STI
MEI/MIEBOM

2021/2022

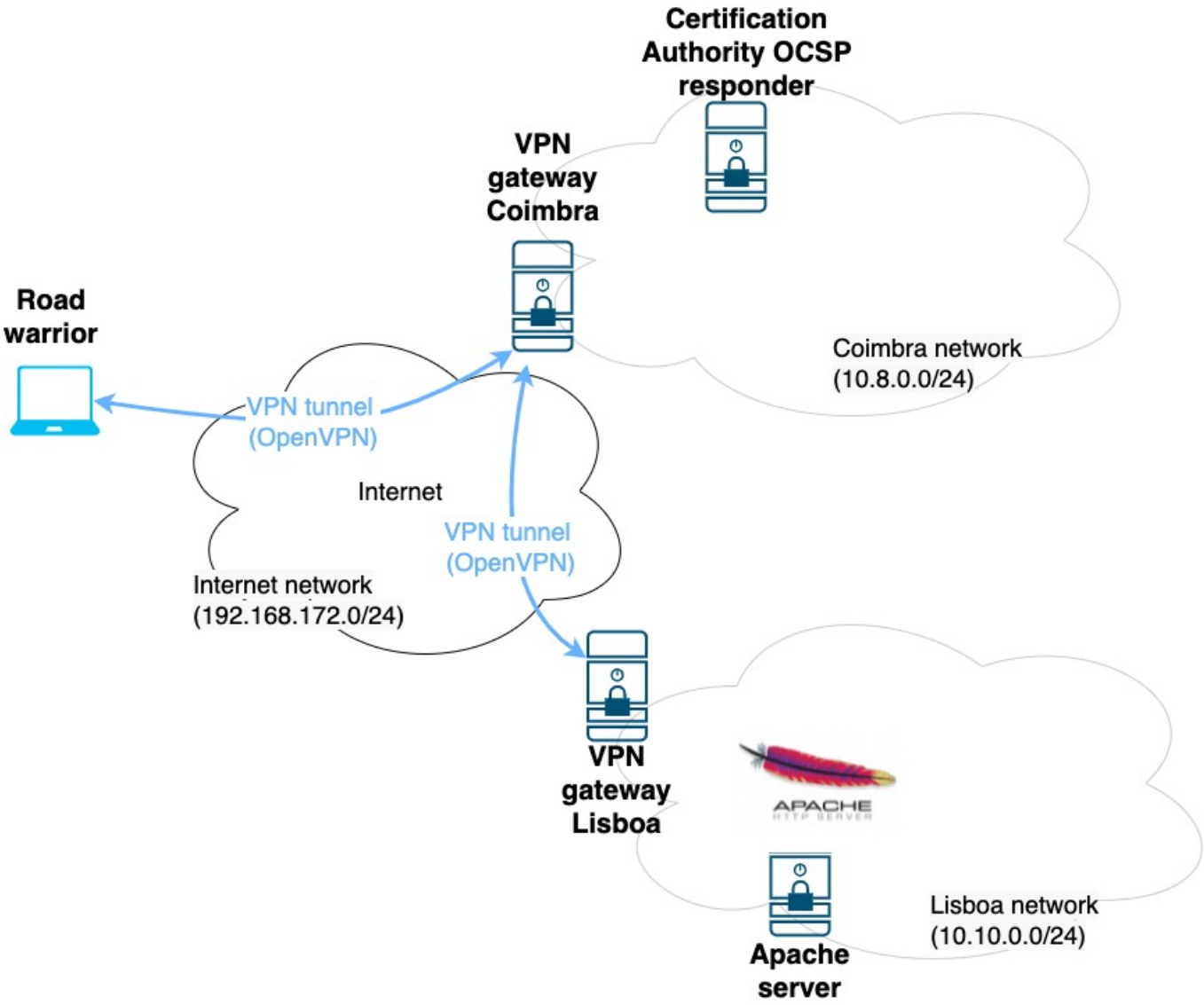
Practical Assignment #1

- VPN scenarios using OpenVPN
- Two-factor user authentication
- X.509 certification authorities and OCSP
- Web server with X.509 certificate

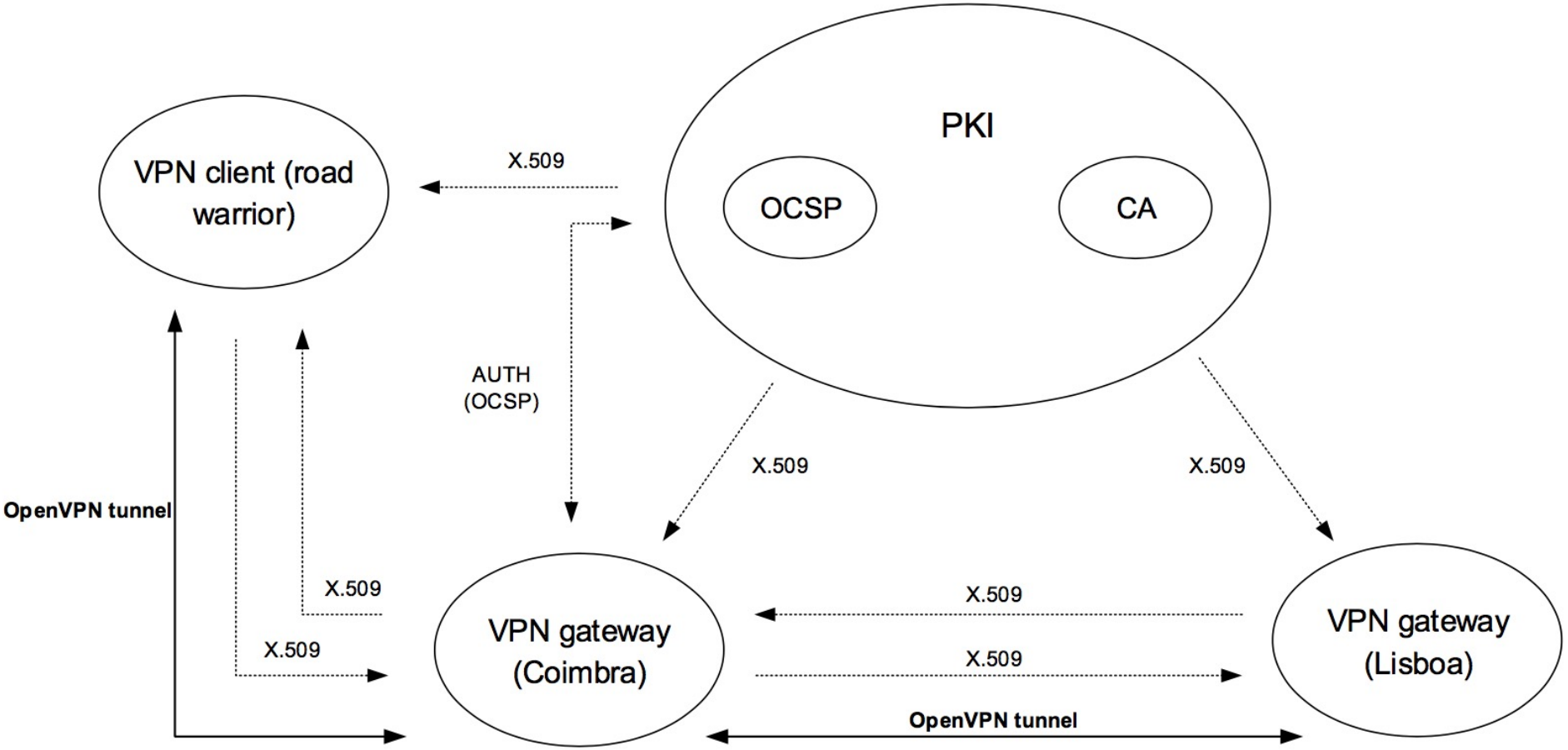
Important:

- Groups of 2 members from the same PL
- Deadline 11/March/2022 (no submissions are allowed after this period)
- Delivery on the respective PL at inforestudante
- Work must be defended by all members of group
- Inform the teacher of your PL regarding the group's members

Scenario


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

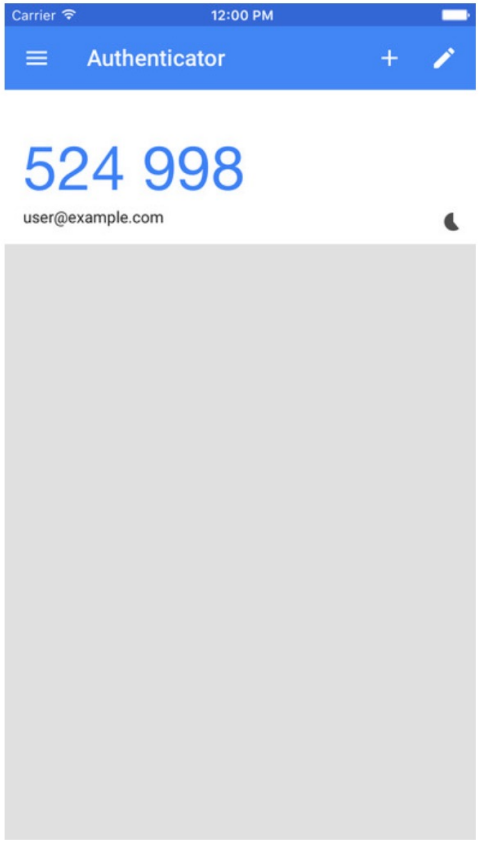
Certification authority and OCSP



Two-factor user authentication

- The user (road warrior) sends a valid account password plus a one-time authentication token to the OpenVPN server

- Generation of a one-time password (according to the TOTP protocol) using, for example, the Google Authenticator app



Practical Considerations

- 3 Virtual Machines:
  1. Road Warrior
  2. Coimbra VPN Server
  3. Lisbon VPN Server

- Services can be binded to the IP in virtual interfaces of VPN Servers belonging to the respective network:
  1. OCSP
  2. Web Server

Example: ifconfig eth0:1 10.8.0.1 netmask 255.255.255.0

Practical Considerations - Routing

- VPN Server of Coimbra
  1. Needs to push routes to the Road Warrior
  2. Needs routing information to the routes of Lisboa network
  3. Need to have IP forwarding activated

     e.g., sysctl -w net.ipv4.ip_forward=1

- VPN Server of Lisbon:
  1. Needs routing information to the routes of Coimbra network