

M11 – Seguretat Informàtica

Pràctica 3. DMZ pfSense

Nil Massó



ASIX 2			
M11 – Seguretat Informàtica – UF1		Tipus	Individual
Cognoms, Nom:	Massó Cabaña, Nil	Curs	2022-23
Observacions:			

Table of Contents

Pràctica 3 – DMZ amb un pfSense.....	1
Exercici 1: Mapa de Xarxa (4 punts).....	1
Exercici 2: Regles del firewall de Xarxa (6 punts).....	4

- A l'hora d'avaluar i qualificar el treball es tindran en compte els aspectes estètics, de correctesa lingüística (sintàctica i ortogràfica) a més del que s'hagi comentat al cicle formatiu sobre la redacció de documentació tècnica i manuals.

- El mòdul professional pertany a uns estudis orientats al món laboral, cosa que fa que un cop complerts els requisits mínims la nota resultant serà condicionada per la quantitat i qualitat del treball individual realitzat per cada alumne.

Pràctica 3 – DMZ amb un pfSense

Objectiu

Configurar un firewall de xarxa per a implementar una DMZ. Establir regles bàsiques de seguretat.

Enllaços

<https://www.ceos3c.com/pfsense/how-to-create-a-dmz-with-pfsense-2-4-2/#step-3-configuring-firewall-rules>

<https://getlabsdone.com/how-to-configure-pfsense-dmz-setup/>

<https://bobcares.com/blog/pfsense-dmz-setup/>

<https://docs.google.com/document/d/19yqQj5GOzNt2YzJuFOnCQeQKN5xBdObuRMirFTmuEmE>

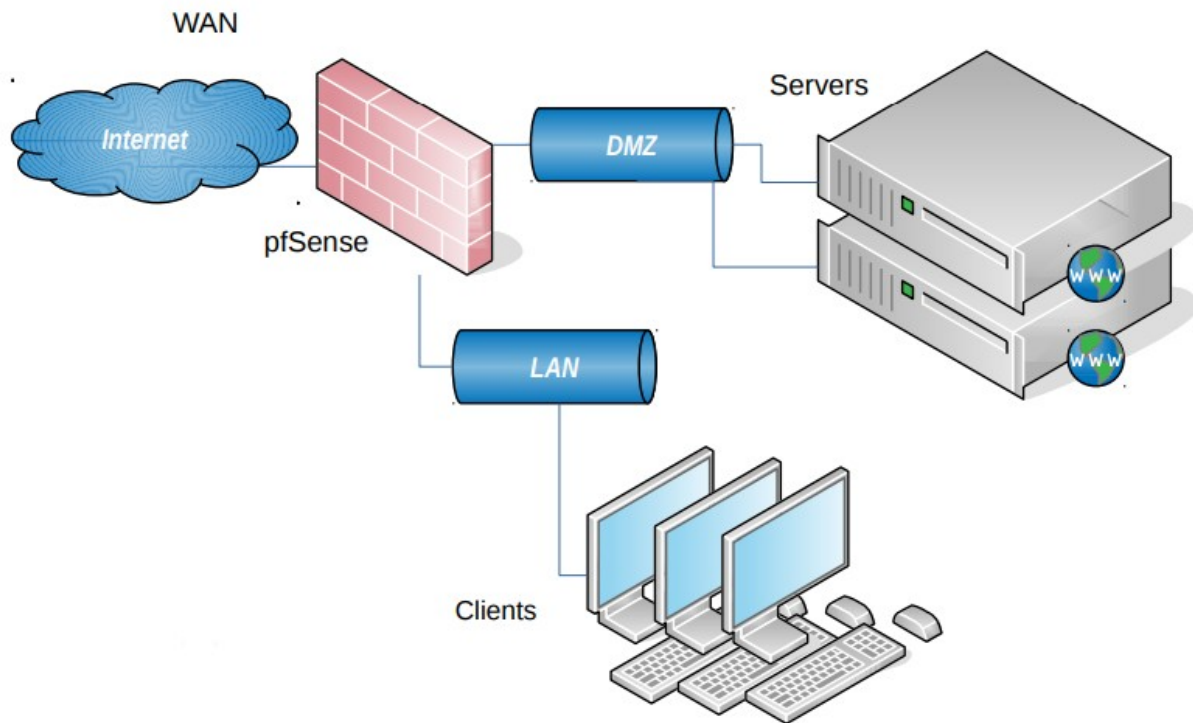
<https://help.ubuntu.com/community/NetworkConfigurationCommandLine/Automatic>

<https://vitux.com/how-to-configure-networking-with-netplan-on-ubuntu/>

<https://youtu.be/lUzSsX4T4WQ?t=387>

Exercici 1: Mapa de Xarxa (4 punts)

La nostra topologia xarxa es basa en una arquitectura de tipus **DMZ** on suposadament el vostre firewall és un hardware dedicat amb el software **PfSense**. La interfície de xarxa **WAN** és la que connecta amb **Internet**, i s'hi fa **NAT** de sortida per a permetre navegar amb una "IP pública" als hosts de les xarxes internes que fan servir adreces IP privades. Hi haurà algun servidor DHCP (per exemple el de la xarxa de l'institut o la de casa vostra) que assignarà adreces als equips de la xarxa WAN. A la interfície de xarxa **LAN** hi penja una xarxa amb com a mínim una màquina, (per exemple un Ubuntu Desktop 20 o equivalent) que agafa l'adreça IP privada de manera automàtica del servidor **DHCP que crea el pfSense**. A la interfície de xarxa **DMZ** hi ha un servidor amb una adreça IP privada estàtica **amb un servidor WEB** funcionant i amb una pàgina WEB de mostra (per exemple un Ubuntu Server 18).



A dins la xarxa WAN, compartint xarxa amb el pfSense, també hi haurà un equip (que pot ser el vostre host en mode bridge) amb diferents serveis instal·lats, així podreu fer més proves. En la meua implementació a casa, en aquesta xarxa (arquitectura SOHO), hi ha un encaminador sense fil que fa de Firewall, de DHCP i de NAT, i que per la seva pròpia WAN connecta amb Internet.

La xarxa on hi teniu la vostra interfície WAN ja us he comentat que és una xarxa amb rang d'adreça privada. **La vostra DMZ és del rang: 10.34.56.16/30**. A nivell de rangs de xarxa LAN, cadascú de vosaltres té el seu rang propi segons la següent taula.

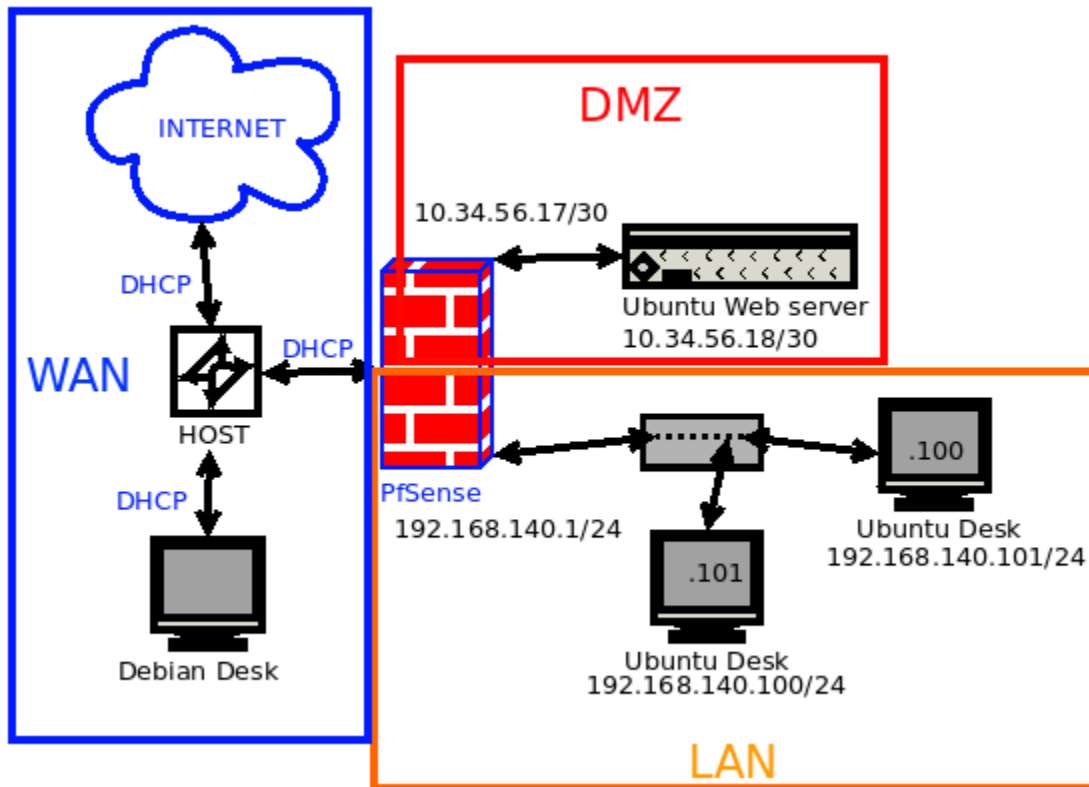
Cognoms, Nom	Xarxa LAN Intranet
Massó Cabaña, Nil	192.168.140.0/24

El mapa que heu de dibuixar ha de seguir els conceptes següents:

- o Hi han de constar els equips de la vostra xarxa DMZ i LAN (0,5 punts)
- o Evidentment cal indicar quina és la part WAN, quina la LAN, quina la DMZ (0,5 punts)
- o També cal dir on s'aplica el NAT i en quin sentit (0,75 punts)
- o Heu de dibuixar el mapa aplicant els vostres rangs IP. Heu d'indicar les IPs de tots els equips dels quals en sabeu (o en podeu saber d'alguna manera) la IP. Podeu inventar-vos IPs sempre i quan siguin del rang que toca i obeeixin les regles de l'exercici. (0,5 punts)
- o Les que són en DHCP també, però només cal que poseu DHCP entre parèntesis al costat. No cal doncs que hi poseu la IP, no sabeu la IP dins del rang assignat de DHCP. (0,25 punts)

- o Hi ha de constar també l'equip que us dic que està a la xarxa WAN (en el meu cas amb SOHO). (0,25 punts)
- o Heu de indicar el "nom" de les màquines (pfsense, ubuntu desktop, ubuntu server, etc). A la part SOHO, podeu indicar quina part és local i quina internet. (0,5 punts)
- o Les interfícies que fan de **default gateway** han de tenir la IP més baixa del rang de xarxa corresponent. (0,75 punts)

Feu l'esquema amb algun programa, si voleu en Windows hi ha el programa Visio, sinó online n'hi ha diversos, com el [Lucidchart](#).



Exercici 2: Regles del firewall de Xarxa (6 punts)

Les regles per les que es regirà la nostra xarxa DMZ són les següents i les haureu d'implementar i demostrar. **Cal una captura de cada regla i una demostració clara de cada regla on es vegin les IPs de la màquina origen i destí.**

He fet servir les IPs que tinc al meu exemple. **Vosaltres feu servir les IPs que escaiguin segons la vostra topologia de xarxa.**

El Pfense funciona fatal, engego les maquines, comprobo que esta tot be, per exemple faig la prova de ping a google i funciona, marxo un moment i cuan torno ja no funciona.

Floating	WAN	LAN	DMZ								
Rules (Drag to Change Order)											
<div></div>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<div><div></div><div>✓</div></div>	0 / 0 B	IPv4 *	*	*	*	*	*	none			<div><div></div><div></div><div></div><div></div><div></div></div>

Floating

WAN

LAN

DMZ

Rules (Drag to Change Order)

States

Protocol

Source

Port

Destination

Port

Gateway

Queue

Schedule

Description

Actions

✓

0 / 0 B

*

*

*

LAN Address

443
80

*

*

Anti-Lockout Rule

⚙

✓

0 / 0 B

IPv4 *

LAN net

*

*

*

*

none

Default allow LAN to any rule

📌

✎

📄

🔄

🗑

✗

0 / 0 B

IPv4 *

*

*

LAN net

*

*

none

📌

✎

📄

🔄

🗑

Floating

WAN

LAN

DMZ

Rules (Drag to Change Order)

States

Protocol

Source

Port

Destination

Port

Gateway

Queue

Schedule

Description

Actions

✓

0 / 0 B

IPv4 *

*

*

*

*

none

Default allow LAN to any rule

📌

✎

📄

🔄

🗑

Des de client intranet NO podem :

- Administrar Firewall amb HTTP (0,5 punts)

HSTS

☒ Disable HTTP Strict Transport Security

When this is unchecked, Strict-Transport-Security HTTPS response header is sent by the webConfigurator to the browser. This will force the browser to use only HTTPS for future requests to the firewall FQDN. Check this box to disable HSTS. (NOTE: Browser-specific steps are required for disabling to take effect when the browser already visited the FQDN while HSTS was enabled.)

The connection has timed out

The server at 192.168.140.1 is taking too long to respond.

- The site could be temporarily unavailable or too busy. Try again in a few moments.
- If you are unable to load any pages, check your computer's network connection.
- If your computer or network is protected by a firewall or proxy, make sure that Firefox is permitted to access the web.

Try Again

webConfigurator

Protocol

☐ HTTP

☒ HTTPS (SSL/TLS)

Des de client intranet **SI** podem accedir a lo que hi ha a la WAN :

- Podem fer ping (0,5 punts):
 - o Cap a l'equip de la xarxa WAN (192.168.1.0/24, 172.202.20.0/24))

```
nil@UD:~$ ping 192.168.122.1
PING 192.168.122.1 (192.168.122.1) 56(84) bytes of data.
64 bytes from 192.168.122.1: icmp_seq=1 ttl=64 time=0.851 ms
64 bytes from 192.168.122.1: icmp_seq=2 ttl=64 time=0.468 ms
64 bytes from 192.168.122.1: icmp_seq=3 ttl=64 time=0.601 ms
^C
--- 192.168.122.1 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2048ms
rtt min/avg/max/mdev = 0.468/0.640/0.851/0.158 ms
```

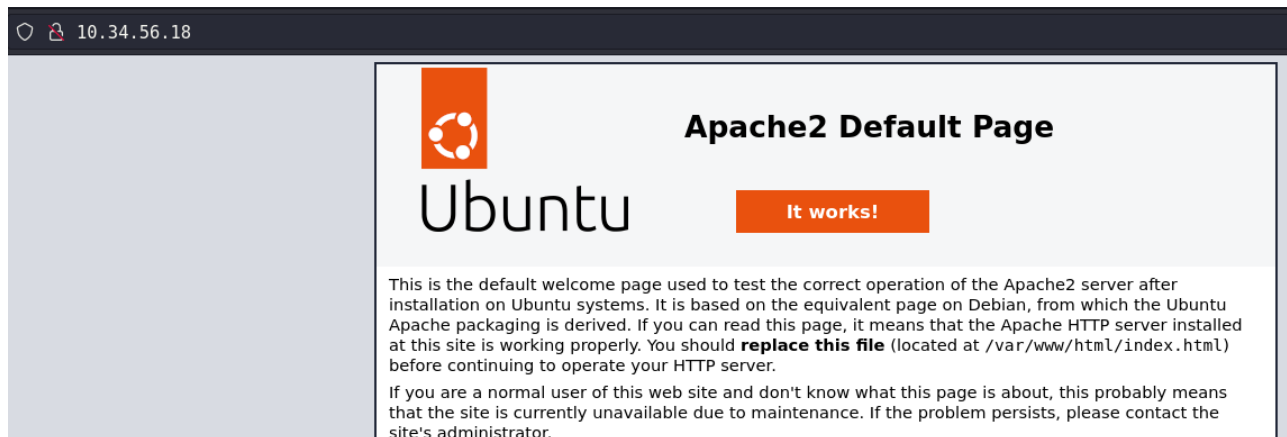
- o Cap al Servidor web DMZ

```
nil@UD:~$ ping 10.34.56.18
PING 10.34.56.18 (10.34.56.18) 56(84) bytes of data.
64 bytes from 10.34.56.18: icmp_seq=1 ttl=63 time=2.15 ms
64 bytes from 10.34.56.18: icmp_seq=2 ttl=63 time=2.53 ms
64 bytes from 10.34.56.18: icmp_seq=3 ttl=63 time=2.02 ms
^C
--- 10.34.56.18 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 2.021/2.235/2.536/0.225 ms
```

- o Cap al servidor que està a www.google.com

```
nil@UD:~$ ping www.google.com
PING www.google.com (142.250.185.4) 56(84) bytes of data.
64 bytes from mad41s11-in-f4.1e100.net (142.250.185.4): icmp_seq=1 ttl=111 time=45.3 ms
64 bytes from mad41s11-in-f4.1e100.net (142.250.185.4): icmp_seq=2 ttl=111 time=20.1 ms
64 bytes from mad41s11-in-f4.1e100.net (142.250.185.4): icmp_seq=3 ttl=111 time=20.5 ms
64 bytes from mad41s11-in-f4.1e100.net (142.250.185.4): icmp_seq=4 ttl=111 time=47.2 ms
^C
--- www.google.com ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 4345ms
rtt min/avg/max/mdev = 20.114/33.300/47.253/13.011 ms
```

- Podem navegar pel servidor WEB DMZ (0,5 punts)



- Connectar via SSH amb servidor WEB DMZ (0,5 punts)


```

nil@UD:~$ ssh nil@10.34.56.18
The authenticity of host '10.34.56.18 (10.34.56.18)' can't be established.
ECDSA key fingerprint is SHA256:K7bodysaJoQJ8kZozo+NxHL75q2SFyCOTr6/q2X7prM.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.34.56.18' (ECDSA) to the list of known hosts.
nil@10.34.56.18's password:
Welcome to Ubuntu 22.04.1 LTS (GNU/Linux 5.15.0-58-generic x86_64)

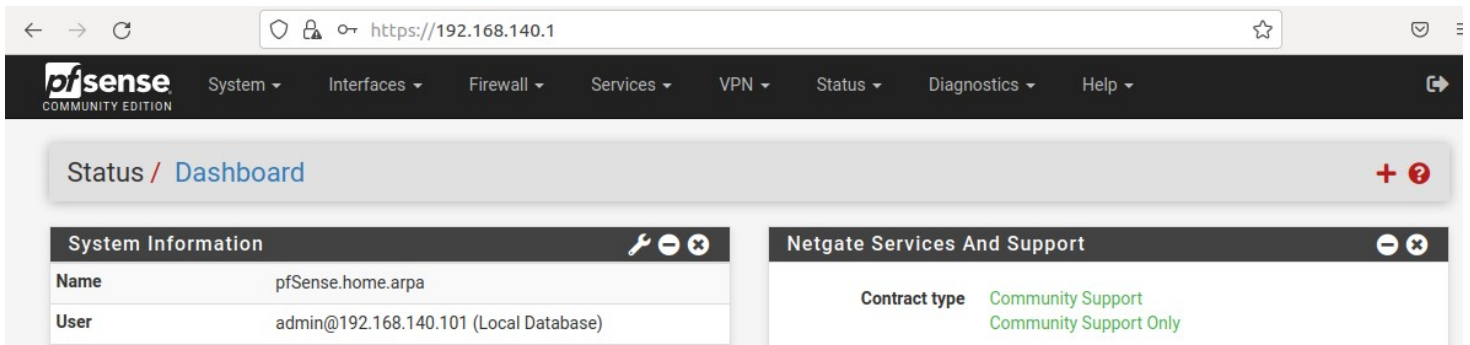
 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

54 updates can be applied immediately.
To see these additional updates run: apt list --upgradable

Last login: Tue Dec 20 22:59:43 2022 from 192.168.122.1
nil@UCLI-NMC:~$

```

- Administrar Firewall **només** amb HTTPS

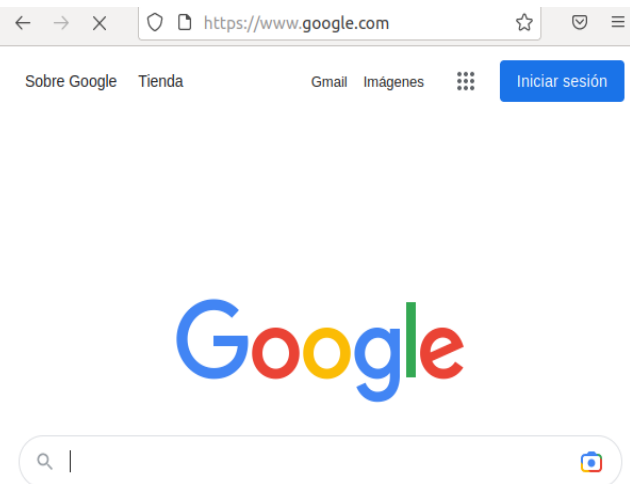


- Navegar per internet (sortir per WAN gràcies al NAT) (0,5 punts)

```

nil@UD:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKN
WN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: ens3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_code
l state UP group default qlen 1000
    link/ether 52:54:00:c9:20:cb brd ff:ff:ff:ff:ff:ff
    inet 192.168.140.101/24 brd 192.168.140.255 scope global dyna
mic noprefixroute ens3
        valid_lft 6903sec preferred_lft 6903sec
    inet6 fe80::a15e:97c5:f1da:80e2/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
nil@UD:~$

```



- Navegar servidor WEB instal·lat a ordinador de la xarxa WAN (192.168.1.0, 172.202.20.0)) (**opcional**) (0,5 punts)

Des de servidor web DMZ NO podem accedir a la LAN:

- No puc fer ping a Host a la xarxa intranet (0,5 punts)

```
root@UCLI-NMC:~# ping 192.168.140.101
PING 192.168.140.101 (192.168.140.101) 56(84) bytes of data.
^C
--- 192.168.140.101 ping statistics ---
39 packets transmitted, 0 received, 100% packet loss, time 38903ms
```

Des de servidor web DMZ podem fer accedir a WAN :

- ping a Host a la xarxa soho (192.168.1.0, 172.202.20.0)) i ping a www.google.com (0,5 punts)

```
root@UCLI-NMC:/home/níl# ping www.google.es
PING www.google.es (142.250.184.163) 56(84) bytes of data.
64 bytes from mad07s23-in-f3.1e100.net (142.250.184.163): icmp_seq=1 ttl=112 time=19.2 ms
64 bytes from mad07s23-in-f3.1e100.net (142.250.184.163): icmp_seq=2 ttl=112 time=20.9 ms
64 bytes from mad07s23-in-f3.1e100.net (142.250.184.163): icmp_seq=3 ttl=112 time=21.0 ms
^C
--- www.google.es ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2004ms
rtt min/avg/max/mdev = 19.249/20.387/20.967/0.805 ms
```

- Sortir a internet per a actualitzar sistema operatiu (0,5 punts)

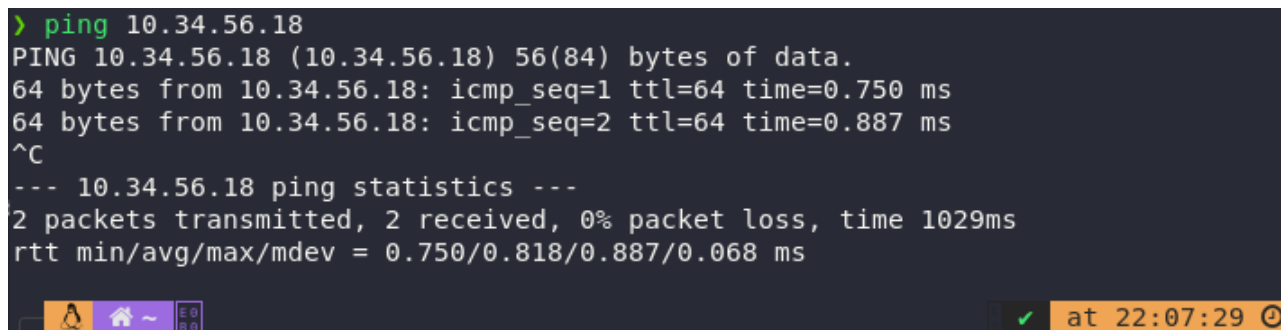
```
Get:22 http://es.archive.ubuntu.com/ubuntu jammy-backports/universe amd64 DEP-11 Metadata [12,5 kB]
Fetched 5.379 kB in 2s (2.565 kB/s)
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
63 packages can be upgraded. Run 'apt list --upgradable' to see them.
root@UCLI-NMC:/home/níl# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: ens3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 52:54:00:e0:51:f9 brd ff:ff:ff:ff:ff:ff
    altname enp0s3
    inet 192.168.122.53/24 brd 192.168.122.255 scope global dynamic noprefixroute ens3
        valid_lft 3535sec preferred_lft 3535sec
    inet6 fe80::8d6a:1627:4e1a:b525/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
```

- Accedir a algun FTP (**opcional**) (0,5 punts)

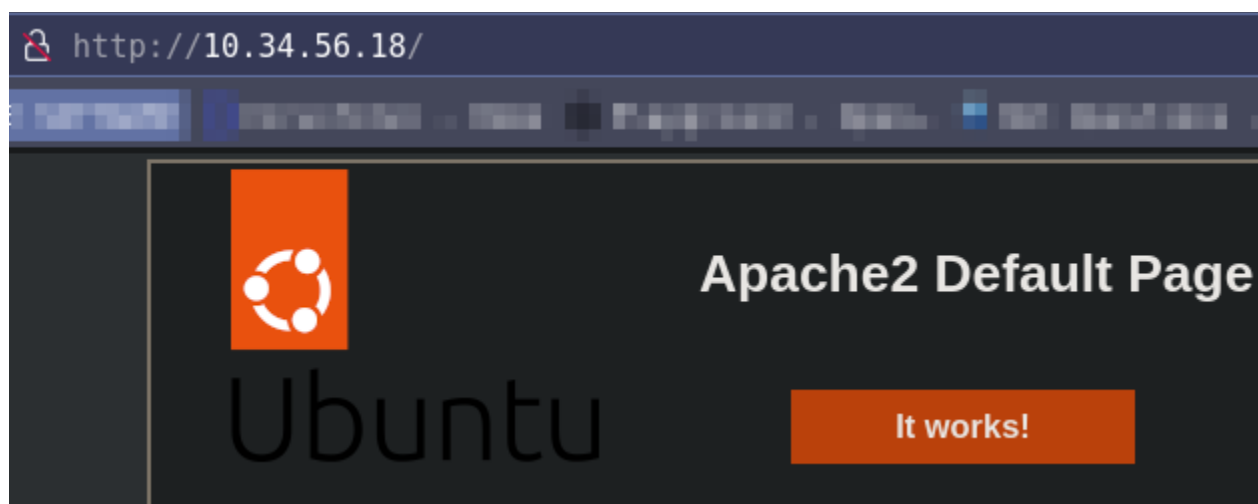
Des de client que està a la xarxa WAN (192.168.1.0, 172.202.20.0)) podem accedir a DMZ (Cal fer-ho amb Port Forwarding):

- fer ping a WEB server a DMZ (0,5 punts)

```
> ping 10.34.56.18
PING 10.34.56.18 (10.34.56.18) 56(84) bytes of data.
64 bytes from 10.34.56.18: icmp_seq=1 ttl=64 time=0.750 ms
64 bytes from 10.34.56.18: icmp_seq=2 ttl=64 time=0.887 ms
^C
--- 10.34.56.18 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1029ms
rtt min/avg/max/mdev = 0.750/0.818/0.887/0.068 ms
```



- navegar WEB Server a DM (0,5 punts)



Des de client que està a la xarxa WAN (192.168.1.0, 172.202.20.0)) **NO** podem accedir a LAN ni al pfSense:

- Fer ping a màquines Intranet (0,5 punts)

```
> ping 192.168.140.101
PING 192.168.140.101 (192.168.140.101) 56(84) bytes of data.
^C
--- 192.168.140.101 ping statistics ---
4 packets transmitted, 0 received, 100% packet loss, time 3065ms
```

- Fer ping a adreça pfSense a la xarxa WAN (0,5 punts)

```
> ping 192.168.122.1
PING 192.168.122.1 (192.168.122.1) 56(84) bytes of data.
64 bytes from 192.168.122.1: icmp_seq=1 ttl=64 time=0.095 ms
64 bytes from 192.168.122.1: icmp_seq=2 ttl=64 time=0.091 ms
^C
--- 192.168.122.1 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1014ms
rtt min/avg/max/mdev = 0.091/0.093/0.095/0.002 ms
```

Haureu d'entregar un document en format PDF i el fitxer de backup de la configuració del pfSense.

Sobretot demostreu que tot el que es demana funciona.

El pdf contindrà:

- Portada amb títol i nom de l'alumne.
- Índex (per tant totes les pàgines, excepte la portada, hauran d'estar numerades).
- Estructurat amb apartats què inclouran una descripció i els comentaris i captures de pantalla que considereu necessaris per a demostrar les regles que es demana implementar.

El fitxer de Backup el creareu desde:

Diagnostics / Backup & Restore / Backup & Restore

Backup & Restore Config History

Backup Configuration

Backup area	All
Skip packages	<input type="checkbox"/> Do not backup package information.
Skip RRD data	<input checked="" type="checkbox"/> Do not backup RRD data (NOTE: RRD Data can consume 4+ megabytes of config.xml space!)
Include extra data	<input type="checkbox"/> Backup extra data. Backup extra data files for some services. ⓘ
Backup SSH keys	<input checked="" type="checkbox"/> Backup SSH keys (otherwise clients would fail to recognize the host keys after restore)
Encryption	<input type="checkbox"/> Encrypt this configuration file.

[Download configuration as XML](#)

El fitxer entregat es dirà **ASIX_M11_UF3_Practica3_Nom_Cognom.zip**