Armado de VPNs con Linux

Indice

A) Introducción:

Como para todo, tenemos muchas opciones para realizar VPNs en Linux. Hay muchísimo material en Internet y en este documento intentaremos ordenar algunos conceptos fundamentales para luego pasar al armado específico de VPNs por SSH.

EN principio una VPN no es más que el uso de protocolos y criptogramas para establecer en medio de una red pública o semi pública un canal de comunicación seguro entre dos extremos.

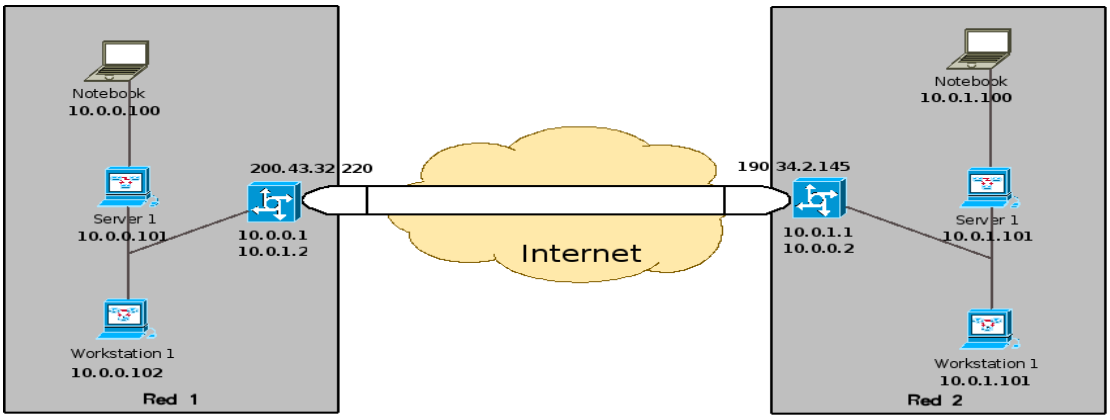
Son muchas las opciones existentes. Los principales protocolos utilizados son

PPTP (Microsoft)
GRE (Estándar utilizado por otros protocolos para realizar el encapsulamiento de paquetes)
L2TP (Microsoft-Cisco, no provee encripción por si mismo)
L2F (Viejo protocolo CISCO)
IPSEC. (Estándar ipso facto para vpns en LINUX)
SSH: No demasiado conocido aún para VPNS, es una reciente implementación muy práctica y sencilla de usar. En este protocolo nos detendremos detalladamente.

Topologías Posibles

Lan2Lan

En este tipo de redes, hay dos sitios que se interconectan a través de la red pública y establecen un "Tunel" entre ambos de manera de poder traficar entre ambos asegurando la "Confidencialidad" o "Privacidad" de lo traficado.



Como se ve en el diagrama, las ips de ambas redes a los extremos pertenecen a dos subredes distintas, esto es solo un ejemplo, pero es una solución conveniente para simplificar la configuración del ruteo.

Los dos concentradores VPN ubicados uno en cada red tienen tres interfases, una de las cuales posee una ip "Pública", es la ip que normalmente nos otorga el ISP y las otras dos interfases tienen ips

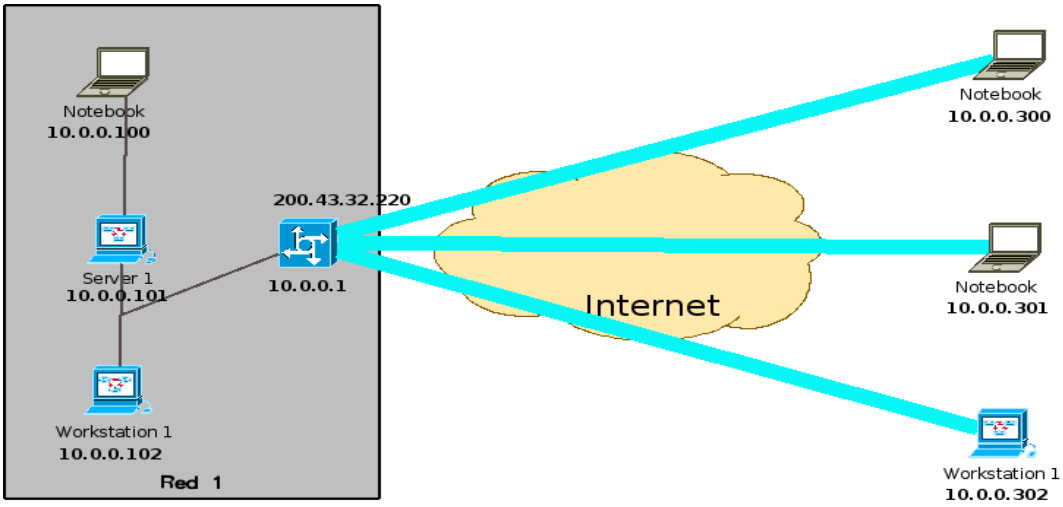
“Privadas”. Las privadas pueden ser de cualquier rango, es conveniente elegirlas de uno de los rangos privados (10.x.x.x / 172.x.x.x / 192.168.x.x). La cantidad de interfases virtuales que podemos tener es independiente de la cantidad de interfases físicas o tarjetas de red. En el caso del ejemplo podrían ser dos interfases físicas, una de las cuales se encuentra conectada a Internet (200.43.32.220), y otra conectada a la red local (10.0.0.1). La ip restante es una interfase virtual que se genera en el momento en que se levanta la vpn (10.0.1.2). En este caso se ha generado del mismo rango que la red ubicada al otro extremo, ya que será la que “hable” con el otro gateway. Reiteramos que el direccionamiento que utilicemos depende únicamente de lo que queramos configurar.

Para configurar el ruteo en este caso simple, se colocan como “default gateways” de todos los hosts de cada red, la ip que corresponda al concentrador ubicado en el borde. Si estos no son los que también conectan a Internet, podríamos rutear simplemente la red del otro extremo para que salga por estos “Concentradores” VPN y utilizar el default gateway que corresponda.

Todo el esquema de enrutamiento, una vez configurado es completamente transparente para todas las aplicaciones de la red. En tanto la VPN es a nivel IP (Capa 2 del modelo TCP/IP o Capa 3 del modelo OSI), para los niveles superiores esto es transparente, es decir, en condiciones normales, una aplicación podrá localizar a cualquier host de ambas redes sin tener que realizar ninguna modificación.

Road Warrior o Acceso Remoto

En este caso de lo que se trata es de que hay varios equipos que se encuentran en viaje o fuera del sitio principal, y requieren acceder a las aplicaciones de los diferentes equipos de la red interna, sin hacer que estos equipos tengan ips públicas.



En el ejemplo se han colocado a los clientes ubicados fuera del sitio, ips del mismo rango que el sitio central. De esta manera, una vez levantada la vpn en cada cliente, trafican exactamente igual que como si estuviesen conectados a un switch del sitio central. Usualmente en este tipo de VPNs, el cliente primero se conecta a Internet por cualquier proveedor, cyber, etc, y luego establece la VPN contra la ip pública del “Concentrador” de VPN ubicado en el sitio central. Por supuesto los cliente pueden adquirir una ip pública en el momento en que se conectan a Internet si lo hacen directamente o bien salen a Internet por el gateway de la red en la que se encuentran, por ejemplo la de un cyber café.

Una vez levantada la VPN; dependerá del enrutamiento configurado al armar la VPN la posibilidad de

que también se conecten los clientes entre si y no solo a equipos de la red central. Al igual que en el caso anterior, para el nivel de las aplicaciones, todo esto es completamente transparente.

¿Qué protocolo decidimos utilizar?

Para responder a esta pregunta todo dependerá de cada configuración particular, sin embargo deben tenerse en cuenta algunas cosas básicas:

- ¿Qué topología necesito?

  ¿Necesito conectar dos redes o son equipos móviles que deben conectarse a un sitio central?

- ¿Los equipos que pretendo conectar, que OS tienen?

  Si voy a utilizar equipos en su mayoría Microsoft y puede haber clientes viejos (Win 98, etc) entonces debo utilizar PPTP que es más compatible con ellos

  Si se trata de equipos más nuevos, es posible utilizar L2TP, pero hay que tener en cuenta que este protocolo no soporta por sí mismo encripción, por lo que debe transportarse a través de un protocolo que si lo soporte como IPSEC.

  Para el caso de una Lan-to-Lan lo único que importa es el Sistema Operativo de los dos concentradores de VPN, siendo indistinto el tipo de clientes que tenga en cualquiera de los dos lados. Todo el trabajo lo realizan los dos concentradores, por lo que la VPN es transparente para las aplicaciones de ambas redes.

  Si la mayoría de los equipos a conectar son UNIX; el standard más conveniente es directamente IPSEC, sin utilizar ni L2TP ni PPTP. Asimismo si el OS se encuentra actualizado se puede utilizar SSH cuya principal ventaja, adicionalmente a su fuerte y flexible encripción, es la facilidad de implementación.

- La comunicación se encuentra encriptada con un algoritmo lo suficientemente fuerte.

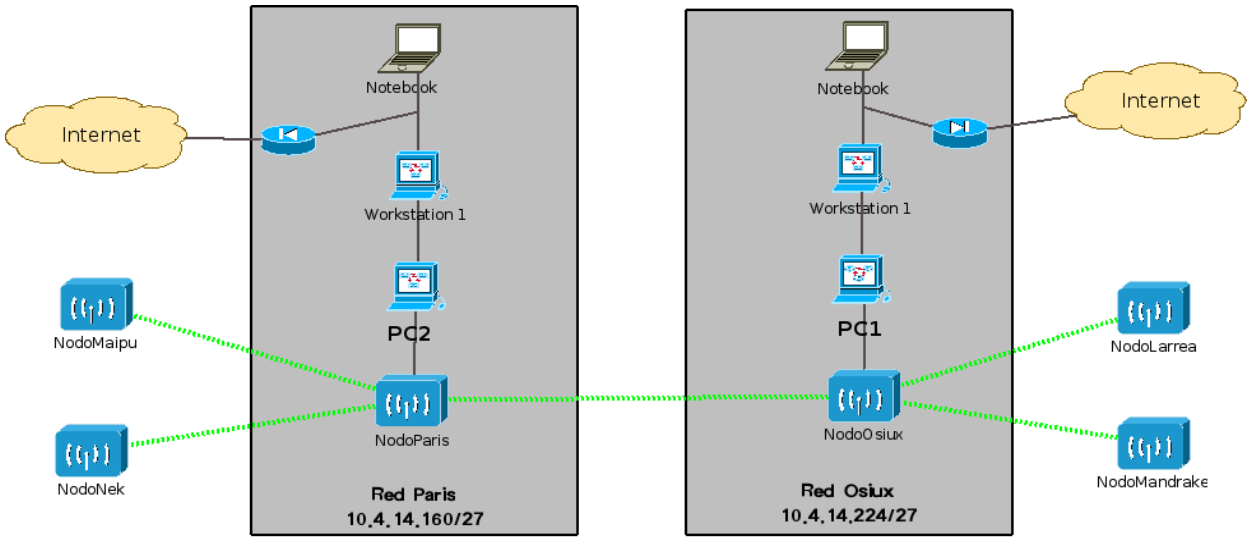
  Diversos protocolos son capaces de utilizar diversos algoritmos y longitudes de claves para la encripción. La única desventaja de ir subiendo el nivel de seguridad es que algoritmos más complejos y longitudes de claves más largas implican un mayor procesamiento de ambos extremos para desencriptar la información.

B) Implementación de un caso concreto de una VPN por ssh entre equipos conectados a través de nodos BAL.

Introducción y presentación

Si bien a fin de ilustrar este paso a paso se tomará un caso concreto realizado en BAL, el mismo no se encuentra limitado a su aplicación dentro de BAL, sino que es lo suficientemente genérico como para implementar en cualquier red.

Esquema de red parcial



Este es el estado previo de la red. Ambas redes se encuentran enlazadas entre si por aire de acuerdo a como se explica en http://wiki.buenosaireslibre.org/NodoOsiux y http://wiki.buenosaireslibre.org/NodoParis .

Los equipos del diagrama son solo a título ilustrativo.

Necesidad:

Se requiere armar un vínculo de emergencia de cada nodo a fin de rutear la conexión a Internet para el caso en que alguno de los dos nodos se quede sin Internet por problemas en el ISP

Topología a utilizar:

Es indistinto, este modo de configurar una VPN se ajusta a cualquiera de las dos topologías mencionadas más arriba.

Protocolo y encripción.

Se ha elegido utilizar ssh debido a:

1. Simplicidad de implementación:

   Para implementarlo, más allá del ruteo: ¡Basta con ejecutar un solo comando de uno de los lados!.

2. Fortaleza del algoritmo de encripción utilizado.

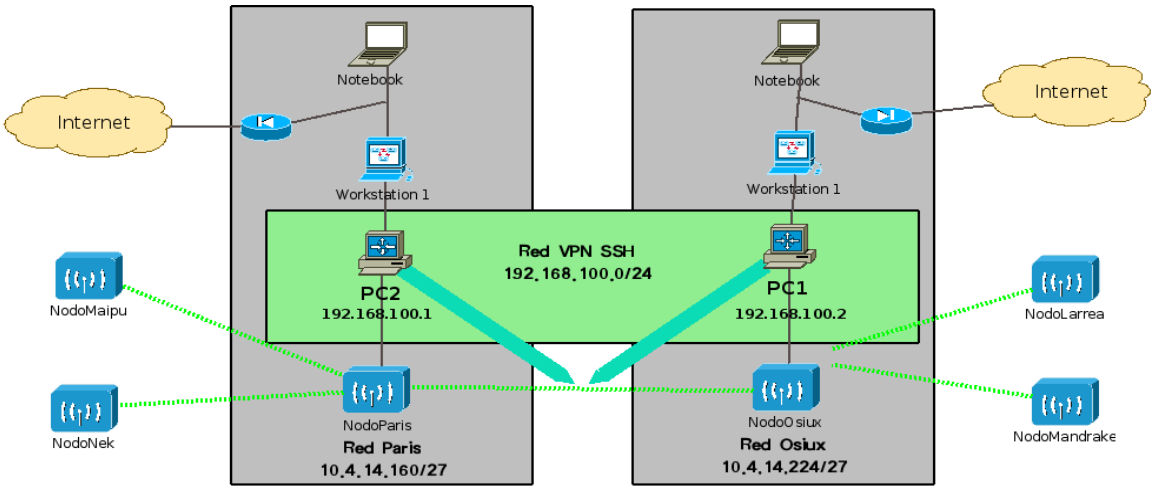
   Es públicamente conocido la fortaleza del algoritmo de encripción del protocolo ssh versión 2 por lo que no es necesario detenerse demasiado en este punto. Este protocolo es perfectamente capaz de soportar

3. Rapidez de transferencia por algoritmo de compresión.

Se utiliza la capacidad del mismo protocolo de comprimir la información antes de enviarla por el túnel.

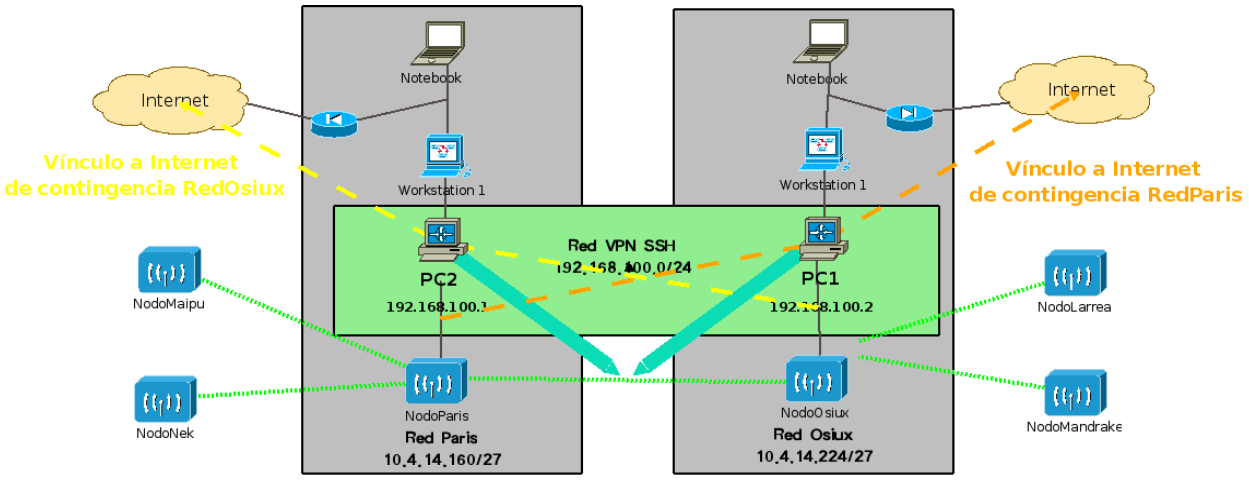
Solución propuesta:

Armar una VPN entre dos equipos correspondientes a cada una de las redes internas de los nodos a fin de utilizarla como Gateway de emergencia. El esquema de la solución de VPN propuesta es:



Este esquema permitirá utilizar la VPN como camino alternativo para el establecimiento del enlace a Internet a través de la red BAL, de modo seguro y encriptado. El esquema actual de enrutamiento de cada una de las redes tiene configurado como gateway a los equipos que hemos denominado “Server 1”, lo que facilita las cosas pero no es una configuración imprescindible. Al caerse el enlace a Internet pueden encaminarse los paquetes a través de la VPN para que salgan por el vínculo a Internet de la otra red. Más abajo explicaremos el enrutamiento correspondiente.

Esquema de los enlaces alternativos terminados:



El amarillo representa el flujo virtual de paquetes del enlace de contingencia a Internet para la red

Osiux. El anaranjado representa el correspondiente pero para la RedParis

Paso a Paso

Esto que parece una solución compleja, veremos en este paso a paso que SE REALIZA CON UNA UNICA LINEA DE COMANDO. Esto independientemente del trabajo de ruteo que quiera realizarse posteriormente.

Recursos Utilizados.

- Concentrador VPN: Pc con LINUX actualizado con ssh instalado (Llamado PC1).
- Cliente VPN: Pc con LINUX actualizado con ssh instalado (Llamado PC2).
- Infraestructura de red LAN existente a ambos lados.
- Infraestructura de red BAL existente con enlace funcionando.
- Software/Drivers adicionales: Ninguno

1) Configuración de uno de los equipos como Server VPN. (La PC1 que será nuestro Concentrador VPN)

Para ello simplemente debemos verificar algunos de los parámetros existentes en el archivo de configuración del servicio de ssh:

/etc/ssh/sshd_config

Debemos chequear la existencia de los siguientes parámetros:

```
PermitRootLogin yes  # En el apartado D se muestra como mejorar la seguridad
de esto seteando este parámetro en without-password y utilizando
certificados.
PermitTunnel yes
TCPKeepAlive yes
StrictModes yes
TCPKeepAlive yes
RSAAuthentication yes
PubkeyAuthentication yes
```

Si alguno de ellos está configurado como no, debemos modificarlo y luego reiniciar el servicio de ssh:

/etc/init.d/ssh restart

Lo podemos hacer remotamente sin peligro ya que esto no mata las sesiones existentes. Este renicio solo se requiere si se cambió algún parámetro.

2) Levantamiento y activación de la VPN ssh desde el otro equipo (la PC2 Cliente VPN)

Se detallan a continuación la compleja cadena de comandos a ejecutar con usuario **root** para establecer la red privada virtual entre los dos extremos:

 # ssh -C2 -w 1:1 10.4.14.226 -l root

Aunque no lo crean, luego de lanzar este comando ya está levantada y funcionando la VPN. Este comando nos ha creado en ambos equipos (PC1 y PC2) un dispositivo de red virtual denominado tun1. Ambos dispositivos están lógicamente enlazados a través del protocolo ssh como si fueran dos dispositivos físicos ethernet conectados a un switch. Solo nos resta configurar las direcciones ip y el ruteo para los dispositivos ya creados.

3) Configuración de dirección Ip de dispositivos y rutas elementales.

De aquí en más ambos dispositivos se configuran de manera exactamente igual a un dispositivo ethernet normal.

PC1 (Concentrador VPN ubicado en Red Osiux)(deben ser ejecutados con root)

 # ifconfig tun1 192.168.100.2 netmask 255.255.255.0

 # ifconfig tun1 up

 # route add -host 192.168.100.1 dev tun1

Con estos comandos hemos realizado:

1. Configuración de dirección ip
2. Levantado de interfase
3. Agregado de ruta de host para llegar al otro extremo de la VPN

PC2 (Cliente VPN ubicado en Red Paris)(deben ser ejecutados con root)

 # ifconfig tun1 192.168.100.1 netmask 255.255.255.0

 # ifconfig tun1 up

 # route add -host 192.168.100.2 dev tun1

Con estos comandos hemos realizado:

1. Configuración de dirección ip
2. Levantado de interfase
3. Agregado de ruta de host para llegar al otro extremo de la VPN

Con estos pasos ya tendríamos que estar en condiciones de pinguear ambos equipos. Es decir ya tenemos un tunel abierto entre ambos por el que toda nuestra comunicación está encriptada.

Para terminar con la solución propuesta, restan sin embargo realizar algunos pasos para enmascarar las conexiones a Internet de ambas redes y poder rutear paquetes desde otros equipos.

Poniendo todos los pasos en un único script:

Podríamos incluir todos los comandos hasta aquí enunciados en un único script que nos levante la vpn y nos configure las interfases con sus direcciones ip y las rutas elementales. En este caso el script se debería lanzar desde la PC2 (Cliente VPN):

#!/bin/bash

```
ssh -C2 -f -w 1:1 10.4.14.226 " \
    ifconfig tun1 192.168.100.2 netmask 255.255.255.0 && \
    ifconfig tun1 up && \
    route add -host 192.168.100.1 dev tun1"
ifconfig tun1 192.168.100.1 netmask 255.255.255.0
ifconfig tun1 up
route add -host 192.168.100.2 dev tun1
```

Comentarios:

- Deben notarse los caracteres especiales:
  - \ indica que la línea de comando no termina sino que continúa en la línea inferior. Podríamos hacer todo el comando en una única línea pero por cuestiones de facilidad de lectura del script se suele utilizar este carácter.
  - && Es el operador "y" del shell. Se utiliza para ejecutar una serie de comandos siempre que el anterior ejecute correctamente. Por ejemplo cmd1 && cmd2 ejecuta primero cmd1, si este da error se detiene la ejecución, si ejecuta sin error cmd1 se ejecuta a continuación cmd2
- El parámetro -f permite ejecutar comandos en el equipo remoto desde donde se está corriendo el script
- De esta manera todos los comandos en azul corresponden a una ejecución remota y podrían escribirse en una única línea larga. Las tres últimas líneas del script corren localmente en el equipo en que se lanza el script.
- El script debe ejecutarse con usuario root y pedirá contraseña cuando intente conectarse al concentrador de VPN PC1. Ver más abajo como evitar que pida contraseña.

Actualización 2013

Para mejorar la seguridad de esta configuración se recomienda leer el apartado D en donde se explica como invalidar el acceso por contraseñas a root desde un sitio remoto así como también evitar la ejecución de otros comandos aparte de la generación de la VPN por parte del cliente en el server.

4) Configuración de enmascaramiento de la conexión a Internet de ambos nodos y switcheo de default gateways.

PC1 (Cliente VPN ubicado en Red Paris)(deben ser ejecutados con root)

```
# iptables -t nat -A POSTROUTING -o ppp0 -j MASQUERADE
# echo 1 >/proc/sys/net/ipv4/ip_forward
# route del default
# route add default gw 192.168.100.2
```

Con estos comandos hemos realizado:

1. Enmascaramiento de la interfase conectada a fibertel en la red OSIUX (eth1). Esto permite el

nateo de la dirección a Internet, permitiendo navegar desde la red interna
2. Permitir que el kernel forwardee paquetes entre las distintas interfases. Esto va a permitir que los paquetes se encaminen entre interfases de acuerdo a las reglas de enrutamiento que se quieran colocar.
3. Borrar el default gateway existente en PC1 (Esto es el que se ha caído)
4. Agregar como default gateway la interfase del otro equipo (PC2)

(CORRESPONDE A FLECHA CORTADA NARANJA EN ESQUEMA DE RED)

PC1 (Concentrador VPN ubicado en Red Osiux)(deben ser ejecutados con root)

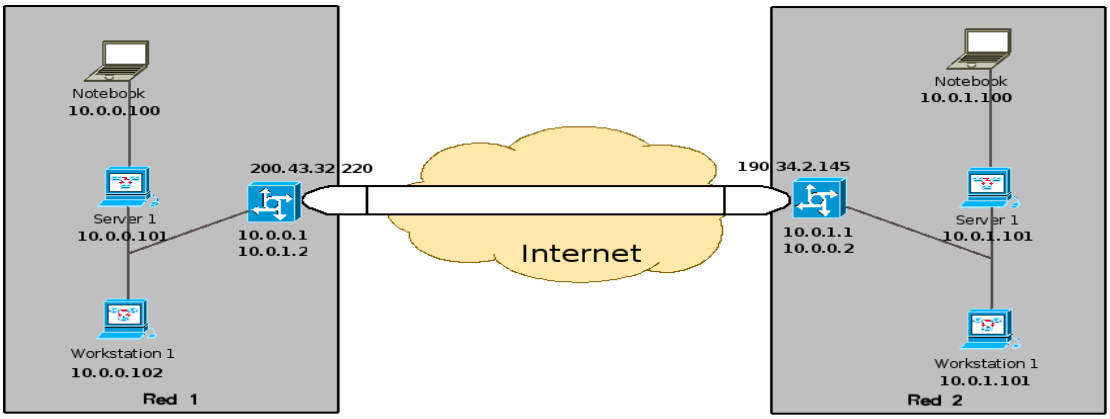
 # iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE
 # echo 1 >/proc/sys/net/ipv4/ip_forward
 # route del default
 # route add default gw 192.168.100.2

Con estos comandos hemos realizado:

1. Enmascaramiento de la interfase conectada a arnet en la red Paris (ppp0). Esto permite el nateo de la dirección a Internet, permitiendo navegar desde la red interna.
2. Permitir que el kernel forwardee paquetes entre las distintas interfases. Esto va a permitir que los paquetes se encaminen entre interfases de acuerdo a las reglas de enrutamiento que se quieran colocar.
3. Borrar el default gateway existente en PC2 (Esto es el que se ha caído)
4. Agregar como default gateway la interfase del otro equipo (PC1)

(CORRESPONDE A FLECHA CORTADA AMARILLA EN ESQUEMA DE RED)

C) Apartado OPTATIVO: Script de Configuración de la VPN de esquema:



Script a ejecutar desde Red 1 en equipo 200.43.32.220

#!/bin/bash

```
ssh -C2 -f -w 1:1 190.34.2.145 " \
    echo 1 >/proc/sys/net/ipv4/ip_forward
    ifconfig tun1 10.0.1.1 netmask 255.255.255.0  && \
    ifconfig tun1 up  &&  \
    route add -net 10.0.0.0 netmask 255.255.255.0 gw 10.0.1.2"
echo 1 >/proc/sys/net/ipv4/ip_forward
ifconfig tun1 10.0.1.2 netmask 255.255.255.0
ifconfig tun1 up
route add -net 10.0.1.0 netmask 255.255.255.0 gw 10.0.1.1
```

Es importante destacar que si la ip es dinámica se puede usar un servicio gratuito de dns dinámica tipo dnsexit y se reemplazan en el script las ips por la url.

D) Apartado OPTATIVO: Configuración de ssh para autenticación por certificados

Esto lo necesitamos para que cuando se ejecutan los scritps de los clientes hacia el concentrador de VPN no sea necesario ingresar la contraseña. Para ello se instala un certificado DEL cliente EN el concentrador de VPN.

1) Crear las keys en el cliente

Para ello debemos loguearnos con el usuario para el que queremos generar el certificado (Para los casos vistos más arriba se debe usar root) y ejecutar el siguiente comando:

```
# ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/root/.ssh/id_rsa):
Created directory '/home/pepe/.ssh'.
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/pepe/.ssh/id_rsa.
Your public key has been saved in /home/pepe/.ssh/id_rsa.pub.
The key fingerprint is:
84:1c:d8:24:d9:ad:65:97:d7:f3:44:83:51:0a:0f:3b pepe@TPMariano
The key's randomart image is:
+--[ RSA 2048]----+
|    .*o.   + o++.|
|    oooo+ o *.+ o|
|      o+.. E o + |
|      ..    .   .|
|        S        |
|                 |
|                 |
|                 |
|                 |
+-----------------+
```

COn esto hemos creado un archivo ubicado en una carpeta .ssh ubicada en la home del usuario con que ejecutamos el comando, que contiene la clave pública que será luego instalada en el concentrador de vpns. Este archivo es

id_rsa.pub

Esto contiene la parte pública clave de 2048 bits. Copiamos el archivo al equipo que va a funcionar como concentrador de vpn y realizamos lo siguiente para instalarlo:

2) Instalar la clave pública en el concentrador de VPN:

```
# cat /tmp/id_rsa.pub >>/root/.ssh/authorized_keys2
# chmod 600 /root/.ssh/authorized_keys2
```

(PRESTAR ESPECIAL ATENCION AL CARACTER ">>", NO USAR UNA SOLA ">" PORQUE SE SOBREESCRIBEN TODOS LOS CERTIFICADOS INSTALADOS PREVIAMENTE)
Una vez completado esto, cuando el usuario root del cliente VPN (PC2 en el ejemplo) intente loguearse al concentrador de VPN (PC1 en el ejemplo más arriba) no se le solicitará contraseña.

Actualización 2013:

Una alternativa mucho más sencilla para copiar la clave pública del cliente al servidor existe en las versiones más modernas de ssh. Simplemente del lado del cliente se tipea:

```
# ssh-copyid <ip del cliente>
```

3) Restringir las posibilidades de ejecución en el server de comandos a root cuando se conecta desde el sitio al que corresponde la clave publica:

Se indica a continuación una opción más segura para evitar el acceso con privilegios root desde el cliente al servidor. Para ello:

- EN EL SERVER:
  - Se restringen los comandos a ejecutar en el archivo /root/.ssh/auhorized_keys para la clave recién instalada, precediéndola por los únicos comandos que podrá ejecutar el usuario desde este cliente conectándose con root (Con la palabra ssh-rsa comienza la clave pública recién instalada, solo debemos precederla de esta manera con cuidado de no modificar ningún carácter en esta clave pública. Solo agregamos lo escrito en rojo):

    tunnel="0",command="ifdown tun0; ifup tun0; ",no-port-forwarding,no-X11-forwarding,no-agent-forwarding,no-pty ssh-rsa AABBBB7NzaCm....

  - Se configura la dirección ip y todos los comandos del script antes mencionados en el archivo /etc/network/interfaces para cada tunel que se desee crear:

    iface tun11 inet static

        address 10.10.0.11 # esta es la ip del tunel del lado del server

netmask 255.255.255.0

pointopoint 10.10.0.101 # esta es la ip del tunel del lado cliente

up route add -host 10.10.0.1 dev tun1 #esto genera la ruta respectiva para llegar al cliente por el tunel.

- EN EL CLIENTE
  - Se cambia el comando ssh que abre el tunel (Ver apartado C) por lo siguiente:

    ssh -C2 -w 1:1 -f vpn.acciardi.com.ar "ifdown tun1 ;ifup tun1"

De esta manera restringimos los comandos que el cliente puede ejecutar en el server conectándose remotamente con root a unicamente “ifdown tun0; ifup tun0”. La configuración de ip y rutas del lado del server se realiza cuando el cliente al conectarse ejecuta estos dos comandos, de acuerdo a lo que se ha colocado en el archivo /etc/networ/interfases, que es el archivo por defecto que utiliza linux para configurar todas sus interfases de red.

ESTA FORMA DE CONFIGURACIÓN ES LEJOS LA MÁS RECOMENDADA PARA NO DAR A LOS CLIENTES PERMISOS PARA REALIZAR NINGUNA OTRA COSA QUE LEVANTAR LA VPN.

Mariano Acciardi
Grupo CATI/UTN - Instructor