Université Joseph Fourier Grenoble
Master MiSCiT 2015-2016, durée: 1 heure

Security of networks

N.B. : Calculators are not allowed. Documents are not allowed

FAMILY NAME : _____
FIRST NAME : _____

I. Networks and security

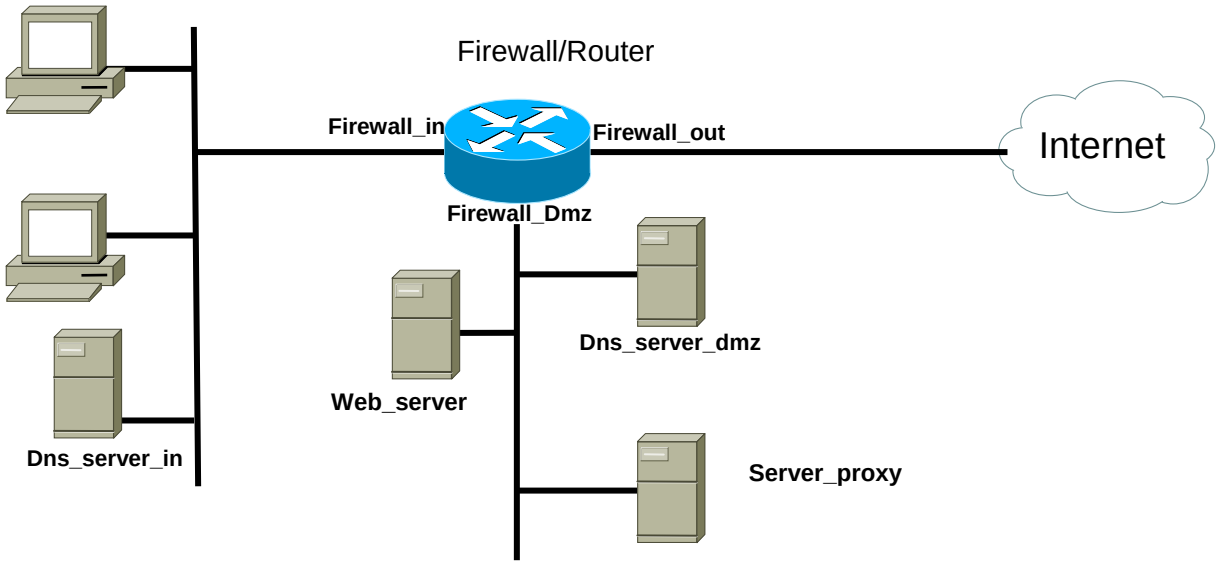
Ex 1 : Firewall

A firewall/router is used at the interface between a corporate network (called "internal network" or "network_in"), and internet. This router/firewall is composed of three interfaces: Firewall_XX.
A DMZ is defined in order to host some servers which can be reached from outside (web, dns…).
You are requested to design a network, around this firewall/router. For that, you will use private IP addressing for the "network_in" and "network_dmz" and we have the public address 137.22.21.207.

1.1 Could you please provide, on the following figure, an IP addressing strategy for the machines and interfaces which are available. The corporate network and the DMZ should use private addresses.

Explain what is the interest to use private addresses…

Explain



Requirements:

In order to run, the following aspects should be taken into account:
- For http: Each machine from the inside network (Network_in) should NOT be able to reach directly any machine outside. The traffic should go through the Server_proxy (you can use the "httpproxy" service or port

number 3128 to reach the proxy and “http” service or port number 80 to reach the final http server). It is considered that the proxy redirection is configured in the client machines. You will have to take care of the infrastructure aspect.
- Each machine from the inside network should be able to ping a machine outside (icmp protocol).
- Each machine from the DMZ network (network_dmz) should be able to ping outside too, but not to ping the Network_In.
- The DNS server from the inside network should be able to reach the DNS server of the DMZ (a set of services called “service_dns” is composed of tcp and udp protocols, on the port 53).
- The DNS server from the DMZ should be able to reach a DNS server outside (IP: 143.210.47.211).

Questions

1.2. Propose translation rules allowing the machines which need it (please define which are the machines which need translation) to be connected on internet. Explain your choices.

We can use a syntax following the example below:

'Source port translated'

Source: IP address of the source machine or of the source network

Port: port (number (ex: 53) or protocol (ex: udp), it is possible to write 'none' or 'any', if necessary)

Translated: public IP address of the machine (or interface) achieving the translation.

Ex:

- 10.3.0.0 http 192.54.10.7
- 172.16.6.0 any 192.27.18.32

P.S. We consider here that the default destination of the translation will be “any”

1.3 Propose filtering rules respecting the **requirements** above. Explain your choices.

We can use the following syntax:

'Protocol source destination service action'

Protocol: type of protocol (we can use 'any' if necessary)

Source: IP address of the source machine or of the source network (we can use 'any' if necessary)

Destination: IP address of the destination machine or of the destination network (we can use 'any' if necessary)

Service: port number (we can use 'any' if necessary). We can also here put a "set of services" (services_intra, services_dns…)

Action: 'pass' or 'block'

Ex:

- tcp 10.3.0.0 172.16.6.0 any pass
- icmp 10.3.0.4 any any block
- any 10.3.0.0 any services_intra pass

Ex 2 : Public and private keys

2.1 A hybrid encryption system is a system combining both the advantages of a symmetrical and an asymmetrical system. Can you please describe what is it and/or how it works?

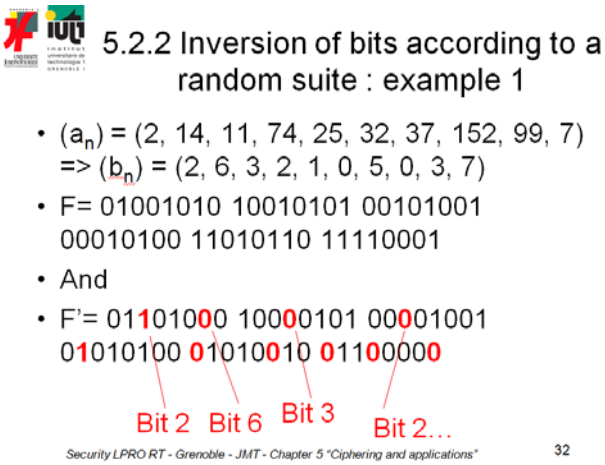
2.2 Two users wants to exchange confidential data in both directions. Can you describe a possible solution in order to succeed? (Please note that several solutions are possible, please focus on one solution, you can of course use the solution proposed in 2.1). Explain clearly how many keys should be used for that and explain clearly the types of keys.

Ex 3 : <u>Encryption: Inversion of bits according to a random suite</u>

Encrypt "Radis" (52 61 64 69 73 in hexadecimal ASCII code) with the random suite $(a_n) = (3, 14, 23, 35, 31, 22, 9, 35, 52, 13…)$ by using the method of the inversion of bits according to a random suite (on 8-bits packets) (if needed, the methodology is recalled below).

Inversion of bits according to a random suite

- Purpose: Transforming each byte of a file F by reversing certain bits by operations of binary negation
- Let's consider a pseudo-random numbers suite (a_n)
- For each byte, the bits to be reversed are obtained by calculating the modulo 8 (8 being the size of the blocks) of the terms of the suite (a_n). The suites of modulo 8-numbers is called (b_n)
- If $b_{n+1} \leq b_n$ then one passes to the following byte => the nbr of bits which are reversed in a byte is random…



Ex 4 : <u>CRC</u>

1) A computer transmits the message 1110 1011 followed by a CRC calculated with the polynomial $G(x)=x^4+x^3+x$.
Calculate the CRC which will be transmitted (give the CRC in a polynomial form).

- **Cyclic codes:**

- Transmitter
  - Data (message): bits suite represented by M(x)
  - The transmitter divides $x^r.M(x)$ by G(x) with G(x) (degree r), generator polynomial
  - $x^r.M(x) = G(x).Q(x) + R(x)$, the maximum degree of R(x) will be r-1
  - Let's transmit the frame $T(x) = x^r.M(x) + R(x)$
- Receiver
  - The receiver divides T(x) by G(x) and should find 0