Tecnicatura Superior en Administración y Software Libre

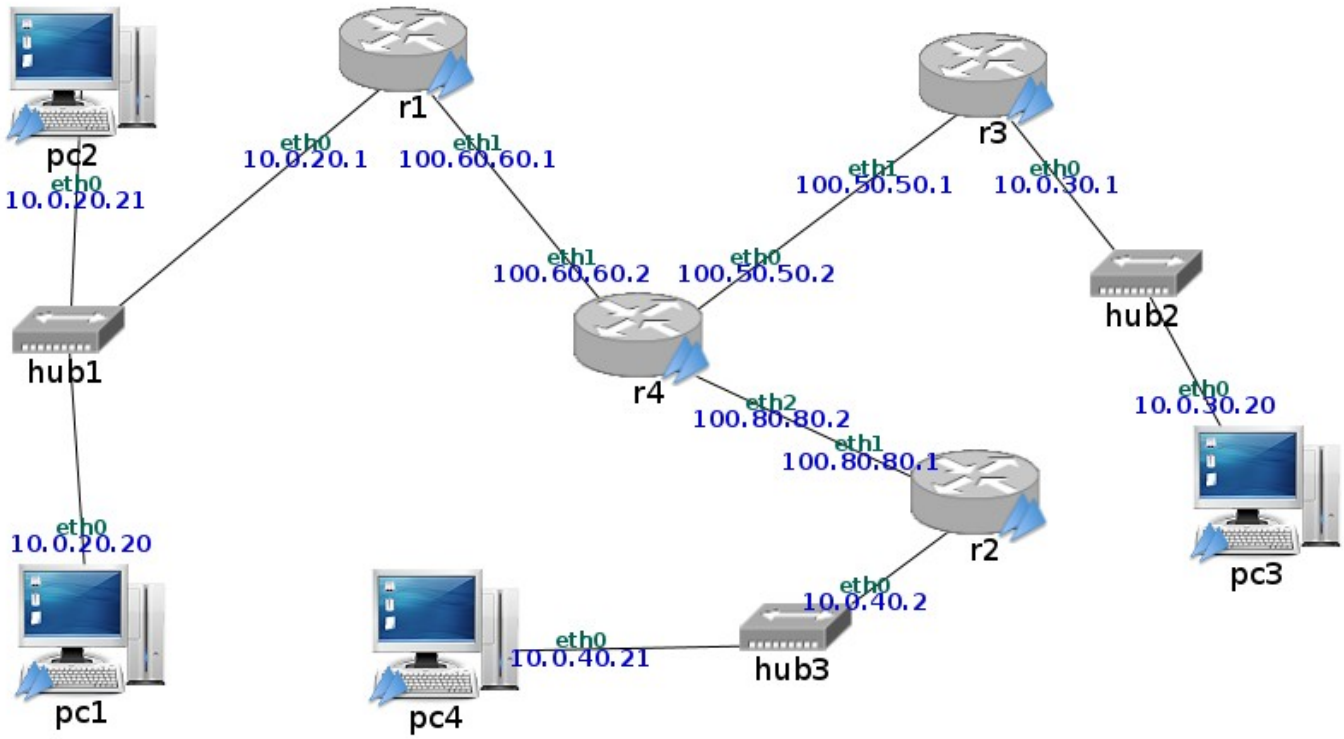
Redes II

LABORATORIO **VPN 1**

Objetivos:

- Entender el funcionamiento de las VPN ***Capa 3***.
- Aprender a utilizar OpenVPN

Laboratorio:



- Utilizar el Netgui en su computadora personal
- O Iniciar en fidebian con el usuario que cada uno tenga:

  - ***xfreerdp /v:aularemota.fi.uncoma.edu.ar:1199***
  - ***rdesktop aularemota.fi.uncoma.edu.ar:1199***

  Abrir el Netgui y cargar el lab.

Comandos útiles:

Ver interfaces activas: ***ifconfig***
Ver todas las interfaces activas: ***ifconfig -a***
Configurar una ruta: ***route add -net*** 192.168.2.0/28 ***gw*** 192.168.10.2
Verificar conexión entre los dispositivos : ***ping*** 192.168.10.1 o ***ping*** r1 o ***ping -c 3*** r1
Verificar ruta entre dispositivos: ***traceroute*** 192.168.10.2 o ***traceroute*** A1
Iniciar/Detener demonio openvpn: ***/etc/init.d/openvpn {start/stop}***
Para monitorear los paquetes: ***tcpdump -i ethX -v -n***
Para ver los servicios y puertos: ***netstat -tuplen***

Bases

OpenVPN es tanto un protocolo VPN como un software que utiliza técnicas VPN para asegurar conexiones punto a punto y de sitio a sitio. Actualmente, es uno de los protocolos VPN más populares.

El protocolo OpenVPN es responsable de manejar las comunicaciones cliente-servidor. Básicamente, ayuda a establecer un "túnel" seguro entre el cliente y el servidor VPN.

Cuando OpenVPN maneja el cifrado y la autenticación, usa la biblioteca OpenSSL de manera bastante extensa. Además, puede usar UDP (Protocolo de Datagramas de Usuario) o TCP (Protocolo de Control de Transmisión).

En los laboratorios utilizaremos algunos routers como clientes y uno como servidor para establecer los túneles VPN. Los archivos de configuración necesarios se encuentran en cada directorio ***/etc/openvpn .*** Los archivos de configuración que determinan el modo de funcionamiento de cada router son: ***client.conf*** y ***server.conf.*** Sólo puede haber uno de ellos y dependiendo de cuál sea el router actuará como cliente o servidor. El resto de los archivos son necesarios para garantizar la seguridad de la conexión y se verán en el próximo laboratorio.

El el servidor se debe agregar por cada cliente en la carpeta ***/etc/openvpn/clients*** un archivo de texto con el nombre del router cliente. El contenido del archivo es: ***iroute NetIP MASK .*** Donde ***NetIP*** y ***MASK*** son la dirección IP de la red y la máscara del router cliente.

Actividades

1. Iniciar todos los routers y pcs**, menos pc4** y **r2**.
2. Verifique conexión entre **pc1** y **pc2**. Ahora entre **pc1** y **pc3**. ¿Qué ocurre con **pc3**?. Detenga **pc2**.
3. Investigue las configuraciones de las **pcs** y de los **routers**.
4. Ejecute un ifconfig en **r1** y **r3**. ¿Qué interfaces están activas?
5. Inicie el servicio **openvpn** en **r3** y luego en **r1** (en ese orden). Ejecute un ifconfig en **r1** y **r3**. ¿Qué interfaces están activas ahora?.
6. Verifique conexión entre todas las **pcs**. ¿Porqué funcionan ahora?
7. Inicie **r2** y **pc4**. ¿ **pc4** se conecta con el resto de las **pcs**?. Encuentre la solución.

   Ayuda1: Incorporar r2 a la VPN.

   Ayuda2: Agregar rutas en r1 y r2 (ver tun0).
8. Indique sus conclusiones teniendo en cuenta el tipo direcciones IP que usan las LANs.