**ANEXO II**

**Práctica 2: Configuración de una VPN con OpenVPN**

**Informe**

* **Documentar las configuraciones aplicadas.**

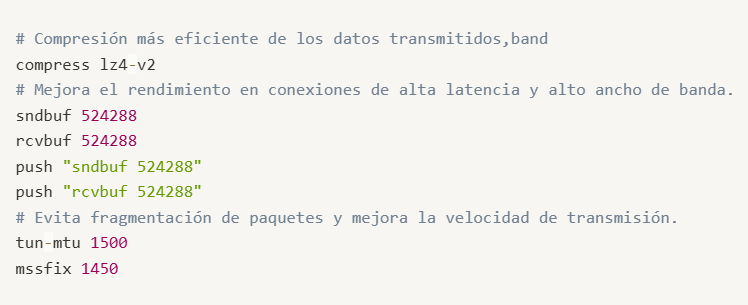
Las configuraciones realizadas se encuentran en la parte procedimiento de la práctica.

* **Presentar las capturas de pantalla, con la debida explicación de los resultados mostrados. Además, indicar el impacto en la seguridad.**

Los resultados obtenidos de la práctica con la debida explicación se muestran en la parte de resultados de la práctica. Y también el impacto que tiene en la seguridad de los dispositivos.

* **Modificar parámetro para maximizar el ancho de banda disponible y configurar autenticación de dos factores (2FA) para el cliente.**

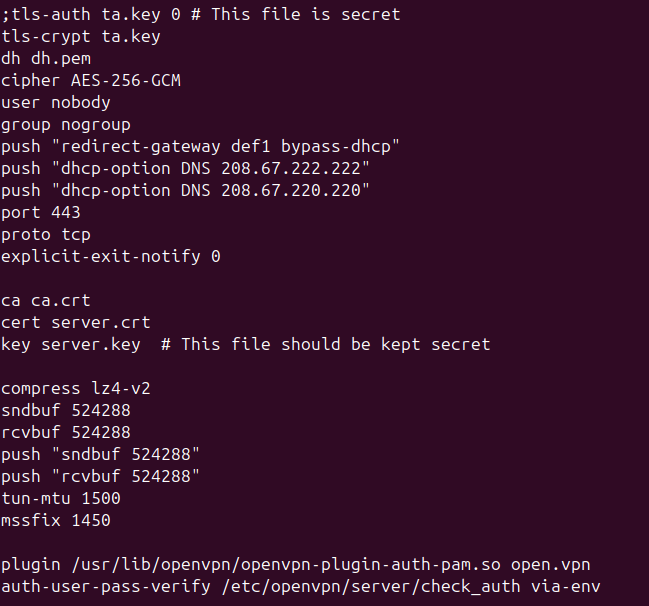
Para maximizar la eficiencia del ancho de banda se debe editar el archivo server.config de la siguiente forma:



**Figura 5.10.** Comandos para maximizar ancho de banda.

Luego para configurar la autenticación de dos factores, en este caso se usa Google Authenticator. Para esto primero se intala el Google Authenticator con el comando sudo apt install libpam-google-authenticator -y. Después se edita el archivo /etc/pam.d/openvpn, incluyendo la siguiente línea auth required pam\_google\_authenticator.so, esto para que la autenticación sea por al autentificador de Google.

De esta forma para que OpenVPN se autentique con Google se debe incluir a la configuración del archivo server.conf las dos últimas líneas que se muestra en la siguiente figura:

****

**Figura 5.11.** Configuración archivo server.conf.

En consecuencia, para que el usuario pueda conectarse se debe los códigos de autenticación para ello se usa el comando google-authenticator, de lo cual se muestra una serie de preguntas, donde se debe responder con yes y escanear el código QR generado desde la aplicación de celular, tal y como se muestra a continuación:

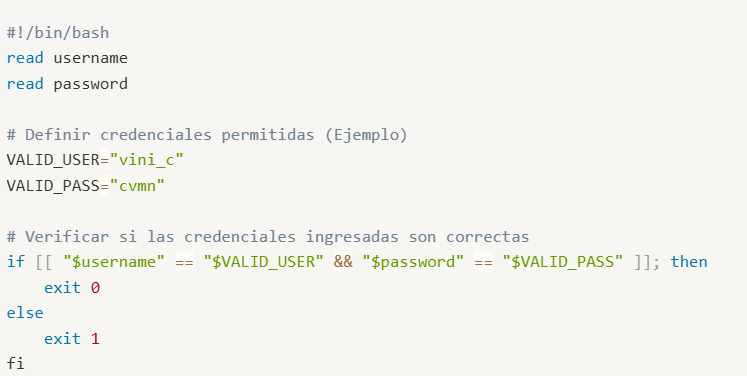
**A screenshot of a qr code

Description automatically generated**

**Figura 5.12.** Generación códigos de autenticación.

Cabe recalcar que para que se apliquen los cambios se debe reiniciar el servicio con el comando sudo systemctl restart openvpn-server@server.service.

Por otra parte, también se debe configurar el archivo check\_auth, el cual se usa para verificar si el usuario y la contraseña coinciden con valores predefinidos. Para ello se requiere el siguiente script, donde se deben ingresar usuarios y contraseñas que deben coincidir al iniciar la VPN por parte del cliente.



**Figura 5.13.** Configuración archivo check\_auth.

Por otro lado, se edita la configuración del cliente de acuerdo con las configuraciones del servidor para que el cliente se pueda conectar. De este modo se configura el archivo base.conf de la siguiente manera:

****

**Figura 5.14.** Configuración archivo base.conf.

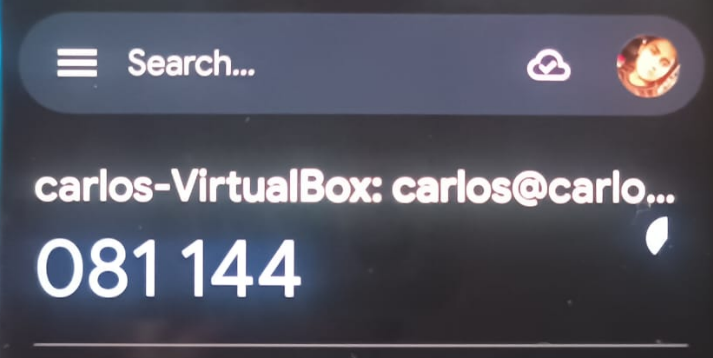
Luego se genera el archivo client.ovpn para importarlo en el dispositivo móvil y así probar la autenticación. De esta forma se carga el nuevo archivo a la aplicación para conectarse y se tiene lo siguiente:

A screenshot of a login page

Description automatically generated

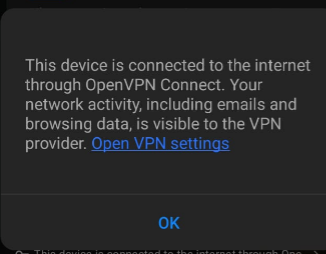
**Figura 5.15.** Petición de contraseña definida

De esta forma se ingresa la contraseña configurada en el archivo check\_auth. Y luego el código de autenticación que se genera en la autenticador del Google y que se renueva cada 30 segundos.



**Figura 5.16.** Código de autenticación de Google

De este modo el dispositivo se conecta a la VPN donde se comprueba que esta conectado a internet con el mensaje que se muestra en la siguiente figura



**Figura 5.17.** Verificación de la conexión a internet a través de la VPN.

También se pueden ver las estadísticas del tráfico entrante y saliente que muestra la aplicación OpenVPN.

A screenshot of a graph

Description automatically generated

**Figura 5.18.** Tráfico que se transmite por la VPN.

En consecuencia, la autenticación de dos factores (2FA) sirve para añadir una capa extra de seguridad a la conexión VPN configurada con OpenVPN debido al código de autenticación, el cual cambia cada 30 segundos, dando como resultado un aumento en la seguridad del servidor lo que hace muy robusto ante ataques como Man-in-the-Middle entre otros. Es decir, mantiene segura la información del usuario y al sistema operativo.