Configuración de una Red Privada Virtual (VPN) Segura

Parte 1: Preparación del Entorno

Paso 1: Actualización del Sistema

```
# Actualizar repositorios y paquetes (en sistemas basados en Debian/Ubuntu)
sudo apt-get update && sudo apt-get upgrade -y

# Instalar dependencias esenciales
sudo apt-get install -y openssl net-tools ufw
```

Paso 2: Instalación de OpenVPN

```
# Instalar OpenVPN y Easy-RSA (herramienta para PKI)
sudo apt-get install -y openvpn easy-rsa
```

Parte 2: Configuración de la VPN

Paso 3: Configuración de la Infraestructura de Certificados (PKI)

1. **Crear directorio para PKI**:

```
mkdir ~/easy-rsa
ln -s /usr/share/easy-rsa/* ~/easy-rsa/
cd ~/easy-rsa
```

2. **Inicializar la PKI y generar certificados**:

```
./easyrsa init-pki
./easyrsa build-ca          # Genera la Autoridad Certificadora (CA)
./easyrsa gen-req server nopass  # Certificado del servidor
./easyrsa sign-req server server  # Firma el certificado del servidor
./easyrsa gen-dh            # Parámetros Diffie-Hellman
```

3. **Generar certificado para cliente(s)**:

```
./easyrsa gen-req cliente1 nopass  # Certificado del cliente
```

./easyrsa sign-req client cliente1 # Firma el certificado del cliente

Paso 4: Configuración del Servidor VPN

1. **Copiar certificados y claves al servidor**:

sudo cp ~/easy-rsa/pki/ca.crt /etc/openvpn/server/

sudo cp ~/easy-rsa/pki/issued/server.crt /etc/openvpn/server/

sudo cp ~/easy-rsa/pki/private/server.key /etc/openvpn/server/

sudo cp ~/easy-rsa/pki/dh.pem /etc/openvpn/server/

2. **Crear archivo de configuración del servidor** (/etc/openvpn/server/server.conf):

ini

port 1194

proto udp

dev tun

ca ca.crt

cert server.crt

key server.key

dh dh.pem

server 10.8.0.0 255.255.255.0

push "redirect-gateway def1 bypass-dhcp"

push "dhcp-option DNS 8.8.8.8"

keepalive 10 120

tls-crypt ta.key # Opcional: cifrado adicional

cipher AES-256-GCM

user nobody

group nogroup

persist-key

persist-tun

status /var/log/openvpn-status.log

verb 3

3. **Habilitar y reiniciar el servicio**:

sudo systemctl enable openvpn-server@server

sudo systemctl start openvpn-server@server

4. **Configurar firewall (UFW)**:

sudo ufw allow 1194/udp

sudo ufw enable

Parte 3: Configuración del Cliente VPN

Paso 5: Configuración del Cliente

1. **Transferir certificados al cliente**:
    - ca.crt
    - cliente1.crt
    - cliente1.key
2. **Crear archivo de configuración del cliente** (cliente1.ovpn):

client

dev tun

proto udp

remote tu_servidor_ip 1194 # Reemplazar con IP pública del servidor

resolv-retry infinite

nobind

user nobody

group nogroup

persist-key

persist-tun

ca ca.crt

cert cliente1.crt

key cliente1.key

remote-cert-tls server

cipher AES-256-GCM

verb 3

3. **Importar el archivo** .ovpn **en el cliente** (usando OpenVPN GUI o CLI).

Parte 4: Verificación y Monitoreo

Paso 6: Verificación de la Conexión VPN

- **En el cliente**:

```
ip addr show tun0  # Verificar la interfaz VPN
ping 10.8.0.1      # Probar conectividad al servidor VPN
```

- **En el servidor**:

```
cat /var/log/openvpn-status.log  # Ver conexiones activas
```

Paso 7: Monitoreo de Conexiones

```
# Ver tráfico en tiempo real
sudo tcpdump -i tun0

# Monitorear logs del servidor
sudo journalctl -u openvpn-server@server -f
```