

VPN y accesos

Openfortivpn

Instalación

Primero hay que instalar la aplicación openfortivpn.

```
sudo apt-get install openfortivpn
```

Configurar VPN

Crear el siguiente fichero.

```
cd /etc/openfortivpn
sudo vi config.unal

# config file for openfortivpn, see man openfortivpn
host=168.176.176.36
port=20443
username=soffidvpn
password=PASSWORD_VAULT
trusted-cert=80e5369f81dbec49f8674e5245e8158a5e2a0a8e19961b85a9582e5e26351f4e
```

Y accedemos a la VPN.

```
svives@svives-ThinkPad-E15-Gen-2:/etc/openfortivpn$ sudo openfortivpn -c /etc/openfortivpn/config.unal
INFO: Connected to gateway.
INFO: Authenticated.
INFO: Remote gateway has allocated a VPN.
Using interface ppp0
Connect: ppp0 <--> /dev/pts/2
INFO: Got addresses: [10.212.134.150], ns [8.8.8.8, 8.8.4.4]
INFO: Negotiation complete.
INFO: Got addresses: [10.212.134.150], ns [8.8.8.8, 8.8.4.4]
INFO: Negotiation complete.
```

```
INFO: Got addresses: [10.212.134.150], ns [8.8.8.8, 8.8.4.4]
INFO: Negotiation complete.
INFO: Got addresses: [10.212.134.150], ns [8.8.8.8, 8.8.4.4]
INFO: Negotiation complete.
INFO: Got addresses: [10.212.134.150], ns [8.8.8.8, 8.8.4.4]
INFO: Negotiation complete.
INFO: Got addresses: [10.212.134.150], ns [8.8.8.8, 8.8.4.4]
INFO: Negotiation complete.
INFO: Got addresses: [10.212.134.150], ns [8.8.8.8, 8.8.4.4]
INFO: Negotiation complete.
INFO: Got addresses: [10.212.134.150], ns [8.8.8.8, 8.8.4.4]
INFO: Negotiation complete.
INFO: Got addresses: [10.212.134.150], ns [8.8.8.8, 8.8.4.4]
INFO: Negotiation complete.
INFO: Got addresses: [10.212.134.150], ns [8.8.8.8, 8.8.4.4]
INFO: Negotiation complete.
local IP address 10.212.134.150
remote IP address 169.254.2.1
INFO: Interface ppp0 is UP.
INFO: Setting new routes...
INFO: Adding VPN nameservers...
INFO: Tunnel is up and running.
```

Si da error de certificado, hay que reemplazarlo en el fichero config.unal.

```
svives@svives-ThinkPad-E15-Gen-2:/etc/openfortivpn$ sudo openfortivpn -c config.unal
ERROR: Gateway certificate validation failed, and the certificate digest is not in the local whitelist. If you trust it,
rerun with:
ERROR:    --trusted-cert 80e5369f81dbec49f8674e5245e8158a5e2a0a8e19961b85a9582e5e26351f4e
ERROR: or add this line to your configuration file:
ERROR:    trusted-cert = 80e5369f81dbec49f8674e5245e8158a5e2a0a8e19961b85a9582e5e26351f4e
ERROR: Gateway certificate:
ERROR:    subject:
ERROR:        CN=*.unal.edu.co
ERROR:    issuer:
ERROR:        C=GB
ERROR:        ST=Greater Manchester
ERROR:        L=Salford
ERROR:        O=Sectigo Limited
ERROR:        CN=Sectigo RSA Domain Validation Secure Server CA
ERROR: sha256 digest:
ERROR:    80e5369f81dbec49f8674e5245e8158a5e2a0a8e19961b85a9582e5e26351f4e
```

Acceso a las máquinas

Máquinas principales (passwords en el vault):

- ssh soffid01@172.16.9.20
- ssh soffid02@172.16.9.35

Máquinas replica (passwords en el vault):

- Bogotá 168.176.235.58 usuarios soffid o syspalmira
- Medellín 168.176.97.165 usuarios soffid o syspalmira
- Manizales 168.176.144.21 usuarios soffid01 o syspalmira

Configuración de réplica de CN=config

192.16.9.20 : Sincroniza configuración desde 172.16.9.20 y 172.16.9.35

192.16.9.35 : Sincroniza configuración desde 172.16.9.20 y 172.16.9.35

Configuración de réplica de o=unal.edu.co

192.16.9.20 : Sincroniza datos desde 172.16.9.20, 172.16.9.35, manizales, bogotá y medellís

192.16.9.35 : Sincroniza datos desde 172.16.9.20, 172.16.9.35, manizales, bogotá y medellín

Manizales: Sincroniza datos desde 172.16.9.20 y 172.16.9.35

Medellín: Sincroniza datos desde 172.16.9.20 y 172.16.9.35

Bogotá: Sincroniza datos desde 172.16.9.20 y 172.16.9.35