SAD.T5P1: VPNs

En esta práctica vamos a ver la puesta en marcha de VPNs. Simularéis las varias sedes con máquinas virtuales. Tenéis tres opciones, cada una de las tres opciones contará como una práctica diferente. Es obligatorio hacer al menos una

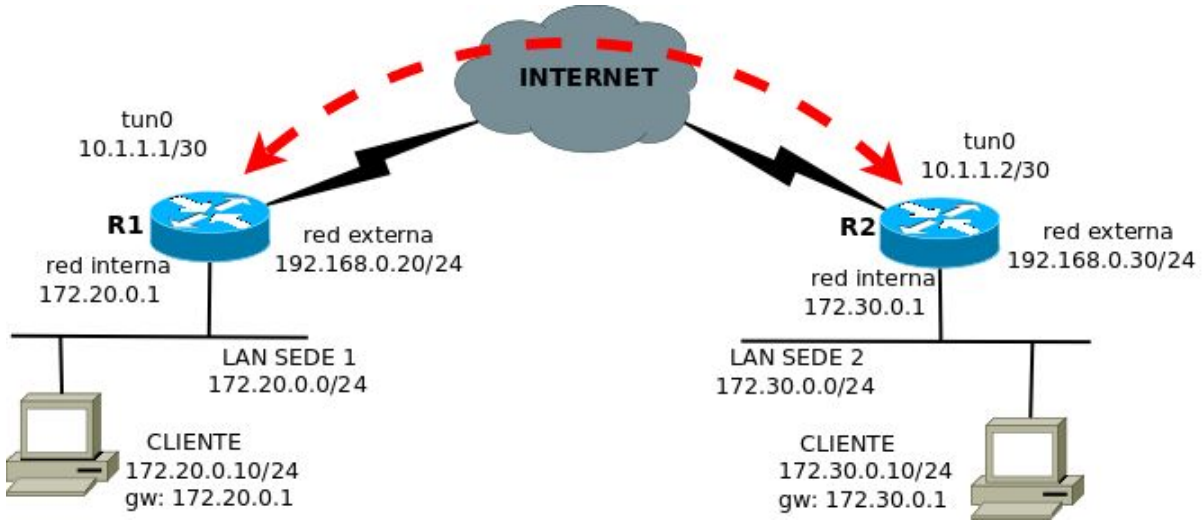
Escenario común para prácticas VPN

En esta sección se va a explicar el laboratorio que el alumno debe preparar para abordar cualquiera de las dos prácticas siguientes relacionadas con redes privadas virtuales.

Se parte de un escenario de simulación de dos redes locales de dos sedes pertenecientes a una organización y conectadas a Internet por un ISP. Supuestamente ambas sedes estarán separadas geográficamente por mucha distancia y posiblemente con diferentes operadores (dependiendo de la oferta de conexión en la zona).

Lo que se pretende es poder interconectar ambas redes remotas de manera segura con una VPN a través de Internet y además esta despliegue lo va a realizar la propia organización y no va a ser contratado a un ISP. Como ya se ha comentado, esta opción de contratar la VPN a un ISP es más cara pero tiene mejores garantías de funcionamiento al garantizar un servicio fiable extremo a extremo. Sin embargo la opción que se va a usar en estas prácticas, es mucho más económica, pero puede sufrir de los problemas de una red no gestionada de extremo a extremo y sin garantías, como retardos, cortes, jitter, pérdida de paquetes, etc. Obviamente en entornos críticos, esta no es una buena solución pero en muchas ocasiones es más que suficiente.

El **escenario** que debe simularse es el siguiente:



Cada sede es representada por un router o pasarela sobre la que se configura la VPN site-to-site y una LAN interna a la que de momento se conectará un sólo PC. El router de cada sede será una máquina GNU/Linux configurada para realizar enrutamiento y NAT para salir a Internet, enmascarando las direcciones privadas de la red local con su dirección IP en la interfaz de la red externa.

Ya que es un escenario simulado, ambas sedes estarán conectadas a la misma red local teniendo por tanto direcciones del mismo rango. En el ejemplo, la sede 1 tiene la dirección 192.168.0.20/24 en su interfaz WAN o externa y la sede 2 tiene la 192.168.0.30/24. En un entorno real serán direcciones IP públicas de diferentes prefijos de Internet en función de la región o país donde se encuentre la sede.

Para montar el escenario, cada alumno es **libre de elegir** una de las siguientes alternativas según su disponibilidad de equipos o características de los mismos:

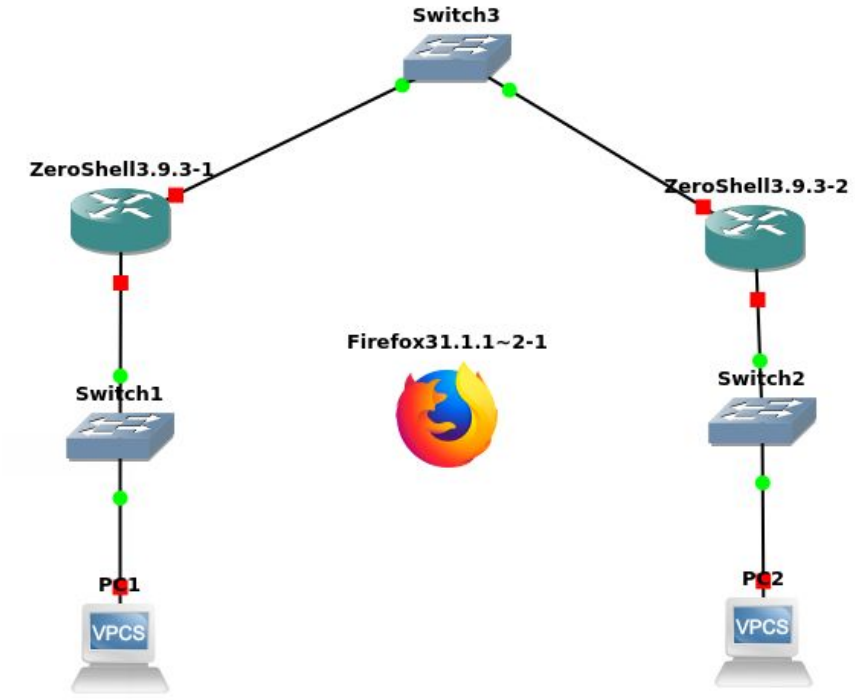
1. Todos los ordenadores de escenario son máquinas reales. Entendemos que esta no va a ser la situación habitual, además de requerir dos tarjetas en los equipos que hagan de router, que deben tener instalado GNU/Linux.

2. Cada sede simulada con un anfitrión, por tanto son necesarios dos ordenadores físicos: en cada anfitrión el router y el PC cliente pueden ser simulados ambos o bien uno de los dos. En caso de simular el router, debe tener la interfaz externa puenteada a la interfaz del anfitrión que tiene conexión a Internet. La interfaz interna será una red virtual host-only o sólo anfitrión, a la que se conectará también el PC cliente.

3. Montar el escenario entre dos alumnos, cada uno simulando una sede desde su casa y obviamente abriendo los puertos del protocolo de VPN utilizado en el router de la conexión a Internet del domicilio, para que ambos puedan tener visibilidad a través de Internet. Este escenario es el más real, pero requiere que dos alumnos de curso se coordinen.

4. Teniendo un anfitrión con suficiente potencia y RAM, simular los cuatro equipos en un sólo anfitrión. Para ello las pasarelas de ambas sedes tendrán una interfaz externa puenteada a la red de anfitrión con conexión a Internet y cada interfaz interna deberá ir puenteada a una red host-only diferente (por ejemplo vboxnet0 y vboxnet1), a las que se conectarán los dos PC cliente simulados también. En caso de no tener suficiente RAM, sería posible simular sólo las dos pasarelas y comprobar que la VPN funciona simplemente haciendo ping entre ambas pasarelas, utilizando obviamente la dirección IP de la interfaz interna, que sin VPN no sería accesible.

5. La última opción y la que os recomiendo es una derivada de la anterior y es que utilicéis GNS3 en vez de un software de virtualización tradicional. GNS3 permite definir una estructura de red mucho más nítida, compleja y versátil. Con otros softwares tendríais que simular la red a base de una combinación de redes internas y externas. Para facilitar la tarea, os he subido a la tarea un proyecto completo (con imágenes base) GNS3. Os he puesto como routers unos Zeroshell, que es un router manejable mediante una interfaz web. Y para facilitar ese manejo os he incluido una máquina ligerísima TinyCoreLinux con Firefox.



El Firefox lo tendríais que conectar al switch correspondiente para configurar los routers. Los routers vienen con un disco duro en blanco sobre el que podéis hacer una instalación. Podéis sustituir los routers por otros Linux y los clientes por otros Linux o Windows. Os incluyo también un proyecto vacío con ReactOS (un Windows libre y ligero) instalado en QEMU por si lo queréis usar.También podéis simular la nube con algo mejor que con un simple switch.

Una vez elegida una de las anteriores opciones para montar el escenario, los PC de las redes locales deberían salir a Internet y hacer ping a direcciones públicas de Internet como a su puerta de enlace, pero obviamente no deberían poder hacerse ping entre las direcciones privadas de las sedes, que son 172.20.0.10 para sede 1 y 172.30.0.10 para sede 2.

Los siguientes pasos para que el escenario esté preparado antes de configurar la VPN site-to-site, son **habilitar** el **ip forwarding** y el **NAT** en el router de cada sede, pues en caso contrario los PC de las redes locales no pueden salir a Internet.

Habilitar ip forwarding

Para habilitar el **ip forwarding** (enrutamiento) en GNU/Linux se puede proceder de la siguiente forma:

- Editar como root el **/etc/sysctl.conf** y poner **net.ipv4.ip_forward=1**
- Aplicar con **sysctl -p**

Habilitar NAT de origen

Para habilitar el **NAT** de origen (realmente es PAT) en el router de la sede, de forma que enmascare las direcciones privadas reemplazándolas por la dirección ip de su interfaz pública, se puede ejecutar como root el comando:

```
iptables -t nat -A POSTROUTING -s 172.20.0.0/24 -o eth0 -j
MASQUERADE
```

Este comando se realizaría en el equipo que hace de router en la sede 1, suponiendo que la interfaz WAN con la ip 192.168.0.20 de la figura, es la eth0. En un entorno de producción, este comando debería ejecutarse en un script de inicio en el sistema, para que sea persistente entre reinicios del router.

Problemas que podemos encontrarnos

Depende de la distribución GNU/Linux usada, en el router puede haber reglas de firewall o no. En caso de que las haya, es necesario deshabilitarlas para la práctica, bien con **iptables -F** o con el comando necesario para parar el firewall como **service iptables stop** o **systemctl stop firewalld.service**. Consultar la documentación de la distribución.

Es posible que tengas que **deshabilitar el firewall de Windows** si los clientes son Windows (pueden ser GNU/Linux perfectamente), para que funcione el ping entre ambos PC una vez establecida la VPN. Puedes pensar que no funciona la VPN y realmente es el firewall de Windows que elimina el ICMP entrante por defecto. La solución más elegante es crear una regla de entrada que permita el ICMP entrante en ambos PC.

Opción 1: VPN site-to-site de "pobres"

Objetivos

Aprender a configurar una VPN site-to-site disponiendo únicamente de servicio SSH entre dos equipos funcionando a modo de pasarela.

Preparación

Se necesita el escenario común explicado en el punto anterior y OpenSSH instalado y funcionando en ambos routers de las sedes

Enunciado

1. Debes configurar una VPN site-to-site entre ambas sedes a través de Internet usando únicamente SSH. Puedes seguir las indicaciones de la siguiente guía para Debian:

Setting up a Layer 3 tunneling VPN with using OpenSSH

2. Es importante que en cada router se añada la ruta para llegar a la red local de la sede remota a través de la VPN. En la guía anterior sólo explica cómo hacerlo en uno de los dos extremos.
3. Una vez establecida la VPN, debes poder hacer **ping** o una **traza** (tracert en Windows, mtr o traceroute en Linux) entre ambos PC a través de la Internet simulada.

Opción 2: VPN site-to-site con OpenVPN

Objetivos

Aprender a configurar una VPN site-to-site con el software OpenVPN

Preparación

Se necesita el escenario común explicado en el punto anterior y OpenVPN instalado en ambos routers de las sedes

Enunciado

1. Debes configurar una VPN site-to-site entre ambas sedes a través de Internet usando OpenVPN.
2. Es importante que en cada router se añada la ruta para llegar a la red local de la sede remota a través de la VPN.
3. Una vez establecida la VPN, debes poder hacer **ping** o una **traza** (tracert en Windows, mtr o traceroute en Linux) entre ambos PC a través de la Internet simulada.

Opción 3: VPN con LogMeIn Hamachi

Es un software comercial muy bien documentado que no tendréis problema en configurar: https://www.vpn.net/

Elabora una memoria como de costumbre.