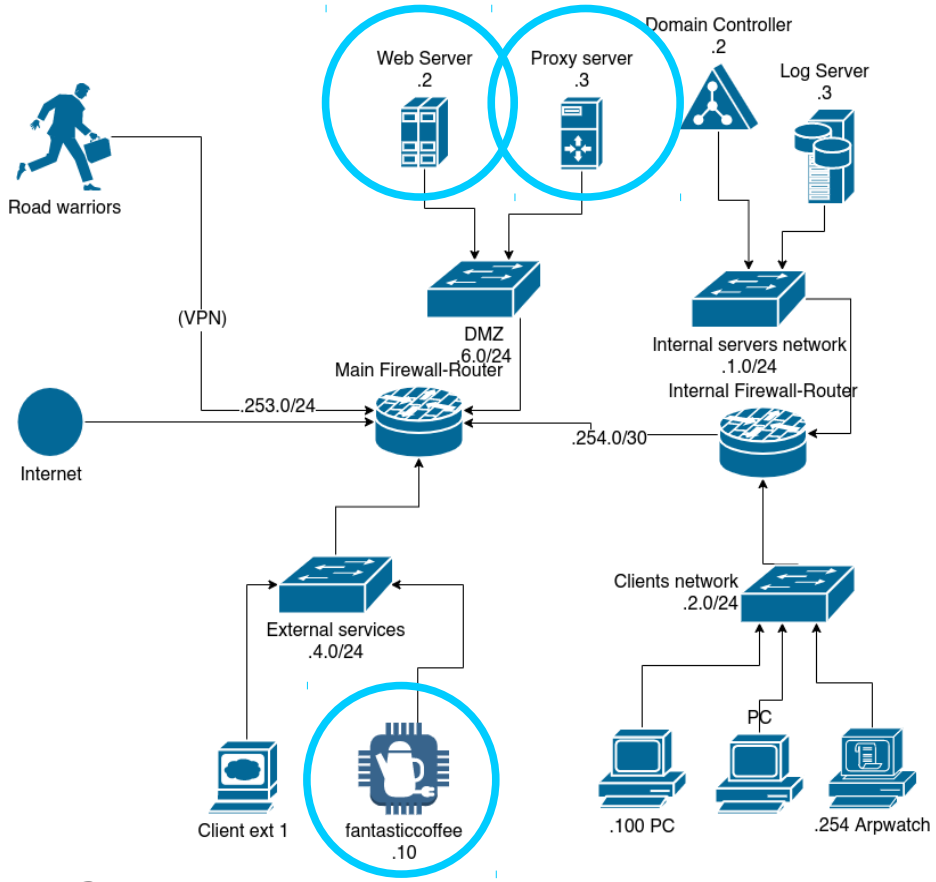
Assignment 3 (v.1.0[1]): proxyes on ACME co.

In this assignment you have to properly configure the services running on the ACME co. networks. In particular, the proxy servers for internal employee and for the external service fantasticcoffee.



SQUID as Forward Proxy

In the DMZ, you have to setup the squid software of the proxyserver host to accept, forward, cache and possibly log the responses of all the HTTP requests coming from the hosts of the ACME co. clients network. HTTPS traffic should go straight to Internet (no TLS bump expected). Clients should not be allowed to navigate in HTTP/HTTPS without using the proxy. Moreover, before accepting their requests, all the clients have to be authenticated using the authentication mechanism you find more suitable. Please, detail your choice in the report. Create at least the three users, namely Nina, Pinta and Maria.

Apache as Reverse Proxy

In the DMZ, you have to configure the webserver apache to act as a reverse proxy to give access to the manufacturer of the ACME's coffee machine (fantasticcoffee), in the External Services network.

Fantasticcoffee machine ONLY uses HTTP and is, very likely, prone to security breaches (→ it has vulnerabilities, 100% guarantee!). Then, you have to secure the coffee machine. For this purpose, a reverse proxy is needed to provide HTTPS support and to limit the access only to the hosts coming from ACME client network.

You have to setup ACME webserver so that it will handle the requests for fantasticcoffee. Use the apache mod_proxy module with TLS settings. Moreover, configure modsecurity[2] in your webserver so that you can filter the requests to be forwarded to the coffee machine: you should only allow requests with proper parameters. Several hints for the configuration can be found in the lab activity of the course (see slides 21-Reverse_proxy_lab.pdf). A possible strategy is:

- reverse engineer the web interface of the coffee machine;

---

1) Last change: 11/05/21

2) Modsecurity handbook: https://www.feistyduck.com/library/modsecurity%2Dhandbook%2D2ed%2Dfree/

- derive the correct parameters;
- set up modsecurity to check the validity of requests.

Please notice that, it is likely that you have to adapt the firewall rules in order to respect the above requirements.

Scheme of your hand-in

You have to prepare a document that reports the activity you have performed to realize the assignment. When uploading your report in classroom, you have also to include the details about how to test the proxy connections of the three accounts above mentioned and the access to the fantasticcoffee services.

The document should be named ACME_XX_a3_report.pdf and should be included together with the configurations of apache, squid the firewalls in a .zip file named ACME_XX_a3.zip. The zip file is the only file your group has to hand-in in classroom (possibly only one of the members). The document 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. Details about squid (the forward proxy) configuration
5. Details about apache (the reverse proxy) configuration
6. Performed tests
7. Final remarks