



ElHamiti News

2024

PROYECTO DE
ADMINISTRACIÓN DE
SISTEMAS INFORMÁTICOS
EN RED

Realizado por:
Felipe Giménez Martínez, Josías González Rubio,
Antonio Perales Calero y Diego Alfonso Chicoma Ibáñez

Tutor: Adrián Ciudad

Resumen

El proyecto de infraestructura de redes para el nuevo edificio de ElHamiti News en Madrid contempla la implementación de dos redes distintas: una red privada y una zona desmilitarizada (DMZ) para acceso público. La DMZ albergará el servidor web que proporcionará noticias de la empresa, mientras que la red privada estará dividida en una red de trabajadores y una red de servidores. La red de servidores alojará servicios internos como DNS, correo corporativo y base de datos. Los equipos corporativos de los empleados se conectarán a la red de trabajadores, con asignación dinámica de IP a través de un servidor DHCP y seguridad gestionada por un firewall. Se facilitará el acceso remoto a los equipos mediante VPN y con bloqueo de contenido no autorizado mediante un proxy transparente. Usuarios y equipos se integrarán en el dominio de la empresa gestionado por LDAP. Este diseño garantiza una infraestructura de red eficiente, segura y compatible con las necesidades de ElHamiti News.

Palabras Clave

DMZ, Red privada, Periódico Digital, Diseño, Desarrollo

INDICE

Resumen.....	1
Palabras Clave.....	1
Introducción	4
Finalidad de la empresa	4
Módulos aplicados	5
Desarrollo del proyecto.....	5
Componentes del equipo.....	7
Fases del proyecto.....	7
Material	8
Partes de la red.....	9
1. DMZ.....	9
1.1. Servidor web.....	9
1.2. Sitio web	9
1.3. DHCP.....	18
2. Red Privada.....	20
2.1. DNS	20
2.2. Firewall.....	24
2.3. Proxy.....	27
2.4. Correo	30
2.5. VPN	34
2.6. LDAP.....	37
2.7. SIEM.....	41
2.8. Base de datos	45
2.9. Rsyslog	47
Conclusiones	48
Bibliografía	49
Tabla de ilustraciones	52
Anexos	54
1. Código fuente del sitio web	54
2. Manual de instalación Proxmox.....	54
3. Archivos de conexión VPN (Wireguard y OpenVPN)	54
4. Reglas de cortafuegos de los routers.....	54

5.	Registro de Rsyslog de un equipo.....	54
6.	Archivos configuración de LDAP	54
7.	Logs de SIEM	54
8.	Correo de ejemplo de newsletter.....	54
9.	Anteproyecto.....	54

Introducción

La empresa ElHamiti News tiene como objetivo proporcionar servicios informativos en el ámbito de la informática, abarcando áreas como la ciberseguridad, el hardware, la programación y la inteligencia artificial, entre otras, dirigidos al público interesado.

Para lograr esto de manera efectiva, la empresa requiere una estructura de red que sea capaz de alojar los servicios necesarios para su correcto funcionamiento interno. Estos servicios incluyen DNS, correo electrónico, DHCP, VPN, base de datos, alojamiento web, firewall y LDAP para la gestión de usuarios y permisos.

Finalidad de la empresa

La motivación detrás de la creación de ElHamiti News radica en la creciente importancia de la tecnología en nuestras vidas y en la necesidad de un medio que no solo informe sobre las últimas tendencias y desarrollos, sino que además promueva la comprensión y el diálogo sobre el impacto de la tecnología en la sociedad.

ElHamiti News opta por un formato de periódico digital, brindando acceso instantáneo a su cobertura en línea, permitiendo a los lectores estar al tanto de las últimas noticias desde cualquier dispositivo conectado a Internet en cualquier parte del mundo.

Se podría comparar con otros periódicos digitales internacionales de renombre, como TechCrunch¹, Wired² o The Verge³, en términos de su enfoque en la tecnología y la informática, así como en la calidad y amplitud de su cobertura.

¹ TechCrunch: [TechCrunch - Wikipedia, la enciclopedia libre](#)

² Wired: [Wired - Wikipedia, la enciclopedia libre](#)

³ The Verge: [The Verge - Wikipedia, la enciclopedia libre](#)

Módulos aplicados

Dado que el trabajo se basa en crear una red lo más real posible, se configuran los servicios necesarios para abordar todas las asignaturas que han sido cursadas. Se incluyen varios ejemplos, como la configuración de un servidor de correo y un servidor DHCP para “Servicios de Red e Internet”. Además, se configura un servidor LDAP para gestionar los trabajadores y sus cuentas en la empresa, sección correspondiente a la asignatura de “Administración de Sistemas Operativos”.

A su vez, se implementa un cortafuegos, contenido correspondiente al módulo de “Seguridad y Alta Disponibilidad”.

Por último, se lleva a cabo la creación de una base de datos y un sitio web para abordar las asignaturas de “Implantación de Aplicaciones Web” y “Administración de Sistemas Gestores de Bases de Datos”. Por último, debido al uso de HTML, CSS y JavaScript, además de las asignaturas mencionadas, se podría sumar a ellas “Lenguajes de Marcas” en el lado del cliente.

Desarrollo del proyecto

Para poder crear la red se ha decidido dividir la red en dos partes, una primera red que se ha configurado como una DMZ o Zona desmilitarizada, la cual permitirá a la empresa exponer su página web de noticias al público en general, es decir, toda persona que busque la web de ElHamiti News va a conectarse al servidor de la empresa, pudiendo ver las diferentes noticias que publique la empresa.

La segunda red será una red privada, a la que solo se puede acceder si se es un trabajador de la empresa. En esta red se podrá distinguir entre la red de los trabajadores y la red de los servidores. En la red de los trabajadores, los usuarios que trabajen para la empresa podrán conectarse con su equipo y trabajar desde el mismo; por otro lado, la red de servidores donde los usuarios no podrán acceder salvo que sean administradores o se quieran conectar a su equipo dentro del servidor del dominio corporativo.

Dentro de la red de servidores se encontrarán los diferentes servicios internos de la empresa como son el servidor DNS o servidor de nombres de dominio, que permite identificar una IP con un nombre que se le asigne a un equipo. También, se encontrará el servidor de correo corporativo, al igual que el servidor de bases de datos, donde se almacenarán los usuarios y noticias que tiene la empresa.

Para poder gestionar las diferentes redes que tendrá la empresa se creará un servidor DHCP, que permite asigna una IP a cada equipo, dicho de otra forma, mediante el DNS se asigna a una IP un nombre dentro del dominio y con el DHCP se permite asignar una IP a cada equipo.

A continuación, además, se gestionará si una red es privada o pública mediante un firewall que permita cuales son las conexiones deseadas y cuáles no. No olvidar, que con referencia a las búsquedas de los usuarios, se bloquearan contenidos de internet con un proxy transparente, el cual sin saber los usuarios que existe, el propio proxy manejará las búsquedas permitidas.

Todo el trabajo se terminará con una VPN, dando a la red un acceso remoto a la red sin pertenecer directamente a ella, o sea, desde cualquier punto se podrá conectar y acceder a la red interna, ya que dicha VPN solo que la podrán tener los trabajadores de la empresa (Administradores) y gestionarán los equipos corporativos usando LDAP.

Componentes del equipo

El equipo está compuesto por los siguientes miembros y las tareas realizadas por cada uno:

- Antonio: servidor DHCP, servidor de VPN, newsletter y firewall.
- Felipe: servidor DNS, servidor proxy y servidor SIEM .
- Alfonso: Desarrollo web (front-end y back-end), newsletter, servidor web y servidor de base de datos.
- Josías: servidor de LDAP, servidor de correo y servidor de Rsyslog.

Fases del proyecto

1^{ra} fase: Instalación de sistema operativo Proxmox, creación de VPN al servidor y contenedores de LXC dentro del servidor. Inicio del desarrollo front-end de la página web.

2^{da} fase: Creación de servidor DHCP y VPN interna.

3^{ra} fase: Creación de servidor DNS, Proxy e inicio LDAP

4^{ta} fase: Terminación del servidor LDAP e inicio servidor de correo.

5^{ta} fase: Creación del servidor web, base de datos y hacer pública la página web.

6^{ta} fase: Terminación del servidor de correo e inicio del desarrollo back-end de la página web.

7^{ma} fase: Terminación del desarrollo back-end de la página web.

8^{va} fase: Creación de la newsletter, el servidor SIEM y el servidor Rsyslog.

Material

El material utilizado durante el proyecto se divide en dos secciones, la parte de software y la de hardware.

En cuanto a hardware se utiliza un mini PC que actúa como servidor alojando el resto de los servicios. En lo que respecta a software se utilizan las siguientes tecnologías:

- **Servidor de Directorio Activo:** OpenLDAP y LDAP-Account-Manager (LAM).
- **Servidor DNS:** Bind9.
- **Dos servidores VPN:** OpenVPN y Wireguard.
- **Servidor Proxy:** Squid.
- **Servidor de base de datos:** MySQL.
- **Sitio web:** CSS, HTML, PHP, JavaScript, jQuery, Git (GitHub).
- **Servidor web:** Apache2.
- **Servidor DHCP:** módulo de DHCP-Server para Ubuntu.
- **Servidor de correo:** Postfix, Dovecot y Roundcube.
- **Se usarán dos sistemas operativos:** Ubuntu 22.04 y Proxmox.
- **Servidor SIEM:** Elasticsearch, Kibana, Filebeat, Nginx y Logstash.
- **Servidor de Logs:** Rsyslog.
- **Newsletter:** PHPMailer, PHP, Postfix.

Partes de la red

En este apartado se incluirán todos los aspectos técnicos de cada servicio de la empresa, desde las herramientas utilizadas hasta el código utilizado en cada una de ellas.

1. DMZ

1.1. Servidor web

Para exponer el sitio web al público, se ha optado por la instalación de un servidor web Apache2 con PHP y un servidor de base de datos (MYSQL).

El servidor Apache2 tendrá todos los archivos necesarios para un funcionamiento correcto del servidor web, para ello se necesita el directorio raíz del proyecto, para ello se colabora con GitHub para guardar el repositorio en su nube y así tenerlo más accesible para su incorporación.

1.2. Sitio web

Como parte fundamental de la empresa, se ha creado un servicio web donde habrá que incluir los documentos: HTML, CSS (como parte del front-end) y JavaScript, PHP y MySQL (como parte del back-end). Se procede a explicar cómo se ha desarrollado cada parte.

1.1.1. Diseño y estructura HTML

Esta estructura permanecerá en todas las diferentes páginas web, como se puede apreciar en la imagen, es una estructura sencilla, pero gracias al empleo de layout “grid” el sitio web queda totalmente responsive.

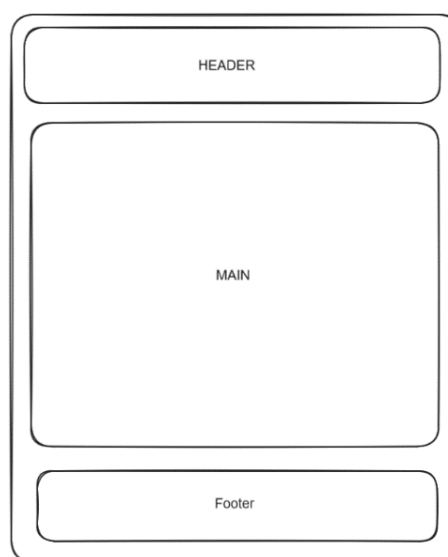


Ilustración 1: Estructura principal

Esta estructura pertenece al elemento **header (cabecera de la página)** donde se encuentran estos cuatro diferentes elementos:

- El logo de la empresa.
- Filtro por título: Donde se puede filtrar dependiendo de que título se busque.
- Páginas web: Una navegación simple a través de la páginas web.
- Utilidades extras: Cambio de modo de lectura y cambio de idioma.

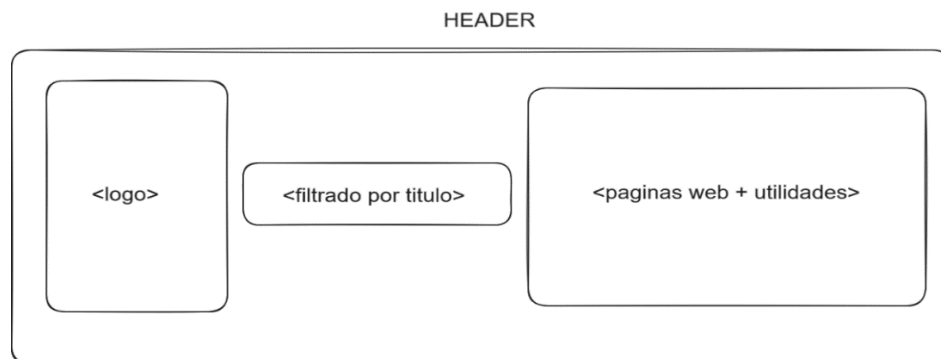


Ilustración 2: Estructura del header

Ahora se continúa con la explicación de la estructura del elemento main (contenido principal), en este apartado se ubica todo lo relacionado con el contenido principal que se mostrará en la página web, este cambiará dependiendo en que página web se encuentre uno.

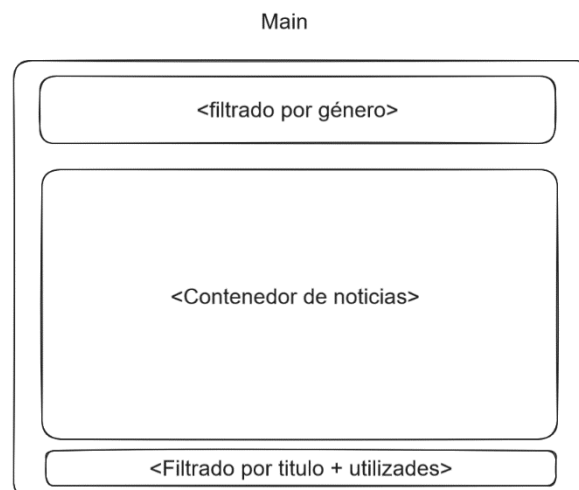


Ilustración 3: Estructura del main

Finalmente se puede encontrar el elemento footer (pie de la página), donde estarán los elementos informativos sobre la licencia del sitio web e hipervínculos referenciando a las redes sociales.

Footer

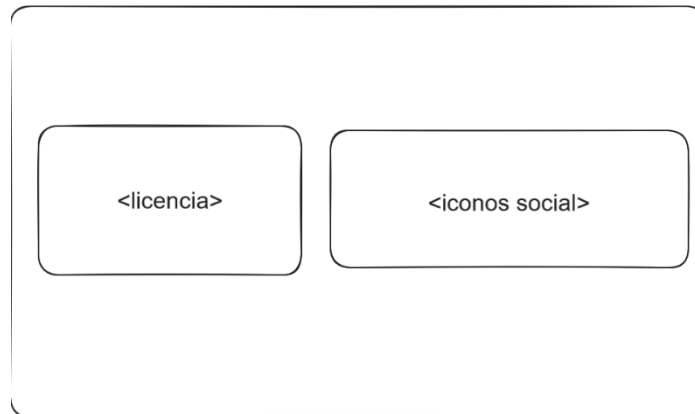


Ilustración 4: Estructura del footer

1.1.2. Descripción etiqueta <header>

Como se ha mencionado en el anterior apartado, el header cuenta con 3 partes, en este apartado se van a describir técnicamente a continuación.

Utilizando los estilos CSS se representa el header de manera horizontal, para la parte del filtrado por título de noticia, se encontrarán con un elemento llamado **<input>** que tendrá un tipo texto, es decir, se podrá poner tanto número como letras como símbolos especiales, para poder filtrar seguido de dos **hipervínculos** que llevan a las diferentes páginas web y finalmente, se encuentran las utilidades de idioma y modo de visión representados por elementos **svg**.

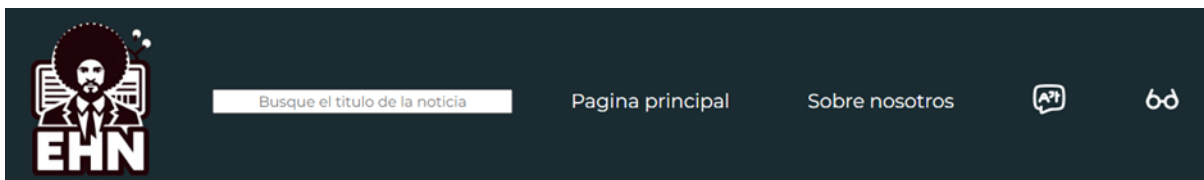


Ilustración 5: Descripción header

1.1.3. Descripción etiqueta <main>

Como se menciona en la estructura del **main**, en este se mostrará el contenido principal de la página web, primero empezar con la descripción de la página web principal.

En esta se ubica una barra de navegación con los diferentes géneros de noticias que se tendrán en el periódico. El siguiente elemento que se encuentra son las diferentes redacciones de noticias, estas son representadas de la siguiente manera: Imagen, título, género y fecha de publicación y descripción de la noticia.



Ilustración 6: Descripción main (Pagina "index")

En la página “sobre nosotros” se encuentran un formato totalmente diferente del elemento **main**. Este se ubicará con dos diferentes columnas, la primera columna está relacionada con el objetivo de la empresa y el equipo que lo forma la empresa y sus respectivas fotos.

En la segunda columna, se encuentran con los servicios que ofrece y la posibilidad de inscribirse en la newsletter creada, que proporcionaría las ultimas noticias que el equipo de redactores haya publicado.



Ilustración 7: Descripción main (Página "SobreNosotros")

1.1.4. Descripción etiqueta <footer>

En el último elemento del sitio web se representa de manera horizontal, con los elementos anteriormente mencionados con una animación de fondo.

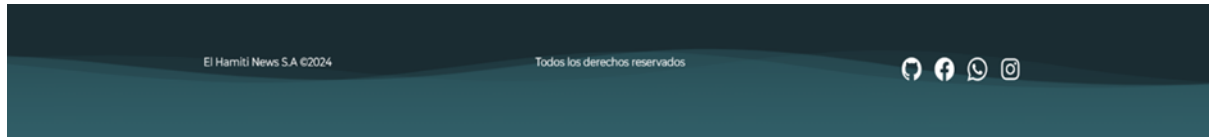


Ilustración 8: Descripción footer

1.1.5. Funciones JavaScript

En este apartado se explican las diferentes funcionalidades del sitio web:

- **Funciones de cambios de estado:** Utilizados principalmente para activar los diferentes botones y a la hora de su ejecución cambiar el estado de ciertos elementos de la página web, por ejemplo, los modos de visión que incluyen tres tipos de cambios de estado dependiendo de cual escoja, en este caso esta función se realizará a la hora de realizar click encima del elemento.
- **Funciones por scroll:** Utilizados para alterar el comportamiento de ciertos elementos según la posición de la viewport, por ejemplo, en la barra de navegación del elemento main solo se mostrará si en el viewport no se ve el header, y este se ocultará cuando llegue al final de la página.
- **Funciones de igualar inputs:** Esta función solo es utilizada para igualar los inputs que se tienen en la página principal, uno en el header y otro en el main.

1.1.6. Funciones PHP

Finalmente, en este apartado se explican las diferentes funcionalidades en lenguaje PHP.

- **Conexión con el servidor de base de datos:** Se realiza un archivo para esta función, ya que se necesitará para las demás funcionalidades relacionadas con la base de datos.
- **Manipulación de la base de datos:** con protección ante inyecciones SQL.
- **Variables de sesión:** para mantener ciertos atributos entre las páginas de la empresa hasta que se cierre sesión o se cambie el valor de las variables.
- **Consultas de la base de datos:** utilizadas para representar el contenido de las noticias.
- **API para los redactores:** Constará de un login con el usuario y contraseña correspondiente a cada uno de nuestros redactores, así como la redacción de las noticias, donde los redactores podrán introducir todos los datos relacionados con las noticias (fecha de publicación, títulos, etc.).
- **Cierre de sesión:** Permite cerrar sesión, exclusivamente para redactores.

1.1.7. Newsletter

Para realizar la newsletter de su empresa, se utilizará PHP y los servicios de correo para su realización. Se comenzará explicando el código PHP que se ha utilizado.

Se ha empleado una biblioteca de PHP llamada PHPMailer, la cual permite establecer una conexión SMTP con el correo de la empresa. Para que esta conexión se realice de manera exitosa y funcional para la empresa, se ha configurado lo siguiente para conectar con el servidor de correo. Además, se necesitará un usuario válido con los permisos correspondientes.

```
<?php  
  
require_once('./PHPMailerAutoload.php');  
  
$mail = new PHPMailer;  
  
$mail->IsSMTP();  
$mail->Host = 'email.server.elhamiti.local';  
$mail->SMTPSecure = 'TLS';  
$mail->Port = 587;  
$mail->SMTPAuth = true;  
$mail->Username = 'admin@server.elhamiti.local';  
$mail->Password = 'admin_elhamiti';  
$mail->From = 'admin@server.elhamiti.local';  
$mail->FromName = 'El hamiti News';  
$mail->CharSet = 'UTF-8';  
?>
```

Aparte de necesitar PHP y el servicio de correo, se necesitará un contenido que enviar. Para ello, la empresa dispone de una plantilla HTML diseñada específicamente para la newsletter, ahora se continuará con la configuración aplicada al servicio de correo



Ilustración 9: Plantilla email por HTML

Para vincular la página web con el servidor de correo se necesita en primer lugar, ir al archivo de alias del contenedor donde se alojará la página web y asignar el nombre del usuario www-data al correo que se verificará como si fuera el que envía el correo automático.


```
GNU nano 6.2 /etc/aliases
postmaster: root
webmaster: root
www-data: admin@server.elhamiti.local
```

Ilustración 10: Asignar el alias a la cuenta de correo

A continuación, se asigna al relayhost el servidor de correo que se tenga configurado para que reciba el correo y lo reenvíe a su destino. Además, hay que habilitar el uso de SALS para que se autentique el servidor web como uso del usuario de correo que se especifica en el archivo `/etc/postfix/sasl_passwd`.

```
GNU nano 6.2 /etc/postfix/main.cf
# See /usr/share/postfix/main.cf.dist for a commented, more complete version

smtpd_banner = $myhostname ESMTP $mail_name (Debian/GNU)
biff = no

# appending .domain is the MUA's job.
append_dot_mydomain = no

# Uncomment the next line to generate "delayed mail" warnings
#delay_warning_time = 4h

alias_maps = hash:/etc/aliases
alias_database = hash:/etc/aliases
mydestination = $myhostname, localhost.$mydomain, localhost
relayhost = email.server.elhamiti.local:587, smtp.office365.com:587
mynetworks = 127.0.0.0/8
inet_interfaces = loopback-only
recipient_delimiter = +

compatibility_level = 2

smtp_sasl_auth_enable = yes
smtp_sasl_password_maps = hash:/etc/postfix/sasl_passwd
smtp_sasl_security_options = noanonymous
smtp_use_tls = yes
smtp_tls_security_level = may
smtp_tls_note_starttls_offer = yes
smtp_tls_CAfile = /etc/ssl/certs/ca-certificates.crt
```

Ilustración 11: Configurar cliente de Postfix para iniciar sesión en el servidor

En el archivo `sasl_passwd` lo que se realizará será asignar la forma en la que se autenticará el servidor web en el de correo, por lo que se incluye el nombre de dominio, el puerto donde hará la conexión para enviar correos, el usuario que usará y la contraseña del usuario.

```
GNU nano 6.2 /etc/postfix/sasl_passwd
[email.server.elhamiti.local]:587 admin@server.elhamiti.local:admin_elhamiti
```

Ilustración 12: Asignación de cuenta para usuario

Lo único que queda es comprobar que se envía el correo y verificar que el correo ha llegado de forma exitosa.

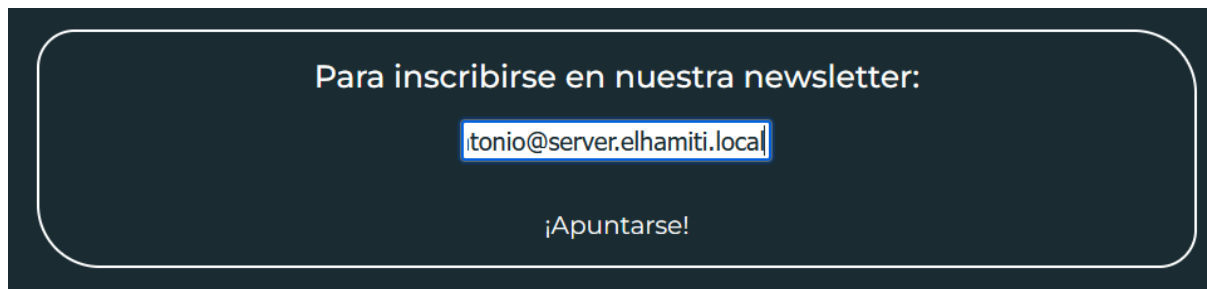


Ilustración 13: Pruebas de envío de correo para la newsletter

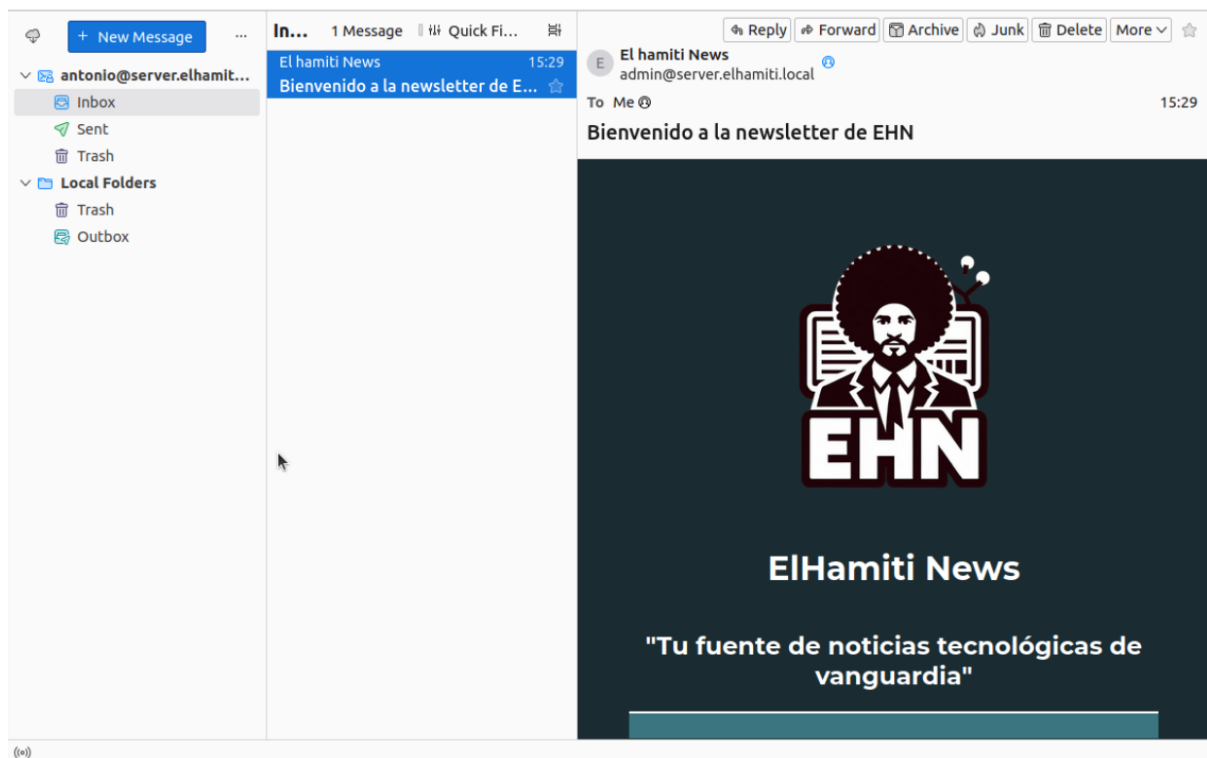


Ilustración 14: Visualización de que ha llegado el correo

1.3. DHCP

Para gestionar la red, se crea un servicio DHCP (Dynamic Host Configuration Protocol) para asignar las IP en la red interna. Se instala el módulo isc-dhcp-server dentro del contenedor que actuará como servidor DHCP y, tras la instalación, se configuran las redes y zonas en /etc/dhcp/dhcpd.conf. La red se divide en cuatro:

- Conexión entre el servidor DHCP y el DHCP Relay (Red 10.5.1.0/24).
- Red para servidores internos (Red 10.5.2.0/24).
- Red DMZ (Red 10.5.3.0/24).
- Red para equipos de trabajo (Red 10.5.4.0/24).

Además de las redes, se asignan IP estáticas a los equipos y servidores mediante la conexión de link de cada puerto. Luego, se configura el equipo como router para acceder al exterior modificando el archivo /etc/sysctl.conf, descomentando la línea para permitir el reenvío de IP e Internet. Se reinicia el servicio para verificar el envío de paquetes IPv4 mediante el comando sysctl -p, y se verifica su funcionamiento con comandos systemctl restart isc-dhcp-server y systemctl status isc-dhcp-server.

Un segundo contenedor actúa como repetidor DHCP (DHCP Relay), con una IP estática en la red 1 (10.5.1.2), y dos interfaces adicionales: eth1 que irá destinada para la red de servidores, con IP 10.5.2.1 y eth2 para la red de trabajadores, que irá con la IP 10.5.4.1. Se instala isc-dhcp-relay y se configuran las interfaces para llevar las IP, con configuraciones que se podrán volver a modificar en /etc/defaults/isc-dhcp-relay y /etc/defaults/isc-dhcp-server, este segundo archivo es en el servidor DHCP. Se reinicia el servicio sysctl para activar el reenvío de IP, y se verifica y reinicia el estado del repetidor DHCP, al igual que se ha hecho en el servidor DHCP.

En Proxmox, se añaden rutas manuales para las redes 10.5.2.0/24 y 10.5.4.0/24 usando el comando ip route en el router principal o servidor DHCP, asegurando que las IP alcancen sus destinos. Para los contenedores ya creados, se asignan IP físicas a través de la interfaz de Proxmox, accediendo a la sección de network y utilizando el comando dhclient eth0 para solicitar una IP, y el comando ip a para verificar la asignación. Se prueba que todas las redes comunican entre sí para poder trabajar con la red.

```
root@BBDD:~# dhclient eth0
root@BBDD:~# 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: eth0@if220: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default qlen 1000
    link/ether bc:24:11:61:d1:00 brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 10.5.2.8/24 brd 10.5.2.255 scope global dynamic eth0
        valid_lft 599sec preferred_lft 599sec
    inet6 fe80::be24:11ff:fe61:d100/64 scope link
        valid_lft forever preferred_lft forever
```

Ilustración 15: IP asignada al equipo de ejemplo

```
root@DHCP:~# ping 10.5.4.1
PING 10.5.4.1 (10.5.4.1) 56(84) bytes of data.
64 bytes from 10.5.4.1: icmp_seq=1 ttl=64 time=0.114 ms
64 bytes from 10.5.4.1: icmp_seq=2 ttl=64 time=0.043 ms
^C
--- 10.5.4.1 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1014ms
rtt min/avg/max/mdev = 0.043/0.078/0.114/0.035 ms
root@DHCP:~# ping 10.5.4.20
PING 10.5.4.20 (10.5.4.20) 56(84) bytes of data.
64 bytes from 10.5.4.20: icmp_seq=1 ttl=63 time=0.093 ms
^C
--- 10.5.4.20 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.093/0.093/0.093/0.000 ms
root@DHCP:~# ping 10.5.2.3
PING 10.5.2.3 (10.5.2.3) 56(84) bytes of data.
64 bytes from 10.5.2.3: icmp_seq=1 ttl=63 time=0.118 ms
64 bytes from 10.5.2.3: icmp_seq=2 ttl=63 time=0.072 ms
^C
--- 10.5.2.3 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1004ms
rtt min/avg/max/mdev = 0.072/0.095/0.118/0.023 ms
root@DHCP:~# ping 10.5.3.2
PING 10.5.3.2 (10.5.3.2) 56(84) bytes of data.
64 bytes from 10.5.3.2: icmp_seq=1 ttl=64 time=0.082 ms
64 bytes from 10.5.3.2: icmp_seq=2 ttl=64 time=0.041 ms
^C
--- 10.5.3.2 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1015ms
rtt min/avg/max/mdev = 0.041/0.061/0.082/0.020 ms
```

Ilustración 16: Comprobación de conexión entre redes

2. Red Privada

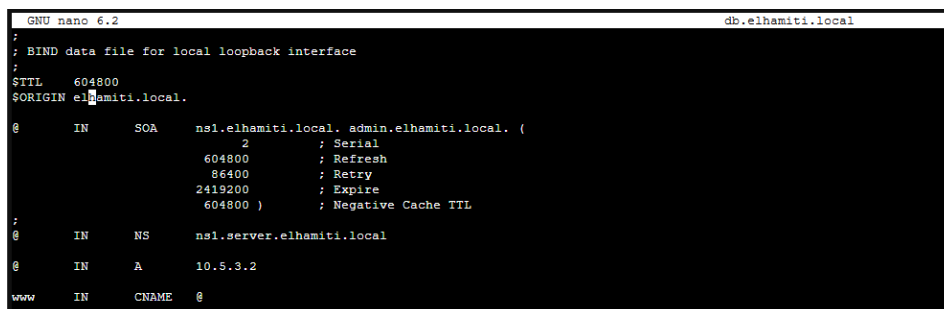
2.1. DNS

Se instala un DNS (Domain Name System) para traducir nombres de dominio en direcciones IP, permitiendo así la navegación en internet mediante nombres legibles para humanos en lugar de direcciones numéricas. Teniendo en cuenta lo anterior, se usará el servidor Bind9 que permite crear el DNS.

Para poder configurar el servidor se necesitan modificar 3 archivos:

- /etc/default/bind9: Aquí se forzará a que se use el formato de IPv4 para asignar el nombre dentro del dominio a la IP.
- /etc/bind9/named.conf.options: En este archivo se busca configurar las opciones básicas que usará el servidor DNS como puede la IP donde escuchará las peticiones DNS el servidor, los equipos que harán de reenviadores, si se permitirá recursividad en el DNS o no, entre otras modificaciones.
- /etc/bind9/named.conf.local: En este archivo se definen las zonas que tendrá la red, la cual como se ha indicado en el DHCP serán 3 (DMZ, red de servidores y red de trabajadores). Además, en este archivo se indica si el tipo de servidor es maestro o esclavo sobre la zona indicada y si es una zona directa o inversa.

Definiendo las zonas que tendrá el servidor, habrá que crear un archivo de zona directa y otro de zona inversa en cada red, para poder hacer resoluciones de cada tipo. El formato que tendrá cada registro se puede ver en las siguientes dos imágenes, donde uno es un ejemplo de zona directa de la DMZ y el segundo es el respectivo archivo de zona inversa.



```
GNU nano 6.2 db.elhamiti.local
;
; BIND data file for local loopback interface
;
$TTL 604800
$ORIGIN elhamiti.local.

@      IN      SOA      ns1.elhamiti.local. admin.elhamiti.local. (
                                2          ; Serial
                                604800     ; Refresh
                                86400      ; Retry
                                2419200    ; Expire
                                604800 )   ; Negative Cache TTL
;
@      IN      NS       ns1.server.elhamiti.local
@      IN      A        10.5.3.2
www    IN      CNAME    @
```

Ilustración 17: Archivo de Zona directa de la DMZ

```
GNU nano 6.2 db.3.5.10
;
; BIND reverse data file for local loopback interface
;
$TTL 604800
$ORIGIN 3.5.10.in-addr.arpa.
@ IN SOA ns1.server.elhamiti.local. admin.elhamiti.local. (
    604800 ; Serial
    604800 ; Refresh
    86400 ; Retry
    2419200 ; Expire
    604800 ) ; Negative Cache TTL
;
@ IN NS ns1.server.elhamiti.local.
2 IN PTR dmz.elhamiti.local.
```

Ilustración 18: Archivo de Zona inversa de la DMZ

Después de crear los seis archivos, se verificará que las zonas no contengan ningún error de sintaxis ni error de registros que no pertenezcan a dicha zona. Se podrá comprobar con los siguientes comando:

- **Named-checkconf:** Permite verificar la sintaxis de los archivos de las zonas.
- **Named-checkzone <zona> <archivo de la zona>:** Permite verificar que todos los registro de la zona se corresponden con la zona.

Como últimos pasos, en primer lugar, simplemente habría que reiniciar el servidor DNS y ver que no haya ningún error de configuración de Bind9, es decir, el status del servidor DNS.

En segundo lugar, se permitirá el registro de paquetes de Bind9 con el servidor DNS y por último, se añadirá el servidor DNS en el servidor DHCP, así como las zonas que tendrá que buscar cada zona DHCP, siendo la asignación de zonas:

- **Red 10.5.3.0/24:** dmz.elhamiti.local
- **Red 10.5.2.0/24:** server.elhamiti.local
- **Red 10.5.4.0/24:** trabajo.elhamiti.local

Finalmente, una vez se ha terminado la configuración completa del servidor DNS, se realizan las comprobaciones para asegurar que todo funciona correctamente.

```
root@WEB:~# resolvectl
Global
  Protocols: -LLMNR -mDNS -DNSOverTLS DNSSEC=no/unsupported
  resolv.conf mode: foreign
  Current DNS Server: 10.5.2.7
  DNS Servers: 10.5.2.7
  DNS Domain: dmz.elhamiti.local

Link 2 (eth0)
  Current Scopes: DNS
  Protocols: +DefaultRoute +LLMNR -mDNS -DNSOverTLS DNSSEC=no/unsupported
  DNS Servers: 10.5.2.7
  DNS Domain: WEB dmz.elhamiti.local
root@WEB:~# ping ldap.server.elhamiti.local
PING ldap.server.elhamiti.local (10.5.2.3) 56(84) bytes of data.
64 bytes from ldap.server.elhamiti.local (10.5.2.3): icmp_seq=1 ttl=62 time=0.095 ms
64 bytes from ldap.server.elhamiti.local (10.5.2.3): icmp_seq=2 ttl=62 time=0.082 ms
^C
--- ldap.server.elhamiti.local ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1020ms
rtt min/avg/max/mdev = 0.082/0.088/0.095/0.006 ms
root@WEB:~# ping dmz.elhamiti.local
PING dmz.elhamiti.local (10.5.3.2) 56(84) bytes of data.
64 bytes from dmz.elhamiti.local (10.5.3.2): icmp_seq=1 ttl=64 time=0.012 ms
64 bytes from dmz.elhamiti.local (10.5.3.2): icmp_seq=2 ttl=64 time=0.021 ms
^C
--- dmz.elhamiti.local ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1010ms
rtt min/avg/max/mdev = 0.012/0.016/0.021/0.004 ms
root@WEB:~# ping clientel.trabajo.elhamiti.local
PING clientel.trabajo.elhamiti.local (10.5.4.19) 56(84) bytes of data.
64 bytes from clientel.trabajo.elhamiti.local (10.5.4.19): icmp_seq=1 ttl=62 time=0.062 ms
64 bytes from clientel.trabajo.elhamiti.local (10.5.4.19): icmp_seq=2 ttl=62 time=0.080 ms
^C
--- clientel.trabajo.elhamiti.local ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1022ms
rtt min/avg/max/mdev = 0.062/0.071/0.080/0.009 ms
```

Ilustración 19: Comprobación de que se ha asignado la zona en un equipo y funciona el servicio DNS

Configuración del DNSSEC

El DNSSEC (Domain Name System Security Extensions) es una extensión del DNS que proporciona una capa extra de seguridad al sistema. Para habilitar el DNSSEC, se configura el archivo `named.conf.options`, y se añade la línea ***dnssec-validation yes***.

A continuación, se crean claves de firma de zona (ZSK) para cada zona. Para ello, se hará uso del comando `dnssec-keygen` con los modificadores:

- **-a:** Permite identificar el tipo de cifrado que usará la clave
- **-b:** La cantidad de bits que usará la clave
- **-n Zone:** Permite firma la zona que vamos a hacer el DNSSEC.

Después de tener creadas las firmas, se ha configurado el archivo `named.conf.local` para cambiar el nombre de los archivos de zona para que reconozca los archivos de zona firmados. Para ello, al final de los archivos firmados se añade la extensión `“.signed”`. Además, hará falta modificar el nombre de dichos archivos para que se reconozcan en el servidor.

Una vez realizados los cambios, se reinicia de nuevo el servidor para que queden guardados. Por último, mediante el comando `dig DNSKEY` se comprueban que las zonas han sido firmadas y con `dig query` se verifica que la respuesta DNS también vaya firmada.

```
root@DNS:/var/cache/bind# dig DNSKEY server.elhamiti.local +multiline
; <<> DiG 9.18.18-Ubuntu0.22.04.2-Ubuntu <<> DNSKEY server.elhamiti.local +multiline
;; global options: +cmd
;; Got answer:
;; WARNING: .local is reserved for Multicast DNS
;; You are currently testing what happens when an mDNS query is leaked to DNS
;; -->HEADER<-- opcode: QUERY, status: NOERROR, id: 24249
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: udp: 1232
; COOKIE: 9e494b7bf4bce7ff0100000663d32b3e95b6b5fe6fb4bd3 (good)
;; QUESTION SECTION:
;server.elhamiti.local. IN DNSKEY

;; ANSWER SECTION:
server.elhamiti.local. 604800 IN DNSKEY 256 3 7 (
AwZARc/sMsB3+teichG2PX1FeKippiVvixhugLWDymn
RA7ndWAmgSh8B0tyVRDVS63Ad3mP7XoDuyW6i9r4uJEwC
xN2ARyYZRtKbaHhA+VZ3CTDg8G3JDOF4+DaWtWaiCv
dR1qgBP1XyYQ4QgX62KuPfnLh7I/vBTcDr5inn1CFow
gVOMG0B/g7o8dPlj+XIBQMgu7J2TEdjfUfVLoj9fv6+A
2el6S012xp1rWkj6H3d8FLXk6ndLi08T/WkiQHV+ZTga
+IPnPSuXme/eW9v8/bm9GfUw7LtgL+WZ/EiXlsofq16P
cLFRSY8jT5eNH8r0sf+1RS1wn16EKj7+wLTezE=
) ; ZSK; alg = NSEC3RSASHA1 ; key id = 53888

;; Query time: 0 msec
;; SERVER: 10.5.2.7#53(10.5.2.7) (UDP)
;; WHEN: Thu May 09 20:31:47 UTC 2024
;; MSG SIZE rcvd: 354
```

Ilustración 20: Zona de servidores firmada

```
aperales@Trabajador1:~$ resolvectl query ldap.server.elhamiti.local
ldap.server.elhamiti.local: 10.5.2.3

-- Information acquired via Protocol DNS in 1.2ms.
-- Data is authenticated: yes; Data was acquired via local or encrypted transport: yes
-- Data from: synthetic
```

Ilustración 21: Confirmación de que la zona está firmada

2.2. Firewall

2.2.1. Router frontera

```

root@DHCP:~# iptables -L -n -v
Chain INPUT (policy DROP 534 packets, 43159 bytes)
  pkts bytes target     prot opt in     out     source               destination
  390 124K ACCEPT     all  --  *      *       0.0.0.0/0            0.0.0.0/0           ctstate RELATED,ESTABLISHED
    0 0 DROP       all  --  *      *       0.0.0.0/0            0.0.0.0/0           ctstate INVALID
    1 84 ACCEPT    icmp  --  *      *       0.0.0.0/0            0.0.0.0/0           icmp-type 8
    0 0 ACCEPT    all  --  lo     *       0.0.0.0/0            0.0.0.0/0
  430 139K ACCEPT   udp   --  *      *       0.0.0.0/0            0.0.0.0/0           multiport dports 67,68

Chain FORWARD (policy DROP 1278 packets, 100K bytes)
  pkts bytes target     prot opt in     out     source               destination
 52979 65M ACCEPT   all  --  *      *       0.0.0.0/0            0.0.0.0/0           ctstate RELATED,ESTABLISHED
    0 0 DROP       all  --  *      *       0.0.0.0/0            0.0.0.0/0           ctstate INVALID
  471 35648 ACCEPT   all  --  *      *       0.0.0.0/0            10.5.3.0/24
  74 4701 ACCEPT   all  --  *      *       10.5.3.0/24          0.0.0.0/0
    4 263 ACCEPT   all  --  *      *       10.5.1.0/24          0.0.0.0/0
 1206 207K ACCEPT   all  --  *      eth0    0.0.0.0/0            0.0.0.0/0
    6 1056 ACCEPT   udp   --  *      *       0.0.0.0/0            10.5.2.5            udp dpt:51820

Chain OUTPUT (policy ACCEPT 3274 packets, 1079K bytes)
  pkts bytes target     prot opt in     out     source               destination
root@DHCP:~# iptables -L -n -v -t nat
Chain PREROUTING (policy ACCEPT 8453 packets, 1239K bytes)
  pkts bytes target     prot opt in     out     source               destination
   33 1796 DNAT     tcp  --  eth0    *       0.0.0.0/0            0.0.0.0/0           multiport dports 80,443 to:10.5.3.2
 5553 751K DNAT     all  --  eth0    *       0.0.0.0/0            0.0.0.0/0           to:10.5.2.5

Chain INPUT (policy ACCEPT 1448 packets, 460K bytes)
  pkts bytes target     prot opt in     out     source               destination
Chain OUTPUT (policy ACCEPT 410 packets, 135K bytes)
  pkts bytes target     prot opt in     out     source               destination
Chain POSTROUTING (policy ACCEPT 9080 packets, 792K bytes)
  pkts bytes target     prot opt in     out     source               destination
 3375 391K MASQUERADE all  --  *      eth0    0.0.0.0/0            0.0.0.0/0

```

Ilustración 22: Reglas de IPTABLES de Router Frontera

En caso del router frontera de forma resumida, lo que se pretende es hacer, por un lado, bloquear los puertos que no se utilicen dentro de este equipo y por otro lado permitir el tráfico de la red (Reglas de Forward) y exponer los servicios como son la web y la VPN corporativa para los administradores (Reglas NAT).

Si se empiezan por las reglas INPUT, con estas lo que se realiza será con una política por defecto a Drop, es decir, rechazar cualquier paquete que no se incluya en las reglas que se indiquen y si se empiezan a desarrollar el resto, sería permitir el tráfico de DHCP (puertos 67,68) que lleguen al DHCP, luego permitir el tráfico de la interfaz de loopback o que va de procesos del propio equipo, y por último dentro de este apartado, permitir que se puedan contestar a las conexiones del comando ping.

Continuando con las reglas de la cadena FORWARD, estas se dividen en tres, la primera sería simplemente poder hacer que llegue todo el tráfico que llegue tanto a la red 10.5.1.0/24 como a la 10.5.3.0/24, debido a que estás interesan para que se lleve el tráfico. La segunda parte, sería permitir el tráfico que llegue por la interfaz eth0, debido a que está será con una regla de la tabla NAT, las cuales permitirá tener Internet en toda la red. Y por último, se encuentra la regla para poder exponer la VPN la cual se especifica con el puerto que usa dicha VPN.

Ya entrando en el apartado de las reglas NAT, se encuentran las reglas PREROUTING, las cuales son reglas que se crean para que se cambie la IP antes de enrutar el paquete a su destino, y las reglas POSTROUTING, las cuales hacen lo mismo que las reglas PREROUTING, pero a la inversa, ya que estas cambian la IP para que después de que se enrute cambie la IP al destino.

2.2.2. Router red privada

Chain FORWARD (policy DROP 1229 packets, 74556 bytes)								
ppts	bytes	target	prot	opt	in	out	source	destination
52632	44M	ACCEPT	all	--	*	*	0.0.0.0/0	0.0.0.0/0
0	0	DROP	all	--	*	*	0.0.0.0/0	0.0.0.0/0
211	64337	ACCEPT	all	--	*	*	0.0.0.0/0	10.5.1.0/24
24	7968	ACCEPT	all	--	*	*	10.5.1.0/24	0.0.0.0/0
8858	2018K	ACCEPT	all	--	*	*	10.5.2.0/24	0.0.0.0/0
16	16711	ACCEPT	tcp	--	*	*	10.5.3.2	10.5.2.4
32	2115	ACCEPT	udp	--	*	*	10.5.3.2	10.5.2.7
146	10430	ACCEPT	tcp	--	*	*	10.5.3.2	10.5.2.8
8251	726K	ACCEPT	all	--	*	*	10.5.4.0/24	10.5.2.0/24
5	880	ACCEPT	udp	--	*	*	0.0.0.0/0	10.5.2.5
54	7215	ACCEPT	all	--	*	*	10.5.4.0/24	0.0.0.0/0
0	0	ACCEPT	all	--	*	*	0.0.0.0/0	10.5.4.0/24

En el servidor DHCP relay se encuentran las conexiones internas dentro de la red, entre ellas, se pueden dividir en 3 grande fases.

La primera fase, se ubica permitir el tráfico entre las red, en este caso se permite el tráfico total entre las redes 10.5.1.0/24, 10.5.2.0/24, 10.5.4.0/24. Cabe aclarar, que dentro de este apartado, se permitirá tanto el tráfico de entrada con la opción -d en la regla de IPTABLES a dicha red, como el tráfico de salida con la opción -s.

Después, como segunda parte, se permite el tráfico desde la red que se expondrá (DMZ) a diferentes puertos internos para que se puedan cumplir diferentes funciones de la web. En primer lugar, permite el tráfico desde la IP del servidor web (10.5.3.2) a la IP del servidor de correo (10.5.2.4) por el puerto 587, que es el que usa para conexión SMTP. En segundo lugar, se realiza lo mismo, pero esta vez a la IP del servidor DNS (10.5.2.7) cambiando el puerto al 53 y el protocolo UDP, debido a que es el que usa DNS para comunicarse y dar la resolución de nombres. En tercer lugar, se gestiona la base de datos de la web comunicándose por el puerto 3306 (MySQL) y la IP del servidor de base de datos (10.5.2.8).

La tercera parte y cierre de las reglas empleadas para la red, ubicar la regla para exponer la VPN en la IP 10.5.2.5 por el puerto de destino 51820, que es el que emplea Wireguard en este caso, mediante el protocolo UDP.

Al igual que se ha hecho en el servidor DHCP, se han cerrado los puertos de INPUT, por lo que sería decir lo mismo. Además, se incluyen las reglas para permitir el tráfico ya existente o nuevo relacionado a conexiones anteriores y bloquear el inválido.

2.3. Proxy

Un proxy es un servidor que actúa como intermediario entre el usuario y el destino final en internet. Oculta la dirección IP original del usuario y en su lugar envía las solicitudes utilizando su propia dirección IP. Esto mejora la seguridad y la privacidad en línea, puede permitir el acceso a contenido bloqueado geográficamente, controlar el acceso a internet, y optimizar el rendimiento de la red. Para crear el servidor se instala el programa Squid.

Se accede al archivo para modificar los datos de configuración (/etc/squid/squid.conf). Se configuran los diferentes parámetros del archivo para el servidor Squid. Entre los ajustes que se modificarán en este archivo están el puerto que usará el proxy, la memoria cache que guardará el dominio o donde se guardarán los logs de Squid.

A continuación, se crea el archivo para generar la ACL con los datos permitidos y los no permitidos en el archivo /etc/squid/conf.d/elhamitinews.conf. En este caso, se generará una ACL para las IP permitidas para navegar por Internet, el contenido prohibido que no se buscará y si se requerirá contraseña para iniciar sesión en proxy.

Una vez creados todos los archivos, se reinicia el servidor para guardar todos los cambios y revisar el estado del proxy para que no haya ningún error de sintaxis.

Después de configurar los aspectos básicos del proxy, se realizará la autenticación de usuarios y para ello se configura el archivo para que se registren los usuarios y claves de Squid en el archivo /etc/squid/squid.conf, y además se instala el paquete apache2 utils para crear las contraseñas y los usuarios. Para poder crear las contraseñas y usuarios del proxy se hará uso del comando htpasswd con el modificador -c que permite indicar que se cree un nuevo archivo de contraseñas con la ruta que se le dará.

Finalmente se configurará el proxy en el cliente y se harán las comprobaciones de que el proxy realiza correctamente los bloqueos del contenido.

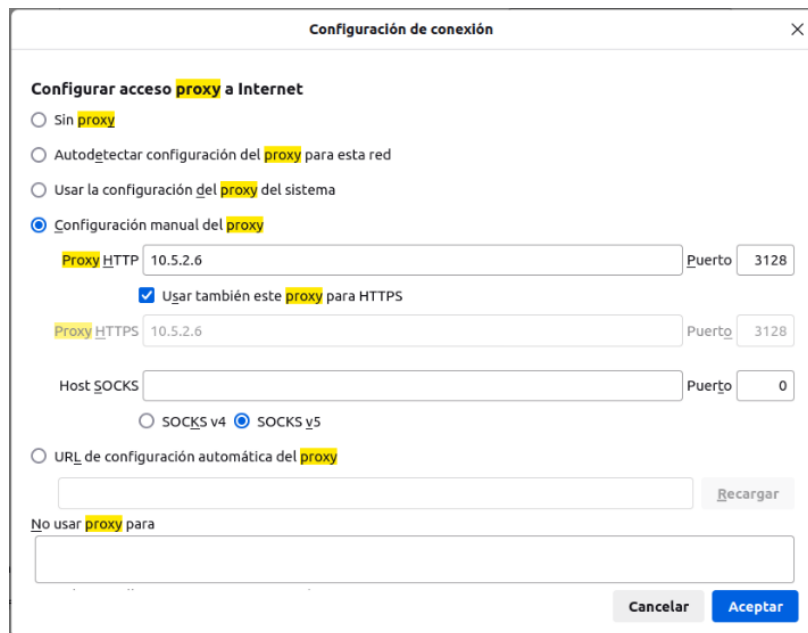


Ilustración 24: Asignación del proxy a un equipo de forma manual



Ilustración 25: Acceso con un usuario creado para poder navegar por Internet



Ilustración 26: Comprobación de dominio bloqueado

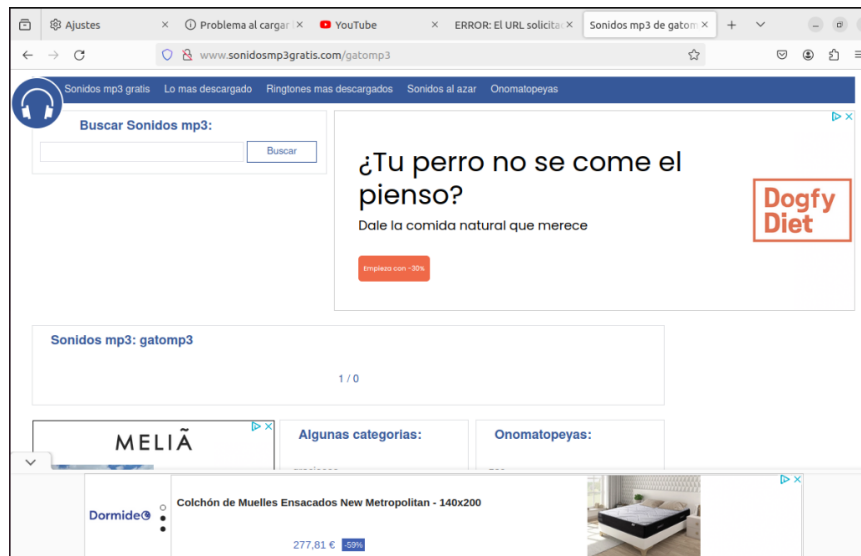


Ilustración 27: Comprobación de dominio no bloqueado ni por extensión ni por dominios

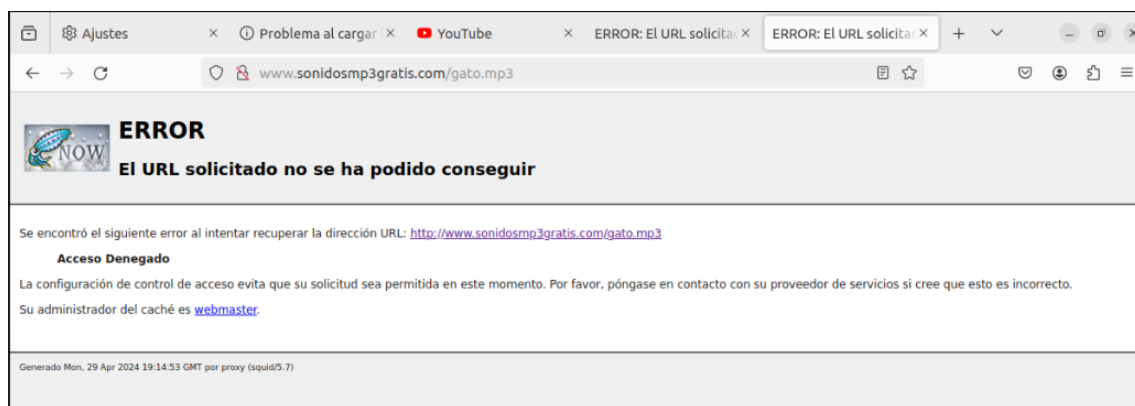


Ilustración 28: Bloqueo de descarga de un archivo con una extensión no permitida



Ilustración 29: Comprobación de una palabra de búsqueda bloqueada

2.4. Correo

2.4.1. Postfix

Se instala Postfix debido a que es un servicio que cumple con las necesidades del proyecto para emplearlo como MTA y MDA, los cuales son agentes de correo tanto de reenvío como de transporte de correo. Para ello, se configura las opciones que se piden como son el dominio, contraseña de la base de datos y el nombre del dominio de este servidor.

Se establece un nombre de dominio en el archivo `/etc/postfix/virtual_mailbox_domains` y con el comando `postmap` se actualiza las tablas de mapeo de `postmap`. Las tablas de mapeo en Postfix son estructuras de datos utilizadas para almacenar y buscar información de manera eficiente. Estas tablas permiten realizar tareas como alias de correo, reescritura de direcciones, controles de acceso y otras funciones relacionadas con la gestión del correo electrónico.

El archivo `master.cf` en Postfix es el archivo de configuración principal que define cómo se inician y administran los diversos servicios que Postfix ofrece. Este archivo especifica los componentes y servicios de Postfix, como los servicios de entrega de correo, los servicios de recolección de correos entrantes, los filtros de contenido, entre otros. En este archivo será importante activar el envío de paquete por el método `Submission` por TLS.

En el archivo de configuración general o `/etc/postfix/main.cf` se configurará todos los parámetros necesarios para que Postfix pueda tanto enviar correos verificándolos por TLS, vincular la base de datos de Dovecot con Postfix para validar los correos que se envían a este servidor desde los usuarios de Dovecot, y por último, alojar la base de datos interna que cargará todos los correos que se envíen desde este servidor. Además, validar el nombre de dominio de servidor empleado en el archivo `/etc/postfix/virtual_mailbox_domains` e identificar su propio nombre de dominio.

2.4.2. Dovecot

Estas configuraciones permiten a Dovecot manejar múltiples servicios de manera eficiente y segura, estableciendo cómo se aceptan y gestionan las conexiones, y cómo interactúan los diferentes componentes del sistema de correo. Para ello se acude al archivo `/etc/dovecot/10-mail.conf`, donde se identificará la carpeta donde se guardarán los correos de cada usuario.

La configuración precisa de `10-master.conf` es fundamental para el correcto funcionamiento y rendimiento del servidor de correo asignado los puertos de escucha del servidor y los permisos con el usuario que se usará para Postfix, que será el que se ha creado al instalarlo.

En el archivo `10-auth.conf` en Dovecot se utiliza para configurar el subsistema de autenticación del servidor de correo. Este archivo contiene diversas opciones que determinan cómo se manejan los procesos de autenticación, qué métodos están permitidos y cómo se configuran las bases de datos de usuarios y contraseñas.

Por último, en el archivo `10-ssl.conf` en Dovecot es una configuración específica para manejar las opciones relacionadas con SSL/TLS. Dovecot es un servidor de correo IMAP y POP3 que permite a los usuarios acceder a su correo de manera segura, y el archivo `10-ssl.conf` se utiliza para definir cómo se deben manejar las conexiones seguras.

Se crean usuarios con los que se podrá acceder a Dovecot desde Roundcube, dado que estos se asignarán en el archivo correspondiente de Roundcube.



```
GNU nano 6.2 /etc/dovecot/dovecot-users
admin@server.elhamiti.local:admin_elhamiti
antonio@server.elhamiti.local:1234
josias@server.elhamiti.local:8432
alfonso@server.elhamiti.local:Qwerty.98
felipe@server.elhamiti.local:Viva_elRealMadrid
```

Ilustración 30: Usuarios de Dovecot

2.4.3. Certificados

Para poder usar el modo de autenticación SSL/TLS se verifican que los certificados y claves estén en la carpeta correspondiente, siendo éstas:

- **/var/www/certs:** Para los certificados que se emplean para la configuración de Dovecot y Postfix.
- **/usr/local/share/ca-certificates:** Para la CA raíz que validará la firma de los certificados de Dovecot y Postfix.
- **/root/ca:** Donde se crean originalmente los certificados para ser empleados en Dovecot y Postfix.

2.4.4. Roundcube

En Roundcube hay que modificar tres archivos principalmente para que funcione correctamente y se pueda acceder al correo que se usará.

En primer lugar, se modificará el VirtualHost ya creado añadiendo la línea de alias que permite buscar la página web en base a la dirección o alias que se le ponga a la ruta a la que va a hacer referencia, es decir, si se tiene que los archivos de configuración de Roundcube están en /usr/share/Roundcube, se puede poner que al buscar /mail acceda a dichos archivos de Roundcube y los muestre al cliente

En segundo lugar, hay que modificar el archivo /etc/Roundcube/config.inc.php, dentro de este archivo se incluirán parámetros del protocolo SMTP e IMAP, tales como el puerto que empleará o el equipo que servirá como servidor de correo.

En tercer lugar, en el archivo /etc/Roundcube/defaults.inc.conf se configurarán los parámetros principales que se usarán en el servidor de correo cuando se conecte el cliente. Dentro de este encontramos el default_host y el default_port que se usará para IMAP, el certificado empleado para validar el acceso por TLS al host de correo y por último, el puerto y el puerto para SMTP.

Por último, se verifica que todo funcione y se manda un correo desde la cuenta de `admin@server.elhamiti.local` a ella misma.

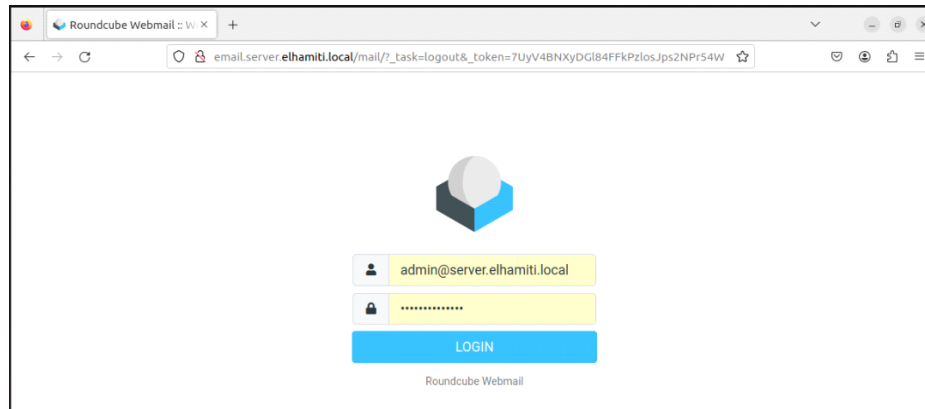


Ilustración 31: Inicio de sesión en Roundcube

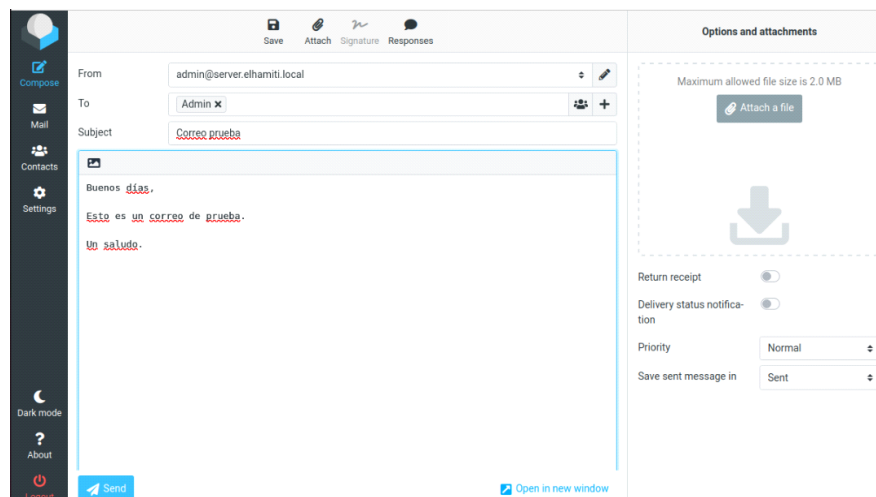


Ilustración 32: Enviar el correo a la cuenta para verificar que funciona

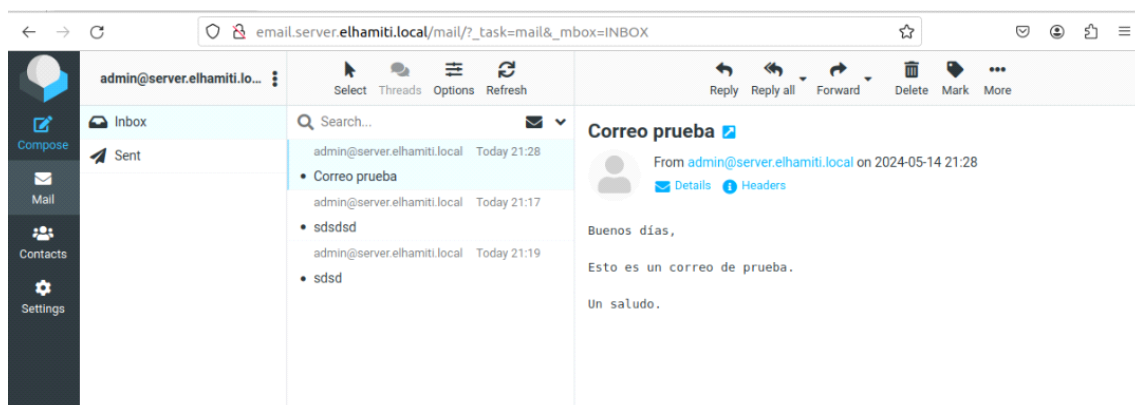


Ilustración 33: Comprobar que ha llegado el correo perfectamente

2.5. VPN

Se instalar el módulo de Wireguard que es una VPN (Virtual Private Network), que a diferencia de OpenVPN no necesita tanta configuración. Para instalar Wireguard lo que se tiene que hacer es ejecutar el comando `apt install Wireguard` con permisos de administrador.

Después de ejecutar el comando de instalación de Wireguard, hay que irse al archivo de `/etc/sysctl.conf` para que se permita el envío de paquete IPv4 y reiniciar el reenvío con el comando `sysctl -p`.

Se generarán los pares de claves públicas y privadas tanto para el servidor como para el cliente, para ello, se utilizarán los comandos `'wg genkey'` y `'wg pubkey'`

Ya teniendo las claves, hay que crear el archivo de configuración del servidor. Para ello, lo primero será crear la interfaz de servidor VPN. En esta interfaz se incluirán la IP del servidor, si se aplicará o no la configuración cuando se guarde algo, entre otras cosas. Además, hay que indicar las reglas de IPTABLES a usar para cuando la conexión se enciende y cuando se apaga. En cuanto al cliente simplemente se pondrá su clave pública, la IP que puede coger el cliente y por último, cuáles son las IP que van a permitirse para tener conexión con la VPN, además del puerto que va a usar.

Ya habiendo configurado hay que irse al cliente, donde al igual que en el servidor se instala Wireguard de la misma forma. Luego de que se instale Wireguard, hay que asistir a la ruta `/etc/wireguard` donde se encuentran todos los archivos de la aplicación, aquí se crea el archivo de configuración del cliente. En este archivo simplemente se tendrá que poner la clave privada del cliente y la pública del servidor. Además, se incluirán las IP de enlace al servidor VPN y la IP que tomará el cliente cuando se conecte a la VPN. Por último, se pondrán todas las ip que permite conectarse el servidor y la IP del servidor DNS que se ha creado para la asignación de nombres del dominio.

Mediante el uso del comando `wg-quick up wgX` se levanta la conexión tanto en el cliente como en el servidor para habilitar la interfaz de VPN y se comprueba que tanto en cliente como servidor se ha levantado la interfaz.

```
4: wg0: <POINTOPOINT,NOARP,UP,LOWER_UP> mtu 1420 qdisc noqueue state UNKNOWN group default qlen 1000
    link/none
    inet 10.0.0.1/32 scope global wg0
        valid_lft forever preferred_lft forever
```

Ilustración 34: Interfaz wg0 en el servidor

```
15: wg0: <POINTOPOINT,NOARP,UP,LOWER_UP> mtu 1420 qdisc noqueue state UNKNOWN group default qlen 1000
    link/none
    inet 10.0.0.2/24 scope global wg0
        valid_lft forever preferred_lft forever
```

Ilustración 35: Interfaz wg0 en el cliente

Además en el caso del cliente se observa como la interfaz wg0 tiene asignado el servidor DNS en el resolver.

```
root@Usuario:/etc/wireguard# resolvectl
Global
    Protocols: -LLMNR -mDNS -DNSoverTLS DNSSEC=no/unsupported
    resolv.conf mode: foreign
    Current DNS Server: 10.5.2.7
    DNS Servers: 10.5.2.7
    DNS Domain: home
```

Ilustración 36: DNS asignado por la interfaz wg0

Únicamente quedaría comprobar que el cliente tiene conexión al servidor y que se resuelven los nombres del dominio. Pero hay que aclarar que para poder hacer que tengan conexión tanto cliente como servidor hay que ver el apartado de 3.2 donde se explica el cortafuego en detalle y las reglas que se hay que poner para poder hacer la conexión.

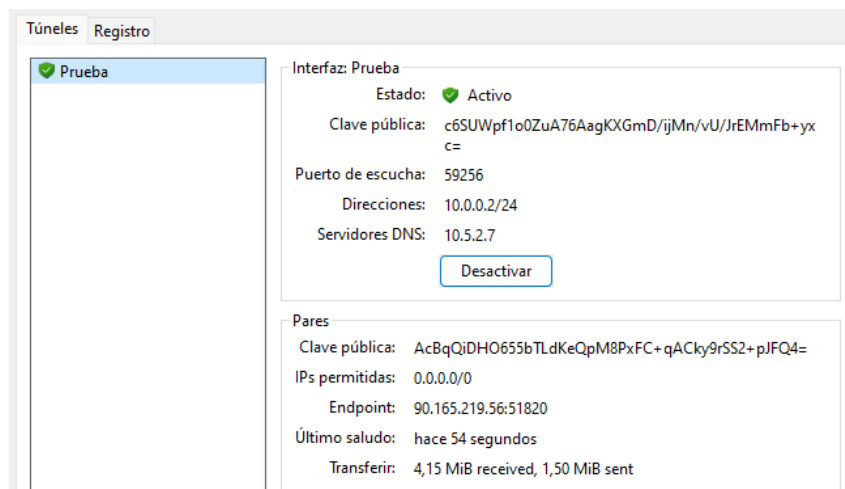


Ilustración 37: Conexión VPN con host fuera de la red

```
root@Usuario:/home/usuario# ping 10.5.1.1
PING 10.5.1.1 (10.5.1.1) 56(84) bytes of data.
64 bytes from 10.5.1.1: icmp_seq=1 ttl=62 time=0.405 ms
64 bytes from 10.5.1.1: icmp_seq=2 ttl=62 time=0.494 ms
64 bytes from 10.5.1.1: icmp_seq=3 ttl=62 time=0.449 ms
^C
--- 10.5.1.1 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2051ms
rtt min/avg/max/mdev = 0.405/0.449/0.494/0.036 ms
```

Ilustración 38: Comprobaciones de conexión sin DNS

```
> ping dmz.elhamiti.local

Haciendo ping a dmz.elhamiti.local [10.5.3.2] con 32 bytes de datos:
Respuesta desde 10.5.3.2: bytes=32 tiempo=5ms TTL=61
Respuesta desde 10.5.3.2: bytes=32 tiempo=7ms TTL=61
Respuesta desde 10.5.3.2: bytes=32 tiempo=7ms TTL=61

Estadísticas de ping para 10.5.3.2:
    Paquetes: enviados = 3, recibidos = 3, perdidos = 0
            (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 5ms, Máximo = 7ms, Media = 6ms
```

Ilustración 39: Comprobación de conexión con DNS

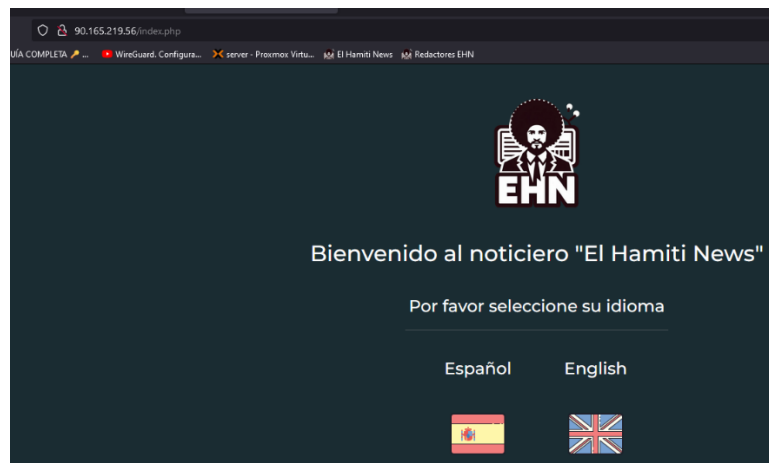


Ilustración 40: Comprobación de que se tiene Internet con la VPN

2.6. LDAP

Para configurar LDAP (Lightweight Directory Access Protocol), primero se instala el software slapd y ldap-utils. Slapd es el daemon que ofrece servicios de directorio, y ldap-utils es un conjunto de herramientas para realizar operaciones comunes con LDAP.

Configuración del dominio en slapd, para ello, se indica el dominio que empleará, el usuario root del dominio y la contraseña de dicho usuario.

El fichero nsswitch.conf sirve para establecer como y en qué orden se debe de buscar la información en el sistema. En este caso, se establece que las contraseñas deben ser buscadas en archivos locales primero (/etc/passwd) y después, en caso de no encontrarse en el passwd, buscas en configuraciones de LDAP.

La resolución de nombres de usuario (libnss) y para la autenticación de usuarios (libpam) serán usados para poder iniciar sesión en los ordenador de los trabajadores.

Con el comando “sudo dpkg-reconfigure ldap-auth-config” se configura el proceso de autenticación en LDAP, el servidor, la cuenta root y su contraseña. Tras ello, se verifica y reinicia el servicio LDAP.

Después de configurar LDAP en el sistema, se puede usar LDAP Account Manager (LAM) para administrar las cuentas de LDAP de manera más sencilla y eficiente. LDAP Account Manager es una herramienta web que proporciona una interfaz gráfica para gestionar entradas LDAP, facilitando la administración de usuarios, grupos y otros datos almacenados en servidor LDAP.

En el archivo ou.ldif, se configuran las diferentes unidades organizativas del dominio. dn es un identificador único para la entrada indica la ubicación en el árbol de LDAP, objectClass top indica que todo el resto de unidades dependerán de esta, y el ou es el nombre.

Un archivo grp.ldif típicamente contiene entradas para uno o más grupos, especificando atributos como el nombre del grupo, la lista de miembros, y otras características relevantes.

El archivo usr.ldif se usa para definir la estructura de los usuarios. Los usuarios en LDAP son entradas que representan a personas o entidades que tienen atributos asociados, como nombres, identificadores, contraseñas, y otros datos personales o de acceso.

Teniendo gestionado el servidor se instala el software de LDAP para configuración, autenticación y herramientas de gestión de LDAP igual que se ha realizado en el servidor. Una vez configurado esto, se podrá acceder vía web para gestionar el directorio del servidor LDAP. Dentro de esta página web podremos:

- **Establecer el árbol del dominio** con el que se trabajará el cual será dc=server, dc=elhamiti, dc=local.
- **Establecer el usuario root** para poder iniciar sesión en la web que será el mismo que para el dominio, pero hay que añadir en el inicio cn=admin, que servirá para identificar el usuario.
- Por último, **establecer la UO (Unidad Organizativa)** de inicio para los usuarios y grupos del dominio.

En la siguiente imagen se pueden observar el árbol del dominio y su jerarquía. Además, los usuarios y grupos del dominio que se crearán, uno por trabajador.

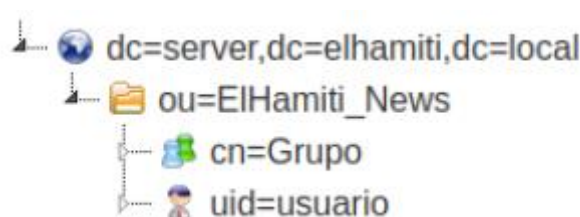


Ilustración 41: Árbol de LDAP tras crear por terminal la UO, el grupo y el usuario

Actions	User name	First name	Last name	UID number	GID number
Sort sequence	▼▲	▼▲	▼▲	▼▲	▼▲
<input type="checkbox"/> Filter ▼					
<input type="checkbox"/>	achicoma	Alfonso	Chicoma	10002	10002
<input type="checkbox"/>	aperales	Antonio	Perales	10000	10001
<input type="checkbox"/>	fgimenez	Felipe	Gimenez	10003	10002
<input type="checkbox"/>	jgonzalez	Josias	Gonzalez	10001	10002
<input type="checkbox"/>	usuario	usuario	Worker	2000	10000

Ilustración 42: Usuarios de LDAP que se usarán

Actions	Group name	GID number	Group members	Group description
Sort sequence	▼▲	▼▲	▼▲	▼▲
<input type="checkbox"/> Filter ▼				
<input type="checkbox"/>	Admin Group	10002	aperales	
<input type="checkbox"/>	aperales	10001		
<input type="checkbox"/>	Grupo	10000		
<input type="checkbox"/>	Local Users	10003	achicoma; fgimenez; jgonzalez	

Ilustración 43: Grupos de LDAP que se usarán

Después de configurar los grupos y usuarios, se modificarán tres archivos importantes para el funcionamiento del LDAP en el cliente:

- **nsswitch.conf:** establece el orden de búsqueda para los usuarios, grupos y sus configuraciones.
- **/etc/pam.d/common-password:** especifica los módulos PAM que deben ser utilizados para gestionar la autenticación de contraseñas.
- **/etc/pam.d/common-session:** define los módulos que se utilizan para gestionar la actividad de un usuario y establece como se debe configurar el directorio /home de los usuarios.

Nslcd es un daemon que se utiliza para conectar un sistema operativo basado en Unix o Linux a un directorio LDAP con el objetivo de añadir los usuarios al directorio. Tras esto se observa que los usuarios del dominio se vincularon con el equipo.

```
usuario:*:2000:10000:usuario:/home/usuario:/bin/bash
aperales:*:10000:10001:Antonio Perales:/home/aperales:/bin/bash
jgonzalez:*:10001:10002:Josias Gonzalez:/home/jgonzalez:/bin/bash
achicoma:*:10002:10002:Alfonso Chicoma:/home/achicoma:/bin/bash
fgimenez:*:10003:10002:Felipe Gimenez:/home/fgimenez:/bin/bash
```

Ilustración 44: Usuarios vinculados con el nuevo equipo

Dependiendo del usuario se agenciaran permisos de root o no y se probará con dicho usuario a iniciar cualquier comando con sudo, que se usa para obtener permisos de root.

```
root@Trabajador1:/home/trabajador1# sudo su - aperales
aperales@Trabajador1:~$ sudo apt update
[sudo] password for aperales:
Get:1 http://security.ubuntu.com/ubuntu jammy-security InRelease [110 kB]
Hit:2 http://es.archive.ubuntu.com/ubuntu jammy InRelease
Get:3 http://es.archive.ubuntu.com/ubuntu jammy-updates InRelease [119 kB]
Hit:4 http://es.archive.ubuntu.com/ubuntu jammy-backports InRelease
Get:5 http://es.archive.ubuntu.com/ubuntu jammy-updates/main amd64 Packages [1.678 kB]
Fetched 1.907 kB in 2s (994 kB/s)
Reading package lists... Done
```

Ilustración 45: Demostración que los usuarios tienen permisos de Root

Por último, se comprueba el iniciar de sesión con los diferentes usuarios que se han creado, junto a los directorios home de cada usuario.

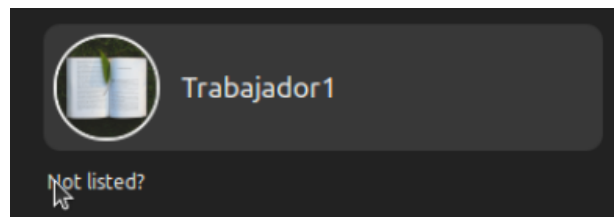


Ilustración 46: Dar a Not Listed para que se pueda iniciar sesión con otro usuario

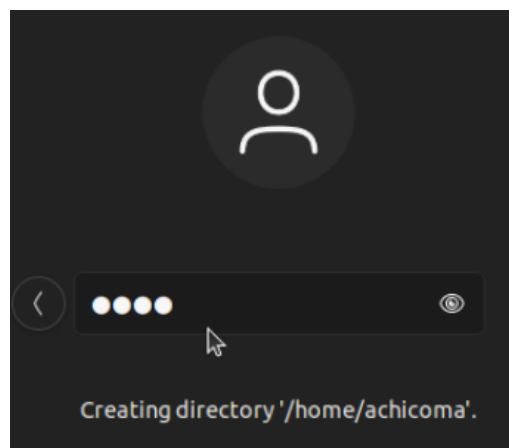


Ilustración 47: Inicio de sesión y creación del directorio Home del nuevo usuario

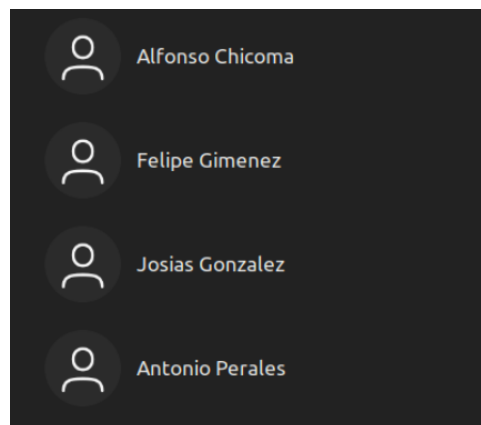


Ilustración 48: Iniciado sesión con todos los usuarios que se deseé del LDAP

```
aperales@Trabajador1:~$ ls /home
achicoma aperales fgimenez jgonzalez trabajador1 usuario
```

Ilustración 49: Demostración de que se han creado todos los directorios Home

2.7. SIEM

Como último punto del trabajo se construye un SIEM. Un SIEM (Service Information and Event Manager) es un equipo que permite monitorear desde un servidor hasta una red entera con el fin de detectar los eventos que ocurran en dichos equipos.

En este trabajo, el servidor SIEM se va a construir con Elasticsearch, Kibana, nginx, Logstash y Filebeat. Se empezará a descargar mediante curl el paquete de configuración de Elasticsearch, dado que este paquete no es nativo del propio Linux, además, se firmará el documento para que tenga validez y no rechace la conexión al querer visualizar el SIEM.

Se instala el paquete de Elasticsearch y dentro de la configuración hay que hacer 3 cosas:

- En el archivo `/etc/elasticsearch/elasticsearch.yml` se configura el `network.host` para que sea el `localhost`, evitando que se exponga el servidor de elasticsearch directamente, debido al que se expondrá será Logstash.
- Con `systemctl start/enable` hay que habilitar el servicio de Elasticsearch.
- Con `curl -X GET` se ven los datos del servidor de Elasticsearch y como son sus datos predefinidos.

A continuación, se instala Kibana y se configura el usuario admin de Kibana. Para poder configuración el usuario se hará mediante el comando `echo` y se firmará con el módulo de OpenSSL. Además, se lleva el comando con el comando `tee` a un archivo donde se configurarán los usuarios de nginx.

Anteriormente, hay que tener descargado nginx para poder crear el VirtualHost del SIEM. Cuando se descargue, en el VirtualHost configuraremos el nombre del equipo en el dominio, además de configurar un proxy inverso, debido a que Kibana actúa en localhost, por lo que para exponerlo se necesitará poner unas reglas especiales como pueden ser las cabeceras del proxy, la caché que tendrá, las conexiones que aceptará y donde se va a crear el proxy.

Se habilitará el VirtualHost y se verifica que la sintaxis sea correcta. Se reinicia el servicio de nginx y se permite el uso de nginx con el cortafuegos de UFW.

Después de configurar los anteriores paquetes, se instala Logstash que será el servidor que se usará para exponerlo y así aceptar todos los paquetes que llevará a Elasticsearch. Dentro de este módulo se configuran dos archivos:

- `/etc/logstash/conf.d/02-beats-input.conf`: En este archivo se especificará el puerto por el que va a escuchar el servicio. Además, el servicio que se usará es beat.
- `/etc/logstash/conf.d/30-elasticsearch-output.conf`: En este archivo al contrario que en el anterior, se especificarán los puertos y hosts a los que va a enviar los paquetes, es decir, va a mandar los paquetes de beat a Elasticsearch mediante localhost y el puerto de Elasticsearch.

Se habilita el servicio con `systemctl start logstash` y como último paquete a descargar será Filebeat. Este módulo se configurará en cada equipo dentro de la red interna para que se envíen logs al SIEM.

Para ello se acudirá al archivo `/etc/filebeat/filebeat.yml` y aquí se configurarán:

- Id: El ID del equipo que mandará los logs
- Habilitar el envío de los logs
- Cambiar el tipo de log que se envía de tipo `filestream` a `log`.
- Poner las rutas de los logs que se enviarán.
- Y por último, comentar el output de Elasticsearch y quitar el comentario del de Logstash, además de poner el host donde se van a enviar los logs.

Se habilita el módulo de System para filebeat y se configura en la ruta `/etc/filebeat/modules.d/system.conf` las rutas de los logs de System y `auth.log`, además, de activar su envío.

Por último, se analizarán los paquete que se envíen desde Filebeat a Elasticsearch mediante el módulo system. Además, de cargar la plantilla que se usará para enviar los paquetes y ver los dashboards que contendrá el filebeat de Kibana. Tras todo esto, se arranca el servicio.

Ya solo quedaría ir al navegador buscar la interfaz de Elastic y visualizar que se envían los logs.

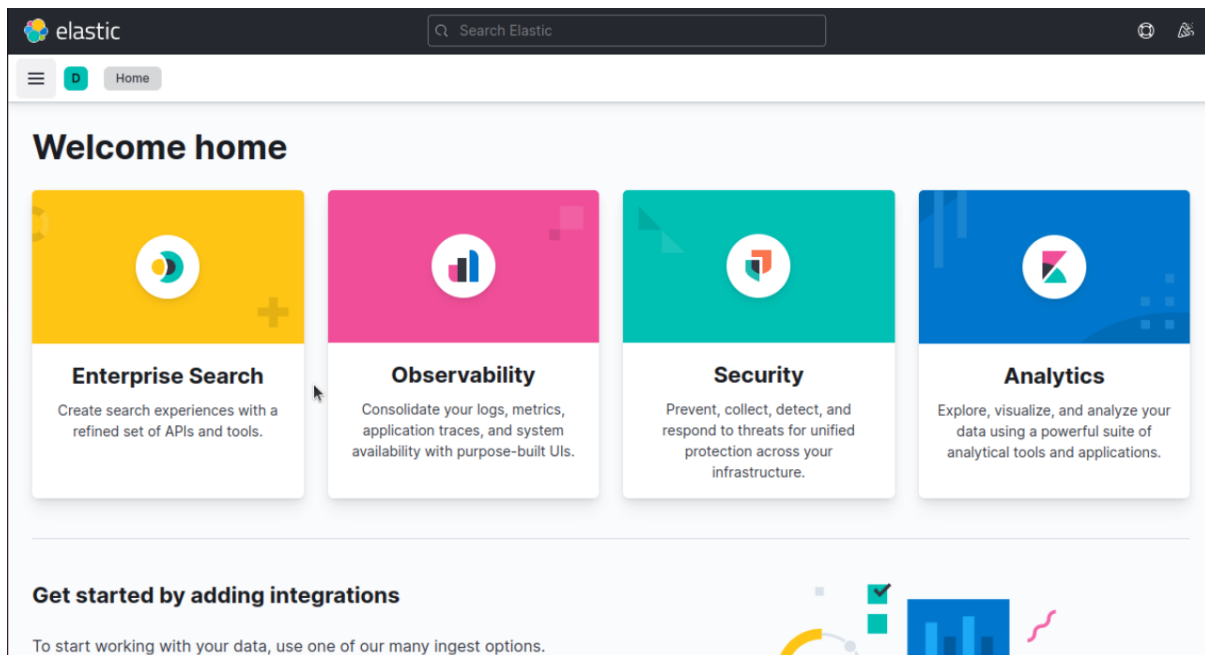


Ilustración 50: Home de Elastic

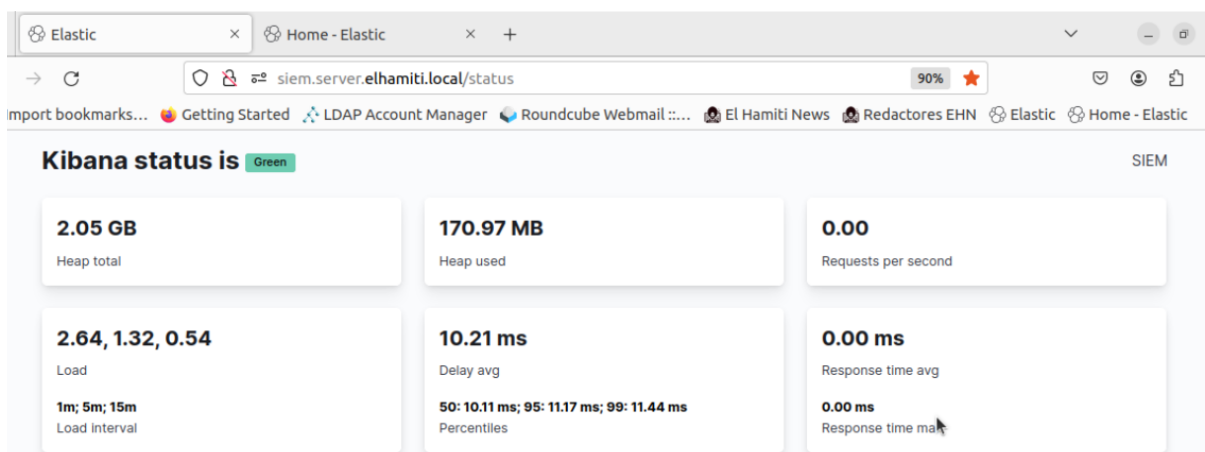


Ilustración 51: Estado del SIEM

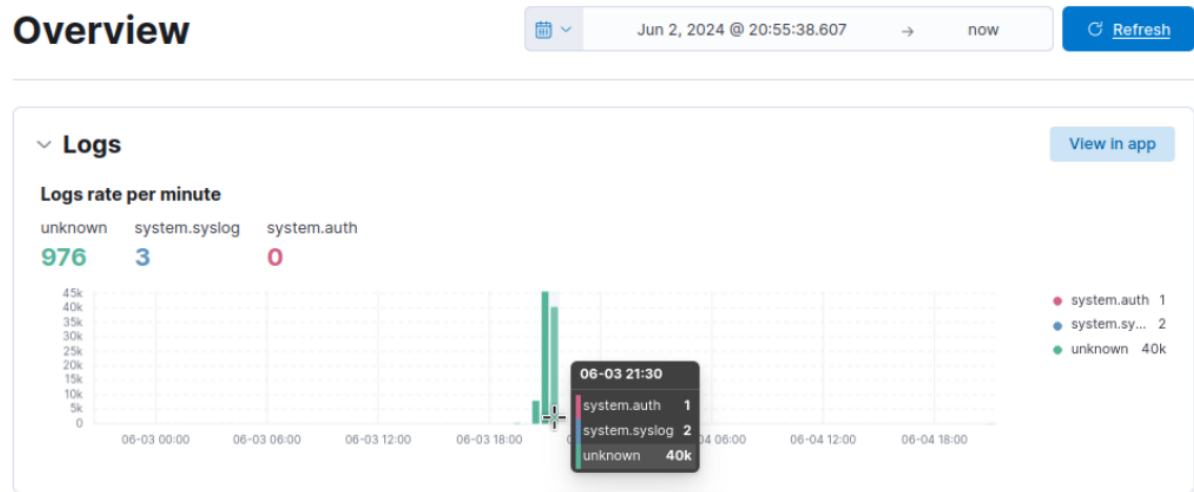


Ilustración 52: Logs registrados hasta ahora

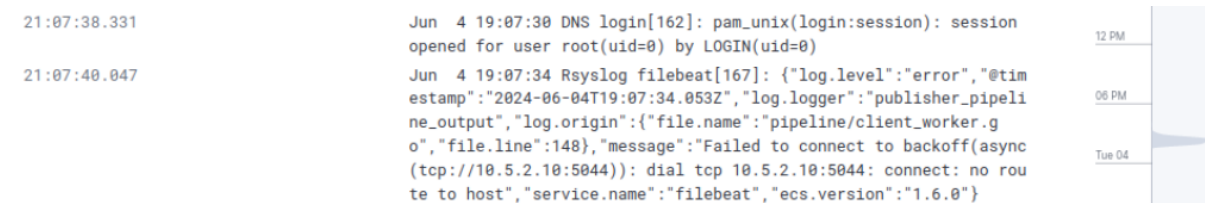


Ilustración 53: Ejemplos de logs

2.8. Base de datos

Para poder vincular página web con PHP se emplea un servidor de base de datos, donde contendrá las noticias, las secciones de las noticias y los usuarios que tienen acceso como administradores de la web y así crear noticias.

Dentro de la tabla de noticias se incluirá un apartado de inglés y otro en español, para poder traducir la noticia. Además, se añadirá la fecha de publicación, la imagen referente a la noticia y el id de la sección a la que pertenecerá dicha noticia. Por último, el título de la noticia aparecerá en inglés o español en función del idioma elegido. Toda noticia va identificada por una ID.

En la tabla de secciones se encontrará el ID de la sección y el nombre de la sección tanto en inglés como en español.

Y por último, en la tabla de redactores se gestionarán con un ID, el nombre del usuario y la contraseña los usuarios que podrán iniciar sesión en la API creada para poder crear noticias como administradores.

Para poder vincular la base de datos se ha descargado tanto en los servidores de base de datos como en el servidor web el módulo de cliente y servidor de MySQL. Además, se ha creado una base de datos y un usuario específico con todos los privilegios sobre esta base de datos para que se pueda gestionar la web de noticias.

```
mysql> select user,host From mysql.user where user="elhamiti_news";
+-----+-----+
| user      | host                |
+-----+-----+
| elhamiti_news | dmz.elhamiti.local |
+-----+-----+
1 row in set (0.00 sec)

mysql> SHOW GRANTS FOR 'elhamiti_news'@'dmz.elhamiti.local';
+-----+-----+
| Grants for elhamiti_news@dmz.elhamiti.local |
+-----+-----+
| GRANT USAGE ON *.* TO `elhamiti_news`@`dmz.elhamiti.local` |
| GRANT ALL PRIVILEGES ON `elhamiti_news`.* TO `elhamiti_news`@`dmz.elhamiti.local` |
| GRANT SELECT ON `mysql`.`user` TO `elhamiti_news`@`dmz.elhamiti.local` |
+-----+-----+
3 rows in set (0.00 sec)

mysql> show databases;
+-----+
| Database |
+-----+
| elhamiti_news |
| information_schema |
| mysql |
| performance_schema |
| sys |
+-----+
5 rows in set (0.00 sec)
```

Ilustración 54: Usuario, privilegios del usuario y la base de datos creada

```
database changed
mysql> show tables;
+-----+
| Tables in elhamiti_news |
+-----+
| Noticias                |
| Secciones               |
| redactores              |
+-----+
3 rows in set (0.00 sec)

mysql> describe Noticias;
+-----+-----+-----+-----+-----+-----+
| Field                | Type      | Null | Key | Default | Extra      |
+-----+-----+-----+-----+-----+-----+
| ID_noticia           | int       | NO   | PRI | NULL    | auto_increment |
| Contenido_noticia    | text      | YES  |     | NULL    |               |
| Fecha_noticia        | date      | YES  |     | NULL    |               |
| ID_seccion           | int       | YES  | MUL | NULL    |               |
| Titulo_noticia       | char(100) | YES  |     | NULL    |               |
| Contenido_noticia_en | text      | YES  |     | NULL    |               |
| Titulo_noticia_en    | char(100) | YES  |     | NULL    |               |
| urlImg              | text      | YES  |     | NULL    |               |
+-----+-----+-----+-----+-----+-----+
8 rows in set (0.01 sec)

mysql> describe Secciones;
+-----+-----+-----+-----+-----+-----+
| Field                | Type      | Null | Key | Default | Extra      |
+-----+-----+-----+-----+-----+-----+
| ID_seccion           | int       | NO   | PRI | NULL    | auto_increment |
| Seccion_noticia      | enum('Ciberseguridad','Tecnologia','IA','Hardware','Software','Todos') | YES  |     | NULL    |               |
| Seccion_noticia_en   | varchar(20) | YES  |     | NULL    |               |
+-----+-----+-----+-----+-----+-----+
3 rows in set (0.01 sec)

mysql> describe redactores;
+-----+-----+-----+-----+-----+-----+
| Field                | Type      | Null | Key | Default | Extra      |
+-----+-----+-----+-----+-----+-----+
| idRedactor           | int       | NO   | PRI | NULL    | auto_increment |
| usuario              | char(50)   | YES  |     | NULL    |               |
| password             | varchar(255) | YES  |     | NULL    |               |
+-----+-----+-----+-----+-----+-----+
3 rows in set (0.00 sec)
```

Ilustración 55: Base de datos creada para la página web

2.9. Rsyslog

Primero de todo se debe configurar el servidor que recibirá los logs, después los clientes que mandarán los logs.

Primero se instala el software de Rsyslog en el servidor, para configurar la recepción de logs en éste.

Ahora se configura el archivo de configuración de Rsyslog. Este archivo permite configurar en el servidor la recepción de logs, y el mismo archivo en el cliente el envío.

En este archivo se han hecho tres configuraciones, las primeras dos son la configuración de recepción de logs por el puerto 514 UDP o TCP. La tercera configuración sirve para automatizar la creación de directorios únicos para cada cliente.

Para configurar el cliente se debe configurar el mismo archivo para mandar los logs al servidor. Dentro de la configuración habrá que indicarle al servidor el tipo de protocolo, la IP del servidor Rsyslog y el puerto que empleará. Para diferenciar entre UDP y TCP se podrá hacer mediante el uso de un '@' que sirve para la configuración UDP y el uso de '@@' se emplea para el protocolo TCP.

Siempre que se aplique cualquier cambio se reiniciará el servidor Rsyslog y se comprobará el estado del servicio

En la siguiente imagen se puede observar un log que pertenece a un correo enviado mediante la newsletter del servidor web.

```
root@Rsyslog:~# cat /var/log/WEB/postfix.log
May 27 10:17:51 WEB postfix/pickup[9009]: D5C7C60114: uid=33 from=<www-data>
May 27 10:17:51 WEB postfix/pickup[9009]: D5C7C60114: uid=33 from=<www-data>
May 27 10:17:51 WEB postfix/cleanup[10371]: D5C7C60114: message-id=<0b56812fd809e5c597557b32b3f3def1@90.165.219.56>
May 27 10:17:51 WEB postfix/cleanup[10371]: D5C7C60114: message-id=<0b56812fd809e5c597557b32b3f3def1@90.165.219.56>
May 27 10:17:51 WEB postfix/qmgr[2100]: D5C7C60114: from=<www-data@WEB.localdomain>, size=14920, nrcpt=1 (queue active)
May 27 10:17:51 WEB postfix/qmgr[2100]: D5C7C60114: from=<www-data@WEB.localdomain>, size=14920, nrcpt=1 (queue active)
May 27 10:17:51 WEB postfix/smtp[10373]: D5C7C60114: to=<antonio@server.elhamiti.local>, relay=email.server.elhamiti.local, dsn=2.0.0, status=sent (250 2.0.0 Ok: queued as ED8F820691)
May 27 10:17:51 WEB postfix/qmgr[2100]: D5C7C60114: removed
May 27 10:17:51 WEB postfix/smtp[10373]: D5C7C60114: to=<antonio@server.elhamiti.local>, relay=email.server.elhamiti.local, dsn=2.0.0, status=sent (250 2.0.0 Ok: queued as ED8F820691)
May 27 10:17:51 WEB postfix/qmgr[2100]: D5C7C60114: removed
```

Ilustración 56: Verificar que recibe los logs

Conclusiones

Se han llevado a cabo proyectos particularmente complejos, como la creación de una página web propia. Este proyecto no solo demandó un diseño atractivo y una experiencia de usuario optimizada, sino que se tuvo en cuenta la proyección al mundo real para darle similitud a otros diarios digitales en formato web.

Otra fase significativa ha sido el desarrollo de un dominio de LDAP. Este apartado es esencial para la gestión de identidades y accesos dentro de la red, proporcionando una base para la autenticación y autorización los usuarios que trabajen en la empresa.

No hay que olvidar, que el resto de proyectos dentro de la web como son el servidor de correo, servidor de DNS, servidor de DHCP, entre otros, son fruto de un gran trabajo en equipo con el objetivo de realizar un proyecto íntegro con conexiones palpables entre todos los servicios, para elaborar una red empresarial como ElHamiti News.

Este proyecto ha requerido un gran trabajo por parte de todos los miembros del grupo, cada cual ha podido elegir libremente que parte del trabajo realizar. Aun así, se ha recibido apoyo por parte de todos para las tareas y ha habido buena dinámica de trabajo.

Bibliografía

- Atlantic.net. (16 de marzo de 2020). *How to Set Up a Fully Featured Mail Server with Postfix, Dovecot and Roundcube on Ubuntu 18.04*. Obtenido de Atlantic.net:
<https://www.atlantic.net/vps-hosting/how-to-set-up-fully-featured-mail-server-with-postfix-dovecot-and-roundcube-on-ubuntu/>
- Binaria, M. (12 de noviembre de 2021). *¡Tu propia VPN GRATIS en 10 MINUTOS!. Como INSTALAR y CONFIGURAR WIREGUARD en UBUNTU Server 20.04*. Obtenido de Youtube: <https://www.youtube.com/watch?v=58paASypYuY>
- CANLOP, O. (7 de abril de 2022). *LDAP Ubuntu Server 20.04 e integración de host al dominio*. Obtenido de Youtube: <https://www.youtube.com/watch?v=4o70ocLIC-o&t=170s>
- CCM. (24 de septiembre de 2023). *Cómo funciona el correo*. Obtenido de CCM:
<https://es.ccm.net/aplicaciones-e-internet/museo-de-internet/enciclopedia/11914-como-funciona-el-correo-electronico/>
- ChatGPT. (26 de mayo de 2024). *Como crear newsletter con Postfix y PHP*. Obtenido de ChatGPT:
<https://chatgpt.com/share/c351b729-4a71-47e9-8f64-6f898fd0f099>
- Cloudflare. (28 de abril de 2024). *¿Qué es DNS? | Cómo funciona*. Obtenido de Cloudflare:
<https://www.cloudflare.com/es-es/learning/dns/what-is-dns/>
- Computer, C. (31 de enero de 2023). *Instalar y configurar OpenLDAP en SERVIDOR y CLIENTE en Ubuntu Server & Desktop 22.04*. Obtenido de Youtube:
<https://www.youtube.com/watch?v=RI032gHFu88>
- Concepto.de. (28 de abril de 2024). *Lenguajes de Programación*. Obtenido de Concepto.de:
<https://concepto.de/lenguaje-de-programacion/>
- DigitalOcean. (19 de marzo de 2014). *How To Setup DNSSEC on an Authoritative BIND DNS Server*. Obtenido de DigitalOcean: <https://www.digitalocean.com/community/tutorials/how-to-setup-dnssec-on-an-authoritative-bind-dns-server-2>
- DigitalOcean. (26 de abril de 2022). *How To Install Elasticsearch, Logstash, and Kibana (Elastic Stack) on Ubuntu 22.04*. Obtenido de DigitalOcean:
<https://www.digitalocean.com/community/tutorials/how-to-install-elasticsearch-logstash-and-kibana-elastic-stack-on-ubuntu-22-04>
- DigitalOcean. (26 de abril de 2022). *How To Set Up and Configure a Certificate Authority On Ubuntu 22.04*. Obtenido de DigitalOcean: <https://www.digitalocean.com/community/tutorials/how-to-set-up-and-configure-a-certificate-authority-on-ubuntu-22-04>
- DigitalOcean. (26 de abril de 2022). *How To Set Up and Configure an OpenVPN Server on Ubuntu 22.04 (Apartados 3-4)*. Obtenido de DigitalOcean:
<https://www.digitalocean.com/community/tutorials/how-to-set-up-and-configure-an-openvpn-server-on-ubuntu-22-04>
- Informática, C. (26 de junio de 2023). *¿Qué es Roundcube y cómo funciona?* Obtenido de Cultura Informática: <https://cultura-informatica.com/conceptos/que-es-roundcube/>

- IONOS, D. G. (12 de marzo de 2024). *Cómo enviar correos electrónicos con PHPMailer*. Obtenido de IONOS: <https://www.ionos.es/digitalguide/correo-electronico/cuestiones-tecnicas/phpmailer/>
- Juanjo, E. R. (6 de enero de 2018). *Gestión de Logs centralizados con Rsyslog*. Obtenido de El Rincón De Juanjo: <https://juanjoselo.wordpress.com/2018/01/06/gestion-de-logs-centralizados-con-rsyslog/>
- libre, a. (29 de abril de 2024). *Configuración de Squid: Restricción de acceso a contenido por extensión*. Obtenido de alcance libre: <https://blog.alcancelibre.org/staticpages/index.php/19-3-como-squid-restriccion-extensiones>
- NASeros. (11 de octubre de 2021). *WireGuard. Configuración paso a paso de la mejor y más rápida VPN*. Obtenido de Youtube: <https://www.youtube.com/watch?v=WS1CZ4X7LOM>
- ProfeSantiago. (5 de noviembre de 2023). *GUÍA COMPLETA: Configura tu VPN GRATIS en un servidor LINUX privado*. Obtenido de Youtube: https://www.youtube.com/watch?v=3Z_7V_TgS54
- ProfeSantiago. (4 de enero de 2024). *Proxmox vs. ESXi: Descubre los HIPERVISORES tipo 1 y aprende a utilizarlos*. Obtenido de Youtube: <https://www.youtube.com/watch?v=Hr0yGVBmWL0>
- Proxmox. (11 de agosto de 2016). *Proxmox VE 4.2 Bug "Default gateway already exists on interface 'vbr0'."*. Obtenido de Proxmox Forum: <https://forum.proxmox.com/threads/proxmox-ve-4-2-bug-default-gateway-already-exists-on-interface-vbr0.28714/>
- Redeszone. (27 de diciembre de 2023). *Qué es el DHCP, funcionamiento y ejemplos de configuración*. Obtenido de Redeszone: <https://www.redeszone.net/tutoriales/internet/que-es-protocolo-dhcp/>
- Sanz, A. C. (12 de mayo de 2024). *Crear Proxy*. Obtenido de Portal del Estudiante Universidad Europea: https://campus.europaeducationgroup.es/courses/58175/assignments/358954?module_item_id=1328998
- Stackoverflow. (6 de agosto de 2014). *IMAP Error: Login failed - Roundcube*. Obtenido de Stackoverflow: <https://stackoverflow.com/questions/18942811/imap-error-login-failed-roundcube>
- Stackoverflow. (24 de febrero de 2021). *Roundcube SSL connection IMAP Error: Login failed*. Obtenido de Stackoverflow: <https://stackoverflow.com/questions/66359856/roundcube-ssl-connection-imap-error-login-failed>
- TecnoMagazine. (28 de abril de 2024). *¿Qué es el correo corporativo y para qué sirve?* Obtenido de TecnoMagazine: <https://tecnomagazine.net/correo-corporativo/>
- TV, P. (27 de febrero de 2023). *Cómo instalar y configurar LDAP Server y Cliente Ubuntu 20.04 - Tutorial 2024*. Obtenido de Youtube: <https://www.youtube.com/watch?v=oJBHbLUMSGY>
- Wikipedia. (26 de junio de 2021). *Dovecot*. Obtenido de Wikipedia: <https://es.wikipedia.org/wiki/Dovecot>
- Wikipedia. (5 de septiembre de 2022). *Iptables*. Obtenido de Wikipedia: <https://es.wikipedia.org/wiki/Iptables>

Wikipedia. (4 de octubre de 2022). *LDAP*. Obtenido de Wikipedia:

https://es.wikipedia.org/wiki/Protocolo_ligero_de_acceso_a_directorios

Wikipedia. (23 de enero de 2024). *Postfix*. Obtenido de Wikipedia:

<https://es.wikipedia.org/wiki/Postfix#:~:text=Postfix%20es%20un%20servidor%20de%20correo%20de%20software,de%20administrar%20y%20segura%20al%20ampliamente%20utilizado%20Sendmail.>

Wikipedia. (13 de febrero de 2024). *Red Privada*. Obtenido de Wikipedia:

https://es.wikipedia.org/wiki/Red_privada

Wikipedia. (17 de marzo de 2024). *Zona desmilitarizada (informática)*. Obtenido de Wikipedia:

[https://es.wikipedia.org/wiki/Zona_desmilitarizada_\(inform%C3%A1tica\)](https://es.wikipedia.org/wiki/Zona_desmilitarizada_(inform%C3%A1tica))

Tabla de ilustraciones

Ilustración 1: Estructura principal	9
Ilustración 2: Estructura del header	10
Ilustración 3: Estructura del main	10
Ilustración 4: Estructura del footer	11
Ilustración 5: Descripción header	11
Ilustración 6: Descripción main (Pagina "index")	12
Ilustración 7: Descripción main (Página "SobreNosotros")	12
Ilustración 8: Descripción footer	13
Ilustración 9: Plantilla email por HTML	15
Ilustración 10: Asignar el alias a la cuenta de correo	16
Ilustración 11: Configurar cliente de Postfix para iniciar sesión en el servidor.....	16
Ilustración 12: Asignación de cuenta para usuario	16
Ilustración 13: Pruebas de envío de correo para la newsletter	17
Ilustración 14: Visualización de que ha llegado el correo	17
Ilustración 15: IP asignada al equipo de ejemplo	19
Ilustración 16: Comprobación de conexión entre redes.....	19
Ilustración 17: Archivo de Zona directa de la DMZ.....	20
Ilustración 18: Archivo de Zona inversa de la DMZ	21
Ilustración 19: Comprobación de que se ha asignado la zona en un equipo y funciona el servicio DNS	22
Ilustración 20: Zona de servidores firmada	23
Ilustración 21: Confirmación de que la zona está firmada.....	23
Ilustración 22: Reglas de IPTABLES de Router Frontera	24
Ilustración 23: Reglas de IPTABLES de Router Replay	25
Ilustración 24: Asignación del proxy a un equipo de forma manual	28
Ilustración 25: Acceso con un usuario creado para poder navegar por Internet	28
Ilustración 26: Comprobación de dominio bloqueado	28
Ilustración 27: Comprobación de dominio no bloqueado ni por extensión ni por dominios	29
Ilustración 28: Bloqueo de descarga de un archivo con una extensión no permitida	29
Ilustración 29: Comprobación de una palabra de búsqueda bloqueada	29
Ilustración 30: Usuarios de Dovecot.....	31
Ilustración 31: Inicio de sesión en Roundcube	33
Ilustración 32: Enviar el correo a la cuenta para verificar que funciona.....	33
Ilustración 33: Comprobar que ha llegado el correo perfectamente	33
Ilustración 34: Interfaz wg0 en el servidor	34
Ilustración 35: Interfaz wg0 en el cliente.....	35
Ilustración 36: DNS asignado por la interfaz wg0	35
Ilustración 37: Conexión VPN con host fuera de la red	35
Ilustración 38: Comprobaciones de conexión sin DNS	35
Ilustración 39: Comprobación de conexión con DNS	36
Ilustración 40: Comprobación de que se tiene Internet con la VPN	36
Ilustración 41: Árbol de LDAP tras crear por terminal la UO, el grupo y el usuario	38
Ilustración 42: Usuarios de LDAP que se usarán	38
Ilustración 43: Grupos de LDAP que se usarán.....	38
Ilustración 44: Usuarios vinculados con el nuevo equipo.....	39
Ilustración 45: Demostración que los usuarios tienen permisos de Root.....	39
Ilustración 46: Dar a Not Listed para que se pueda iniciar sesión con otro usuario	40
Ilustración 47: Inicio de sesión y creación del directorio Home del nuevo usuario	40
Ilustración 48: Iniciado sesión con todos los usuarios que se desee del LDAP	40
Ilustración 49: Demostración de que se han creado todos los directorios Home.....	40
Ilustración 50: Home de Elastic.....	43
Ilustración 51: Estado del SIEM.....	43

Ilustración 52: Logs registrados hasta ahora.....	44
Ilustración 53: Ejemplos de logs.....	44
Ilustración 54: Usuario, privilegios del usuario y la base de datos creada.....	45
Ilustración 55: Base de datos creada para la página web.....	46
Ilustración 56: Verificar que recibe los logs	47

Anexos

1. Código fuente del sitio web

En el siguiente enlace: <https://github.com/MrRobot4042212/El-Hamiti-News.github.io.git>

2. Manual de instalación Proxmox

Se encuentra en la carpeta de anexos llamada
Grupo05_ManualInstalaciónProxmox_ElHamitiNews.

3. Archivos de conexión VPN (Wireguard y OpenVPN)

Se encuentra en la carpeta de anexos llamada
Grupo05_OpenVPN_ElHamitiNews y Grupo05_Wireguard_ElHamitiNews.

4. Reglas de cortafuegos de los routers

Se encuentra en la carpeta de anexos llamada
Grupo05_Firewall_ElHamitiNews.

5. Registro de Rsyslog de un equipo

Se encuentra en la carpeta de anexos llamada
Grupo05_Rsyslog_ElHamitiNews.

6. Archivos configuración de LDAP

Se encuentra en la carpeta de anexos llamada
Grupo05_LDAP_ElHamitiNews.

7. Logs de SIEM

Se encuentra en la carpeta de anexos llamada Grupo05_SIEM_ElHamitiNews.

8. Correo de ejemplo de newsletter

Se encuentra en la carpeta de anexos llamada
Grupo05_Correo_ElHamitiNews.

9. Anteproyecto

Se encuentra en la carpeta de anexos llamada
Grupo05_Anteproyecto_ElHamitiNews.