Departamento de Tecnología Electrónica
ESCUELA TÉCNICA SUPERIOR DE INGENIERÍA INFORMÁTICA

Laboratorio 4
VNPs: Open VPN y TINC

Enunciados de Prácticas de Laboratorio
Tecnologías Avanzadas de la Información

1. Introducción y objetivos

El uso de tecnologías VPN es fundamental para interconectar redes privadas a través de redes públicas de forma segura. En la teoría de esta asignatura se tratan ampliamente las VPNs y las técnicas de cifrado en las que se basan estas tecnologías. Para profundizar en los conocimientos teóricos se propone en este laboratorio la puesta en funcionamiento de dos tipos de VPNs, una centralizada (OpenVPN) y otra distribuida (TINC). La duración estimada de esta sesión de laboratorio es de **4 horas**.

Tanto OpenVPN como TINC son soluciones VPNs open source basadas en SSL. Con ellas se cubre un amplio rango de aplicaciones como: acceso remoto, unión de nodos remotos mediante VPN, seguridad Wi-Fi, balanceo de carga, etc. Su principal ventaja frente a otras soluciones comerciales es la facilidad y reducido coste de implantación. Ambas tecnologías operan en la capa 2 o 3 del modelo OSI uniendo mediante túneles todos los nodos distribuidos por la red. Se requiere una instalación tanto en el cliente como en el servidor y son compatibles con Linux, Windows, OSX, Android y algunos más.

En esta sesión de laboratorio el alumno debe poner operativas dos VPNs en el entorno virtual de laboratorio. Se desarrolla de manera guiada en las primeras secciones la instalación y la puesta en marcha básica de la VPN. Posteriormente se plantean tareas de mayor dificultad para realizar de manera no guiada, no siendo necesaria la realización de las últimas propuestas de configuración.

Para facilitar el desarrollo de la sesión de laboratorio se propone la instalación de los paquetes indicados en la tabla 1, donde se indica la máquina donde debe instalarlo.

 Paulino Ruiz de Clavijo Vázquez <paulino@dte.us.es>

Nombre del paquete	Descripción	Ubicación
xca	Utilidad gráfica para gestión de certificados digitales	Máquina local o máquina *Gateway* (requiere entorno gráfico)
openvpn	OpenVPN	Todas la máquinas
tinc	TINC	Todas la máquinas
mc	Recomendación: Administrador de archivos para consola de texto	Todas las máquinas

Tabla 1. Programas necesarios para la realización de la sesión de laboratorio.

2. Instalación de OpenVPN

La instalación de OpenVPN se realiza de manera similar a la de cualquier aplicación en Debian. La mayoría de los paquetes en Debian tras la instalación contienen una configuración mínima para la puesta en marcha del servicio correspondiente, como puede ser, el servidor *ssh* por ejemplo. En cambio, la puesta en funcionamiento de OpenVPN requiere una configuración manual, especificando para cada máquina el perfil que tendrá: servidor VPN, cliente VPN o ambos. Por ello el sistema de paquetes Debian no incluye una configuración predeterminada, pero facilita la configuración con una serie de ejemplos de configuración incluidos en la documentación del paquete.

Para realizar la sesión de laboratorio con mayor comodidad se recomienda la instalación de los paquetes adicionales de la tabla 1:

Tarea 1.- Debe realizar las siguientes instalaciones de paquetes para llevar a cabo todas las posteriores tareas:

T1.1.- Compruebe que tiene instalado el servidor *ssh* en todas las máquinas virtuales para poder realizar transferencias de ficheros entre máquinas. El paquete a instalar es *openssh-server*.

T1.2.- Instale el paquete *mc*, el cual es un administrador de archivos que funciona en la consola que permite conexiones remotas para copiar archivos entre diferentes máquinas de la red.

T1.3.- Instale el paquete *xca*, en la máquina *Gateway* o en la máquina anfitrión. Es una utilidad de gestión de certificados, aunque no es necesario facilitará en gran medida el desarrollo de la sesión de laboratorio.

A continuación se instalará OpenVPN, tras la instalación los archivos de configuración deben ubicarse en el directorio `/etc/openvpn` pero por defecto, no trae establecida ninguna configuración. El directorio `/usr/share/doc/openvpn` incluye documentación y ejemplos para la puesta en funcionamiento. En este mismo directorio hay un conjunto de *scripts* para generar las claves RSA y certificados, pero para mejorar la comprensión del proceso se recomienda el uso de XCA.

Tarea 2.- Instale el paquete *openvpn* en la máquina *Gateway*, como se ha comentado no trae ninguna configuración predeterminada, por lo que no se activará ningún servicio en la máquina.

T2.1.- Acceda a la carpeta `/usr/share/doc/openvpn` y encontrará toda la documentación y ejemplos disponibles para la configuración. Entrando en el directorio `examples` encontrará un directorio llamado `sample-config-files` con ejemplos para utilizar en la configuración tanto del cliente como el servidor.

T2.2.- Antes de la puesta en funcionamiento de OpenVPN será necesario crear los certificados digitales necesarios para que opere correctamente, llegados a este punto existen dos posibilidades:

1. La opción recomendada en esta sesión de laboratorio es el uso de XCA, ya que mostrará de una forma más clara como se están creando los certificados.
2. La opción rápida (no recomendada) es utilizar easy-rsa el cual debe haberse instalado automáticamente. Para ello debe seguir los pasos indicados en el *howto* de OpenVPN en la siguiente dirección: https://openvpn.net/community-resources/how-to. Si elige esta opción obvie la Tarea 3.- y la Tarea 4.-

2.1. Generación de los certificados digitales

OpenVPN opera utilizando certificados digitales en cada nodo de la VPN, incluido el propio servidor. Para asegurar la red VPN y administrar los certificados se utilizará una autoridad de certificación encargada de firmar todos los certificados y con posibilidad de incluir una lista de revocación (CRL). Todos estos componentes forman una infraestructura de clave pública (PKI) utilizada para operar en la VPN.

La fortaleza de la seguridad en la VPN recae en la clave privada de la autoridad de certificación, por ello debe mantenerse en lugar seguro. Los requerimientos de claves y certificados se pueden resumir como sigue:

- El administrador de la VPN crea su clave pública, su clave privada y un certificado digital que incluye su clave pública. Actuará como autoridad de certificación, por tanto, este certificado estará firmado por él mismo (autofirmado). El administrador debe mantener la clave privada de la autoridad de certificación en secreto.
- Para el servidor se crea una clave pública, una privada y un certificado que incluye la clave pública. La autoridad de certificación firma el certificado digital del servidor con su clave privada.
- Cada cliente de la VPN se genera su clave pública y su clave privada. La autoridad firma, para cada cliente, un certificado digital que incluye la clave pública del cliente en cuestión.
- El administrador publica para todos los clientes/servidores la clave pública de la autoridad en un certificado, para que así puedan validar todas las firmas digitales.

En la tabla 2 se muestran los componentes requeridos en cada uno de los equipos conectados a OpenVPN. Se puede resumir que cada equipo (incluido el servidor) dispondrá de tres claves: la clave pública de la autoridad de certificación, su propia clave pública y su clave privada. Además de los ficheros indicados, el servidor requiere unos parámetros extra, necesarios para realizar un intercambio seguro de claves utilizando el protocolo de intercambio de claves de *Diffie-Hellman*.

Contenido	Ubicación	Secreto
Clave privada de la autoridad de certificación	Ubicación de máxima seguridad, incluso *offline* en un medio extraíble.	**Sí**, sólo accesible al administrador de la VPN
Certificado de la autoridad (incluye la clave pública)	En todos los clientes y el servidor	**No**
Clave privada del servidor VPN	En el servidor con los permisos adecuados para evitar su copia	**Sí**, sólo accesible al servidor
Certificado firmado con la clave pública del servidor VPN	En el servidor	**No**
Clave privada de cada cliente	Cada clave sólo en el cliente correspondiente con los permisos adecuados para evitar su copia	**Sí**, sólo accesible para el cliente
Certificado firmado con la clave pública de cada cliente	Cada certificado sólo en el cliente correspondiente	**No**

Tabla 2. Ubicación de los certificados firmados y claves privadas necesarias.

Todos estos elementos se generarán a continuación con la herramienta XCA. Con esta herramienta se pueden realizar todos los pasos indicados anteriormente.

Tarea 3.- Instale el paquete *xca* desde el gestor de paquetes e inicie el programa. Se utilizará este programa para crear los certificados de la siguiente forma:

T3.1.- Inicie el programa *xca* y cree una nueva base de datos para almacenar sus certificados.

T3.2.- Cree una nueva autoridad de certificación encargada de firmar todos los certificados de los clientes que se conectarán a la VPN. Para ello, acceda a la pestaña Certificates y pulse el botón New certificate. Utilice la figura 1 para configurar correctamente las dos primeras pestañas:

- Cada alumno debe rellenar con su nombre y a apellidos el campo organizationalUnitName.
- El correo electrónico debe estar en el campo emailAddress.
- En el resto de pestañas deje con los valores predeterminados.

T3.3.- El siguiente paso es crear un certificado para el servidor. Para conseguirlo, cree un nuevo certificado y configure las diferentes opciones según se indica en la figura 2. Siga la figura 2 correctamente considerando los siguientes requerimientos:

- El certificado debe estar firmado por la autoridad certificadora.
- El campo de uso de clave (*Key Usage*) debe contener *Digital Signature* y *Key Encipherment*
- El campo extendido de uso (*Extended Key Usage*) debe contener *TLS Web Server Authentication*.

T3.4.- En el caso de los clientes se debe repetir el proceso pero con otras opciones. Debe crear un certificado para el cliente firmado por la autoridad certificadora y con la configuración mostrada en la figura 3. Los requerimientos son los siguientes:

- El certificado debe estar firmado por la autoridad certificadora.
- El campo de uso de clave (*Key Usage*) debe contener *Digital Signature* y *Key Agreement*
- El campo extendido de uso (*Extended Key Usage*) debe contener *TLS Web Client Authentication*.

La herramienta XCA mantiene todos los datos sobre los certificados en un único fichero que actúa como

base de datos. Ahora se deben extraer las diferentes claves privadas y certificados en diferentes ficheros para incluirlos en la configuración de OpenVPN.

Tarea 4.- Se procederá a la exportación de los certificados y de las claves privadas de la siguiente forma:

> **T4.1.-** Se exportarán las claves privadas del servidor y del cliente. No debe exportar la clave privada de la autoridad, ésta sólo se utiliza para el firmado y debe permanecer bajo un máximo nivel de seguridad. Para ello acceda a la pestaña Private Keys y seleccione las claves del cliente y el servidor y use el botón Export. Use las opciones predeterminadas en la exportación de los ficheros, se generarán ficheros con extensión *.pem*.

Ahora se procederá a la exportación de los certificados desde la pestaña Certificates. Seleccione todos los certificados, incluido la autoridad, y expórtelos con las opciones por defecto, obtendrá diferentes ficheros con extensión *.crt*. Estos ficheros contienen las claves públicas.

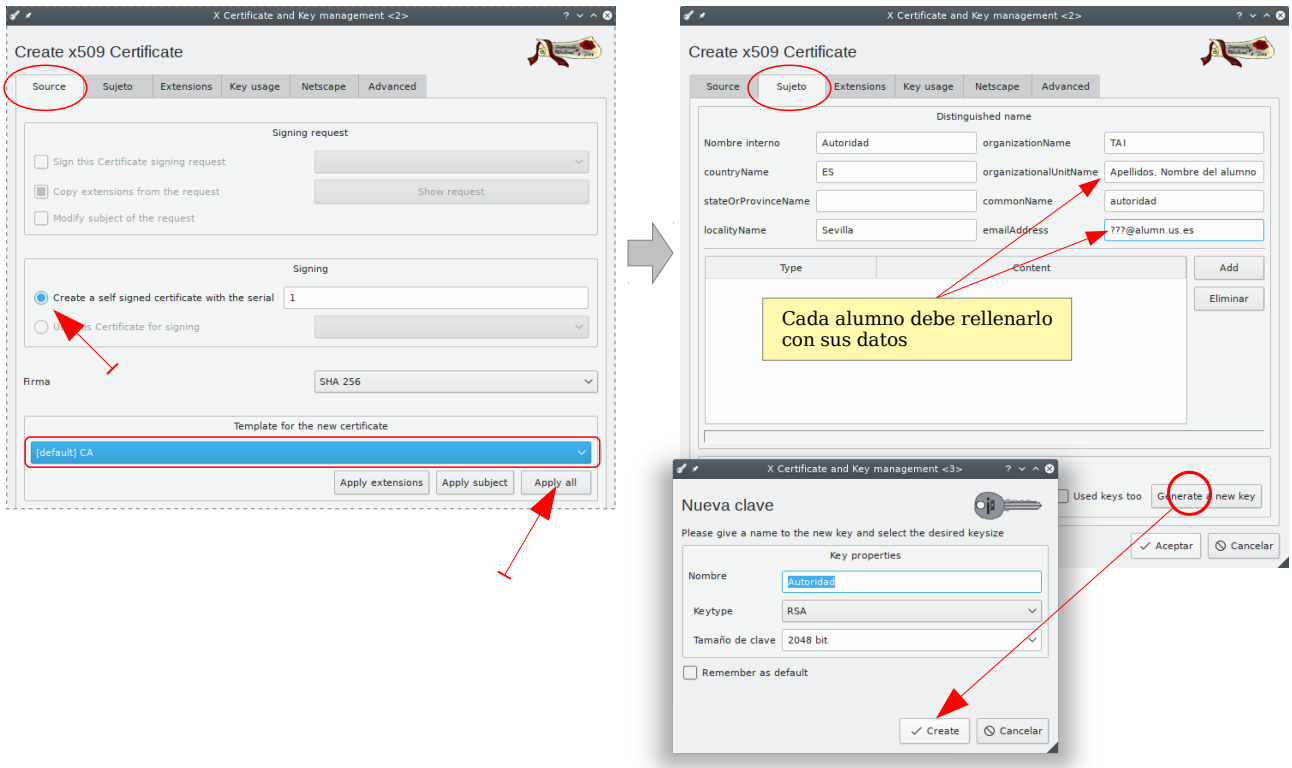

Figura 1. Generación de la autoridad de certificación.

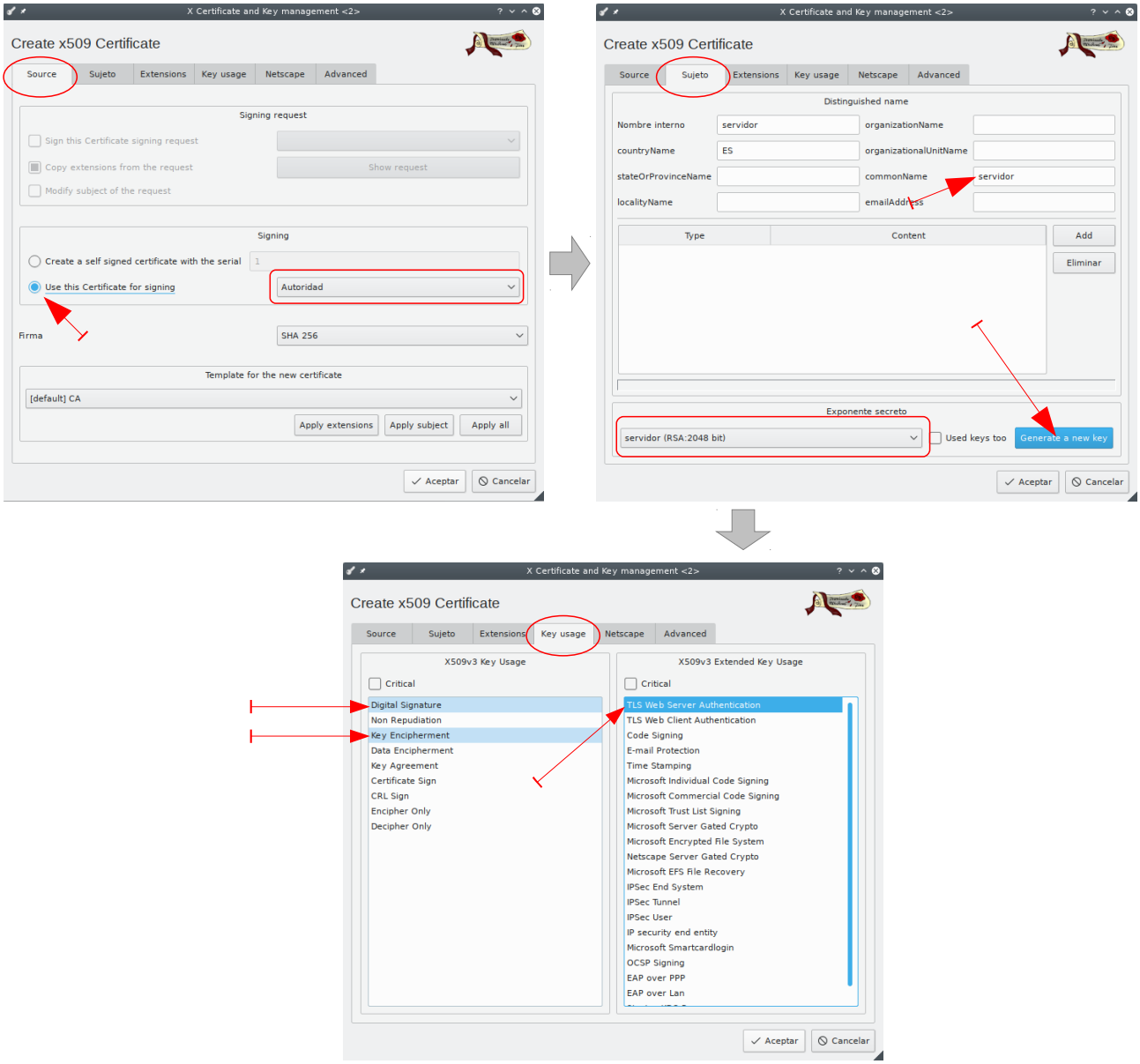

Figura 2. Generación del certificado del servidor.

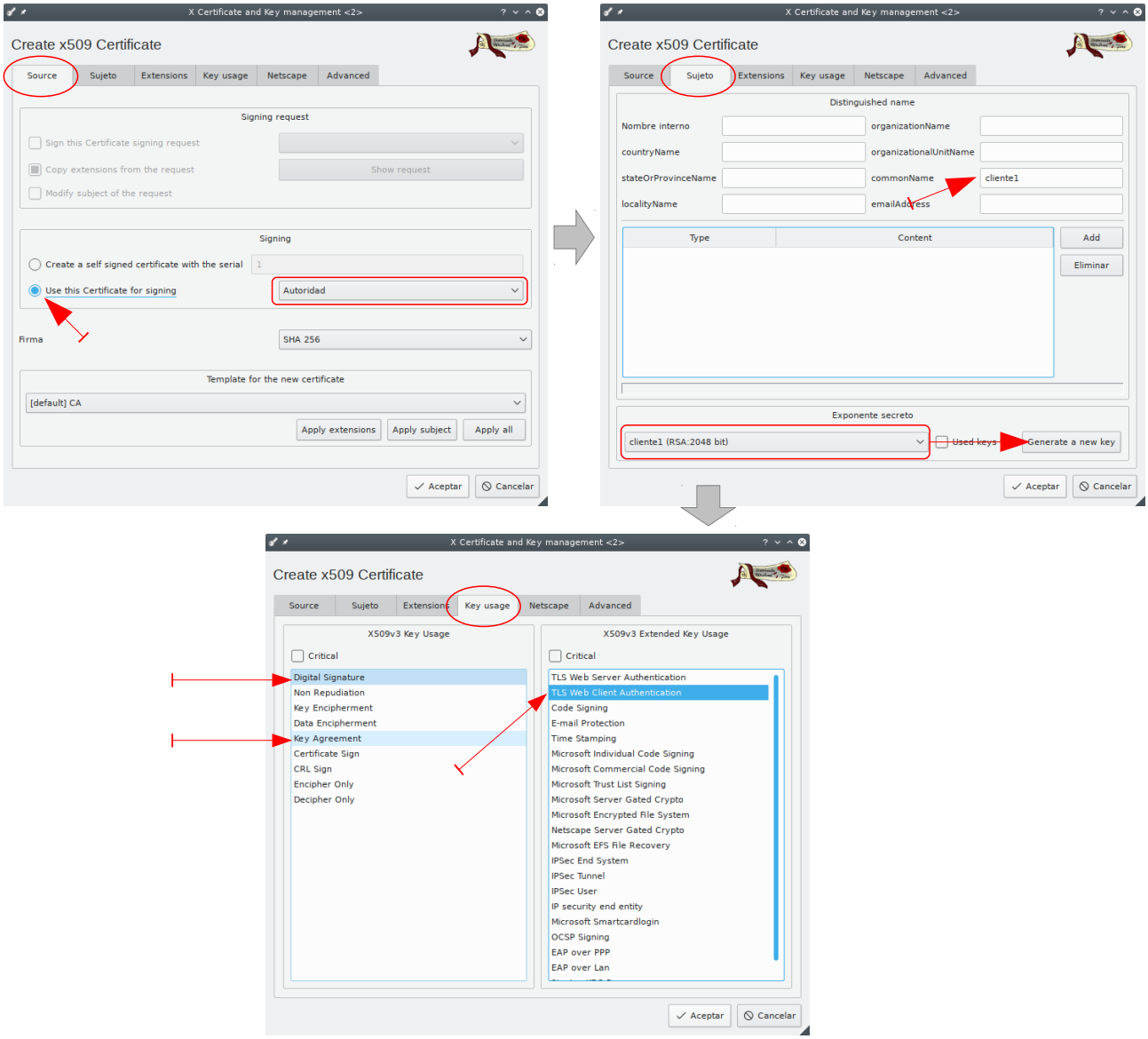

Figura 3. Generación del certificado del cliente.

2.2. Configuración del servidor y los clientes

Los ficheros obtenidos anteriormente se deben distribuir adecuadamente entre los clientes y el servidor OpenVPN. Además, hay que asegurarse de proteger adecuadamente aquellos que contienen las claves privadas, sólo deberían ser accesibles por el programa OpenVPN o el usuario root en su caso, en cada uno de los equipos.

Se procederá a la configuración del servidor y de los clientes, utilice la figura 4 para tener una visión global de cómo deben quedar los certificados y claves en cada una de los equipos virtuales.

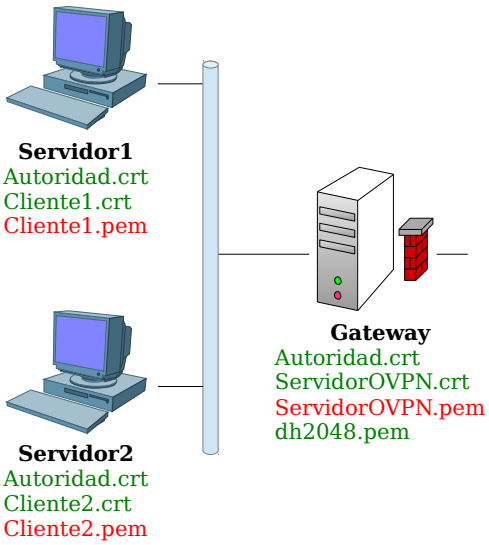

Figura 4. Ubicación de certificados y claves en la VPN.

Tarea 5.- Para comenzar la configuración del servidor asegúrese de tener instalado el paquete *openvpn.*

T5.1.- La configuración del servidor requiere un fichero adicional llamado parámetros de *Diffie-Hellman* utilizados para el intercambio seguro de claves privados. Desde XCA genere este fichero usando el menú Extra → Generate DH parameter. Obtendrá un fichero necesario sólo en el servidor.

T5.2.- En el servidor debe copiar 4 ficheros en la ubicación `/etc/openvpn`, deberá transferirlos por *ssh*, puede utilizar el comando *scp* o el programa *mc* o *filezilla*. Los ficheros son los indicados en la tabla 3, los nombres pueden variar según como los hubiera guardado de la tarea anterior.

Fichero	Contenido
Autoridad.crt	Certificado de la autoridad certificadora con su clave pública
dh2048.pem	Parámetros Diffie-Hellman generados en T5.1.-
Servidor.crt	Certificado del servidor con la clave pública firmado por la autoridad de certificación
Servidor.pem	Clave privada del servidor

Tabla 3. Ficheros necesarios en el servidor OpenVPN.

T5.3.- Copie el fichero /usr/share/doc/openvpn/examples/sample-config-files/server.conf.gz que contiene una configuración de ejemplo a /etc/openvpn y descomprímalo con el programa gunzip desde la interfaz de comandos.

T5.4.- Ahora debe editar el fichero de configuración /etc/openvpn/server.conf y establecer los nombres de los ficheros de certificados a los nombres adecuados cambiando las líneas indicadas a continuación:

```
# Any X509 key management system can be used.
# OpenVPN can also use a PKCS #12 formatted key file
# (see "pkcs12" directive in man page).
ca Autoridad.crt
cert Servidor.crt
```

```
key Servidor.pem  # This file should be kept secret

# Diffie hellman parameters.
# Generate your own with:
#   openssl dhparam -out dh1024.pem 1024
# Substitute 2048 for 1024 if you are using
# 2048 bit keys.
dh dh2048.pem

# ¡Comente esta opción!
# tls-auth ta.key 0
```

Código 1. Cambios en el fichero de configuración para el servidor OpenVPN.

T5.5.- Como administrador liste el directorio `/etc/openvpn` con el comando `ls -l`. Cambie los permisos del todos los ficheros asegurándose que pertenezcan al usuario *root* y que sólo el usuario *root* tenga permiso de lectura sobre el fichero con la clave privada del servidor.

T5.6.- Ejecute el comando `openvpn server.conf` para iniciar el servidor desde la línea de comandos. Este inicio es temporal para comprobar que no existen errores de configuración. Para parar el servidor pulse CTRL+C.

T5.7.- Inicie el servicio OpenVPN mediante el comando `systemctl start openvpn@server`. Si todo ha ido bien, con el comando `ip a` aparecerá una nueva interfaz llamada `tun0` con una IP asignada. Ésta es la red interna de la VPN, perteneciendo esta IP al servidor. Si no inicia correctamente, use el comando `systemctl status openvpn@server` para leer los mensajes de error y corregirlos.

T5.8.- En un terminal visualice la bitácora del sistema con el comando `journalctl -f -u openvpn@server`, verá los cambios en tiempo real mientras trabaja en el resto de tareas y le ayudará a detectar problemas cuando otros clientes se conecten al servidor.

Para continuar con la configuración hay que añadir los clientes en la VPN. Cada uno de los clientes necesitará tres ficheros para poder unirse a la VPN:

- Certificado de la autoridad certificadora con su clave pública: *Autoridad.crt*
- Certificado del cliente con la clave pública y firmado por la autoridad: *Cliente.crt*
- Clave privada del cliente: *Cliente.pem*

Tarea 6.- Para configurar un cliente siga los siguientes pasos:

T6.1.- Asegúrese que tiene instalado el paquete *openvpn* en el cliente.

T6.2.- Copie el fichero de configuración de ejemplo para los clientes desde la ubicación `/usr/share/doc/openvpn/examples/sample-config-files/client.conf` en el directorio `/etc/openvpn`.

T6.3.- Transfiera por *ssh* o con *mc* los tres ficheros necesarios a la ubicación `/etc/openvpn` del cliente.

T6.4.- Establezca los permisos de los ficheros del directorio `/etc/openvpn` adecuadamente como se hizo en T5.5.-.

T6.5.- Edite el fichero `/etc/openvpn/client.conf` estableciendo los valores correctos para los certificados y claves tal y como se mostró en el código 1. Considere que ahora los dos últimos ficheros tienen nombres diferentes.

T6.6.- También en el mismo fichero de configuración debe establecer la dirección IP del servidor

VPN, busque en este fichero la directiva `remote` para establecerla a `remote 192.168.7.1`.

T6.7.- Inicie OpenVPN en una consola mediante el comando `openvpn client.conf` para ver si inicia correctamente o muestra mensajes de error. Este inicio es temporal para comprobar que no existen errores de configuración.

T6.8.- Sin parar la ejecución del paso anterior, use una nueva consola y mediando el comando `ip a` compruebe si se ha conectado la interfaz `tun0` y tiene una IP asignada en caso contrario puede tener mal generados los certificados o la configuración.

T6.9.- Si el paso anterior fue correcto, pare la consola donde se está ejecutando OpenVPN usando CTRL+C e inicie el servicio de manera correcta `systemctl start openvpn@client`. Si no inicia, use el comando `systemctl status openvpn@client` para solucionar el problema.

T6.10.- Acceda a la bitácora del servicio OpenVPN para ver los mensajes de información y/o error tanto en el cliente como en el servidor con el comando `journalctl -u openvpn@server` y `journalctl -u openvpn@server` y deberá interpretar el resultado de la negociación entre el cliente y el servidor de la VPN.

Si tiene problemas de conexión por parte del cliente lea la última sección de este documento donde se comentan algunos problemas típicos que surgen durante el proceso de configuración (C1-C3).

Tarea 7.- Añada la segunda máquina de la red interna a la VPN generando nuevos certificados y repitiendo los pasos de la tarea anterior.

Tarea 8.- En el servidor VPN visualice el contenido del fichero del directorio /etc/openvpn llamado openvpn-status.log. Interpretando correctamente el contenido realice lo siguiente:

T8.1.- Ejecute el comando *ping* desde el servidor a los clientes a través de la VPN.

T8.2.- Ejecute el comando *ping* desde un cliente a otro cliente a través de la VPN.

T8.3.- Si en el paso anterior los paquetes no llegaron entre los diferentes equipos de la VPN. Edite el fichero de configuración del servidor VPN y busque una directiva que habilite la visibilidad entre los diferentes clientes. Tras los cambios debe reiniciar el servicio OpenVPN tanto en el servidor como en todos los clientes.

2.3. Revocación de certificados

Una situación habitual en la administración de cualquier VPN es la expulsión de equipos de la red. Independientemente del motivo (claves comprometidas, bajas de equipos, etc.), OpenVPN implementa este procedimiento usando una lista de revocación de certificados (CRL en inglés). Un CRL es una parte esencial de un PKI y no es más que la lista de certificados revocados firmado por la autoridad de certificación. Desde XCA generar el listado CRL es fácil. En el siguiente ejemplo revocaremos el certificado de la segunda máquina virtual y se configurará el servidor para operar correctamente con el CRL.

Tarea 9.- Inicie XCA y revoque el certificado de la segunda máquina virtual. Se puede revocar seleccionando el certificado y usando el menú flotante que aparece con el botón derecho del ratón sobre el certificado.

T9.1.- Ahora seleccione el certificado de la autoridad de certificación y vuelva a desplegar el menú con el botón derecho. Aparecerá un submenú CA → Generate CRL.

T9.2.- En la pestaña Revocation lists aparecerá la lista recién creada, use el botón exportar para generar el fichero CRL, establezca el nombre del fichero a *AutoridadCRL.pem*.

Tarea 10.- El último paso es cambiar la configuración del servidor OpenVPN.

T10.1.- Copie el fichero CRL llamado *AutoridadCRL.pem* en el directorio /etc/openvpn del servidor.

T10.2.- Edite la configuración del servidor (fichero /etc/openvpn/server.conf) y añada la directiva indicada en el código 2 con el nombre del fichero CRL.

```
ca Autoridad.crt
cert Servidor.crt
key Servidor.pem
crl-verify AutoridadCRL.pem  # Este es fichero contiene la lista de certificados
                             # revocados
```

Código 2. Configuración del listado CRL en OpenVPN.

T10.3.- Reinicie el servicio OpenVPN del servidor con `systemctl restart openvpn@server` y utilice el comando `journalctl -f -u openvpn@server` para observar el comportamiento del servidor. Debe reiniciar los clientes ya que tardan cierto tiempo en reconectar al servidor.

T10.4.- ¿Observa el aviso en el servidor sobre el cliente con el certificado revocado? ¿Que ocurriría si se revoca el certificado del servidor?

2.4. Modos de funcionamiento de OpenVPN (opcional)

Las siguientes tareas se consideran opcionales ya que algunas presentan cierta dificultad. Se propone que tras conseguir el funcionamiento básico de OpenVPN con las tareas anteriores, se pruebe ahora diversas configuraciones y modos de funcionamiento avanzados. Si lee detenidamente los comentarios del fichero de configuración del servidor, observará multitud de ejemplos y directivas comentadas que alteran el funcionamiento predeterminado de OpenVPN, tanto en los clientes como en el servidor.

Las siguientes tareas debe resolverlas cambiando los ficheros configuración del servidor y los clientes según los ejemplos indicados en los propios ficheros de configuración. Haga una copia de seguridad de los ficheros de configuración antes de afrontar las siguientes tareas.

Tarea 11.- ¿Como está funcionando su VPN usando UDP o TCP? Averígüelo y cambie el modo de funcionamiento. Use el comando `ss` para localizar el puerto donde está el servidor.

Tarea 12.- En la configuración realizada de OpenVPN se comentó la directiva `tls-auth`, búsquela en el archivo de configuración y lea el motivo por el cual no se debe comentar. ¿Tras el cambio en la tarea Tarea 11.- es necesaria activarla?

Tarea 13.- Opcional-4a: Establezca una IP fija para cada cliente, para ello mire el ejemplo indicado donde se utilizan ficheros ubicados en un directorio llamado *ccd*.

T13.1.- Añada la configuración correspondiente en el servidor DNS para que reconozca equipos en la red VPN dando un nombre distintivo a cada equipo de la VPN: *gateway.vpn*, *servidor1.vpn* y *servidor2.vpn*.

T13.2.- Ejecute el comando *ssh* utilizando estos nombres de hosts para ver si la VPN opera correctamente.

3. TINC

TINC es una solución software para la creación de VNPs distribuidas (mesh). Este software es capaz de autoconfigurar las rutas de manera dinámica para que todos los clientes de la VPN sean accesibles entre sí. TINC distingue dos tipos de nodos, aquellos que permiten a otros nodos que se conecten a él (nodo maestro/servidor) y nodos clientes. La principal diferencia con OpenVPN es la existencia de tantos nodos de tipo servidor como se deseen, así la red queda asegurada ante posibles desconexiones de servidores. Otra característica de este tipo de VPN es que cada nodo no tiene por qué tener asignada una única dirección IP, si no que puede ser responsable de una subred completa, dando acceso a la VPN a esa misma red, aunque este tipo de configuración no se tratará en este laboratorio.

La autoconfiguración de esta VPN se realiza intercambiando claves públicas entre los clientes y servidores que forman la red y usando un canal de comunicación para intercambiar metadatos sobre la red. Usando el cifrado asimétrico, TINC intercambia claves de cifrado simétricos para usarlo en la comunicación de datos entre los nodos. La figura 5 muestra un ejemplo de funcionamiento de una VPN con TINC, la conexión de los clientes a la red se inicia contra los dos nodos maestros marcados con una M. Inicialmente los clientes abren un canal de comunicación para intercambiar metadatos sobre la red (indicados en rojo). Esta comunicación de metadatos incluye la información necesaria para que los nodos puedan establecer una comunicación directa entre sí. Esta comunicación directa están indicadas en verde en la figura y corresponde a intercambio de datos entre nodos. En caso de estar dos nodos tras algún tipo de *firewall* y no poder comunicarse directamente, los nodos maestros intentan hacer de puente (relay) entre dichos nodos, este tipo de comunicación está indicada en naranja en la figura.

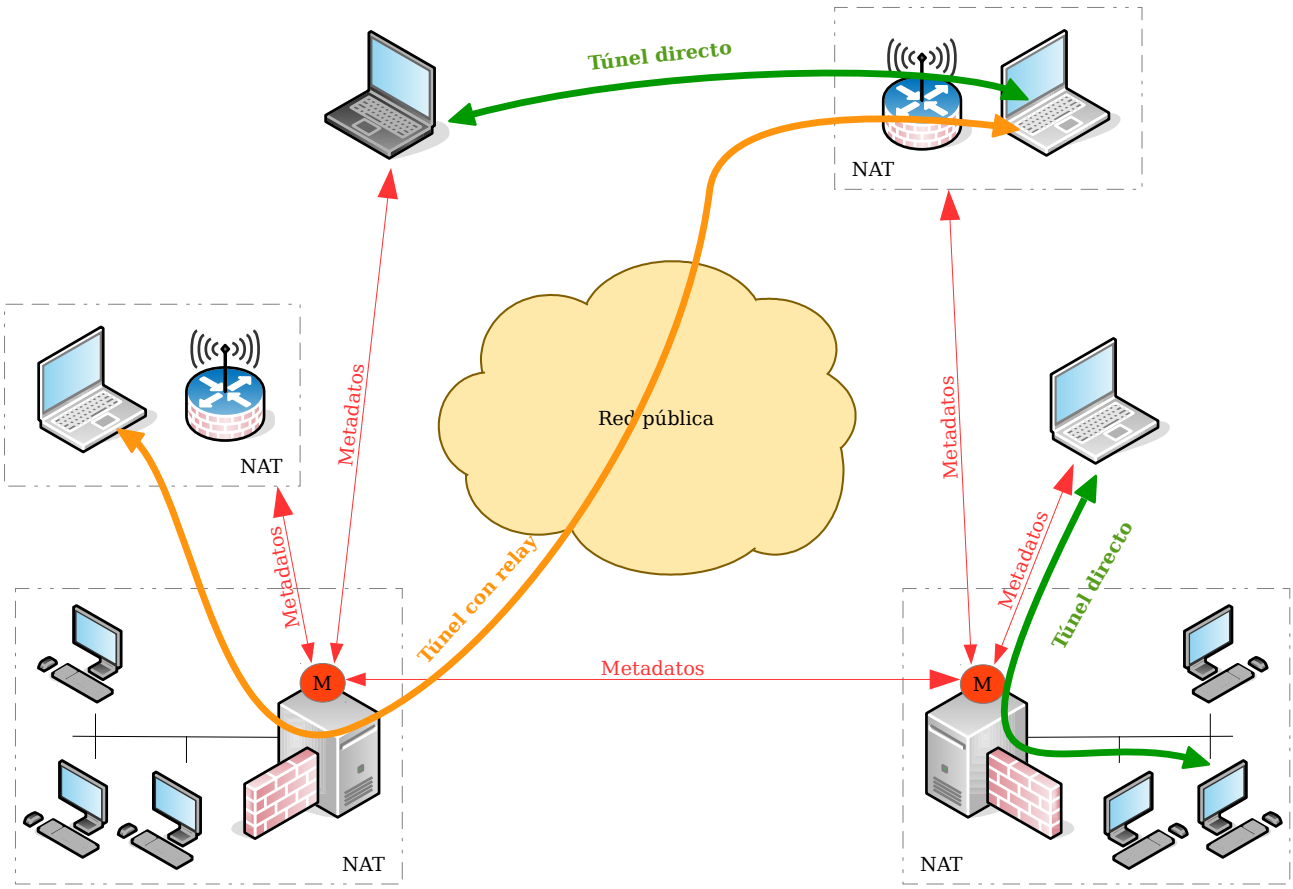

Figura 5. Ejemplo de comunicaciones en una VPN mesh con TINC.

En esta parte del laboratorio cada alumno no creará su propia VPN como se hizo con OpenVPN. Se propone conectarse a una única VPN creada por el profesor en la que los alumnos añadirán sus máquinas virtuales como nodos. Una vez conectados a la VPN de la asignatura, se proponen una serie de tareas para verificar el funcionamiento de VPN. Siga los siguientes pasos indicados a continuación para realizar la configuración de TINC:

Tarea 14.- Agregue reglas al *firewall* del *Gateway* que permita a los equipos internos (*vbox1* y *vbox2*) conectar a equipos exteriores al puerto 655 usando el protocolo TCP. Compruebe el correcto funcionamiento de esta regla usando el comando `nc` conectando a un equipo externo en dicho puerto.

Tarea 15.- Se procederá a agregar el equipo *Servidor1* a la VPN creada por el profesor y llamada *redtai*. Para conectar los equipos restantes deberá seguir el mismo procedimiento:

T15.1.- Instale el paquete *tinc* en el equipo virtual *Servidor1*.

T15.2.- La conexión o creación de VPNs en TINC se consigue dando nombres a las redes. Cada nombre de red corresponde a un directorio dentro de */etc/tinc*. Para crear la nueva configuración para conectarse a *redtai* basta con crear el directorio */etc/tinc/redtai* con el comando `mkdir`.

T15.3.- Una vez creado el directorio debe crear un archivo de configuración dentro de éste mediante `nano /etc/tinc/redtai/tinc.conf` cuyo contenido debe ser el siguiente:

```
Name = minombre
AddressFamily = ipv4
ConnectTo = profesor
```

Código 3. Configuración inicial de conexión a redtai con TINC.

T15.4.- En la primera línea del código anterior sustituya *minombre* por un nombre a su elección que sea único para toda la VPN. **Importante:** Este nombre no puede contener caracteres especiales ni guiones, sólo letras y números.

La última línea del fichero anterior contiene la directiva *ConnectTo*. Esta directiva indica un nodo maestro con el que intercambiar metadatos sobre la red distribuida. Inicialmente sólo está disponible el nodo del profesor, pero es posible añadir a los compañeros para mantener la VPN operativa en caso de desconexión del nodo inicial, para ello, deberá añadir líneas adicionales con los nodos e intercambiar los ficheros y se abordará al final de este laboratorio. Se procederá inicialmente a conectar a la VPN usando únicamente el nodo del profesor.

Tarea 16.- Para conectar al nodo maestro *profesor* es necesario conocer su dirección IP pública y su clave pública. Toda esta información deberá estar en un fichero llamado igual que el nodo al que se conectará, en este caso *profesor*.

T16.1.- Cree un directorio nuevo para almacenar los ficheros de los nodos maestros con `mkdir /etc/tinc/redtai/hosts` y cree un nuevo fichero dentro llamado *profesor*. Copie lo siguiente en dicho fichero:

```
Address = 150.214.141.189
Subnet = 10.0.20.0/24
Port = 80

-----BEGIN RSA PUBLIC KEY-----
MIICCgKCAgEAz63id6Z7ECGC8aUn3/UWx1WkbqhKPvg9kueeOUh41Fzu78hobt+U
HuJMdfekBhlKHTvU3CccFrCbNctzhjuwCoHAyNGa2pu176/T2QWxHOa832d5RMqs
HJZnIY21nd4Jw8/bYsBCoCRM2HNs1IEbjN4Cy7sMgSQyUvEwwWIXGu2Y4ILdjry3
RGWiO3/FGnixIM5pJJhq9XG/l0xVpbHJNxOAxAgXyr4TAIuEBsX2/deMSVCqPILf
IuSbinMBuzcszpWD09QhJ3SMI4NMplZITUSxVyNILbJLBjNcn17Scim3F+Qdun2r
eCRJpu9JVAQ813tW4KV7pzuv/gIABbYViKzXqUUZbNm3EID/psYf965syNt3tZeZ
svr/BETBOBPJWNdJ9HeczmiGEnCfoncXMYuutN5jx2Aqn9bLxR92LlQaxbZ7QsYR
biqJKJjaVZtEaF3Yg7mtLYiwp4qdio6I9GhwV3jCW3tkX3ODYTy421NJBn8hTn14
W9AqnWpRVa9y+4QaaIuTvAC54suN7eqItmNjvyYbaga2imN8s5HH1hm55fMVqqzR
lL0zXoQVV5xa3GdpHCFlzPCqGkRbuY4anJ1RT5GcBJInwWIpxTpGSivjHetg7QB9
0yjCLlq/iEgqbmZKFeGs9fBaWeMgyYz9Nx1YSD1/wCd7CN7CWMyLw+0CAwEAAQ==
-----END RSA PUBLIC KEY-----
```

Código 4. Fichero profesor para la conexión con el nodo inicial.

T16.2.- Ahora el siguiente paso es crear una configuración para nuestro nodo cliente y un fichero con la clave pública, similar al mostrado paso anterior.

T16.3.- Cree un fichero nuevo en */etc/tinc/redtai/hosts* exactamente con el nombre indicado en la directiva *name* del código 3. Este fichero debe contener únicamente la dirección IP de la VPN que usará el equipo. Es importante no generar conflictos de direcciones IP, por ello, solicite al profesor 3 direcciones IP para sus máquinas. Cree el fichero con el siguiente contenido (sustituyendo X por la IP asignada):

```
Subnet = 10.0.20.X/32
```

Código 5. Fichero local con la dirección IP estática asignada al nodo cliente.

T16.4.- El siguiente paso es generar y anexar a esta configuración la clave pública. Esto se puede realizar automáticamente con el comando: `tincd -n redtai -K4096`. ¿En que fichero se ha generado la clave privada?, edite dicho fichero para ver su contenido.

T16.5.- Vuelva a abrir el fichero creado en el paso T16.3.- y compruebe si se ha anexado una clave pública.

T16.6.- Envíe este fichero o el contenido del mismo al profesor para que incluya este nodo en la VPN.

Llegado a este punto la red VPN no está operativa, queda indicar como configurar el interfaz de túnel que se creará , para ello, TINC ejecuta automáticamente el *script tinc-up* cuando se conecta a la VPN. En este *script* se debe configurar el adaptador de red con la IP asignada. Este *script* permite añadir rutas u otra configuración adicional a la red, pudiéndose alcanzar así redes adicionales a través de la VPN. Del mismo modo, en la desconexión de la VPN, TINC ejecuta el *script tinc-down*, en el cual se debe desconfigurar la interfaz y eliminar cualquier ruta establecida previamente.

Tarea 17.- Entre en el directorio */etc/tinc/redtai* y cree dos ficheros: *tinc-up* y *tinc-down* con el contenido mostrado a continuación:

```
#!/bin/sh
ip link set $INTERFACE up
ip address add 10.0.20.X/24 dev $INTERFACE
```

Código 6. Script tinc-up para configuración del adaptador túnel de la VPN.

```
#/bin/sh
ip addr del 10.0.20.X dev $INTERFACE
ip link set $INTERFACE down
```

Código 7. Script tinc-down para desconfigurar la VPN.

T17.1.- Estos *scripts* necesitan tener permiso de ejecución para ser ejecutados por TINC debe use el comando: `chmod +x tinc-up tinc-down` para conseguirlo.

T17.2.- Para comprobar si se ha configurado correctamente se ejecutará TINC en modo de depuración en un terminal. En un nuevo terminal ejecute el comando `tincd -n redtai -D -d5`. Considere que este terminal se quedará bloqueado por TINC y no se puede parar ni usando CONTROL+C.

T17.3.- Desde otro terminal use el comando *ping* hacia 10.0.20.1 que es el equipo del profesor y así comprobar si está conectado a la VPN. Si no funciona debe revisar los mensajes de depuración del terminal donde está ejecutándose TINC.

T17.4.- Para parar TINC cuando está modo de depuración, debe ejecutar el comando `pkill tincd` desde otro terminal.

T17.5.- Para iniciar la red como servicio del sistema ejecute el comando `systemctl start tinc@redtai` y compruebe con `ip a` si aparece una interfaz llamada *redtai* con la IP correspondiente.

T17.6.- Para automatizar el inicio de la VPN con el inicio del sistema debe ejecutar `systemctl enable tinc@redtai`. Compruebe si funciona reiniciando la máquina.

Una vez conectada una máquina a la VPN debe repetir le proceso para añadir las restantes. Además, se propone como ejercicio hacer un escaneo de la red para localizar a los compañeros que ya están en la VPN y buscar un equipo oculto que contiene un Wiki.

Tarea 18.- Añada el equipo *Servidor2* y el *Gateway* a la VPN, para ello solicite dos IPs adicionales al profesor si no se las asignaron con anterioridad.

T18.1.- Utilizando los conocimientos adquiridos en el primer tema de esta asignatura, escanee la VPN intentado localizar los equipos *Servidor1* y *Servidor2* de otros compañeros. Compruebe si sus compañeros han establecido un mínimo de seguridad en sus máquinas virtuales cambiando la clave por defecto.

T18.2.- Opcional-4b: Intente localizar un equipo en la VPN que contiene un Wiki, una vez que lo localice, navegue el Wiki y deje una reseña indicando su nombre y como lo ha encontrado. Use el ejemplo existente en la propia Wiki y no borre las reseñas de sus compañeros.

3.1. Instalación de un nodo maestro (opcional)

En esta sección se muestra como instalar un nodo maestro que permita salvaguardar la red cuando el

nodo del profesor no esté disponible. Este nodo maestro debe ejecutarse en un equipo que tenga una dirección IP pública conocida, por ello, debe realizarse en el equipo *gateway*.

Tarea 19.- Opcional-4c: Edite el fichero */etc/tinc/redtai/hosts/minombre* y añada la directiva *Address* con su dirección IP pública, fíjese como se ha hecho en el código 4.

T19.1.- Este fichero debe intercambiarlo con algún compañero que haya realizado el mismo procedimiento. Puede utilizar la propia Wiki existente en la VPN para pegar el contenido de estos ficheros y poder intercambiarlos. Suba el contenido de este fichero al Wiki de la VPN.

T19.2.- Use el fichero TINC con la clave pública de algún otro compañero, cópielo a */etc/tinc/redtai/hosts*. A partir de este momento su compañero puede conectarse para usar su equipo como nodo maestro.

T19.3.- Una vez intercambiadas las claves públicas edite la configuración de TINC en */etc/tinc/redtai/tinc.conf* y añada tantas directivas *ConnectTo* como compañeros con los que intercambie las claves públicas. Fíjese en el ejemplo:

```
Name = raspberry
AddressFamily = ipv4
ConnectTo = profesor
ConnectTo = eva
ConnectTo = francis
ConnectTo = berta
```

Código 8. Fichero tinc.conf con conexión a múltiples nodos.

4. FAQ y recomendaciones

C1: Para comprobar si un certificado está firmado correctamente ejecute el siguiente comando.

```
openssl verify -CAfile ca.crt client1.crt
```

C2: En caso de no iniciar correctamente el servicio VPN, la interfaz tun no parecerá, debe comprobar lo ocurrido en la bitácora del sistema /var/log/syslog. Si no hay suficiente información puede indicar a *OpenVPN* que muestre más información cambiando en el fichero el configuración del servidor el nivel de la variable verb, se recomienda no pasar de 4.

C3: Si en el fichero /var/syslog aparecen errores del tipo TLS Error el principal motivo puede ser una generación de certificados incorrecta. Compruebe que los certificados contienen alguna de la combinación de la tabla (use el botón Show Details de XCA):

Nodo	Key usage	Extended key usage
Cliente	digitalSignature	TLS Web Client Authentication
	keyAgreement	
	digitalSignature, keyAgreement	

Servidor	digitalSignature, keyEncipherment	TLS Web Server Authentication
	digitalSignature, keyAgreement	