Como Dar Seguridad Al Trafico Que Entra Y Sale A Tu Android

Hay pocos problemas de seguridad y una buena dosis de paranoia, y algunos conocimientos técnicos que no hay que descuidar. En el presente articulo veremos la manera de asegurar el envío y recepción de datos móviles en tu dispositivo con **Android** contra los bugs que hay para este SO mediante un simple túnel **SSH**.

Seguramente si estas leyendo esto es por que te gustaría implementar **mayor seguridad** en tu **dispositivo con Android**. Solo sigue los siguientes pasos para lograr esto ;)

Lo Que Necesitara Para El Túnel SSH Para Android

Para esta guía paso a paso necesitaras lo siguiente:

- Un teléfono **Android** con Android OS 1.6 ó superior.
- Una copia gratuita de túnel SSH para Android.
- Un servidor SSH para conectarse.

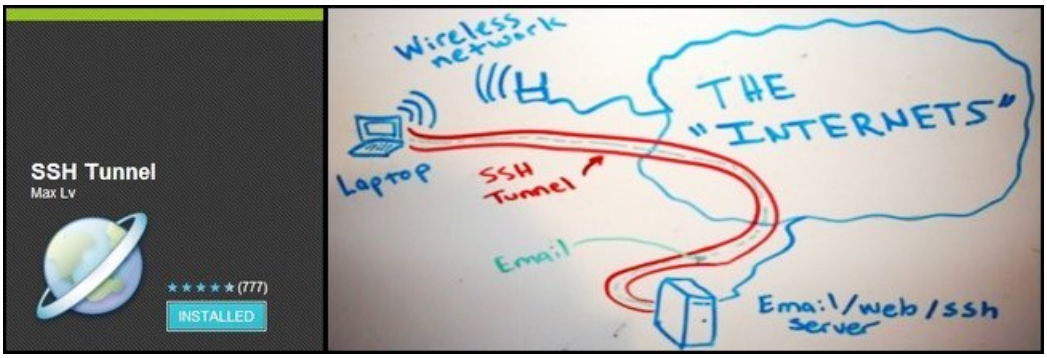
Antes de continuar, es necesario que el dispositivo con Android este **rooteado**, en otras palabras que cuente con **Super**

Usuario. Si el dispositivo aun no esta **rooteado** puede mirar el siguiente articulo para hacerlo. Ademas de lo anterior, debemos de contar con un servidor SSH, podemos tener uno de dos formas, montar un servidor local, y la otra es comprar un **VPS** ó **Servidor dedicado**, si das click en cada opción te llevará a unas magnificas promociones de **Servidor VPS** y **Servidor Dedicado**. Es mejor comprar un **servicio de hosting**, ya que podemos ser mas técnicos y poder mostrar la implementación en cualquier momento.

Ahora bien, en este punto supongo que tendrás tu nombre de usuario y contraseña asignada por el **Servidor SSH.** Ahora si, comencemos!

Descargando Y Configurando Túnel SSH Para Android

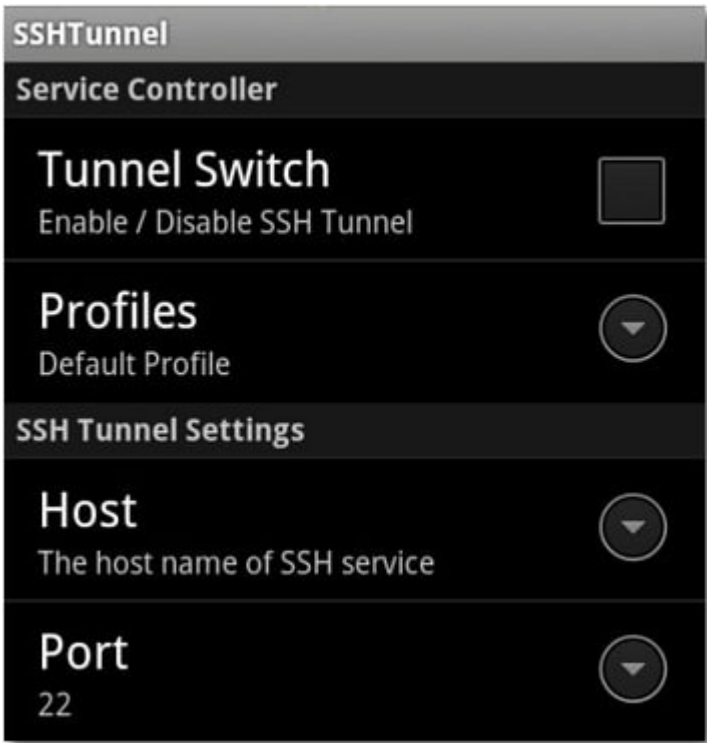
SSH Tunnel, no es la única herramienta para Android, pero si nos inclinamos por esta, ya que es fácil de instalar, configurar facilidad de uso, y ademas es usada en países que registren el uso de libre de la internet (China, entre otros). Si ha funcionado bastante bien para ellos, por que no usarlo nosotros?



Instala esta APP de forma gratuita en la tienda de **Google Play,** en caso dado que no puedas encontrarla, baja el APK e instala manualmente la APP.

Instale la aplicación y al ejecutarla por primera vez

comenzara el proceso para la configuración. El primer pantallazo que verá será el siguiente:



Luego iremos a la parte de «**SSH Tunnel Settings**«, en la parte de **Host** configuraremos la **ip del servidor de SSH,** el puerto por defecto es el 22, pero si tu servidor conecta por otro puerto, cambialo.

En la sección **Account Information**, ingrese su **nombre de usuario** y **contraseña** provista del **servidor SSH**. En este punto tenemos suficiente información introducida para formar una simple conexión entre el **túnel SSH y el servidor SSH** con la autorización basada en la contraseña.

Una vez que tenga el archivo de clave privada (**que termina en. PPK**) tendrás que copiarlo en la siguiente direccion de la SD: **/sdcard/sshtunnel/key/**. Para utilizar la clave, pulse el botón de menú del teléfono para abrir las siguiente opciones :

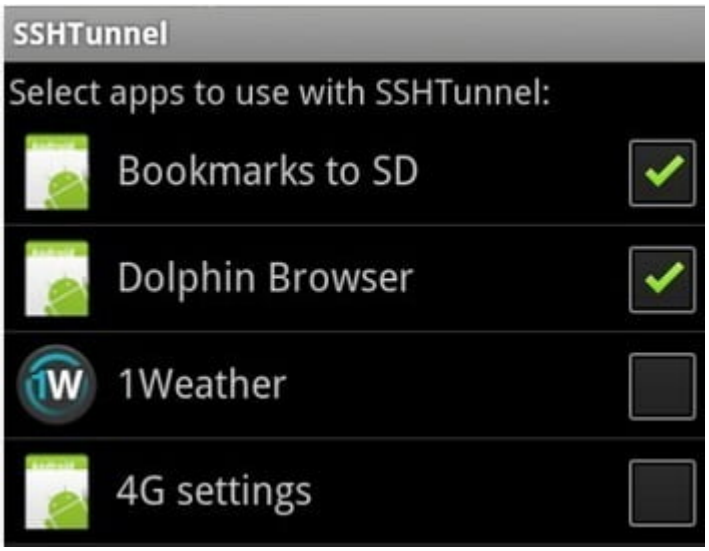
Presione la opción de **Key File Manager** y vaya al directorio /sshtunnel/key/. Seleccione la kEY apropiada para su servidor de SSH. Puede que tengamos diferentes accesos en diferentes servidores SSH, así que un consejo seria renombrar las KEY por algo como: **LlaveServidor1.ppk** o **LlaveServidor2.ppk**.

Una vez que haya establecido, ya sea de la contraseña y / o clave privada, es el momento de terminar la última configuración.

En la sección **Account Information** esta la sección **Port Forwarding**. Con el fin de agilizar el proceso, le sugerimos habilitar en el servidor, los Sockets del proxy integrado con el fin de aumentar la compatibilidad de las aplicaciones con SSH Tunnel. Simplemente marque «**Use socks proxy**» para habilitarlo.

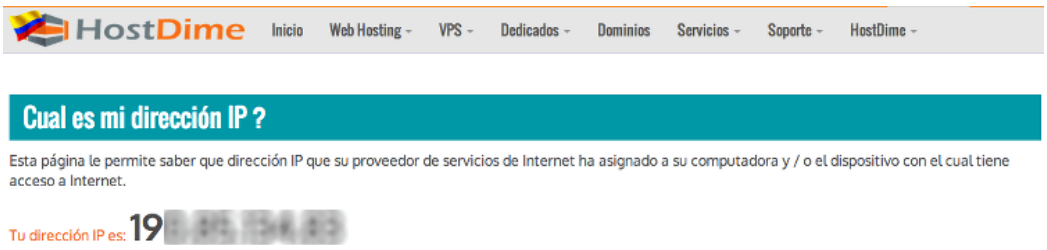
Por último, es el momento de decidir si desea enrutar toda su conexión de datos Android a través de su servidor SSH o

seleccion las aplicaciones que redirigiran las solicitudes a través del servidor. Para dirigir todas las conexiones iremos a «**Global Proxy**«. Para seleccionar las aplicaciones elegimos «**Proxy Individual**» y luego comprobar las aplicaciones individuales que desea enrutar, tales como su navegador web y Facebook, por ejemplo.



SSH Tunnel Funcionando En Android

Para ver el funcionamiento de este método para cubrir nuestros datos, verificamos primero nuestra ip, desde nuestro celular vamos a **https://www.hostdime.com.co/direccion-ip-en-colombia/**, en la parte de abajo veremos la ip en «Tu dirección IP es». Esto lo debemos de hacer mientras este desactivado el SSH Tunnel, con la finalidad de verificar.

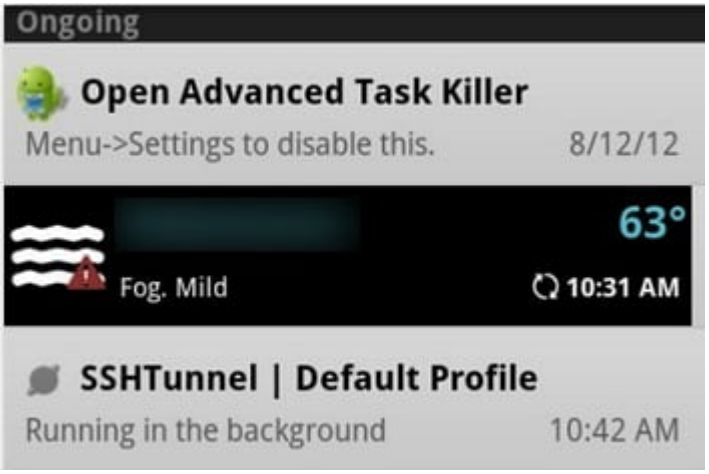


Esa seria la dirección **IP asignada por el proveedor** de telefonía móvil en nuestro **smartphone Android**. Aunque tenemos SSH túnel configurado, todavía no esta funcionando y todavía estamos enviando todas nuestras peticiones DNS y solicitudes

de datos sin la protección que nos da el túnel SSH.

Abrimos SSH Tunnel y, en la parte superior, verifique **Tunnel Switch**. Esto activa el SSH Tunnel, la primera vez tendremos que dar permisos de Super Usuario para el correcto de funcionamiento. Está bien, adelante y marque la casilla Recordar (de lo contrario tendrá que autorizarla cada vez que se conecta).

Hay que esperar un momento para conectar, este nos notificara cuando se haya conectado. Si dejó las notificaciones en el menú de configuración, también verá un aviso en su desplegable buzón de notificaciones de este modo:



Ahora es el momento de comprobar si el navegador está enrutado correctamente a través del **túnel SSH**. Para esto usaremos de nuevo la direccion de **https://www.hostdime.com.co/direccion-ip-en-colombia/**, para verificar que nuestra ip ha cambiado, si ha sido asi, es por que ya estamos protegiendo nuestra seguridad de los datos en nuestro dispositivo con **Android**.