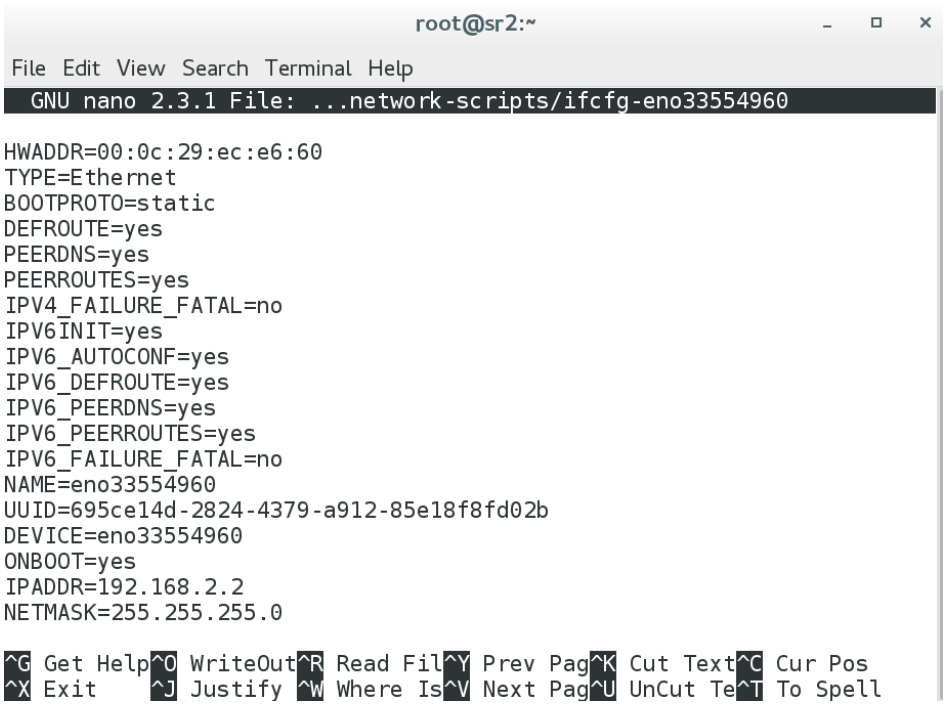
*#nano /etc/sysconfig/network-scripts/ifcfg-eno16777736*




*#nano /etc/sysconfig/network-scripts/ifcfg-eno33554960*




+ On VPN Gateway 2:



```
root@sr2:~
File  Edit  View  Search  Terminal  Help
  GNU nano 2.3.1 File: ...network-scripts/ifcfg-eno16777736

HWADDR=00:0c:29:ec:e6:56
TYPE=Ethernet
BOOTPROTO=static
DEFROUTE=yes
PEERDNS=yes
PEERROUTES=yes
IPV4_FAILURE_FATAL=no
IPV6INIT=yes
IPV6_AUTOCONF=yes
IPV6_DEFROUTE=yes
IPV6_PEERDNS=yes
IPV6_PEERROUTES=yes
IPV6_FAILURE_FATAL=no
NAME=eno16777736
UUID=680c4e33-a8f2-44cc-914b-d9c6ad81ab3a
DEVICE=eno16777736
ONBOOT=yes
IPADDR=10.0.0.3
NETMASK=255.0.0.0
GATEWAY=10.0.0.2

^G Get Help^O WriteOut^R Read Fil^Y Prev Pag^K Cut Text^C Cur Pos
^X Exit     ^J Justify ^W Where Is^V Next Pag^U UnCut Te^T To Spell
```

+ On Ubuntu 1:

*#nano /etc/mạng/giao diện*

```
root@nghi1-pc: /
  GNU nano 2.2.6          File: /etc/network/interfaces                Modified

# interfaces(5) file used by ifup(8) and ifdown(8)
auto lo
iface lo inet loopback
auto eth0
iface eth0 inet static
address 192.168.1.3
netmask 255.255.255.0
gateway 192.168.1.2
network 192.168.1.0


^G Get Help  ^O WriteOut  ^R Read File ^Y Prev Page ^K Cut Text  ^C Cur Pos
^X Exit      ^J Justify   ^W Where Is  ^V Next Page ^U UnCut Text^T To Spell
```

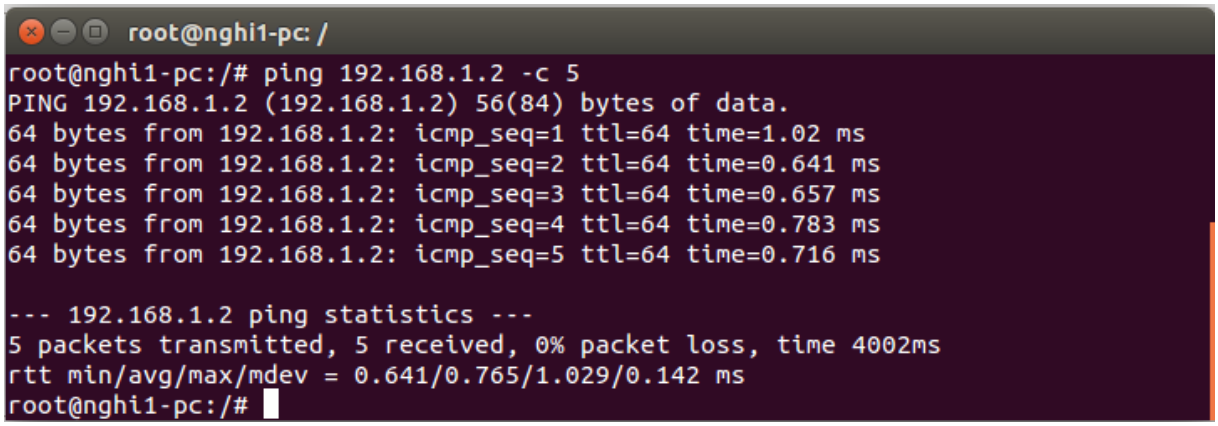
+ On Ubuntu 2:

```
nghi1@nghi1-pc: ~
  GNU nano 2.2.6          File: /etc/network/interfaces                Modified

# interfaces(5) file used by ifup(8) and ifdown(8)
auto lo
iface lo inet loopback
auto eth0
iface eth0 inet static
address 192.168.2.3
netmask 255.255.255.0
gateway 192.168.2.2
network 192.168.2.0


^G Get Help  ^O WriteOut  ^R Read File ^Y Prev Page ^K Cut Text  ^C Cur Pos
^X Exit      ^J Justify   ^W Where Is  ^V Next Page ^U UnCut Text^T To Spell
```

- Check connection between machines via Ping command:

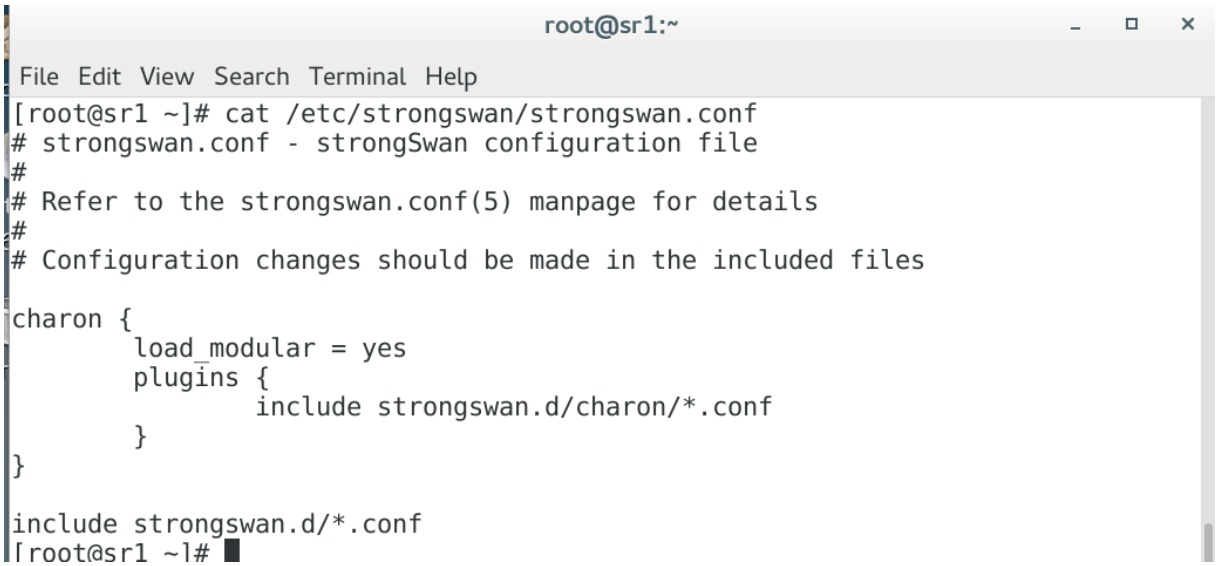



- Install Strongswan software on VPN Gateways:

*#yum cài đặt epel-release*

*#yum cài đặt strongswan*

*#cat /etc/strongswan/strongswan.conf*




- IPSec Site to Site VPN configuration parameters:

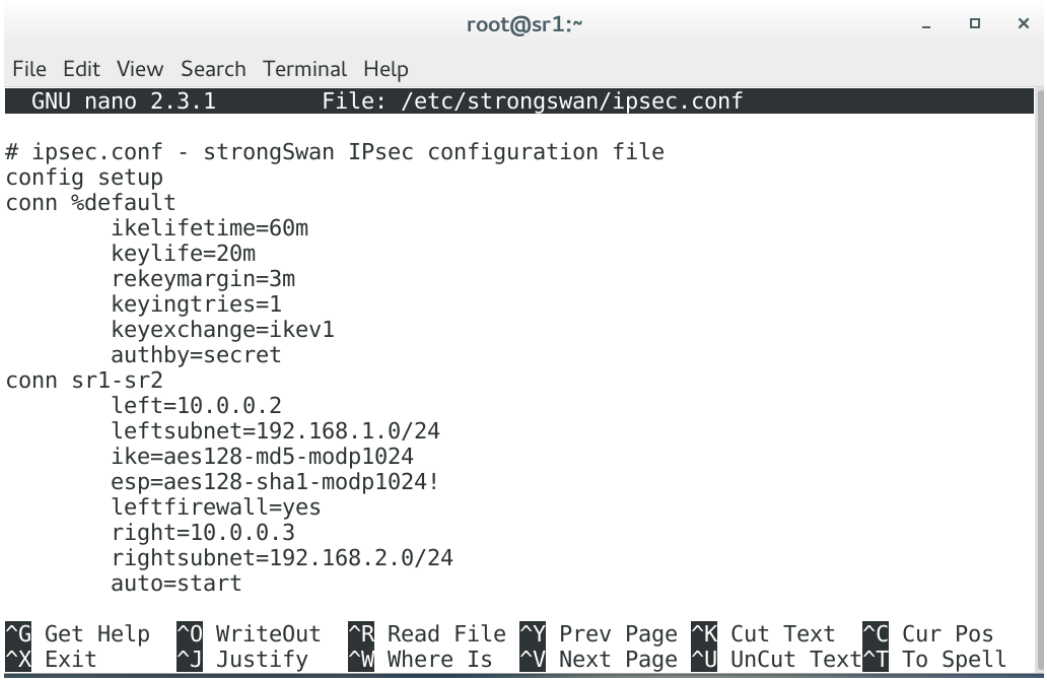
| Numerical order | Parameter | Value | |
|---|---|---|---|
| 1 | Device | VPN Gateway 1 | VPN Gateway 2 |
| 2 | Tunnel IP Address | 10.0.0.2 | 10.0.0.3 |
| 3 | Private IP Address | 192.168.1.0/24 | 192.168.2.0/24 |
| 4 | IKE Version | IKEv1 | IKEv1 |
| 5 | authenticate | MD5 | MD5 |

| | | | |
|---|---|---|---|
| 6 | Encryption Algorithm in IKE | AES-128 | AES-128 |
| 7 | Authentication algorithm in ESP | SHA-1 | SHA-1 |
| 8 | Encryption Algorithms in ESP | AES-128 | AES-128 |
| 9 | Firewall | True | True |
| 10 | Key exchange algorithm: DH-Group | 2 | 2 |
| 11 | Authentication Type | PSK | PSK |
| 12 | Key PSK | Kiểm tra123456 | Kiểm tra123456 |
| 13 | isa-kmp lifetime (seconds) | 3600 | 3600 |
| 14 | ipsec-lifetime (seconds) | 1200 | 1200 |
| 15 | ipsec operating mode | Tunnel | Tunnel |
| 16 | Negotiation mode | primarily | primarily |

- Configuration IPSec Site to Site VPN:

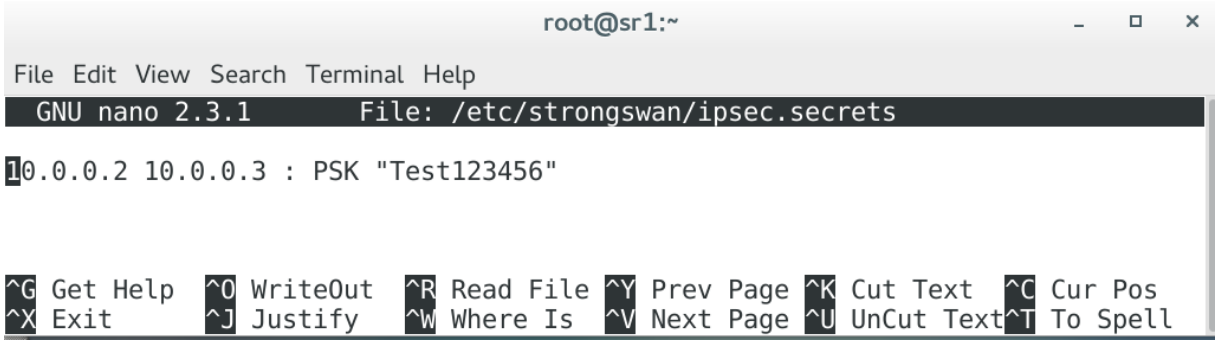
+ Edit the ipsec.conf file as follows:

*#nano /etc/strongswan/ipsec.conf*



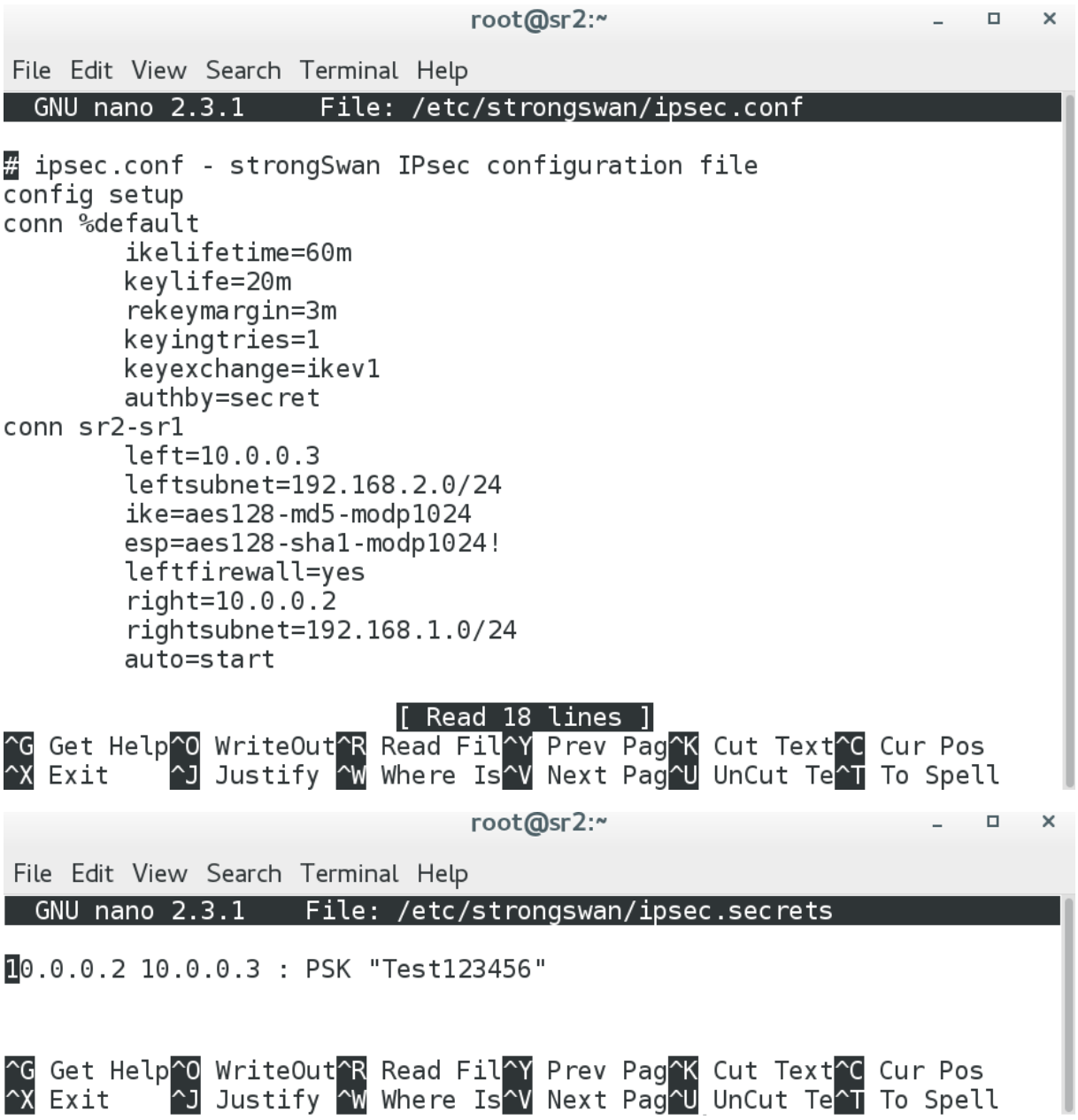
+ Edit the ipsec.secrets file as follows:

*#nano /etc/strongswan/ipsec.secrets*



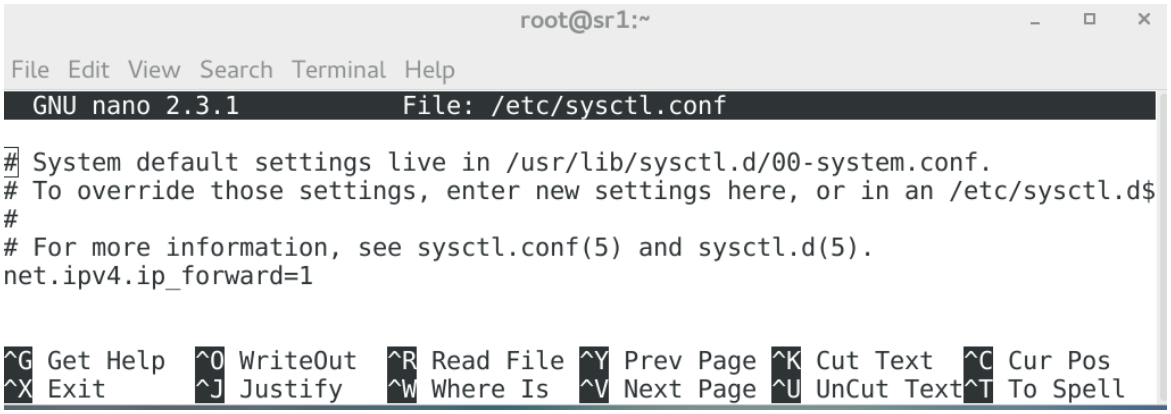

• Note: The configuration file should not contain blank lines.

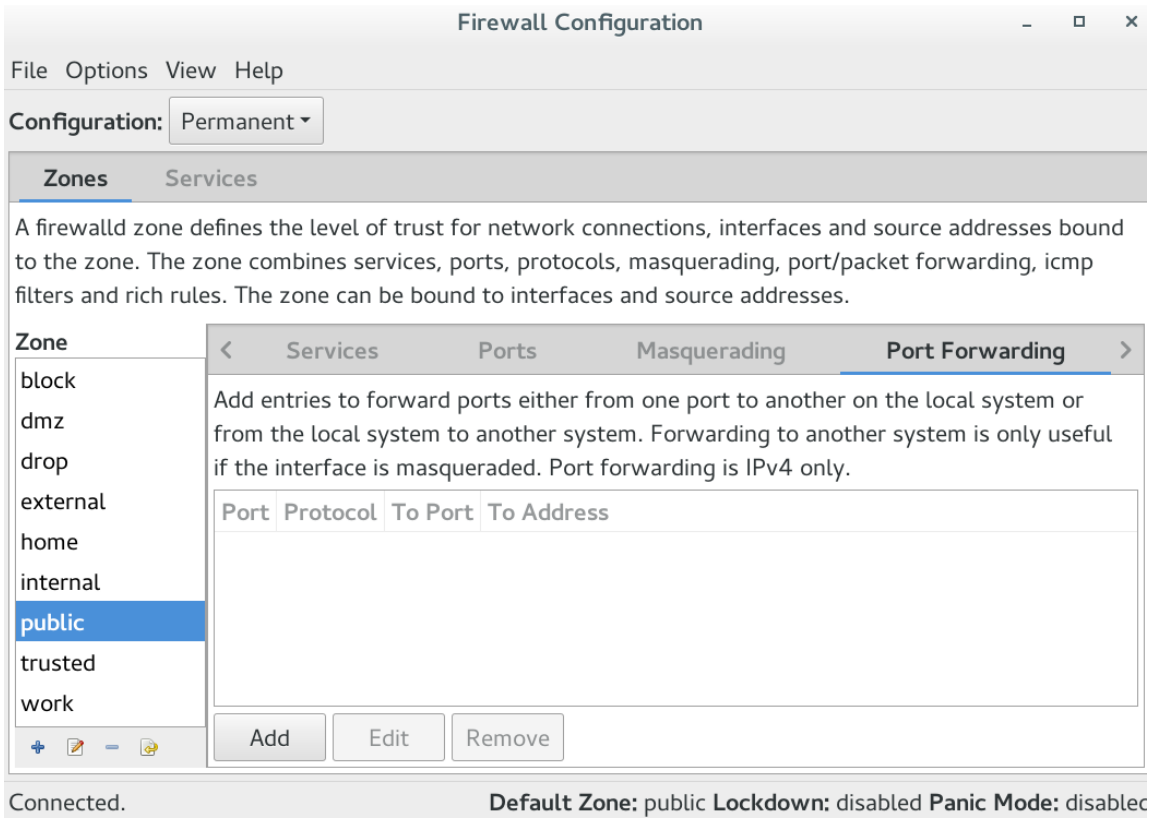
+ Same on VPN Gateway 2:



+ Enable IP Forwarding mode on both VPN Gateways, by adding the parameter net.ipv4.ip _forward=1 to the sysctl.conf file as follows:

```
#nano /etc/sysctl.conf
```



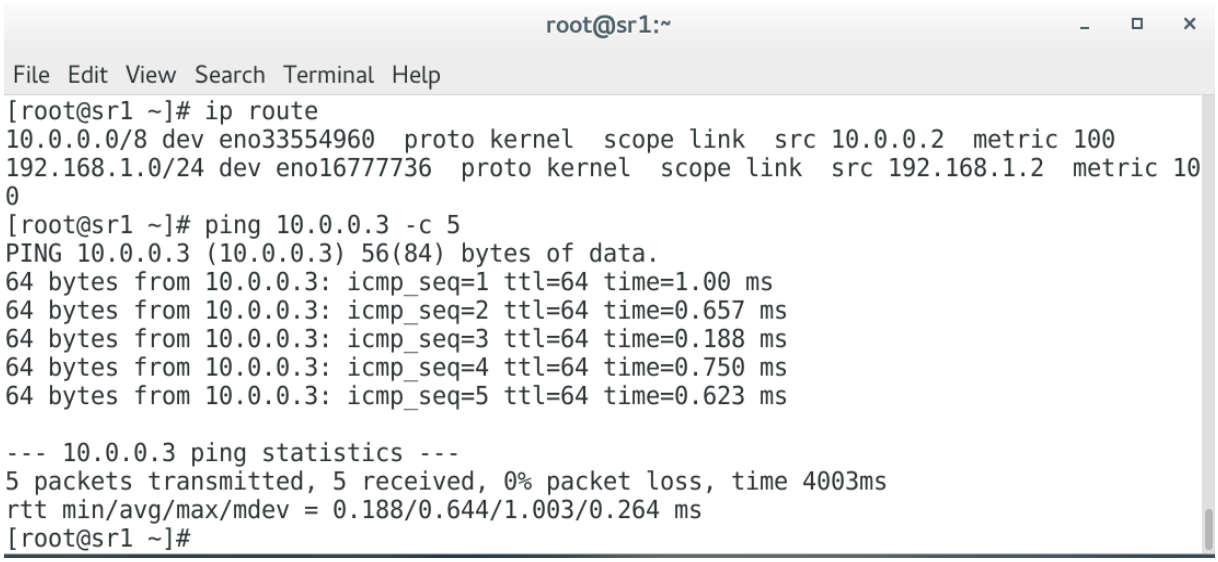




Note: In the Port Forwarding Tab of the Firewall, users can add rules to open ports UDP 500 for IKE and TCP 51 for ESP to allow Site to Site VPN traffic.

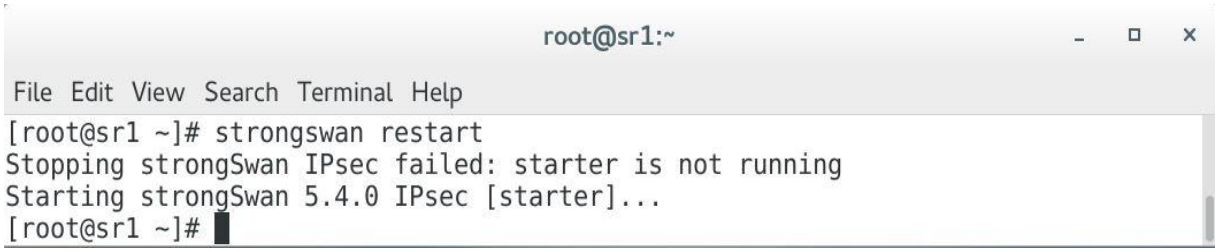
• In this guide, the Firewall is implemented via the command line as follows:

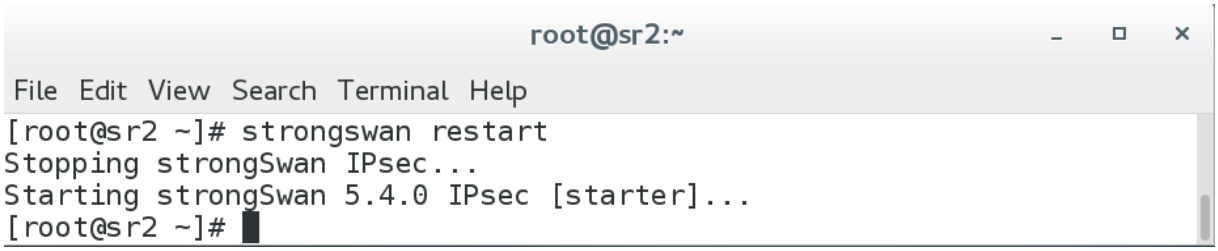
```
#firewall-cmd --permanent --add-service="ipsec"
#firewall-cmd --permanent --add-port=4500/udp
#firewall-cmd --permanent --add-masquerade
# firewall -cmd --reload
```

- Run and test Site to Site VPN operation:

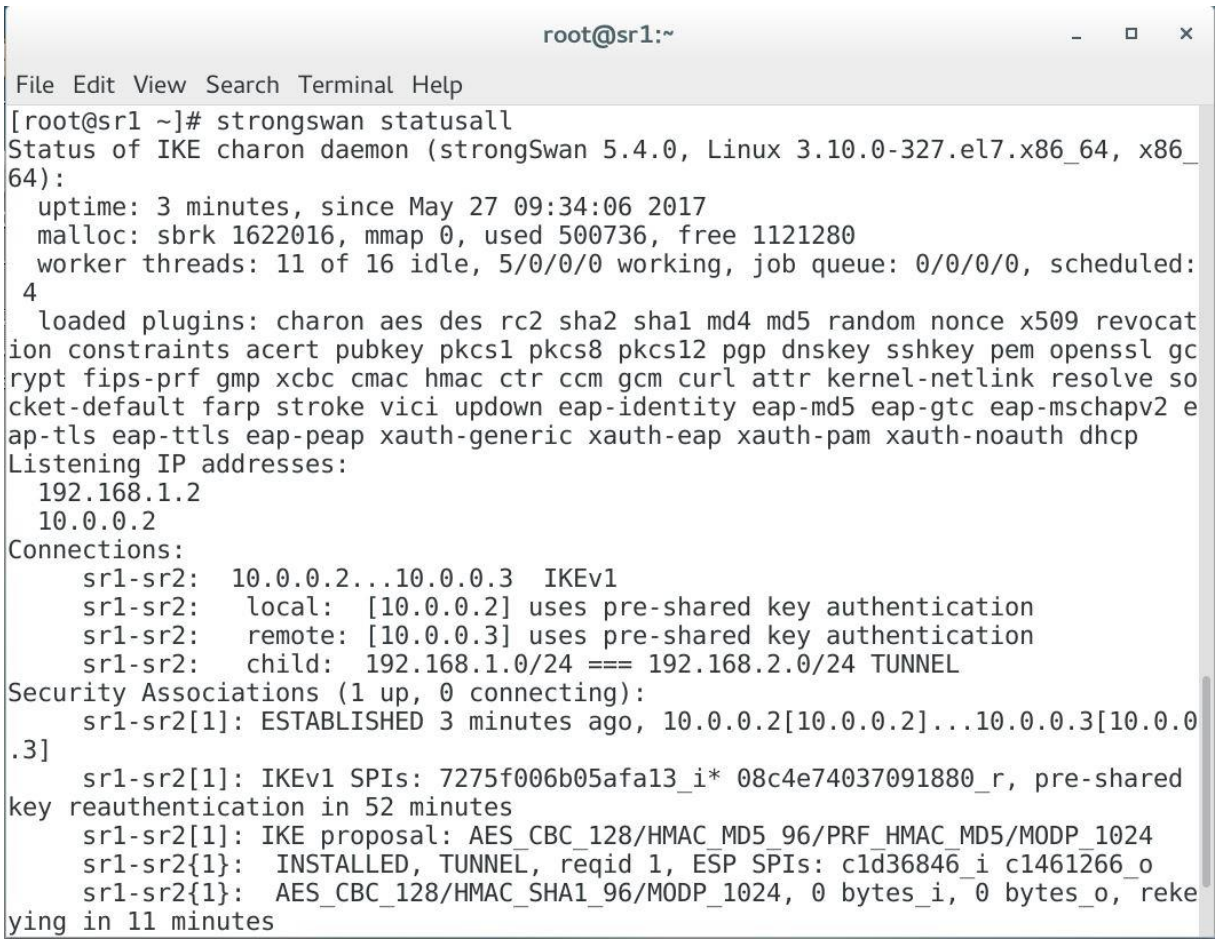



+ Start Strongswan (on both VPN Gateways):

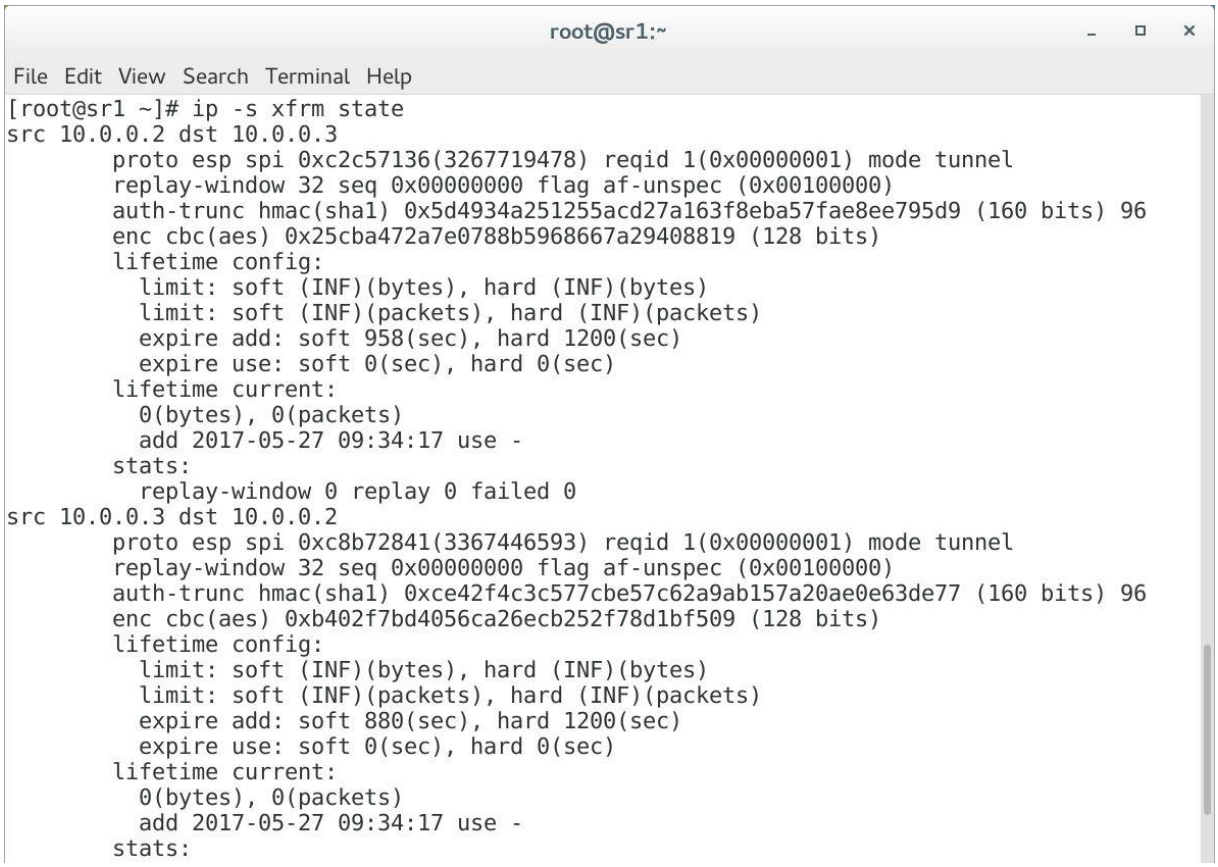


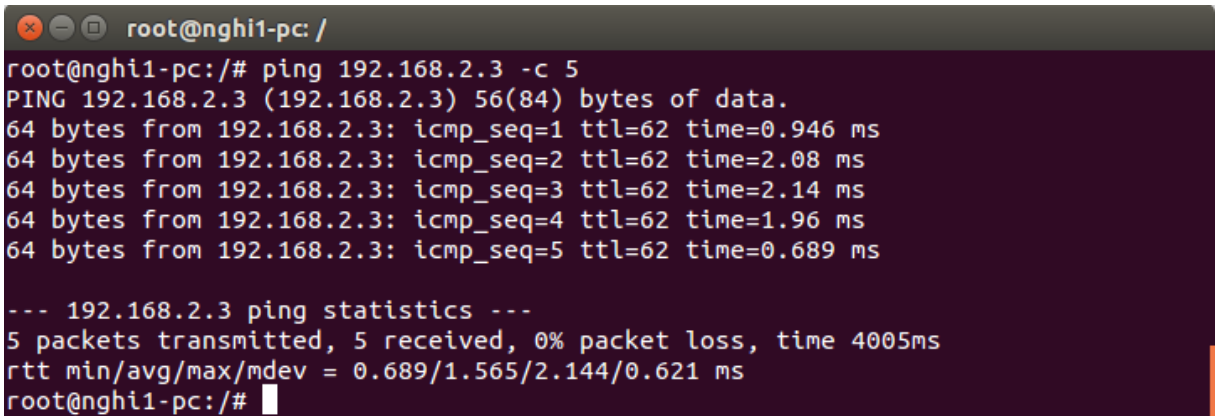

+ Check the operating status of Strongswan and make sure that the parameters (IKE, ESP) are configured correctly:




+ Check Ipsec data packets using xfrm:



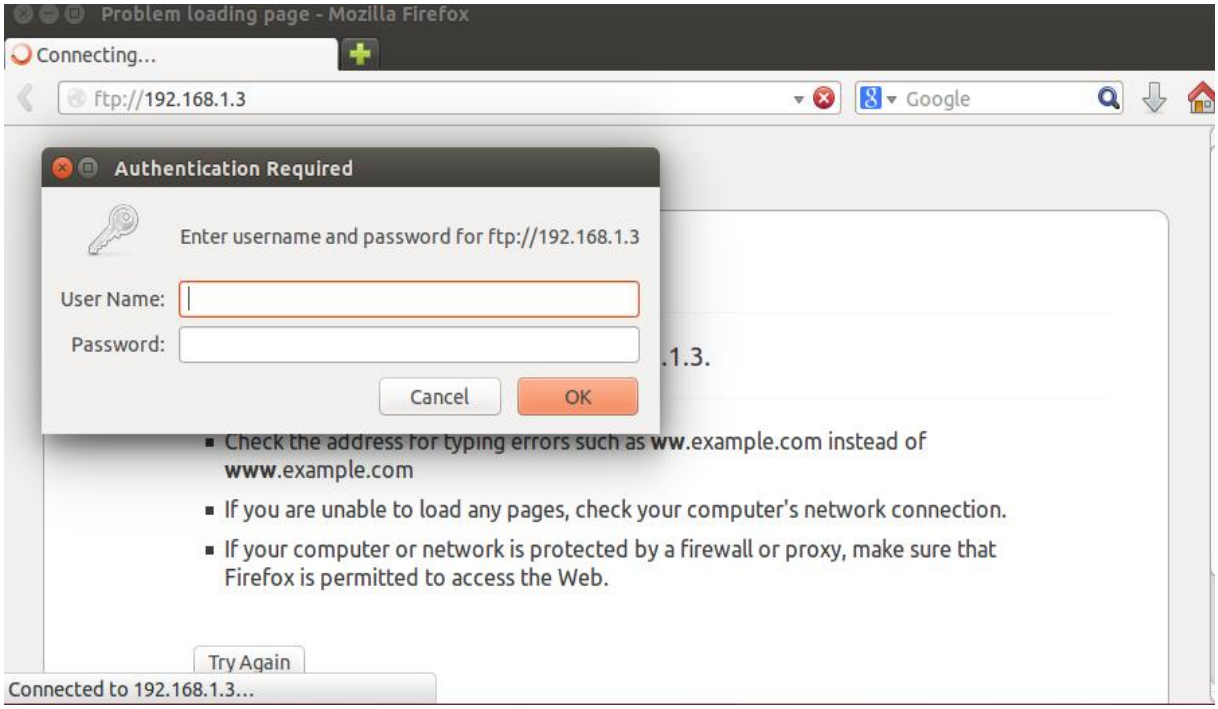
+ Check connection from Ubuntu 1 at Site 1 to Ubuntu 2 at Site 2:




- Configure FTP data sharing service via Site to Site VPN:

+ On Ubuntu 1 machine, install FTP service to share data for machines at Site KMA 2 via Site to Site VPN:

+ Ubuntu 2 machine accesses shared data from Ubuntu 1 machine:




**End of practice**