STI MSI/MSE 2022/2023

Practical Assignment #1 CA + OpenVPN

RULES:

1- Ideally 2 members in a group
2- The work must be defended by both students of the group
3- Inform the teacher regarding the group members

1. Goals

- Configure VPN tunnels in the “network-to-network” and “road warrior” scenarios.
- Enable two-factor user authentication for OpenVPN.
- Manage certification authorities, X.509 certificates and OCSP responders.
- Provide access to a web service through the VPN tunnel.

2. General description

Figure 1 illustrates the scenario considered for our practical assignment. As illustrated, secure communications are supported by VPN tunnels established between remote clients (*road warriors*) and the Coimbra VPN gateway, and between the two VPN gateways (Coimbra and Lisboa). To enable VPN tunnels, we will use OpenVPN (https://openvpn.net).

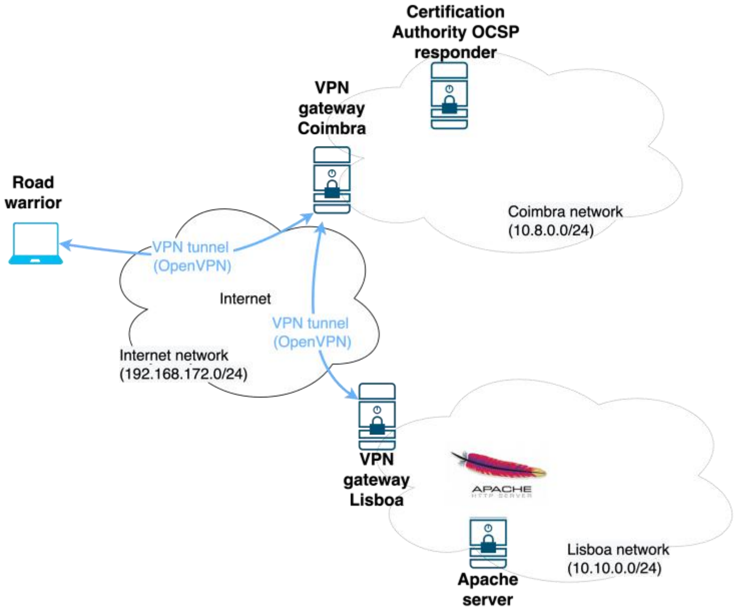
Certification Authority OCSP responder
VPN gateway Coimbra
Road warrior
VPN tunnel (OpenVPN)
Coimbra network (10.8.0.0/24)
Internet
VPN tunnel (OpenVPN)
Internet network (192.168.172.0/24)
VPN gateway Lisboa
APACHE HTTP SERVER
Lisboa network (10.10.0.0/24)
Apache server

Figure 1 – Scenario for the Practical Assignment #1

Coimbra includes an internal network with the following services:

- Certification Authority (CA)
- Online Certificate Status Protocol (OCSP) service

Lisboa also includes an internal network with a web service using Apache, to which the road warriors can connect.

Regarding authentication, all communication entities participating in VPN tunnels (road warriors and the two VPN gateways) should possess valid X.509 certificates, which we will create with a private Certification Authority (CA). The VPN tunnel established between the Coimbra and Lisboa networks is authenticated using X.509 certificates. On the other end, users establishing remote connections to the Coimbra VPN gateway (road warriors) will also use two-factor authentication.

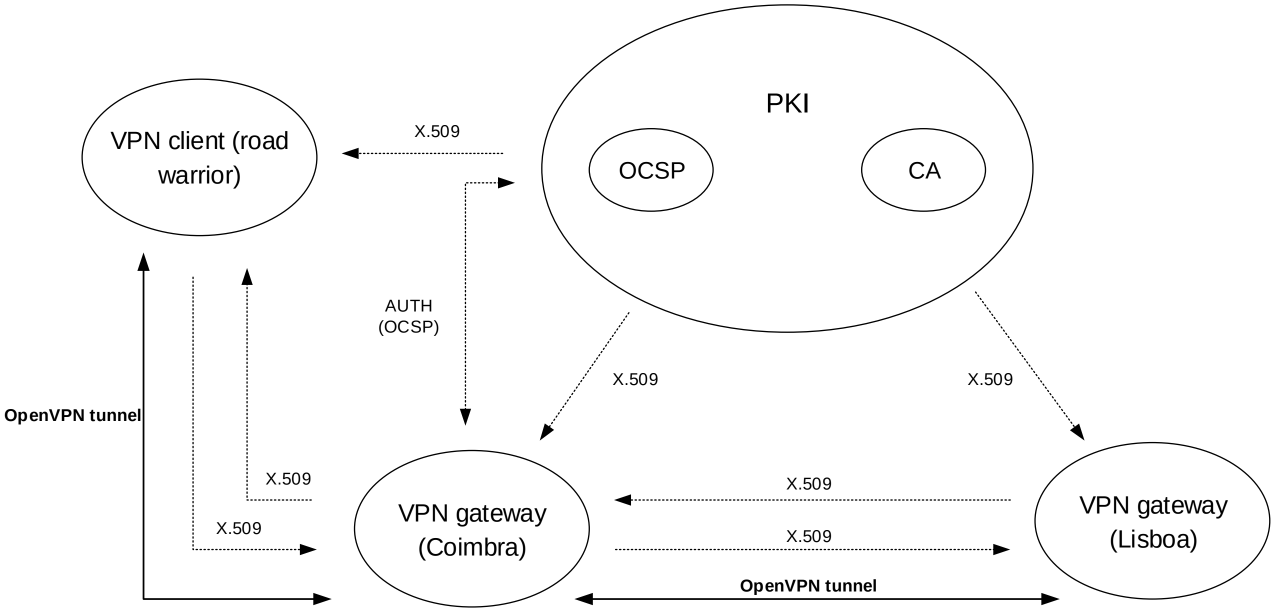

Figure 2 – X.509 mutual authentication and OCSP

As we can observe in Figure 2, the VPN gateways and road warriors must verify the status of validity of certificates using OCSP (Online Certificate Status Protocol). In addition, the road warrior should also be authenticated using two-factor authentication (further details on section 3).

3. VPN tunnels

VPN "network-to-network" tunnel between Coimbra and Lisboa

As illustrated in Figure 1, the Coimbra and Lisboa internal networks are interconnected securely using a VPN tunnel. This tunnel should encrypt communications between hosts on such networks, and communications between remote clients (road warriors) and hosts in the Lisboa network. For instance, between road warrior and the web server apache. The following configuration requirements should be considered in this VPN tunnel:

a) The Coimbra and Lisboa VPN gateways perform mutual authentication using X.509 certificates. Such certificates are created using the private CA, which is configured in the internal network of Coimbra.
b) X.509 certificates are considered valid by the gateways if they have been issued by the private CA and have not been revoked.
c) The VPN tunnel secures communications between the Coimbra and Lisboa networks, and between road warriors and hosts in the Lisboa network (to the web server).

Remote VPN clients (road warriors)

Referring again to Figure 1, remote clients (road warriors) can connect to the Coimbra VPN gateway, and using the tunnel remotely access hosts in the Coimbra and Lisboa networks. The following configuration requirements should be considered:

a) To establish a VPN tunnel with the Coimbra gateway, the road warrior must be in the possession of a valid X.509 certificate, created with the private CA that is configured in the internal network of Coimbra.
b) The road warrior and the Coimbra VPN gateway must perform mutual authentication using X.509 digital certificates.
c) The Coimbra VPN gateway should contact the OCSP responder to obtain the validity status of the X.509 certificate presented by the road warrior. In case the certificate is revoked, the gateway should refuse the connection.
d) To authorize the remote user, the Coimbra gateway should also enforce two-factor authentication: the user must present a one-time password (or authentication token), as described next.
e) The road warrior must be able to connect to the web server in the Lisboa internal network.

Two-factor user authentication

Remote users (road warriors) connecting to the Coimbra VPN gateway are authenticated by a one-time password (authentication token) generated by an appropriate application.

The one-time password may be generated using the TOTP (Time-based One-time Password Algorithm). This algorithm employs a secret key shared between the user and the remote VPN gateway, plus a timestamp (obtained from the current system time), to obtain a one-time password.

To generate a one-time password, the user may use an application such as Google Authenticator, illustrated in Figure 3. This application periodically generates a new one-time password that can be used to authenticate the user with the remote service employing two-factor authentication, in our case, the OpenVPN service supported by the Coimbra VPN gateway. This application is available for iOS and Android [1].

[1] For Android: https://play.google.com/store/apps/details?id=com.google.android.apps.authenticator2&hl=en and for Apple iOS: https://itunes.apple.com/us/app/google-authenticator/id388497605?mt=8

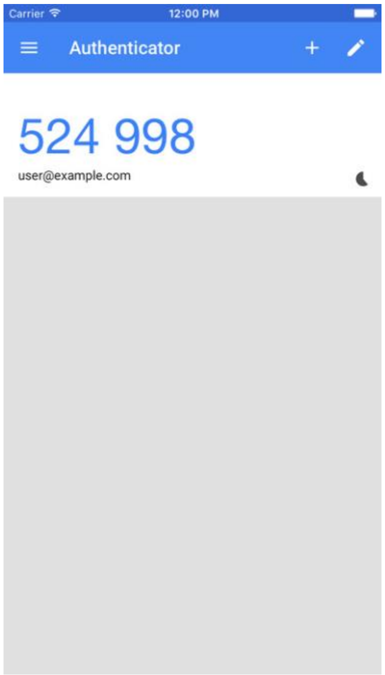

Figure 3 – Google Authenticator app, to generate a one-time password to access services enabled with two-factor authentication

4. Services

Certification Authority

The goal is to use OpenSSL to configure a private Certification Authority, as well as to issue and revoke X.509 digital certificates for the VPN gateways and remote users. The following configuration requirements should be considered:

a) The Certification Authority is used to issue certificates for the VPN gateways (Coimbra and Lisboa) and for remote VPN clients (road warriors).

b) The Certification Authority allows the revocation of certificates previously issued.

c) The Certification Authority also supports a OCSP responder.

Web Server

The goal of the web server is to provide access to web pages using X.509 digital certificates issued by the private Certification Authority. The following configuration requirements should be considered:

a) The server is hosted in the internal network of Lisboa

b) The server should be configured with a valid X.509 certificate issued by the Certification Authority.

5. Delivery of the Practical Assignment

With the assignment, please also deliver a report, containing the following information:

- Descriptions of the configurations for the implementation of the previous requirements (for VPN tunnels and Services).
- A description of how the private Certification Authority was created using OpenSSL.
- A description of how X.509 certificates were issued and revoked using the private Certification Authority.
- A description of the tests performed to validate the functionalities implemented.
- Remaining information considered relevant.

For the delivery of the assignment, put your report, as well as the relevant configuration files, in a single archive (zip format). This archive should be signed using your PGP key and encrypted using the following PGP key:
http://pgp.dei.uc.pt/pks/lookup?op=get&search=0x650e8cc7fe3756a7

Please note that assignments without PGP will **not** be accepted.
The archive file must be submitted to inforestudante in the respective PL class.

Delivery deadline:

- The deadline for the delivery of the assignment (configuration files and report) is **March 11th 2023**.