UNIVERSIDAD TECNICA
FEDERICO SANTA MARIA

Redes de Computadores I

Enlace web remoto a travez de SSh

Juan Badilla Riquelme

Anibal Espinoza Moraga

Cesar Reyes Pino

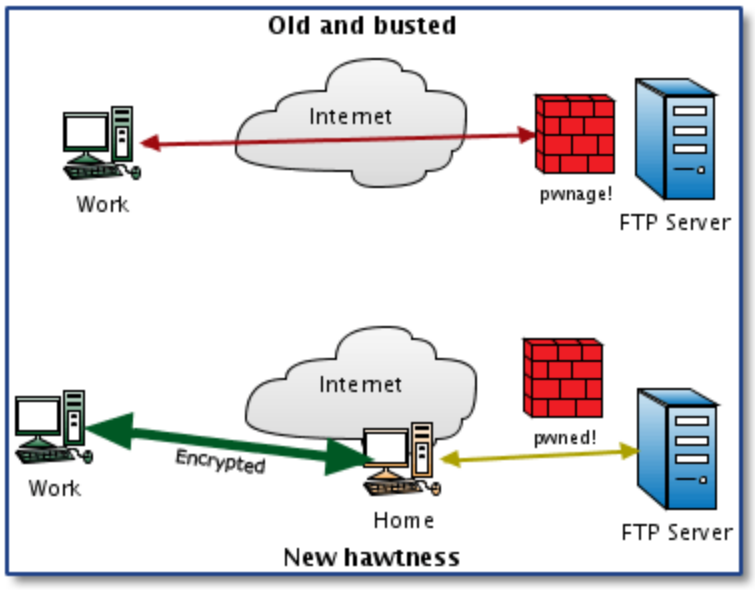
Introducción

Es trabajo tiene el fin de entregar la información necesaria a los usuarios para que por si mismo puedan entender los conceptos de tunneling y otros protocolos que le permitirán crear una conexión con el servidor de la universidad y de esta forma acceder a sitios web que solo se puede acceder desde la universidad. Esta configuración le brindara al usuario un plus frente a los demás porque podrá acceder a información desde la comodidad de su hogar.

En este articulo se vera como lograr lo dicho bajo el comando de ssh (openSSH), trabajando claro, en una maquina con un sistema operativo basado en unix. En windows también se puede lograr, pero se necesita software adicional, el cual es pagado.

Tunneling

Para entender como funciona ssh primero debemos entender lo que es el tunneling. Basicamente esta es una tecnica para comunicarse a través de Internet consiste en encapsular un protocolo de red sobre otro (protocolo de red encapsulador) creando un túnel dentro de una red de computadoras.

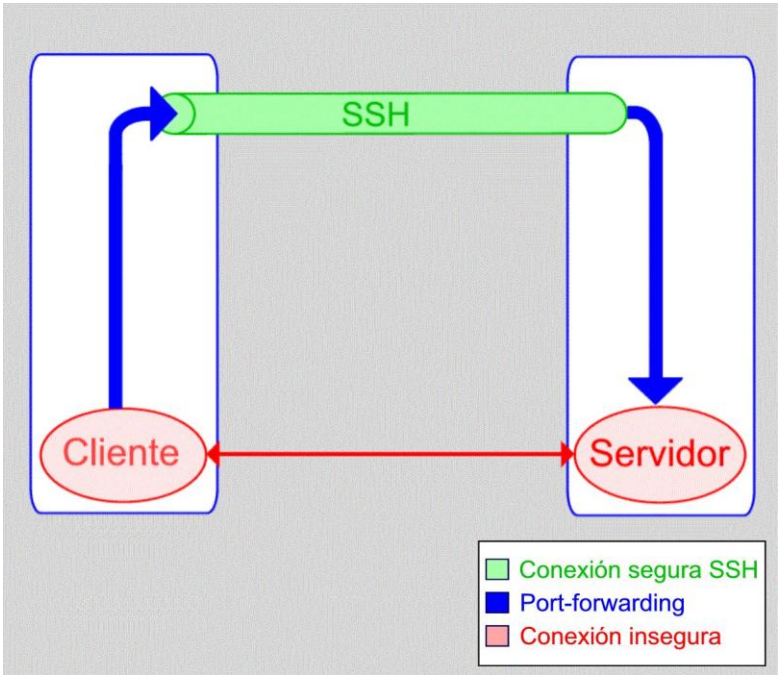


El uso de esta técnica persigue diferentes objetivos, dependiendo del problema que se esté tratando, como por ejemplo la comunicación de islas en escenarios multicast, la redirección de tráfico, etc. Uno de los ejemplos más claros de utilización de esta técnica consiste en la redirección de tráfico en escenarios IP Móvil.

Imaginemos que un Tunneling es como un paquete enviado por una mensajería (ej. chilexpress). El que envia el aquete en una caja que se carga en el camion de chilexpress y viaja por la autopista. El camión (protocolo carrier) viaja por la autopista (Internet) a casa del destinatario (salida del tunnel) y entrega la caja (protocolo de encapsulamiento). El destiantario abre la caja y saca el paquete.

SSH (Secure Shell)

Es un protocolo de red creado creado por el Finlandés Tatu Ylönen en 1995 el cual sirve para acceder a maquinas remotas a través de una red. Permite controlarla por completo a través de un intérprete de comandos.
Ssh de cierta forma llego a reemplazar a Telnet ya que funciona de igual forma, pero con la diferencia que en Telnet la información se envía como texto plano lo que lo hacía muy vulnerable a que una tercera persona pudiera interceptar estos datos.
En SSh la información se envía con una técnica de cifrado de 128bits que hace que la información viaje de manera no legible para terceras personas, lo que se traduce en una mayor seguridad para el usuario.



Opción –D

Para este procedimiento usaremos en específico la opción de Ssh –D la cual hace que cambie el puerto con el cual trabaja por defecto (puerto 22) por cualquier otro puerto asignado por el usuario siempre cuando no esté en uso y sea un puerto mayor al 1023.

SOCKS

SOCKS es un protocolo de Internet que permite a las aplicaciones Cliente-servidor usar de manera transparente los servicios de un firewall de red.

Los clientes que hay detrás de un firewall, los cuales necesitan acceder a los servidores del exterior, pueden conectarse en su lugar a un servidor proxy SOCKS. Tal servidor proxy controla que cliente puede acceder al servidor externo y pasa la petición al servidor. SOCKS puede ser usado también de la forma contraria, permitiendo a los clientes de fuera del firewall("clientes exteriores") conectarse a los servidores de dentro del firewall (servidores internos), este es el caso de una conexión ftp en modo pasivo.

La tecnología del proxy genérico Socks deja al cortafuego el control de las aplicaciones, redes separadas en la Capa de Transporte y deja a los clientes un puerto de peticiones fijo (típicamente 1080). Los clientes realizan peticiones al Socks, especificando el tipo de los servidores y servicios (como HTTP, SMTP o FTP). El proxy Socks (también conocido como servidor Socks) autentifica los clientes y autoriza el acceso a los clientes, configura la conexión al servidor y de forma transparente reenvía cualquier dato enviado o recibido.

El nombre Socks proviene de Socket, el título original del trabajo fue SOCK-et- S. Hay dos versiones principales: Socks v4 y v5. Ambos protocolos se insertan en el modelo OSI entre las capas de transporte y Aplicación. La versión 4 está limitada al manejo de solicitudes de conexión, reglas del proxy y envío de datos. No proporciona ningún tipo de autentificación y está restringido para TCP. Socks v5 (RFC 1928)añade mecanismos de autenticación robustos y soporte extendido a UDP e Ipv6.

Aplicación

Como alumnos de Universidad Técnica Federico Santa María nos interesa aprovechar al máximo los recursos que esta nos brinda, para ellos queremos acceder a sitios que solo son visibles desde esta, como es el caso de la IEEE-Xplore y las revistas y libros digitales que provee la biblioteca USM.

- **Problema**

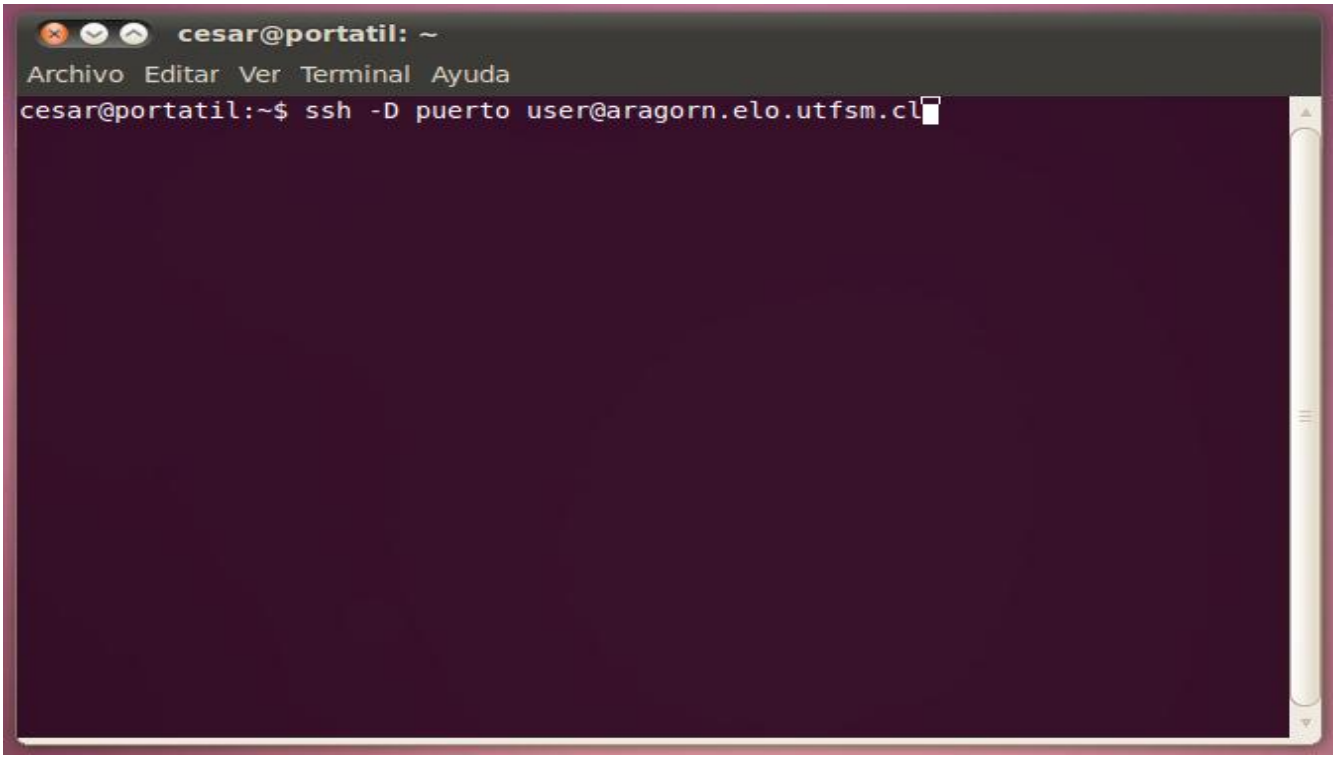
Estas páginas reconocen la ip de la universidad y la autentifican permitiéndole acceder casi toda la información, mientras que si lo hacemos desde nuestra casa, esto no será posible porque nosotros no hemos pagado para poder ver los artículos por lo que nos pedirá autentificarnos y no podremos acceder a la información.

- **Solución**

Crear un túnel a través de open-ssh para conectarnos al servidor aragorn del departamento de Electrónica y de esta forma salir a internet, con ella lograremos hacer la solicitud al sitio web con la ip de la universidad estando en nuestras casa. Para poder enviar la información desde nuestro navegador crearemos un servidor SOCKS.

- **Como hacerlo**

La solución está diseñada para ser ejecutada en Linux (por el momento).
Lo primero que hay que hacer es conectarse al servidor aragorn a travez de open ssh, para esto abrir una terminal y escribir
ssh -D (puerto) user@aragorn.elo.utfsm.cl
Donde puerto es cualquier puerto mayor que 1023 para este caso usaremos el 6969, user es el nombre de usuario que se asigna en el departamento.
Quedando algo así.



Luego hay que configurar el navegador, acá usaremos firefox.
Abrir Firefox e irse a Editar->Preferencias->Avanzado->Red->Configuraciones en esta ventana hay que seleccionar configuración manual de proxy y en Servidor SOCKS colocar localhost y el puerto que pusimos en la conexión de ssh, la opción de la versión el SOCKS para este caso es irrelevante así que puede ser cualquiera.

Por ultimo solo falta comprobar si nuestra configuración es correcta o no. Para ello iremos a este sitio web http://redes.dcsc.utfsm.cl/cualesmiip.html el cual nos dirá nuestra ip, si todo esta bien debería decirnos que somos **200.1.17.102** (juan.elo.utfsm.cl) como lo muestra la figura.

Con esto ya podremos disfrutar tranquilamente de los servicios que nos facilita la universidad desde la tranquilidad de nuestro hogar.

Conclusión

Al utilizar Ssh, se logra realizar un tunneling exitoso, con esto logramos obtener material necesario para el estudio en cualquier parte en la que nos encontremos. Esto nos demuestra lo importante que es el avance y la seguridad en redes, ya que esto es posible gracias al trabajo de muchos. Ahora bien, el uso de esta técnica queda a juicio de cada uno, ya que podemos utilizarla tanto para métodos de estudios como para burlar la censura que impongan en algún trabajo, hay que conocer ambos mundos para darse cuenta de lo bueno y lo malo.

Referencias

1.- SOCK v4 y v5 . http://es.wikipedia.org/wiki/SOCKS
2.- Calcetines para el proxy. http://www.linux-magazine.es/issue/09/Socks.pdf
3.-Tunneling: - http://es.wikipedia.org/wiki/Tunneling
- http://www.34t.com/box-docs.asp?doc=649
4.- SSH http://es.wikipedia.org/wiki/Secure_Shell

Anexo

Video con el procedimiento paso a paso hecho por nosotros.
http://www.youtube.com/watch?v=i54GmEz0Qws