Assignment: Firewalls

Angelo Spognardi

2017-18

This is an exercise to give you some experience in setting up a set of firewalls which reflect a firewall policy, using a specific rule specification language, `iptables`, available in all modern Linux-based systems, i.e. ones with a Linux kernel version 2.4 or later. This assignment exercise extends some of the simple exercises which you have done previously to cover more requirements and a more complex network, such as you might find in a large high-tech company. You are welcome to consult any sources of information, if this is necessary for you to understand or solve the task described below. However, you should remember to include references to all such material in your report—please note the warning in Section 3 about the inclusion in your report of material which you have not personally written.

1 System Architecture

OneMoreComp is a large high-tech company in the chip industry. The company's administrative headquarters and main research establishment are in Rome. The architecture of the IT system at Rome whose firewalls are to be set up is sketched in Figure 1. This is a split DMZ architecture, with an external DMZ network which

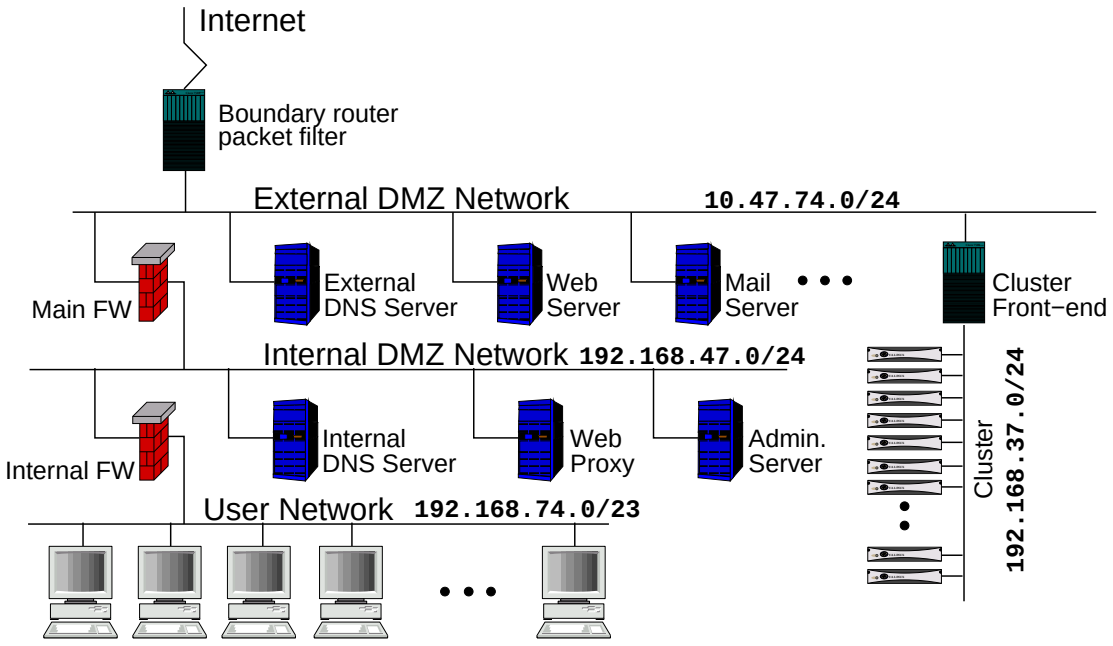

Figure 1: System Architecture

contains a number of servers which are to be accessible from outside the company,

and an internal DMZ network containing servers which are only to be accessible from inside the company. For security reasons, the OneMoreComp does not allow its research or administrative personnel direct access to the internal servers, which may contain highly sensitive company material, from home workplaces. The internal DMZ network also contains an internal firewall, separating it from the protected User Network, on which company employees have their workplace computers. In addition, the external DMZ contains a front-end giving access to a large computer cluster which the company's scientists in all the company's departments (not just at Rome) can use for performing extensive scientific calculations; the front-end acts as a firewall which also performs Network Address Translation (NAT) for the computers in the cluster.

IP addresses are allocated as indicated in the figure:

1. Addresses on the External DMZ Network belong to `10.47.74.0/24`.
2. Addresses on the Internal DMZ Network belong to `192.168.47.0/24`.
3. Computers in the User Network have addresses in the set `192.168.74.0/23`.
4. Computers in the Cluster have addresses in the set `192.168.37.0/24`.

All computers in the system have static IP addresses (i.e. DHCP is not used).

Each of the firewalls has two network interfaces, `eth0` and `eth1`, of which `eth0` faces "outwards" (in the direction of the Internet) and `eth1` "inwards". The IP are assigned as shown in Table 1.

Boundary	`eth0`	`External address`
	`eth1`	`10.47.74.254`
Cluster Front-end	`eth0`	`10.47.74.252`
	`eth1`	`192.168.37.254`
Main FW	`eth0`	`10.47.74.253`
	`eth1`	`192.168.47.254`
Internal FW	`eth0`	`192.168.47.253`
	`eth1`	`192.168.75.254`

Table 1: IP assignment

2 Basic Task

Your basic task is to suggest a set of firewall rules for the Boundary router packet filter, the Main and Internal firewalls and the Cluster front-end, in order to maintain the policy expressed by the following policy rules. It should be noted that the company's full policy is even more complex than this, as it deals with several more services than the ones mentioned below.

1. For the DNS servers:
   (a) User lookups from the Internet are allowed, and should be dealt with by the External DNS Server (assumed to contain all the information which the "outside world" needs to know about OneMoreComp's systems).

(b) The External DNS Server should only permit external systems to resolve names for systems in the External DMZ. Queries from the outside world should therefore not be allowed to reach the Internal DNS Server.
(c) User lookups from the User Network are allowed, and should be dealt with by the Internal DNS Server.
(d) User lookups from the Cluster computers are allowed, and should be dealt with by the External DNS Server.
(e) Zone transfers from the outside world should not be allowed to reach the Internal DNS Server.
(f) Zone transfers from the outside world to the External DNS Server should only be accepted from known trusted servers. (You can define a suitable set of IP addresses for "trusted servers" for yourselves.)

2. For the Web server and proxy:
   (a) HTTP Queries from the Internet should be allowed, and should be responded to by the Web server in the External DMZ.
   (b) HTTP Queries from the User Network go via the HTTP Proxy in the Internal DMZ. This proxy should be able to pass the query on to the relevant HTTP server and pass this server's response back to the source of the original query in the User Network.
3. For the Mail and Admin servers:
   (a) The "Mail server" in the External DMZ offers an SMTP service only, and users in the Internet should be able to use SMTP to send mail to this server.
   (b) The Mail server should forward mail for internal company users via SMTP to the Admin server, and users in the User Network should be able to use POP to fetch mail from this server. To protect the users' passwords, the POP connection to the Admin server should use an SSL-protected channel.
   (c) Users in the User Network use the Admin server as an SMTP proxy for sending mail to internal users and to users in the Internet.
4. For the Cluster:
   (a) In order to send tasks to the Cluster, it should be possible for personnel working at the computers in the User Network or at other company sites (accessible via the Internet) to perform an SSH login to the Cluster front-end and to copy files to and from the front-end using the secure copying (scp) feature of SSH. It should not be possible to login directly to the computers in the cluster.
   (b) Computers in the cluster must be able to send mail in order to keep users informed of the progress of their jobs. For this purpose they need to be able to contact mail servers such as the SMTP server in the External DMZ or SMTP servers out in the Internet. There is no requirement for the cluster computers to be able to fetch or receive incoming mail.
   (c) The front-end must be able to communicate with the cluster computers by using SSH/SCP, and to test the integrity of the cluster network by using ICMP-based testing ("ping").

All services used within the system may be assumed to be offered at the standard "well known" ports assigned by the IANA. If you are in doubt about these, consult `http://www.iana.org/assignments/port-numbers`.

3 Documentation Requirements

Your solution to this assignment exercise must be documented in a short report, which presents and explains the sets of iptables rules which are to be used in:

1. The Boundary router packet filter
2. The Main firewall
3. The Internal firewall
4. The Cluster front-end

in order to satisfy the policies stated in the task description. Each of the four sets of rules should be presented as a shell script containing the appropriate sequence of iptables commands, together with any other shell commands which are necessary. In order to improve the presentation, you are recommended to include comments, explaining what the purpose of the individual groups of commands is, in the shell scripts. (Comments in Linux shell scripts are lines starting with a #-sign. See the examples in the iptables tutorial referred to above.)

You may use variables to define IPs for the servers placed on *Internal DMZ* and *External DMZ*. You can find an example at: `http://www.frozentux.net/iptables-tutorial/scripts/rc.firewall.txt` Using variables has significant advantages:

- The ruleset script is easier to read and understand.
- Modifying IPs for Network entities is simple, you just need to change the value of a variable instead of going through the whole script.
- It reduces the chance of errors due to IP mistyping.

If you are in doubt about the interpretation of some of the requirements, or feel it is necessary to make some assumptions, you should carefully explain what you in fact did and why you believe this was necessary.

Please note: You are welcome to search for advice and ideas in the printed literature and on the Internet. However, any material which you include in your report, and which ***is not your own personal work****, must be clearly marked, and you must give a reference to its source.*

4 Testing environment

A virtual environment that simulates the network described in Section 1 has been prepared and can be found on the web pages of the lecturer[1]. You will be able to use it to test your rules and see whether they actually work or not. As the virtual environment will undergo several testing during the assignment period, it is very likely that it will be updated several times. Each update will be notified in the Google group and the latest version will supersede the previous ones. Then,

[1] `http://people.compute.dtu.dk/angsp/security2017-assignment.html`

check at a regular basis that you are using the latest version in order to reduce the chances of discrepancies between the assignment specifications and the virtual environment.

Instructions on how to set up and use the virtual environment can be found in the lecturer's webpages.

5 Handing in your Report

Your report should follow the usual structure for technical reports, starting with a brief description of the problem being dealt with, followed by a description of the technical solution, finishing with a short conclusion describing what has been done (and what, if any, remains to be done) and a list of references to sources of information that you have consulted (if any). Please try to be as concise and clear as possible.