

## Assignment no. 1 (v.1.0<sup>1</sup>): FIREWALL CONFIGURATION

In this assignment, you have to properly configure the ACME network in the virtual environment of your group and the company firewalls to enforce your ACME's security policy.

In addition, you also have to describe the process you have followed and the type of tests you have performed to check your solution.

If you suspect something is wrong or not as expected, please comment on the Classroom page so that all the students can see and possibly, agree or disagree.

### Hand-in dates

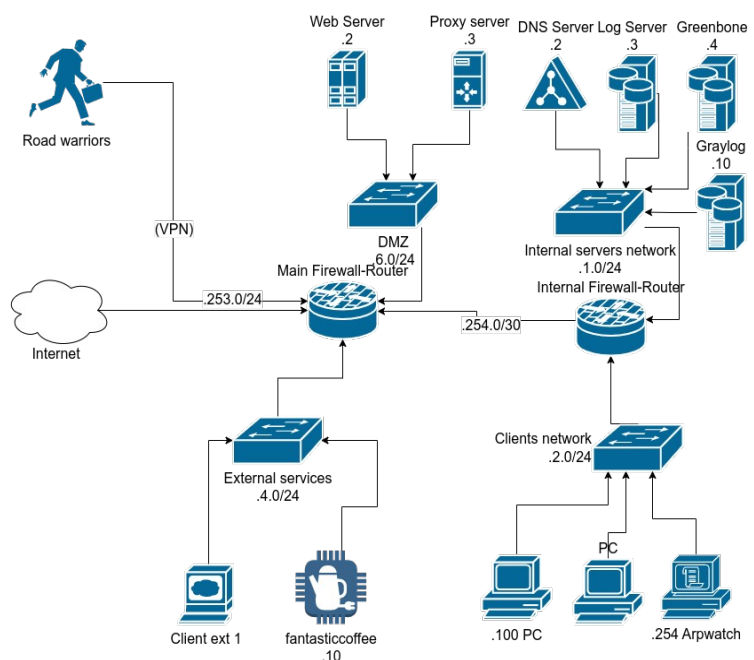
Remember: you must submit the assignment before taking the written exam. The evaluation will consider completeness, clearness, and proficiency.

### SECURITY POLICY ENFORCEMENT

You have to implement the provided security policy properly, configuring the firewall rules of the Main Firewall-Router and the Internal Firewall-Router. Once done, the configurations of the two firewalls should be exported (→backup) and included in the submission package (see later) with the name ACME\_XX\_main.xml and ACME\_XX\_internal.xml.

### SERVICES OF THE ACME co.


1. A web service on the standard ports (in the Web Server host);
2. A DNS on the standard port (in the DNS Server host);
3. A syslog server in the UDP standard port (in the Log Server host)
4. A proxy server (in the Proxy server host). It will be used by the hosts of the ACME network to request connections via HTTP or HTTPS to the Internet and by the Internet hosts;
5. A log collector (in the Graylog host);
6. A vulnerability scanner (in the Greenbone host).
7. A vending machine in the external services network (in the fantasticcoffee host).



To allow complete testing of the policies, you should adequately configure 1. the web service, 2. the DNS, and 3. the syslog service mentioned above, even with a simple setting (e.g., HTTPS page or HTTP redirect to HTTPS for the web service).

### SECURITY POLICY OF ACME co.

- All the ACME hosts must use the internal DNS Server as a DNS resolver.
- The DNS Server should be able to answer DNS requests coming from the Internet.

- The HTTP/HTTPS service provided in the DMZ has to be accessible from the Internet. It can also be accessed using the WAN address of the main firewall.
- The proxy service provided in the DMZ has to be accessible by the hosts of the ACME network and from the Internet.
- Besides the DNS resolver, the other services in the Internal server network must be accessible only to hosts of the Client and DMZ networks.
- All the hosts (but the Client network hosts) have to use the syslog and the log collector services on the Log server (syslog) and Graylog server.
- The Greenbone server must be able to scan all the network hosts.
- All network hosts must be managed via SSH only from hosts within the Client network, so be sure that all the hosts have the SSH service up and running.
- The Client network hosts have only access to external web services (HTTP/HTTPS) through the proxy server in the DMZ.
- Any packet the Main Firewall receives on port 65000 should be redirected to port 80 of the proxy host.
-  • All the internal hosts should use the public IP address of the Main Firewall to exit towards the Internet.
- All the hosts of the ACME network should be able to ping (and receive replies of) the other hosts and the Internet hosts.
- Only hosts in the DMZ should be reachable using the ping and traceroute tools from the Internet.
- ICMP redirect packets should not cross any network.
- Anything that is not explicitly allowed has to be denied.

### **Scheme of your hand-in**

You have to prepare a document that reports the activities you have performed to realize the assignment tasks. The document should be named `ACME_XX_a1_report.pdf` and should be included together with the exported firewall configurations in **one single** .zip file named `ACME_XX_a1.zip`, without any subdirectory, if not needed (i.e., testing scripts). The zip file is the **only thing** your group has to submit in **classroom**, only one of the members.

The document report should be clear and concise (few pages, please...) and have at least the following pieces of information:

1. Group number
2. Student names and numbers
3. Initial brainstorming (where you write your considerations about what to do and how)
4. Evaluation of the security policy
5. Policy implementation in OPNsense
6. Test of the configuration
7. Final remarks