

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

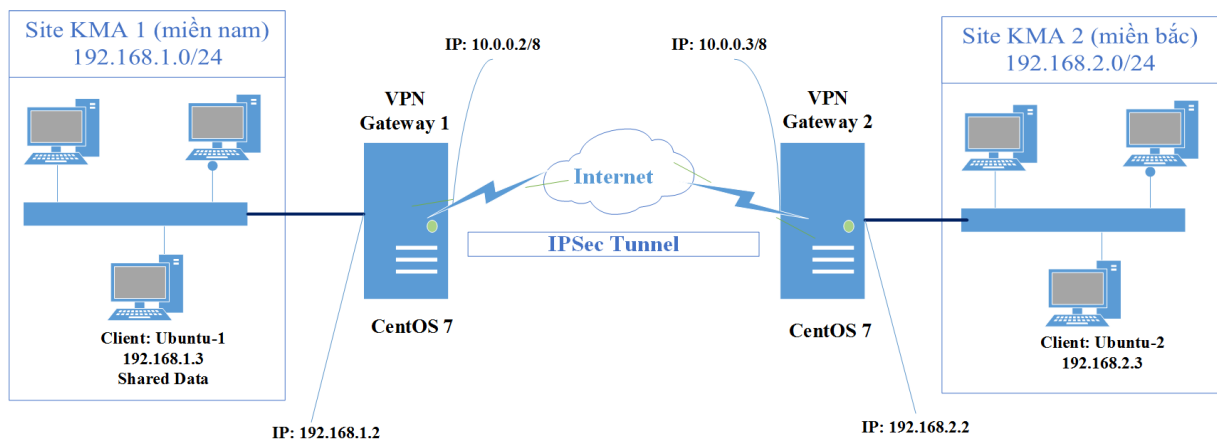
1.1. Description

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:

```
#ifconfigi -a
```

```
root@sr1:~  
File Edit View Search Terminal Help  
[root@sr1 ~]# ifconfig -a  
eno16777736: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500  
    inet6 fe80::20c:29ff:fe05:2abe prefixlen 64 scopeid 0x20<link>  
    ether 00:0c:29:05:2a:be txqueuelen 1000 (Ethernet)  
    RX packets 210 bytes 27337 (26.6 KiB)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 58 bytes 7952 (7.7 KiB)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
eno33554960: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500  
    inet6 fe80::20c:29ff:fe05:2ac8 prefixlen 64 scopeid 0x20<link>  
    ether 00:0c:29:05:2a:c8 txqueuelen 1000 (Ethernet)  
    RX packets 190 bytes 23373 (22.8 KiB)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 131 bytes 19256 (18.8 KiB)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536  
    inet 127.0.0.1 netmask 255.0.0.0  
    inet6 ::1 prefixlen 128 scopeid 0x10<host>  
    loop txqueuelen 0 (Local Loopback)
```

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 ifcfg-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
```

```
root@sr1:~  
File Edit View Search Terminal Help  
GNU nano 2.3.1 File: ...sconfig/network-scripts/ifcfg-eno16777736  
  
HWADDR=00:0c:29:05:2a:be  
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=b11b1946-af44-4ddc-a004-cf43a4579875  
DEVICE=eno16777736  
ONBOOT=yes  
IPADDR=192.168.1.2  
NETMASK=255.255.255.0  
  
^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
```

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

```
root@sr1:~  
File Edit View Search Terminal Help  
GNU nano 2.3.1 File: ...sconfig/network-scripts/ifcfg-eno33554960 Modified  
HWADDR=00:0c:29:05:2a:c8  
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=eno33554960  
UUID=015b0efd-c604-4541-8e5b-ce43373f77f6  
DEVICE=eno33554960  
ONBOOT=yes  
IPADDR=10.0.0.2  
NETMASK=255.0.0.0  
GATEWAY=10.0.0.3  
^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 VPN Gateway 2:

```
root@sr2:~  
File Edit View Search Terminal Help  
GNU nano 2.3.1 File: ...network-scripts/ifcfg-eno33554960  
HWADDR=00:0c:29:ec:e6:60  
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=eno33554960  
UUID=695ce14d-2824-4379-a912-85e18f8fd02b  
DEVICE=eno33554960  
ONBOOT=yes  
IPADDR=192.168.2.2  
NETMASK=255.255.255.0  
^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
```

```
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 File ^Y Prev Page ^K Cut Text ^C Cur Pos
^X Exit ^J Justify ^W Where Is ^V Next Page ^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:

```

root@ngni1-pc: /
root@ngni1-pc:/# ping 192.168.1.2 -c 5
PING 192.168.1.2 (192.168.1.2) 56(84) bytes of data.
64 bytes from 192.168.1.2: icmp_seq=1 ttl=64 time=1.02 ms
64 bytes from 192.168.1.2: icmp_seq=2 ttl=64 time=0.641 ms
64 bytes from 192.168.1.2: icmp_seq=3 ttl=64 time=0.657 ms
64 bytes from 192.168.1.2: icmp_seq=4 ttl=64 time=0.783 ms
64 bytes from 192.168.1.2: icmp_seq=5 ttl=64 time=0.716 ms

--- 192.168.1.2 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4002ms
rtt min/avg/max/mdev = 0.641/0.765/1.029/0.142 ms
root@ngni1-pc:/#

```

- Install Strongswan software on VPN Gateways:

```

#yum cài đặt epel-release

#yum cài đặt strongswan

#cat /etc/strongswan/strongswan.conf

```

```

root@sr1:~
File Edit View Search Terminal Help
[root@sr1 ~]# cat /etc/strongswan/strongswan.conf
# strongswan.conf - strongSwan configuration file
#
# Refer to the strongswan.conf(5) manpage for details
#
# Configuration changes should be made in the included files

charon {
    load_modular = yes
    plugins {
        include strongswan.d/charon/*.conf
    }
}

include strongswan.d/*.conf
[root@sr1 ~]#

```

- IPSec Site to Site VPN configuration parameters:

Numerical order	Parameter	Value	
		VPN Gateway 1	VPN Gateway 2
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

```

root@sr1:~
File Edit View Search Terminal Help
GNU nano 2.3.1 File: /etc/strongswan/ipsec.conf

# ipsec.conf - strongSwan IPsec configuration file
config setup
conn %default
    ikelifetime=60m
    keylife=20m
    rekeymargin=3m
    keyingtries=1
    keyexchange=ikev1
    authby=secret
conn sr1-sr2
    left=10.0.0.2
    leftsubnet=192.168.1.0/24
    ike=aes128-md5-modp1024
    esp=aes128-sha1-modp1024!
    leftfirewall=yes
    right=10.0.0.3
    rightsubnet=192.168.2.0/24
    auto=start

^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

```


+ Edit the ipsec.secrets file as follows:

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

```
root@sr1:~  
File Edit View Search Terminal Help  
GNU nano 2.3.1 File: /etc/strongswan/ipsec.secrets  
10.0.0.2 10.0.0.3 : PSK "Test123456"  
  
^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
```

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

+ Same on VPN Gateway 2:

```
root@sr2:~  
File Edit View Search Terminal Help  
GNU nano 2.3.1 File: /etc/strongswan/ipsec.conf  
# ipsec.conf - strongSwan IPsec configuration file  
config setup  
conn %default  
    ikelifetime=60m  
    keylife=20m  
    rekeymargin=3m  
    keyingtries=1  
    keyexchange=ikev1  
    authby=secret  
conn sr2-sr1  
    left=10.0.0.3  
    leftsubnet=192.168.2.0/24  
    ike=aes128-md5-modp1024  
    esp=aes128-sha1-modp1024!  
    leftfirewall=yes  
    right=10.0.0.2  
    rightsubnet=192.168.1.0/24  
    auto=start  
  
[ Read 18 lines ]  
^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
```

```
root@sr2:~  
File Edit View Search Terminal Help  
GNU nano 2.3.1 File: /etc/strongswan/ipsec.secrets  
10.0.0.2 10.0.0.3 : PSK "Test123456"  
  
^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
```

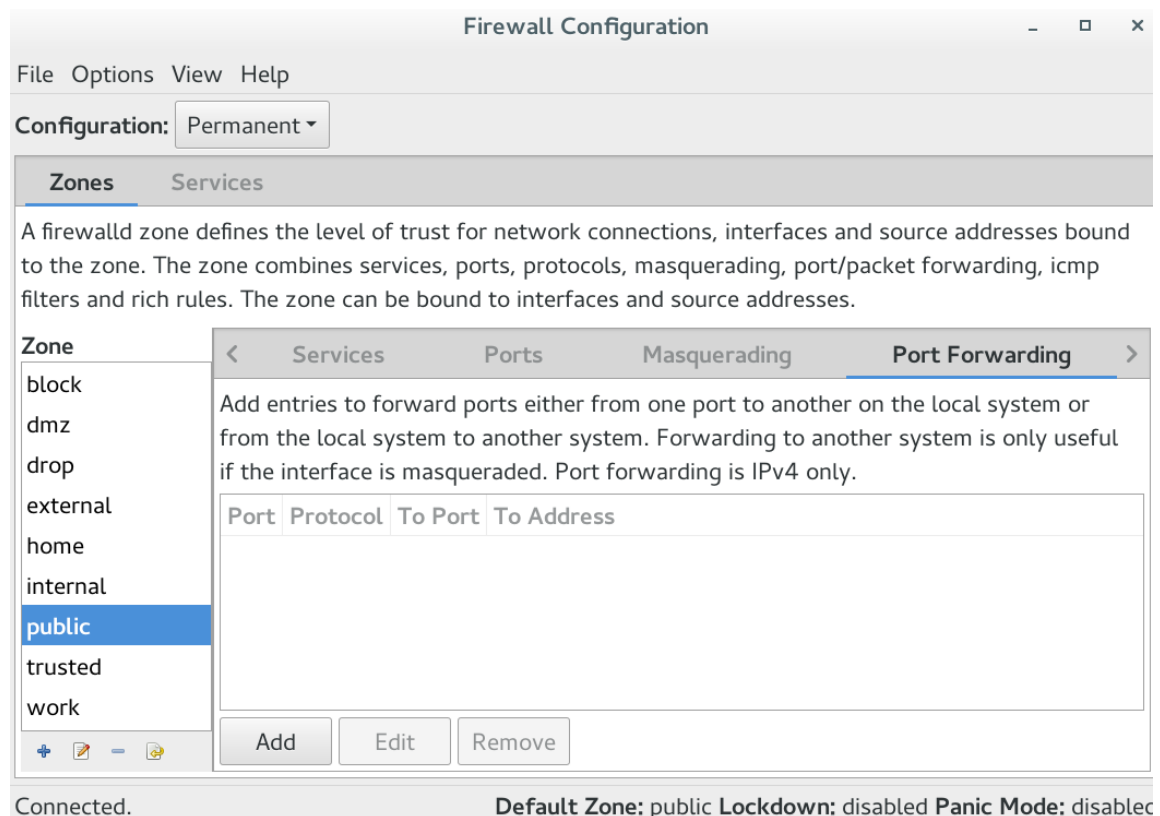
+ Enable IP Forwarding mode on both VPN Gateways, by adding the parameter `net.ipv4.ip_forward=1` to the `sysctl.conf` file as follows:

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

```
root@sr1:~
File Edit View Search Terminal Help
GNU nano 2.3.1 File: /etc/sysctl.conf

# System default settings live in /usr/lib/sysctl.d/00-system.conf.
# To override those settings, enter new settings here, or in an /etc/sysctl.d$
#
# For more information, see sysctl.conf(5) and sysctl.d(5).
net.ipv4.ip_forward=1

^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
```



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:

```
root@sr1:~  
File Edit View Search Terminal Help  
[root@sr1 ~]# ip route  
10.0.0.0/8 dev eno33554960 proto kernel scope link src 10.0.0.2 metric 100  
192.168.1.0/24 dev eno16777736 proto kernel scope link src 192.168.1.2 metric 10  
0  
[root@sr1 ~]# ping 10.0.0.3 -c 5  
PING 10.0.0.3 (10.0.0.3) 56(84) bytes of data.  
64 bytes from 10.0.0.3: icmp_seq=1 ttl=64 time=1.00 ms  
64 bytes from 10.0.0.3: icmp_seq=2 ttl=64 time=0.657 ms  
64 bytes from 10.0.0.3: icmp_seq=3 ttl=64 time=0.188 ms  
64 bytes from 10.0.0.3: icmp_seq=4 ttl=64 time=0.750 ms  
64 bytes from 10.0.0.3: icmp_seq=5 ttl=64 time=0.623 ms  
  
--- 10.0.0.3 ping statistics ---  
5 packets transmitted, 5 received, 0% packet loss, time 4003ms  
rtt min/avg/max/mdev = 0.188/0.644/1.003/0.264 ms  
[root@sr1 ~]#
```

+ Start Strongswan (on both VPN Gateways):

```
root@sr1:~  
File Edit View Search Terminal Help  
[root@sr1 ~]# strongswan restart  
Stopping strongSwan IPsec failed: starter is not running  
Starting strongSwan 5.4.0 IPsec [starter]...  
[root@sr1 ~]# █
```

```
root@sr2:~  
File Edit View Search Terminal Help  
[root@sr2 ~]# strongswan restart  
Stopping strongSwan IPsec...  
Starting strongSwan 5.4.0 IPsec [starter]...  
[root@sr2 ~]# █
```

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

```
root@sr1:~
File Edit View Search Terminal Help
[root@sr1 ~]# strongswan statusall
Status of IKE charon daemon (strongSwan 5.4.0, Linux 3.10.0-327.el7.x86_64, x86_64):
  uptime: 3 minutes, since May 27 09:34:06 2017
  malloc: sbrk 1622016, mmap 0, used 500736, free 1121280
  worker threads: 11 of 16 idle, 5/0/0/0 working, job queue: 0/0/0/0, scheduled: 4
  loaded plugins: charon aes des rc2 sha2 sha1 md4 md5 random nonce x509 revocation constraints acert pubkey pkcs1 pkcs8 pkcs12 pgp dnskey sshkey pem openssl gcrypt fips-prf gmp xcbc cmac hmac ctr ccm gcm curl attr kernel-netlink resolve socket-default farp stroke vici updown eap-identity eap-md5 eap-gtc eap-mschapv2 eap-tls eap-ttls eap-peap xauth-generic xauth-eap xauth-pam xauth-noauth dhcp
Listening IP addresses:
  192.168.1.2
  10.0.0.2
Connections:
  sr1-sr2: 10.0.0.2...10.0.0.3 IKEv1
  sr1-sr2: local: [10.0.0.2] uses pre-shared key authentication
  sr1-sr2: remote: [10.0.0.3] uses pre-shared key authentication
  sr1-sr2: child: 192.168.1.0/24 === 192.168.2.0/24 TUNNEL
Security Associations (1 up, 0 connecting):
  sr1-sr2[1]: ESTABLISHED 3 minutes ago, 10.0.0.2[10.0.0.2]...10.0.0.3[10.0.0.3]
    sr1-sr2[1]: IKEv1 SPIs: 7275f006b05afa13_i* 08c4e74037091880_r, pre-shared key reauthentication in 52 minutes
    sr1-sr2[1]: IKE proposal: AES_CBC_128/HMAC_MD5_96/PRF_HMAC_MD5/MODP_1024
  sr1-sr2{1}: INSTALLED, TUNNEL, reqid 1, ESP SPIs: c1d36846_i c1461266_o
  sr1-sr2{1}: AES_CBC_128/HMAC_SHA1_96/MODP_1024, 0 bytes_i, 0 bytes_o, rekeying in 11 minutes
```

+ Check Ipsec data packets using xfrm:

```
root@sr1:~
File Edit View Search Terminal Help
[root@sr1 ~]# ip -s xfrm state
src 10.0.0.2 dst 10.0.0.3
  proto esp spi 0xc2c57136(3267719478) reqid 1(0x00000001) mode tunnel
  replay-window 32 seq 0x00000000 flag af-unspec (0x00100000)
  auth-trunc hmac(sha1) 0x5d4934a251255acd27a163f8eba57fae8ee795d9 (160 bits) 96
  enc cbc(aes) 0x25cba472a7e0788b5968667a29408819 (128 bits)
  lifetime config:
    limit: soft (INF)(bytes), hard (INF)(bytes)
    limit: soft (INF)(packets), hard (INF)(packets)
    expire add: soft 958(sec), hard 1200(sec)
    expire use: soft 0(sec), hard 0(sec)
  lifetime current:
    0(bytes), 0(packets)
    add 2017-05-27 09:34:17 use -
  stats:
    replay-window 0 replay 0 failed 0
src 10.0.0.3 dst 10.0.0.2
  proto esp spi 0xc8b72841(3367446593) reqid 1(0x00000001) mode tunnel
  replay-window 32 seq 0x00000000 flag af-unspec (0x00100000)
  auth-trunc hmac(sha1) 0xce42f4c3c577cbe57c62a9ab157a20ae0e63de77 (160 bits) 96
  enc cbc(aes) 0xb402f7bd4056ca26ecb252f78d1bf509 (128 bits)
  lifetime config:
    limit: soft (INF)(bytes), hard (INF)(bytes)
    limit: soft (INF)(packets), hard (INF)(packets)
    expire add: soft 880(sec), hard 1200(sec)
    expire use: soft 0(sec), hard 0(sec)
  lifetime current:
    0(bytes), 0(packets)
    add 2017-05-27 09:34:17 use -
  stats:
```

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

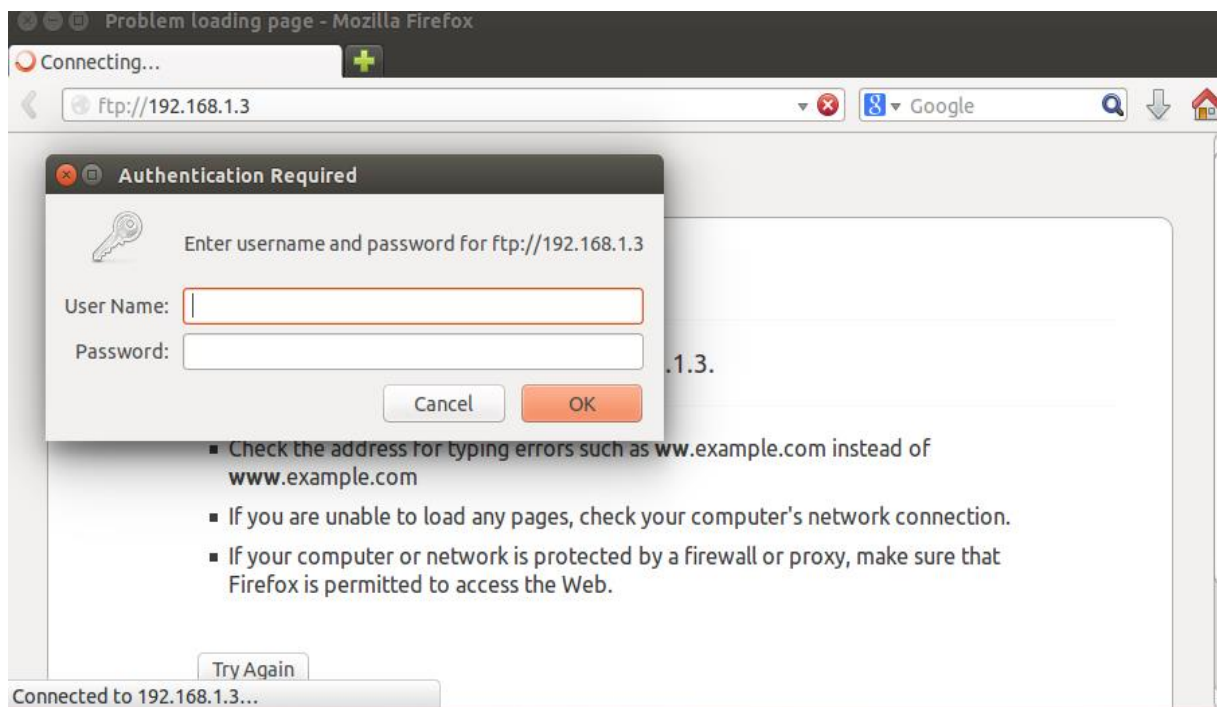
```
root@ngni1-pc: /
root@ngni1-pc:/# ping 192.168.2.3 -c 5
PING 192.168.2.3 (192.168.2.3) 56(84) bytes of data.
64 bytes from 192.168.2.3: icmp_seq=1 ttl=62 time=0.946 ms
64 bytes from 192.168.2.3: icmp_seq=2 ttl=62 time=2.08 ms
64 bytes from 192.168.2.3: icmp_seq=3 ttl=62 time=2.14 ms
64 bytes from 192.168.2.3: icmp_seq=4 ttl=62 time=1.96 ms
64 bytes from 192.168.2.3: icmp_seq=5 ttl=62 time=0.689 ms

--- 192.168.2.3 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4005ms
rtt min/avg/max/mdev = 0.689/1.565/2.144/0.621 ms
root@ngni1-pc:/#
```

- 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