Practical Network Defense lab access

1 Requirements

In order to access the lab, you need:

- OpenVPN client >= 2.4 (command line client, TunnelBlick for macOS, NetworkManager for GNU/Linux/Gnome, etc)
- A modern web browser (Mozilla Firefox, etc)
- SSH client (on Windows you can use PuTTY)

2 Accessing the lab VPN

In order to access the lab, you can use one of the two VPN profiles that you should have received from us:

- `ACME-00_donaldduck.ovpn`: Primary VPN profile, it uses UDP and the standard OpenVPN port, which might be blocked in some networks (even here in Sapienza);
- `ACME-00_donaldduck_TCP.ovpn`: Backup VPN profile which is configured with a TLS tunnel and a TCP port that should be allowed even in restricted networks (so you can use this if the first one doesn't work)

In order to connect, you can import VPN profiles in your OpenVPN client, or you can launch the profile directly using the command line client:

```
# openvpn ACME-00_donaldduck.ovpn
```

Once connected, you should have a new route in your routing table, for the network `100.64.0.0/12`. If so, the connection is successful.

3 Accessing your VMs

Each group owns an ACME company, which is a set of VMs (see figure 1). The subnet of your company is a `/16` (no NAT or private addresses). The subnet is based on the ACME Id, using this formula: `100.%d.0.0/16` where `%d` is `65 + acmeId` (for example, for ACME 01, the subnet is `100.66.0.0/16`)

The subnet should be reachable by VPN as if you're an external/internet host.

In order to access to the console of VMs, or reboot/shutdown/poweron switches, you need to access to the management panel at the address:

```
https://100.64.0.2:8006/
```

You will receive a warning regarding TLS certificate: you can check the SHA256 fingerprint:

```
A0:89:B2:72:40:A0:67:43:DE:30:53:96:67:AF:87:51:91:6A:BA:A8:22
    :1F:B8:FC:E8:F5:47:33:B8:FB:42:72
```

Default credentials for the web panel are:

- Username: `acme-00`
- Password: `testpwd`
- Realm: `Proxmox VE authentication server`

You must change the web panel password as soon as possible

4 Rules

1. You must not use lab machines for other uses (eg. you must use them only for assignments)
2. You must not interfere with other groups (trying to steal their credentials, log-in in web panel with some other user credentials, etc)
3. You must not interfere with the lab environment itself
4. You must not try to scan/attack other groups or the lab network. You can scan and attack your own machines in the lab.
5. Each issue with the lab (error, data leak, bug, etc) must be reported (and not used to gain advantages)

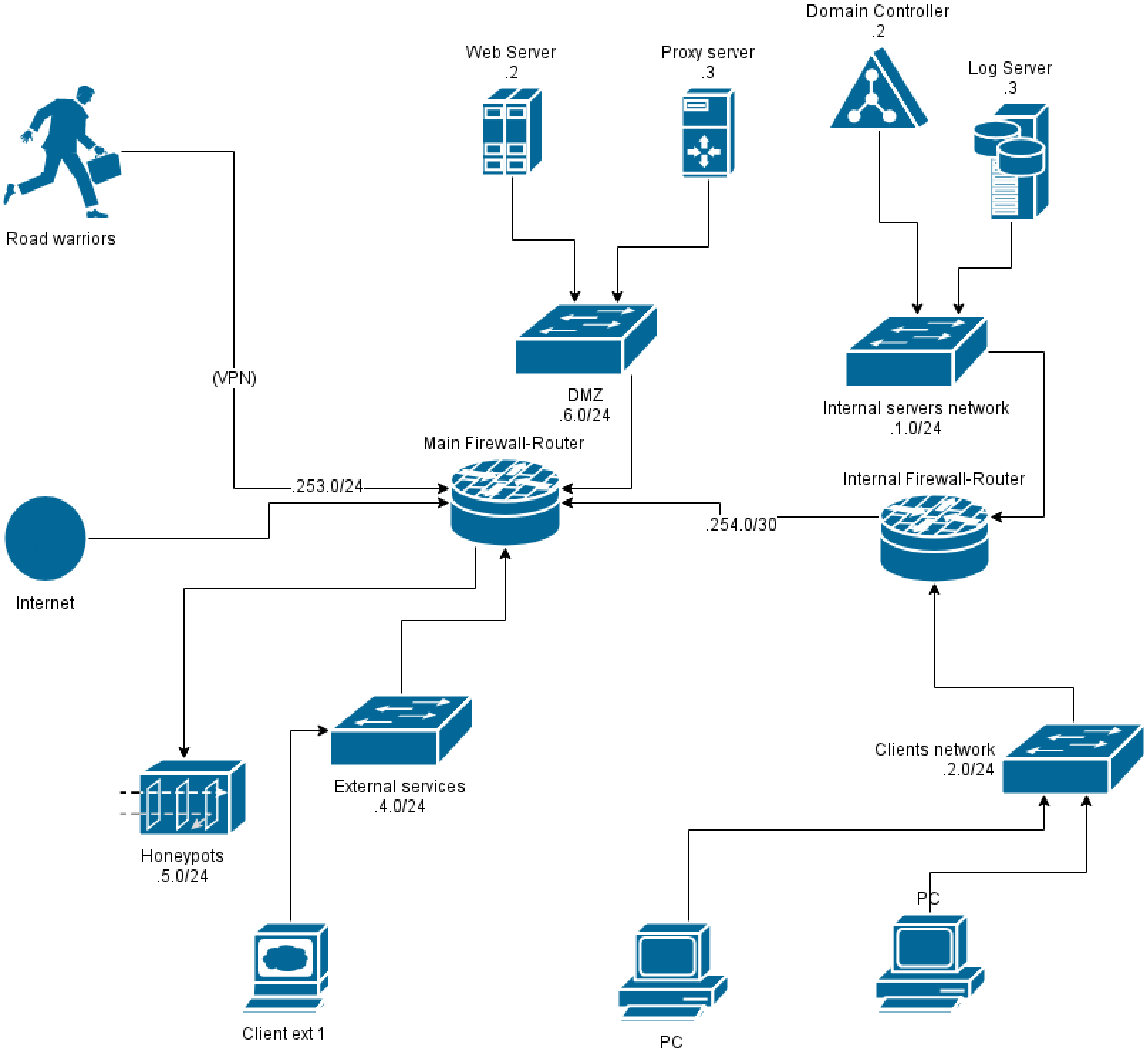

Figure 1: ACME network schema