



# M011-SEGURETAT INFORMÀTICA i ALTA SEGURETAT

***UF3- Instal.lació i Configuració d'un servidor intermediari***

**PRÀCTICA 5 : Entorn d'administració  
Webmin per a firewalls i servidors intermitjos**

**Curs:** 2018-19

**CFGS:** ASIX2

**Alumne :** Arnau Subirós Puigarnau

**Data :** 24-03-2019

Nom i Cognoms	Data
Arnau Subirós Puigarnau	24-03-2019

## PRÀCTICA 5 : Entorn d'administració Webmin per a firewalls i servidors intermitjos

### Tasca 1:

Per fer la tasca 1, hauràs de instal·lar i documentar webmin. Per fer-ho pot seguir la guia que t'adjunto en el següent enllaç:<http://mundo.openit.com.bo/?p=716>

Aquest link és força didàctic i explica alguns temes interessants de squid als quals farem referència més endavant. Concretament instal·la primer squid així que pots guardar-te les captures si instal·les primer squid com fa la guia per adjuntar-les a la tasca 3

#### Consideracions importants:

- L'accés a webmin a través del navegador l'heu de fer a través de https i s'ha de crear una excepció. Si no no us funcionarà
- Les credencials d'accés són les del vostre usuari administrador

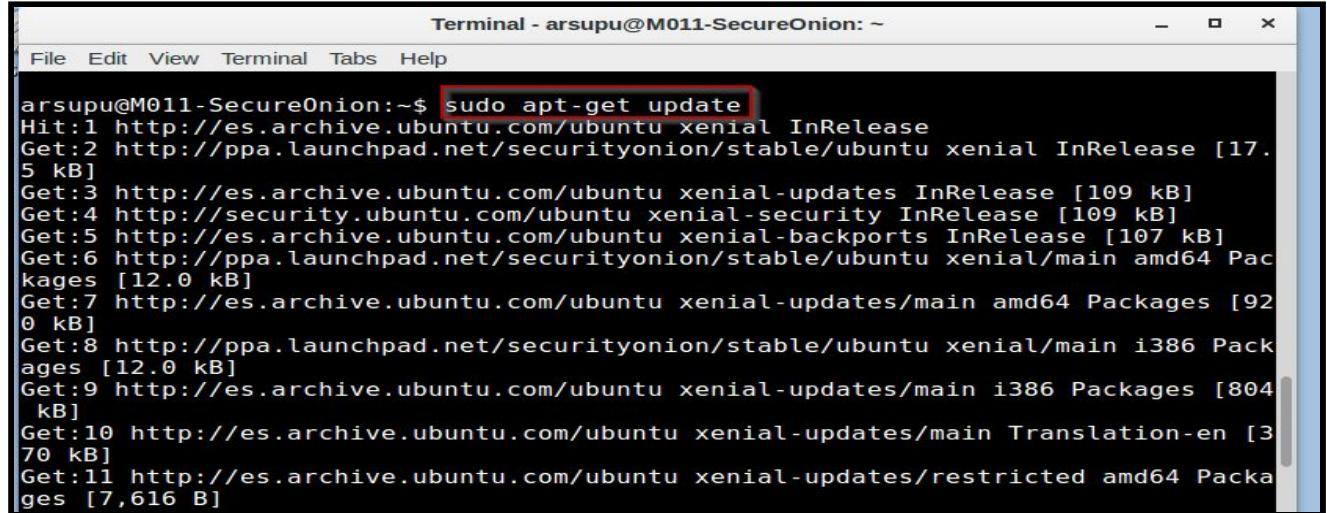
Un cop hagueu entrar a webmin, feu una ullada i expliqueu amb captures de pantalla ítems importants en l'administració d'un sistema servidor.

Concretament heu d'explicar i veure on es troben els següents ítems:

- Informació del sistema
- Monitorització d'ample de banda i interfícies de xarxa
- Mòduls disponibles (identifica'n 5 que creus que són importants o hagis configurat en altres UF)

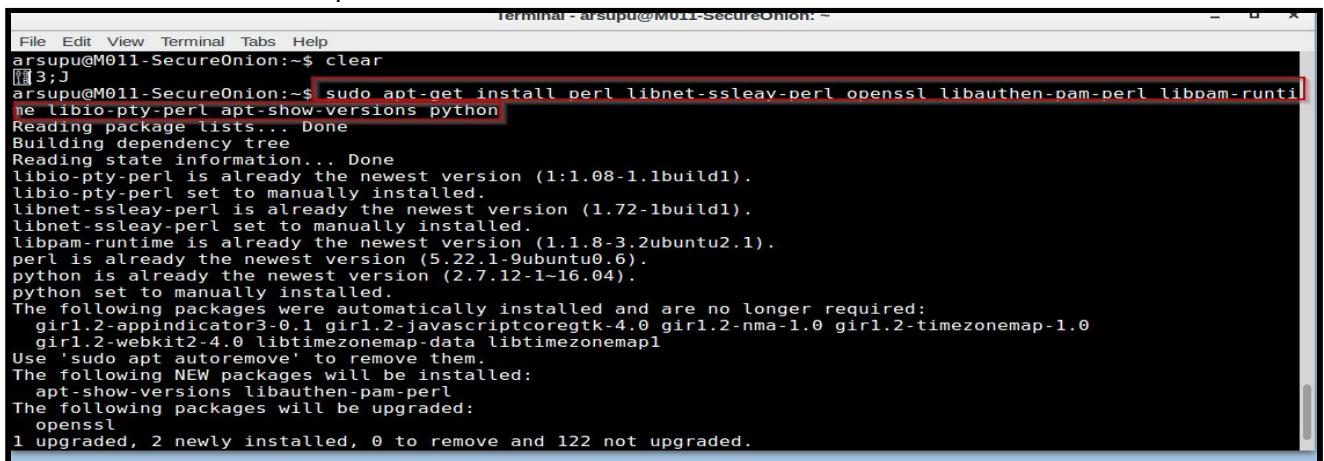
Nom i Cognoms	Data
Arnau Subirós Puigarnau	24-03-2019

- Primer de tot actualitzo els repositoris



```
Terminal - arsupu@M011-SecureOnion: ~
File Edit View Terminal Tabs Help
arsupu@M011-SecureOnion:~$ sudo apt-get update
Hit:1 http://es.archive.ubuntu.com/ubuntu xenial InRelease
Get:2 http://ppa.launchpad.net/securityonion/stable/ubuntu xenial InRelease [17.
5 kB]
Get:3 http://es.archive.ubuntu.com/ubuntu xenial-updates InRelease [109 kB]
Get:4 http://security.ubuntu.com/ubuntu xenial-security InRelease [109 kB]
Get:5 http://es.archive.ubuntu.com/ubuntu xenial-backports InRelease [107 kB]
Get:6 http://ppa.launchpad.net/securityonion/stable/ubuntu xenial/main amd64 Pac
kages [12.0 kB]
Get:7 http://es.archive.ubuntu.com/ubuntu xenial-updates/main amd64 Packages [92
0 kB]
Get:8 http://ppa.launchpad.net/securityonion/stable/ubuntu xenial/main i386 Pack
ages [12.0 kB]
Get:9 http://es.archive.ubuntu.com/ubuntu xenial-updates/main i386 Packages [804
kB]
Get:10 http://es.archive.ubuntu.com/ubuntu xenial-updates/main Translation-en [3
70 kB]
Get:11 http://es.archive.ubuntu.com/ubuntu xenial-updates/restricted amd64 Packa
ges [7,616 B]
```

- Ara instal.lo les dependencies



```
Terminal - arsupu@M011-SecureOnion: ~
File Edit View Terminal Tabs Help
arsupu@M011-SecureOnion:~$ clear
[3;J
arsupu@M011-SecureOnion:~$ sudo apt-get install perl libnet-ssleay-perl openssl libauthen-pam-perl libpam-runtime libio-pty-perl apt-show-versions python
Reading package lists... Done
Building dependency tree
Reading state information... Done
libio-pty-perl is already the newest version (1:1.08-1.1build1).
libio-pty-perl set to manually installed.
libnet-ssleay-perl is already the newest version (1.72-1build1).
libnet-ssleay-perl set to manually installed.
libpam-runtime is already the newest version (1.1.8-3.2ubuntu2.1).
perl is already the newest version (5.22.1-9ubuntu0.6).
python is already the newest version (2.7.12-1-16.04).
python set to manually installed.
The following packages were automatically installed and are no longer required:
  gir1.2-appindicator3-0.1 gir1.2-javascriptcoregtk-4.0 gir1.2-nma-1.0 gir1.2-timezonemap-1.0
  gir1.2-webkit2-4.0 libtimezonemap-data libtimezonemap1
Use 'sudo apt autoremove' to remove them.
The following NEW packages will be installed:
  apt-show-versions libauthen-pam-perl
The following packages will be upgraded:
  openssl
1 upgraded, 2 newly installed, 0 to remove and 122 not upgraded.
```

Nom i Cognoms	Data
Arnau Subirós Puigarnau	24-03-2019

- Descargo **webmin** desde Internet en formato deb

Terminal - arsupu@M011-SecureOnion: ~

```

File Edit View Terminal Tabs Help
arsupu@M011-SecureOnion:~$ sudo wget http://www.webmin.com/download/deb/webmin-current.deb
--2019-03-15 16:29:31-- http://www.webmin.com/download/deb/webmin-current.deb
Resolving www.webmin.com (www.webmin.com)... 216.105.38.10
Connecting to www.webmin.com (www.webmin.com)|216.105.38.10|:80... connected.
HTTP request sent, awaiting response... 302 Moved Temporarily
Location: https://prdownloads.sourceforge.net/webadmin/webmin_1.900_all.deb [following]
--2019-03-15 16:29:32-- https://prdownloads.sourceforge.net/webadmin/webmin_1.900_all.deb
Resolving prdownloads.sourceforge.net (prdownloads.sourceforge.net)... 216.105.38.13
Connecting to prdownloads.sourceforge.net (prdownloads.sourceforge.net)|216.105.38.13|:443... connected.
HTTP request sent, awaiting response... 301 Moved Permanently
Location: https://downloads.sourceforge.net/project/webadmin/webmin/1.900/webmin_1.900_all.deb [following]
--2019-03-15 16:29:33-- https://downloads.sourceforge.net/project/webadmin/webmin/1.900/webmin_1.900_all.deb
Resolving downloads.sourceforge.net (downloads.sourceforge.net)... 216.105.38.13
Connecting to downloads.sourceforge.net (downloads.sourceforge.net)|216.105.38.13|:443... connected.
HTTP request sent, awaiting response... 301 Moved Permanently
Location: https://datapacket.dl.sourceforge.net/project/webadmin/webmin/1.900/webmin_1.900_all.deb [following]
--2019-03-15 16:29:34-- https://datapacket.dl.sourceforge.net/project/webadmin/webmin/1.900/webmin_1.900_all.deb
Resolving datapacket.dl.sourceforge.net (datapacket.dl.sourceforge.net)... 185.152.64.70
Connecting to datapacket.dl.sourceforge.net (datapacket.dl.sourceforge.net)|185.152.64.70|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 15846232 (15M) [application/octet-stream]
Saving to: 'webmin-current.deb'

webmin-current.deb          100%[=====] 15.11M  1.04MB/s   in 34s

2019-03-15 16:30:11 (451 KB/s) - 'webmin-current.deb' saved [15846232/15846232]

```

- Instal·lem el paquet .deb

Terminal - arsupu@M011-SecureOnion: ~

```

File Edit View Terminal Tabs Help
arsupu@M011-SecureOnion:~$ ls
Desktop Documents Downloads Music Pictures Public Templates Videos webmin-current.deb
arsupu@M011-SecureOnion:~$ sudo dpkg -i webmin-current.deb
Selecting previously unselected package webmin.
(Reading database ... 141242 files and directories currently installed.)
Preparing to unpack webmin-current.deb ...
Unpacking webmin (1.900) ...
Setting up webmin (1.900) ...
Webmin install complete. You can now login to https://M011-SecureOnion:10000/
as root with your root password, or as any user who can use sudo
to run commands as root.
Processing triggers for systemd (229-4ubuntu21.10) ...
Processing triggers for ureadahead (0.100.0-19) ...
arsupu@M011-SecureOnion:~$ 

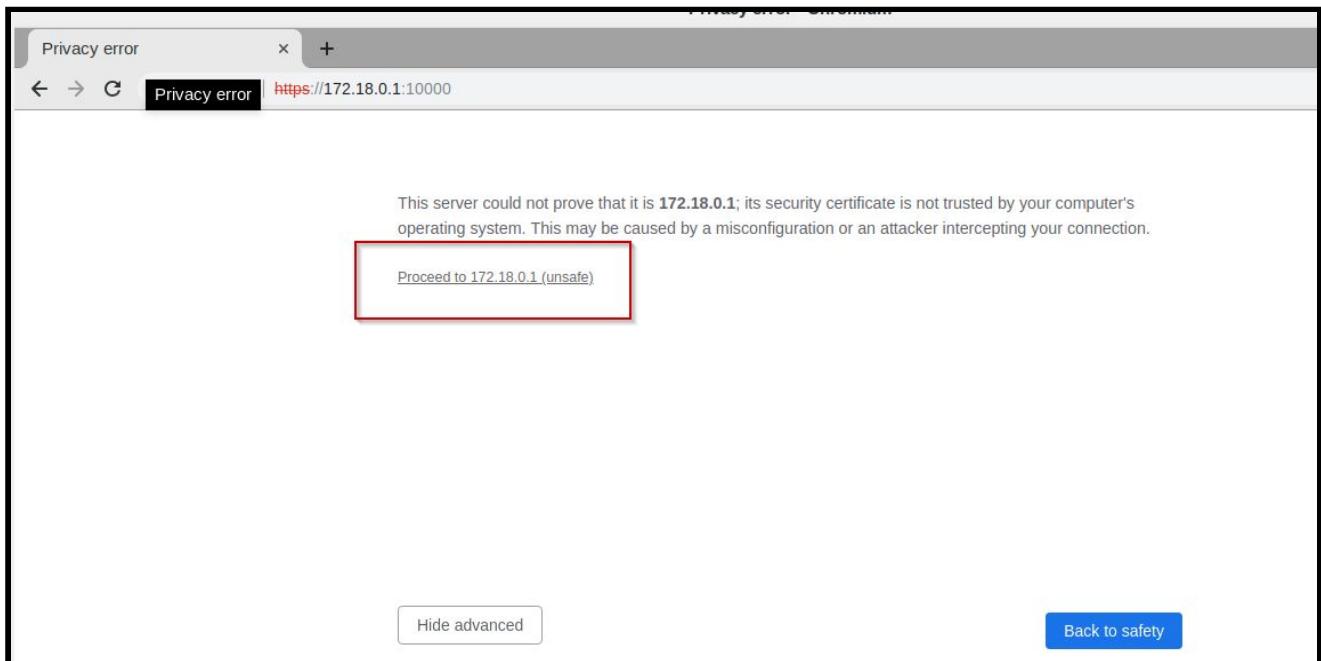
```

Nom i Cognoms	Data
Arnau Subirós Puigarnau	24-03-2019

- Abans d'accendir al navegador revisem la nostre IP

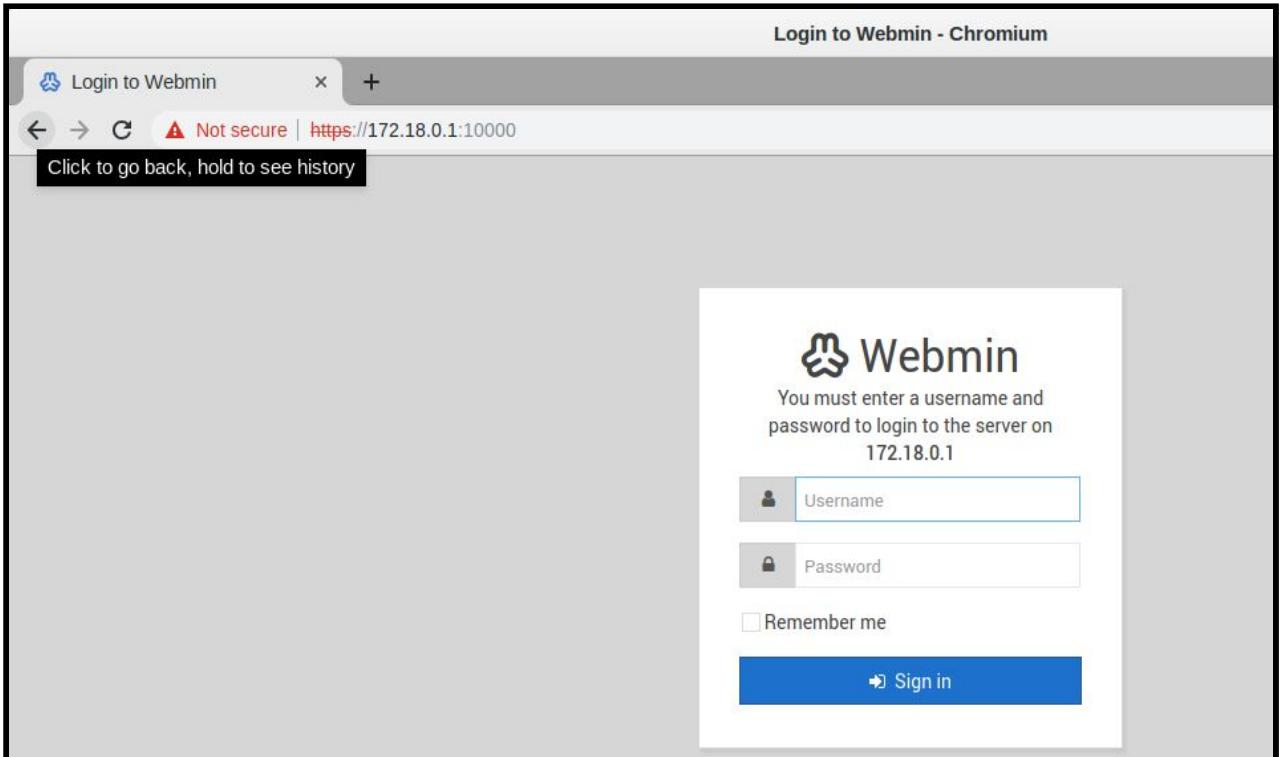
Terminal - arsupu@M011-SecureOnion: ~

```
File Edit View Terminal Tabs Help
arsupu@M011-SecureOnion:~$ ip a | grep br-32cfbc9efdff | grep inet
inet 172.18.0.1/16 brd 172.18.255.255 scope global br-32cfbc9efdff
arsupu@M011-SecureOnion:~$
```

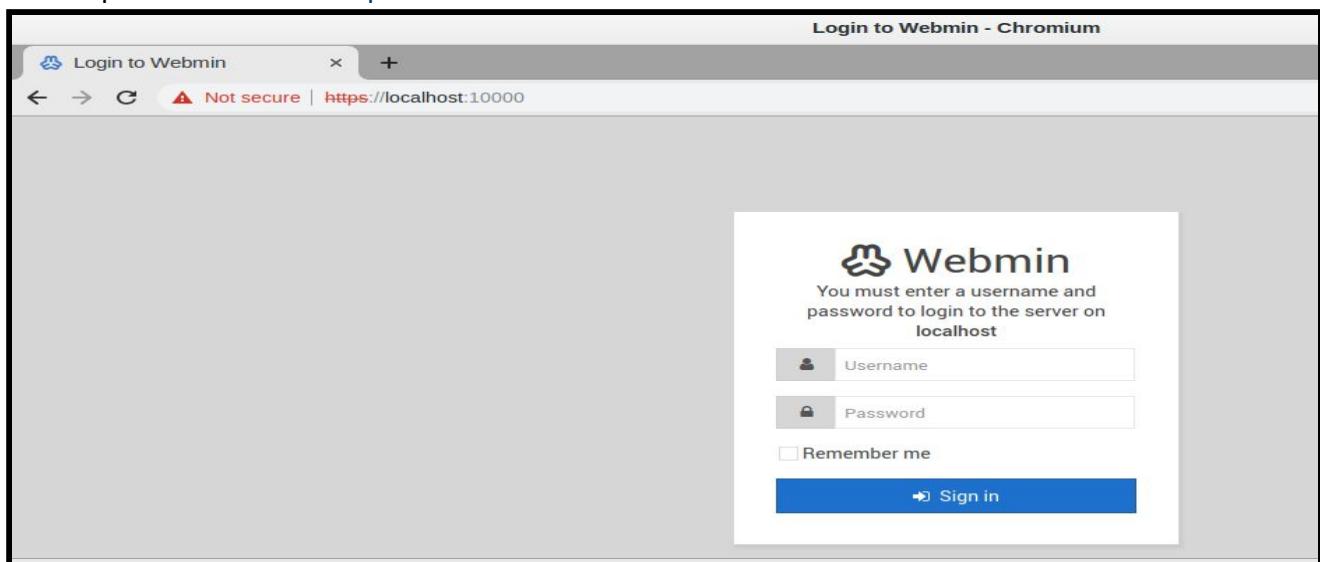


Nom i Cognoms	Data
Arnau Subirós Puigarnau	24-03-2019

- Desde el navegador utilizarem https (mode segur) esciurem la nostre IP i el port 10000

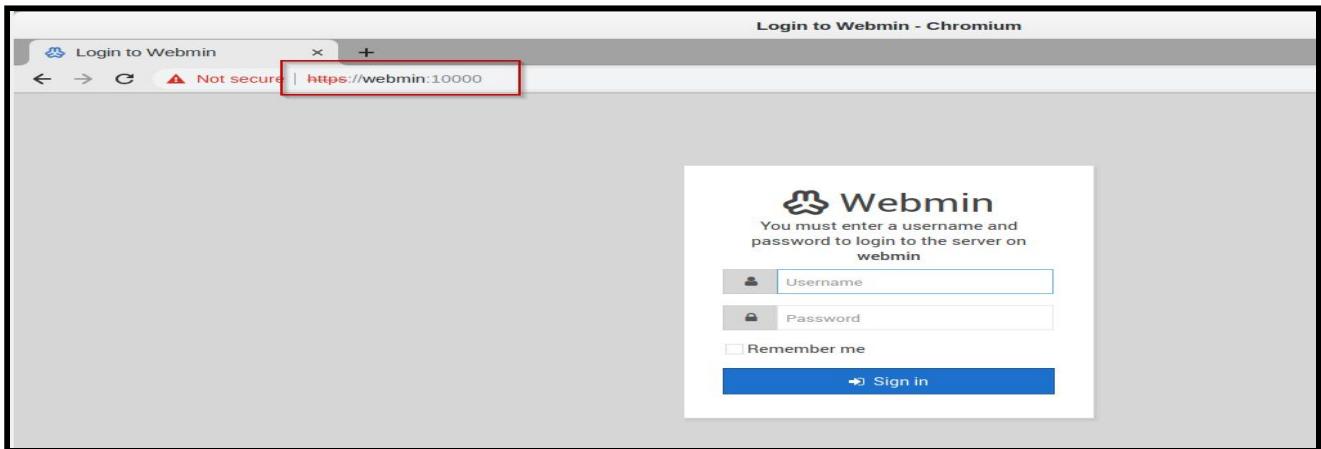


- També podríem accedir <https://localhost:10000>



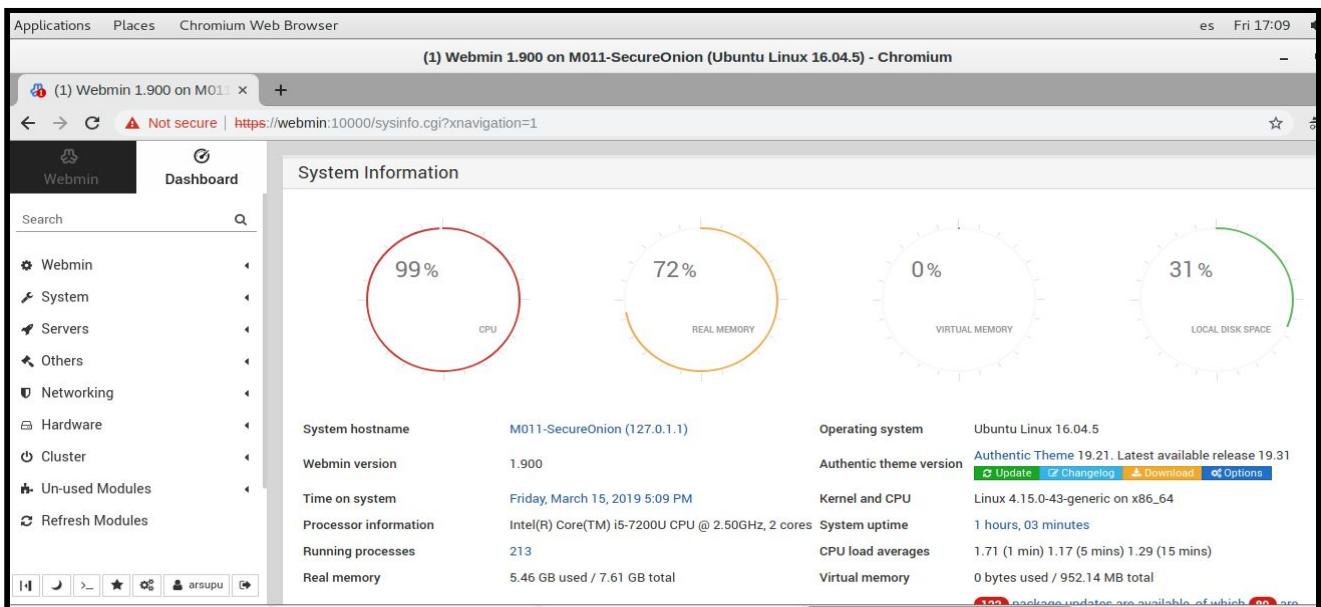
Nom i Cognoms	Data
Arnau Subirós Puigarnau	24-03-2019

- Però com que no ens enrecordarem de l'IP (dinamica, es pot modificar l'arxiu /etc/hosts afegim la IP i el nom , en aquest cas Webmin). Així la proxima vegada que canvi la IP només haure de revisar la IP en aquest arxiu, modificar-lo. Però des de el navegador accedirem sempre <https://Webmin:10000>



- Accedim com usuari Arsupu (no és root, però format part del grup sudo)

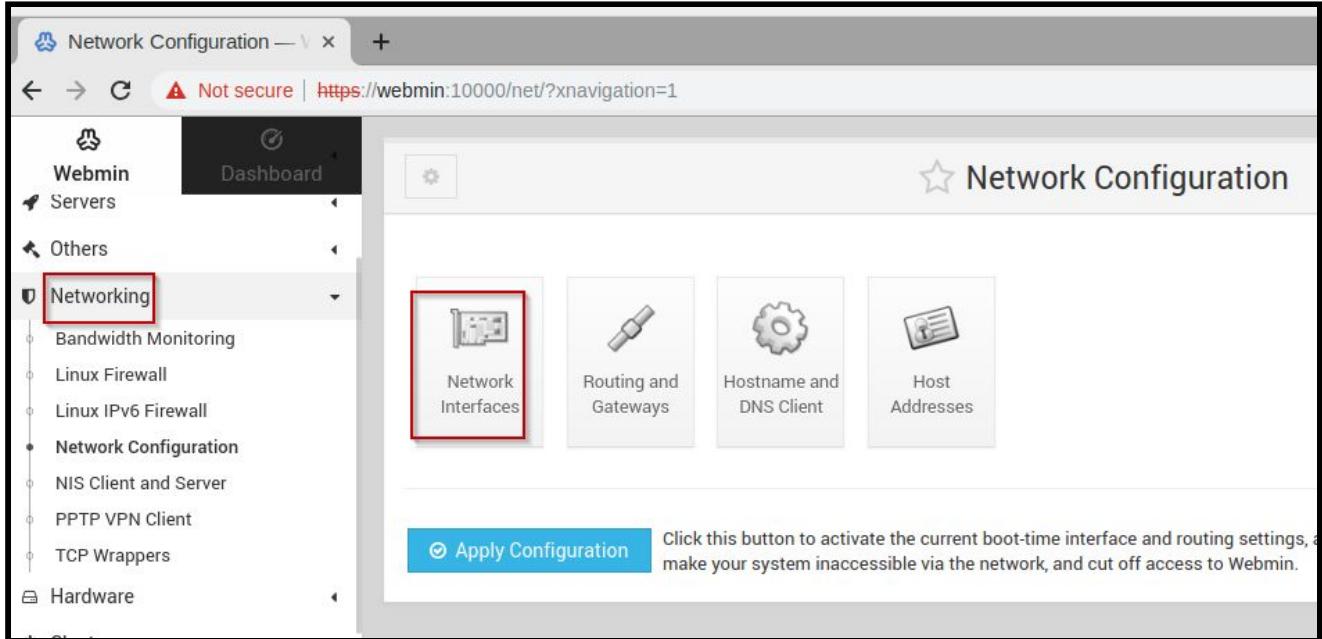
### ❖ Informació del sistema



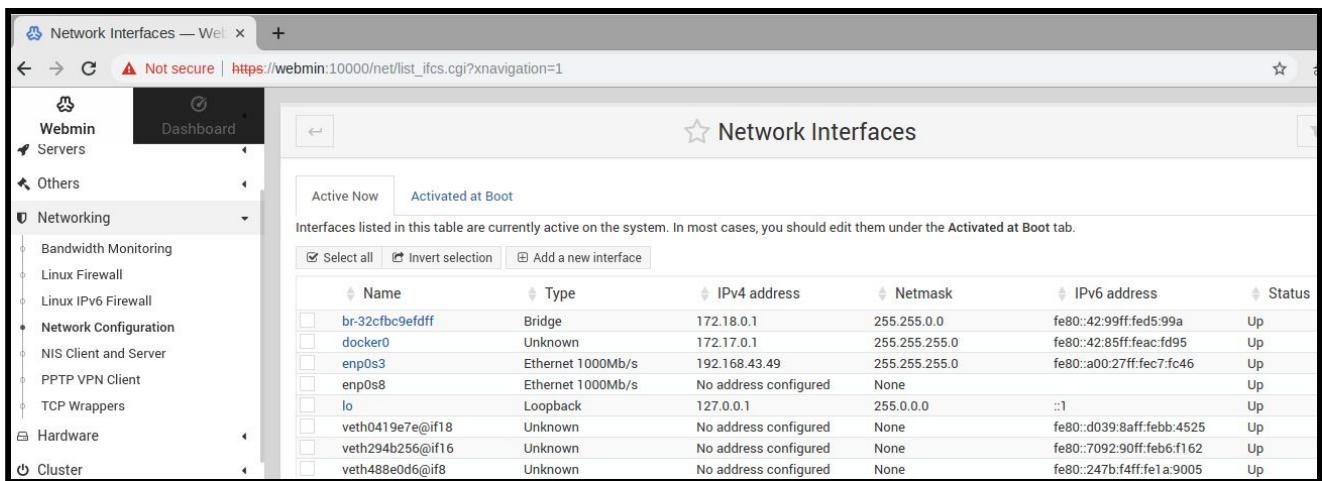
Nom i Cognoms	Data
Arnau Subirós Puigarnau	24-03-2019

❖ Monitorització d'ample de banda i interfícies de xarxa

1. *Seleccionem Network Interfaces*



The screenshot shows the Webmin Network Configuration interface. The left sidebar has 'Networking' selected. The main area shows four icons: 'Network Interfaces' (highlighted with a red box), 'Routing and Gateways', 'Hostname and DNS Client', and 'Host Addresses'. A button at the bottom says 'Apply Configuration'.



The screenshot shows the 'Network Interfaces' list in Webmin. The sidebar has 'Networking' selected. The main area lists network interfaces with columns for Name, Type, IPv4 address, Netmask, IPv6 address, and Status. The table includes rows for br-32cfbc9efdf, docker0, enp0s3, enp0s8, lo, veth0419e7e@if18, veth294b256@if16, and veth488e0d6@if8.

Name	Type	IPv4 address	Netmask	IPv6 address	Status
br-32cfbc9efdf	Bridge	172.18.0.1	255.255.0.0	fe80::42:9fff:fed5:99a	Up
docker0	Unknown	172.17.0.1	255.255.255.0	fe80::42:85ff:feac:fd95	Up
enp0s3	Ethernet 1000Mb/s	192.168.43.49	255.255.255.0	fe80:a00:27ff:ec7:fc46	Up
enp0s8	Ethernet 1000Mb/s	No address configured	None		Up
lo	Loopback	127.0.0.1	255.0.0.0	::1	Up
veth0419e7e@if18	Unknown	No address configured	None	fe80::d039:8aff:febb:4525	Up
veth294b256@if16	Unknown	No address configured	None	fe80::7092:90ff:feb6:f162	Up
veth488e0d6@if8	Unknown	No address configured	None	fe80::247b:f4ff:fe1a:9005	Up

Nom i Cognoms	Data
Arnau Subirós Puigarnau	24-03-2019

 Network Interfaces

Active Now		Activated at Boot			
Interfaces listed in this table will be activated when the system boots up, and will generally be active now too.					
<input checked="" type="checkbox"/> Select all	 Invert selection	 Add a new interface	 Add a new bonding Interface	 Add Vlan Tagged Interface	 Add a new bridge
◆ Name	◆ Type	◆ IPv4 address	◆ Netmask	◆ IPv6 address	◆ Active
<input type="checkbox"/> enp0s3	Ethernet	From DHCP	From DHCP		Yes
<input type="checkbox"/> enp0s8	Ethernet	No address configured	None		Yes
<input type="checkbox"/> lo	Loopback	No address configured	None		Yes

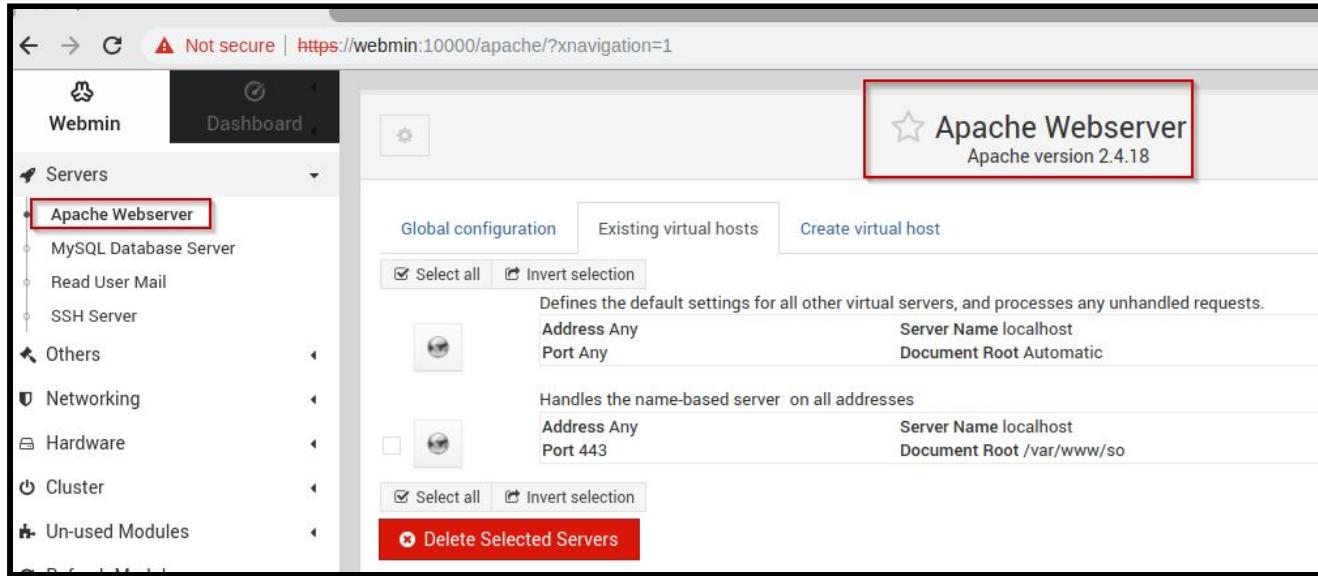
 Host Addresses

<input checked="" type="checkbox"/> Select all		 Invert selection	 Add a new host address
◆ IP Address	◆ Hostnames		
<input type="checkbox"/> 127.0.0.1	localhost		
<input type="checkbox"/> 127.0.1.1	M011-SecureOnion		
<input type="checkbox"/> ::1	ip6-localhost , ip6-loopback		
<input type="checkbox"/> fe00::0	ip6-localnet		
<input type="checkbox"/> ff00::0	ip6-mcastprefix		
<input type="checkbox"/> ff02::1	ip6-allnodes		
<input type="checkbox"/> ff02::2	ip6-allrouters		
<input type="checkbox"/> 172.18.0.1	Webmin		

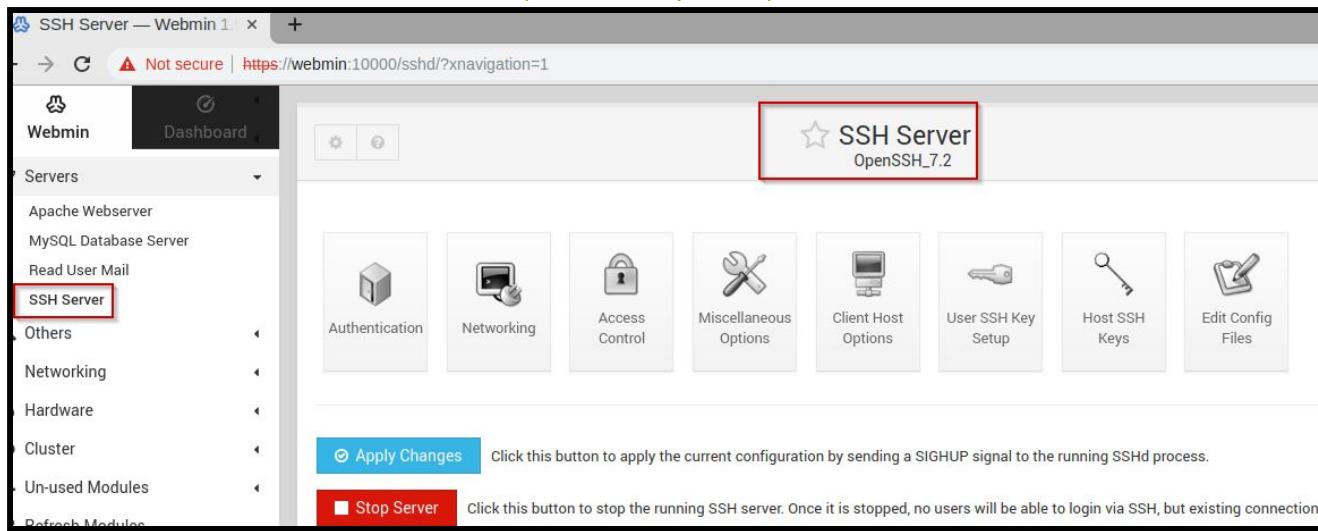
Nom i Cognoms	Data
Arnau Subirós Puigarnau	24-03-2019

❖ Mòduls disponibles (identifica'n 5 que creguis que són importants o hagis configurat en altres UF)

### 1. Apache :Servidor Web (utilitzant el port 443)



### 2. Servidor SSH (utilitzant el port 22)



Nom i Cognoms	Data
Arnau Subirós Puigarnau	24-03-2019

**★ Networking**

**Networking options**

( All addresses  Entered below ..)

Listen on addresses	Address	Port
	▼	<input checked="" type="radio"/> Default <input type="radio"/>

Listen on port  Default (22)  22

Accept protocols  SSH v1  SSH v2

Disconnect if client has crashed?  Yes  No

Time to wait for login  Forever  120 seconds

Allow TCP forwarding?  Yes  No

Allow connection to forwarded ports?  Yes  No

**Save**

### 3. Modulos Perl ( mostrem alguns submoduls d'aquest llenguatge de programació )

Not Secure | https://webmin.10.0.0.1:10000/epanix | Xnavigation | 1

**Perl Modules**  
Perl version v5.22.1

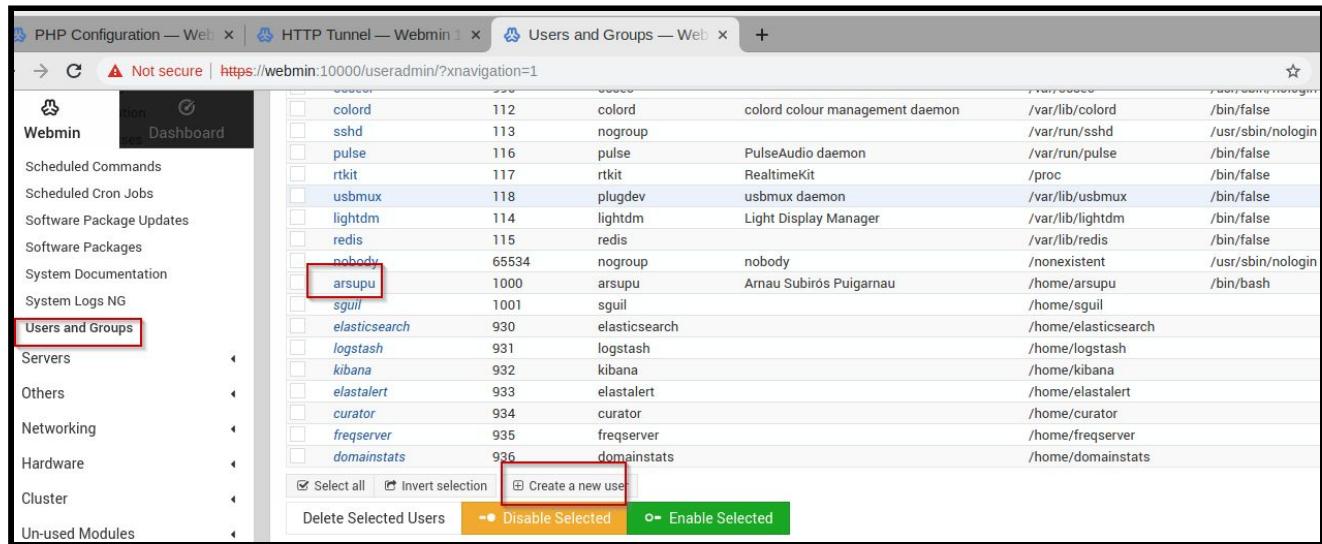
Module	Submodules	Description	Version	Installed on
<input type="checkbox"/> Algorithm::Diff	1	Compute 'intelligent' differences between two files / lists	1.19	03/15/2019 4:37 P
<input type="checkbox"/> Algorithm::Diff::XS	0	Algorithm::Diff with XS core loop	0.04	03/15/2019 4:37 P
<input type="checkbox"/> Algorithm::Merge	0	Three-way merge and diff	0.08	03/15/2019 4:37 P
<input type="checkbox"/> AptPkg::PkgRecords	8	APT package description class	1.2	03/15/2019 4:37 P
<input type="checkbox"/> Archive::Zip	11	Provide an interface to ZIP archive files.	1.56	03/15/2019 4:37 P
<input type="checkbox"/> Authen::PAM	0	Perl interface to PAM library	0.16	03/15/2019 4:37 P
<input type="checkbox"/> Authen::SASL	10	SASL Authentication framework	2.1600-1	03/15/2019 4:37 P
<input type="checkbox"/> Bytes::Random::Secure	0	Perl extension to generate cryptographically-secure random bytes.	0.28	03/15/2019 4:37 P
<input type="checkbox"/> Cairo	1	Perl interface to the cairo 2d vector graphics library	1.106	03/15/2019 4:37 P
<input type="checkbox"/> CGI	8	Handle Common Gateway Interface requests and responses	4.26-1	03/15/2019 4:37 P
<input type="checkbox"/> CGI::Fast	0	CGI Interface for Fast CGI	2.10-1	03/15/2019 4:37 P
<input type="checkbox"/> Class::Accessor	2	Automated accessor generation	0.34-1	03/15/2019 4:37 P
<input type="checkbox"/> Class::Copy	0	recursively copy Perl datatypes	0.38	03/15/2019 4:37 P

**Nom i Cognoms**

Arnau Subirós Puigarnau

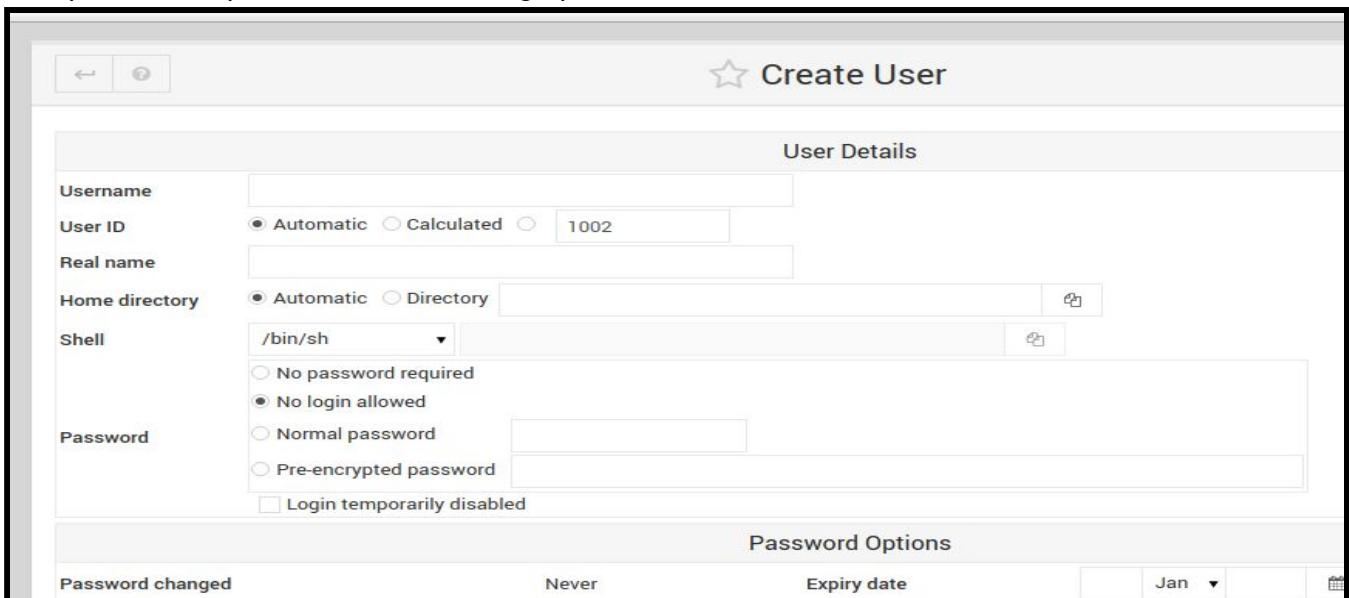
**Data**

24-03-2019

**4. Mòdul: Usuaris i Grups**


The screenshot shows the 'Users and Groups' section of the Webmin interface. On the left, there's a sidebar with various system management links. The 'Users and Groups' link is highlighted with a red box. The main area displays a table of users with columns for name, ID, group, description, home directory, shell, and other details. The user 'arsupu' is selected and highlighted with a red box. At the bottom of the list, there are several buttons: 'Select all', 'Invert selection', 'Create a new user' (which is also highlighted with a red box), 'Delete Selected Users', 'Disable Selected', and 'Enable Selected'.

en aquest mòdul podem crear usuaris i grups



The screenshot shows the 'Create User' dialog box. The 'User Details' tab is active, displaying fields for Username (empty), User ID (set to Automatic, ID 1002), Real name (empty), Home directory (Automatic), Shell (/bin/sh), and Password options (No password required, No login allowed, Normal password, Pre-encrypted password, Login temporarily disabled). Below this is the 'Password Options' tab, which includes fields for Password changed (Never), Expiry date (Jan), and a calendar icon.

Nom i Cognoms	Data
Arnau Subirós Puigarnau	24-03-2019

Login temporarily disabled

### Password Options

Password changed	Never	Expiry date	Jan
Minimum days	<input type="text"/>	Maximum days	<input type="text"/>
Warning days	<input type="text"/>	Inactive days	<input type="text"/>
Force change at next login?	<input type="radio"/> Yes <input checked="" type="radio"/> No		

### Group Membership

Primary group	<input type="radio"/> New group with same name as user <input type="radio"/> New group <input checked="" type="radio"/> Existing group users
Secondary groups	All groups: root, daemon, bin, sys In groups:

**Upon Creation..**

Create home directory?  Yes  No  
 Copy template files to home directory?  Yes  No  
 Create user in other modules?  Yes  No

**Create**

[Return to users and groups list](#)

## 5. Mòdul: Linux Firewall(IPTables)

Linux IPTables Firewall — Webmin 1.900 on M011-SecureOnion (Ubuntu Linux 16.04.5) - Chromium

PHP Configuration — Web Not secure | https://webmin:10000/firewall/?xnavigation=1

Showing IPTable: Packet filtering (filter)

Add a new chain named:

Incoming packets (INPUT) - Only applies to packets addressed to this host

Action	Condition	Move	Add
<input type="checkbox"/> Jump to chain ufw-before-logging-input	Always		
<input type="checkbox"/> Jump to chain ufw-before-input	Always		
<input type="checkbox"/> Jump to chain ufw-after-input	Always		
<input type="checkbox"/> Jump to chain ufw-after-logging-input	Always		
<input type="checkbox"/> Jump to chain ufw-reject-input	Always		
<input type="checkbox"/> Jump to chain ufw-track-input	Always		

Select all  Invert selection

Set Default Action To: Drop  Delete Selected  Move Selected **Add Rule**

Forwarded packets (FORWARD) - Only applies to packets passed through this host

**Nom i Cognoms**
**Data**

Arnau Subirós Puigarnau

24-03-2019

**Forwarded packets (FORWARD) - Only applies to packets passed through this host**

Action	Condition	Move	Add
Jump to chain DOCKER-USER	Always		
Jump to chain DOCKER-ISOLATION-STAGE-1	Always		
<b>Accept</b>	If output interface is docker0 and state of connection is RELATED,ESTABLISHED		
Jump to chain DOCKER	If output interface is docker0		
<b>Accept</b>	If input interface is docker0 and output interface is not docker0		
<b>Accept</b>	If input interface is docker0 and output interface is docker0		
<b>Accept</b>	If output interface is br-32cfbc9efdf and state of connection is RELATED,ESTABLISHED		
Jump to chain DOCKER	If output interface is br-32cfbc9efdf		
<b>Accept</b>	If input interface is br-32cfbc9efdf and output interface is not br-32cfbc9efdf		
<b>Accept</b>	If input interface is br-32cfbc9efdf and output interface is br-32cfbc9efdf		
Jump to chain ufw-before-forward	Always		
Jump to chain ufw-before-forward	Always		
Jump to chain ufw-after-forward	Always		
Jump to chain ufw-after-logging-forward	Always		
Jump to chain ufw-reject-forward	Always		
Jump to chain ufw-track-forward	Always		

**Outgoing packets (OUTPUT) - Only applies to packets originated by this host**

Action	Condition	Move	Add
Jump to chain ufw-before-logging-output	Always		
Jump to chain ufw-before-output	Always		
Jump to chain ufw-after-output	Always		
Jump to chain ufw-after-logging-output	Always		
Jump to chain ufw-reject-output	Always		
Jump to chain ufw-track-output	Always		

**Set Default Action To:** **Accept** **Delete Selected** **Move Selected** **Add Rule**

**Chain DOCKER**

Action	Condition	Move	Add
<b>Accept</b>	If protocol is TCP and destination is 172.17.0.4/32 and input interface is not docker0 and		

Nom i Cognoms	Data
Arnau Subirós Puigarnau	24-03-2019

## Tasca 2:

Ves a l'apartat de configuracions del firewalls i identifica els conceptes que hem explicat a la UF.

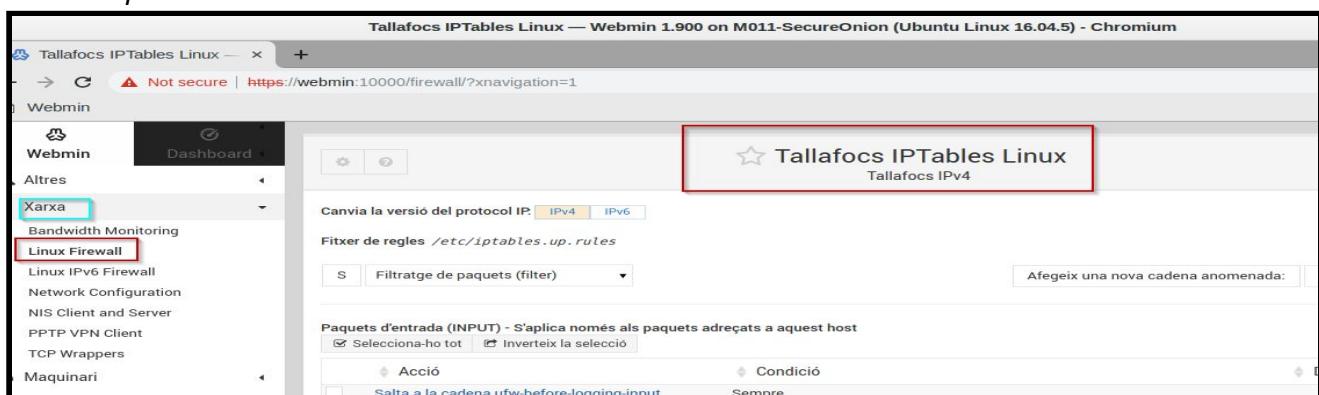
- Iptables
- Cadenes
- Regles

Explica que és i per a que serveix buscant informació a la xarxa el fitxer:

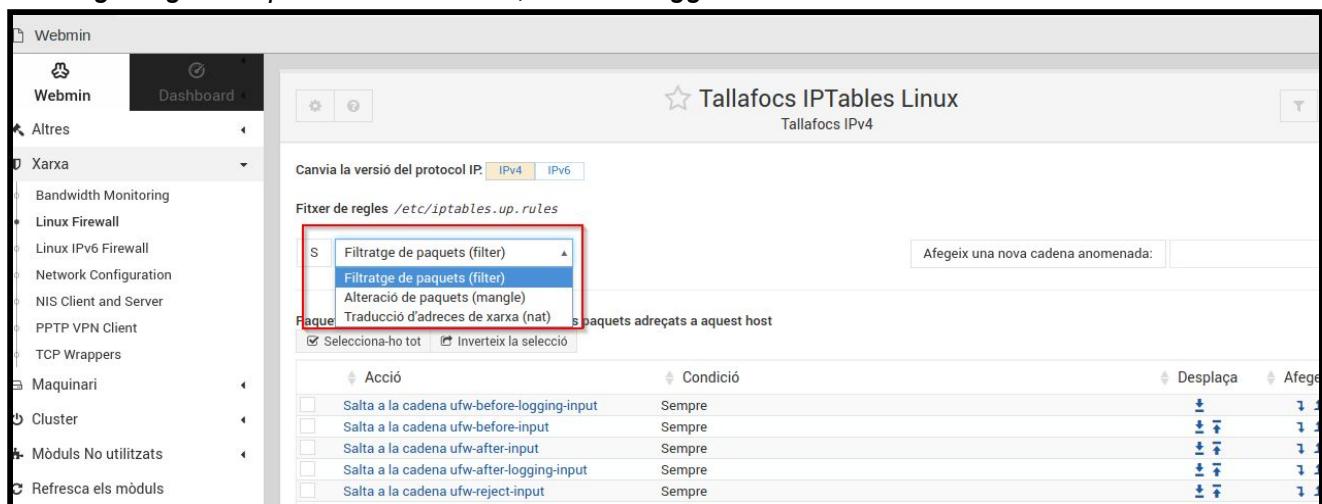
/etc/webmin/firewall/iptables.save

Diges quines són els avantatges d'administrar les iptables amb webmin

- Des de el panell de Webmin accedim a Xarxa i seleccionem Linux Firewall



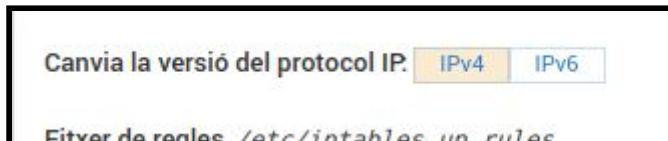
- Filtratge segon el tipus de taula : Filter, Nat o Manggle



Acció	Condició	Desplaça	Afegeix
Salta a la cadena ufw-before-logging-input	Sempre		
Salta a la cadena ufw-before-input	Sempre		
Salta a la cadena ufw-after-input	Sempre		
Salta a la cadena ufw-after-logging-input	Sempre		
Salta a la cadena ufw-reject-input	Sempre		

Nom i Cognoms	Data
Arnau Subirós Puigarnau	24-03-2019

- Segons el protocol IP, en aquest cas IPv4



- En aquesta captura, es filtra per la taula Filter on hem seleccionat els paquets d'entrada (input)



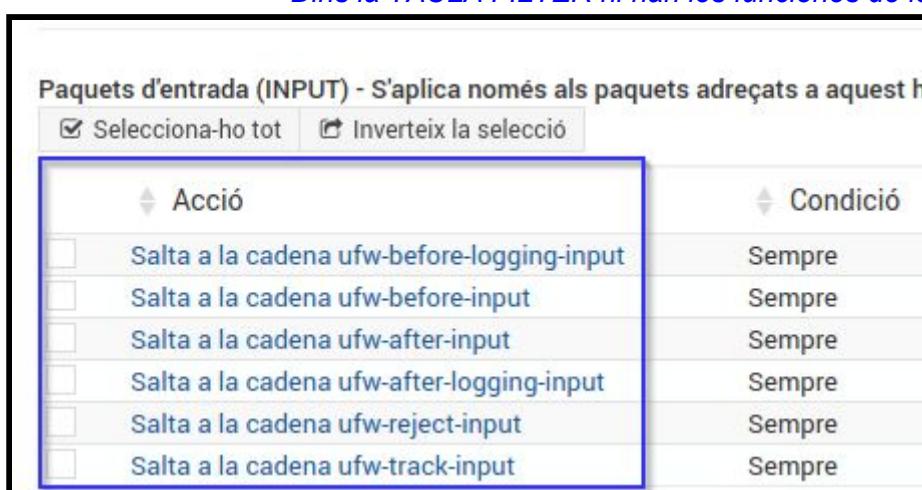
Acció	Condició	Desplaça	Afegeix
<input type="checkbox"/> Salta a la cadena ufw-before-logging-input	Sempre		
<input type="checkbox"/> Salta a la cadena ufw-before-input	Sempre		
<input type="checkbox"/> Salta a la cadena ufw-after-input	Sempre		
<input type="checkbox"/> Salta a la cadena ufw-after-logging-input	Sempre		
<input type="checkbox"/> Salta a la cadena ufw-reject-input	Sempre		
<input type="checkbox"/> Salta a la cadena ufw-track-input	Sempre		

Selecciona-ho tot  Inverteix la selecció

Estableix l'Acció per Defecte A:  Suprimeix les Seleccionades  Afegeix Regla

Destruïx Desplaça les Seleccionades

- Dins la TAULA FILTER hi han les funcions de les cadenes



Acció	Condició
<input type="checkbox"/> Salta a la cadena ufw-before-logging-input	Sempre
<input type="checkbox"/> Salta a la cadena ufw-before-input	Sempre
<input type="checkbox"/> Salta a la cadena ufw-after-input	Sempre
<input type="checkbox"/> Salta a la cadena ufw-after-logging-input	Sempre
<input type="checkbox"/> Salta a la cadena ufw-reject-input	Sempre
<input type="checkbox"/> Salta a la cadena ufw-track-input	Sempre

Nom i Cognoms	Data
Arnau Subirós Puigarnau	24-03-2019

- Afegim o editem regles que afectaran a les cadenes



- En aquesta captura, es filtra per la taula Filter on hem seleccionat els paquets forward (reenviats)



Acció	Condició	Desplaça	Afegeix
Salta a la cadena DOCKER-USER	Sempre	↑ ↓	↑ ↓
Salta a la cadena DOCKER-ISOLATION-STAGE-1	Sempre	↑ ↓	↑ ↓
Accepta	Si la intereficie de sortida és docker0 i la intereficie de sortida no és docker0 i la intereficie de sortida és docker0 i la intereficie de sortida és docker0	↑ ↓	↑ ↓
Salta a la cadena DOCKER	Si la intereficie de sortida és docker0	↑ ↓	↑ ↓
Accepta	Si la intereficie d'entrada és docker0 i la intereficie de sortida no és docker0	↑ ↓	↑ ↓
Accepta	Si la intereficie d'entrada és docker0 i la intereficie de sortida és docker0	↑ ↓	↑ ↓
Accepta	Si la intereficie de sortida és br-32cfbc9efdff i state of connection is RELATED,ESTABLISHED	↑ ↓	↑ ↓
Salta a la cadena DOCKER	Si la intereficie de sortida és br-32cfbc9efdff	↑ ↓	↑ ↓
Accepta	Si la intereficie d'entrada és br-32cfbc9efdff i la intereficie de sortida no és br-32cfbc9efdff	↑ ↓	↑ ↓
Accepta	Si la intereficie d'entrada és br-32cfbc9efdff i la intereficie de sortida és br-32cfbc9efdff	↑ ↓	↑ ↓
Salta a la cadena ufw-before-logging-forward	Sempre	↑ ↓	↑ ↓

Nom i Cognoms	Data
Arnau Subirós Puigarnau	24-03-2019

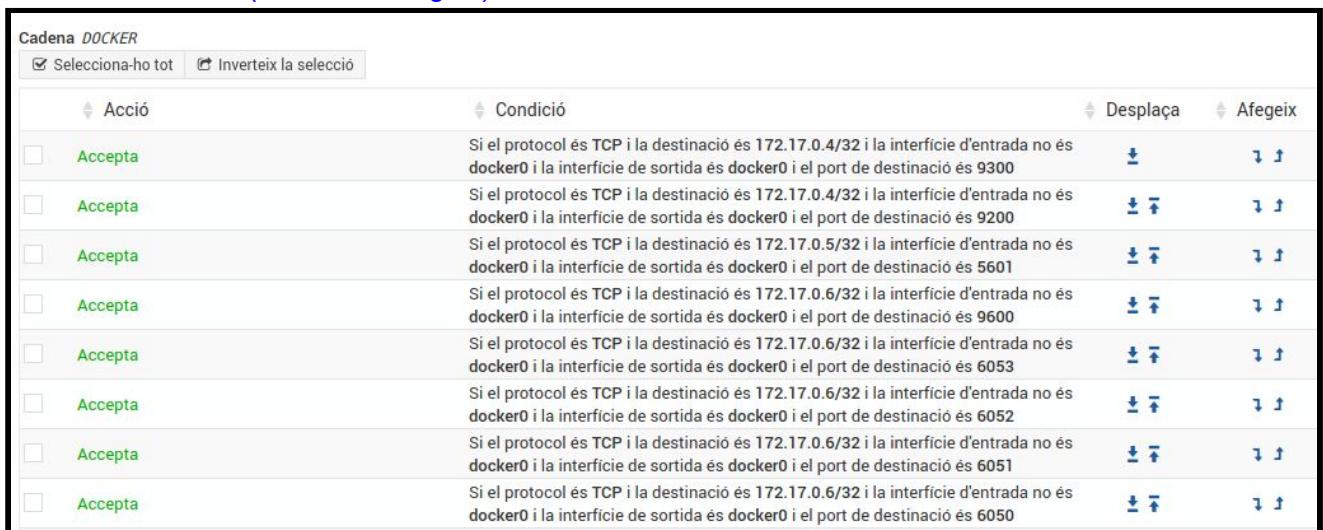
- En aquesta captura, es filtra per la taula Filter on hem seleccionat els paquets out (sortida)



The screenshot shows a table of rules for the 'Paquets de sortida (OUTPUT)' chain. The table has columns for Acció (Action), Condició (Condition), Desplaça (Move), and Afegeix (Add). Most rules have the action 'Salta a la cadena ufw-before-logging-output' and the condition 'Sempre'. One rule has the action 'Destruix'.

Acció	Condició	Desplaça	Afegeix
Salta a la cadena ufw-before-logging-output	Sempre	↑	↑ ↓
Salta a la cadena ufw-before-output	Sempre	↑ ↓	↑ ↓
Salta a la cadena ufw-after-output	Sempre	↑ ↓	↑ ↓
Salta a la cadena ufw-after-logging-output	Sempre	↑ ↓	↑ ↓
Salta a la cadena ufw-reject-output	Sempre	↑ ↓	↑ ↓
Salta a la cadena ufw-track-output	Sempre	↑	↑ ↓

- Cadena Docker (i les seves regles)



The screenshot shows a table of rules for the 'Cadena DOCKER' chain. All rules have the action 'Accepta' (Accept) and the condition 'Si el protocol és TCP i la destinació és 172.17.0.4/32 i la intereficie d'entrada no és docker0 i la intereficie de sortida és docker0 i el port de destinació és [port]'. The table has columns for Acció (Action), Condició (Condition), Desplaça (Move), and Afegeix (Add).

Acció	Condició	Desplaça	Afegeix
Accepta	Si el protocol és TCP i la destinació és 172.17.0.4/32 i la intereficie d'entrada no és docker0 i la intereficie de sortida és docker0 i el port de destinació és 9300	↑	↑ ↓
Accepta	Si el protocol és TCP i la destinació és 172.17.0.4/32 i la intereficie d'entrada no és docker0 i la intereficie de sortida és docker0 i el port de destinació és 9200	↑ ↓	↑ ↓
Accepta	Si el protocol és TCP i la destinació és 172.17.0.5/32 i la intereficie d'entrada no és docker0 i la intereficie de sortida és docker0 i el port de destinació és 5601	↑ ↓	↑ ↓
Accepta	Si el protocol és TCP i la destinació és 172.17.0.6/32 i la intereficie d'entrada no és docker0 i la intereficie de sortida és docker0 i el port de destinació és 9600	↑ ↓	↑ ↓
Accepta	Si el protocol és TCP i la destinació és 172.17.0.6/32 i la intereficie d'entrada no és docker0 i la intereficie de sortida és docker0 i el port de destinació és 6053	↑ ↓	↑ ↓
Accepta	Si el protocol és TCP i la destinació és 172.17.0.6/32 i la intereficie d'entrada no és docker0 i la intereficie de sortida és docker0 i el port de destinació és 6052	↑ ↓	↑ ↓
Accepta	Si el protocol és TCP i la destinació és 172.17.0.6/32 i la intereficie d'entrada no és docker0 i la intereficie de sortida és docker0 i el port de destinació és 6051	↑ ↓	↑ ↓
Accepta	Si el protocol és TCP i la destinació és 172.17.0.6/32 i la intereficie d'entrada no és docker0 i la intereficie de sortida és docker0 i el port de destinació és 6050	↑ ↓	↑ ↓

Nom i Cognoms	Data
Arnau Subirós Puigarnau	24-03-2019

- Cadena Docker-Isolation-Stage-1(i les seves regles)

Cadena DOCKER-ISOLATION-STAGE-1

Acció	Condició	Desplaça	Afegeix
<input type="checkbox"/> Salta a la cadena DOCKER-ISOLATION-STAGE-2	Si la interfície d'entrada és docker0 i la interfície de sortida no és docker0		
<input type="checkbox"/> Salta a la cadena DOCKER-ISOLATION-STAGE-2	Si la interfície d'entrada és br-32cfbc9efdff i la interfície de sortida no és br-32cfbc9efdff		
<input type="checkbox"/> a la Cadena de sortida	Sempre		

Selecciona-ho tot

- Cadena Docker-Isolation-Stage-2(i les seves regles)

Cadena DOCKER-ISOLATION-STAGE-2

Acció	Condició	Desplaça	Afegeix
<input type="checkbox"/> Destruix	Si la interfície de sortida és docker0		
<input type="checkbox"/> Destruix	Si la interfície de sortida és br-32cfbc9efdff		
<input type="checkbox"/> a la Cadena de sortida	Sempre		

Selecciona-ho tot

- Cadena Docker-User(i les seves regles)

Cadena DOCKER-USER

Acció	Condició	Desplaça	Afegeix
<input type="checkbox"/> Accepta	Si la interfície d'entrada no és docker0 i la interfície de sortida és docker0 i l'estat de la connexió és RELATED,ESTABLISHED		
<input type="checkbox"/> Destruix	Si la interfície d'entrada no és docker0 i la interfície de sortida és docker0		
<input type="checkbox"/> a la Cadena de sortida	Sempre		

Selecciona-ho tot

**Nom i Cognoms**

Arnau Subirós Puigarnau

**Data**

24-03-2019

- **Cadena UFW-After-Input**

**Cadena ufw-after-input**

Selecciona-ho tot  Inverteix la selecció

Acció	Condició	Desplaça	Afegeix
<input type="checkbox"/> Salta a la cadena ufw-skip-to-policy-input	Si el protocol és UDP i el port de destinació és 137		
<input type="checkbox"/> Salta a la cadena ufw-skip-to-policy-input	Si el protocol és UDP i el port de destinació és 138		
<input type="checkbox"/> Salta a la cadena ufw-skip-to-policy-input	Si el protocol és TCP i el port de destinació és 139		
<input type="checkbox"/> Salta a la cadena ufw-skip-to-policy-input	Si el protocol és TCP i el port de destinació és 445		
<input type="checkbox"/> Salta a la cadena ufw-skip-to-policy-input	Si el protocol és UDP i el port de destinació és 67		
<input type="checkbox"/> Salta a la cadena ufw-skip-to-policy-input	Si el protocol és UDP i el port de destinació és 68		
<input type="checkbox"/> Salta a la cadena ufw-skip-to-policy-input	Sempre		

Selecciona-ho tot  Inverteix la selecció

Suprimeix la Cadena  Buida Totes les Regles  Afegeix Regla

Renomena la Cadena  Suprimeix les Seleccionades  Desplaça les Seleccionades

- **Cadena UFW-After-logging-forward**

**Cadena ufw-after-logging-forward**

Selecciona-ho tot  Inverteix la selecció

Acció	Condició	Desplaça	Afegeix
<input type="checkbox"/> Registra el paquet	Si el ritme és menor que 3/min i el ritme inicial és menor que 10		

Selecciona-ho tot  Inverteix la selecció

Suprimeix la Cadena  Buida Totes les Regles  Afegeix Regla

Renomena la Cadena  Suprimeix les Seleccionades  Desplaça les Seleccionades

- **Cadena UFW-After-loginn-input**

**Cadena ufw-after-logging-input**

Selecciona-ho tot  Inverteix la selecció

Acció	Condició	Desplaça	Afegeix
<input type="checkbox"/> Registra el paquet	Si el ritme és menor que 3/min i el ritme inicial és menor que 10		

Selecciona-ho tot  Inverteix la selecció

Suprimeix la Cadena  Buida Totes les Regles  Afegeix Regla

Renomena la Cadena  Suprimeix les Seleccionades  Desplaça les Seleccionades

**Nom i Cognoms**
**Data**

Arnau Subirós Puigarnau

24-03-2019

- **Cadena UFW-Before-forward**

**Cadena ufw-before-forward**

Selecciona-ho tot  Inverteix la selecció

Acció	Condició	Desplaça	Afegeix
Accepta	Si state of connection is RELATED,ESTABLISHED	↑ ↓	↑ ↓
Accepta	Si el protocol és ICMP i el tipus ICMP és 3	↑ ↓	↑ ↓
Accepta	Si el protocol és ICMP i el tipus ICMP és 4	↑ ↓	↑ ↓
Accepta	Si el protocol és ICMP i el tipus ICMP és 11	↑ ↓	↑ ↓
Accepta	Si el protocol és ICMP i el tipus ICMP és 12	↑ ↓	↑ ↓
Accepta	Si el protocol és ICMP i el tipus ICMP és 8	↑ ↓	↑ ↓
Salta a la cadena ufw-user-forward	Sempre	↑ ↓	↑ ↓

Selecciona-ho tot  Inverteix la selecció

**Buida Totes les Regles** **Suprimeix la Cadena** **Suprimeix les Selecionades** **Afegeix Regla** **Renomena la Cadena** **Desplaça les Selecionades**

- **Cadena UFW-Before-input**

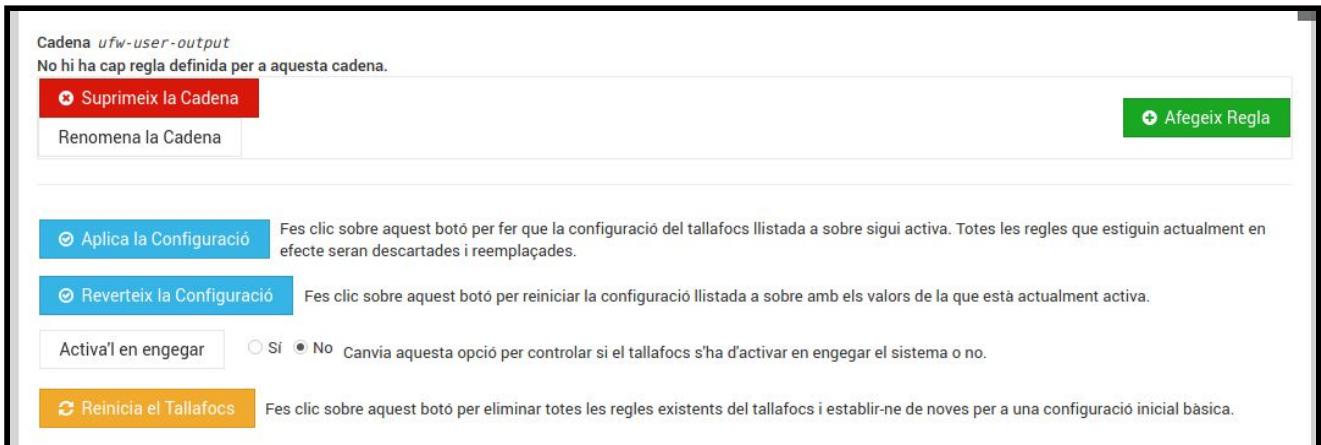
**Cadena ufw-before-input**

Selecciona-ho tot  Inverteix la selecció

Acció	Condició	Desplaça	Afegeix
Accepta	Si la intereficie d'entrada és lo	↑ ↓	↑ ↓
Accepta	Si state of connection is RELATED,ESTABLISHED	↑ ↓	↑ ↓
Salta a la cadena ufw-logging-deny	Si state of connection is INVALID	↑ ↓	↑ ↓
Destruïx	Si state of connection is INVALID	↑ ↓	↑ ↓
Accepta	Si el protocol és ICMP i el tipus ICMP és 3	↑ ↓	↑ ↓
Accepta	Si el protocol és ICMP i el tipus ICMP és 4	↑ ↓	↑ ↓
Accepta	Si el protocol és ICMP i el tipus ICMP és 11	↑ ↓	↑ ↓
Accepta	Si el protocol és ICMP i el tipus ICMP és 12	↑ ↓	↑ ↓
Accepta	Si el protocol és ICMP i el tipus ICMP és 8	↑ ↓	↑ ↓
Accepta	Si el protocol és UDP i el port de destinació és 68 i el port origen és 67	↑ ↓	↑ ↓
Salta a la cadena ufw-not-local	Sempre	↑ ↓	↑ ↓
Accepta	Si el protocol és UDP i la destinació és 224.0.0.251/32 i el port de destinació és 5353	↑ ↓	↑ ↓
Accepta	Si el protocol és UDP i la destinació és 239.255.255.250/32 i el port de destinació és 1900	↑ ↓	↑ ↓
	Sempre	↑ ↓	↑ ↓

Nom i Cognoms	Data
Arnau Subirós Puigarnau	24-03-2019

- I després de totes les cadenes ( s'ha volgut seleccionar les més importants). Hi ha varis opçions per aplicar al servidor



Cadena `ufw-user-output`  
 No hi ha cap regla definida per a aquesta cadena.

Suprimeix la Cadena  Renomena la Cadena  Afegeix Regla

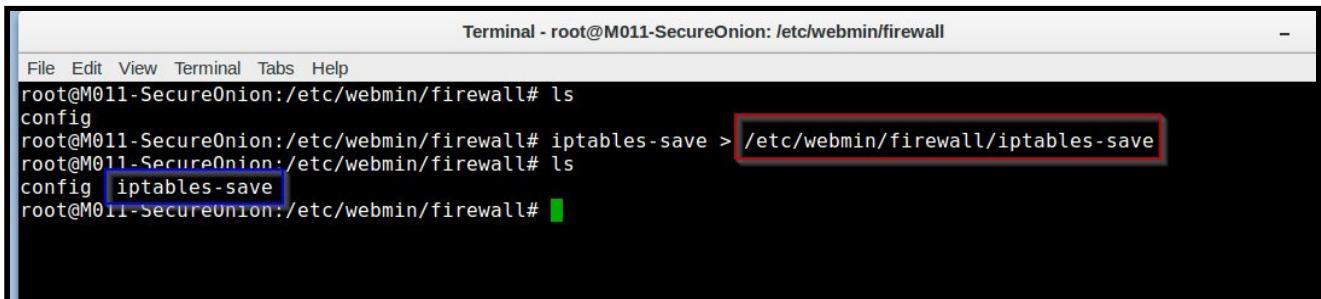
Aplica la Configuració Fes clic sobre aquest botó per fer que la configuració del tallafocs llistada a sobre sigui activa. Totes les regles que estiguin actualment en efecte seran descartades i reemplaçades.

Reverteix la Configuració Fes clic sobre aquest botó per reiniciar la configuració llistada a sobre amb els valors de la que està actualment activa.

Sí  No Canvia aquesta opció per controlar si el tallafocs s'ha d'activar en engegar el sistema o no.

Reinicia el Tallafocs Fes clic sobre aquest botó per eliminar totes les regles existents del tallafocs i establir-ne de noves per a una configuració inicial bàsica.

- Per guardar les regles desde la consola guardo les regles al arxiu: `iptables.save`



```
Terminal - root@M011-SecureOnion: /etc/webmin/firewall
File Edit View Terminal Tabs Help
root@M011-SecureOnion:/etc/webmin/firewall# ls
config
root@M011-SecureOnion:/etc/webmin/firewall# iptables-save > /etc/webmin/firewall/iptables-save
root@M011-SecureOnion:/etc/webmin/firewall# ls
config  iptables-save
root@M011-SecureOnion:/etc/webmin/firewall#
```

- Avantatges d'administrar Iptables amb Webmin

Com s'ha pogut veure anteriorment, Webmin es una eina de configuració basada en tecnologia web per l'administració de servidors Linux

- ❖ Es una eina molt potent que agilitza molt, ja que utilitza una interfície gràfica
- ❖ Al administrar Iptables tenim moltes opciones per filtrar
- ❖ Al crear una regla, hem d'omplir allo que necessitem, com un formulari.
- ❖ Fent-ho més senzill per al usuari ja que tot i la complexitat, no hem d'escriure manualment les regles

Nom i Cognoms	Data
Arnau Subirós Puigarnau	24-03-2019

## **Tasca 3:**

Abans de començar amb les configuracions bàsiques de squid convé contextualitzar-se una mica.  
 Llegiu el següent link i contesteu les preguntes que venen a continuació  
[http://www.ite.educacion.es/formacion/materiales/85/cd/linux/m6/proxy\\_squid.html](http://www.ite.educacion.es/formacion/materiales/85/cd/linux/m6/proxy_squid.html)

1. Menciona amb les teves paraules els avantatges i inconvenients de la utilització dels Proxy
2. En el link es parla de squid. Existeixen altres opcions a squid per a la configuració de proxys?
3. Explica les opcions d'autenticació
4. Digues quines possibilitats en ofereixen les ACL's.
5. Que vol dir que squid pot treballar en mode transparent?
6. Com es configura els clients perquè utilitzin els Proxy que volem?
7. Té fitxer de log squid? Busca a la xarxa algun exemple i analitza'l breument

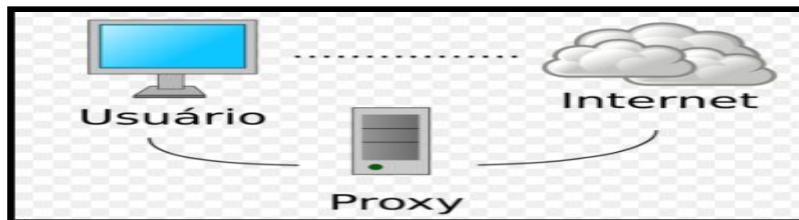
Ara, seguiu les configuracions de la pràctica del link que s'ha adjuntat a la tasca 1 i comproveu-ne el funcionament.

### **1. ¿QUE ÉS UN PROXY ?**

Un proxy serveix per a permetre l'accés a Internet a tots els equips d'una organització quan solament es pot disposar d'un únic equip connectat, això és, una única adreça IP. És a dir, intercepta el trànsit en la xarxa.

Els servidors proxy són màquines que acceleren la navegació emmagatzemant còpies locals dels llocs web que nosaltres normalment visitem. Això significa que després que nosaltres accedim a un lloc per primera vegada, no haurem d'esperar una altra vegada que la pàgina es carregui des d'un servidor web molt lent o molt llunyà.

Llavors els llocs web que ja hem visitat, es carreguen ràpidament des del proxy local. El servidor proxy també actualitza les pàgines cada vegada que tornem a visitar un lloc web.



Nom i Cognoms	Data
Arnau Subirós Puigarnau	24-03-2019

## 1.1. Avantatges d'utilitzar Proxy

- ❑ **Control:** Solament l'intermediari fa el treball real, per tant es poden limitar i restringir els drets dels usuaris, i donar permisos solament al proxy.
- ❑ **Estalvi:** Per tant, solament un dels usuaris (el proxy) ha d'estar equipat per a fer el treball real.
- ❑ **Velocitat:** Si diversos clients demanen el mateix recurs, el proxy pot fer de caixet: guardar la resposta d'una petició per a donar-la directament quan un altre usuari la demanés. Així d'aquesta manera no ha de tornar a contactar amb la destinació, i acaba sent més ràpid.
- ❑ **Filtrat:** El proxy pot negar-se a respondre algunes peticions si detecta que estan prohibides, gràcies a les polítiques de seguretat.
- ❑ **Modificació:** Com a intermediari que és, un proxy pot falsificar informació, o modificar-la seguint un algorisme.

## 1.2. Inconvenients d'utilitzar Proxy

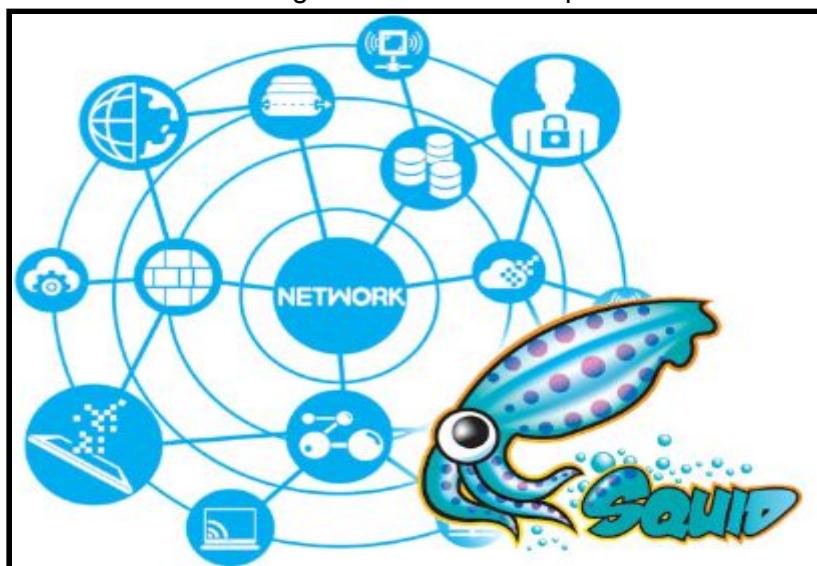
- ❑ **Abús:** En estar disposat a rebre peticions de molts usuaris i respondre'ls, és possible que faci algun treball que no toca. Per tant, ha de controlar qui té accés i qui no, cosa que normalment és molt difícil.
- ❑ **Càrrega:** Un proxy ha de fer el treball de molts usuaris.Intromissió (és un pas més entre l'origen i la destinació), i alguns usuaris poden no voler passar pel proxy. I menys si fa de caixet i guarda còpies de les dades.
- ❑ **Irregularitat:** El fet que el proxy representi a més d'un usuari dóna problemes en molts escenaris, en concret els quals suposen una comunicació directa entre un emissor i un receptor (com TCP/IP)
- ❑ **Anonimat:** Si tots els usuaris s'identifiquen com un només, és difícil que el recurs accedit pugui diferenciar-los. Però això pot ser dolent, per exemple quan cal fer la identificació.

Nom i Cognoms	Data
Arnau Subirós Puigarnau	24-03-2019

## 2. SQUID

És un servidor proxy de Linux que guarda les pàgines web visitades per sol·licituds posteriors ( si intentes visita la mateixa pàgina web o una altre, la facilitarà desde el servidor proxy)

- Fa que la navegació web sigui més ràpida i redueix el tràfic
- Els servidors de enmagatzemament en cache poden reduir molt tràfic extern.



### 2.1. Eines complementaries a SQUID

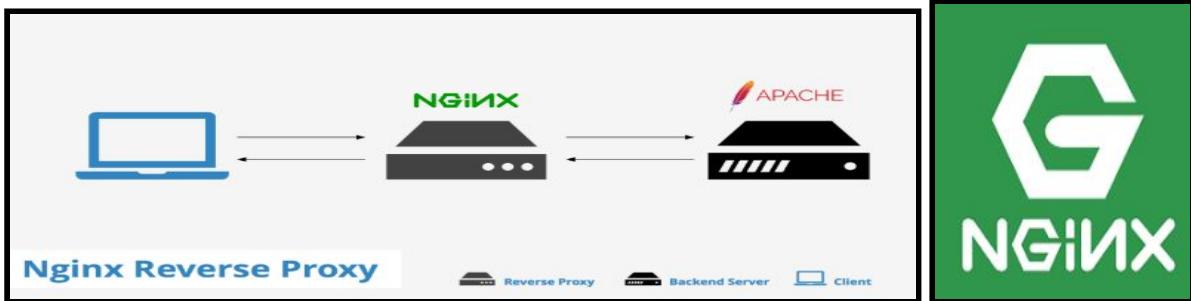
- 2.1.1. **DansGuardian**: Ajudar a bloquejar els llocs potencialment perillosos en la red local . Se situa entre el navegador client i el Proxy. En instal·lar el paquet la configuració per defecte ja limita les visites a pàgines prohibides per a menors, però disposa de gran quantitat d'arxius de configuració per a dur a terme un ajust del servei més personalitzat.



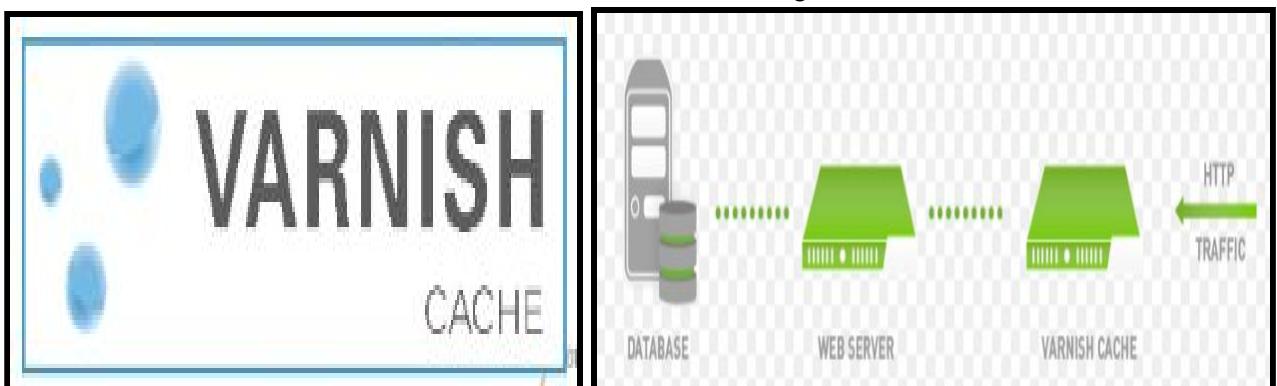
Nom i Cognoms	Data
Arnau Subirós Puigarnau	24-03-2019

## 2.2. Alternatives a SQUID

- 2.2.1. **Nginx**: És un proxy orientat al protocol HTTP i HTTPS , tot i que també podria actuar sobre el protocol IMAP (correo electrònic)



- 2.2.2. **Varnish**: El servidor on es troba el contingut de la pàgina web inicia Varnish directament com un proxy invers. Quan un usuari visita el web, la sol·licitud és processada inicialment pel servidor original, mentre que el Varnish emmagatzema la sol·licitud i els continguts. Així, quan el servidor rep una sol·licitud semblant, les dades es carregaran directament des Varnish Cache.



Nom i Cognoms	Data
Arnau Subirós Puigarnau	24-03-2019

### 3. OPCIONS D'AUTENTIFICACIÓ DEL SQUID

Aquí s'estableixen les opcions d'autenticació del Proxy. Es pot configurar SQUID perquè sol·liciti usuari i contrasenya per a poder navegar per Internet.

- Si es vol fer ús d'aquesta funcionalitat, el normal seria tenir emmagatzemats els usuaris i les contrasenyes en un servidor LDAP i en funció dels grups als quals pertanyin els usuaris, podríem habilitar o deshabilitar l'accés.
  - Això pot ser interessant en empreses, on l'administrador de xarxa dóna accés a Internet sola als usuaris que ho necessiten.
  - En un centre educatiu suposaria bastant treball portar una administració d'aquest tipus ja que caldria crear i gestionar un usuari per a cada alumne i per a cada professor. És més fàcil administrar per xarxes i per aules.

#### 3.1. Requisits

Per dur a la pràcticar l'accés a Squid per autentificació necessitarem :

- Squid
- Servidor Apache
- Servidor Openldap

#### 3.2. Mòdul d'autentificació

- 3.2.1. Mòdul LDAP: Suposant que s'ha configurat correctament OpenLDAP com a servidor d'autentificació , necessitarem definir el directori ( o subdirector ) i el servidor LDAP a utilitzar

La sintaxis utilizada para squid\_ldap\_auth és la següent:

**squid\_ldap\_auth -b "Directori\_a\_utilitzar" servidor-ldap-a-utilizar**

exemple: squid\_ldap\_auth -b "cn=arsupu,dc=fje,dc=edu" 127.0.0.1

- 3.2.2. Mòdul NCSA :Squid pot utilitzar el mòdul ncsa\_\*auth, de la NCSA (National Center for Supercomputing Applications), ja que ve inclòs com a part del paquet principal de Squid en la majoria de les distribucions actuals. Aquest mòdul proveeix una autenticació molt senzilla a través d'un fitxer de text simple les claus del qual d'accés van ser creades amb htpassw

#### EXAMPLE:

- Creem un arxiu buit en el directori squid

arsupu@server:~# sudo touch /etc/squid/claus\_squid

Nom i Cognoms	Data
Arnau Subirós Puigarnau	24-03-2019

- Fem que aquest arxiu només tingui permis d'escriptura i lectura el usuari squid

```
arsupu@server:~# sudo chmod 600 /etc/squid/claus_squid
arsupu@server:~# sudo chown squid:squid /etc/squid/claus_squid
```

- A continuació haurem de donar d'alta els comptes necessaris utilitzant el comando "htpasswd"

```
arsupu@server:~# sudo htpasswd /etc/squid/claus_squid Arnau_SP
```

### 3.2.2.1. Mòdul NCSA -Paràmetres en /etc/squid/squid.conf

- S'ha d'especificar que programa d'autentificació s'utilitzarà. Per defecte no està especificat cap programa
- El mòdul NCSA (**ncsa\_auth**) es localitza a **/usr/lib/squid/ncsa\_auth** procedim afegir-lo amb el següent paràmetre:**sudo auth\_param basic program /usr/lib/squid/ncsa\_auth /etc/squid/claus\_squid**

## 4. CONTROL D'ACCÉS (ACL) DEL SQUID

- Especificarem una denominada passwd la qual es configurarà per a utilitzar obligatòriament l'autenticació per a poder accedir a Squid. Ha de localitzar-se la secció de Llistes de Control d'Accés i afegir-se la següent línia:

```
acl password proxy_*auth REQUIRED
```

- Havent fet això , haurem de tenir en la secció de Llistes de Control d'Accés així:

```
# Recommended minimum configuration:
acl all src 0.0.0.0/0.0.0.0
acl manager proto cache_object
acl localhost src 127.0.0.1/255.255.255.255
acl redlocal src 192.168.1.0/255.255.255.0
acl password proxy_auth REQUIRED
```

- Procedim llavors a modificar la regla de control d'accisos que ja teníem per a permetre l'accés a Internet. On abans teníem el següent:

```
http_access allow redlocal
```

Nom i Cognoms	Data
Arnau Subirós Puigarnau	24-03-2019

- Li afegim passwd, la definició de la Llista de Control d'Accés que requereix utilitzar clau d'accés, a la nostra regla actual, de manera que quedi com vam mostrar a continuació:  
`http_access allow redlocal password`
- Havent fet l'anterior, la zona de regles de control d'accés hauria de quedar més o menys d'aquesta manera:

```

#
# INSERT YOUR OWN RULE(S) HERE TO allow ACCESS FROM YOUR CLIENTS
#
http_access allow redlocal
http_access allow redlocal password

http_access deny all

```

- Finalment procedim a reiniciar Squid perquè tinguin efecte els canvis.

```
arsupu@server:~# sudo systemctl restart squid
```

## 5. PROXY TRANSPARENT AMB SQUID

- Configurar Squid en mode transparent fa que l'usuari, o dispositiu, no necessiti executar cap configuració per a navegació, sent aquestes assignades a l'arquitectura de seguretat.
- Fàcil implementació, però previament es necessari conèixer com treballar l'aplicació per evitar problemes:
  - ❖ Això es deu al fet que el funcionament de l'estructura de proxy transparent es produeix a través de la redirecció de trànsit en el port 80 per al servei intern del proxy, i hi ha molts altres ports que poden utilitzar el protocol HTTP o el mètode CONNECT que no passaran per aquesta regla.
- Encaminar el trànsit de tots els ports al proxy, d'altra banda, no és una opció perquè no coneix el funcionament d'altres protocols, la qual cosa farà que altres aplicacions no HTTP deixin de funcionar.

Nom i Cognoms	Data
Arnau Subirós Puigarnau	24-03-2019

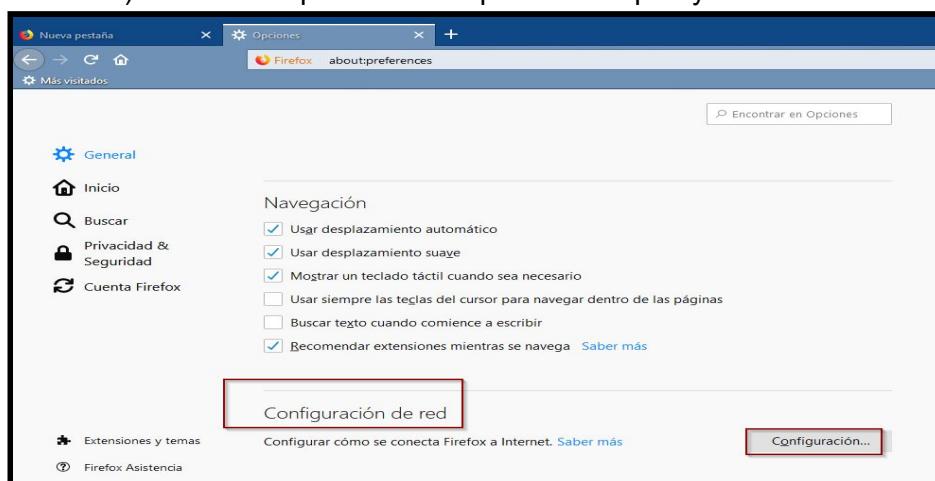
- Hem de tenir en compte que bona part de les aplicacions web actualment utilitzen connexions HTTPS (port 443), llavors és necessari també que el proxy posseeixi la característica d'interacció amb aquest tipus de trànsit
- Un altre aspecte interessant és el **recurs de caching** que molts posseeixen de manera integrada. Aquesta facilitat permet l'estalvi de banda ja que els objectes d'Internet s'emmagatzemem en memòria o emmagatzematge secundari i es descarreguen localment (sense l'ús d'Internet) per als usuaris que sol·licitin

### 5.1. Limitacions del Mode Transparent amb Squid

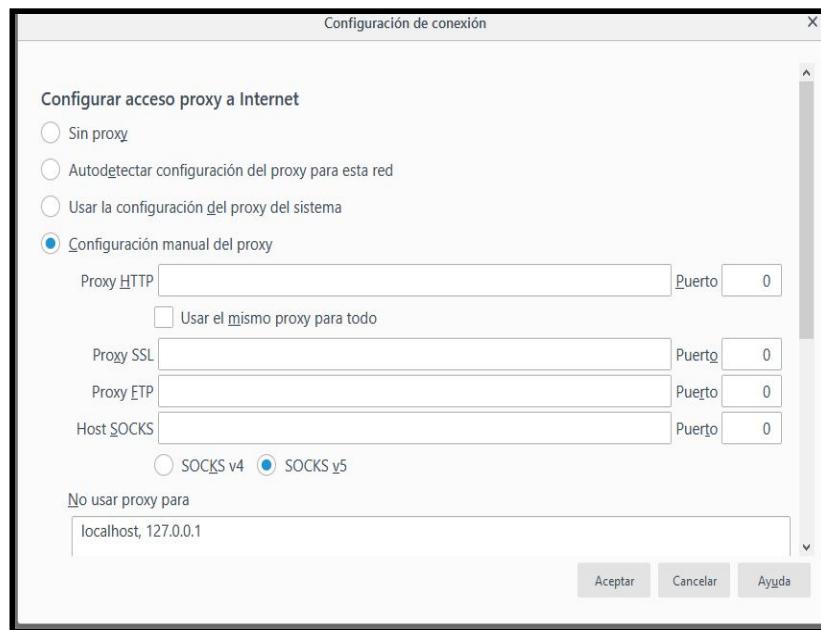
- L'ús d'HTTPS dins d'una estructura de proxy depèn que el servei intercepti la connexió i lliuri un certificat propi, que deu ser acceptat pel client per a donar continuïtat a la comunicació. Aquest procés, tret que l'equip tingui el certificat importat, generarà una alerta per a l'usuari de connexió insegura.
- S'ha de tenir en compte quan s'utilitza aquest mode ja que no tota aplicació es basa en el protocol HTTP. Això significa que milers d'altres ports poden passar per fora del proxy, facilitant fins i tot l'estructura de bypass.

## 6. CONFIGURACIÓ DEL PROXY EN EL CLIENT

- Hi ha diverses formes per a configurar els clients perquè utilitzin el proxy. Una opció senzilla seria configurar directament els navegadors clients ( Mozilla Firefox, Chrome..) de manera que emitin les peticions al proxy de la nostra xarxa



Nom i Cognoms	Data
Arnau Subirós Puigarnau	24-03-2019



Nom i Cognoms	Data
Arnau Subirós Puigarnau	24-03-2019

## 7. LOGS DE SQUID

Hi ha diversos arxius de registre mantinguts per Squid. Alguns han d'activar-se explícitament durant el temps de compilació, uns altres poden desactivar-se de manera segura durant el temps d'execució

**7.1. cache.log** : Conté els missatges de depuració i error que genera Squid. Si s'inicia el Squid usant l'opció de línia de comando **-s** , una còpia de certs missatges anirà a **syslog**. És una qüestió de preferències personals utilitzar un arxiu separat per a les dades de registre de Squid.

**7.2. acces.log** : La majoria de programes d'anàlisis de registre utilitzen aquesta entrada

7.2.1. **Squidview** : Utilitzant aquest programa pots monitoritzar el log de Squid /var/log/squid/acces.log de forma amigable, oferint informació amb més detall en temps real, permetent crear estadístiques en pantalla, IP o hosts registrar en el log.

7.2.2. **Format acces.log :**

```
1261571024.931 0 192.168.1.32 TCP_NEGATIVE_HIT/204 298 GET http://clients1.google.es/generate_204 - NONE/-text/html
1261574127.986 0 192.168.1.27 TCP_MEM_HIT/200 7324 GET
http://www.ajsolucionesinformaticas.com/imagenes/aecmycs/AjpdSoft_aecmycs_1.png - NONE/-image/PNG
```

Les dades que guarda per ordre:

- Data i hora en format Unix UTC
- Duració de la transacció ( temps de resposta)
- Direcció IP del client ( equip que fa la petició)
- Resultat de la transacció
- Tamany de la descarga
- Mètode de sol.licitud
- URL sol.licitada
- Codi de la jerarquia de la informació
  - TIME OUT
  - Codi que indica com ha sigut manejada la sol.licitud (ex: NONE)
  - IP o hostname de l'equip que fa la sol.licitud (: ex: TCP\_NEGATIVE\_HIT)
- Tipus d'objecte descargat( com indica en l'encapçalat HTTP)

**7.3. store.log** : En aquest arxiu hi ha els objectes actualment guardats en el disc o els eliminats, com un tipus de diari amb finalitats de depuració

Nom i Cognoms	Data
Arnau Subirós Puigarnau	24-03-2019

## 8. PRÀCTICA AMB SQUID

- Utilitzarem la màquina virtual- Secure Onion

Terminal - arsupu@M011-SecureOnion: ~

```

File Edit View Terminal Tabs Help
arsupu@M011-SecureOnion:~$ hostname
M011-SecureOnion
arsupu@M011-SecureOnion:~$ hostnamectl
    Static hostname: M011-SecureOnion
          Icon name: computer-vm
            Chassis: vm
        Machine ID: 220367b45a2e2544428637d15b635477
            Boot ID: 14a19bcacdbd4980acefd9710026e6bc
      Virtualization: oracle
Operating System: Ubuntu 16.04.5 LTS
      Kernel: Linux 4.15.0-43-generic
     Architecture: x86-64
arsupu@M011-SecureOnion:~$ 
```

- Revisem les intereficies enp0s3 i enp0s8
  - enps03(mode DHCP) per accés a Internet
  - enps08( mode estatic) pel servidor Proxy

Terminal - arsupu@M011-SecureOnion: ~

```

File Edit View Terminal Tabs Help
arsupu@M011-SecureOnion:~$ ip a | grep enp0s3
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP
group default qlen 1000
    inet 192.168.1.66/24 brd 192.168.1.255 scope global enp0s3
arsupu@M011-SecureOnion:~$ ip a | grep enp0s8
3: enp0s8: <BROADCAST,MULTICAST,NOARP,PROMISC,UP,LOWER_UP> mtu 1500 qdisc pfifo_
fast state UP group default qlen 1000
    inet 192.168.1.12/24 brd 255.255.255.255 scope global enp0s8
arsupu@M011-SecureOnion:~$ 
```

Nom i Cognoms	Data
Arnau Subirós Puigarnau	24-03-2019

- Instal·lem SQUID

```
Terminal - arsupu@M011-SecureOnion: ~
File Edit View Terminal Tabs Help
arsupu@M011-SecureOnion:~$ sudo apt-get install squid
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages were automatically installed and are no longer required:
  girl1.2-appindicator3-0.1 girl1.2-javascriptcoregtk-4.0 girl1.2-nma-1.0
  girl1.2-timezonemap-1.0 girl1.2-webkit2-4.0 libtimezonemap-data libtimezonemap1
Use 'sudo apt autoremove' to remove them.
The following additional packages will be installed:
  libcap3 squid-common squid-langpack
Suggested packages:
  squidclient squid-cgi squid-purge smbclient winbindd
The following NEW packages will be installed:
  libcap3 squid squid-common squid-langpack
0 upgraded, 4 newly installed, 0 to remove and 129 not upgraded.
Need to get 2,655 kB of archives.
After this operation, 10.8 MB of additional disk space will be used.
Do you want to continue? [Y/n] █
```

- Revisem el seu status

```
Terminal - arsupu@M011-SecureOnion: ~
File Edit View Terminal Tabs Help
arsupu@M011-SecureOnion:~$ sudo systemctl status squid.service
● squid.service - LSB: Squid HTTP Proxy version 3.x
  Loaded: loaded (/etc/init.d/squid; bad; vendor preset: enabled)
  Active: active (running) since Sat 2019-03-23 10:57:21 UTC; 18s ago
    Docs: man:systemd-sysv-generator(8)
   CGroup: /system.slice/squid.service
           └─5396 /usr/sbin/squid -YC -f /etc/squid/squid.conf
               ├─5406 (squid-1) -YC -f /etc/squid/squid.conf
               ├─5407 (logfile-daemon) /var/log/squid/access.log
               └─5432 (pinger)

Mar 23 10:57:21 M011-SecureOnion systemd[1]: Stopped LSB: Squid HTTP Proxy version 3.x.
Mar 23 10:57:21 M011-SecureOnion systemd[1]: Starting LSB: Squid HTTP Proxy version 3.x...
Mar 23 10:57:21 M011-SecureOnion squid[5329]: * Starting Squid HTTP Proxy squid
Mar 23 10:57:21 M011-SecureOnion squid[5329]: ...done.
Mar 23 10:57:21 M011-SecureOnion systemd[1]: Started LSB: Squid HTTP Proxy version 3.x.
arsupu@M011-SecureOnion:~$ █
```

Nom i Cognoms	Data
Arnau Subirós Puigarnau	24-03-2019

- Configuració /etc/squid/squid.conf

Terminal - arsupu@M011-SecureOnion: /etc/squid

```
File Edit View Terminal Tabs Help
arsupu@M011-SecureOnion:/etc/squid$ sudo gedit squid.conf
```

- Afegim el nom del hostname

```
#Default.
# httpd_suppress_version_string off

# TAG: visible_hostname
visible_hostname M011-SecureOnion

# If you want to present a special hostname in error messages
# define this. Otherwise, the return value of gethostname()
# will be used. If you have multiple caches in a cluster
# get errors about IP-forwarding you must set them all
# with this setting.
#Default.
```

```
#

# Squid normally listens to port 3128
http_port 3128

# TAG: https_port
# Note: This option is only available if Squid was built with SSL support
```

- Fem un exemple senzill per confirmar que funciona

```
### EXEPLE ACL

acl block1 url_regex as facebook
http_access deny block1

# TAG: clientside_tos
# Allows you to select a TOS/DSCP value for packets
# on the client-side, based on an ACL.
#
```

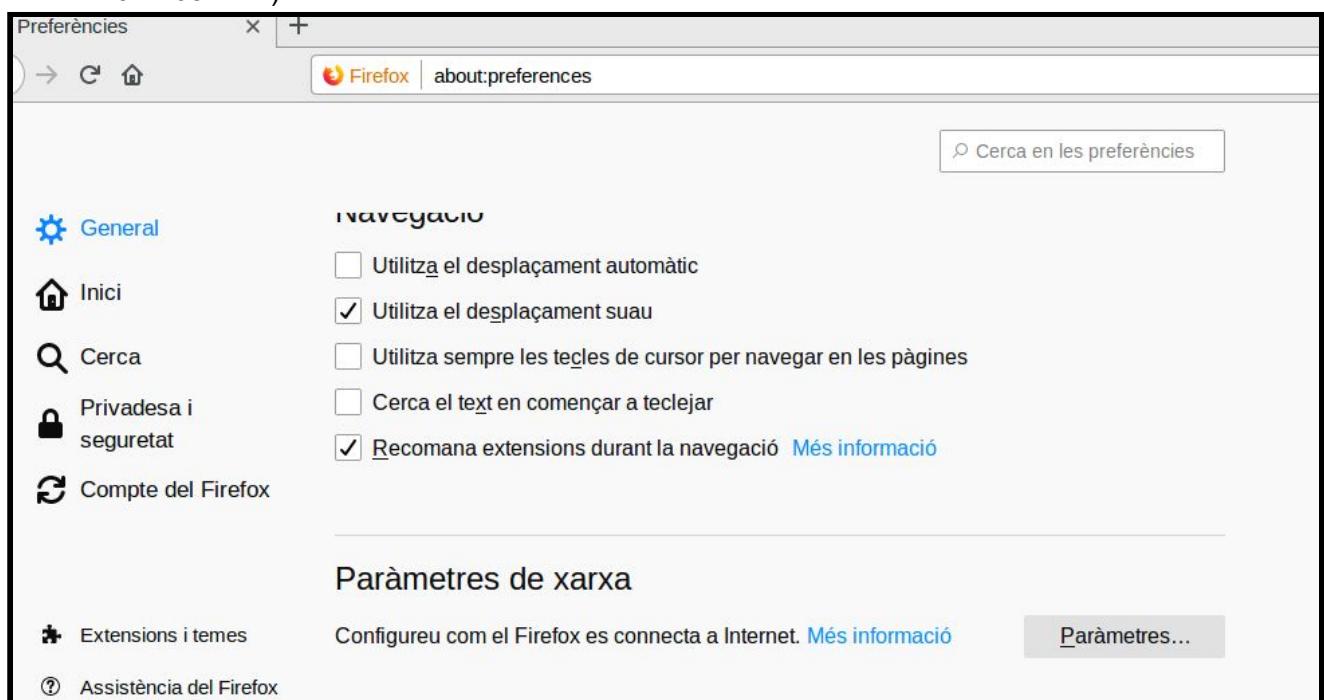
Nom i Cognoms	Data
Arnau Subirós Puigarnau	24-03-2019

- Tornem a iniciar el servei Squid

```
arsupu@M011-SecureOnion:~$ sudo systemctl start squid
arsupu@M011-SecureOnion:~$ sudo systemctl status squid
● squid.service - LSB: Squid HTTP Proxy version 3.x
  Loaded: loaded (/etc/init.d/squid; bad; vendor preset: enabled)
  Active: active (running) since Sat 2019-03-23 11:56:46 UTC; 1s ago
    Docs: man:systemd-sysv-generator(8)
 Process: 27360 ExecStop=/etc/init.d/squid stop (code=exited, status=0/SUCCESS)
 Process: 27467 ExecStart=/etc/init.d/squid start (code=exited, status=0/SUCCESS)
   Tasks: 4
  Memory: 19.8M
    CPU: 172ms
   CGroup: /system.slice/squid.service
           ├─27524 /usr/sbin/squid -YC -f /etc/squid/squid.conf
           ├─27526 (squid-1) -YC -f /etc/squid/squid.conf
           ├─27527 (logfile-daemon) /var/log/squid/access.log
           └─27528 (pinger)

Mar 23 11:56:46 M011-SecureOnion systemd[1]: Starting LSB: Squid HTTP Proxy version 3.x.
Mar 23 11:56:46 M011-SecureOnion squid[27467]: * Starting Squid HTTP Proxy squid
...
```

- CLIENT: Configurem al navegador web ( Firefox) els paràmetres de xarxa, configuració del servidor intermediari per accedir a Internet. Anotem la IP del nostre servidor Proxy ( 192.168.1.12)



Nom i Cognoms	Data
Arnau Subirós Puigarnau	24-03-2019



- Confirmem que no podem accedir a Facebook, el nostre Proxy funciona.

**S'ha produït un problema** x | +

El servidor intermediari està rebutjant les connexions

El Firefox està configurat per utilitzar un servidor intermediari que està rebutjant les connexions.

- Comproveu els paràmetres del servidor intermediari per assegurar-vos que siguin correctes.
- Poseu-vos en contacte amb l'administrador de la xarxa per assegurar-vos que el servidor intermediari funciona.

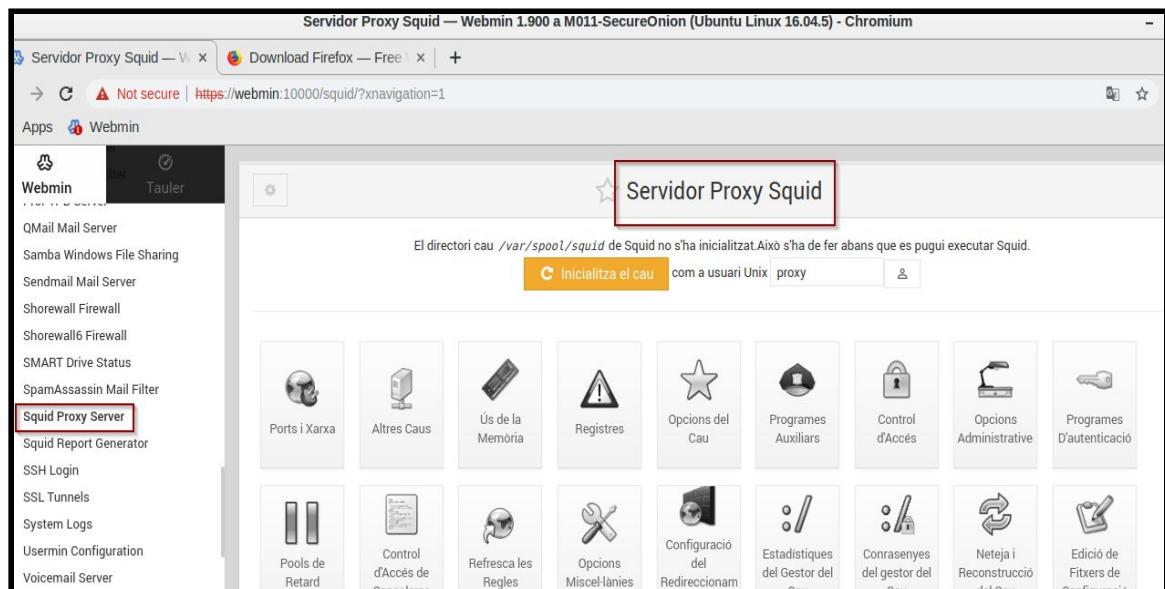
[Torna-ho a provar](#)

**Nom i Cognoms**
**Data**

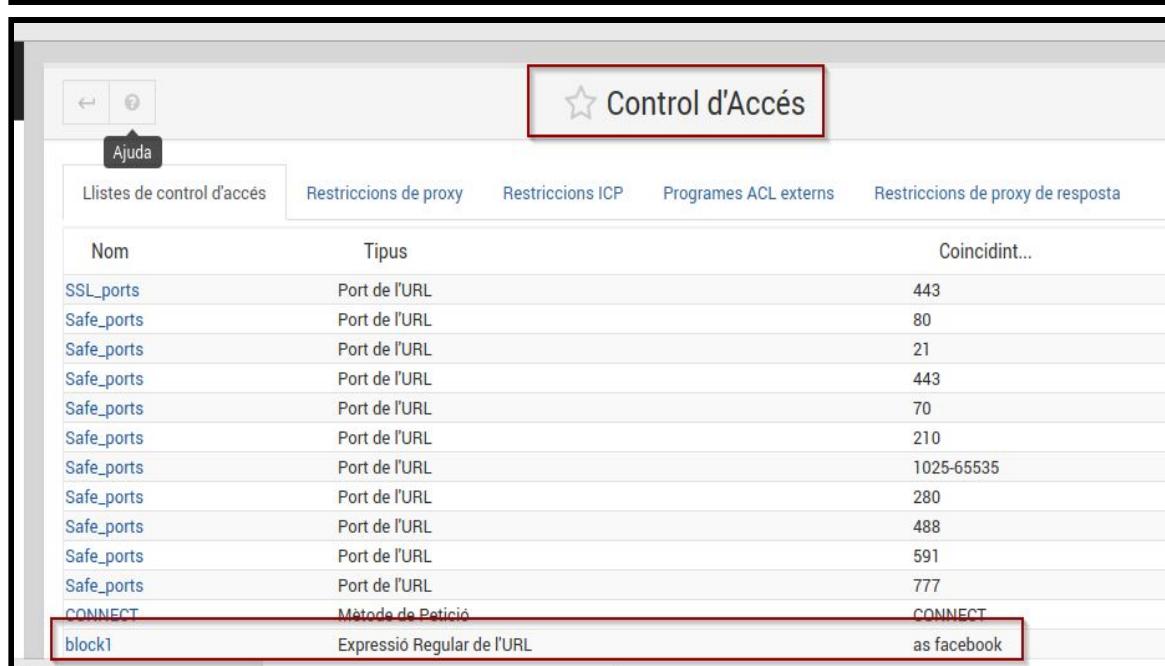
Arnau Subirós Puigarnau

24-03-2019

- Per finalitzar si volem modificar la configuració de Squid amb una intereficie gràfica podríem accedir a Webmin



The screenshot shows the Webmin interface for a Squid proxy server. The main title bar says "Servidor Proxy Squid — Webmin 1.900 a M011-SecureOnion (Ubuntu Linux 16.04.5) - Chromium". The left sidebar lists various services, with "Squid Proxy Server" highlighted. The main content area is titled "Servidor Proxy Squid" and contains a message about the Squid directory. Below it is a button labeled "Inicializa el cau". A grid of icons represents different configuration options like ports, memory usage, and statistics.

The screenshot shows the "Control d'Accés" (Access Control) configuration page. It has tabs for "Ajuda", "Listes de control d'accés", "Restriccions de proxy", "Restriccions ICP", "Programes ACL externs", and "Restriccions de proxy de resposta". The "Listes de control d'accés" tab is active. It displays a table of access control lists:

Nom	Tipus	Coincidint...
SSL_ports	Port de l'URL	443
Safe_ports	Port de l'URL	80
Safe_ports	Port de l'URL	21
Safe_ports	Port de l'URL	443
Safe_ports	Port de l'URL	70
Safe_ports	Port de l'URL	210
Safe_ports	Port de l'URL	1025-65535
Safe_ports	Port de l'URL	280
Safe_ports	Port de l'URL	488
Safe_ports	Port de l'URL	591
Safe_ports	Port de l'URL	777
CONNECT	Mètode de Petició	CONNECT
<b>block1</b>	Expressió Regular de l'URL	as facebook