redNEREA
LA RED INTERADMINISTRATIVA DE ANDALUCÍA

Manual Usuario VPN de NEREA en Plataformas Linux

ABRIL 2021

INDICE

0 OBJETO 3
1 DESCRIPCIÓN DEL SEVICIO 3
2 CONFIGURACION CLIENTE LINUX 3

0 Objeto

El objetivo del presente documento es proporcionar una guía de instalación sencilla para el servicio de VPN de NEREA, que proporcionará acceso seguro a los recursos de Red NEREA/SARA, de modo que sus usuarios conozcan la configuración que deben implementar sobre sus equipos.

1 Descripción del Sevicio

Para el acceso al servicio de VPN de Red NEREA se requiere la instalación de un software del fabricante Fortinet. La solución se basa en SSL en entornos Linux, concediéndose el acceso al servicio mediante autenticación por medio de usuario/contraseña, y estableciéndose el túnel mediante certificado de la FNMT expedido por el usuario. En caso de que no dispongamos de él se puede consultar el proceso de solicitud y descarga en el Anexo I. También allí se detalla cómo exportar el certificado a un fichero PKCS#12 si únicamente lo tenemos en el navegador.

2 Configuracion cliente linux

Actualmente de la página oficial de Fortinet no podemos descargarnos una versión TLS del cliente VPN FortiClient, por ello el equipo de soporte de Red NEREA proveerá el cliente a instalar. Pasos a seguir para la instalación en un equipo con distribución Ubuntu instalada:

Copiamos en el escritorio el archivo proporcionado por el equipo de Red NEREA: “forticlientsslvpn_linux_4.4.2328.tar.gz”. Procedemos a descomprimir el archivo:

```
$ tar xvzf forticlientsslvpn_linux_4.4.2328.tar.gz
```

```
:~/Escritorio$ tar xvzf forticlientsslvpn_linux_4.4.2328.t
ar.gz
forticlientsslvpn/
forticlientsslvpn/32bit/
forticlientsslvpn/32bit/helper/
forticlientsslvpn/32bit/helper/setup.linux.sh
forticlientsslvpn/32bit/helper/fortisslclient.key
forticlientsslvpn/32bit/helper/fortisslcacert.pem
forticlientsslvpn/32bit/helper/printcert
forticlientsslvpn/32bit/helper/config
forticlientsslvpn/32bit/helper/waitppp.sh
forticlientsslvpn/32bit/helper/subproc
forticlientsslvpn/32bit/helper/fctrouternke.kext/
forticlientsslvpn/32bit/helper/fctrouternke.kext/Contents/
forticlientsslvpn/32bit/helper/fctrouternke.kext/Contents/MacOS/
forticlientsslvpn/32bit/helper/fctrouternke.kext/Contents/MacOS/fctrouternke
forticlientsslvpn/32bit/helper/fctrouternke.kext/Contents/Resources/
forticlientsslvpn/32bit/helper/fctrouternke.kext/Contents/Resources/English.lpro
j/
forticlientsslvpn/32bit/helper/fctrouternke.kext/Contents/Resources/English.lpro
j/InfoPlist.strings
forticlientsslvpn/32bit/helper/fctrouternke.kext/Contents/Info.plist
forticlientsslvpn/32bit/helper/fctrt
forticlientsslvpn/32bit/helper/License.txt
forticlientsslvpn/32bit/helper/construct_trustca
forticlientsslvpn/32bit/helper/fortisslclient.crt
forticlientsslvpn/32bit/helper/showlicense
forticlientsslvpn/32bit/forticlientsslvpn
forticlientsslvpn/32bit/forticlientsslvpn_cli
```

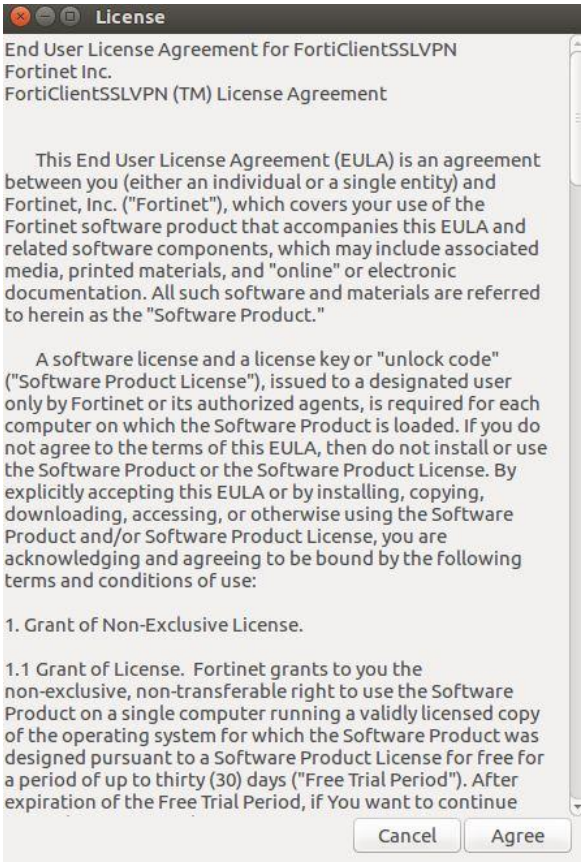
1. Accedemos a la carpeta creada y ejecutamos el cliente pesado:

```
$ cd forticlientesslvpn
$ sudo ./fortisslvpn.sh
```

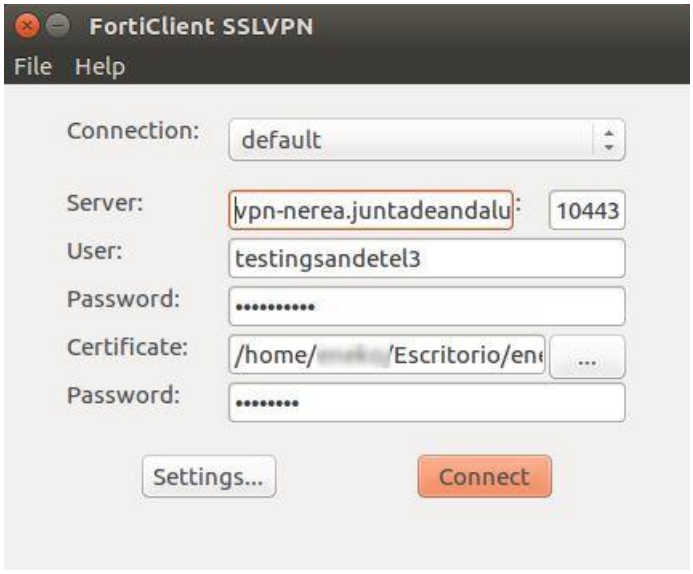
```
:~/Escritorio$ cd forticlientsslvpn
:~/Escritorio/forticlientsslvpn$ sudo ./fortisslvpn.sh

(showlicense:7009): IBUS-WARNING **: The owner of /home/eneko/.config/ibus/bus i
s not root!
```

2. Aceptamos la Licencia:



3. Tras aceptar la licencia, nos aparece la pantalla donde tenemos que rellenar los datos de configuración del usuario VPN:
   -Server: vpn-nerea.juntadeandalucia.es (en el siguiente recuadro 10443)
   -User: “usuario proporcionado por Red NEREA”
   -Password: “password proporcionada por Red NEREA”
   -Certificate: “ruta donde se encuentra el certificado de usuario de la FNMT”
   -Password: “password del certificado de la FNMT”



4. Túnel en funcionamiento: