ECOLE POLYTECHNIQUE DE BRUXELLES

IRELE - MA1 Electrical Engineering

ELEC-H417

Report Lab 5
Certificate Authority and NAT

Authors :

Amaury ARICO

Alexis BOLLENGIER

Emmeran COLOT

Sefa GÖNEN

Professor :

Jean-Michel DRICOT

Assistant :

Navid LADNER

Academic year :

2024 - 2025

Contents

0 Mission 0 - Certificate Authority

0.1 Question - Authentication method between PC1 and PC2 before CA

Authentication method between PC1 and PC2 before CA

Explain the authentication method used in the previous lab. On what assumption does this method works ? Why would a certificate be necessary ? How would the authentication procedure work ?

In the previous lab, we used the **Pre-Shared Key Authentication** method : a **secret key** is **shared** between PC1 and PC2 and is used to authenticate both parties before establishing connection. This method works on the assumption that this key is *kept secret* and *shared in a secure way* but more importantly that PC1 and PC2 **agreed on the secret key** (so they already met before).

In the case that a connection between two PCs that **never met**[1] must be established, the *private/public key* cryptography is used. In this approach, a certificate is necessary to prove that the public key is actually owned by the right PC. The authentication procedure would be then based on the certificates : the public key of one entity is encrypted within the certificate. Another entity can have this public key if it decrypts the certificate using the **public key of the certificate authority** (or CA). By trusting the CA, the authentication is validated and the public key can be used to establish connection. This method is based on trust between the receiver/emitter and the CA.

0.2 Question - Importance of clock generation in the CA server

Importance of clock generation in the CA server

Explain the importance of the clock set up in the router.

Every certificate has an **expiration date**. It is important to set up the clock in the router to be able to check that a certificate isn't expired. The figure 1 shows the expiration date of the CA's self-signed certificate. Having a *local* time on the router different from the one on the other devices of the network could lead to it considering an outdated certificate valid or a valid one out of date, which are situations to avoid.

[1] so they didn't agree on a secret shared key before they try to contact each other on an untrusted network

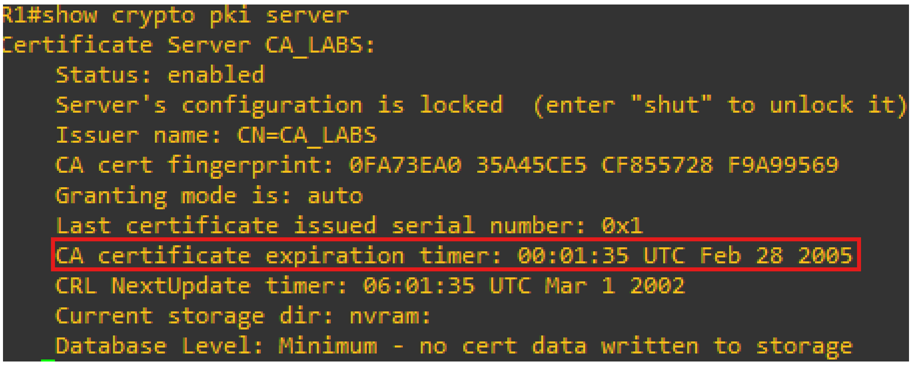

Figure 1: Show `crypto pki server` command result for CA router

0.3 Question - Certificate

Certificate

From the router perspective, will you need to accept the certificate ? Capture the certificate exchange in Wireshark.

From the router perspective, we will need to accept or refuse the certificate depending on the authentication of the CA. In fact, the `crypto pki authenticate TRUSTPOINT_CA_LABS` command is used by the router to authenticate the CA : the CA provides the router its self-signed certificate (which contains the public key of the CA). Once the CA has been authenticated, the router can enroll for certificates from the CA. The figure 2 shows the certificate exchange.

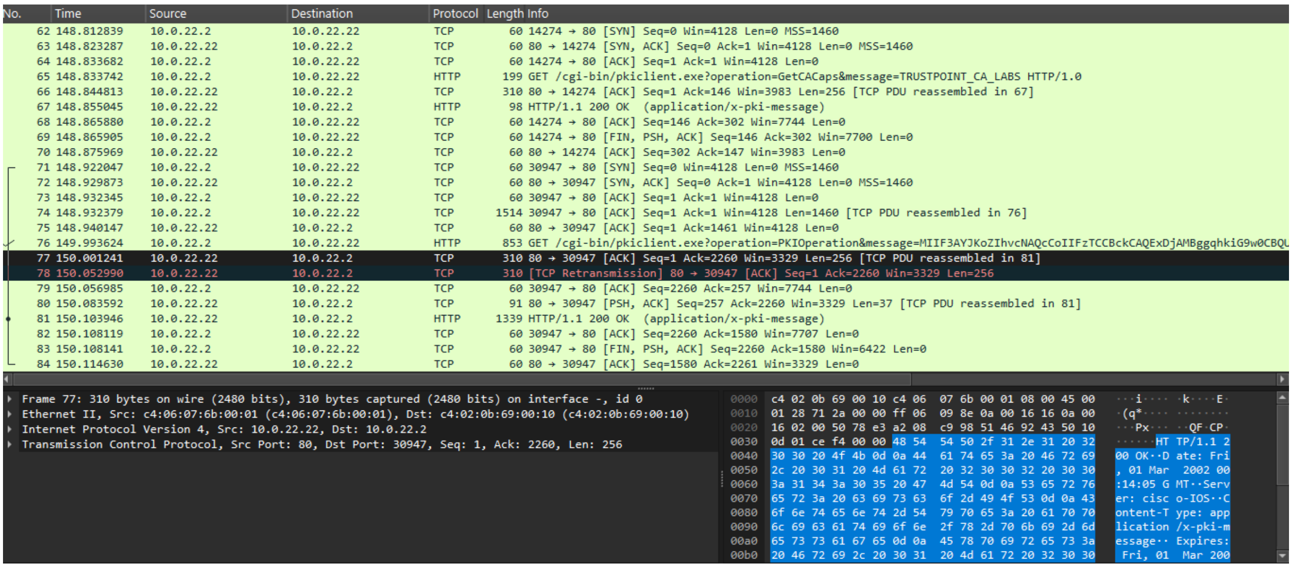

Figure 2: Wireshark capture between CA (10.0.22.22) and Router2 (10.0.22.2) - `crypto pki enroll TRUSTPOINT_CA_LABS` command result

1 Mission 1 - IPsec & VPN (again)

1.1 Question - Diffie-Hellman

Diffie-Hellman

Explain how a DH key exchange protocol works. Show the packets used for the protocol using Wireshark.

The **DH** (Diffie-Hellman) **key exchange protocol** is a protocol used for *securely generating a symmetric cryptographic key over a public channel*[1] and works as following :

- Both entities agree on public parameters (numbers) that don't have to be kept secret.
- They combine their private key with the public parameters, creating public keys.
- Both entities exchange these public keys with each other using the public channel.
- They recombine their private key with the received public key.
- The result is a secret key that both entities possess and wasn't shared at any point in the public channel.

The figures 1.1 and 1.2 show the packets used for the protocol.

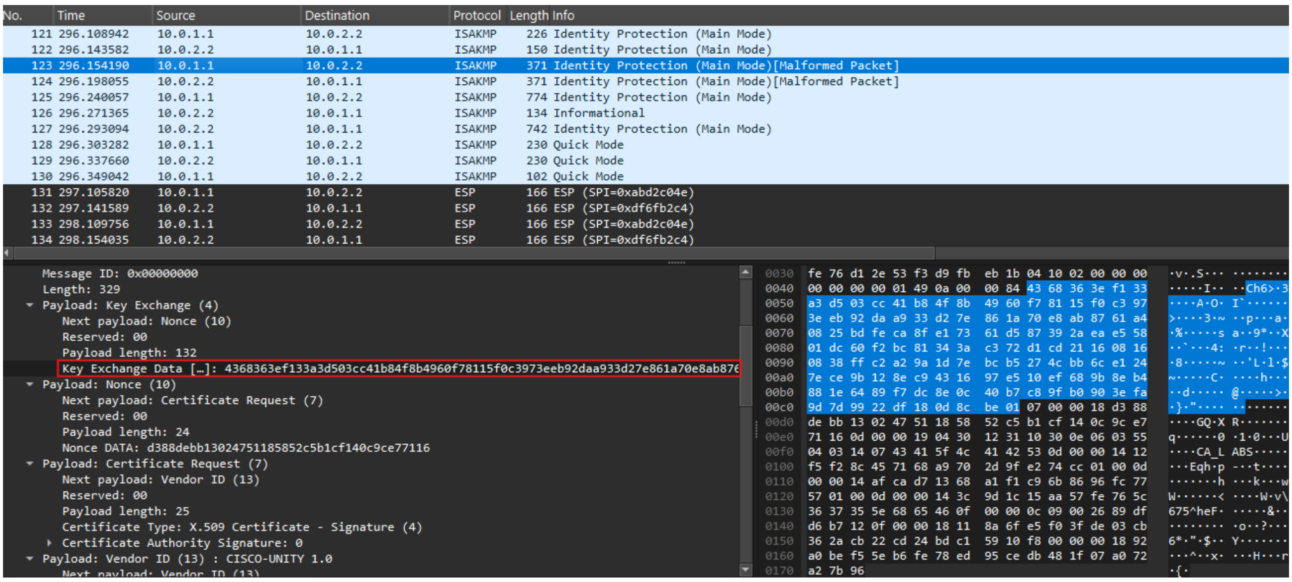

Figure 1.1: Wireshark capture between Router1 (10.0.1.1) and Internet - ping from Linux1 to Linux2 command result. Red frame shows the key exchange data from Router1 to Router2 (10.0.1.1)

[1] Source : `https://en.wikipedia.org/wiki/Diffie-Hellman_key_exchange`

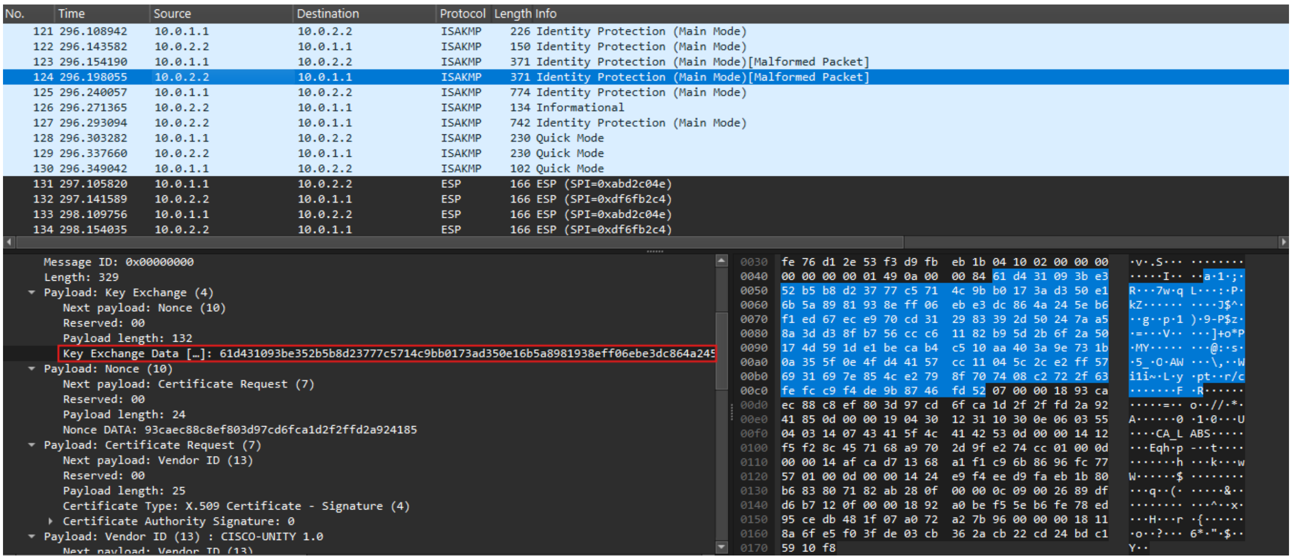

Figure 1.2: Wireshark capture between Router1 (10.0.1.1) and Internet - ping from Linux1 to Linux2 command result. Red frame shows the key exchange data from Router2 (10.0.2.2) to Router1 (10.0.1.1)

2

Mission 2 - NAT

2.1 Question - What is a NAT

What is a NAT

Explain in a few words what is a NAT and how it is suppose to work.

NAT or Network Address Translation is a method used to manipulate the IP address of incoming/outgoing packets in a local network : all devices in a local network **share just one public IPv4 address**. In other words, the NAT changes the IP address of all packets going out of the local network to one source NAT IP address. The port associated to each packet however depends on the source IP and port. The mapping (public IP + public port ⇔ local IP + port) is stored in a table, the NAT table, which is used to forward the incoming packets to the intended receiver.

Incoming packets use the source NAT IP address and the new port number as destination address and destination port number. Then the NAT uses its table to translate this port number to the right local IP address and port number.

2.2 Question - Ping ?

Ping ?

Try to ping using the following commands:

1. **PC3 port 8080 to PC6 port 80**
2. **PC3 port 80 to PC6 port 80**
3. **PC4 port 80 to PC6 port 80**
4. **PC6 port 80 to PC3 port 80**
5. **PC6 port 80 to PC3 port 1111**
6. **PC6 port 80 to Router3 port 1111**
7. **PC6 port 80 to Router3 port 2222**

What do you observe ? Explain the results you see on the terminal and on Wireshark.

1. There is nothing unusual, the packets are showing PC3's IP address, see figure 2.1

2. In this case, the NAT translates the IP of PC3. That's because we are sending the ping requests with source port 80 of PC3 : we've set up the NAT to translate everything coming from PC3 (192.168.3.3) with port number 80 to 10.0.3.3:1111 NAT IP address and port number, see figure 2.2.

3. Again, the NAT translates the IP and port number of the packets to 10.0.3.3:2222 (we've set up it like that in our table).

4. We get a timeout. PC6 expects a response from PC3 (192.168.3.3:80) but it is the translated packet that it receives (10.0.3.3:1111), see figure 2.3.

5. Because we didn't set the port 1111 of PC3 to be translated by the NAT, we get an usual ping command result.

6. This time, we resolve the timeout we got at the 4th point. The ping requests arrive at the router 3 (10.0.3.3:1111) but because of the NAT, the packets are redirected to PC3. So rather than router 3 responding to the ping, we have in fact packets going from router 3 to PC3. This case is similar to the second point.

7. This exactly the same case as before but this time, it is PC4 that responds to the ping requests because in the NAT table, the port 2222 is mapped to PC4 (192.168.3.4:80).

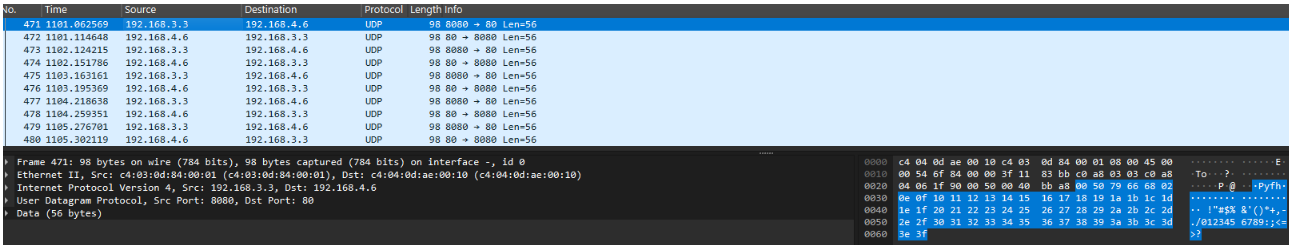

Figure 2.1: Wireshark capture between Router3 (10.0.3.3) and Internet - ping from PC3 port 8080 to PC6 port 80 result

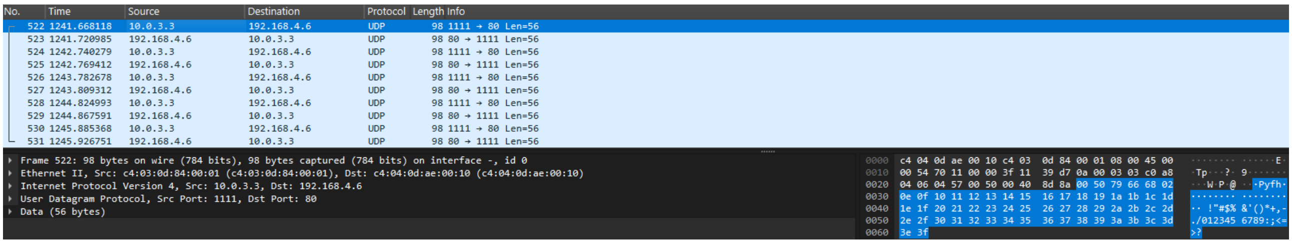

Figure 2.2: Wireshark capture between Router3 (10.0.3.3) and Internet - ping from PC3 port 80 to PC6 port 80 result. The NAT translates 192.168.3.3:80 to 10.0.3.3:1111

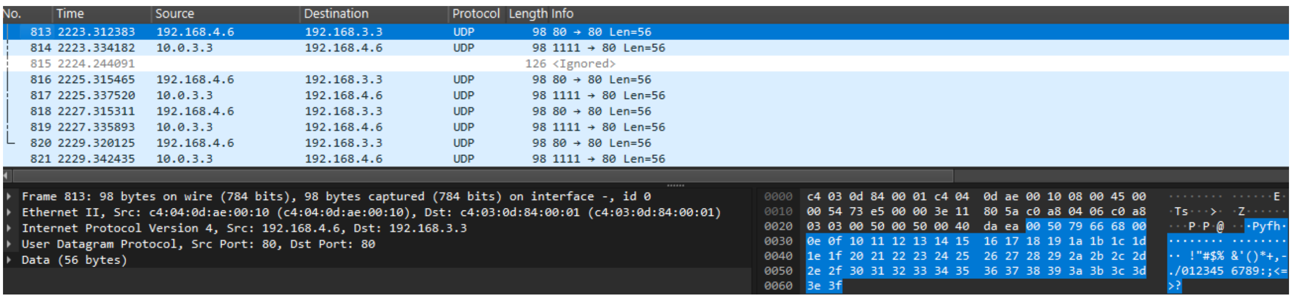

Figure 2.3: Wireshark capture between Router3 (10.0.3.3) and Internet - ping from PC6 port 80 to PC3 port 80 result

2.3 Question - Usage of NAT

Usage of NAT

Explain how a NAT could be useful in terms of security. Develop some advantages and disadvantages.

NAT offers some security benefits. It masks private/local IP addresses, preventing external access. NAT also helps reducing the number of IPv4 addresses (limited number of possible IPv4 Addresses) and with NAT, it is possible to change addresses in the local network without notifying the outside world as well as changing the ISP without changing addresses of the devices in the local network.

However, NAT does have its disadvantages. First, in order to get a packet from some server, you must connect to it at least once. Also, there is a limited amount of ports (64k ports) and the table needs to be cleaned. Moreover, the NAT adds a bottleneck (all traffic goes through the NAT) and a layer of complexity, which can make troubleshooting more difficult. Some protocols, such as Voice over IP (VoIP) or File Transfer Protocol (FTP), may encounter problems with NAT, requiring adjustments.