Assignment 1 (v.1.0[1]): addressing and firewall configuration

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

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

If there is something you suspect is wrong or is not as you expect, please write a comment in the Classroom page, so that all the students can see and, possibly, agree or disagree.

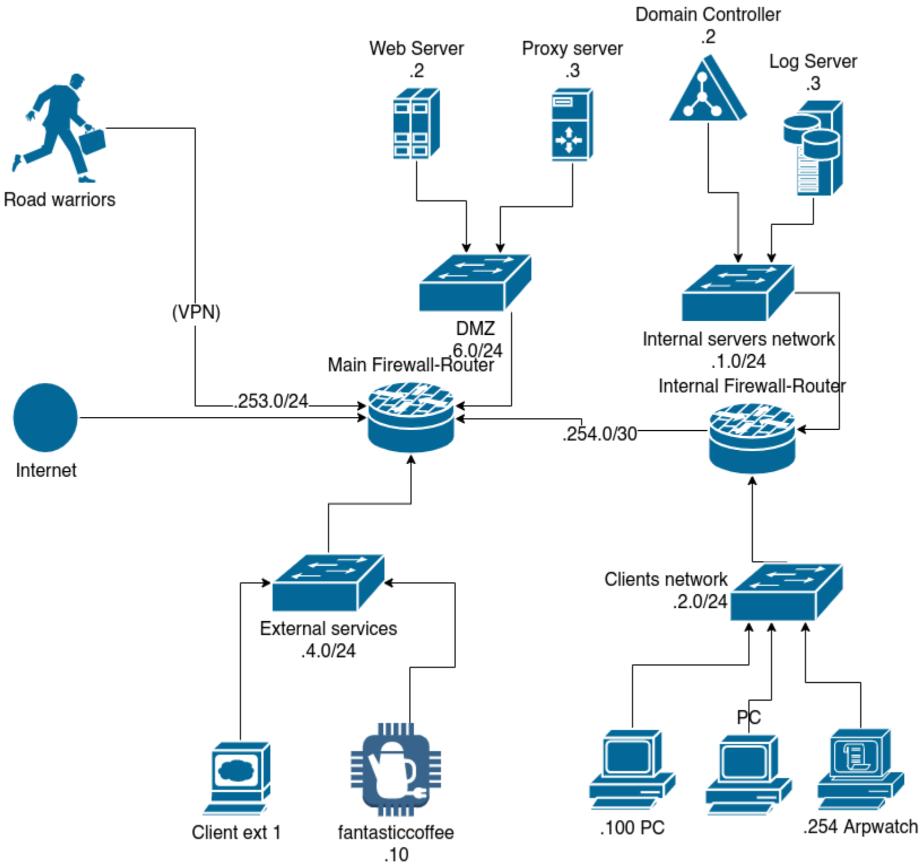
Hand-in dates

The assignment has to be handed-in before taking the written exam. The evaluation will be done considering both the completeness, clearness and proficiency, as detailed in the **Evaluation** section below.

ACME co. topology

The ACME co.'s governance has bought new appliances and hired your group to properly manage and keep safe the new network architecture. They want to introduce IPv6 and, also, enforce a new security policy.

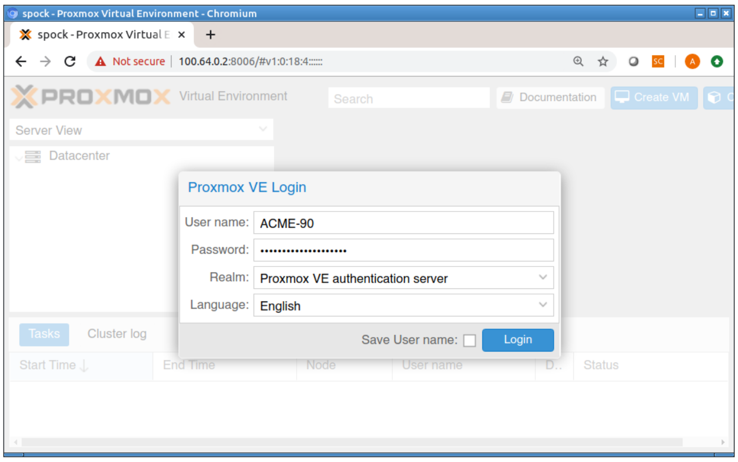
Then, you are responsible for the security of all networks that compose the ACME co.'s topology. A diagram of the whole network topology is shown in the next figure. All the IP address shown in the diagram belong to the network 100.100.0.0/16.



The ACME networks are accessible through the VPN you have received by email. When starting the VPN you will be grant the access to the https://100.64.0.2:8006/ URI, where you can access your proxmox panel, as in Figure 1.

When you enter your credentials, you will be able to access all the hosts in the networks. The control panel of proxmox is represented in Figure 2. When you select a host, you can access its console for using the command line interface or its desktop, depending on the host OS.

[1] Last change: 06/04/20



Proxmox VE Login

User name: ACME-90

Password: ••••••••••••••••••••

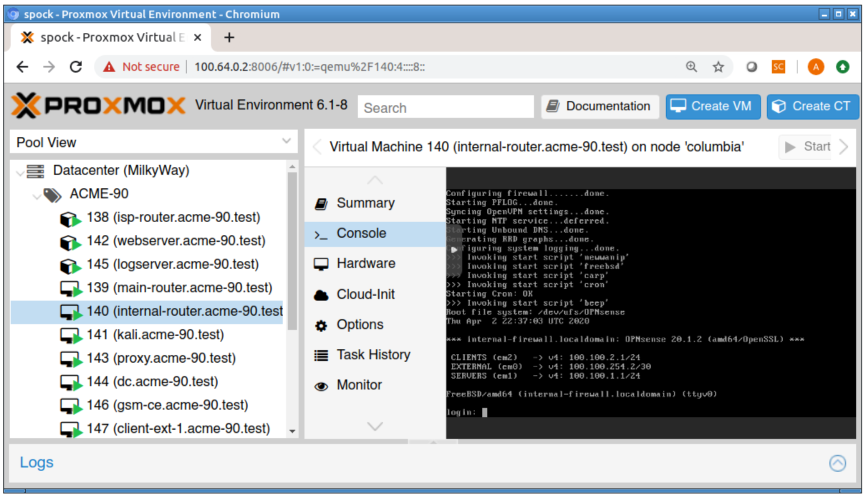
Realm: Proxmox VE authentication server

Language: English

Save User name: □

spock - Proxmox Virtual Environment - Chromium
Not secure | 100.64.0.2:8006/#v1:0:18:4:::::
PROXMOX Virtual Environment
Search
Documentation
Create VM
Server View
Datacenter
Tasks
Cluster log
Start Time
End Time
Node
User name
Status
Login

Figure 1: The proxmox panel for ACME co.



Virtual Machine 140 (internal-router.acme-90.test) on node 'columbia'

```
Configuring firewall.......done.
Starting PFLOG...done.
Syncing OpenVPN settings...done.
Starting NTP service...deferred.
Starting Unbound DNS...done.
Generating RRD graphs...done.
Configuring system logging...done.
>>> Invoking start script 'newwanip'
>>> Invoking start script 'freebsd'
>>> Invoking start script 'carp'
>>> Invoking start script 'cron'
Starting Cron: OK
>>> Invoking start script 'beep'
Root file system: /dev/ufs/OPNsense
Thu Apr  2 22:37:03 UTC 2020

*** internal-firewall.localdomain: OPNsense 20.1.2 (amd64/OpenSSL) ***

 CLIENTS (em2)   -> v4: 100.100.2.1/24
 EXTERNAL (em0)  -> v4: 100.100.254.2/30
 SERVERS (em1)   -> v4: 100.100.1.1/24

FreeBSD/amd64 (internal-firewall.localdomain) (ttyv0)

login:
```

spock - Proxmox Virtual Environment - Chromium
Not secure | 100.64.0.2:8006/#v1:0:=qemu%2F140:4::::8::
PROXMOX Virtual Environment 6.1-8
Search
Documentation
Create VM
Create CT
Pool View
Datacenter (MilkyWay)
ACME-90
138 (isp-router.acme-90.test)
142 (webserver.acme-90.test)
145 (logserver.acme-90.test)
139 (main-router.acme-90.test)
140 (internal-router.acme-90.test
141 (kali.acme-90.test)
143 (proxy.acme-90.test)
144 (dc.acme-90.test)
146 (gsm-ce.acme-90.test)
147 (client-ext-1.acme-90.test)
Summary
Console
Hardware
Cloud-Init
Options
Task History
Monitor
Start
Logs

Figure 2: The console pane of a host in the network.

Some hosts (like the two routers) have to be accessed via their web interfaces. This can be done from your host (if the firewall rules allow it) or from the kali host, that is an internal host with GUI. In the latter case, the best option is to use the SPICE protocol, as described in https://pve.proxmox.com/wiki/SPICE. The other option is to use the VNC client, that is also web based, embedded in the web browser.

Assignment tasks

1. IPv6 addressing

The ISP of ACME co. is IPv6-ready and ready to distribute IPv6 addresses and delegate prefixes to his customers. You have to enable IPv6 on the Main Firewall-Router and enable the prefix redistribution in DMZ network, so that the services exposed to the outside are IPv6-ready. Moreover, you have to properly configure the other sub-networks, according to your network design. Take into account the follow requirements:

- hosts in DMZ should be accessible from outside (namely, their IP can not be random)

- hosts in server network should be accessible from hosts in DMZ (namely, their IP can not be random).

You have to configure the Main Firewall in order to ask the ISP for /56 prefixes. Moreover, you can use the SOLICIT option in order to perform the prefix assignment.

2. Configuring the DNS server

All the internal hosts have to be able to access the internal DNS in the Server network. For this purpose you CAN configure the DNS service in the Domain Controller (dc) machine (100.100.1.2) using zentyal, but alternative DNS services can be considered, since zentyal DOES NOT WORK with IPv6 (!!).

If you want to configure the IPv4 DNS with zentyal, more or less the procedure is the following:

1. From the administrative zentyal portal (https://100.100.2.1:8443), select DNS on the sidebar.
2. Add as forwarders the following IP addresses: 151.100.4.2 and 151.100.4.13
3. Create the domain name for your Acme network.
4. Select the hostnames and the IP addresses your internal DNS should provide (this will also help connecting to the different hosts, yon can use the chosen hostnames).
5. Once done, apply the changes, clicking on the diskette icon on the top right of the page.
6. Open a console and edit the `/etc/zentyal/dns.conf` file, modifying the line with the intnets value as follows: `intnets = 100.100.2.0/24,100.100.4.0/24,100.100.6.0/24`
7. From the administrative portal, select System→Halt/Reboot on the sidebar, then Reboot to make the last change effective.
8. The last step to do is to modify the hosts in the network to use the new DNS server:
   - for the DMZ and the Server network, this will be done by our network admins, once you notify that you are ready for the switch (you can send an email to bassetti@di.uniroma1.it or spognardi@di.uniroma1.it)
   - for the External services and Internal clients networks, you have to disable the Service Unbound DNS in the main and internal firewall, respectively, and add the dc machine IP as the DNS to distribute with the DHCP server

3. Security policy enforcement

The ACME co.'s governance has introduced two new network firewalls, running opnsense. You have to properly implement the provided security policy, 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 hand-in package (see later) with name ACME_XX_main.xml and ACME_XX_internal.xml.

Security policy of ACME co.

- All the host have to use as DNS resolver the internal DNS.
- Only the webserver service provided in the DMZ has to be accessible from the Internet.
- The proxy service provided in the DMZ has to be accessible only from the hosts of the Acme network. However, the proxy needs internet access (see below, section Services of the ACME co.)
- All the services provided by hosts in the Internal server network have to be accessible only by Client network and DMZ hosts.
- Anything that is not specifically allowed has to be denied.
- All the hosts (but the Client network hosts) have to use the syslog service on the Log server (syslog).
- All the host of the network have to be managed via ssh only from hosts within the Client network.
- All the Client network hosts have to only access external web services (http/https).

Services of the ACME co.

- A web service in the standard port (in Web Server host)
- A DNS in the standard port (in Domain Controller host)
- A syslog server in the UDP standard port (in Log Server host)
- A proxy server that can be used by the hosts of the ACME network to request connections via HTTP or HTTPS to external hosts.

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 a .zip file named ACME_XX_a1.zip. The zip file is the only thing your group has to hand-in in classroom (possibly 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. Setup of the infrastructure for IPv6 addressing (here you should detail the steps you've done to properly setup all the hosts. You should also include details and explanation about the network structure you opted for and any difficulties you've faced and –hopefully– solved)
5. DNS configuration
6. Evaluation of the security policy
7. Policy implementation in opnsense
8. Test of the configuration
9. Final remarks