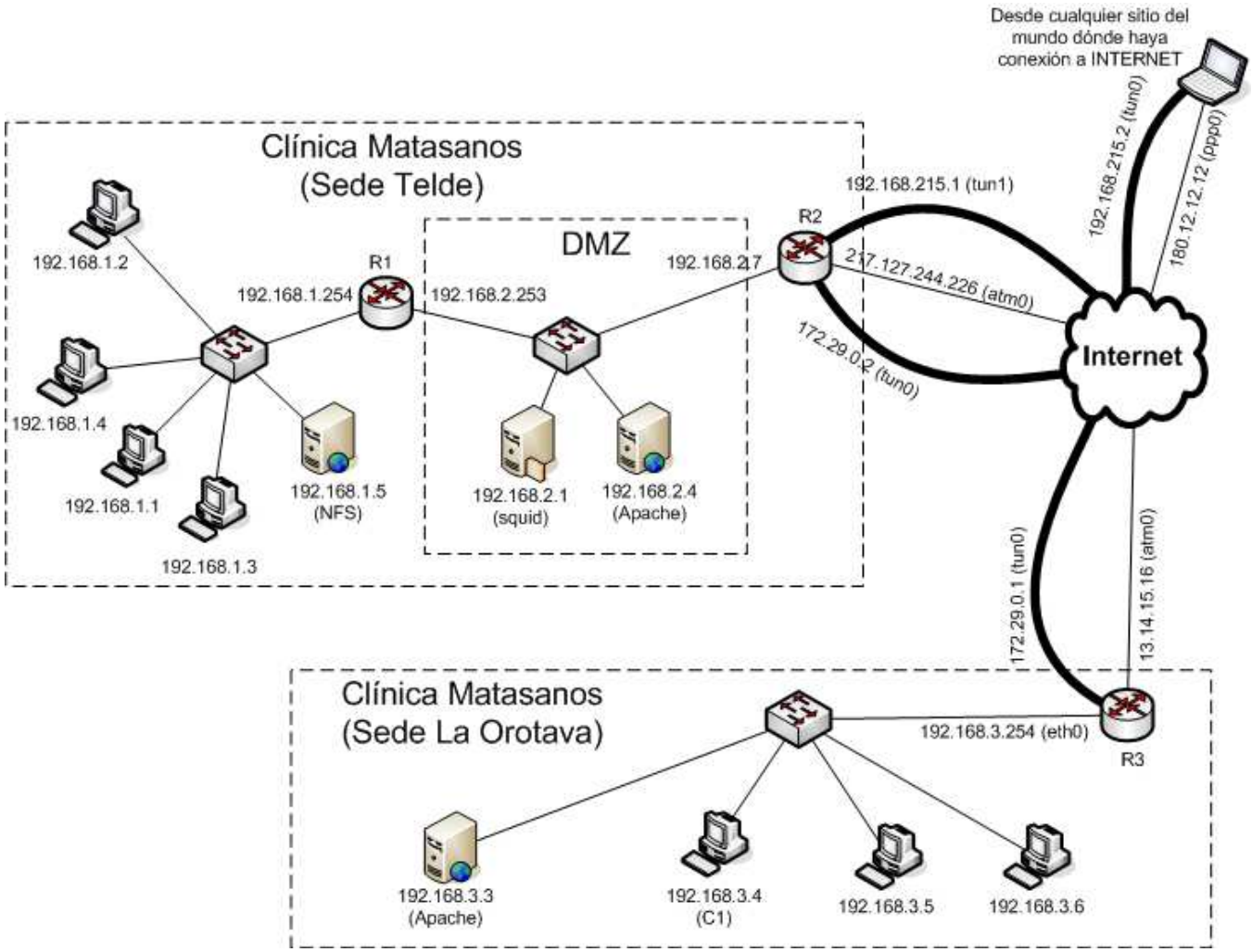
Unidad de Trabajo nº9 – Actividad de desarrollo – VPN con openvpn
Redes de Área Local - 2º CAS (Noche)- I.E.S. El Rincón
Curso 2008-2009 (Doc. nº91– 28/4/2009)

- ***Objetivo general:*** Configuración sencilla de VPN con openvpn.
- ***Duración prevista:*** 2 horas aproximadamente.
- ***Software:*** Distribución Fedora Core 8.
- ***Mínimos que se persiguen en la actividad:***
  - Realizar una configuración sencilla de openvpn.
  - Conocer los distintos métodos de encriptación utilizados en vpn:
    - SSL (secure socket layer)(usado por openvpn)
    - PPTP (point to point tunneling protocol)
    - L2TP (layer 2 tunneling protocol)
    - IPSEC (usado por openswan por ejemplo)
  - Diferenciar entre los dos tipos de conexiones:
    - conexión red-a-red.
    - conexión host a host
    - Road Warrior
- ***Documentación:***
  - www.openswan.org, home de openswan
  - openvpn.net, home de openvpn
  - http://www.ecualug.org/?q=2007/02/06/comos/centos/c_mo_instalar_y_configurar_openvpn, excelente tutorial de openvpn
- ***Introducción teórica:***



VPN (Virtual Private Network), o sea, red privada virtual, viene a solucionar el problema de poder comunicar dos redes privadas de forma segura a través de un canal inseguro.

En este dibujo se observa que hay dos sedes de la Clínica Matasanos que se pueden comunicar a través de INTERNET. Surgen los siguientes problemas (Suponiendo que no tenemos los dos túneles VPN que ya aparecen en el dibujo):

- INTERNET es un canal inseguro.
- Un equipo cualquiera como C1 no puede hacer ping 192.168.1.5 puesto que ambas sedes utilizan direcciones IP privadas y éstas no pueden ser enrutadas a través de INTERNET.
- Otra cuestión sería, por ejemplo, que queramos que los médicos que realizan visitas a domicilio o que se encuentran en congresos internacionales puedan, con su portátil, conectarse directamente a la clínica como si estuvieran en ella.

Para solucionar estas cuestiones tenemos las VPN o redes privadas virtuales. Se trata de crear túneles seguros a través de INTERNET por los que pueden circular los paquetes de nuestra red privada virtual.

- ***Ejemplo detallado del viaje de una petición de echo al hacer ping 192.168.1.5 desde C1:***

1. Se crea un paquete de petición de echo en C1. A continuación se muestra sólo la parte correspondiente a IP.

IP Origen	IP destino	Datos
192.168.3.4	192.168.1.5	(echo request)

2. La tabla de encaminamiento en C1 dirige el paquete al router R3.
3. El paquete llega a R3
4. En R3 la tabla de encaminamiento dirige el paquete a la interfaz tun0.
5. El paquete original se encripta y posteriormente se inserta dentro de un paquete normal que viaja por INTERNET, es decir:

IP Origen	IP destino	Datos
192.168.3.4	192.168.1.5	(echo request)

↓ El paquete se encripta

IP Origen	IP destino	Datos
$%&/()/(/	%%&&&/	%%&&//((()=&%%

↓ El paquete encriptado se encapsula en un paquete IP que se envía por la conexión real ppp0 a INTERNET

IP Origen	IP destino	Cabecera Túnel	IP Origen	IP destino	Datos
13.14.15.16	217.127.244.226	X	$%&/()/(/	%%&&&/	%%&&//((()=&%%

6. El paquete llega a R2 y allí se desencapsula y desencripta y se envía a su destino.

IP Origen	IP destino	Cabecera Túnel	IP Origen	IP destino	Datos
13.14.15.16	217.127.244.226	X	$%&/()/(/	%%&&&/	%%&&//((()=&%%

↓ El paquete se desencapsula

IP Origen	IP destino	Datos
$%&/()/(/	%%&&&/	%%&&//((()=&%%

↓ El paquete desencriptado se suelta en la red privada de la sede de Telde y llega al equipo de destino

IP Origen	IP destino	Datos
192.168.3.4	192.168.1.5	(echo request)

Ejemplo de conexión VPN de red a red: (comunica los equipos de dos redes)

Como se puede observar, el ejemplo descrito anteriormente hace uso de un túnel entre las dos sedes de la Clínica Matasanos solucionando de esta manera los problemas planteados para la comunicación entre dichas sedes. En dicho ejemplo se podría hablar de una conexión VPN que une dos redes privadas a través de un túnel VPN logrando así una red privada virtual. En esta red privada virtual se ha realizado una conexión punto a punto entre los dos routers R2 y R3, y se han configurado las tablas de encaminamiento que permiten el correcto tránsito de los paquetes.

Ejemplo de conexión VPN de Road Warrior: (comunica un equipo con una red)

Por otro lado, cada vez que un usuario se quiera conectar desde cualquier parte del mundo a la Clínica lo puede hacer a través de un túnel dedicado para dicha conexión como se muestra en el ejemplo del portátil. En este caso hay que tener en cuenta que se puede dar direcciones dinámicas al extremo del túnel que se conecta al router R2. A este extremo (el portátil en el ejemplo) se le suele conocer en Argot como Road Warrior.

Ejemplo de conexión host a host: (comunica un host con otro host)

Podría ser una conexión VPN entre dos hosts de manera que el túnel comunica los dos hosts exclusivamente.

El ejemplo descrito paso a paso anteriormente, en el que se indica el contenido de la cabecera de túnel como X, supone realmente una simplificación puesto que existen diversos métodos para crear un Túnel VPN. Algunos de los protocolos utilizados son los siguientes:

- SSL (secure socket layer)(usado por openvpn)
- PPTP (point to point tunneling protocol)
- L2TP (layer 2 tunneling protocol)
- IPSEC (usado por openswan por ejemplo)

- ***Ejemplo de implementación de un túnel de host a host con openVPN y claves simétricas:***

  El ejemplo se explicará a partir del esquema de red anterior que une las dos sedes de la Clínica Matasanos. Para ello, los routers R2 y R3 se supone que tienen instalado Linux con tarjetas de red ATM para acceder a INTERNET. Y además utilizaremos para ello encriptación de clave simétrica.

  - Paso 1: Instala el paquete de openvpn.
    yum install openvpn

  - *Paso 2*: Vamos a utilizar un método de clave simétrica para la encriptación del túnel. Para ello, debes crear una clave para la encriptación.
    openvpn --genkey --secret static.key

    Nota: Un método de clave simétrica quiere decir que en ambos lados del túnel se utiliza la misma clave tanto para encriptar como desencriptar la clave. Lo más seguro sería cambiar cada cierto tiempo esta clave para que nadie tenga tiempo suficiente para crackearla.

  - *Paso 3*: Por medio del comando scp, por ejemplo, copia el fichero con la clave, es decir, static.key al otro router. También lo podrías hacer por FTP, TFTP o cualquier otro medio.
    scp 13.14.15.16:/etc/openvpn/secret.key /etc/openvpn

- *Paso 4*: Crea el fichero de configuración para el servidor, que vamos a suponer que es el extremo de Telde. El fichero podría tener el nombre: server.conf.

```
dev tun
port  1194
proto  udp
ifconfig  172.29.0.2  172.29.0.1
secret  static.key
user  nobody
group  nobody
# la transmission irá comprimida con lzo
comp-lzo
# Se enviará un ping cada 15 seg. Para no perder la conexión por inactividad
ping  15
# Para mostrar información de la línea
verb  1
```

- *Paso 5*: Crea el fichero de configuración para el cliente, que vamos a suponer que es el extremo de La Orotava. Nombre del fichero: client1.conf.

```
remote 217.127.244.226
dev tun
port  1194
proto  udp
ifconfig  172.29.0.1  172.29.0.2
secret  static.key
user  nobody
group  nobody
# la transmission irá comprimida con lzo
comp-lzo
# Se enviará un ping cada 15 seg. Para no perder la conexión por inactividad
ping  15
# Para mostrar información de la línea
verb  1
```

- *Paso 6*: Utiliza el fichero anterior para arrancar el servicio VPN desde Telde.

```
service openvpn start
```

- *Paso 7*: Utiliza el fichero anterior para arrancar el servicio VPN desde La Orotava.

```
service openvpn start
```

- *Paso 8*: Realiza los mismos pasos en el extremo del túnel que se encuentra en La Orotava. Una vez realizado comprueba que existe una nueva interfaz de red tun0 en ambos routers R2 y R3; y que además puedes hacer ping de uno a otro.

```
ping  172.29.0.2      (desde R3)
ping  172.29.0.1      (desde R2)
```

- *Paso 9*: La configuración anterior sería en realidad una configuración host a host puesto que sólo se podrían comunicar a través del túnel dos extremos del túnel. Para ello, observa las tablas de encaminamiento en ambos extremos y verás que no se puede:

Desde R2 al ejecutar el comando route –n obtenemos:

Kernel IP routing table

Destination	Gateway	Genmask	Flags	Metric	Ref	Use	Iface
172.29.0.1	*	255.255.255.255	UH	0	0	0	tun0
192.168.1.0	192.168.2.253	255.255.255.0	UG	0	0	0	eth1
192.168.2.0	*	255.255.255.0	U	0	0	0	eth1
217.127.244.0	*	255.255.248.0	U	0	0	0	eth0
default	217.127.244.1	0.0.0.0	UG	0	0	0	eth0

Desde R3 al ejecutar el comando route –n obtenemos:

Kernel IP routing table

Destination	Gateway	Genmask	Flags	Metric	Ref	Use	Iface
172.29.0.2	*	255.255.255.255	UH	0	0	0	tun0
192.168.3.0	*	255.255.255.0	UG	0	0	0	eth1
13.14.15.16	*	255.255.248.0	U	0	0	0	eth0
default	13.14.15.1	0.0.0.0	UG	0	0	0	eth0

- ***Ejemplo de implementación de un túnel de red a red con openVPN y claves simétricas:***

  - Paso 10: Para que los demás equipos de ambas redes puedan hacer ping unos a otros tienes dos posibilidades:
    - Configurar las tablas de encaminamiento de los dos routers a mano.
    - Incluir las rutas correspondientes en los ficheros de configuración de la VPN de tal manera que:

      En server.conf se incluye:

      route 192.168.3.0 255.255.255.0

      En client.conf se incluye:

      route 192.168.2.0 255.255.255.0

      route 192.168.1.0 255.255.255.0

    De esta manera las tablas de encaminamiento quedarían:

  Desde R2 al ejecutar el comando route –n obtenemos:

Kernel IP routing table

Destination	Gateway	Genmask	Flags	Metric	Ref	Use	Iface
172.29.0.1	*	255.255.255.255	UH	0	0	0	tun0
192.168.3.0	172.29.0.1	255.255.255.0	UG	0	0	0	tun0
192.168.1.0	192.168.2.253	255.255.255.0	UG	0	0	0	eth1
192.168.2.0	*	255.255.255.0	U	0	0	0	eth1
217.127.244.0	*	255.255.248.0	U	0	0	0	eth0
default	217.127.244.1	0.0.0.0	UG	0	0	0	eth0

  Desde R3 al ejecutar el comando route –n obtenemos:

Kernel IP routing table

Destination	Gateway	Genmask	Flags	Metric	Ref	Use	Iface
172.29.0.2	*	255.255.255.255	UH	0	0	0	tun0
192.168.1.0	172.29.0.2	255.255.255.0	UG	0	0	0	tun0
192.168.2.0	172.29.0.2	255.255.255.0	UG	0	0	0	tun0
192.168.3.0	*	255.255.255.0	UG	0	0	0	eth1
13.14.15.16	*	255.255.248.0	U	0	0	0	eth0
default	13.14.15.1	0.0.0.0	UG	0	0	0	eth0

  - *Paso 10*: No olvides que para que se puedan reenviar paquetes a través del router es necesario habilitar el ip forwarding, o sea, debes añadir la siguiente línea:

    echo 1 > /proc/sys/net/ipv4/ip_forward

- ***Ejemplo de implementación de un túnel de red a roadwarrior con openVPN y claves asimétricas:***

  - *Paso 11*: En este caso debes realizar los siguientes pasos:
    - *Crear los ficheros de claves.*
    - *Colocar los ficheros de claves correspondientes en el directorio /etc/openvpn del cliente y del servidor*
    - *Crear los ficheros de configuración para el cliente y para el servidor.*

- *Paso 12*: Para crear las claves lo mejor es utilizar los scripts que trae openvpn. Para ello copia dichos scripts al directorio /etc/openvpn.

  cp –a /usr/share/openvpn/easy-rsa/2.0/ /etc/openvpn
  cd /etc/openvpn

- *Paso 13*: Una vez dentro del directorio /etc/openvpn ejecuta los siguientes comandos:

  . ./vars
  ./clean-all
  ./build-ca

  Al ejecutar estos comandos realizarás lo siguiente:

  - Inicializando variables.
  - Borrar potenciales archivos viejos.
  - Generar el certificado de la autoridad de certificación CA. Lo más fácil es dejar todo por defecto.

- *Paso 14*: A continuación crea el certificado y el fichero de claves del servidor:

  ./build-key-server server

  Nota: Deja todas las opciones por defecto.

- *Paso 15*: A continuación crea el certificado y el fichero de claves de cada cliente:

  ./build-key client1

  Nota: Piensa que para cada cliente sólo cambiarías el número.

- *Paso 16*: Genera el parámetro de Diffie-Hellman:

  ./build-dh

- *Paso 17*: A continuación copia los ficheros necesarios al extremo del túnel servidor:

  mv ca.crt /etc/openvpn
  mv ca.key /etc/openvpn
  mv server.crt /etc/openvpn
  mv server.key /etc/openvpn
  mv dh1024.pem /etc/openvpn

- *Paso 18*: A continuación copia los ficheros necesarios al extremo del túnel cliente:

  scp ca.crt 172.29.0.1:/etc/openvpn
  scp client1.crt 172.29.0.1:/etc/openvpn
  scp client1.key 172.29.0.1:/etc/openvpn

- *Paso 19*: Ahora hay que crear el fichero /etc/openvpn/server.conf:

```
port 1194
proto udp
dev tun
ca ca.crt
cert server.crt
key server.key
dh dh1024.pem
server 172.29.0.0  255.255.255.0
ifconfig-pool-persist ipp.txt
push "route 192.168.1.0 255.255.255.0"
push "route 192.168.2.0 255.255.255.0"
keepalive 10 120
comp-lzo
;max-clients 100
user nobody
group nobody
persist-key
persist-tun
status openvpn-status.log
verb 3
```

- *Paso 20*: Ahora hay que crear el fichero /etc/openvpn/client1.conf:

```
client
dev tun
proto udp
remote 217.127.244.226  1194
resolv-retry infinite
nobind
user nobody
group nobody
persist-key
persist-tun
ca ca.crt
cert client1.crt
key client1.key
comp-lzo
verb 4
```

- *Paso 21*: Ahora hay que rearrancar el servicio openvpn desde ambos extremos:

  Service openvpn restart

  De esta manera las tablas de encaminamiento quedarían:

Desde R2 al ejecutar el comando route –n obtenemos:

Kernel IP routing table

Destination	Gateway	Genmask	Flags	Metric	Ref	Use	Iface
172.29.0.2	*	255.255.255.255	UH	0	0	0	tun0
172.29.0.0	172.29.0.2	255.255.255.255	UH	0	0	0	tun0
192.168.1.0	192.168.2.253	255.255.255.0	UG	0	0	0	eth1
192.168.2.0	*	255.255.255.0	U	0	0	0	eth1
217.127.244.0	*	255.255.248.0	U	0	0	0	eth0
default	217.127.244.1	0.0.0.0	UG	0	0	0	eth0

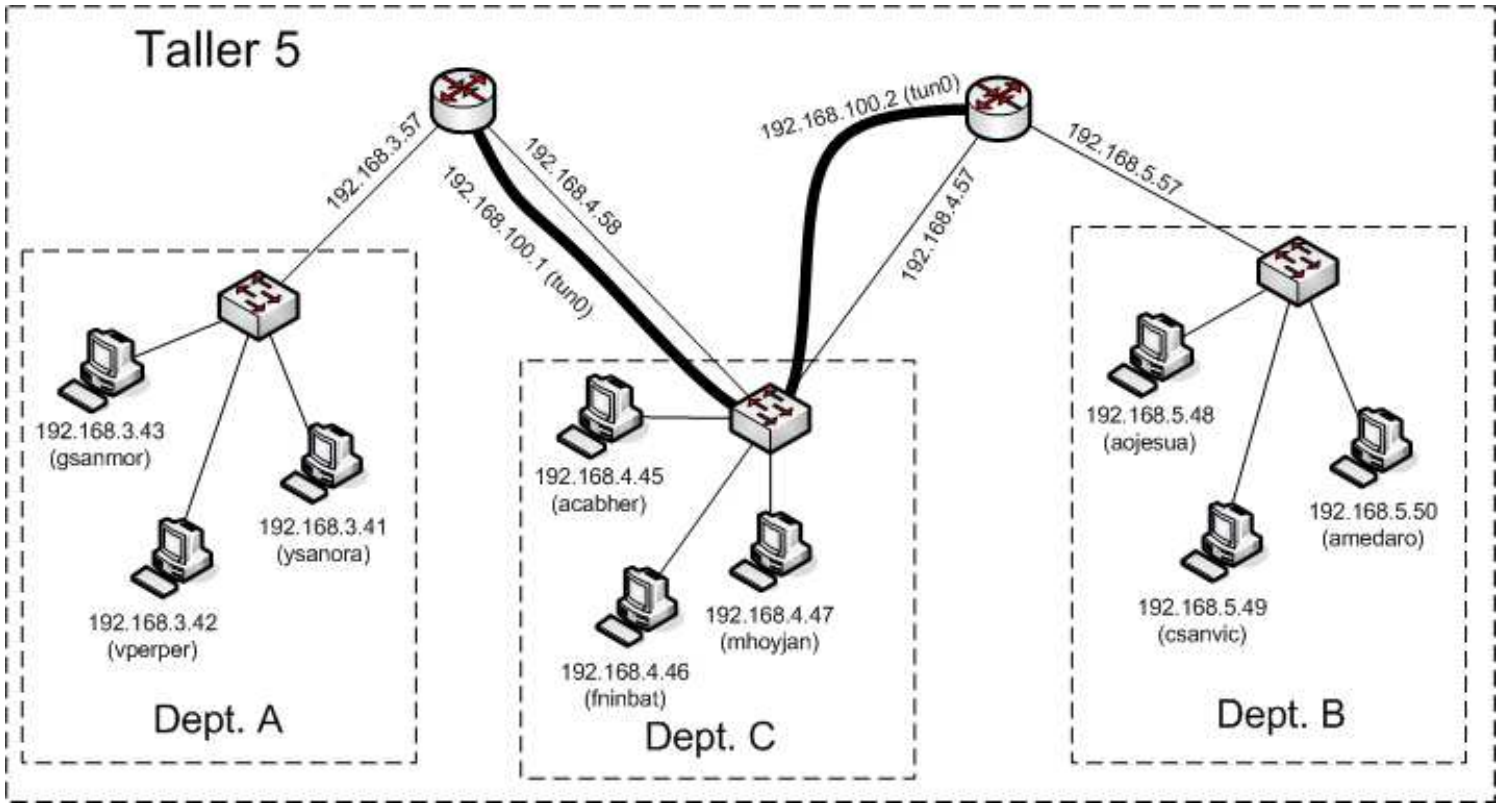
Desde R3 al ejecutar el comando route –n obtenemos:

Kernel IP routing table

Destination	Gateway	Genmask	Flags	Metric	Ref	Use	Iface
172.29.0.5	*	255.255.255.255	UH	0	0	0	tun0
172.29.0.1	172.29.0.5	255.255.255.255	UH	0	0	0	tun0
192.168.1.0	172.29.0.5	255.255.255.0	UG	0	0	0	tun0
192.168.2.0	172.29.0.5	255.255.255.0	UG	0	0	0	tun0
192.168.3.0	*	255.255.255.0	UG	0	0	0	eth1
13.14.15.16	*	255.255.248.0	U	0	0	0	eth0
default	13.14.15.1	0.0.0.0	UG	0	0	0	eth0

- ***Práctica a realizar en el instituto creando un túnel entre dos redes dentro de la clase:***

  El objetivo consiste en crear en la clase un túnel sin tener que salir a INTERNET. Esto resulta también práctico en situaciones reales cuando queremos tener un canal seguro entre dos departamentos de una empresa, para evitar que otros departamentos puedan fisgonear. En el dibujo que aparece a continuación se ha creado un túnel para que el departamento A y el departamento B puedan comunicarse por un canal seguro de manera que el departamento C no pueda acceder a los datos aunque pueda esnifar el cable.



Esta última práctica la puedes realizar en el taller 5 de varias maneras:

- Si el profesor te proporciona dos tarjetas de red extra para conseguir los 2 routers, y además te proporciona los switch necesarios.
- Creando alias de red.
- Utilizando routers hardware que el profesor te puede proporciona.