INGI2347 : Exercises[*]

Lab session 5

Xavier Carpent, Xiao Chen

March 24, 2015

Exercise 1: Design of a corporate firewall

The enterprise Us&L is a small business that organizes lessons in computer science. In addition to the desktop computers, managers have decided to permit the trainees to work directly on their own laptop.
The architecture is depicted on Fig. 1. The prefix allocated to the network is 23.47.0.0/16. This network mainly contains LANs on which desktop computers for trainees are connected. Only two subnetworks of the whole prefix are used for another purpose. The subnetwork 23.47.12.0/24 is used to permit trainees to connect with their own laptop. The subnetwork 23.47.6.0/24 is reserved for the enterprise employees. FW1 and FW2 are two devices that are used for routing and packet filtering. For the sake of simplicity, we will ignore name resolutions (DNS) in this exercise.

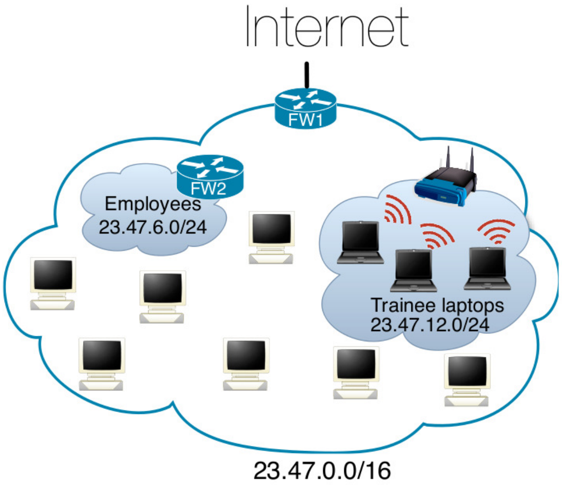

Figure 1: Us&L network architecture

The system administrator defines a list of security policies and actions that have to be implemented in FW1.

1. **Policy:** For any device (even for employees and trainees), connections initiated from the Internet are not allowed. **Action:** Only allow already established connection to the IP prefix of the enterprise.

2. **Policy:** The policies applied to the employees will be implemented on FW2. **Action:** Allow everything from the employee network.

[*] A part of these exercises comes from the book "Computer System Security". The reproduction and distribution of these exercises or a part of them are thus forbidden.

3. **Policy:** Trainee desktops (on which only system administrators are root/admin) can access the Internet (web, e-mail, . . .). However, administrators would like to definitely avoid the use of P2P clients by the trainee desktops. **Action:** The administrator observes that the P2P services he monitors use high ports (e.g., 4662 and 4672 for Emule). Since the users do not have the administration (root) access rights on the desktops, he decides to deny connections to servers on Internet running on unprivileged ports (i.e., ≥ 1024).
4. **Policy:** Trainee laptops must have a limited access to the Internet, they should only have access to the web. **Action:** Only allow HTTP and HTTPS requests (ports 80 and 443) from this subnet.
5. **Policy:** If a trainee computer (either a desktop or a laptop) runs a server (any kind of server), it cannot be accessed by any other trainee computer. **Action:** Connections from the enterprise prefix to the enterprise prefix are not allowed.

Following these policies and actions, the administrator creates the firewall table of FW1. Here is a dump of this table :

```
target prot source         destination
DROP   all  23.47.0.0/16   23.47.0.0/16
ACCEPT all  anywhere       23.47.0.0/16  state ESTABLISHED
ACCEPT all  23.47.6.0/24   anywhere      state NEW,ESTABLISHED
ACCEPT tcp  23.47.0.0/16   anywhere      state NEW,ESTABLISHED tcp dpts:1:1023
ACCEPT udp  23.47.0.0/16   anywhere      state NEW,ESTABLISHED udp dpts:1:1023
ACCEPT tcp  23.47.12.0/24  anywhere      state NEW,ESTABLISHED tcp dpt:80
ACCEPT tcp  23.47.12.0/24  anywhere      state NEW,ESTABLISHED tcp dpt:443
DROP   all  anywhere       anywhere
```

For each policy enumerated above :

- Is the action relevant to the corresponding security policy ? If not, justify. (you do not have to discuss the relevancy of the policy)
- Has the action (even if it is not really relevant) been correctly implemented in the firewall table ? If not, justify. Note that according more rights than needed is not considered correct.

Exercise 2: Filtering Rules for a Stateless Firewall

We consider a stateless firewall whose filtering criteria are based on SYN packets (packets whose SYN flag is 1 and ACK flag is 0). We want the internal network's mail server (128.178.1.1) to be capable of sending and receiving mails, to and from the Internet. Fill in the firewall's filtering rules in the following table.

source	port	destination	port	protocol	SYN	action

Exercise 3: Filtering Rules for a Stateless Firewall

Let us consider a stateless firewall that shelters machine 203.167.75.1. The machine's user wishes to surf the Web, receive telnet connections originating from outside the internal network, as well as receive and initiate SSH connections to and from the Internet. Knowing that HTTP, telnet and SSH servers use ports 80, 23 and 22 respectively, write the firewall's filtering table using filtering criteria based on `SYN` packets (`SYN` flag is 1 and `ACK` flag is 0).

Exercise 4: Stateless vs stateful firewalls

1. Make a quick drawing showing the flags "ack" and "syn" in the first four messages exchanged during a TCP connection.
2. A stateless firewall is a firewall whose filtering is entirely based on packet content. Explain how we can, in stateless firewall, design rules to accept only outgoing connections in a corporate network (in other word, a new connection cannot be initialized from the Internet to our network).
3. Explain how a stateful firewall works. Write down some rules to accept only outgoing connections in a network.
4. *Iptables/Netfilter* (the firewall used on Linux) implements a finite state machine but does not look at TCP flags by default to determine whether a connection is already established. Why do you think implementers made this choice ?
5. What about UDP or ICMP ?

Exercise 5: Filtering Rules for a Stateful Firewall

Consider the architecture given in Figure 2. Let us suppose that the Web server's address is `10.0.0.2` and that the SMTP, HTTP and DNS proxies have addresses `192.168.10.25`, `192.168.10.80` and `192.168.10.53` respectively. The three proxies are used in direct (i.e., towards Internet) and inverse (i.e., from Internet) mode. The Web server must also be accessible from the internal network. We designate all addresses from the proxy zone by `dmz_proxy` and all addresses from the Web server zone by `dmz_web`. Write the filtering table for the external stateful firewall (FW1).

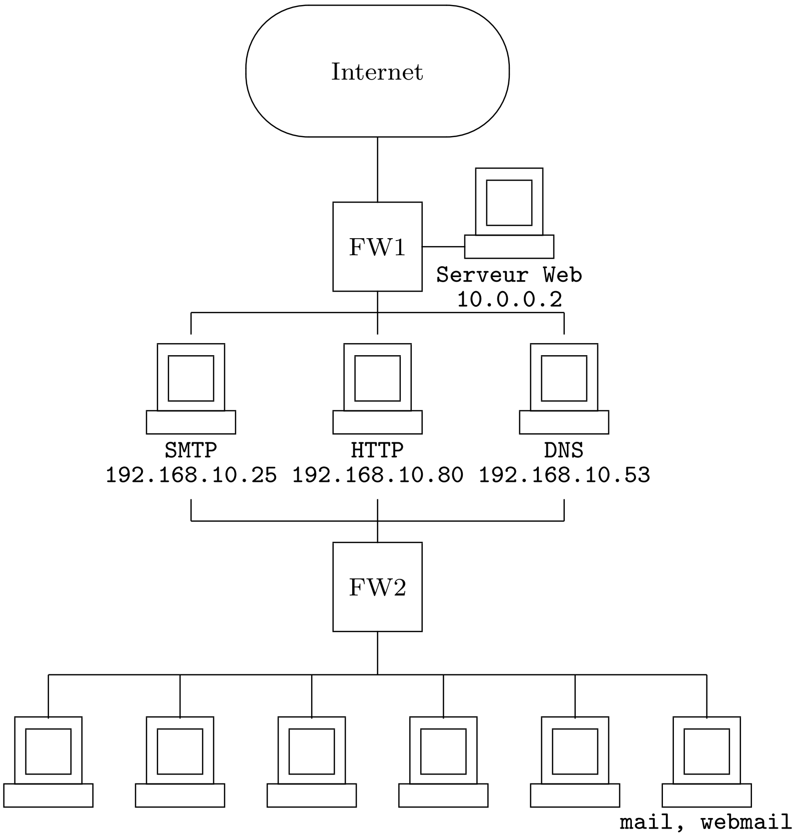

Figure 2: Example of a sandwiched architecture