DeSec

Redes, sistemas y seguridad informática.

Bypassing SQUID Proxy with SSH Tunneling

con 2 comentarios

Recientemente, en el instituto en el cual estoy cursando el Ciclo Formativo de Grado Medio de informática, han aplicado ciertas configuraciones de seguridad para que los alumnos no podamos acceder a ciertos sitios Web. Algo que me ha parecido maravilloso por ciertas circunstancias.

Lo que han recurrido a utilizar, es un servidor proxy transparente con un cache de sitios Web (SQUID) con el propósito de ahorrar ancho de banda, mayormente a consecuencia del streaming que solemos acceder normalmente la juventud de hoy en día para visualizar ciertas chorradas, o redes ~~anti~~sociales.

Así que en este breve documento, me gustaría explicarles como sobre pasar dicha seguridad de una forma simple y eficiente sin necesidad de utilizar un servidor proxy configurándolo en nuestro 'addon' de Firefox o instalar ciertos programas como Tor, además, teniendo la ventaja de que nuestros datos viajarán a través de la red ~~in~~seguramente.

Introducción

Este simple método consiste en realizar un túnel por el cual viajarán nuestras tramas de red de una manera segura haciendo uso del protocolo **SSH (Secure Shell)**, a lo que denominamos, "tunneling", desde el equipo del departamento de administración de la empresa en la cual trabajamos (un simple ejemplo), hacia un equipo remoto; por ejemplo el de nuestra casa o un servidor virtual privado (VPS) que tengamos contratado. *Véase la figura 1.1*.

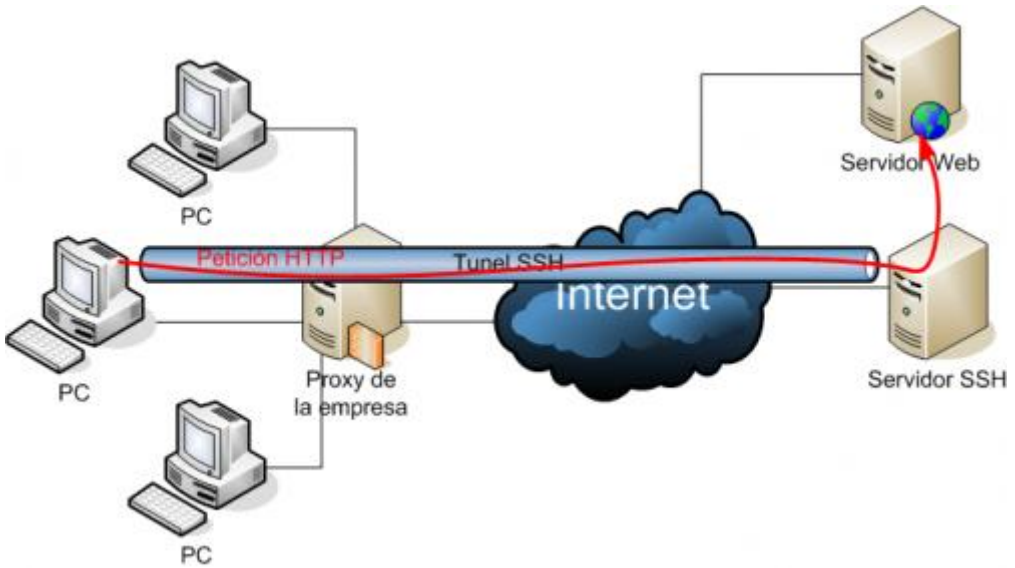

Figura 1.1: SSH Tunneling Architecture

Requisitos básicos

Para comenzar, los requisitos básicos e imprescindibles que necesitaremos, es tener instalado un *servidor* SSH en el **equipo que utilizaremos como túnel.** Si utilizamos un sistema Windows, podemos descargarnos SSHWindows desde SourceForge, si utilizamos GNU/Linux, Open/Solaris, FreeBSD, etc., desde los propios gestores de paquete o manualmente mediante el propio código fuente.

Finalmente, en el **equipo de la empresa** desde donde nos conectaremos a nuestro servidor para abrir dicho túnel, tendremos la posibilidad de instalar Cygwin, activando en la propia instalación a que nos instale el paquete SSH. Otra alternativa factible también puede ser SSHWindows, o bien, PuTTY.

Configuración mínima

Una vez finalizada la instalación del servidor SSH, deberemos de alterar ciertas configuraciones. Normalmente el archivo de configuración en GNU/Linux se encuentra en (*/etc/ssh/sshd_config*), aunque puede ser diferente depende de la distribución que utilicemos o sistema operativo.

Estando en el archivo de configuración del servidor, deberemos de activar la directiva **AllowTcpForwarding** y afirmarla, con el fin de así poder permitir el reenvío o redirección de puertos.

Además, tenemos la posibilidad de aplicarle ciertas configuraciones de seguridad al servidor, para así mantener nuestro sistema más seguro de ciertos *bichos en la red*. Por ejemplo, añadiendo la siguiente directiva al final del archivo: **Match User juanita,pepa,pepote** para que así, tan solo ciertos usuarios del sistema tuvieran acceso a utilizar nuestro tunneling.

Si quisiéramos, también podríamos especificarle a qué grupos permitirle la conexión con la siguiente directiva: **Match Group secretaria**, la cual quiere decir que todos los usuarios pertenecientes al grupo **secretaria** en nuestro sistema, podrían abrir una conexión tunneling.

Creando el túnel

Para ello, abrimos una shell desde donde queramos abrir el túnel y simplemente introducimos el siguiente comando:

```
ssh -D 9999 -C usuario@servidor_ssh_remoto
```

Recuerda: que si estás utilizando Windows, debes de tener instalado SSHWindows, en cambio, si estás utilizando sistemas basados en *nix, depende siempre de la distribución, pero normalmente vienen por defecto instalados.

Éstas son algunas de las opciones que podremos incluir en nuestras configuraciones:

-1 ó **-2**: Fuerza a utilizar la versión 1 ó 2 de la versión de SSH
-4 ó **-6**: Fuerza a utilizar la versión 4 ó 6 del protocolo IP (IPv4 o IPv6)
-f: Pasa en segundo plano la ejecución de SSH (**fork**)
-v: Nos da información adicional durante el proceso (**verbose mode**).

Para más información: **man ssh**

Configurando nuestro navegador

Finalmente, deberemos de configurar nuestro túnel en nuestro navegador como servidor proxy, en el apartado llamado SOCKS, el cual nos permite utilizar de manera transparente los servicios de un firewall de red. *Véase la figura 4.1*.

Figura 4.1: Firefox Proxy (SOCKS) configuration

Algo a tener en cuenta también, es el cifrado de búsquedas de las DNS. Para ello, simplemente nos dirigimos a la configuración de Mozilla Firefox, si es el navegador que estamos utilizando (**about:config**), y modificamos el valor de **network.proxy.socks_remote_dns** a **true** ;-).

Referencias

http://www.ietf.org/rfc/rfc4251.txt
http://www.ietf.org/rfc/rfc1928.txt