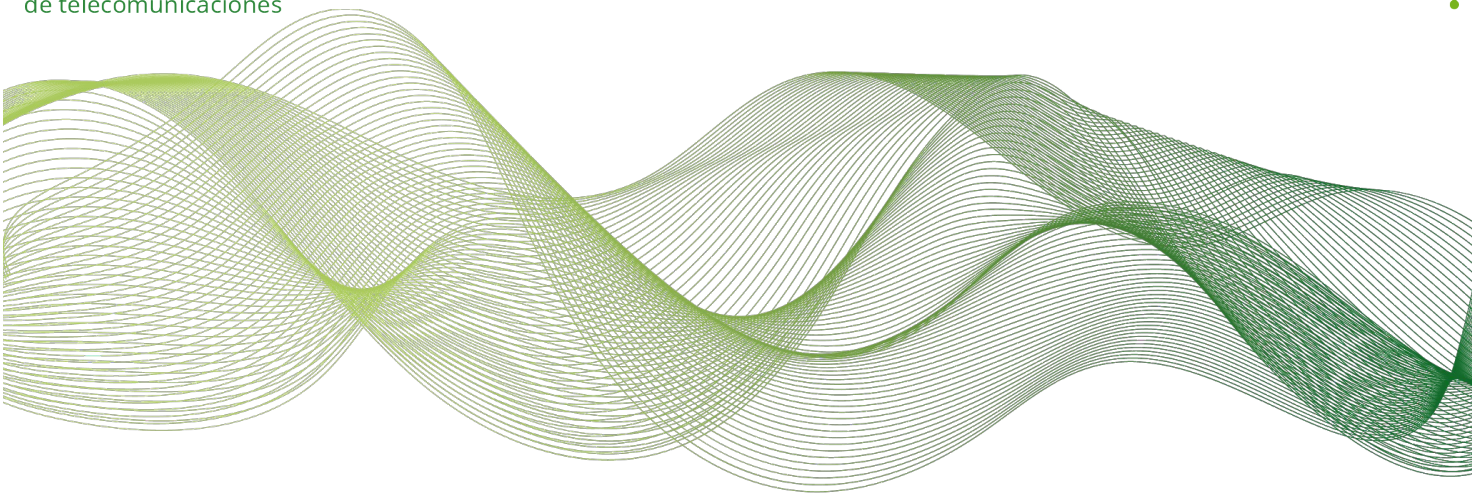
Manual

Red Corporativa
de telecomunicaciones



Manual Cliente VPN Linux Checkpoint RCJAv5

Ingeniería SANDETEL

Junta de Andalucía
Consejería de la Presidencia, Administración Pública e Interior

ÍNDICE

1Objetivo

Manual de usuario del cliente VPN Checkpoint SSL Network Extender (SNX) en Sistema Operativo Linux. El presente documento tiene como objetivo mostrar los pasos de instalación, conexión y desinstalación del cliente SNX para Linux. Este cliente es el que se empleará en RCJAv5 para dar continuidad al servicio VPN.

2Versiones Soportadas

Linux

Mobile Access Portal Agent se soporta en los siguientes sistemas *nix:

- openSUSE 42.1, 42.2, 42.3, Leap 15 – 15.5
- CentOS 7.3 – 9
- Fedora 24 – 39
- Ubuntu 16.04 – 23.10
- RHEL 7.3 – 9.3 (Workstation)

3Instalación

La instalación se realiza de forma automática una vez que se realiza la autenticación, aunque requiere los siguientes paquetes instalados previamente:

Java

- Todas las versiones de SO Linux necesitan tener Java instalado. El Portal Agent es compatible con las siguientes:
    - Oracle JRE versions 8
    - Oracle JDK versions 11 – 20
    - Oracle OpenJDK versions 11 – 20

Herramientas requeridas

- certutil (part of Mozilla NSS tools)
- openssl
- xterm

A continuación, puede verse un listado de comandos* para instalarlas:

	certutil	openssl	xterm	bzip2
CentOS	yum install nss-tools	yum install openssl	yum install xterm	
Fedora	dnf install nss-tools	dnf install openssl	dnf install xterm	
openSuse Leap	zypper install mozilla-nss-tools	zypper install openssl	zypper install xterm	
RHEL Workstation	yum install nss-tools	yum install openssl	yum install xterm	
Ubuntu	apt-get install libnss3-tools	apt-get install openssl	apt-get install xterm	apt-get install bzip2

*Es necesario ser usuario root para ejecutar estos comandos

Librerías requeridas

Linux distribution	64-bit version	Installation commands*
CentOS	• glibc.i686 • pam.i686 • libX11.i686 • libnsl.i686 • libstdc++.i686	yum install glibc.i686 pam.i686 libX11.i686 libnsl.i686 libstdc++.i686
Fedora	• glibc.i686 • pam.i686 • libX11.i686 • libnsl.i686 • libstdc++.i686	dnf install glibc.i686 pam.i686 libX11.i686 libnsl.i686 libstdc++.i686
openSUSE Leap	• glibc-32bit • pam-32bit • libX11-6-32bit • libstdc++6-32bit	zypper install glibc-32bit pam-32bit libX11-6-32bit libstdc++6-32bit
RHEL Workstation	• glibc.i686 • pam.i686 • libX11.i686 • libnsl.i686 • libstdc++.i686	yum install glibc.i686 pam.i686 libX11.i686 libnsl.i686 libstdc++.i686
Ubuntu**	• libpam0g:i386 • libx11-6:i386 • libstdc++6:i386	apt-get install libpam0g:i386 libx11-6:i386 libstdc++6:i386

*Es necesario ser usuario root para ejecutar estos comandos

** Podría ser necesario habilitar los siguientes repositorios de 32 bits:

```
dpkg --add-architecture i386
apt-get update
```

4Alta usuario

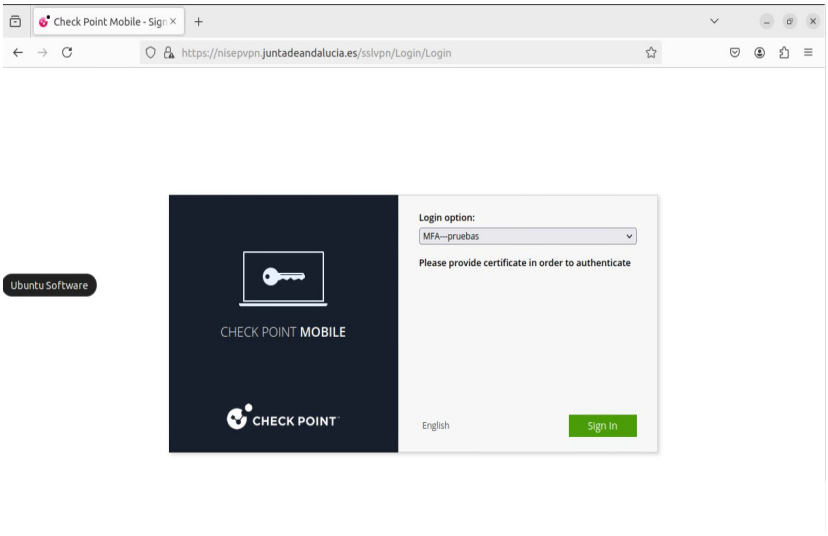
Para que los usuarios que usan el cliente VPN Linux puedan conectarse, y recibir su dirección ip de VPN, es necesario previamente realizar una configuración específica en el servicio VPN asociada a su usuario LDAP.

Dicha configuración asocia el atributo del certificado que hace referencia al DNI con la ip asignada y una vez aplicada los usuarios solo podrán usar una cuenta o usuario LDAP para la conexión mediante VPN, con independencia de que dispongan de más de un usuario LDAP asociado al mismo DNI.

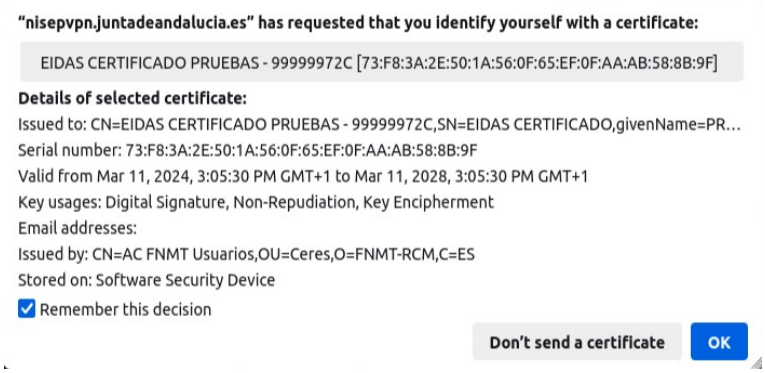
No será posible establecer la conexión hasta que no se haya completado dicha configuración. Aunque si es posible llevar a cabo las tareas iniciales asociadas a la primera conexión indicadas en el siguiente apartado.

5Conexión

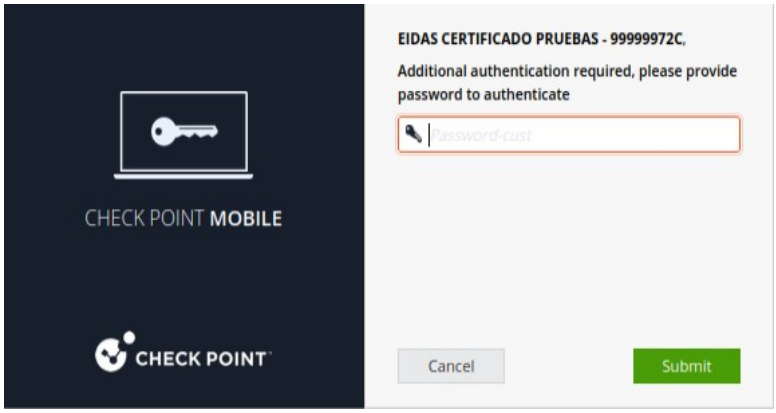
La conexión se realiza desde el portal web https://nisepvpn.juntadeandalucia.es



Tras esto nos aparecerá la primera vez un warning del sistema acerca de que el sitio web nisepvpn.juntadeandalucia.es ha solicitado que se use un certificado de usuario almacenado en el equipo para que este se autentique.



Tras hacer clic en OK en el paso anterior, el portal solicitará la contraseña LDAP del usuario asociado al certificado como segundo método de autenticación:



*** NOTA 1: Importante** lo que hay que introducir es la **contraseña LDAP**, no la contraseña del certificado. La solución utiliza el certificado digital introducido para obtener el DNI del usuario, con el DNI se identifica el usuario LDAP en el LDAP de la Junta de Andalucia y se utiliza la contraseña del usuario LDAP como doble factor de autenticación (2FA).

*** NOTA 2:** Tal y como se indicó en el apartado previo una vez se haya realizado la configuración necesaria para que los usuarios puedan utilizar el cliente VPN Linux estos solo podrán usar una cuenta o usuario LDAP para la conexión mediante VPN, con independencia de que dispongan de más de un usuario LDAP asociado al mismo DNI.

Una vez introducida correctamente y por tanto autenticado el usuario *, aparecerá el botón de conectar:

La primera vez que se haga uso del cliente será necesario realizar la instalación del software "SSL Network Extender (SNX)" y "Mobile Access Portal Agent".

Esto podemos hacerlo pulsando la opción "Settings" y haciendo uso de los enlaces incluidos en el cuadro "Native Applications Settings" descargar el software asociado a "SSL Network

Extender" (Download installation for Linux) y "Check Point Mobile Access Portal Agent" (Download installation for Linux).

Y una vez descargados ejecutar los scripts de instalación "snx_install.sh" y "cshell_install.sh" con permisos del usuario "**root**".

usuario@equipo:~/Downloads$ **./cshell_install.sh**

The installation script requires root permissions

Please provide the root password

[sudo] password for usuario:

Start Check Point Mobile Access Portal Agent installation

Extracting Mobile Access Portal Agent... Done

Installing Mobile Access Portal Agent... Done

Installing certificate...

Firefox must be closed to proceed with Mobile Access Portal Agent installation.

Press [ENTER] key to continue...

Enter Password or Pin for "NSS Certificate DB":

Done

Starting Mobile Access Portal Agent... Done

Installation complete

usuario@equipo:~/Downloads$ **./snx_install.sh**

The installation script requires root permissions

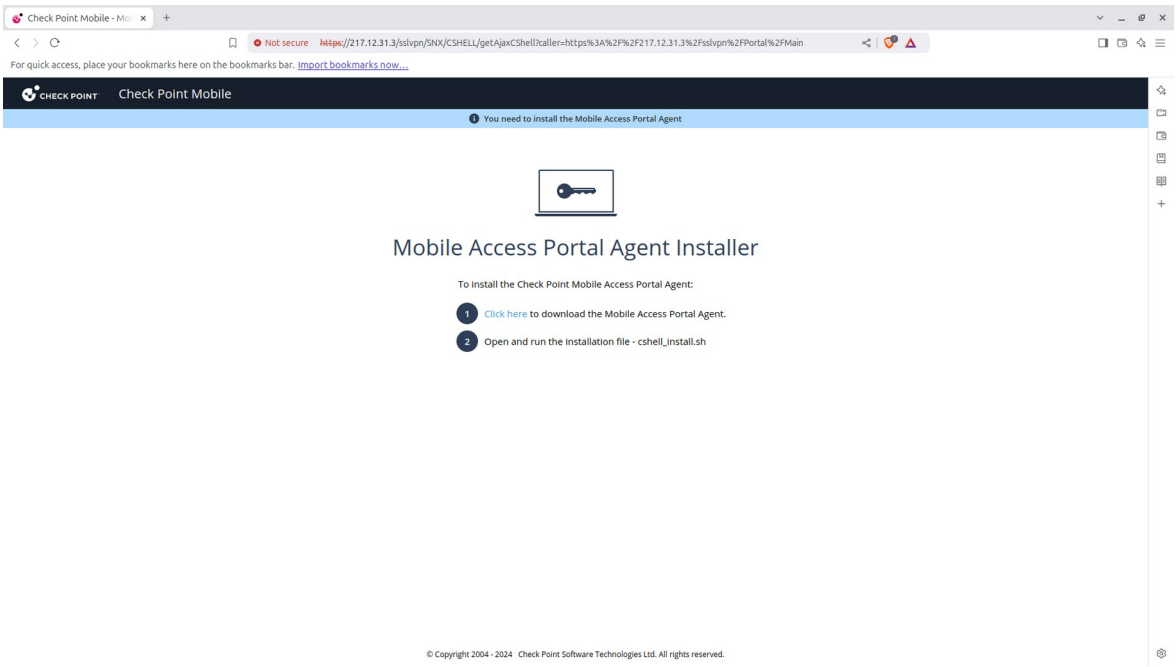
Please provide the root password

Password:

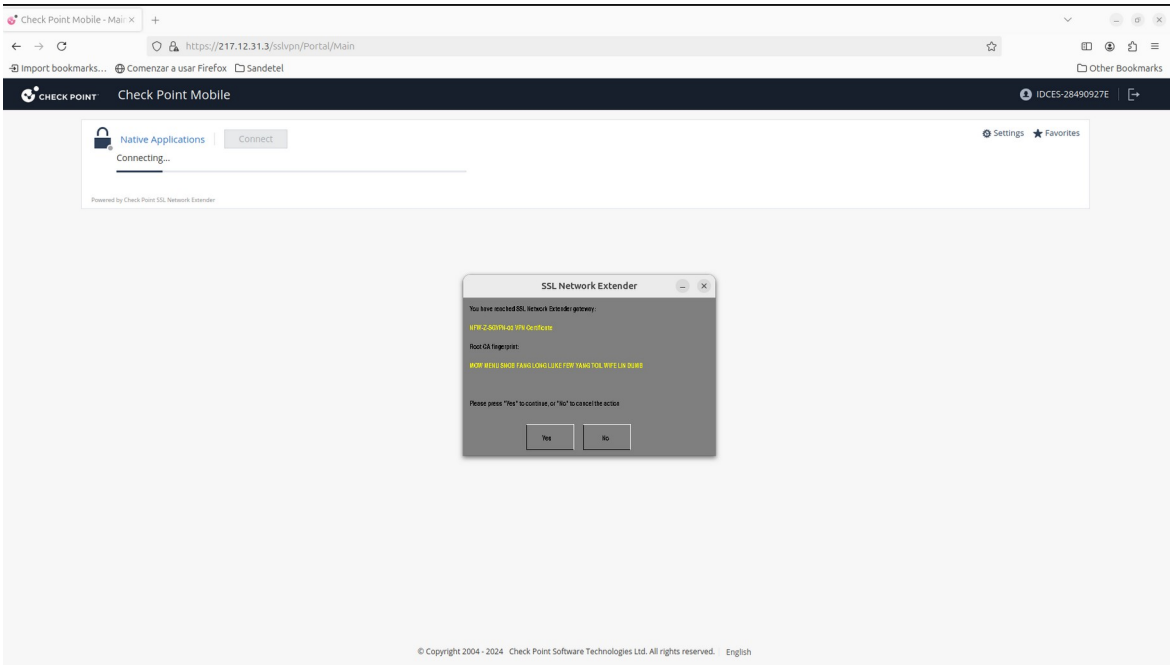
Installation successfull

O si no hemos realizado los pasos indicados previamente y directamente pulsamos la opción "Connect" se lanzará desde el portal la instalación de "SSL Network Extender (SNX)", dicha instalación aunque se ejecuta de manera desatendida podrá requerir que proporcionemos la contraseña del usuario "**root**".

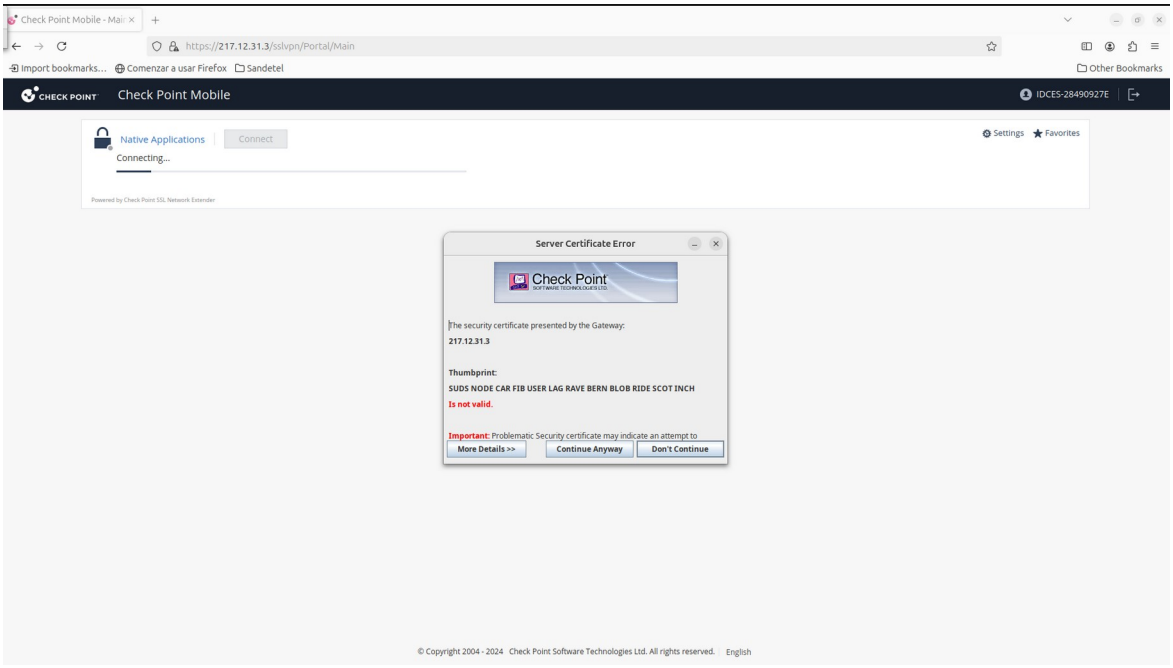
Igualmente en este caso nos pedirá que realicemos la instalación de "Check Point Mobile Access Portal Agent".



Adicionalmente la primera vez que realicemos la conexión se nos solicitará que validemos el certificado del servidor. Tanto por parte de “SSL Network Extender (SNX)” (pulsar “Yes”).



Como por parte de “Check Point Mobile Access Portal Agent” (pulsar “Continue Anyway”).



En veces sucesivas y tras realizar la autenticación solo será necesario pulsar el botón de “Connect” (1) y se establecerá la conexión. Si queremos que la conexión se establezca de forma automática tras la autenticación correcta, haremos clic en “Settings” (2):

Se han reportado casos en los que tras realizar la instalación previamente descrita cuando se pulsa el botón “Connect” aparece un error indicando que no está instalada o funcionando la aplicación “SSL Network Extender (SNX)”. En este caso podemos comprobar si efectivamente la aplicación SNX está arrancada y accesible:

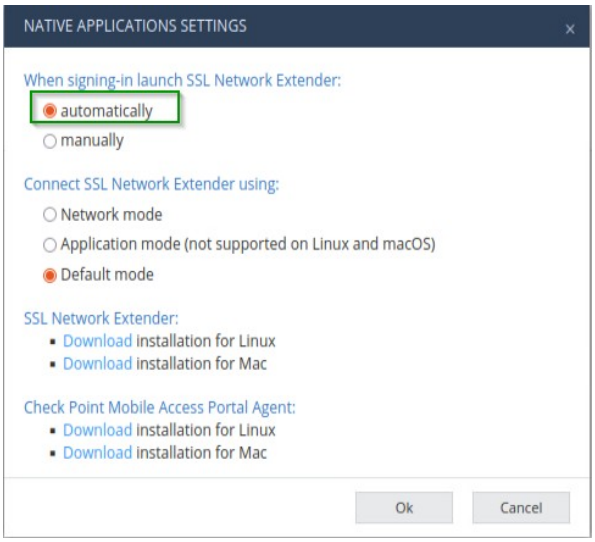
```
usuario@equipo:~$ ps ax|grep cshell

  2439 ?        Sl     1:21 java -jar /usr/bin/cshell/CShell.jar /tmp/cshell.fifo

usuario@equipo:~$ netstat -lptn

Proto  Recib Enviad Dirección local       Dirección remota      Estado      PID/Program name

....

tcp6       0      0 127.0.0.1:14186         :::*                    ESCUCHAR    2439/java
```

usuario@equipo:~$ wget -q -O- --no-check-certificate https://localhost:14186/id

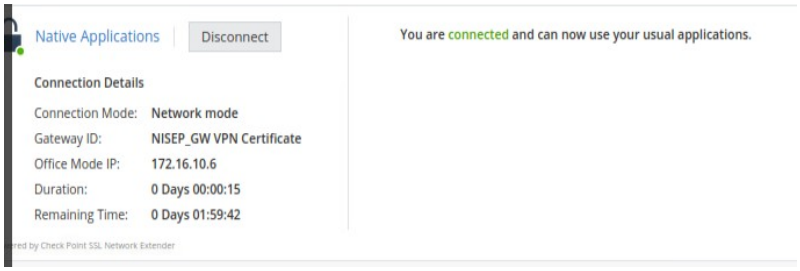
{"id":"a3655507-96c8-49c6-9514-e3f70412a730","version":800007049}

Y posteriormente acceder desde el navegador a la URL "https://localhost:14186/id" y aceptar el certificado ofrecido. Tras lo cual ya deberíamos poder conectarnos correctamente.

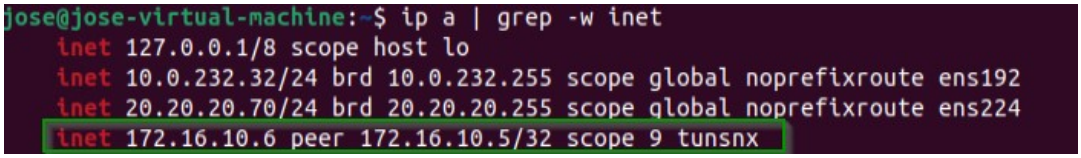
En Settings, seleccionaremos "automatically", para queremos que la conexión se establezca de forma automática tras la autenticación correcta:



Tras pulsar en "Connect", o tras ajustar la conexión automática tras autenticar, se realizará la conexión:



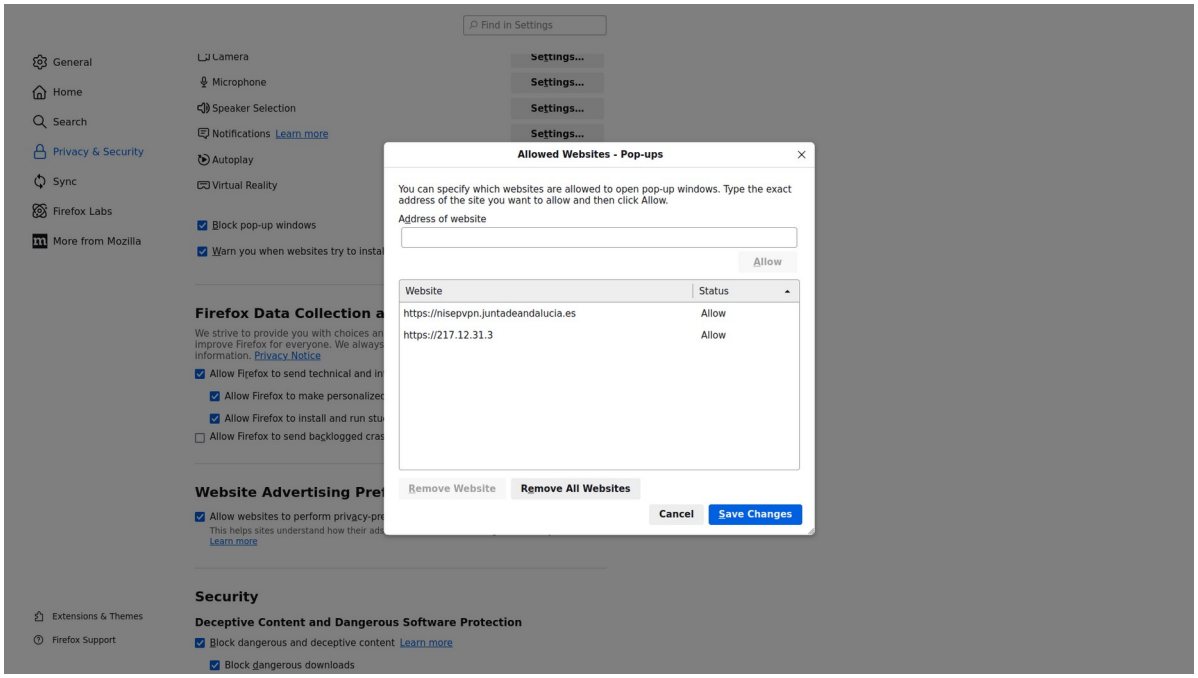
Si comprobamos en la terminal de Linux vemos que habrá aparecido una nueva interfaz "tunsnx":



Una vez establecida la conexión esta se mantendrá activa durante el periodo de tiempo indicado en "Remaining Time:". Cuando "Remaining Time:" llegue a 5min aparecerá una ventana emergente solicitando que nos volvamos a autenticar realizado lo cual volverá al valor inicial (cuando se estableció la conexión).

En caso de no hacerlo la conexión se cerrara cuando “Remaining Time:” llegue a cero.

Para poder llevar a cabo este procedimiento es necesario que en nuestro navegador estén permitidas las ventanas emergentes para la URL https://nisepvpn.juntadeandalucia.es.



6Desinstalación

Al realizarse conexión sin cliente, no es necesario desinstalar ningún paquete salvo que queramos desinstalar los paquetes de herramientas y aplicaciones mencionados en los prerrequisitos.

Junta de Andalucía

Consejería de la Presidencia,
Administración Pública e Interior