Alojamiento de Servidor Web

Andrea Sánchez Reque

Blanca Molero de Ávila

Felipe García Ledrado

Sergio Siles Gómez

Alejandro Ríos Holguín

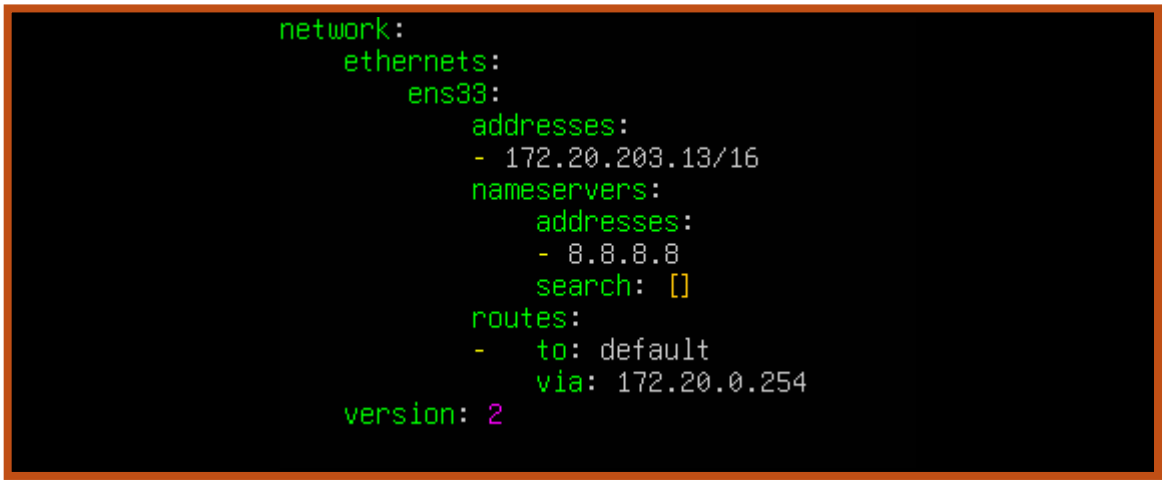
DAW

IES Azarquiel

1. Creación y configuración de MV

a. Como primer paso descargamos la ISO de Ubuntu Server y la instalamos la máquina virtual de VMWare para iniciar el proceso.

b. Configuramos el archivo netplan para tener conexión a internet.



Descargamos ufw para configurar el firewall de Ubuntu Server y otras herramientas para gestionar mejor la red.

- Para manejar el cortafuegos de la máquina: ***sudo apt install ufw***
- Para descargar herramientas de consulta y configuración de red (ifconfig): ***sudo apt install net-tools***
- Para descargar herramientas para consultar el DNS: **sudo apt install dns-utils**
- Contiene la herramienta para hacer “ping”: **sudo apt install iputils-ping**

Detenemos systemd-resolved ya que suele dar problemas.

- systemctl stop system-resolved

Desabilitamos systemd-resolved.

- systemctl disable system-resolved

Quitamos de systemctl a systemd-resolved.

- ✓ sudo systemctl mask systemd-resolved

Configuramos el DNS entrando en rm resolv.conf.

Comprobamos en nslookup que funciona el DNS.

- ✓ nslookup open.ai.

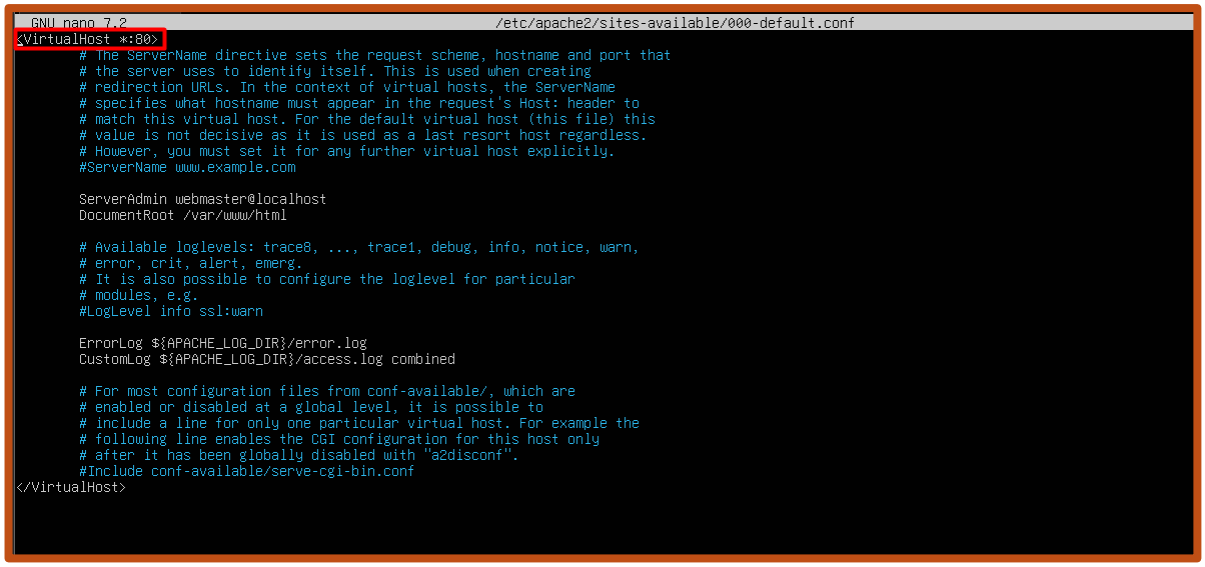
Descargamos apache2 y lo configuramos para que escuche en el puerto 80

- sudo apt install apache2

```
grupomaravilla@grupomaravilla:~$ sudo apt install apache2
[sudo] password for grupomaravilla:
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Leyendo la información de estado... Hecho
Se instalarán los siguientes paquetes adicionales:
  apache2-bin apache2-data apache2-utils libapr1t64 libaprutil1-dbd-sqlite3 libaprutil1-ldap libaprutil1t64 liblua5.4-0 ssl-cert
Paquetes sugeridos:
  apache2-doc apache2-suexec-pristine | apache2-suexec-custom www-browser
Se instalarán los siguientes paquetes NUEVOS:
  apache2 apache2-bin apache2-data apache2-utils libapr1t64 libaprutil1-dbd-sqlite3 libaprutil1-ldap libaprutil1t64 liblua5.4-0 ssl-cert
0 actualizados, 10 nuevos se instalarán, 0 para eliminar y 0 no actualizados.
Se necesita descargar 2.086 kB de archivos.
Se utilizarán 8.090 kB de espacio de disco adicional después de esta operación.
¿Desea continuar? [S/n] S
Ign:1 http://es.archive.ubuntu.com/ubuntu noble-updates/main amd64 libapr1t64 amd64 1.7.2-3.1ubuntu0.1
Ign:2 http://es.archive.ubuntu.com/ubuntu noble/main amd64 libaprutil1t64 amd64 1.6.3-1.1ubuntu7
Ign:3 http://es.archive.ubuntu.com/ubuntu noble/main amd64 libaprutil1-dbd-sqlite3 amd64 1.6.3-1.1ubuntu7
Ign:4 http://es.archive.ubuntu.com/ubuntu noble/main amd64 libaprutil1-ldap amd64 1.6.3-1.1ubuntu7
Ign:5 http://es.archive.ubuntu.com/ubuntu noble/main amd64 liblua5.4-0 amd64 5.4.6-3build2
Ign:6 http://es.archive.ubuntu.com/ubuntu noble-updates/main amd64 apache2-bin amd64 2.4.58-1ubuntu8.8
Ign:7 http://es.archive.ubuntu.com/ubuntu noble-updates/main amd64 apache2-data all 2.4.58-1ubuntu8.8
Ign:8 http://es.archive.ubuntu.com/ubuntu noble-updates/main amd64 apache2-utils amd64 2.4.58-1ubuntu8.8
Ign:9 http://es.archive.ubuntu.com/ubuntu noble-updates/main amd64 apache2 amd64 2.4.58-1ubuntu8.8
Ign:10 http://es.archive.ubuntu.com/ubuntu noble/main amd64 ssl-cert all 1.1.2ubuntu1
Ign:1 http://es.archive.ubuntu.com/ubuntu noble-updates/main amd64 libapr1t64 amd64 1.7.2-3.1ubuntu0.1
Ign:2 http://es.archive.ubuntu.com/ubuntu noble/main amd64 libaprutil1t64 amd64 1.6.3-1.1ubuntu7
Ign:3 http://es.archive.ubuntu.com/ubuntu noble/main amd64 libaprutil1-dbd-sqlite3 amd64 1.6.3-1.1ubuntu7
Ign:4 http://es.archive.ubuntu.com/ubuntu noble/main amd64 libaprutil1-ldap amd64 1.6.3-1.1ubuntu7
Ign:5 http://es.archive.ubuntu.com/ubuntu noble/main amd64 liblua5.4-0 amd64 5.4.6-3build2
Ign:6 http://es.archive.ubuntu.com/ubuntu noble-updates/main amd64 apache2-bin amd64 2.4.58-1ubuntu8.8
Ign:7 http://es.archive.ubuntu.com/ubuntu noble-updates/main amd64 apache2-data all 2.4.58-1ubuntu8.8
Ign:8 http://es.archive.ubuntu.com/ubuntu noble-updates/main amd64 apache2-utils amd64 2.4.58-1ubuntu8.8
Ign:9 http://es.archive.ubuntu.com/ubuntu noble-updates/main amd64 apache2 amd64 2.4.58-1ubuntu8.8
Ign:10 http://es.archive.ubuntu.com/ubuntu noble/main amd64 ssl-cert all 1.1.2ubuntu1
0% [Trabajando]_
```

Configuración para que escuche el puerto 80:

```
  GNU nano 7.2                                                  /etc/apache2/ports.conf
# If you just change the port or add more ports here, you will likely also
# have to change the VirtualHost statement in
# /etc/apache2/sites-enabled/000-default.conf

Listen 80

<IfModule ssl_module>
        Listen 443
</IfModule>

<IfModule mod_gnutls.c>
        Listen 443
</IfModule>
```



Usamos netstat –ltnp para ver los puertos que están escuchando

Comprobamos en ifconfig la ip de la MV y comprobamos buscando en otro equipo que hay salida por apache2

2. Configuración de la MV para conexiones http y ssh exclusivamente

Empezamos utilizando los comandos:

- ✓ ***sudo ufw default deny incoming***: Bloquea todo el tráfico que entra por el firewall (solo pueden entrar los que especifiquemos)
- ✓ ***sudo ufw default allow outgoing***: Permite acceder/salir a internet sin restricciones.

```
grupomaravilla@grupomaravilla:~$ sudo ufw default deny incoming
Default incoming policy changed to 'deny'
(be sure to update your rules accordingly)
grupomaravilla@grupomaravilla:~$ sudo ufw default allow outgoing
Default outgoing policy changed to 'allow'
(be sure to update your rules accordingly)
grupomaravilla@grupomaravilla:~$
```

```
grupomaravilla@grupomaravilla:~$ sudo ufw allow ssh
Rules updated
Rules updated (v6)
grupomaravilla@grupomaravilla:~$ sudo ufw allow http
Rules updated
Rules updated (v6)
grupomaravilla@grupomaravilla:~$
```

Habilitamos el firewall y comprobamos con el comando ***sudo ufw status*.**

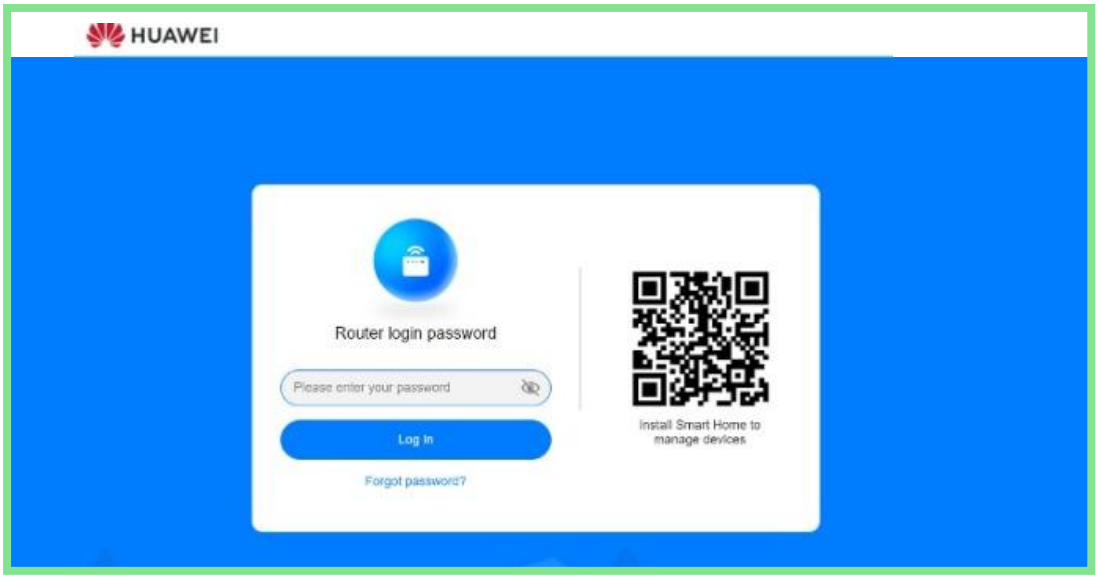
```
grupomaravilla@grupomaravilla:~$ sudo ufw enable
Firewall is active and enabled on system startup
grupomaravilla@grupomaravilla:~$ sudo ufw status
Status: active

To                         Action      From
--                         ------      ----
22/tcp                     ALLOW       Anywhere
80/tcp                     ALLOW       Anywhere
22/tcp (v6)                ALLOW       Anywhere (v6)
80/tcp (v6)                ALLOW       Anywhere (v6)

grupomaravilla@grupomaravilla:~$
```

3.Configuración del Router 3G sin CGNAT

Cuando se reinicia el router 3G la contraseña a usar para acceder a la configuración es la contraseña admin que se encuentra en la parte trasera del router. Si no se reinicia, se usa la contraseña común.

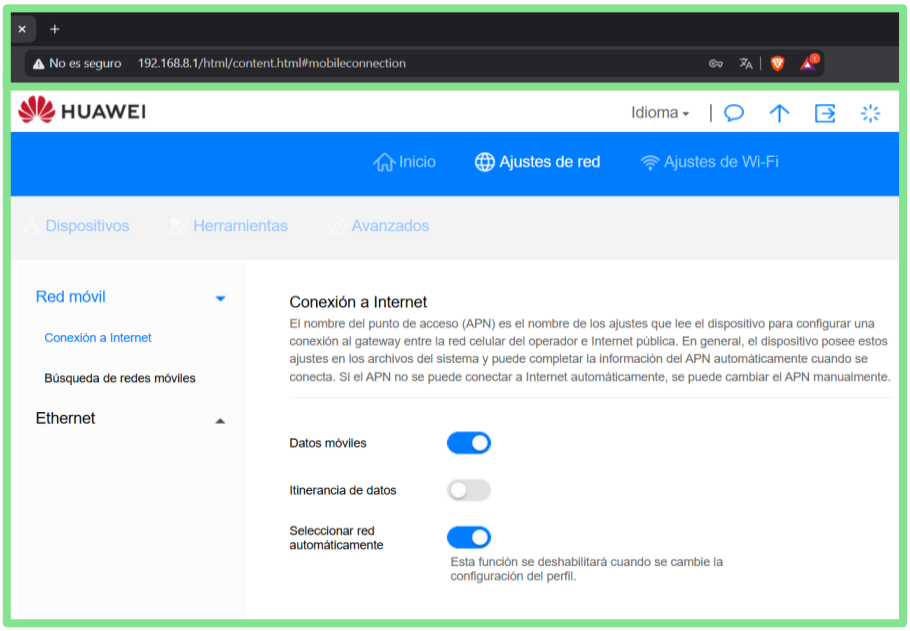
a. El primer paso es poner el router de fabrica para que no nos de problemas a la hora de empezar a hacer nuestra primera configuración
b. Despues introduciremos la sim al router y comprobaremos mediante nuestro terminal que ip nos está mostrando.
   - Comando: IPCONFIG.
   Que mostraría la ip:192.168.8.1
c. Ahora accederemos al router a través de su ip 192.x.x.1 y comprobaremos que tenemos conexión a internet, a través del reinicio tendremos que introducir la contraseña de admin y nos pediría cambiar la clave de acceso a la que os indico aquí abajo.

   Contraseña configurada: GRUPOMARAVILLA

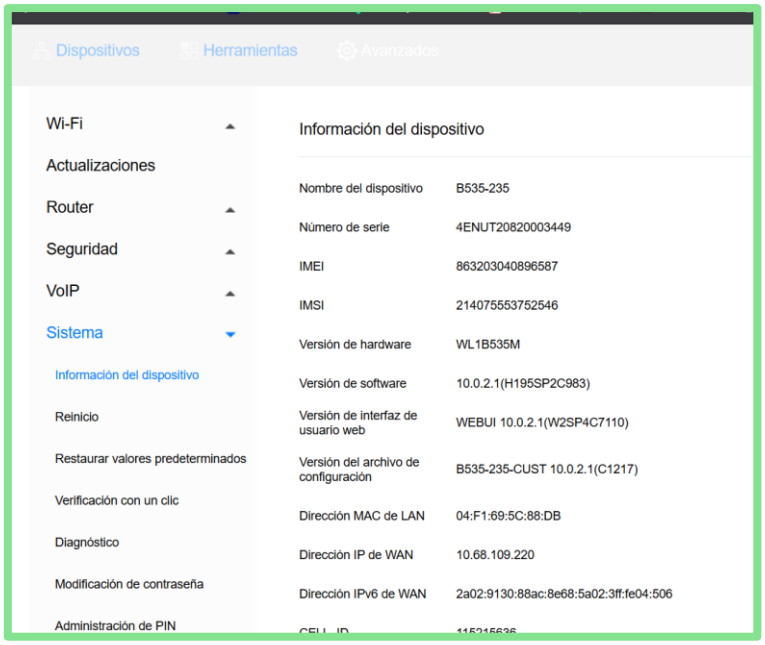


Después de haber configurado estos pasos se mostraría esta imagen que verifica que tenemos internet

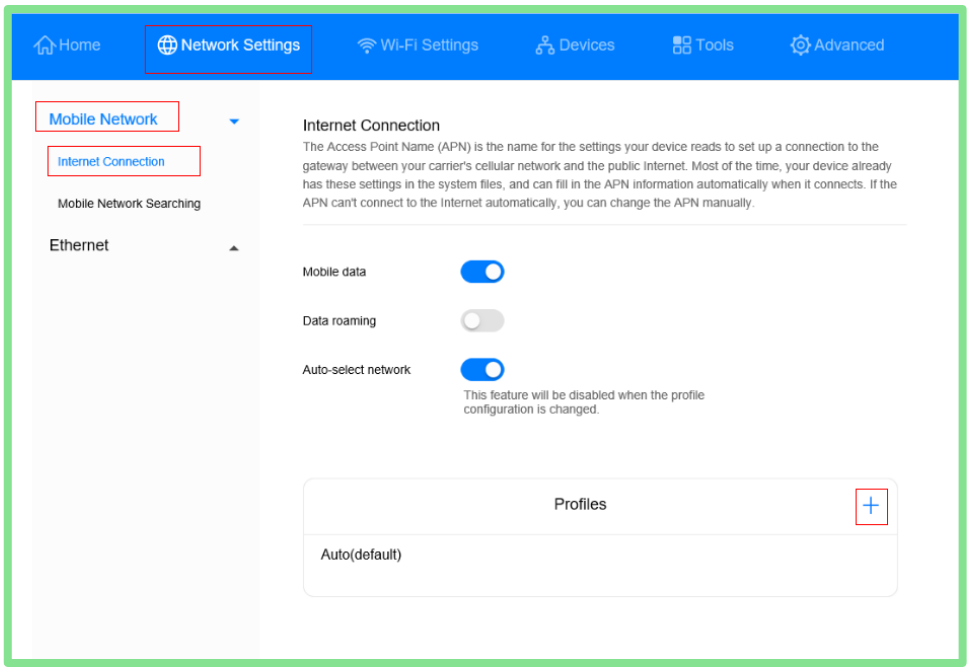
Pulsamos a ajustes de red y aparece la ventana de red móvil y tiene que decir que tenemos los datos móviles



Aquí vamos a pinchar en opción de Avanzadas, y pulsaríamos en sistema>información de dispositivo, si la dirección WAN es 10.x.x.2 usa CGNAT si no, no usa CGNAT como indico abajo esta red tiene CGNAT, vamos a proceder a cambiarlo en los siguientes pasos.



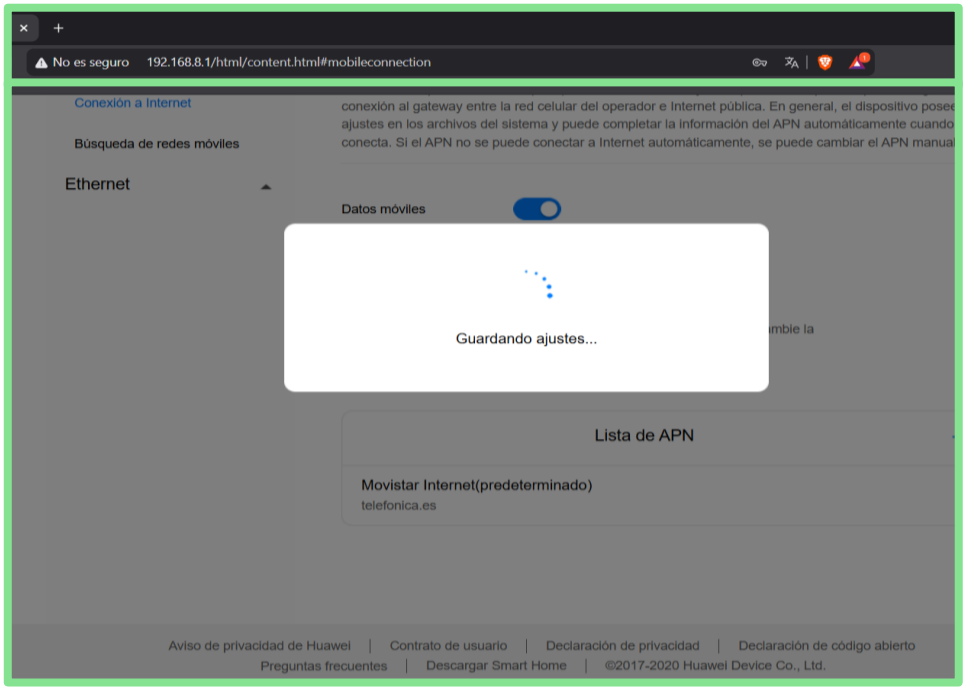
Vamos a pulsar en internet connection agregar apn.



Aqui indico mi APN sin cgnat que sería la que indico en esta foto que la busque mediante la web movistar, indico abajo su enlace

https://comunidad.movistar.es/discussions/ayuda_tecnica_movil/quitar-cgnat-de-mi-linea-movil-4g/4536277

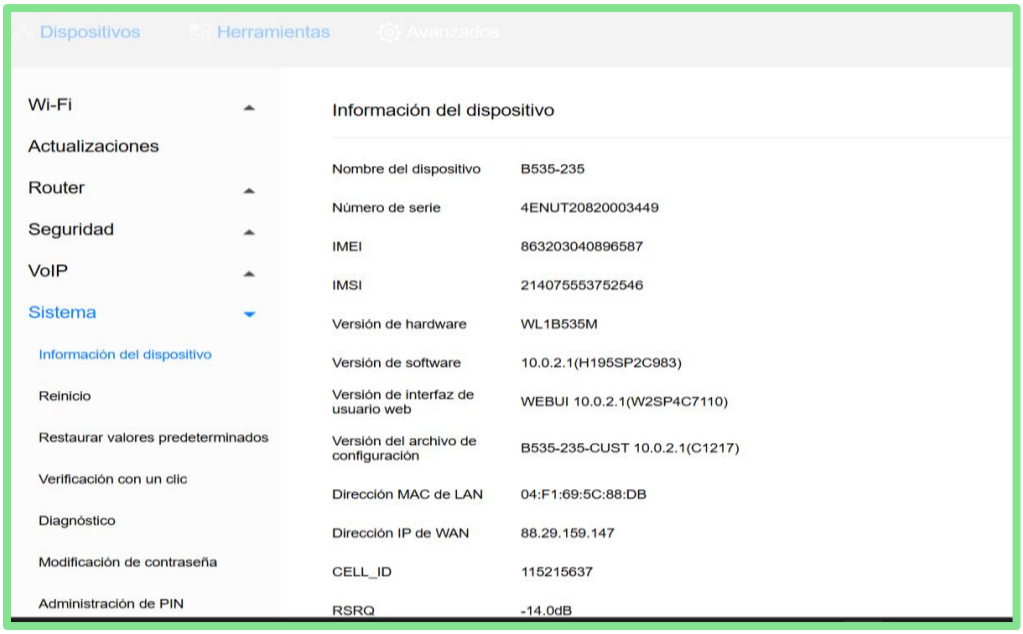
Aqui guardamos la configuración de la nueva APN

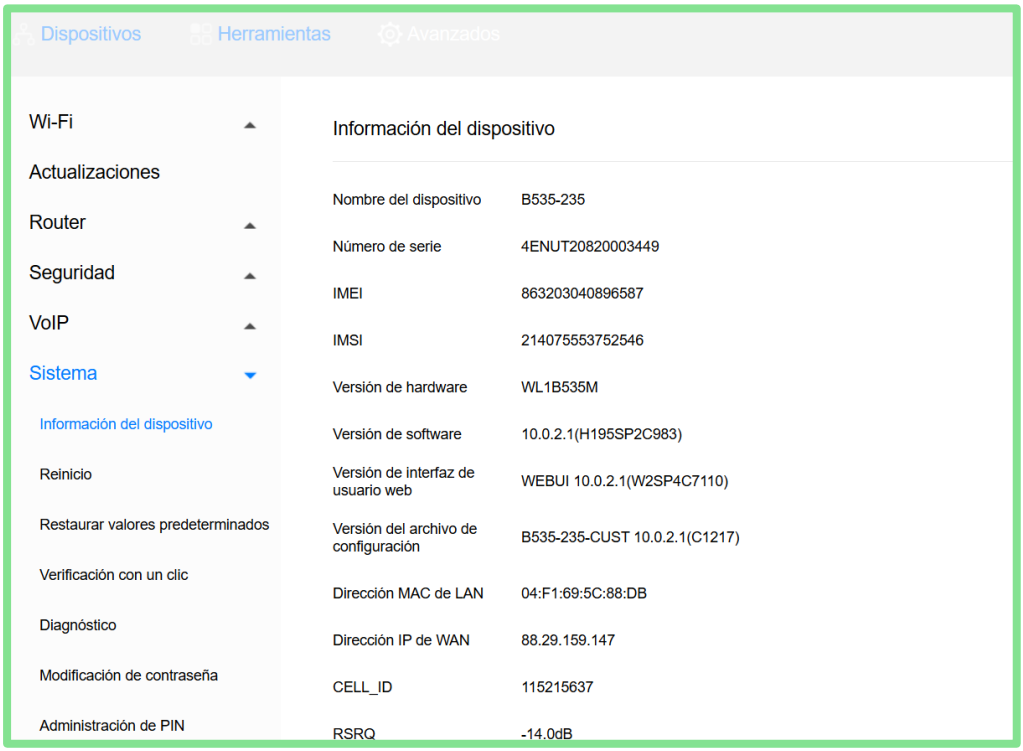


Y hacemos los pasos anteriores para verificar la nueva ip sin cgnat, esto también se verifica mediante la web showmyip

IP:88.29.129.147

https://www.showmyip.com

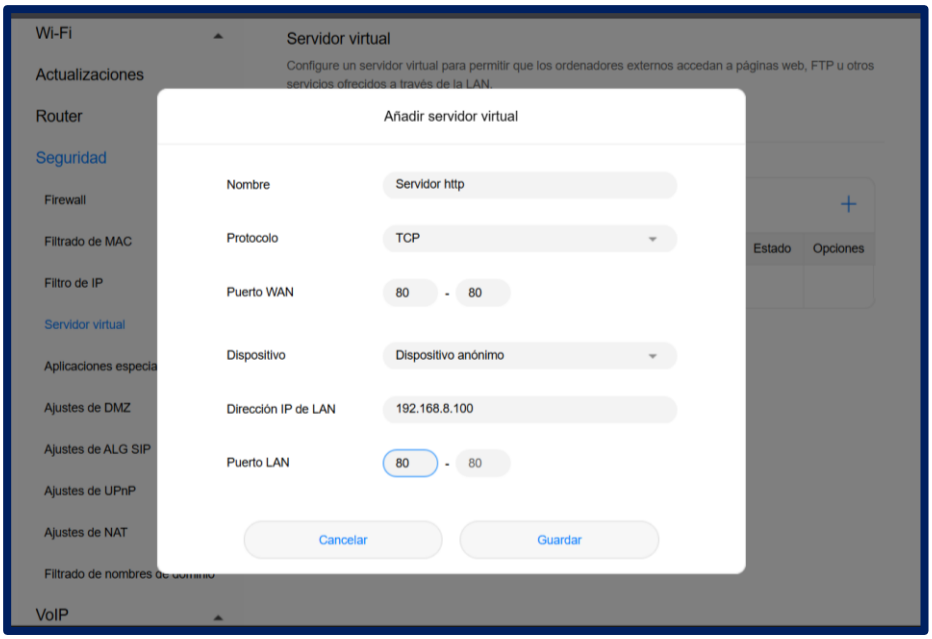

Dispositivos
Herramientas
Avanzados
Wi-Fi
Actualizaciones
Router
Seguridad
VoIP
Sistema
Información del dispositivo
Reinicio
Restaurar valores predeterminados
Verificación con un clic
Diagnóstico
Modificación de contraseña
Administración de PIN
Información del dispositivo
Nombre del dispositivo B535-235
Número de serie 4ENUT20820003449
IMEI 863203040896587
IMSI 214075553752546
Versión de hardware WL1B535M
Versión de software 10.0.2.1(H195SP2C983)
Versión de interfaz de usuario web WEBUI 10.0.2.1(W2SP4C7110)
Versión del archivo de configuración B535-235-CUST 10.0.2.1(C1217)
Dirección MAC de LAN 04:F1:69:5C:88:DB
Dirección IP de WAN 88.29.159.147
CELL_ID 115215637
RSRQ -14.0dB


Dispositivos
Herramientas
Avanzados
Wi-Fi
Actualizaciones
Router
Seguridad
VoIP
Sistema
Información del dispositivo
Reinicio
Restaurar valores predeterminados
Verificación con un clic
Diagnóstico
Modificación de contraseña
Administración de PIN
Información del dispositivo
Nombre del dispositivo B535-235
Número de serie 4ENUT20820003449
IMEI 863203040896587
IMSI 214075553752546
Versión de hardware WL1B535M
Versión de software 10.0.2.1(H195SP2C983)
Versión de interfaz de usuario web WEBUI 10.0.2.1(W2SP4C7110)
Versión del archivo de configuración B535-235-CUST 10.0.2.1(C1217)
Dirección MAC de LAN 04:F1:69:5C:88:DB
Dirección IP de WAN 88.29.159.147
CELL_ID 115215637
RSRQ -14.0dB

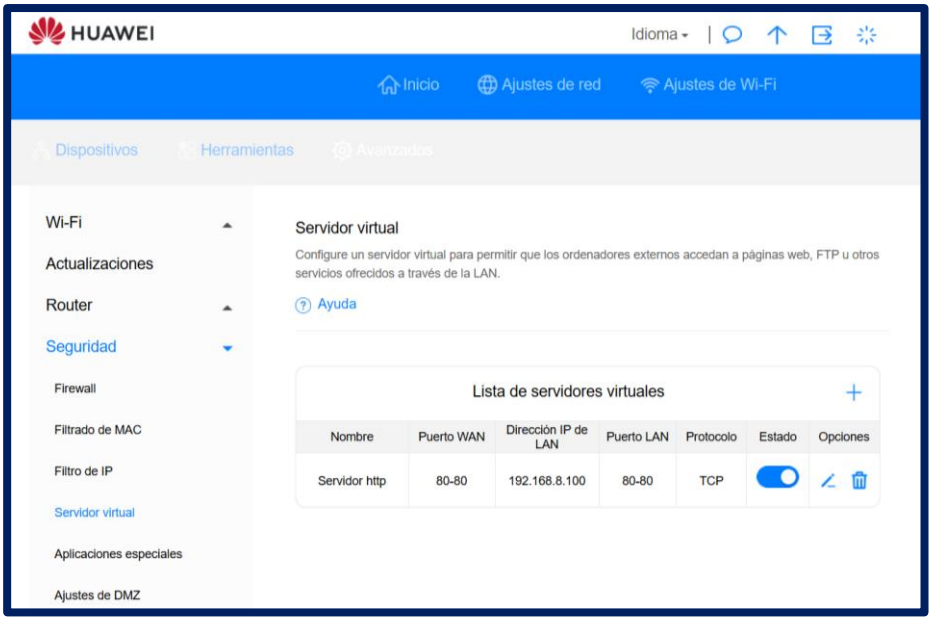
4.Configuración del mapeo del puerto 80

Establecemos que el protocolo de conexión es tcp (comunicación fiable de extremo a extremo por paquetes/segmentos).

Mapeamos el puerto 80 para permitir el paso de las peticiones por dicho puerto en red WAN y LAN.



Ponemos de ip 192.168.x.x porque nos permite el uso de dhcp para la asignación automática de ip dinámicas a la hora de navegar por internet. También sirve como una ip local propia de la máquina y el router.



5.Configuración de Firewall para permitir conexiones desde móviles

1. Activamos el modo más restrictivo

sudo ufw default deny incoming # Bloquea todas las conexiones entrantes no permitidas

```
root@grupomaravilla:/home/grupomaravilla# ufw default deny incoming
Default incoming policy changed to 'deny'
(be sure to update your rules accordingly)
root@grupomaravilla:/home/grupomaravilla# _
```

sudo ufw default allow outgoing # Permite que el servidor se conecte al exterior

```
root@grupomaravilla:/home/grupomaravilla# ufw default allow outgoing
Default outgoing policy changed to 'allow'
(be sure to update your rules accordingly)
root@grupomaravilla:/home/grupomaravilla#
```

2. Permitimos únicamente el servicio web (HTTP y HTTPS)

sudo ufw allow 80/tcp # Puerto HTTP

sudo ufw allow 443/tcp # Puerto HTTPS

```
root@grupomaravilla:/home/grupomaravilla# sudo ufw allow 80/tcp
Skipping adding existing rule
Skipping adding existing rule (v6)
root@grupomaravilla:/home/grupomaravilla# sudo ufw allow 443/tcp
Skipping adding existing rule
Skipping adding existing rule (v6)
root@grupomaravilla:/home/grupomaravilla#
```

3. Activamos el firewall

sudo ufw enable

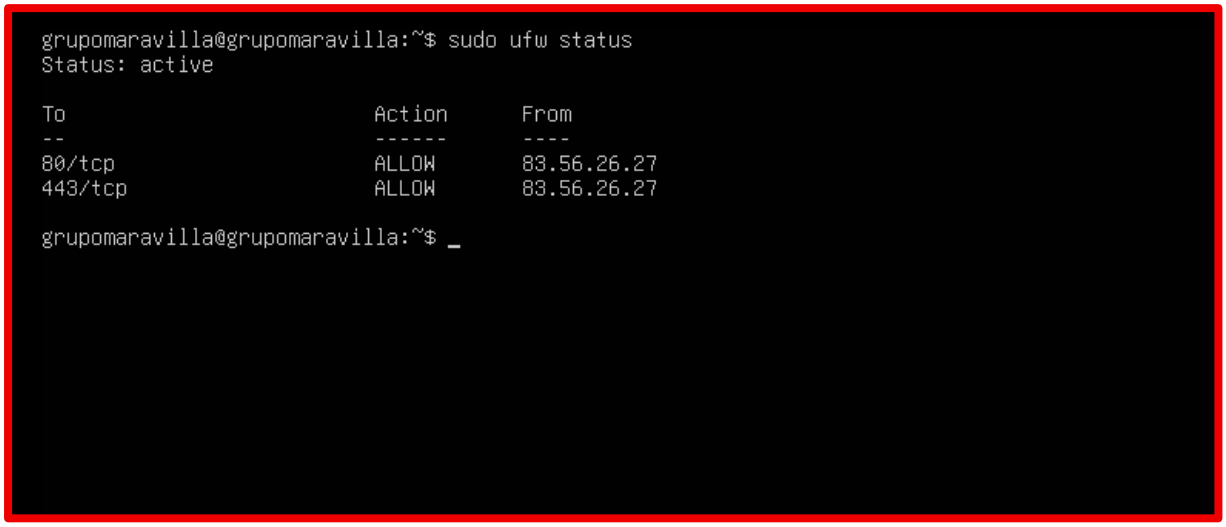
```
root@grupomaravilla:/home/grupomaravilla# sudo ufw enable
Firewall is active and enabled on system startup
root@grupomaravilla:/home/grupomaravilla#
```

Comprobamos las reglas activas

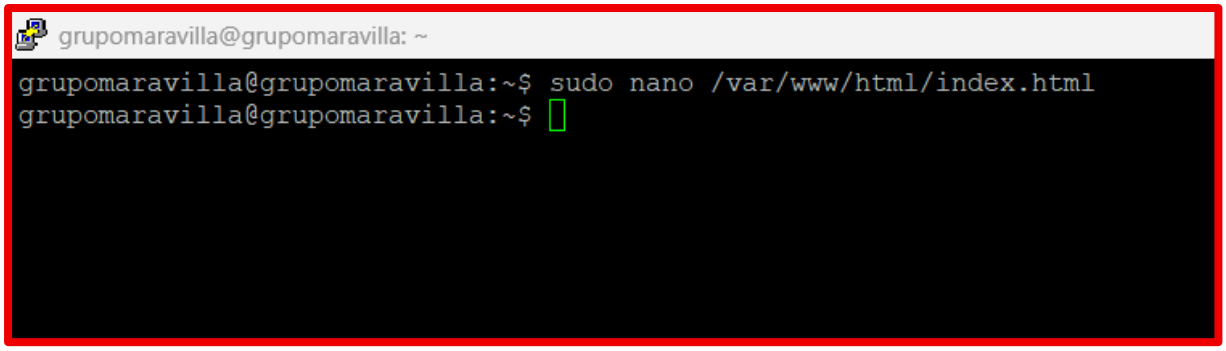
sudo ufw status verbose

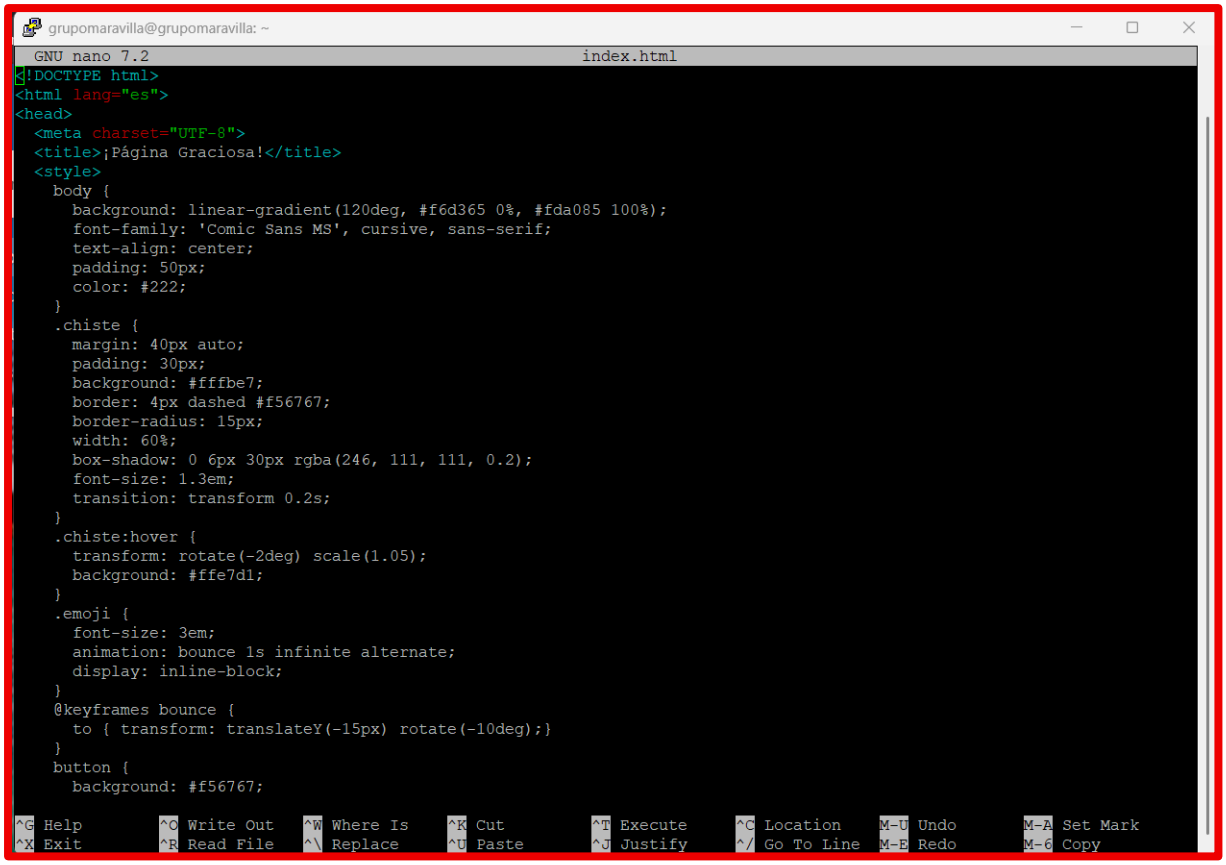
6.Configuración de Firewall para permitir conexiones a la web en equipos de clase.

Permitimos el acceso solo a las personas que tengan la ip 83.56.26.27 tanto en http como https.



Y por último, para cambiar la página por defecto para las personas que entren por medio de la ip debemos modificar el index de apache2:





Modificamos los permisos para que se pueda leer bien el archivo con el nuevo html ingresado (no recomendado).