



Configuración y securización de una red local mediante Webmin

Jorge Mas Freire

Ciclo Superior de Administración de Sistemas Informáticos en Redes

IES Medina Azahara

Fecha entrega: 15 de Junio de 2023



Esta obra está sujeta a una licencia de Reconocimiento
- No Comercial - Sin Obra Derivada [3.0 España de
Creative Commons](https://creativecommons.org/licenses/by-nc-nd/3.0/es/)

FICHA DEL PROYECTO FINAL

Título del trabajo:	Configuración y securización de una red local mediante Webmin.
Nombre del autor:	Jorge Mas Freire
Fecha de entrega (mm/aaaa):	06/2023
Área del Trabajo Final:	Administración de redes y seguridad informática.
Ciclo Grado Superior:	Administración de Sistemas Informáticos en Red
Resumen del Trabajo (máximo 250 palabras):	
<p>El presente proyecto consta en la configuración y securización básica de una red local mediante Webmin para un servidor Linux. Durante el proceso se demostrará que gracias a este software dicha tarea será más cómoda, rápida y sencilla para un administrador de red, resolviendo problemas como el de recordar rutas y sintaxis correcta. Los servicios que se van a configurar son: DHCP, DNS, Linux Firewall, Fail2Ban y Proxy Transparente. Por último, se realizará un seguimiento y control del estado de esos servicios con sus respectivas copias de seguridad.</p>	

Índice

Lista de imágenes.....	1
1. Introducción.....	3
1.1. Contexto y justificación del Proyecto.....	3
1.2. Objetivos del Proyecto.....	3
2. Propuesta de solución.....	4
2.1. Análisis descriptivo.....	4
2.2. Análisis de requisitos.....	4
3. Temporalización.....	5
3.1. Identificación de tareas.....	5
3.2. Secuenciación.....	6
4. Memoria técnica.....	7
4.1. Esquema de la red.....	7
4.2. Instalación Webmin.....	8
4.3. SERVIDOR DHCP.....	9
4.3.1. Explicación qué es el DHCP.....	9
4.3.2. Instalación del módulo de DHCP.....	9
4.3.3. Configuración básica DHCP server.....	10
4.3.4. Comprobación del servidor DHCP.....	13
4.4. SERVIDOR DNS.....	14
4.4.1. Explicación qué es el DNS.....	14
4.4.2. Instalación del módulo de DNS server.....	14
4.4.3. Configuración básica DNS server.....	15
4.4.4. Comprobación del DNS server.....	20
4.5. FAIL2BAN.....	20
4.5.1. Explicación qué es FAIL2BAN.....	20
4.5.2. Instalación del módulo de FAIL2BAN.....	21
4.5.3. Configuración del FAIL2BAN.....	21
4.5.4. Comprobación del FAIL2BAN.....	24
4.6. LINUX FIREWALL.....	24
4.6.1. Explicación qué es LINUX FIREWALL.....	24
4.6.2. Configuración del LINUX FIREWALL.....	25
4.6.3. Comprobación del LINUX FIREWALL.....	28
4.7. PROXY.....	29
4.7.1. Explicación qué es un PROXY TRANSPARENTE.....	29

4.7.2.	Instalación del módulo de PROXY.....	29
4.7.3.	Configuración del PROXY.	30
4.7.4.	Comprobación del PROXY.....	34
4.8.	Seguimiento y control.....	34
4.8.1.	Panel de control.....	34
5.	Estudio presupuestario.	38
6.	Conclusiones.	38
6.1.	Debilidades.....	39
6.2.	Amenazas.....	39
6.3.	Fortalezas.	39
6.4.	Oportunidades.	39
6.5.	Ampliaciones futuras.	39
6.6.	Escalabilidad.....	40
7.	Bibliografía. (Ralph Droms, 2002)	40
8.	Anexos.	40

Lista de imágenes:

Ilustración 1 - Diagrama de Gantt	6
Ilustración 2 - Esquema de la Red	7
Ilustración 3 - Panel de control Webmin.....	8
Ilustración 4 - Instalación del módulo DHCP	9
Ilustración 5 - Instalación de los paquetes de DHCP	9
Ilustración 6 - Panel principal DHCP.....	10
Ilustración 7 - Creación de una subnet.....	11
Ilustración 8 - Configuración del cliente	12
Ilustración 9 - Selección de la interfaz	13
Ilustración 10 - Comprobación del cliente	13
Ilustración 11 - Comprobación del archivo dhcpd.conf	14
Ilustración 12 - Instalación del módulo DNS.....	15
Ilustración 13 - Instalación de los paquetes DNS.....	15
Ilustración 14 - Panel principal DNS	15
Ilustración 15 - ACL de DNS.....	17
Ilustración 16 - Creación de la zona maestra.....	17
Ilustración 17- Creación de la zona inversa	18
Ilustración 18 - Creación de la dirección.....	18
Ilustración 19 - Editar la dirección	18
Ilustración 20 - Creación de un alias	19
Ilustración 21 - Comprobación de BIND CFG	19
Ilustración 22 - Edición de los registros	19
Ilustración 23 - Comprobación del DNS	20
Ilustración 24 - Instalación del módulo Fail2Ban.....	21
Ilustración 25 - Instalación de los paquetes Fail2Ban.....	21
Ilustración 26 -Panel principal Fail2Ban.....	21
Ilustración 27 - Selecccion de servicios	22
Ilustración 28 - Configuración de la regla para SSH	22
Ilustración 29 - Configuración de la regla para Webmin	23
Ilustración 30 - Comprobación Fail2Ban (1)	24
Ilustración 31 - Comprobación Fail2Ban (2)	24
Ilustración 32 - Panel principal Linux Firewall	25
Ilustración 33 - Creación regla SNAT	27
Ilustración 34 - Configuración reglas iptables Proxy	27
Ilustración 35 - Comprobación Linux Firewall.....	28
Ilustración 36 - Instalación módulo Squid Proxy	29
Ilustración 37 - Instalación paquetes Squid Proxy	29
Ilustración 38 - Panel principal Squid Proxy	30
Ilustración 39 - Creacion de la ACL en Squid Proxy	31
Ilustración 40 - Parámetros introducidos en ACL.....	32
Ilustración 41 - Comprobación de que la ACL se ha creado.....	32
Ilustración 42 - Campo Proxy restrictions.....	32
Ilustración 43 - Creación de la restricción Proxy.....	33
Ilustración 44 - Comprobación del archivo squid.conf	33
Ilustración 45 - Comprobación desde el cliente	34
Ilustración 46 - Panel de control	35

Ilustración 47 - Panel System and Server Status	35
Ilustración 48 - Creación de tarea de monitorización de los servicios	36
Ilustración 49 - Registro de Logs	36
Ilustración 50 - Creación de tare del backup (1).....	37
Ilustración 51 - Creación de tare del backup (2).....	37
Ilustración 52 - Recuperación del backup	38
Ilustración 53 -Acceso desde la terminal al servidor.....	40

1. Introducción.

En el presente proyecto técnico, se aborda la configuración y securización de una red local mediante el uso de Webmin, el cual es un software que te permite modificar parámetros de un servidor vía web. El enfoque principal se centra en la configuración básica de servicios esenciales como DHCP, DNS, Fail2ban, Firewall y Proxy, aprovechando su interfaz gráfica que es intuitiva y más rápida que la configuración manual.

1.1. Contexto y justificación del Proyecto.

Como administrador de servidores se puede perder mucho tiempo en la configuración desde 0 de un servidor y luego al realizar cambios para su mantenimiento si tienes que recordar donde están todos los archivos de configuración y editarlos manualmente, pudiendo cometer fácilmente errores hasta el administrador más avanzado. Por ello, en este proyecto se ofrece la configuración y securización (DHCP, DNS, Fail2Ban, Firewall y Proxy) básica de la red mediante Webmin que puede facilitar mucho la configuración del sistema sin tener que recordar todos los archivos de configuración, sus rutas y su sintaxis precisa. Obviamente los administradores antes tienen que tener conocimiento de cómo funcionan los servicios. El uso de Webmin ahorrará muchos quebraderos de cabeza consiguiendo ganar tiempo a la hora de realizar el trabajo, el cual es una necesidad actual ya que con ese tiempo ahorrado puedes atender a más clientes y por lo tanto generar más dinero en una empresa o tú mismo si eres autónomo.

1.2. Objetivos del Proyecto.

El **objetivo general** de este proyecto es configurar y administrar un servidor de DHCP, DNS con un firewall, servidor proxy y el uso de Fail2Ban utilizando el software gratuito Webmin, de manera fácil y sencilla a través su interfaz gráfica. Gracias a esto se conseguirá simplificar la configuración y gestión de la red, así como fortalecer la seguridad y protección contra ataques en una pequeña empresa.

El **objetivo específico** es realizar una configuración de red para una pequeña con su securización incluida, a través de la interfaz gráfica de una manera fácil y sencilla, evitando al máximo los posibles errores que ocurren creando y modificando los archivos desde la terminal, todo esto en mínimo tiempo posible. Para ello vamos a configurar los siguientes servicios de esta manera:

- **Servidor DHCP** – Se configurará un servidor DHCP que otorgara un rango de IP dinámicas, dichas IPs durarán tendrán un tiempo máximo
- **Servidor DNS** – Se configurará un servidor DNS para que sea capaz de hacer la resolución de nombres de los equipos conectados en la red interna.
- **Fail2ban** – Se bloqueará el acceso a servicio SSH desde el exterior al intentar un número determinado de intentos fallidos. El ban será por IP.
- **Firewall** – Se enrutará el adaptador de red de la interfaz de la red interna para que tenga salida a internet por una segunda interfaz, a parte exteriormente no se podrá acceder a los equipos internos, la comunicación solo existirá si ha sido establecida por un equipo local primero.

- **Proxy Squid** – Se creará un proxy transparente que bloqueará el (Cricket Liu, 2006) acceso de los usuarios de la red interna a las siguientes páginas: Facebook, Instagram y twitter.

2. Propuesta de solución.

2.1. Análisis descriptivo.

El proyecto se enfoca en la configuración y securización de una red local utilizando la herramienta Webmin cuya interfaz gráfica basada en web que facilita la administración y configuración de servicios esenciales de red, como DHCP, DNS, Fail2ban, Firewall y Proxy.

Alcance del proyecto: Nos centramos en la configuración básica de los servicios mencionados anteriormente, estableciendo una base sólida para el funcionamiento eficiente y seguro de una red local. Esto implica la implementación y configuración adecuada de DHCP para la asignación de direcciones IP, DNS para la resolución de nombres de dominio, Fail2ban para la protección contra ataques de fuerza bruta, Firewall para establecer políticas de seguridad y Proxy para la gestión del tráfico de red.

Identificación de requisitos: Los requisitos serán un servidor compatible con Webmin (proporcionado por el cliente) con sistema operativo Linux, acceso a Internet, hardware de red adecuado, ordenador para el administrador de red y conocimientos.

Análisis de riesgos: Los riesgos pueden que nos podemos encontrar son: vulnerabilidades de seguridad, compatibilidad de hardware o software y posibles interrupciones del servicio durante la implementación por parte de la red al realizarse de forma remota.

Descripción de actividades: Las actividades es la instalación de Webmin en el servidor, la configuración de los servicios DHCP, DNS, Fail2ban, Firewall y Proxy a través de la interfaz gráfica de Webmin, la realización de pruebas de funcionamiento y la posible documentación de la configuración realizada.

2.2. Análisis de requisitos.

Para realizar el siguiente proyecto solo se necesitan los siguientes requisitos por parte del administrador:

Hardware:

- Un PC o portátil con tarjeta de red.
- Conexión a internet.

Software:

- Ubuntu Desktop 22.04.

Como puede observarse los requisitos son mínimos, cualquier administrador de red con un portátil, PC o incluso un móvil con conexión a internet y un S.O instalado puede acceder a un servidor en cualquier parte del mundo y realizar la configuración de red planteada.

3. Temporalización.

3.1. Identificación de tareas.

El procedimiento y desarrollo nuestro trabajo sería el siguiente:

1. **Investigación y comprensión de las funcionalidades de Webmin:** Se realiza una investigación sobre las capacidades y características de Webmin en relación a la configuración de servidores de DHCP, DNS, firewall, servidor proxy y Fail2Ban. Ver cómo Webmin realmente simplifica la administración de estos servicios.
2. **Captación de clientes** – Se realiza la búsqueda de clientes interesados en obtener los servicios que ofrecemos.
3. **Instalación y configuración de Webmin:** Se realiza la instalación y configuración a de Webmin en el servidor, asegurando su correcto funcionamiento. Esto implica familiarizarse con los requisitos del sistema, la instalación de los paquetes necesarios y la configuración de los permisos y accesos necesarios para administrar los servicios.
4. **Configuración del servidor de DHCP:** A través de la interfaz gráfica de se configura y se administra el servidor de DHCP. Esto incluye la asignación de direcciones IP dinámicas a los clientes de la red, la configuración de opciones y parámetros específicos, y la gestión de las concesiones de direcciones.
5. **Configuración del servidor DNS:** A través de la interfaz gráfica se configura y se administra el servidor de DNS. Esto incluye la creación y gestión de zonas, registros de DNS, configuración de resoluciones y la vinculación de nombres de dominio a direcciones IP.
6. **Configuración del firewall:** A través de la interfaz gráfica se configura y se administra el firewall de Ubuntu server 22.04. Esto implica establecer reglas de filtrado, permitir o bloquear puertos y servicios, y garantizar la seguridad de la red.
7. **Configuración del servidor proxy:** A través de la interfaz gráfica se configura y se administra el servidor proxy, creando un proxy transparente que bloquea el ingreso de los usuarios a Facebook, Twitter e Instagram.

8. **Configuración del módulo de Fail2Ban:** A través de la interfaz gráfica se configura y se administra el módulo Fail2Ban, que proporciona protección contra ataques de fuerza bruta y abusos en los servicios del servidor. En nuestro caso para el SSH y Webmin.
9. **Comprobación y seguimiento del correcto funcionamiento:** Una vez realizado la instalación y configuración de todos los servicios necesitaremos comprobar que todo funciona correctamente y estar atentos a posibles fallos que puedan haberse producido
10. **Documentación del proceso realizado:** Paralelamente se realizará una documentación de los parámetros de configuración establecidos y el porqué de dichos parámetros atendiendo a las necesidades del cliente.

3.2. Secuenciación.

La secuenciación aquí descrita detalla el tiempo que llevaría al administrador de la red en realizar su trabajo. La captación de clientes es continua, pero para efectos prácticos del proyecto se va a suponer que en 5 días se consigue un cliente, se escucha sus necesidades de configuración y se le ofrece nuestro servicio.

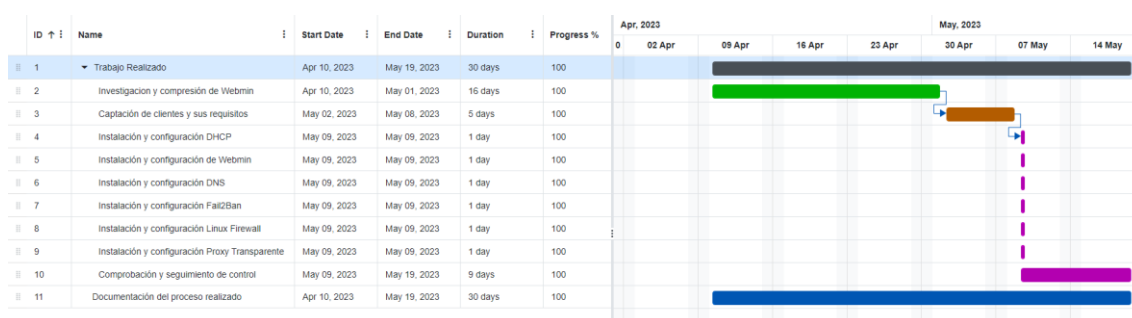


Ilustración 1 - Diagrama de Gantt

4. Memoria técnica.

En este apartado se va a proceder a describir como se instala Webmin y se configuran los servicios básicos de DHCP, DNS, firewall, Fail2ban y proxy en un servidor Ubuntu 22.04. Para ello se cuenta con un dispositivo externo (nuestro ordenador que primero se conectara mediante SSH al servidor para poder instalar Webmin, una vez instalado aplicaremos los conocimientos adquiridos para poder configurar todos los parámetros. A continuación, se realizarán un seguimiento y control de su correcto funcionamiento.

4.1. Esquema de la red.

Para el propósito del presente proyecto se detalla un esquema a modo de ejemplo de cómo estarían conectados los distintos dispositivos. En primer lugar, el administrador de red estaría en su propia red, después tendríamos el servidor con una interfaz de red con salida a internet y otra interfaz de red para la red local.

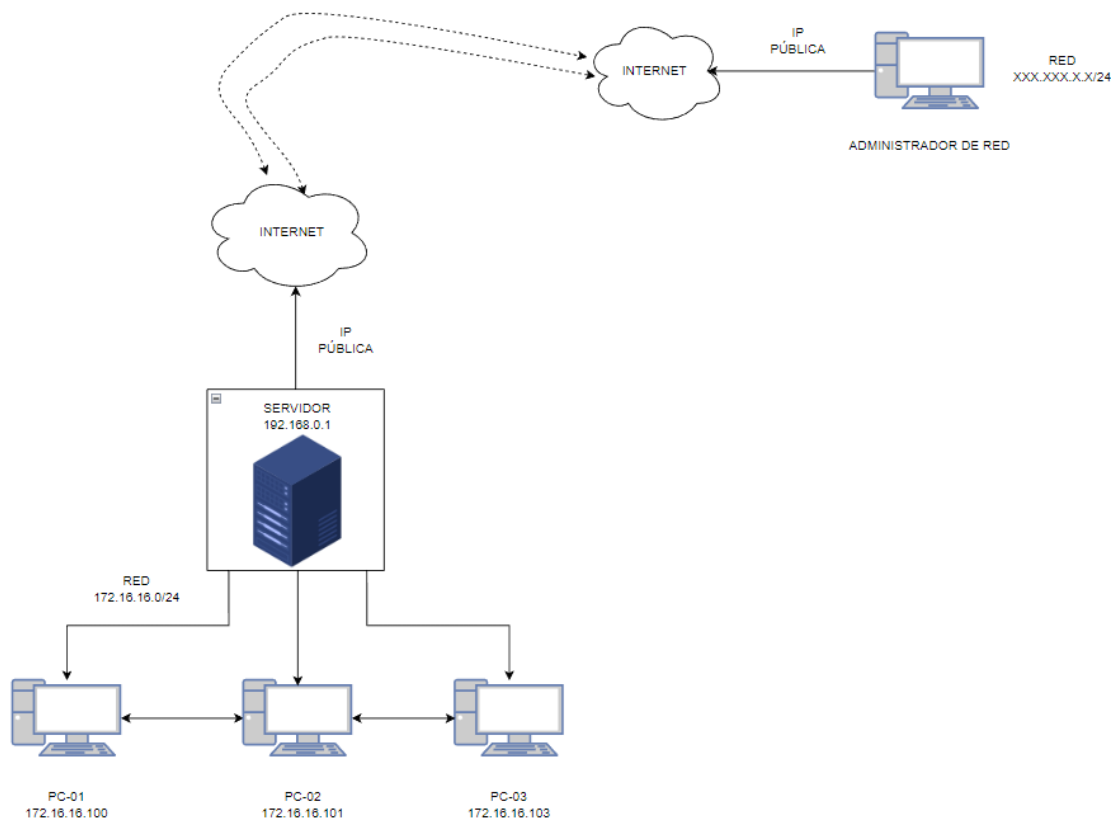


Ilustración 2 - Esquema de la Red

4.2. Instalación Webmin.

Webmin no viene en los repositorios oficiales por eso lo tenemos que añadirlo para ello a la lista de fuentes, también hay que añadir la clave PGP de Webmin a la lista de claves del sistema y finalmente se procede a instalar Webmin.

Lista de comandos utilizados:

```
sudo nano /etc/apt/sources.list
wget -q -O- http://www.webmin.com/jcameron-key.asc | sudo apt-key add
sudo apt update
sudo apt install webmin
```

Repositorio utilizado:

```
deb http://download.webmin.com/download/repository sarge contrib
```

Para poder acceder a Webmin se introduce la IP del servidor donde ha sido instalado junto con el puerto 10000.

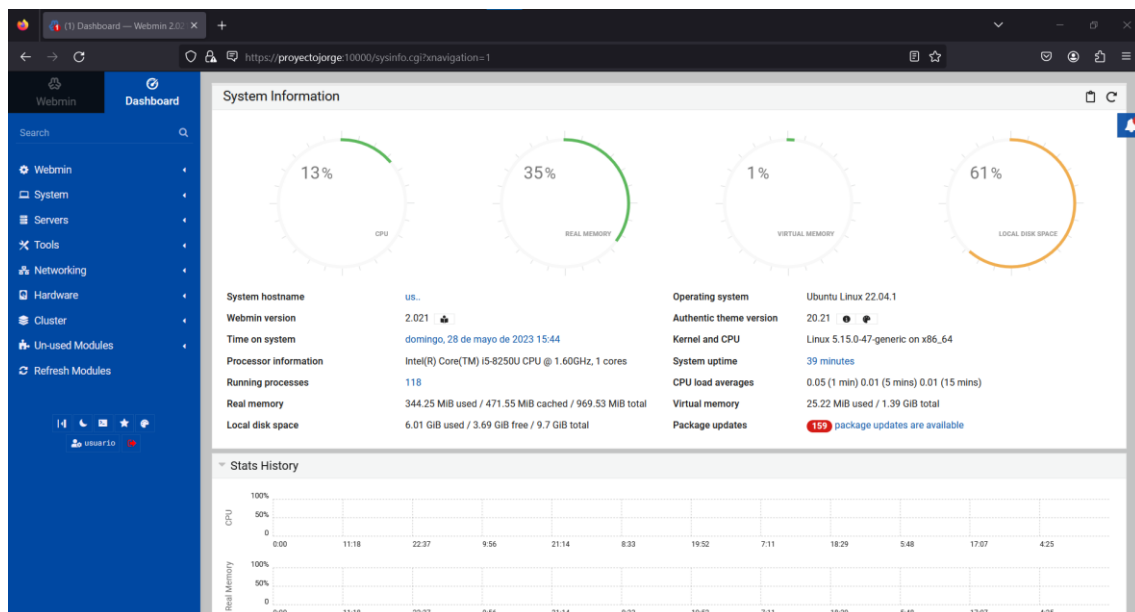


Ilustración 3 - Panel de control Webmin

4.3. SERVIDOR DHCP.

4.3.1. Explicación qué es el DHCP.

El protocolo DHCP (Protocolo de configuración dinámica de host) o también conocido como Dynamic Host Configuration Protocol, es un protocolo de red que utiliza una arquitectura cliente-servidor. Por tanto, tendremos uno o varios servidores DHCP y también uno o varios clientes, que se deberán comunicar entre ellos correctamente para que el servidor DHCP brinde información a los diferentes clientes conectados. Este protocolo se encarga de asignar de manera dinámica y automática una dirección IP, ya sea una dirección IP privada desde el router hacia los equipos de la red local, o también una IP pública por parte de un operador que utilice este tipo de protocolo para el establecimiento de la conexión.

4.3.2. Instalación del módulo de DHCP

Por defecto el módulo de DHCP server no viene instalado así que lo que deberemos hacer es irnos al apartado de **Un-used Modules** y seleccionar **instalar ahora**.

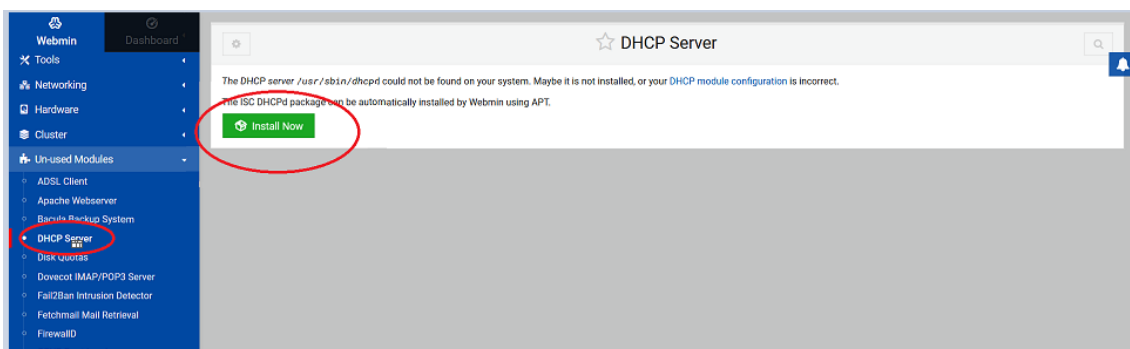


Ilustración 4 - Instalación del módulo DHCP

A continuación, nos mostrara los paquetes que se van a instalar:

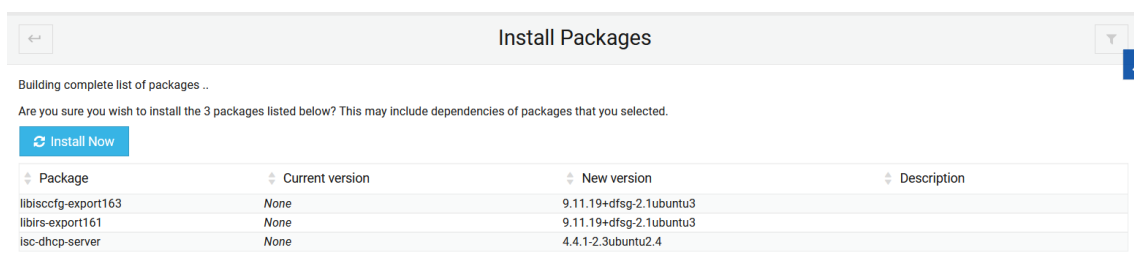


Ilustración 5 - Instalación de los paquetes de DHCP

Y con eso ya tendremos instalado el ISC-DHCP.

4.3.3. Configuración básica DHCP server.

Una vez instalado nos vamos a Network y vemos las opciones de interfaz.

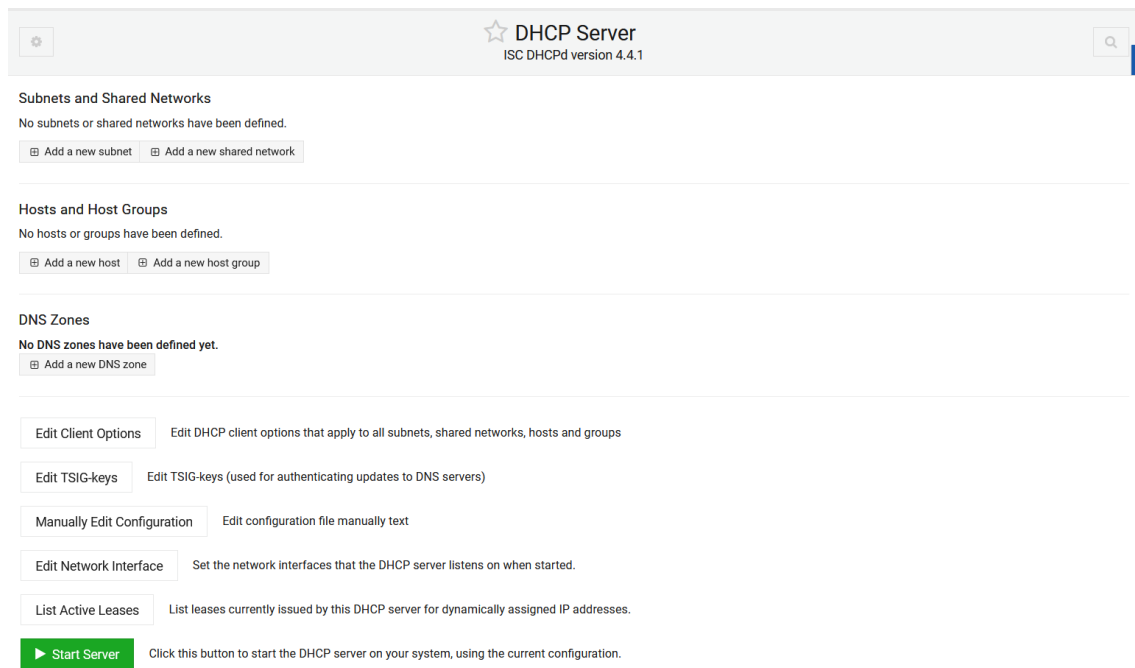


Ilustración 6 - Panel principal DHCP

Los principales parámetros que encontramos aquí son los siguientes:

- **Subnet** Una subnet es una red IP entera como puede ser 172.16.16.0. Las Entradas de este tipo se utilizan para asignar dinámicamente direcciones dentro de ciertos rangos a clientes dentro de la red.
- **Shared network** Una shared network es un grupo de subnets que comparten la misma red física.
- **Host** Es un único cliente identificado por su dirección MAC asignada a una IP fija.
- **Group** Es un grupo de hosts para el cual se pueden configurar las mismas opciones.
- **DNS** No se aplica ahora.
- **Edit Client Options** Permite editar las opciones del cliente que se aplican a todas las subnets, shared networks, hosts y grupos
- **Edit TSIG-keys** Se usa para autenticar las actualizaciones hacia los servidores DNS.
- **Manually Edit Configuration** Permite la edición del fichero de forma manual.
- **Edit Network Interface** Elige los adaptadores de red por los que el DHCP va a escuchar cuando se inicie.
- **List Active Leases** Lista los clientes que el servidor de DHCP a asignado una dirección IP de forma dinámica.
- **Start Server** Sirve para empezar el DHCP.

Para empezar nuestra configuración básica lo primero que haremos será crear una subnet. Se configurará como en la siguiente imagen:

Ilustración 7 - Creación de una subnet

Los campos que rellenaremos aquí serán los siguientes:

Subnet description – El nombre que le vamos a dar la subnet.

Network Address – La dirección de red.

Netmask – La máscara de subred.

Address range – El rango que el servidor DHCP va a proporcionar a los clientes conectados en esta subred.

Default lease time – Es el tiempo por defecto que se le concede esa IP.

Maximum lease time – Tiempo máximo que se le puede conceder a un cliente por la configuración que tiene ese cliente en la petición de IP.

Allow unknown clients? – Permitir conectarse a clientes desconocidos.

Otros datos que se pueden rellenar, un poco más avanzados son:

Dynamic BOOTP – es un protocolo TCP/IP q permite a un cliente encontrar su dirección IP y el nombre de un archivo de carga en un servidor de la red.

Lease length for BOOTP clients – Tiempo que se le concede a los clientes anteriores.

Hosts directly in this subnet – Introducir a los hosts directamente en esta subnet, para poder organizarlo mejor.

A continuación, pasaremos a configurar las opciones para los clientes:

Client Options					
Client hostname	<input checked="" type="radio"/> Default <input type="radio"/>	<input type="text"/>	Default routers	<input type="radio"/> Default <input checked="" type="radio"/>	<input type="text" value="172.16.16.1"/>
Subnet mask	<input checked="" type="radio"/> Default <input type="radio"/>	<input type="text"/>	Broadcast address	<input type="radio"/> Default <input checked="" type="radio"/>	<input type="text" value="172.16.16.255"/>
Domain name	<input checked="" type="radio"/> Default <input type="radio"/>	<input type="text"/>	DNS servers	<input type="radio"/> Default <input checked="" type="radio"/>	<input type="text" value="172.16.16.2"/>
DNS domains to search	<input checked="" type="radio"/> Default <input type="radio"/>	<input type="text"/>	Log servers	<input checked="" type="radio"/> Default <input type="radio"/>	<input type="text"/>
Time servers	<input checked="" type="radio"/> Default <input type="radio"/>	<input type="text"/>	Root disk path	<input checked="" type="radio"/> Default <input type="radio"/>	<input type="text"/>
Swap server	<input checked="" type="radio"/> Default <input type="radio"/>	<input type="text"/>	NIS servers	<input checked="" type="radio"/> Default <input type="radio"/>	<input type="text"/>
NIS domain	<input checked="" type="radio"/> Default <input type="radio"/>	<input type="text"/>	XDM servers	<input checked="" type="radio"/> Default <input type="radio"/>	<input type="text"/>
Font servers	<input checked="" type="radio"/> Default <input type="radio"/>	<input type="text"/>	NetBIOS name servers	<input checked="" type="radio"/> Default <input type="radio"/>	<input type="text"/>
Static routes	<input checked="" type="radio"/> Default <input type="radio"/>	<input type="text"/>	NetBIOS node type	<input checked="" type="radio"/> Default <input type="radio"/>	<input type="text"/>
NTP servers	<input checked="" type="radio"/> Default <input type="radio"/>	<input type="text"/>	DHCP server identifier	<input checked="" type="radio"/> Default <input type="radio"/>	<input type="text"/>
NetBIOS scope	<input checked="" type="radio"/> Default <input type="radio"/>	<input type="text"/>			
Time offset	<input checked="" type="radio"/> Default <input type="radio"/>	<input type="text"/>			
SLP directory agent IPs	<input checked="" type="radio"/> Default <input type="radio"/>	<input type="text"/>	<input type="checkbox"/> These IPs only?		
SLP service scope	<input checked="" type="radio"/> Default <input type="radio"/>	<input type="text"/>	<input type="checkbox"/> This scope only?		
Option definition					
Option name	<input type="text"/>	Number	<input type="text"/>	Type	<input type="text"/>
Use name as client hostname?					
<input type="radio"/> Yes <input type="radio"/> No <input checked="" type="radio"/> Default					
Boot filename	<input checked="" type="radio"/> None <input type="radio"/> <input type="text"/>				
Boot file server	<input checked="" type="radio"/> This server <input type="radio"/> <input type="text"/>				
Lease length for BOOTP clients	<input checked="" type="radio"/> Forever <input type="radio"/> <input type="text"/> secs				
Dynamic DNS enabled?	<input type="radio"/> Yes <input type="radio"/> No <input checked="" type="radio"/> Default				
Dynamic DNS reverse domain	<input checked="" type="radio"/> Default <input type="radio"/> <input type="text"/>				
Dynamic DNS update style	<input type="radio"/> Ad-hoc <input checked="" type="radio"/> Interim <input type="radio"/> None <input type="radio"/> Default				
Allow unknown clients?	<input type="radio"/> Allow <input type="radio"/> Deny <input type="radio"/> Ignore <input checked="" type="radio"/> Default				
Can clients update their own records?	<input type="radio"/> Allow <input type="radio"/> Deny <input type="radio"/> Ignore <input checked="" type="radio"/> Default				
Server is authoritative for all subnets?	<input type="radio"/> Yes <input checked="" type="radio"/> No				
<input checked="" type="radio"/> Save					

Ilustración 8 - Configuración del cliente

En este apartado para un funcionamiento básico solo necesitaremos rellenar los siguientes campos:

Default route - La IP por defecto del router

Broadcast address - La dirección IP broadcast

DNS servers - La dirección de los servidores de DNS la cual en mi caso ya he puesto la que se va a configurar para el servidor BIND 9.

Default lease time - Es el tiempo por defecto que se le concede esa IP.

Maximum lease time - Tiempo máximo que se le puede conceder a un cliente por la configuración que tiene ese cliente en la petición de IP

Server name - Nombre del servidor.

Y por último el adaptador de red por el que va a escuchar en mi caso enp0s3.

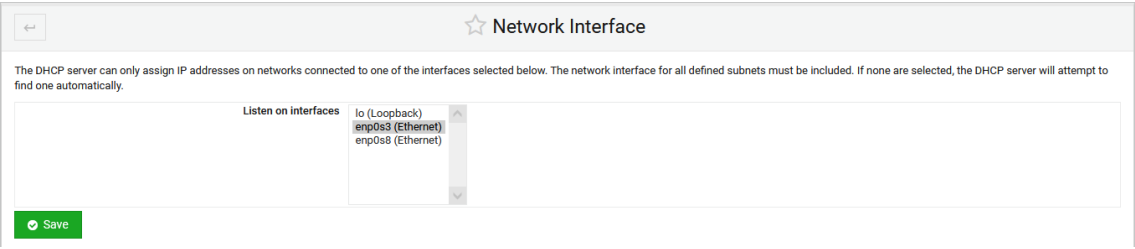


Ilustración 9 - Selección de la interfaz

4.3.4. Comprobación del servidor DHCP.

Para comprobar el DHCP conectamos un cliente a nuestra red interna 172.16.16.0 y dentro del apartado **List Active Leases** podemos ver que se le ha asignado una dirección IP (172.16.16.100) cuando se le ha asignado y cuando será liberada esa IP, lo cual coincide con los parámetros que le hemos asignado.

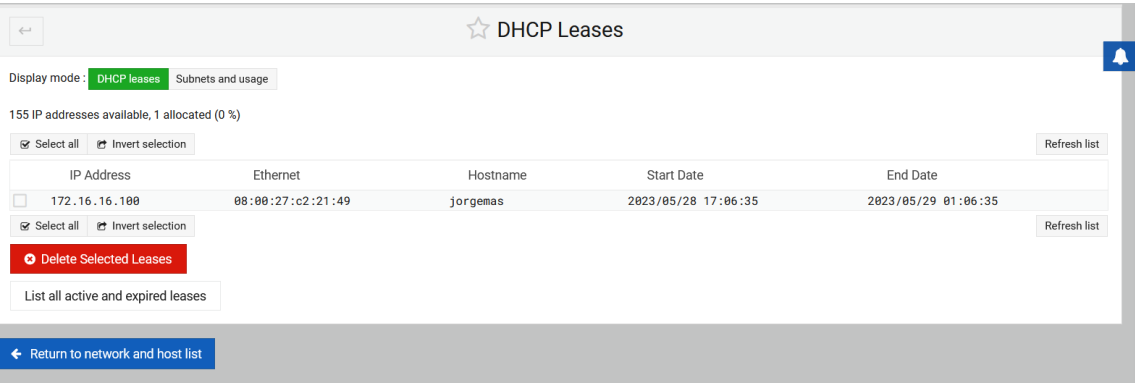
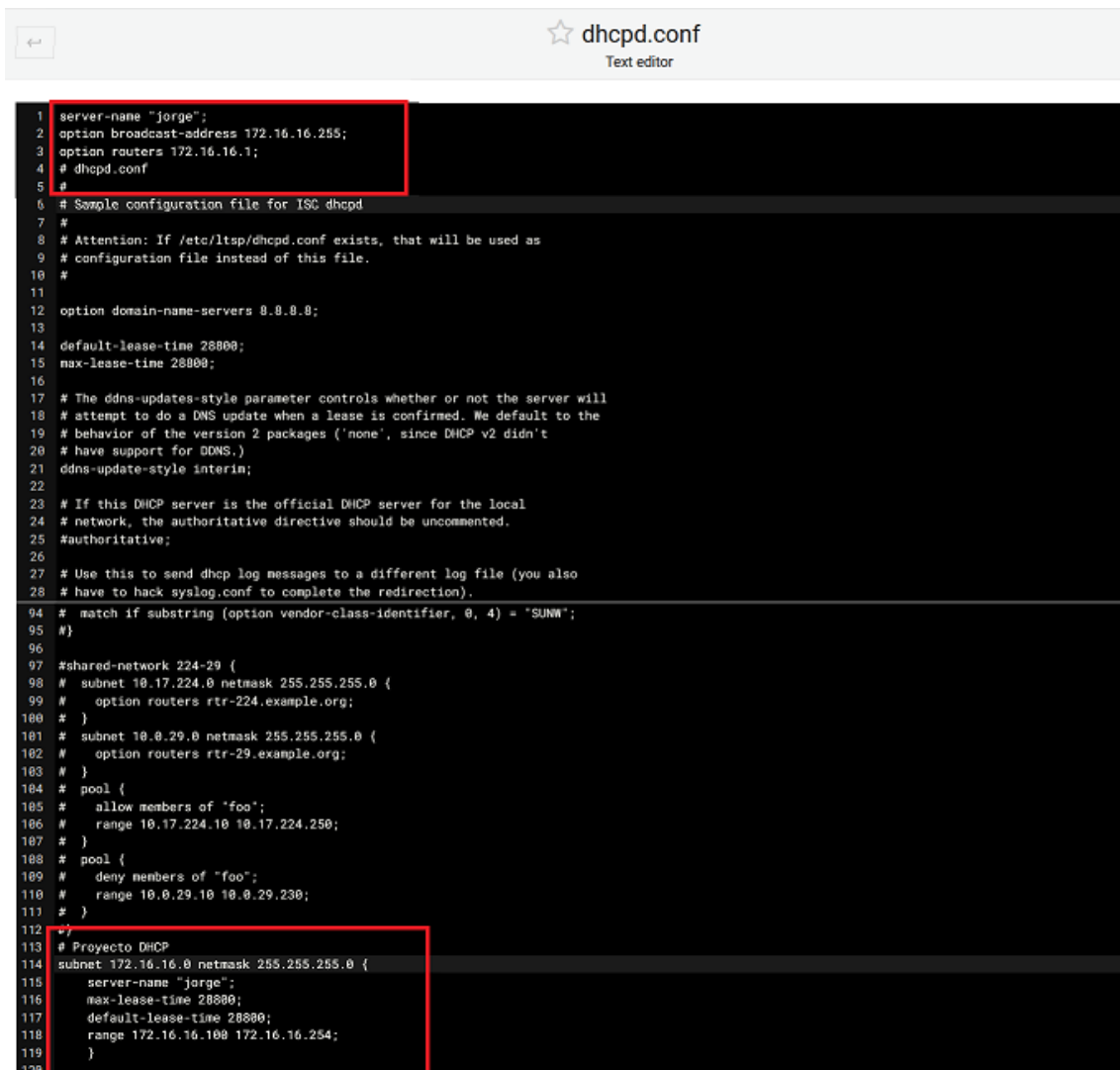


Ilustración 10 - Comprobación del cliente

También podemos ver como se ha creado y configurado el archivo dhcpd.conf en **Manually Edit Configuration**. Debido a la longitud del archivo solo se incluyen las partes más relevantes. Cabe mencionar que también se puede modificar el fichero desde ese editor.



```
1 server-name "jorge";
2 option broadcast-address 172.16.16.255;
3 option routers 172.16.16.1;
4 # dhcpd.conf
5 #
6 # Sample configuration file for ISC dhcpd
7 #
8 # Attention: If /etc/ltsp/dhcpd.conf exists, that will be used as
9 # configuration file instead of this file.
10 #
11
12 option domain-name-servers 8.8.8.8;
13
14 default-lease-time 28800;
15 max-lease-time 28800;
16
17 # The ddns-updates-style parameter controls whether or not the server will
18 # attempt to do a DNS update when a lease is confirmed. We default to the
19 # behavior of the version 2 packages ('none', since DHCP v2 didn't
20 # have support for DDNS.)
21 ddns-update-style interim;
22
23 # If this DHCP server is the official DHCP server for the local
24 # network, the authoritative directive should be uncommented.
25 #authoritative;
26
27 # Use this to send dhcp log messages to a different log file (you also
28 # have to hack syslog.conf to complete the redirection).
29
30 # match if substring (option vendor-class-identifier, 0, 4) = "SUNW";
31 #}
32
33 #shared-network 224-29 {
34 # subnet 10.17.224.0 netmask 255.255.255.0 {
35 #   option routers rtr-224.example.org;
36 # }
37 # subnet 10.0.29.0 netmask 255.255.255.0 {
38 #   option routers rtr-29.example.org;
39 # }
40 # pool {
41 #   allow members of "foo";
42 #   range 10.17.224.10 10.17.224.250;
43 # }
44 # pool {
45 #   deny members of "foo";
46 #   range 10.0.29.10 10.0.29.230;
47 # }
48 #}
49
50 # Proyecto DHCP
51 subnet 172.16.16.0 netmask 255.255.255.0 {
52   server-name "jorge";
53   max-lease-time 28800;
54   default-lease-time 28800;
55   range 172.16.16.100 172.16.16.254;
56 }
```

Ilustración 11 - Comprobación del archivo dhcpd.conf

4.4. SERVIDOR DNS.

4.4.1. Explicación qué es el DNS.

DNS es el acrónimo de Domain Name System o Sistema de Nombres de Dominio, que es el método utilizado por Internet para traducir, de forma fácil de recordar, los nombres de dominios en lugar de su IP (y viceversa) de manera que sean entendibles por las personas y más fácil que si se trata de recordar secuencias numéricas, como es el caso de las direcciones IP.

4.4.2. Instalación del módulo de DNS server.

Por defecto el módulo de DNS server no viene instalado así que lo que deberemos hacer es irnos al apartado de **Un-used Modules** y seleccionar **instalar ahora**.

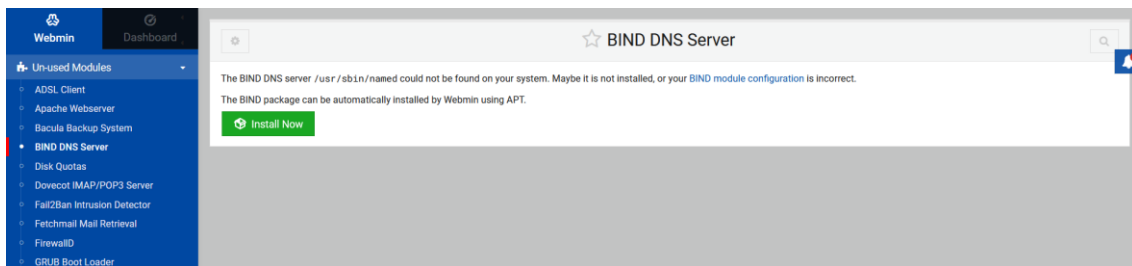


Ilustración 12 - Instalación del módulo DNS

A continuación, nos mostrara los paquetes que se van a instalar y le damos a continuar:

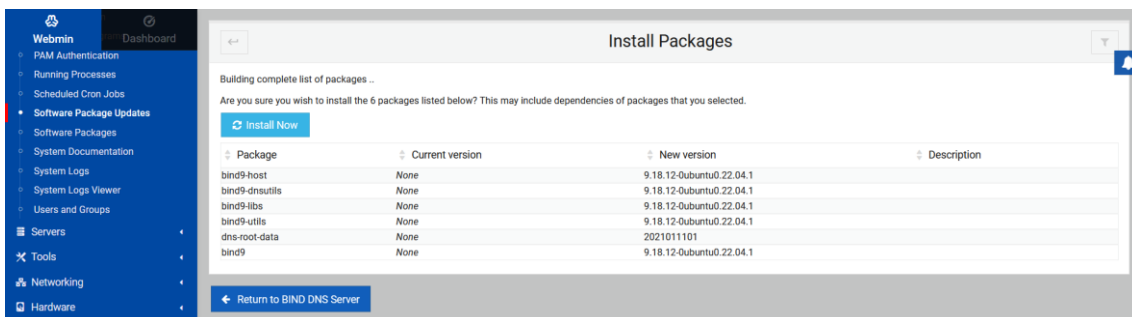


Ilustración 13 - Instalación de los paquetes DNS

4.4.3. Configuración básica DNS server.

Este es el menú principal del panel de configuración del BIND DNS Server en el cual encontramos las siguientes opciones:

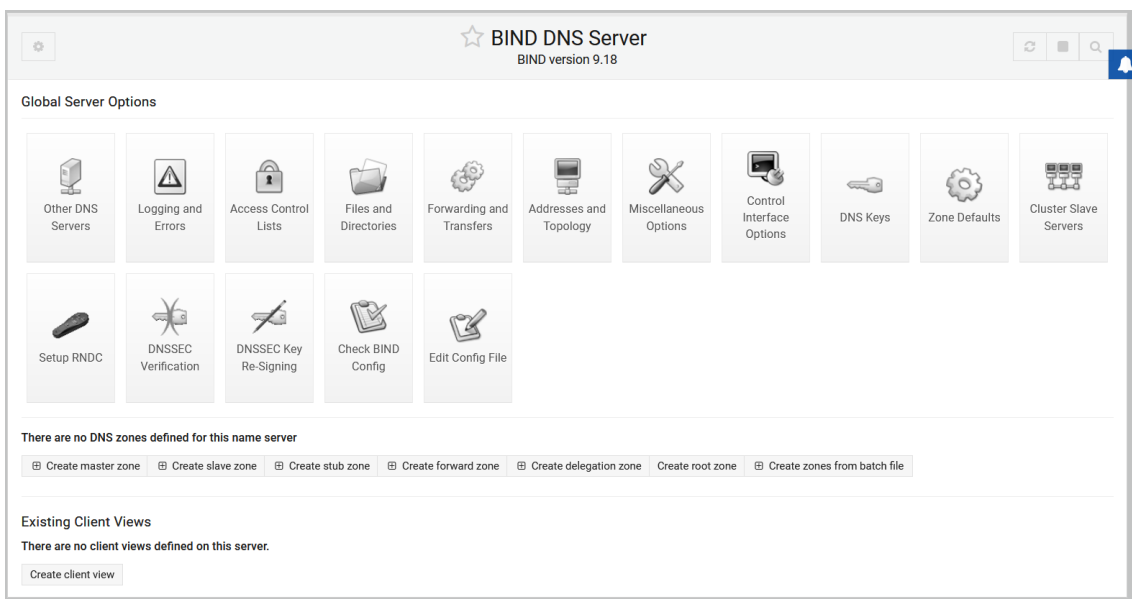


Ilustración 14 - Panel principal DNS

En el cual encontramos los siguientes parámetros:

- **Other DNS Server** - Este parámetro permite configurar otros servidores DNS a los que BIND puede consultar en caso de no poder resolver una consulta de DNS localmente. Aquí se pueden especificar servidores DNS externos adicionales.
- **Logging and Errors** - Este parámetro controla la configuración de registro de eventos y errores del servidor DNS. Permite especificar qué tipo de eventos se deben registrar y dónde se deben almacenar los registros.
- **Access Control List** – Sirve para definir las listas de control de acceso (ACL) que permiten o deniegan el acceso a diferentes recursos del servidor DNS-
- **Files and Directories** – Sirve para definir las ubicaciones de los archivos de configuración y datos del servidor DNS.
- **Forwarding and Transfers** – Sirve para especificar la configuración de reenvío y transferencia de zona.
- **Addresses and Topology** – Sirve para definir las direcciones IP y las interfaces de red en las que BIND escucha las consultas DNS entrantes.
- **Miscellaneous Options** - Se encuentra otras opciones de configuración adicionales que no se ajustan a las categorías anteriores.
- **Control Interface Options** - Este parámetro permite configurar la interfaz de control de BIND, que proporciona una forma de gestionar y controlar el servidor DNS mediante comandos remotos.
- **DNS Keys** – Sirve para generar, importar y administrar claves de DNS para la autenticación y seguridad en la comunicación entre servidores DNS.
- **Zone Defaults** – Sirve para establecer opciones y configuraciones predeterminadas para las nuevas zonas que se crean en el servidor DNS.
- **Cluster Slave Servers** - Puedes especificar los servidores DNS esclavos en el clúster y configurar la sincronización y transferencia de zona entre ellos.
- **Setup RNDNC** - RNDNC (Remote Name Daemon Control) es una herramienta para administrar y controlar servidores DNS BIND de forma remota.
- **DNSSEC Verification** - DNSSEC (Domain Name System Security Extensions) es una extensión del sistema de nombres de dominio que proporciona autenticación y seguridad a las respuestas DNS.
- **Check BIND Config** – Sirve para verificar la sintaxis y la validez del archivo de configuración
- **Edit Config File** - Sirve para realizar cambios directos en el archivo de configuración.

Para crear nuestra configuración básica lo primero que haremos será crear una ACL para nuestra red interna, en nuestro caso la 172.16.16.0/24

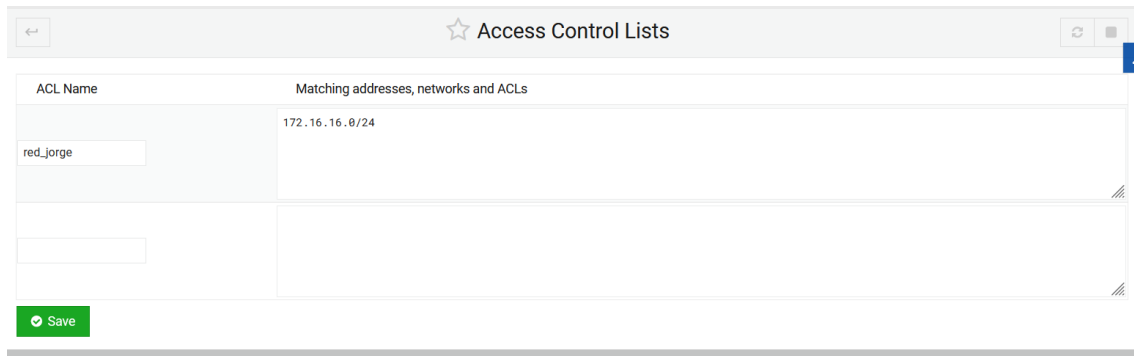


Ilustración 15 - ACL de DNS

Después creamos la zona maestra de la siguiente manera, rellenando estos 4 parámetros:

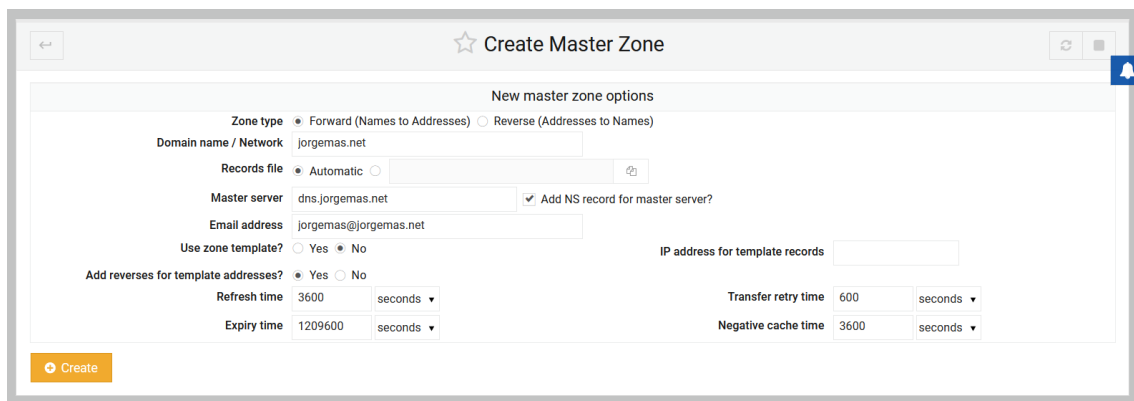


Ilustración 16 - Creación de la zona maestra

Estos son los parámetros que modificaremos:

Zone type - Seleccionamos la zona directa.

Domain name - El nombre de dominio que queremos darle.

Master server - El nombre del servidor maestro con su dominio.

Email address - Esto es opcional.

Hacemos lo mismo con la zona inversa, con la diferencia de que aquí ponemos la IP de la red y seleccionamos Reverse.

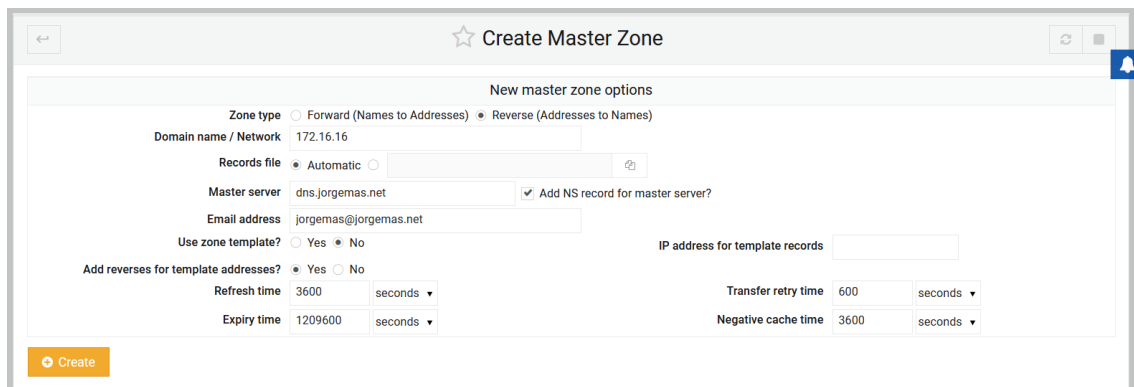


Ilustración 17- Creación de la zona inversa

Una vez creada la zona maestra, nos vamos a Address Records y rellenamos los siguientes parámetros:

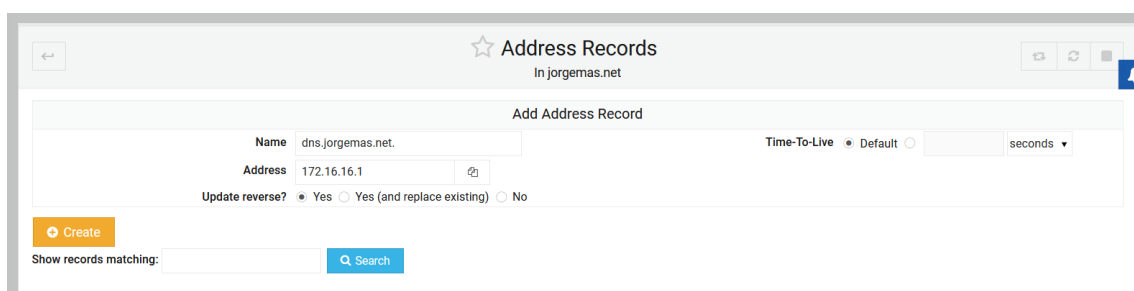


Ilustración 18 - Creación de la dirección

Name - Mismo nombre que el master server. Muy importante añadirle el punto al final.

Address - IP del servidor.

Update reverse - Seleccionamos que sí, para que también actualice la zona inversa.

A continuación, nos vamos a editar Address Record y rellenamos los siguientes parámetros:

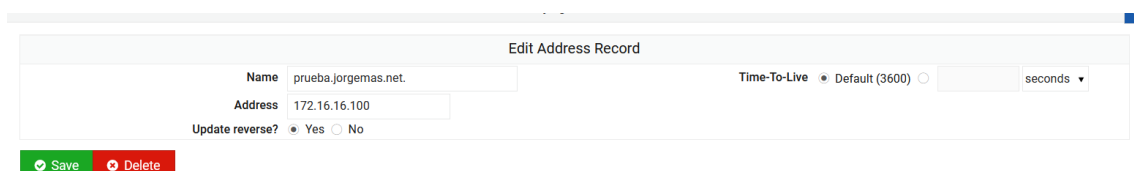


Ilustración 19 - Editar la dirección

Name - El nombre que le queramos dar al equipo local.

Address - La dirección IP del equipo local.

Update reverse - Seleccionamos que sí, para que también actualice la zona inversa.

Y ya de paso le creamos un alias con el nombre blog.

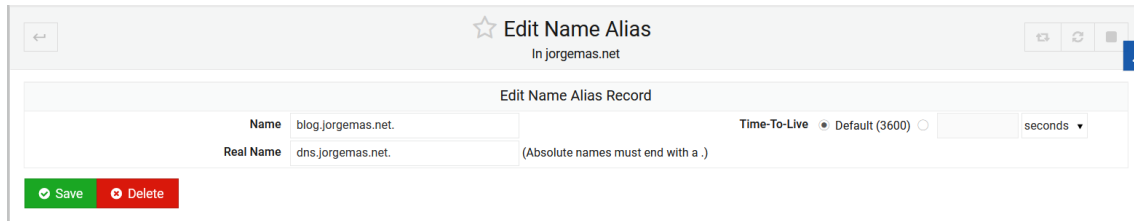


Ilustración 20 - Creación de un alias

Name - Seleccionamos el nombre del alias.

Real name - El nombre real al que apunta.

Por último, comprobamos que no existe ningún error en la configuración del BIND.

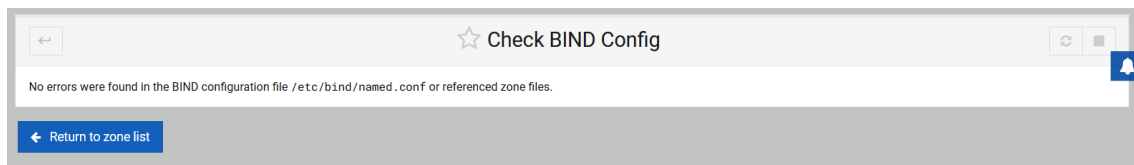


Ilustración 21 - Comprobación de BIND CFG

Podemos ver como ha quedado nuestro fichero una vez ha sido configurado.

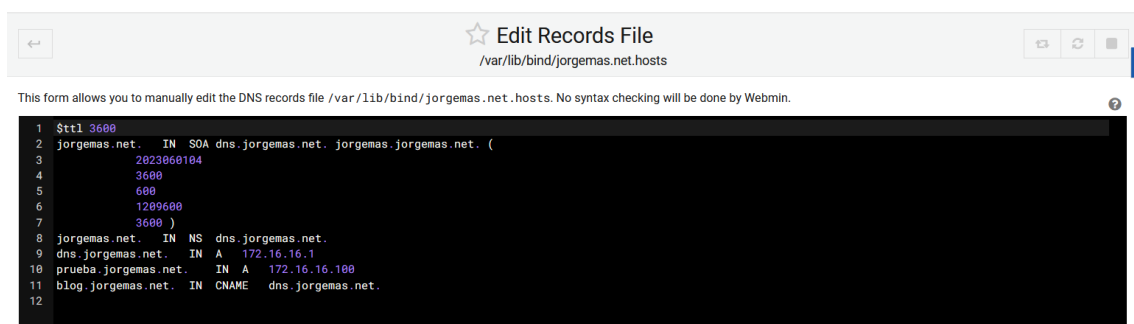
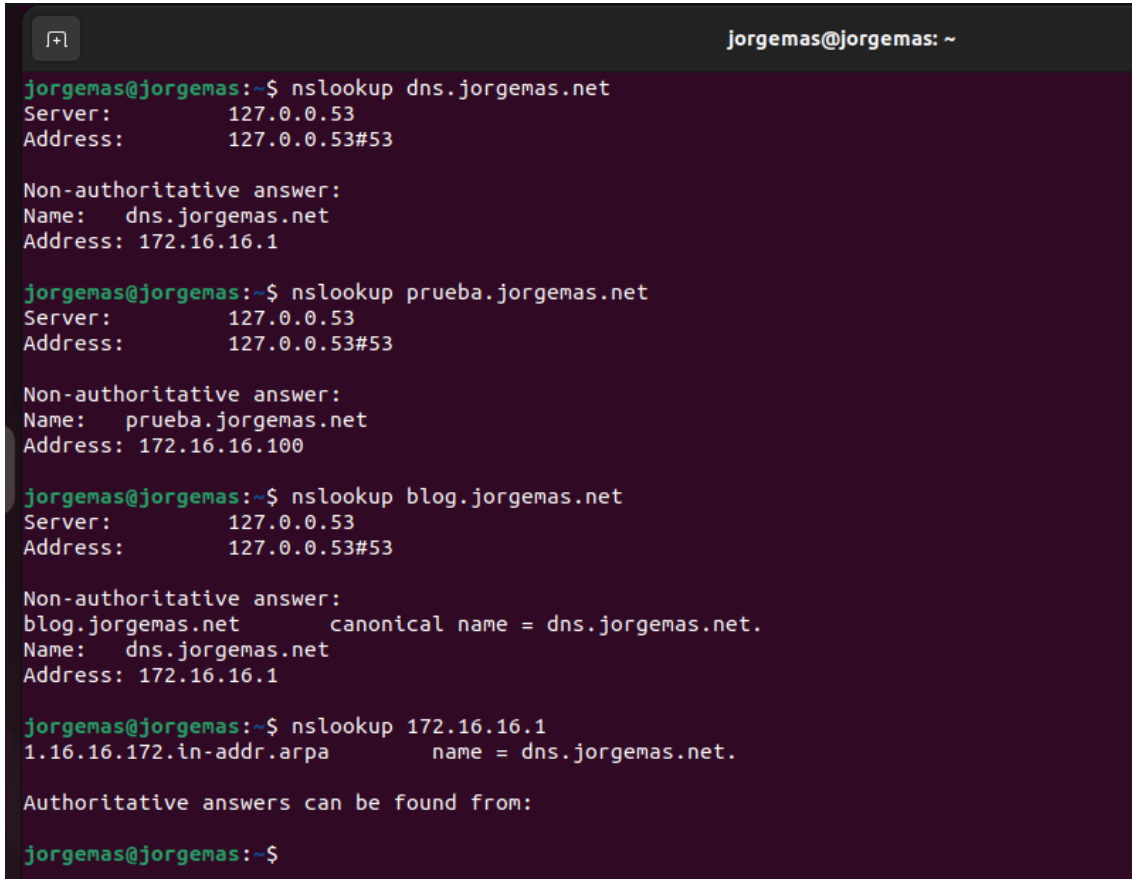


Ilustración 22 - Edición de los registros

4.4.4. Comprobación del DNS server.

Para comprobar que todo ha salido correctamente nos conectamos con nuestro cliente y realizamos las siguientes comprobaciones:

A screenshot of a terminal window with a dark background. The window title is 'jorgemas@jorgemas: ~'. The terminal shows four 'nslookup' commands and their outputs. The first command is 'nslookup dns.jorgemas.net', showing the server as 127.0.0.53 and the address as 127.0.0.53#53, with a non-authoritative answer for dns.jorgemas.net at 172.16.16.1. The second command is 'nslookup prueba.jorgemas.net', showing the same server and address, with a non-authoritative answer for prueba.jorgemas.net at 172.16.16.100. The third command is 'nslookup blog.jorgemas.net', showing the same server and address, with a non-authoritative answer for blog.jorgemas.net at 172.16.16.1, and a canonical name of dns.jorgemas.net. The fourth command is 'nslookup 172.16.16.1', showing the name as dns.jorgemas.net. The terminal ends with 'Authoritative answers can be found from:' and a prompt.

```
jorgemas@jorgemas:~$ nslookup dns.jorgemas.net
Server:      127.0.0.53
Address:     127.0.0.53#53

Non-authoritative answer:
Name:   dns.jorgemas.net
Address: 172.16.16.1

jorgemas@jorgemas:~$ nslookup prueba.jorgemas.net
Server:      127.0.0.53
Address:     127.0.0.53#53

Non-authoritative answer:
Name:   prueba.jorgemas.net
Address: 172.16.16.100

jorgemas@jorgemas:~$ nslookup blog.jorgemas.net
Server:      127.0.0.53
Address:     127.0.0.53#53

Non-authoritative answer:
blog.jorgemas.net canonical name = dns.jorgemas.net.
Name:   dns.jorgemas.net
Address: 172.16.16.1

jorgemas@jorgemas:~$ nslookup 172.16.16.1
1.16.16.172.in-addr.arpa name = dns.jorgemas.net.

Authoritative answers can be found from:

jorgemas@jorgemas:~$
```

Ilustración 23 - Comprobación del DNS

4.5. FAIL2BAN.

4.5.1. Explicación qué es FAIL2BAN.

Fail2ban es una aplicación escrita en Python para la prevención de intrusos en un sistema, que actúa penalizando o bloqueando las conexiones remotas que intentan accesos por fuerza bruta. Se distribuye bajo licencia GNU y típicamente funciona en sistemas POSIX que tengan interfaz con un sistema de control de paquetes o un firewall local (como iptables).

4.5.2. Instalación del módulo de FAIL2BAN.

Para instalar el módulo de Fail2Ban se siguen los mismos pasos que anteriormente:

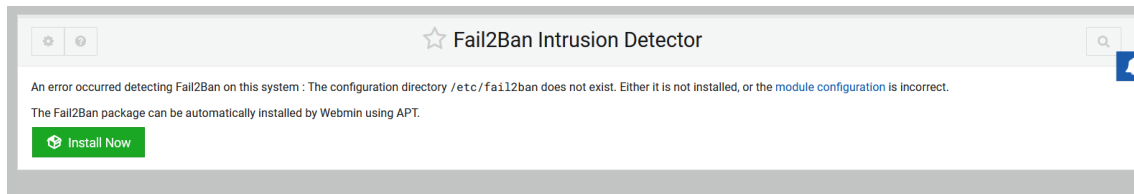


Ilustración 24 - Instalación del módulo Fail2Ban

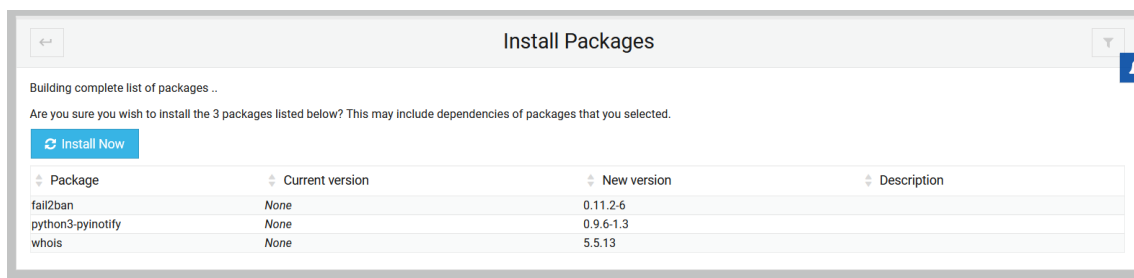


Ilustración 25 - Instalación de los paquetes Fail2Ban

4.5.3. Configuración del FAIL2BAN.

Una vez instalado nos encontramos con su menú principal:

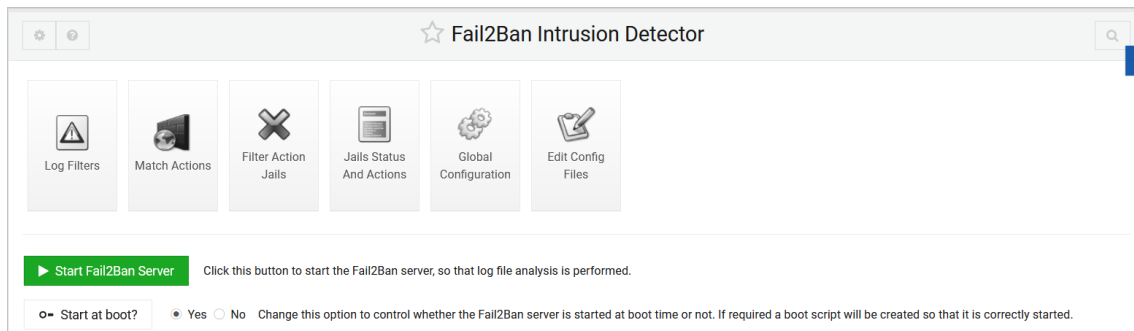


Ilustración 26 -Panel principal Fail2Ban

Este menú principal cuenta con los siguientes parámetros:

- **Log Filters** - Los filtros de registro permiten definir patrones de búsqueda para identificar eventos de registro específicos que indican intentos de intrusión o comportamiento malicioso. Aquí se pueden configurar y personalizar los filtros para analizar los registros del sistema en busca de eventos sospechosos.
- **Match Actions** – Sirven para establecer que acciones tomar como bloquear la dirección IP del atacante, enviar notificaciones por correo electrónico o registrar la actividad sospechosa.

- **Filter Action Jails** - Sirven configurar las acciones específicas que se deben tomar cuando se activa un jail. Estas acciones pueden incluir bloquear direcciones IP, enviar notificaciones o realizar otras medidas de seguridad.
- **Jails Status and Actions** - Este parámetro muestra el estado actual de los jails y permite realizar acciones específicas sobre ellos.
- **Global Configuration** - Aquí se puede acceder a la configuración global de Fail2ban, donde se pueden establecer opciones como el tiempo de bloqueo de las direcciones IP, los destinos de notificación, los registros y otras configuraciones globales.
- **Edit Config Files** - Este parámetro permite editar directamente los archivos de configuración de Fail2ban.

En nuestro caso solo vamos a bloquear 2 servicios, el SSH y Webmin. Para ello seleccionamos primero SSH.

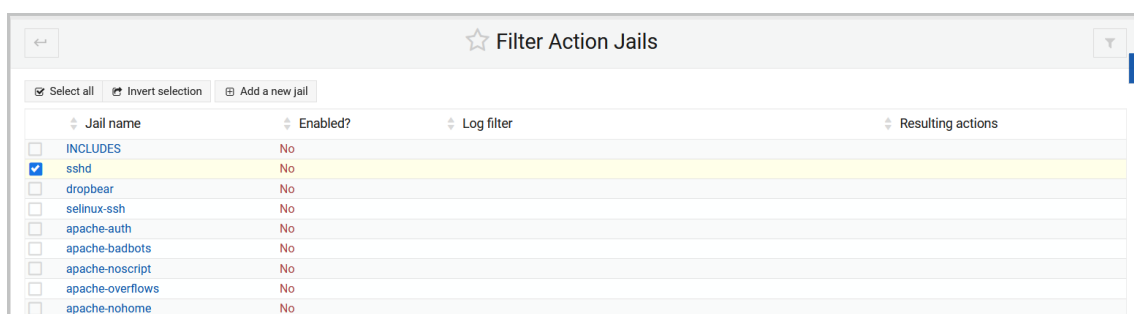


Ilustración 27 - Selección de servicios

Y editamos la regla:

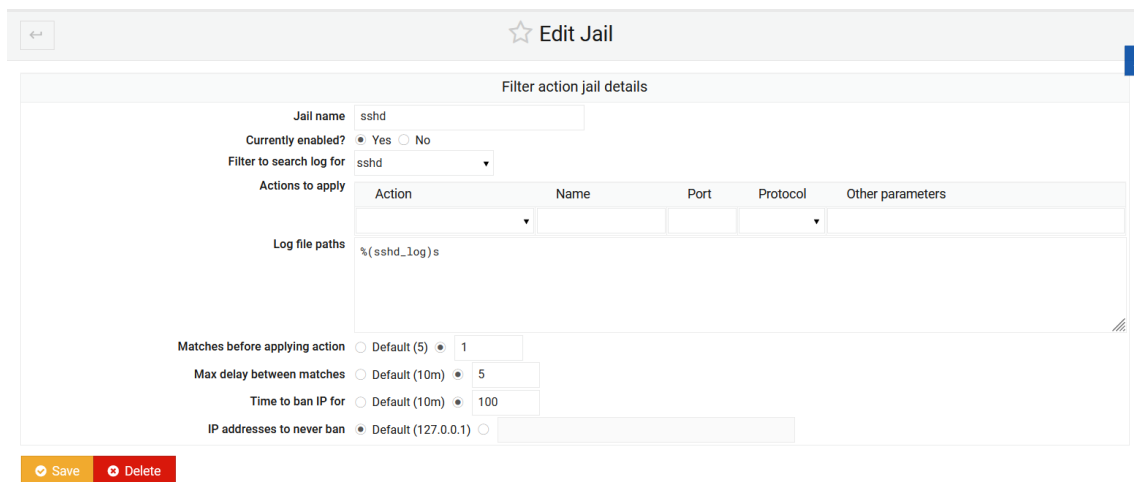


Ilustración 28 - Configuración de la regla para SSH

Jail name - El nombre de la regla

Currently enabled? - Si está actualmente activada.

Matches before applying action - El número de veces que tienen que equivocarse para que salte esa regla.

Max delay between matches - El retraso máximo entre intentos.

Time to ban IP for - El tiempo que se va a banear esa IP

Ip addresses to never ban - IP que nunca se van a banear.

A continuación, hacemos lo mismo para Webmin.

Filter action jail details

Jail name: webmin-auth

Currently enabled? ☒ Yes ☐ No

Filter to search log for: <Default>

Actions to apply

Action	Name	Port	Protocol	Other parameters

Log file paths: %(syslog_authpriv)s

Matches before applying action: ☐ Default (5) ☒ 3

Max delay between matches: ☐ Default (10m) ☒ 100

Time to ban IP for: ☐ Default (10m) ☒ 100

IP addresses to never ban: ☐ Default (127.0.0.1) ☒ Nuestra IP

Save Delete

Return to list of jails

Ilustración 29 - Configuración de la regla para Webmin

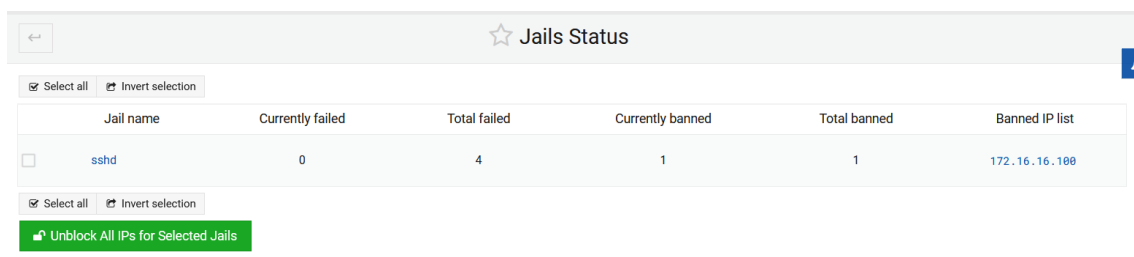
4.5.4. Comprobación del FAIL2BAN.

Para comprobarlo, nos vamos a cliente he intentamos conectarnos por SSH fallando la contraseña. Después de superar el número de fallos permitidos nos bloqueará.

```
jorgemas@jorgemas: ~  
jorgemas@jorgemas:~$ ssh usuario@172.16.16.1  
The authenticity of host '172.16.16.1 (172.16.16.1)' can't be established.  
ED25519 key fingerprint is SHA256:mmPq8PwsPe6IRYXAJrGJNm0t0gErgy46U8z8qLV9GXc.  
This key is not known by any other names  
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes  
Warning: Permanently added '172.16.16.1' (ED25519) to the list of known hosts.  
usuario@172.16.16.1's password:  
Permission denied, please try again.  
usuario@172.16.16.1's password:  
Permission denied, please try again.  
usuario@172.16.16.1's password:  
usuario@172.16.16.1: Permission denied (publickey,password).  
jorgemas@jorgemas:~$
```

Ilustración 30 - Comprobación Fail2Ban (1)

Y veremos que aparecerá nuestra IP en el apartado de Jail Status de nuestro Webmin.



Jail name	Currently failed	Total failed	Currently banned	Total banned	Banned IP list
ssh	0	4	1	1	172.16.16.100

Ilustración 31 - Comprobación Fail2Ban (2)

4.6. LINUX FIREWALL.

4.6.1. Explicación qué es LINUX FIREWALL.

El Linux Firewall se basa en iptables cuya función es analizar cada uno de los paquetes del tráfico de red entra en una máquina y decidir, en función de un conjunto de reglas, qué hacer con ese paquete, siempre desde un punto de vista amplio, ya que iptables permite hacer muchas cosas diferentes con el tráfico de red.

4.6.2. Configuración del LINUX FIREWALL.

Ha diferencia de los módulos anteriores Linux Firewall ya viene instalado en el apartado de Networking, lo cual es lógico ya que viene incluido en el propio Kernel de Linux. Aquí se muestra una imagen de su menú principal.

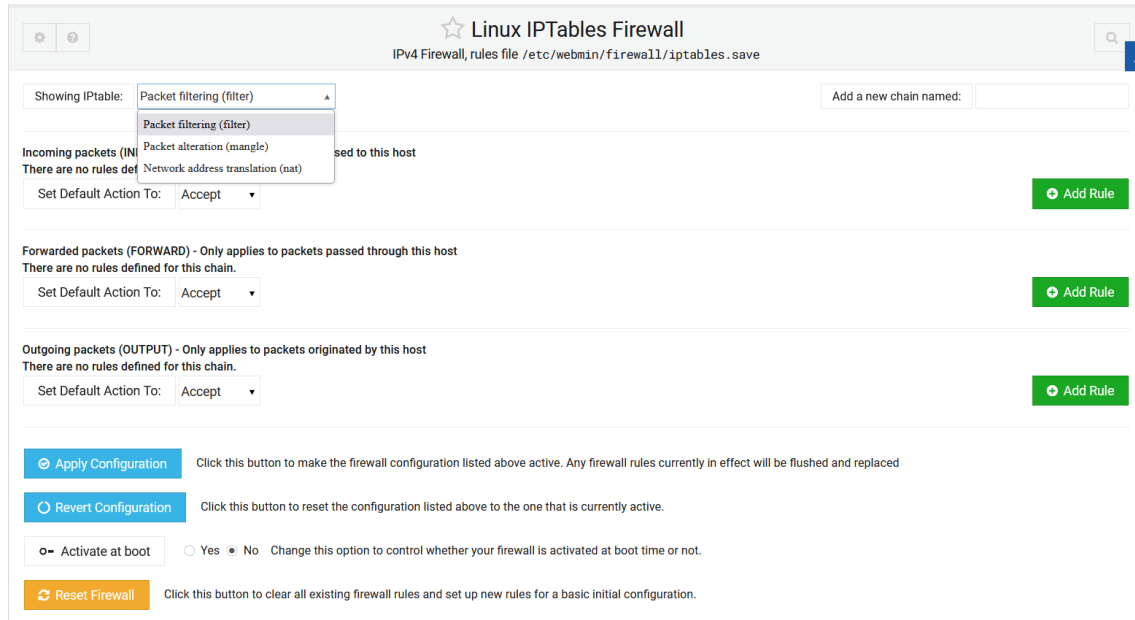


Ilustración 32 - Panel principal Linux Firewall

En este menú principal tenemos las siguientes opciones dependiendo de la configuración que queramos realizar, estas son las 3 cadenas principales, aunque se pueden crear más cadenas:

Packet Filtering - Sirve para filtrar paquetes según criterios predefinidos, permitiendo o denegando su paso a través del firewall.

Packet Alteration (Mangle) - Sirve para modificar campos o características de los paquetes mientras pasan por el firewall.

Network Address Translation (NAT) - Sirve para traducir direcciones IP y puertos entre redes diferentes, permitiendo compartir una única dirección IP pública u ocultar la estructura interna de una red.

Y dentro de cada tabla encontramos las siguientes opciones:

Prerouting - Se aplica a los paquetes entrantes antes del enrutamiento.

Postrouting - Se aplica a los paquetes salientes después del enrutamiento.

Input - Se aplica a los paquetes destinados al sistema local.

Output - Se aplica a los paquetes generados por el sistema para ser enviados.

Forward - Se aplica a los paquetes en tránsito entre interfaces de entrada y salida.

Como ocuparía mucho espacio introducir todas las reglas se va a mostrar cómo se introduciría una regla básica que permite establecer el enrutamiento entre interfaces, así sería la regla escrita:

```
sudo iptables -t nat -A POSTROUTING -o enp0s3 -j MASQUERADE
```

Para introducir la misma regla, elegimos la tabla NAT y nos pinchamos sobre POSTROUTING. A continuación, escribimos un comentario sobre la regla para identificarla y seleccionamos que la acción a tomar sea Masquerade. En nuestra red tenemos 2 interfaces así que elegimos que en incoming interface sea igual a enp0s8 que es la de la red interna y outgoing interface equals enp0s3 que es la que da salida a internet. Simplemente con eso hemos conseguido el mismo resultado que escribiendo la regla anterior.

Part of chain: Packets after routing (POSTROUTING)
 Rule comment: Salida a internet
 Action to take: ☐ Do nothing ☒ Accept ☐ Drop ☐ Masquerade ☐ Source NAT ☐ Run chain

Source ports for masquerading: ☐ Any ☐ Port range: to
 IPs and ports for SNAT: ☒ Default ☐ IP range: to Port range: to

Conditions below are met:

Condition details

Source address or network:

Destination address or network:

Incoming interface: Equals

Outgoing interface: Equals

Fragmentation: ☒ Ignored ☐ Is fragmented ☐ Is not fragmented

Network protocol:

Source TCP or UDP port: ☐ Port range: to

Destination TCP or UDP port: ☐ Port range: to

Source and destination port(s):

TCP flags set: SYN ACK FIN RST URG PSH out of

TCP option number is set:

ICMP packet type: any

Ethernet address:

Packet flow rate: / second

Packet burst rate:

Connection states: New connection Existing connection Related to existing Not part of any connection Not tracked Source NATd Destination NATd

Type of service:

Incoming physical interface:

Outgoing physical interface:

Packet incoming on bridge interface:

Packet outgoing on bridge interface:

Packet is being bridged:

Matching IPset: on incoming traffic

Additional IPtables modules:

Additional parameters:

Ilustración 33 - Creación regla SNAT

Aquí, se muestra diferentes reglas de securización que se han establecido para poder configurar posteriormente el proxy transparente.

Linux IPTables Firewall
 IPv4 Firewall, rules file /etc/webmin/firewall/iptables.save

Showing IPTable: Packet filtering (filter)

Add a new chain named:

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

Select all Invert selection

Action	Condition	Move	Add
<input type="checkbox"/> Accept	If state of connection is RELATED,ESTABLISHED	<input type="text"/>	<input type="text"/>
<input type="checkbox"/> Accept	If input interface is lo and state of connection is NEW	<input type="text"/>	<input type="text"/>

Select all Invert selection

Set Default Action To:

Delete Selected Move Selected

Add Rule

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

There are no rules defined for this chain.

Set Default Action To:

Add Rule

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

Select all Invert selection

Action	Condition	Move	Add
<input type="checkbox"/> Accept	If state of connection is RELATED,ESTABLISHED	<input type="text"/>	<input type="text"/>
<input type="checkbox"/> Accept	If output interface is lo and state of connection is NEW	<input type="text"/>	<input type="text"/>
<input type="checkbox"/> Accept	If protocol is UDP and destination is 8.8.8.8/24 and output interface is enp0s3 and destination port is 53	<input type="text"/>	<input type="text"/>
<input type="checkbox"/> Accept	If protocol is UDP and destination is 192.168.0.1/24 and output interface is enp0s3 and destination port is 53	<input type="text"/>	<input type="text"/>
<input type="checkbox"/> Accept	If protocol is TCP and output interface is enp0s3 and destination ports are 80,443	<input type="text"/>	<input type="text"/>

Select all Invert selection

Set Default Action To:

Delete Selected Move Selected

Add Rule

Apply Configuration Click this button to make the firewall configuration listed above active. Any firewall rules currently in effect will be flushed and replaced

Revert Configuration Click this button to reset the configuration listed above to the one that is currently active.

Activate at boot ☐ Yes ☒ No Change this option to control whether your firewall is activated at boot time or not.

Reset Firewall Click this button to clear all existing firewall rules and set up new rules for a basic initial configuration.

Ilustración 34 - Configuración reglas iptables Proxy

Estas son las reglas establecidas:

Reglas ESTABLISHED y RELATED

```
sudo iptables -A INPUT -m conntrack --ctstate ESTABLISHED,RELATED -j ACCEPT
sudo iptables -A OUTPUT -m conntrack --ctstate ESTABLISHED,RELATED -j ACCEPT
```

Redirigir el trafico que entra por la red interna al puerto del Proxy.

```
sudo iptables -t nat -A PREROUTING -i enp0s8 -p tcp -m multiport --dports 80,443 -j REDIRECT --to-port 3128
```

Prohibir todo el tráfico

```
sudo iptables -P INPUT DROP
sudo iptables -P OUTPUT DROP
sudo iptables -P FORWARD DROP
```

4.6.3. Comprobación del LINUX FIREWALL.

Como comprobación se añade que la regla de la tabla NAT cumple su función. Como podemos ver el cliente no es capaz de resolver Ubuntu.com una vez aplicada la regla, la resuelve perfectamente y con traceroute podemos ver que el da un salto a la 172.16.16.1 para salir por la 192.168.0.1

```
jorgemas@jorgemas:~$ 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: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:02:ad:be brd ff:ff:ff:ff:ff:ff
    inet 172.16.16.100/24 brd 172.16.16.255 scope global noprefixroute enp0s3
        valid_lft forever preferred_lft forever
    inet6 fe80::cd76:f4b0:2c97:8311/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
jorgemas@jorgemas:~$ ping ubuntu.com
ping: ubuntu.com: Fallo temporal en la resolución del nombre
jorgemas@jorgemas:~$ ping ubuntu.com -c 2
PING ubuntu.com (185.125.190.29) 56(84) bytes of data.
64 bytes from website-content-cache-3.ps5.canonical.com (185.125.190.29): icmp_seq=1 ttl=56 time=41.6 ms
64 bytes from website-content-cache-3.ps5.canonical.com (185.125.190.29): icmp_seq=2 ttl=56 time=42.6 ms

--- ubuntu.com ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1002ms
rtt min/avg/max/mdev = 41.582/42.099/42.617/0.517 ms
jorgemas@jorgemas:~$ traceroute -I ubuntu.com
No se ha encontrado la orden «traceroute», pero se puede instalar con:
sudo apt install inetutils-traceroute # version 2:2.2-2, or
sudo apt install traceroute # version 1:2.1.0-2
jorgemas@jorgemas:~$ traceroute -I ubuntu.com
traceroute to ubuntu.com (185.125.190.21), 30 hops max, 60 byte packets
 1 _gateway (172.16.16.1) 0.549 ms 0.504 ms 0.489 ms
 2 192.168.0.1 (192.168.0.1) 2.346 ms * 2.327 ms
 3 10.10.20.10 (10.10.20.10) 9.080 ms 9.066 ms 9.678 ms
 4 he.as6939.et0.mad.txplay.global (185.1.90.14) 9.324 ms * *
 5 * * *
 6 * * *
 7 port-channel1.core1.lon6.he.net (184.104.198.170) 42.357 ms 41.997 ms 41.939 ms
 8 swp9.il3-core2.canonical.com (216.66.89.222) 41.930 ms 41.924 ms 41.918 ms
 9 website-content-cache-2.ps5.canonical.com (185.125.190.21) 40.523 ms 41.904 ms 41.897 ms
jorgemas@jorgemas:~$
```

Ilustración 35 - Comprobación Linux Firewall

4.7. PROXY.

4.7.1. Explicación qué es un PROXY TRANSPARENTE.

Un servidor proxy transparente combina un servidor proxy con un cortafuegos de manera que las conexiones son interceptadas y desviadas hacia el proxy sin necesidad de configuración en el cliente, y habitualmente sin que el propio usuario conozca de su existencia.

4.7.2. Instalación del módulo de PROXY.

La instalación del servidor Proxy es llevada a cabo de la misma manera que las anteriores.

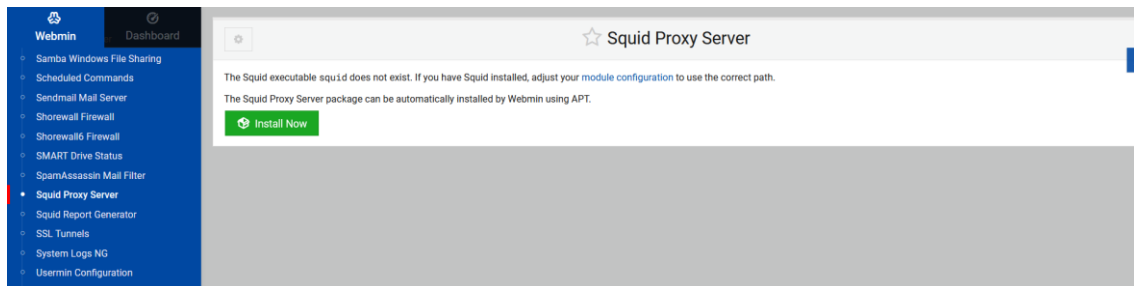


Ilustración 36 - Instalación módulo Squid Proxy

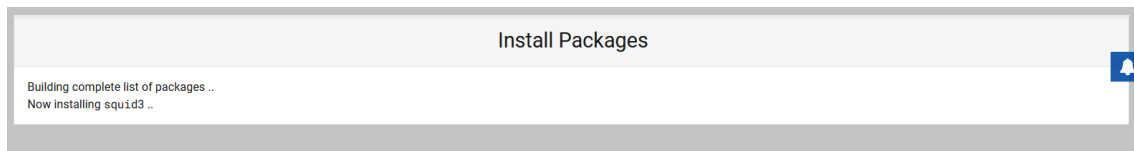


Ilustración 37 - Instalación paquetes Squid Proxy

4.7.3. Configuración del PROXY.

Una vez instalado nos encontramos el siguiente menú principal:

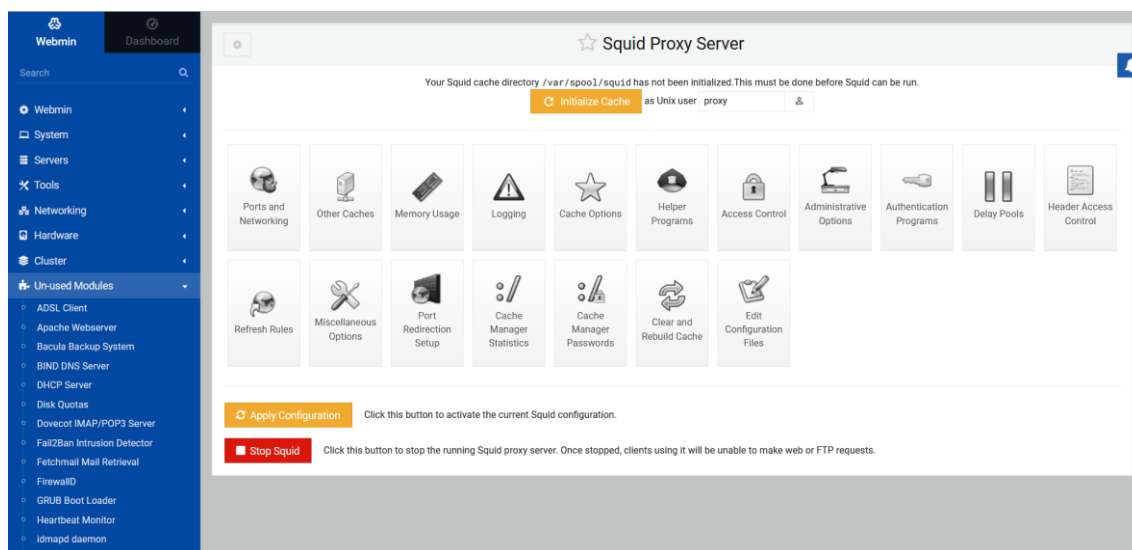


Ilustración 38 - Panel principal Squid Proxy

Y explicamos sus parámetros de configuración:

- **Ports and Networkin** – Sirve para configurar los puertos y la configuración de red utilizados por Squid Proxy Server.
- **Other Caches** - Sirve para configurar Squid para que utilice otras cachés adicionales, como cachés de nivel superior o cachés secundarias.
- **Memory Usage** - Sirve para configurar la cantidad de memoria utilizada por Squid para almacenar en caché objetos y metadatos.
- **Logging** - Sirve para configurar las opciones de registro de Squid Proxy Server.
- **Cache Options** - Sirve para configurar opciones adicionales relacionadas con la caché, como el tamaño máximo de los objetos en caché, la duración de la retención de objetos en caché y las políticas de almacenamiento en disco.
- **Helper Programs** - Sirve para configurar los programas auxiliares utilizados por Squid Proxy Server.
- **Access Control** - Sirve para definir las reglas de control de acceso para restringir o permitir el acceso a ciertos recursos o sitios web.
- **Administrative Option** - Sirve para establecer opciones administrativas para la gestión de Squid Proxy Server.
- **Authentication Programs** - Sirve para configurar programas de autenticación para verificar las credenciales de los usuarios que intentan acceder al proxy.
- **Delay Pools** - Sirve para configurar piscinas de demora para controlar el ancho de banda utilizado por ciertos tipos de tráfico.
- **Header Access Control** - Sirve para configurar reglas para controlar y manipular los encabezados HTTP en las solicitudes y respuestas que pasan a través del proxy.
- **Refresh Rules** - Sirve para controlar la frecuencia con la que Squid debe actualizar los objetos en caché y volver a solicitar recursos al servidor de origen.

- **Miscellaneous Options** - Esta sección contiene opciones adicionales para la configuración de Squid Proxy Server que no se ajustan a las categorías anteriores. Puede incluir configuraciones relacionadas con DNS, SSL, configuración de TCP, entre otros.
- **Port Redirection Setup** - Sirve para configurar la redirección de puertos para redirigir el tráfico a través del proxy a diferentes destinos.
- **Cache Manager Statistics** - Proporciona estadísticas y métricas sobre el rendimiento y el uso de la caché.
- **Cache Manager Passwords** - Sirve para gestionar las contraseñas para acceder a la interfaz de administración de Squid Proxy Server, que es conocida como el "Cache Manager".
- **Clear and Rebuild Cache** - Sirve para borrar y reconstruir la caché de Squid Proxy Server.
- **Edit Configuration Files** - Sirve para editar directamente los archivos de configuración de Squid Proxy Server.

En nuestro caso vamos a crear un proxy transparente para que si un usuario de una red local se quiera conectar a Instagram, Facebook o Twitter, no pueda. Para ello nos vamos a Access Control y creamos una nueva ACL que será del tipo URL Regexp.

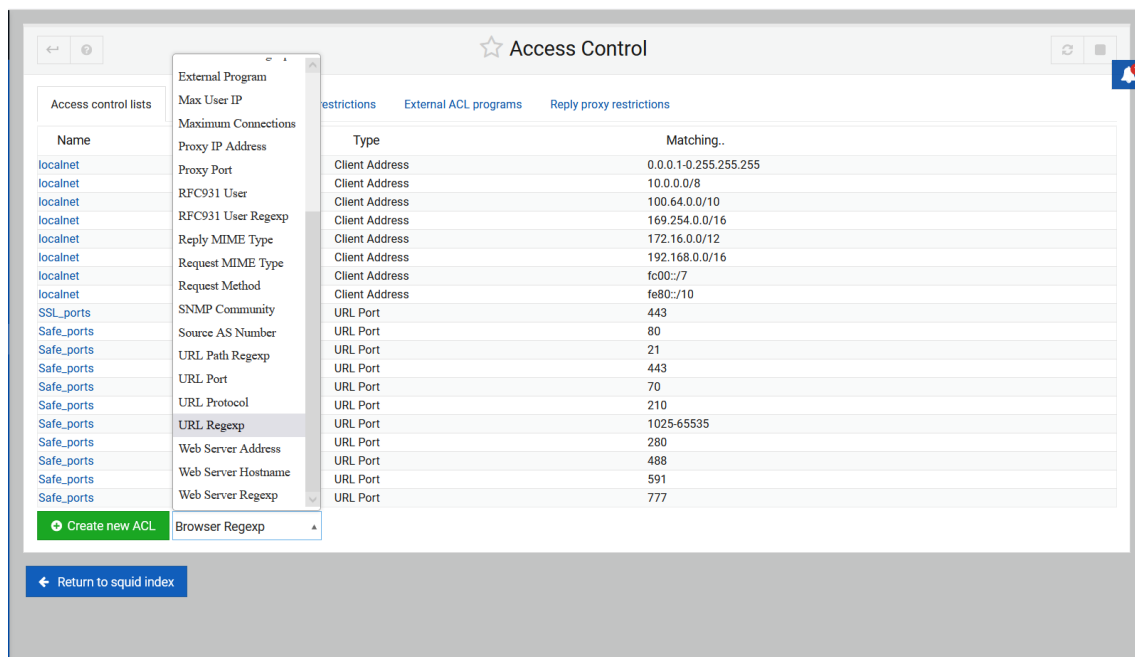


Ilustración 39 - Creacion de la ACL en Squid Proxy

En los parámetros de configuración rellenaremos los siguientes apartados:

The screenshot shows the 'Create ACL' interface. The title is 'URL Regexp ACL'. The 'ACL Name' field contains 'jorgeproyecto'. The 'Regular Expressions' field contains 'facebook', 'twitter', and 'instagram'. The 'Failure URL' field is empty. The 'Store ACL values in file' section has 'Squid configuration' selected. There are buttons for 'Save', 'Return to ACLs', and 'Return to index'.

Ilustración 40 - Parámetros introducidos en ACL

ACL Name – Nombre que se le quiere dar a la ACL.

Regular Expressions – Se introduce la lista de expresiones.

Comprobamos que se ha creado correctamente:

Safe_ports	URL Port	280
Safe_ports	URL Port	488
Safe_ports	URL Port	591
Safe_ports	URL Port	777
jorgeproyecto	URL Regexp	facebook twitter instagram

Buttons: Create new ACL, Browser Regexp, Return to squid index

Ilustración 41 - Comprobación de que la ACL se ha creado

Ahora volvemos a Access Control, pero esta vez en el apartado Proxy restrictions y seleccionamos jorgeproyecto.

The screenshot shows the 'Access Control' interface with the 'Proxy restrictions' tab selected. It displays a table of proxy restrictions. The table has columns for 'Action', 'ACLs', and 'Move'. The rows show various restrictions like 'ISafe_ports', 'CONNECT ISSSL_ports', 'localhost manager', 'localhost', and 'all'. There is a 'Delete Selected Restrictions' button at the bottom.

Ilustración 42 - Campo Proxy restrictions

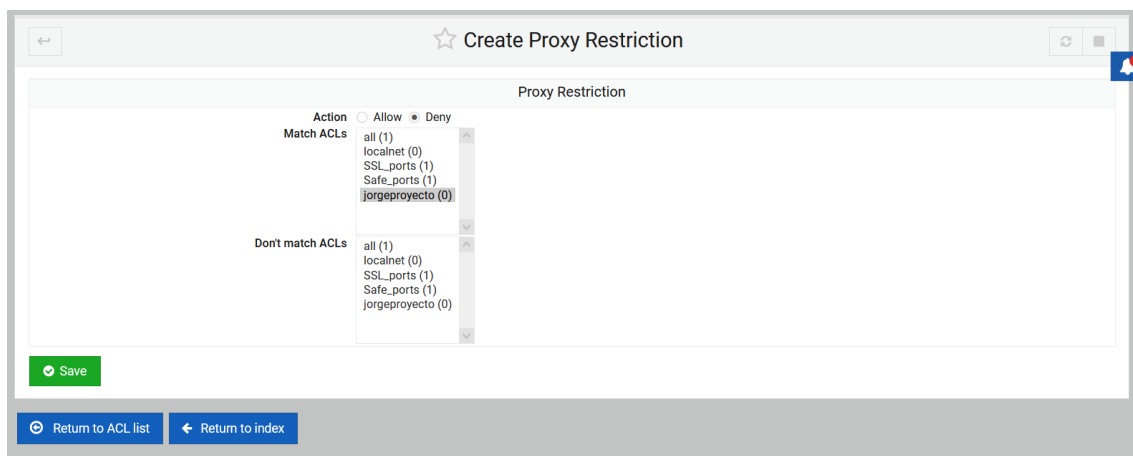


Ilustración 43 - Creación de la restricción Proxy

Con eso ya estaría listo gracias a la configuración de enrutamiento que hicimos anteriormente, como podemos ver se ha creado perfectamente esa regla del proxy. Para su correcta visualización se han eliminado los comentarios y los espacios en blanco del archivo.

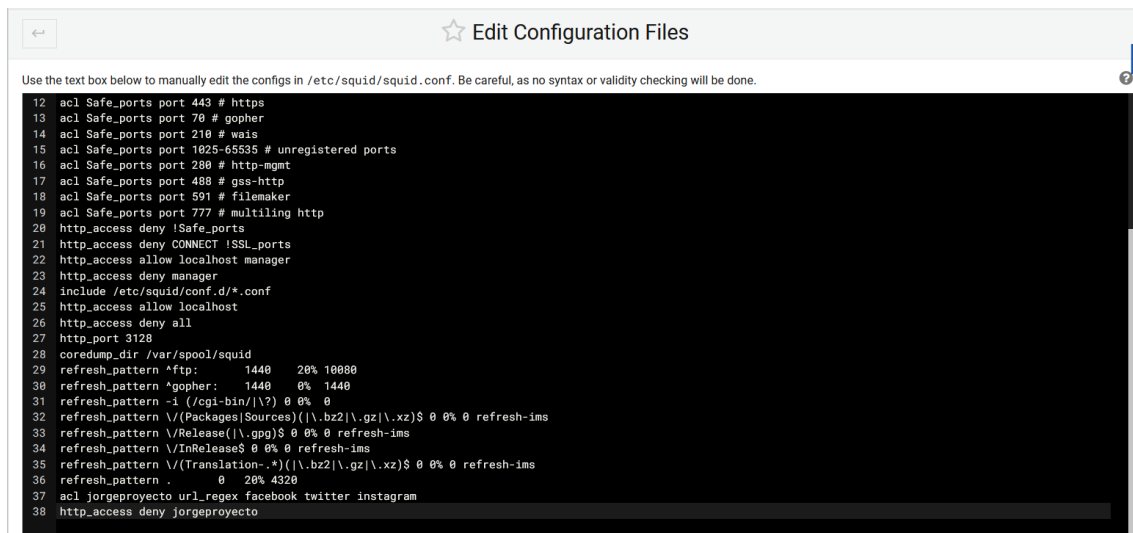


Ilustración 44 - Comprobación del archivo squid.conf

4.7.4. Comprobación del PROXY.

Ahora desde el cliente se puede observar que el proxy está rechazando las conexiones a esas páginas.

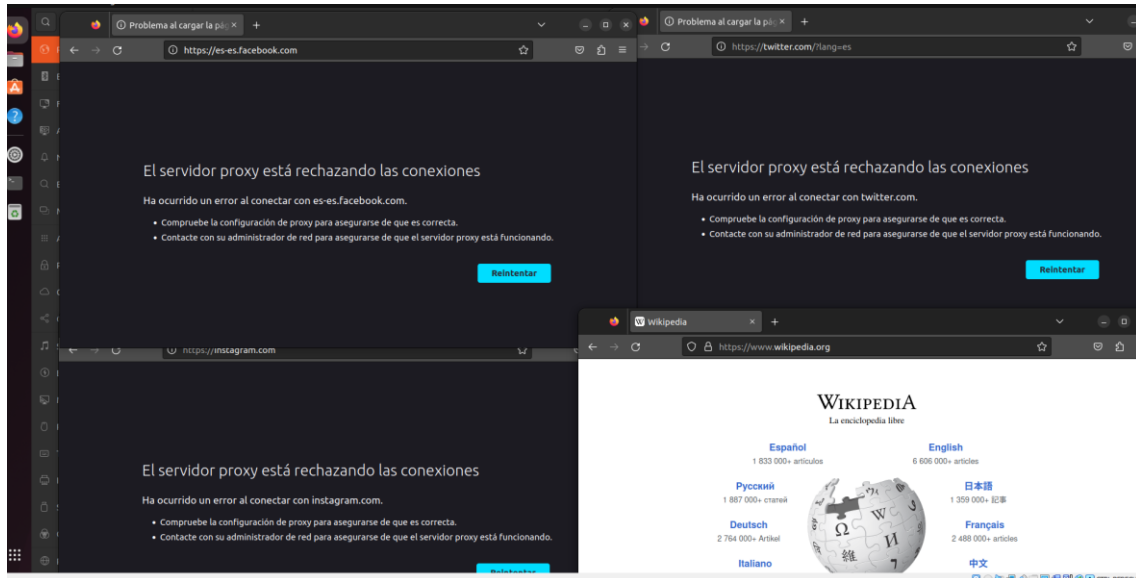


Ilustración 45 - Comprobación desde el cliente

4.8. Seguimiento y control.

Para poder realizar un seguimiento y control de nuestra instalación Webmin y configuración de los servicios disponemos de varias herramientas muy útiles.

4.8.1. Panel de control.

Desde el panel de control el cual arranca automáticamente podemos ver el estado del servidor, con un simple vistazo podemos ver el uso de la CPU, memoria Ram, memoria virtual y espacio disponible en el disco. Esto nos permite avisar a un cliente si su servidor necesita ser ampliado o está sufriendo cualquier tipo de problema.

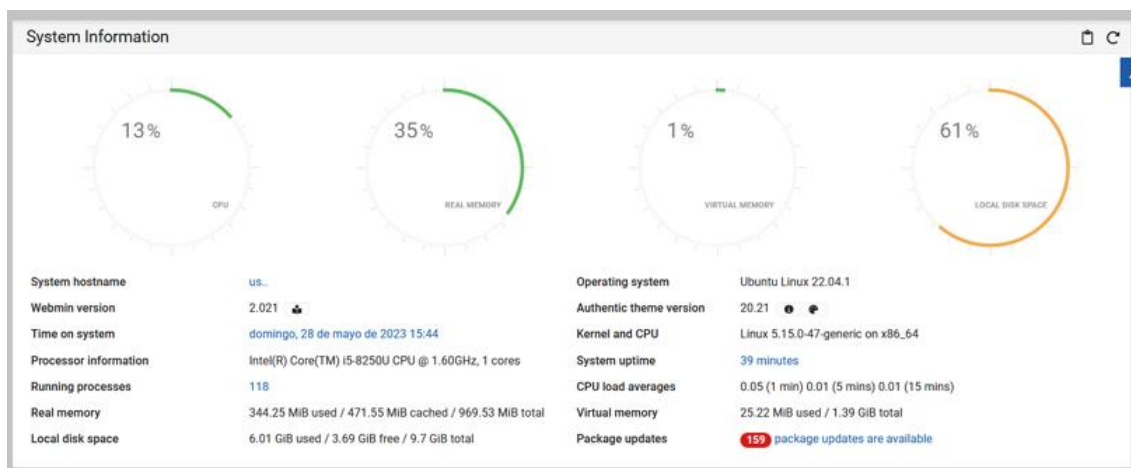


Ilustración 46 - Panel de control

Pero el que más nos interesa es el apartado de System and Serve Status, en el cual podemos monitorizar el estado de los servicios ofrecidos. En este apartado podemos comprobar que todos los servicios tienen un estado validado.

System and Server Status		
Add monitor of type: Alive System		
<input checked="" type="checkbox"/> Select all <input type="checkbox"/> Invert selection		
Monitoring	On host	Status
<input type="checkbox"/> Squid Proxy Server	Local	✓
<input type="checkbox"/> BIND DNS Server	Local	✓
<input checked="" type="checkbox"/> Select all <input type="checkbox"/> Invert selection		
<input checked="" type="button" value="Delete Selected"/> <input checked="" type="button" value="Refresh Selected"/>		
Add monitor of type: Alive System		

Ilustración 47 - Panel System and Server Status

A parte podemos crear una tarea de comprobación, con el horario que queramos para realizar la comprobación y nos avise por email y SMS si alguno de los servicios se ha caído. En mi caso he elegido cada 8h todos los días de la semana.

Scheduled Monitoring

Scheduled background monitoring options

Scheduled checking enabled?

☒ Yes ☐ No

Check every

5 minutes with offset 0

Run monitor during hours

00:00	06:00	12:00	18:00
01:00	07:00	13:00	19:00
02:00	08:00	14:00	20:00
03:00	09:00	15:00	21:00
04:00	10:00	16:00	22:00
05:00	11:00	17:00	23:00

Send one email per service?

☐ Yes ☒ No

Run monitor on days

Sunday
Monday
Tuesday
Wednesday
Thursday
Friday
Saturday

Send email when

☐ When a service changes status ☒ When a service goes down ☐ As long as the service is up ☐ Any time service is down

Email status report to

☐ Don't send email ☒ Email status report to

From: address for email

☐ Default (webmin) ☒ jorge@proyecto.com

Send mail via

☒ Local mail server ☐ SMTP server

Page status report to number

☒ Don't send pages ☐

Send SMS to

☐ Nobody ☒ Phone on carrier T-COM with number 1111111111

Subject line for SMS messages

☒ None (alert is in the body)
☐ Alert text (leave body empty)
☐ Custom text

Save

A continuación, realizaremos una tarea para la creación automática de las copias de seguridad de los servicios instalados, para ello tenemos el apartado de Create Scheduled Backup, donde seleccionaremos los módulos que queremos hacer copia, donde queremos guardar esa copia y la frecuencia con la que se realizarán esas copias. Por razones obvias esa copia se guardará en otro destino distinto del servidor. Para mi caso se realizará a las 0:00 todos los días del año.

Create Scheduled Backup

Scheduled backup options

Modules to backup

- ADSL Client
- Apache Webserver
- BIND DNS Server**
- Bacula Backup System
- Bandwidth Monitoring
- Bootup and Shutdown
- Custom Commands

Backup destination

☐ Local file

☒ FTP server

16.16.16.1 file on server

Login as user jorgemas with password *****

Server port ☒ Default

☐ SSH server

file on server

Login as user with password

Server port ☒ Default

Include in backup

☒ Webmin module configuration files ☒ Server configuration files ☐ Other listed files ..

Ilustración 50 - Creación de tarea del backup (1)

Backup schedule

Email result to address jorgemas@jorgemas.net

When to send email ☒ Always ☐ Only when an error occurs

Scheduled backup enabled? ☐ No ☒ Yes, at times selected below ..

☐ Simple schedule .. Hourly ☒ Times and dates selected below ..

Minutes

☐ All ☒ Selected ..

0	12	24	36	48
1	13	25	37	49
2	14	26	38	50
3	15	27	39	51
4	16	28	40	52
5	17	29	41	53
6	18	30	42	54
7	19	31	43	55
8	20	32	44	56
9	21	33	45	57
10	22	34	46	58
11	23	35	47	59

Hours

☐ All ☒ Selected ..

0	12
1	13
2	14
3	15
4	16
5	17
6	18
7	19
8	20
9	21
10	22
11	23

Days

☐ All ☒ Selected ..

1	13	25
2	14	26
3	15	27
4	16	28
5	17	29
6	18	30
7	19	31
8	20	
9	21	
10	22	
11	23	
12	24	

Months

☒ All ☐ Selected ..

January
February
March
April
May
June
July
August
September
October
November
December

Weekdays

☐ All ☒ Selected ..

Sunday
Monday
Tuesday
Wednesday
Thursday
Friday
Saturday

Note: Ctrl-click (or command-click on the Mac) to select and de-select minutes, hours, days and months.

Create

Ilustración 51 - Creación de tarea del backup (2)

En caso de que surja algún problema, recuperaremos la copia de seguridad desde Filesystem BackUp, seleccionando la ruta donde se encuentra dicha copia y el formato en el que esta.

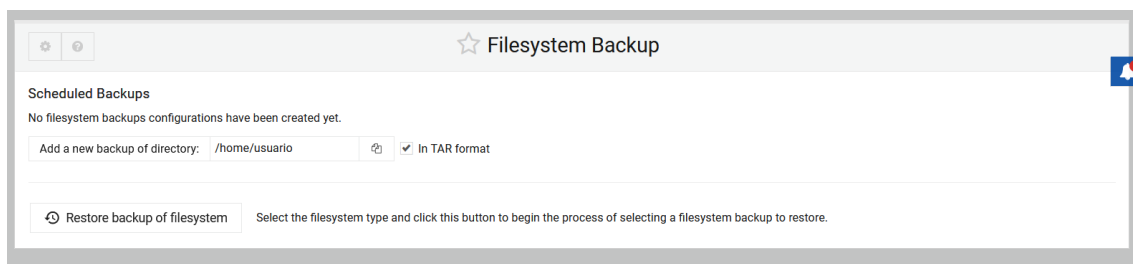


Ilustración 52 - Recuperación del backup

5. Estudio presupuestario.

Se procede a identificar lo que costaría poder implementar este servicio en la actualidad, desglosando los materiales y el software necesario. Se obvian evidentemente otros gastos como puede ser la luz.

Coste para el administrador:

- Equipo informático completo: 600€
- Conexión a internet 1 GB Fibra óptica DIGI: 20€ mensuales
- Software Webmin: Gratis.

Como se puede observar el precio es irrisorio para el servicio que puede ofrecer un administrador de red desde cualquier parte del mundo.

Coste para el cliente:

- Coste de la implementación y configuración básicos: 400€
- Coste de mantenimiento y soporte básico: 100€ mensuales.
- Ampliaciones u otros: Precio variable dependiendo del servicio, lo cual podría aumentar también el coste de mantenimiento y soporte.

Como puede observarse sería un negocio viable dependiendo del número de clientes que se tengan.

6. Conclusiones.

Durante la investigación, desarrollo y documentación de este proyecto, se llega a la conclusión que Webmin es una herramienta gratuita, altamente eficaz a la hora de poder configurar un servidor sin tener que saber rutas específicas y la nomenclatura de los servicios. Su interfaz ayuda mucho al administrador ahorrándole tiempo y el cometer posibles errores de sintaxis. Contiene numerosos módulos de los servicios más comunes, aunque se echan en falta otros más actuales como puede ser el proxy NGINX y otros están obsoletos. En el ámbito laboral facilitará la labor del administrador de red en la implementación de los servicios que un cliente quiera, además puede ofrecerle una futura mejora y escalabilidad dependiendo de sus necesidades. En resumen, es una forma fácil de controlar los servicios de un servidor y ofrecer un buen servicio al cliente.

6.1. Debilidades.

Falta de módulos: No todos los servicios que están disponibles para Linux están incluidos en Webmin y algunos de los que están incluidos están obsoletos

Posibles vulnerabilidades de seguridad: Es esencial mantener Webmin actualizado junto con sus módulos para evitar posibles vulnerabilidades de seguridad que podrían ser explotadas por atacantes.

6.2. Amenazas.

Ataques de fuerza bruta: Los servidores de Webmin pueden ser objeto de ataques de fuerza bruta, donde los atacantes intentan adivinar las credenciales de inicio de sesión.

Exposición a Internet: Como Webmin va a estar configurado para ser accesible desde Internet, existe el riesgo de que se convierta en un objetivo para ataques externos.

Routers que ya incluyen estas funciones: Existen routers que con su sistema operativo ya puedes realizar lo mismo. Un ejemplo sería RouterOS 7 de Mikrotik.

6.3. Fortalezas.

Interfaz gráfica amigable: Webmin proporciona una interfaz gráfica intuitiva y fácil de usar que permite a los administradores de sistemas administrar y configurar servicios de forma eficiente, sin la necesidad de editar manualmente archivos de configuración.

Amplia compatibilidad: Webmin es compatible con una amplia variedad de sistemas operativos Linux, lo que lo hace una herramienta versátil para la administración de servidores.

6.4. Oportunidades.

Comunidad activa y soporte: Webmin cuenta con una comunidad activa de usuarios y desarrolladores, lo que brinda oportunidades de obtener soporte, compartir conocimientos y beneficiarse de las actualizaciones y mejoras continuas de la herramienta.

6.5. Ampliaciones futuras.

Un apartado importante es que Webmin permite la instalación de módulos adicionales, también conocidos como "módulos Webmin", los cuales pueden agregar nuevas funcionalidades y servicios. Estos módulos pueden ser desarrollados por la comunidad o por terceros, y pueden ampliar la gama de opciones de administración.

6.6. Escalabilidad.

Webmin se ejecuta en un servidor por lo que su escalabilidad está relacionada con la capacidad de dicho servidor para manejar las demandas del sistema y del tráfico de red. La escalabilidad en este sentido implica asegurarse de que el servidor en el que se ejecuta Webmin tenga suficientes recursos, como potencia de procesamiento, memoria y almacenamiento, para soportar un crecimiento en el número de sistemas y dispositivos de red administrados, así como un aumento en la carga de trabajo de la administración. (Karzynski, 2014)

7. Bibliografía. (Ralph Droms, 2002)

Cricket Liu, P. A. (2006). *DNS and BIND, 5th Edition*. Sebastopol, CA: O'Reilly Media, Inc.

Evi Nemeth, G. S. (2001). *Unix and Linux System Administrator Handbook, 4th Edition*. Boston: Prentice Hall.

Karzynski, M. (2014). *Webmin Administrator's Cookbook*. Birmingham : Packt.

Ralph Droms, T. L. (2002). *The DHCP Handbook, 2nd Edition*. Indianapolis: SAMS.

8. Anexos.

Como anexo se incluye, que Webmin ofrece en herramientas, el acceso a la terminal, por si hay que hacer un cambio manual de alguna configuración del propio sistema. Esto sería utilizado como último recurso y por ello no esta incluido en la memoria técnica del proyecto.

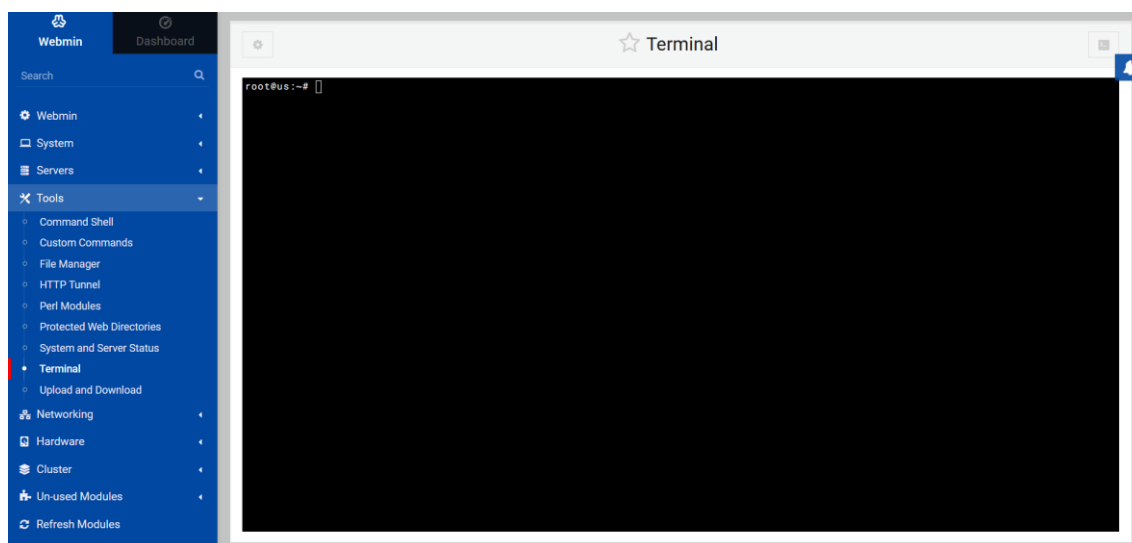


Ilustración 53 -Acceso desde la terminal al servidor.