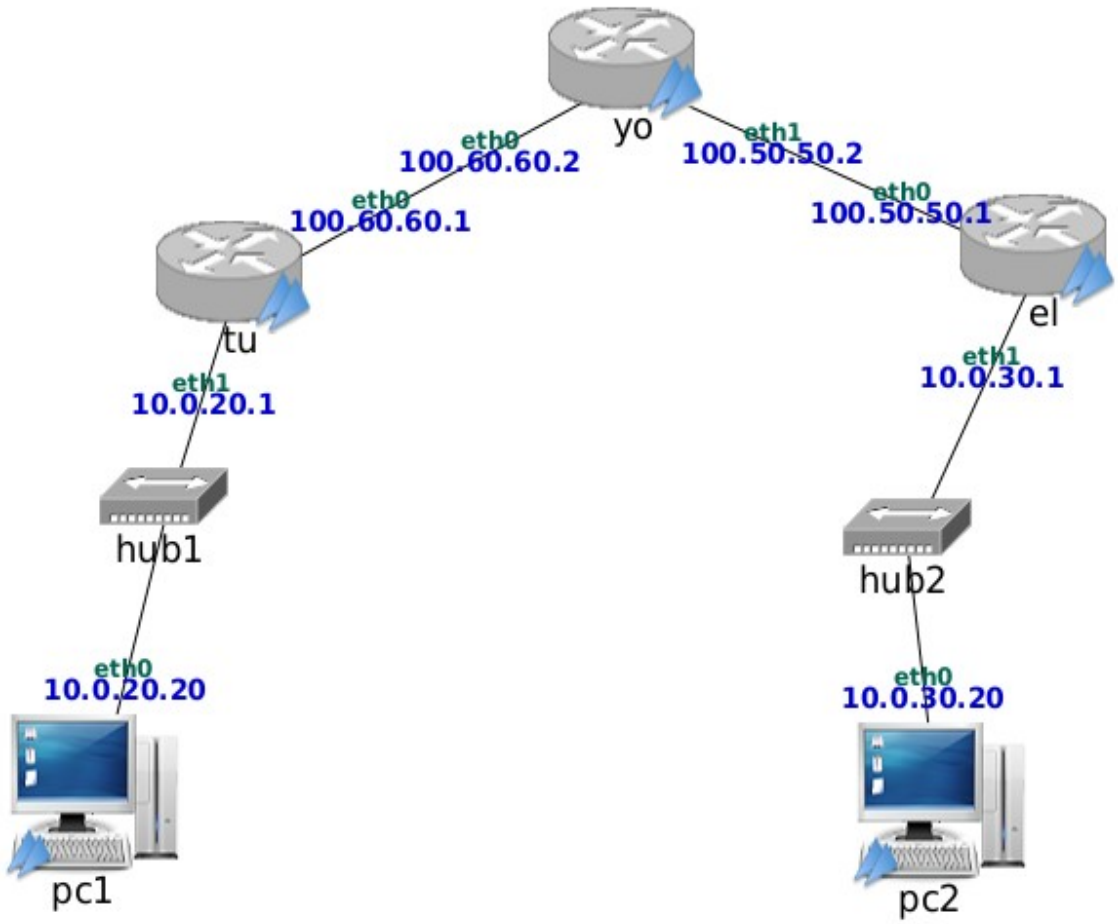
Universidad Nacional del Comahue
Facultad de Informática
2025

LABORATORIO VPN 2

Redes II, Tecnicatura en Administración de Sistemas y Software Libre

1.



2.

```
pc1:~# ping -c 3 pc2
PING pc2 (10.0.30.20) 56(84) bytes of data.

--- pc2 ping statistics ---
3 packets transmitted, 0 received, 100% packet loss, time 2003ms

pc1:~#
```

```
pc2:~# ping -c 3 pc1
PING pc1 (10.0.20.20) 56(84) bytes of data.

--- pc1 ping statistics ---
3 packets transmitted, 0 received, 100% packet loss, time 2003ms
```

```
pc2:~#
```

3.

instalamos y configuramos easy-rsa.

```
yo:~# cd /hostlab
yo:/hostlab# dpkg -i easy-rsa_2.2.2-1_all.deb
Selecting previously deselected package easy-rsa.
(Reading database ... 30874 files and directories currently installed.)
Unpacking easy-rsa (from easy-rsa_2.2.2-1_all.deb) ...
Setting up easy-rsa (2.2.2-1) ...
Processing triggers for man-db ...
yo:/hostlab# cp -r /usr/share/easy-rsa/ /home
yo:/hostlab# cd /home/easy-rsa/
yo:/home/easy-rsa# vi vars
…
export KEY_COUNTRY="AR"
export KEY_PROVINCE="NQN"
export KEY_CITY="Neuquen Capital"
export KEY_ORG="FAI"
export KEY_EMAIL="franco.ojeda@est.fi.uncoma.edu.ar"
export KEY_OU="FAIREDES"
…
yo:/home/easy-rsa# . ./vars
NOTE: If you run ./clean-all, I will be doing a rm -rf on /home/easy-rsa/keys
yo:/home/easy-rsa# ./clean-all
yo:/home/easy-rsa# ./build-ca
Generating a 2048 bit RSA private key
.............+++
............+++
writing new private key to 'ca.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AR]:
State or Province Name (full name) [NQN]:
Locality Name (eg, city) [Neuquen Capital]:
Organization Name (eg, company) [FAI]:
Organizational Unit Name (eg, section) [FAIREDES]:
```

```
Common Name (eg, your name or your server's hostname) [FAI CA]:
Name [EasyRSA]:
Email Address [franco.ojeda@est.fi.uncoma.edu.ar]:
yo:/home/easy-rsa# ./build-dh
Generating DH parameters, 2048 bit long safe prime, generator 2
This is going to take a long time
.....+.....
    +.....
    +.....
    +.....
    ...+.....
    +.....+....++*++*
```

```
yo:/home/easy-rsa# ./build-key-server "El"
Generating a 2048 bit RSA private key
.....+++
.....+++
writing new private key to 'Yo.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AR]:
State or Province Name (full name) [NQN]:
Locality Name (eg, city) [Neuquen Capital]:
Organization Name (eg, company) [FAI]:
Organizational Unit Name (eg, section) [FAIREDES]:
Common Name (eg, your name or your server's hostname) [El]:
Name [EasyRSA]:
Email Address [franco.ojeda@est.fi.uncoma.edu.ar]:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
Using configuration from /home/easy-rsa/openssl-0.9.8.cnf
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
countryName           :PRINTABLE:'AR'
stateOrProvinceName   :PRINTABLE:'NQN'
```

```
localityName          :PRINTABLE:'Neuquen Capital'
organizationName      :PRINTABLE:'FAI'
organizationalUnitName:PRINTABLE:'FAIREDES'
commonName            :PRINTABLE:'El'
name                  :PRINTABLE:'EasyRSA'
emailAddress          :IA5STRING:'franco.ojeda@est.fi.uncoma.edu.ar'
Certificate is to be certified until Oct  9 20:03:02 2035 GMT (3650 days)
Sign the certificate? [y/n]:y


1 out of 1 certificate requests certified, commit? [y/n]y
Write out database with 1 new entries
Data Base Updated\
yo:/home/easy-rsa# ./build-key "Tu"
Generating a 2048 bit RSA private key
.....................................................+++
.....................+++
writing new private key to 'Tu.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AR]:
State or Province Name (full name) [NQN]:
Locality Name (eg, city) [Neuquen Capital]:
Organization Name (eg, company) [FAI]:
Organizational Unit Name (eg, section) [FAIREDES]:
Common Name (eg, your name or your server's hostname) [Tu]:
Name [EasyRSA]:
Email Address [franco.ojeda@est.fi.uncoma.edu.ar]:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
Using configuration from /home/easy-rsa/openssl-0.9.8.cnf
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
countryName           :PRINTABLE:'AR'
```

```
stateOrProvinceName   :PRINTABLE:'NQN'
localityName          :PRINTABLE:'Neuquen Capital'
organizationName      :PRINTABLE:'FAI'
organizationalUnitName:PRINTABLE:'FAIREDES'
commonName            :PRINTABLE:'Tu'
name                  :PRINTABLE:'EasyRSA'
emailAddress          :IA5STRING:'franco.ojeda@est.fi.uncoma.edu.ar'
Certificate is to be certified until Oct  9 20:04:22 2035 GMT (3650 days)
Sign the certificate? [y/n]:y
1 out of 1 certificate requests certified, commit? [y/n]y
Write out database with 1 new entries
Data Base Updated
yo:/home/easy-rsa/keys#
```

```
yo:/home/easy-rsa/keys# scp ca.crt root@el:/etc/openvpn/ca.crt
root@el's password:
ca.crt                                    100% 5530     5.4KB/s   00:00
yo:/home/easy-rsa/keys# scp El.crt root@el:/etc/openvpn/El.crt
root@el's password:
El.crt                                    100% 5530     5.4KB/s   00:00
yo:/home/easy-rsa/keys#  scp El.key root@el:/etc/openvpn/El.key
root@el's password:
El.key                                     100% 1679     1.6KB/s   00:00
yo:/home/easy-rsa/keys#  scp dh2048.pem root@el:/etc/openvpn/dh2048.pem
root@el's password:
dh2048.pem                                      100% 1679     1.6KB/s   00:00
```

```
yo:/home/easy-rsa/keys#   scp ca.crt root@tu:/etc/openvpn/ca .crt
root@tu's password:
ca.crt                                    100% 5530     5.4KB/s   00:00
yo:/home/easy-rsa/keys# scp Tu.crt root@tu:/etc/openvpn/Tu.crt
root@tu's password:
Tu.crt                                     100% 5530     5.4KB/s   00:00
yo:/home/easy-rsa/keys#  scp Tu.key root@tu:/etc/openvpn/Tu.key
root@tu's password:
Tu.key                                     100% 1679     1.6KB/s   00:00
yo:/home/easy-rsa/keys#  scp dh2048.pem root@tu:/etc/openvpn/dh2048.pem
root@tu's password:
dh2048.pem                                      100% 1679     1.6KB/s   00:00
```

* importante generar la clave del servidor con ./build-key-server y los clientes con ./build-key .

4. configuracion de router El

```
el:/etc/openvpn# vi server.conf
...
#Servidor (completar)
server 10.8.0.0 255.255.255.0
port 1194
proto tcp
dev tun
ca ca.crt
cert El.crt
key El.key
dh dh2048.pem
#
# Rutas
#push "route RED-LOCAL MASCARA"
#client-config-dir clients
    #route RED-REMOTA MASCARA
#
push "route 10.0.30.0 255.255.255.0"
client-config-dir clients
route 10.0.20.0 255.255.255.0


ifconfig-pool-persist ipp.txt
keepalive 10 120
comp-lzo
persist-key
persist-tun
status openvpn-status.log
log openvpn.log
verb 3
…
el:/etc/openvpn# vi clients/Tu
…
iroute 10.0.20.0 255.255.255.0
...
```

En en cliente Tu configuramos el client.conf

```
#client (Completar)
client
port 1194
proto tcp
dev tun
remote 100.50.50.1 1194
ca ca.crt
```

```
cert Tu.crt
key Tu.key
dh dh2048.pem
keepalive 10 120
comp-lzo
persist-key
persist-tun
status openvpn-status.log
log openvpn.log
verb 3
```

Iniciamos openvpn en El y Tu.

```
el:~# /etc/init.d/openvpn start
Starting virtual private network daemon: serverOut of memory: kill process 325 (portmap)
    score 439 or a child
Killed process 325 (portmap)
Out of memory: kill process 538 (openssl-vulnkey) score 322 or a child
Killed process 538 (openssl-vulnkey)
.
el:~# ifconfig
eth0      Link encap:Ethernet  HWaddr aa:bb:cc:00:01:11
          inet addr:100.50.50.1  Bcast:100.50.50.255  Mask:255.255.255.0
          inet6 addr: fe80::58ac:e9ff:fe74:b406/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:6 errors:0 dropped:0 overruns:0 frame:0
          TX packets:6 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:384 (384.0 B)  TX bytes:468 (468.0 B)
          Interrupt:5

eth1      Link encap:Ethernet  HWaddr aa:bb:cc:00:01:12
          inet addr:10.0.30.1  Bcast:10.0.30.255  Mask:255.255.255.0
          inet6 addr: fe80::c0b2:8dff:fee8:8980/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:6 errors:0 dropped:0 overruns:0 frame:0
          TX packets:6 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:384 (384.0 B)  TX bytes:468 (468.0 B)
          Interrupt:5

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:2 errors:0 dropped:0 overruns:0 frame:0
```

```
          TX packets:2 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:100 (100.0 B)  TX bytes:100 (100.0 B)

tun0      Link encap:UNSPEC  HWaddr 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-
    00
          inet addr:10.8.0.1  P-t-P:10.8.0.2  Mask:255.255.255.255
          UP POINTOPOINT RUNNING NOARP MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:100
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)

el:~#
```

```
tu:~# /etc/init.d/openvpn start
Starting virtual private network daemon: clientOut of memory: kill process 325 (portmap)
    score 439 or a child
Killed process 325 (portmap)
Out of memory: kill process 542 (openssl-vulnkey) score 326 or a child
Killed process 542 (openssl-vulnkey)
.
tu:~# ifconfig
eth0      Link encap:Ethernet  HWaddr aa:bb:cc:00:01:06
          inet addr:100.60.60.1  Bcast:100.60.60.255  Mask:255.255.255.0
          inet6 addr: fe80::1cb9:74ff:fee0:1287/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:101 errors:0 dropped:0 overruns:0 frame:0
          TX packets:101 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:12877 (12.5 KiB)  TX bytes:12397 (12.1 KiB)
          Interrupt:5

eth1      Link encap:Ethernet  HWaddr aa:bb:cc:00:01:05
          inet addr:10.0.20.1  Bcast:10.0.20.255  Mask:255.255.255.0
          inet6 addr: fe80::38e5:9dff:fee5:2198/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:6 errors:0 dropped:0 overruns:0 frame:0
          TX packets:6 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:384 (384.0 B)  TX bytes:468 (468.0 B)
          Interrupt:5

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
```

```
        inet6 addr: ::1/128 Scope:Host
        UP LOOPBACK RUNNING  MTU:16436  Metric:1
        RX packets:2 errors:0 dropped:0 overruns:0 frame:0
        TX packets:2 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:0
        RX bytes:100 (100.0 B)  TX bytes:100 (100.0 B)

tun0      Link encap:UNSPEC  HWaddr 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-
    00
        inet addr:10.8.0.6  P-t-P:10.8.0.5  Mask:255.255.255.255
        UP POINTOPOINT RUNNING NOARP MULTICAST  MTU:1500  Metric:1
        RX packets:0 errors:0 dropped:0 overruns:0 frame:0
        TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:100
        RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)

tu:~#
```

Ahora tenemos las interfaces tun0 en El y Tu.

5. Provamos desde pc1 la conexión con pc2 y viceversa.

```
pc1:~# ping -c 3 pc2
PING pc2 (10.0.30.20) 56(84) bytes of data.
64 bytes from pc2 (10.0.30.20): icmp_seq=1 ttl=62 time=21.1 ms
64 bytes from pc2 (10.0.30.20): icmp_seq=2 ttl=62 time=2.39 ms
64 bytes from pc2 (10.0.30.20): icmp_seq=3 ttl=62 time=0.855 ms

--- pc2 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 1998ms
rtt min/avg/max/mdev = 0.855/8.139/21.167/9.233 ms
pc1:~#
```

```
pc2:~# ping -c 3 pc1
PING pc1 (10.0.20.20) 56(84) bytes of data.
64 bytes from pc1 (10.0.20.20): icmp_seq=1 ttl=62 time=0.695 ms
64 bytes from pc1 (10.0.20.20): icmp_seq=2 ttl=62 time=3.21 ms
64 bytes from pc1 (10.0.20.20): icmp_seq=3 ttl=62 time=3.28 ms

--- pc1 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2017ms
rtt min/avg/max/mdev = 0.695/2.398/3.283/1.206 ms
pc2:~#
```