Lab 9: PKI HTTPS PROXY

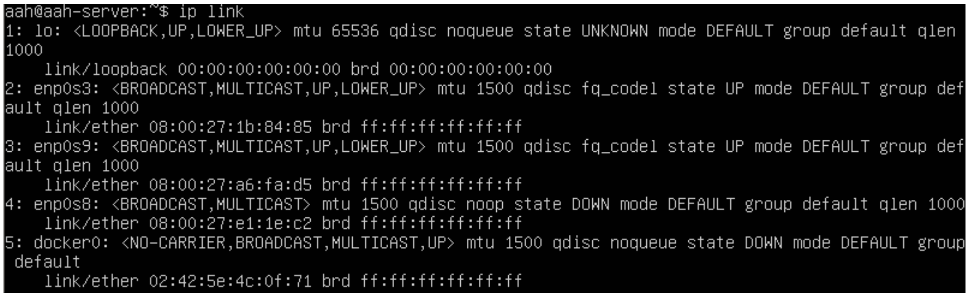
Alexander Hoffmann Sofiane Rahli Yvan Compaore

March 23, 2020

1 Network configuration

1. As we start the PC Router virtual machine, we need to modify the IP configuration. First, enable the interface connected to the internet. To show all the available interfaces, use:

```
ip link
```



```
aah@aah-server:~$ ip link
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN mode DEFAULT group default qlen
1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP mode DEFAULT group def
ault qlen 1000
    link/ether 08:00:27:1b:84:85 brd ff:ff:ff:ff:ff:ff
3: enp0s9: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP mode DEFAULT group def
ault qlen 1000
    link/ether 08:00:27:a6:fa:d5 brd ff:ff:ff:ff:ff:ff
4: enp0s8: <BROADCAST,MULTICAST> mtu 1500 qdisc noop state DOWN mode DEFAULT group default qlen 1000
    link/ether 08:00:27:e1:1e:c2 brd ff:ff:ff:ff:ff:ff
5: docker0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state DOWN mode DEFAULT group
 default
    link/ether 02:42:5e:4c:0f:71 brd ff:ff:ff:ff:ff:ff
```

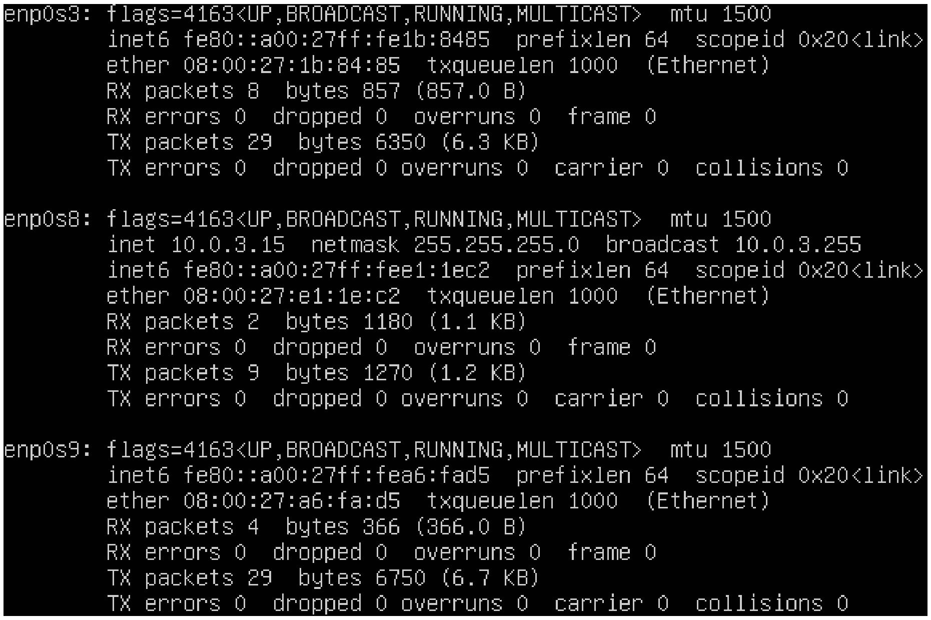
There are 3 ip interfaces that interest us. `enp0s3` and `enp0s9` are host-only adapters. Observe that interface `enp0s8` is down. It corresponds to the NAT interface in the VirtualBox network configuration. We need to enable the interface and assign it an IP address using DHCP.

```
ifconfig enp0s8 up
```

Now the interface is enabled but it does not have an IP address. To ask for a new DHCP lease, use:

```
dhclient enp0s8
```

Now the DHCP sent a lease and the interface now has an IP address and an active internet connection.

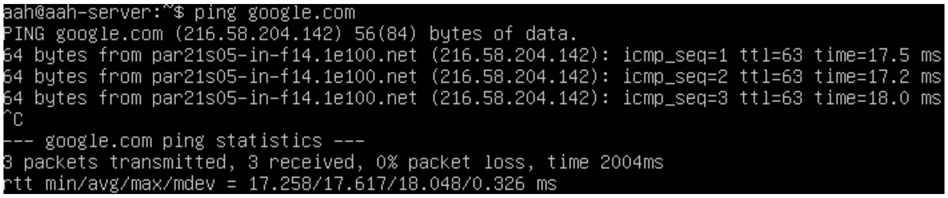


```
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet6 fe80::a00:27ff:fe1b:8485  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:1b:84:85  txqueuelen 1000  (Ethernet)
        RX packets 8  bytes 857 (857.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 29  bytes 6350 (6.3 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

enp0s8: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.3.15  netmask 255.255.255.0  broadcast 10.0.3.255
        inet6 fe80::a00:27ff:fee1:1ec2  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:e1:1e:c2  txqueuelen 1000  (Ethernet)
        RX packets 2  bytes 1180 (1.1 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 9  bytes 1270 (1.2 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

enp0s9: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet6 fe80::a00:27ff:fea6:fad5  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:a6:fa:d5  txqueuelen 1000  (Ethernet)
        RX packets 4  bytes 366 (366.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 29  bytes 6750 (6.7 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

To prove that the VM is connected to the internet, we ping the `google.com` server.



```
aah@aah-server:~$ ping google.com
PING google.com (216.58.204.142) 56(84) bytes of data.
64 bytes from par21s05-in-f14.1e100.net (216.58.204.142): icmp_seq=1 ttl=63 time=17.5 ms
64 bytes from par21s05-in-f14.1e100.net (216.58.204.142): icmp_seq=2 ttl=63 time=17.2 ms
64 bytes from par21s05-in-f14.1e100.net (216.58.204.142): icmp_seq=3 ttl=63 time=18.0 ms
^C
--- google.com ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2004ms
rtt min/avg/max/mdev = 17.258/17.617/18.048/0.326 ms
```

2. Set the IP addresses of the other devices in the network using:

```
ifconfig <interface> <ip-address> netmask <netmask> up
```

To add a default gateway to a network interface, use:

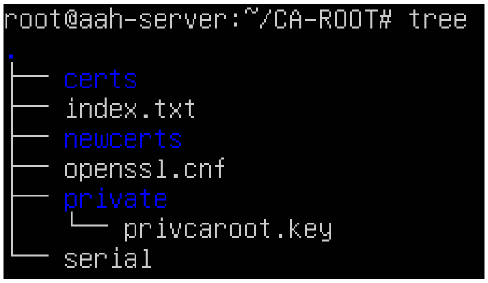
```
route add default gw <ip-address>
```

VM	IP Address
PC1	192.168.11.2
PC2	192.168.22.2
Server	192.168.11.3

2 CA ROOT

1. Connect to PC2.

2. Here is a screenshot of the file structure.



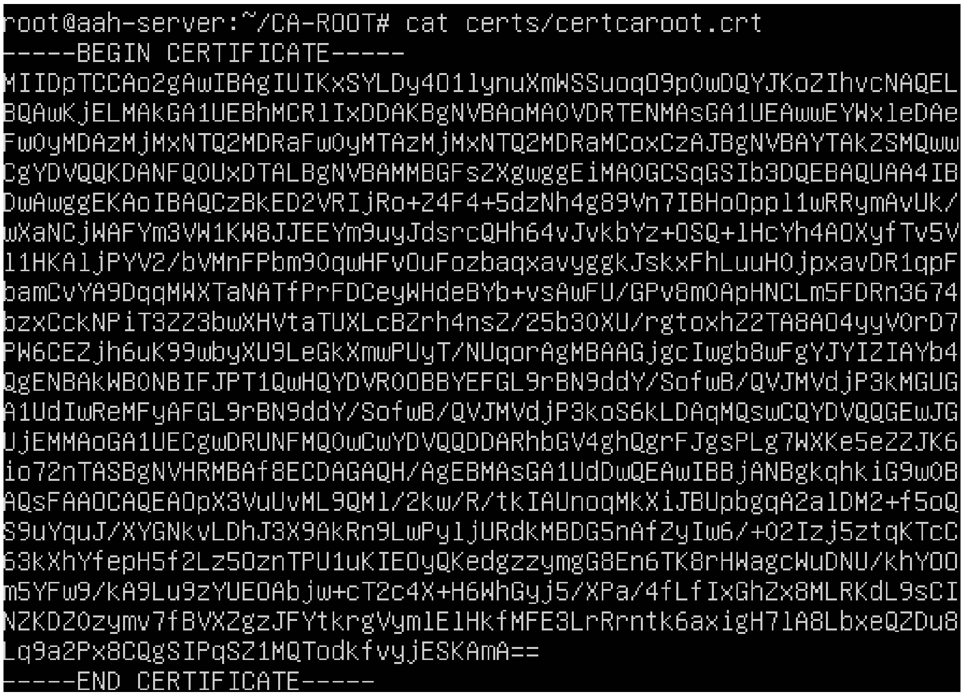
```
root@aah-server:~/CA-ROOT# tree
.
├── certs
├── index.txt
├── newcerts
├── openssl.cnf
├── private
│   └── privcaroot.key
└── serial
```

3. To generate a private RSA key, use:

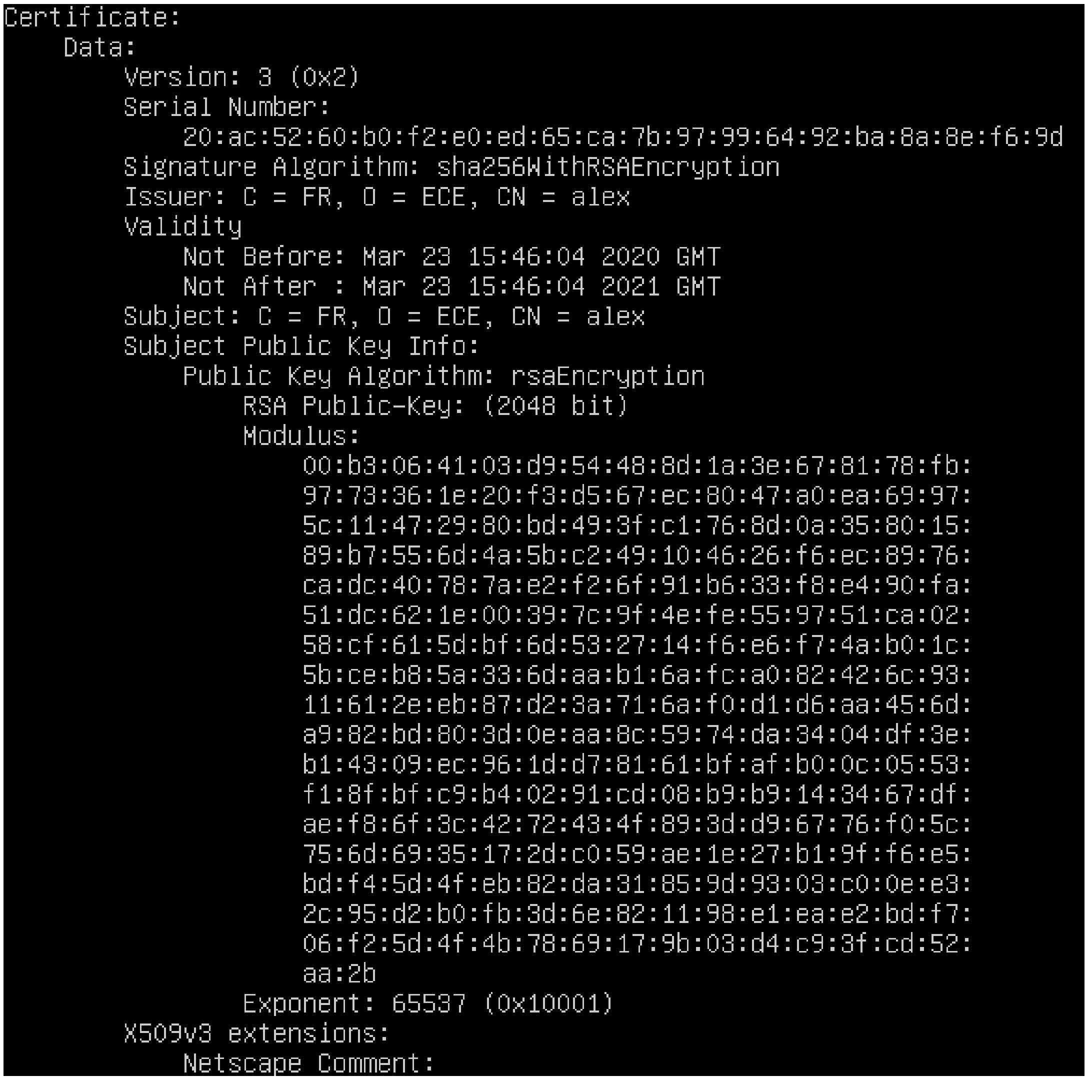
```
openssl genrsa -out privcaroot.key -des3 2048
```

4. To create a self-signed certificate:

```
openssl req -new -x509 -days 365 -key private/privcaroot.key -out
certs/certcaroot.crt -config ./openssl.cnf -extensions CA_ROOT
```



```
root@aah-server:~/CA-ROOT# cat certs/certcaroot.crt
-----BEGIN CERTIFICATE-----
MIIDpTCCAo2gAwIBAgIUIKxSYLDy401lynuXmWSSuoq09p0wDQYJKoZIhvcNAQEL
BQAwKjELMAkGA1UEBhMCR1IxDDAKBgNVBAoMA0VDRTENMAsGA1UEAwwEYWxleDAe
Fw0yMDAzMjMxNTQ2MDRaFw0yMTAzMjMxNTQ2MDRaMCoxCzAJBgNVBAYTAkZSMQww
CgYDVQQKDANFQ0UxDTALBgNVBAMMBGFsZXgwggEiMA0GCSqGSIb3DQEBAQUAA4IB
DwAwggEKAoIBAQCzBkED2VRIjRo+Z4F4+5dzNh4g89Vn7IBHoOppl1wRRymAvUk/
wXaNCjWAFYm3VW1KW8JJEEYm9uyJdsrcQHh64vJvkbYz+0SQ+1HcYh4A0XyfTv5V
l1HKAljPYV2/bVMnFPbm9OqwHFvOuFozbaqxavyggkJskxFhLuuHOjpxavDR1qpF
bamCvYA9DqqMWXTaNATfPrFDCeyWHdeBYb+vsAwFU/GPv8m0ApHNCLm5FDRn3674
bzxCckNPiT3ZZ3bwXHVtaTUXLcBZrh4nsZ/25b30XU/rgtoxhZ2TA8AO4yyVOrD7
PW6CEZjh6uK99wbyXU9LeGkXmwPUyT/NUqorAgMBAAGjgcIwgb8wFgYJYIZIAYb4
QgENBAkWB0NBIFJPT1QwHQYDVR0OBBYEFGL9rBN9ddY/SofwB/QVJMVdjP3kMGUG
A1UdIwReMFyAFGL9rBN9ddY/SofwB/QVJMVdjP3koS6kLDAqMQswCQYDVQQGEwJG
UjEMMAoGA1UECgwDRUNFMQ0wCwYDVQQDDARhbGV4ghQgrFJgsPLg7WXKe5eZZJK6
io72nTASBgNVHRMBAf8ECDAGAQH/AgEBMAsGA1UdDwQEAwIBBjANBgkqhkiG9w0B
AQsFAAOCAQEAOpX3VuUvML9QMl/2kw/R/tkIAUnoqMkXiJBUpbgqA2alDM2+f5oQ
S9uYquJ/XYGNkvLDhJ3X9AkRn9LwPyljURdkMBDG5nAfZyIw6/+O2Izj5ztqKTcC
63kXhYfepH5f2Lz5OznTPU1uKIEOyQKedgzzymgG8En6TK8rHWagcWuDNU/khYOO
m5YFw9/kA9Lu9zYUEOAbjw+cT2c4X+H6WhGyj5/XPa/4fLfIxGhZx8MLRKdL9sCI
NZKDZOzymv7fBVXZgzJFYtkrgVymlElHkfMFE3LrRrntk6axigH7lA8LbxeQZDu8
Lq9a2Px8CQgSIPqSZ1MQTodkfvyjESKAmA==
-----END CERTIFICATE-----
```



```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            20:ac:52:60:b0:f2:e0:ed:65:ca:7b:97:99:64:92:ba:8a:8e:f6:9d
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C = FR, O = ECE, CN = alex
        Validity
            Not Before: Mar 23 15:46:04 2020 GMT
            Not After : Mar 23 15:46:04 2021 GMT
        Subject: C = FR, O = ECE, CN = alex
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                RSA Public-Key: (2048 bit)
                Modulus:
                    00:b3:06:41:03:d9:54:48:8d:1a:3e:67:81:78:fb:
                    97:73:36:1e:20:f3:d5:67:ec:80:47:a0:ea:69:97:
                    5c:11:47:29:80:bd:49:3f:c1:76:8d:0a:35:80:15:
                    89:b7:55:6d:4a:5b:c2:49:10:46:26:f6:ec:89:76:
                    ca:dc:40:78:7a:e2:f2:6f:91:b6:33:f8:e4:90:fa:
                    51:dc:62:1e:00:39:7c:9f:4e:fe:55:97:51:ca:02:
                    58:cf:61:5d:bf:6d:53:27:14:f6:e6:f7:4a:b0:1c:
                    5b:ce:b8:5a:33:6d:aa:b1:6a:fc:a0:82:42:6c:93:
                    11:61:2e:eb:87:d2:3a:71:6a:f0:d1:d6:aa:45:6d:
                    a9:82:bd:80:3d:0e:aa:8c:59:74:da:34:04:df:3e:
                    b1:43:09:ec:96:1d:d7:81:61:bf:af:b0:0c:05:53:
                    f1:8f:bf:c9:b4:02:91:cd:08:b9:b9:14:34:67:df:
                    ae:f8:6f:3c:42:72:43:4f:89:3d:d9:67:76:f0:5c:
                    75:6d:69:35:17:2d:c0:59:ae:1e:27:b1:9f:f6:e5:
                    bd:f4:5d:4f:eb:82:da:31:85:9d:93:03:c0:0e:e3:
                    2c:95:d2:b0:fb:3d:6e:82:11:98:e1:ea:e2:bd:f7:
                    06:f2:5d:4f:4b:78:69:17:9b:03:d4:c9:3f:cd:52:
                    aa:2b
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            Netscape Comment:
```

3 CA LAB

3. Generate private RSA key.

```
openssl genrsa -des3 -out private/privcalab.key 2048
```

4. Generate certificate.

```
openssl req -new -key private/privcalab.key -out certs/certcalab.csr
```

```
-config ./openssl.cnf
```