Asegurando nuestras comunicaciones con WireGuard

Descripción

Introducción

En muchos casos como SysAdmins debemos o queremos mantener comunicación con algún servidor desde un punto donde el canal de comunicación puede ser revisado (con sniffers) por otras personas o sistemas. Algunos ejemplos serían:

- Administrar nuestros servidores desde Internet.
- Darle acceso a usuarios a servicios sobre un canal inseguro.
- Brindar seguridad ante sniffer en un canal independientemente de la seguridad de los servicios que brinde.
- Queremos darle acceso a algún servicio de monitoreo al encargado de Seguridad que se encuentra fuera de la red de administración.
- Entre otros…

Una de las soluciones que se presenta para este tipo de problema son las VPN (Virtual Private Network), que permiten crear una red dentro de otra y generalmente cifrada, por lo que los datos que se transmiten se ocultan a los ojos de los interesados, no importa que sean

a servicios no seguros, pues se comunican a través del túnel creado por este servicio.

En la actualidad hay 2 herramientas que son ampliamente para este menester:

- IPSec
- OpenVPN

Ambos son muy buenos en esa tarea y gozan de un gran soporte por todos los equipamientos de red (IPSec más al ser el estándar de facto en muchos routers, como los de CISCO o HUAWEI). El problema a veces con éstos es que su instalación, configuración y puesta en marcha puede resultar un poco tediosa.

Hoy vengo con una propuesta que está ganando mucho terreno a pesar de ser un producto en desarrollo, pero que muchos le han puesto el ojo, es WireGuard y supone una ventaja con respecto a los anteriores por:

- Extremadamente fácil en su instalación y despliegue, ellos indican que *«(…) aims to be easy to configure and deploy as SSH (…)»*.
- Usan criptografía *state-of-the-art* que no es más que la utilización de los algoritmos más modernos de éstos menesteres.
- Al igual que IPSec es compilado como módulo del kernel a través de DKMS. Lo que logra un rendimiento mucho mayor que OpenVPN (pues este es *user-space*).
- Usa los algoritmos de cifrado *Noise Protocol Framework, Curve25519, ChaCha20, Poly1305, BLAKE2, SipHash24, HKDF*.
- Se ha implementado teniendo en cuenta menor cantidad de código, lo que permite una mejor auditoría de código y una menor área de ataque. Está pensado para que una persona pueda auditar todo el código sin complicaciones.
- Entre otras ….

WireGuard por ahora no soporta la asignación dinámica de IP, por lo que cada cliente que tengamos se le debe establecer el ip en su configuración. Además que WireGuard no permite la comunicación de un cliente que no tenga el IP especificado en su fichero de configuración.

Algunas gráficas sobre el rendimiento de WireGuard con respecto a IPSec y OpenVPN pueden verse en Performance of WireGuard

Instalación

Me voy a centrar en la instalación sobre Debian, pues es lo que uso en mis servidores. Debido a que WireGuard es un proyecto en desarrollo, encontrarás los paquetes de su instalación en el repositorio de *sid* que es el repositorio «intestable»:

- wireguard-dkms
- wireguard-tools

Luego de haber bajado los paquetes *.deb* solo debemos instalarlos, además de los *headers* del kernel para la compilación de los módulos del kernel, por ej:

```
apt install dkms
dpkg -i wireguard-dkms.deb wireguard-tools.deb
```

Luego de haberse instalado, el módulo se compila y se integra al kernel actual. Ahora sólo basta configurarlo e iniciar el servidor.

Configuración y despliegue

Hay 2 vías por donde configurar WireGuard, una manual y otra a través de ficheros de configuración que utilizaría la utilidad `wg-quick` para levantarla. La última es la que utilizaré en este manual por ser la más rápida y cómoda.

Lo primero que debemos hacer es generar una llave privada del servidor

```
# wg genkey
iBAnhqypjo6detnodQiHUEL/Wzg/OO5e4IXef6TOnGw=
```

Para generar la llave pública a partir de una privada podemos usar el comando wg pubkey :

```
# echo "iBAnhqypjo6detnodQiHUEL/Wzg/OO5e4IXef6TOnGw=" | wg pubkey
teRk63YIGMHoaDCxS6xxwRd91oek2e378a+X6zunTy8=
```

Esa sería la llave privada del servidor, una duda que me surgió en su momento fue acerca del por qué una llave privada tan pequeña con respecto a las que utilizaba en OpenVPN y en las investigaciones y correos de la lista, esto es debido a que los algoritmos de cifrado que utilizan que es ECC (Elliptic Curve Cryptography) utilizan menos bits para llegar a la misma complejidad criptográfica que RSA a un nivel

superior de bits. Una tabla descriptiva sería:

ECC comparación con RSA

Image not found or type unknown

ECC comparación con RSA

En WireGuard no se define el tamaño de la llave, puesto que WireGuard define ese tamaño para evitar una mala configuración por parte del usuario. WireGuard se asegura que el tamaño de la llave sea lo suficientemente segura para evitar un ataque en intento de descifrar la llave privada desde la pública.

Los ficheros de configuración residen en `/etc/wireguard/` por lo que crearemos nuestro fichero de configuración con el nombre de la interfaz virtual que queremos que tenga, en nuestro ejemplo será `empresa.conf`

```
# Definición de la Interfaz
[Interface]

# Establecer el IP de la interfaz con la máscara de red
Address = 172.16.0.1/24

# Puerto UDP de escucha del servidor
ListenPort = 51820

# Llave privada generada anteriormente
PrivateKey = iBAnhqypjo6detnodQiHUEL/Wzg/OO5e4IXef6TOnGw=

# Indica que cada configuración establecida a través de la interfaz de
# WireGuard sea salvada en el fichero una vez detenido el servidor
SaveConfig = false


# Por cada cliente se establece una sección como esta
[Peer]

# Llave pública del cliente
PublicKey = R2G89C5dpuEOrU9IEzVuuoP3liQzsdnsUyY+cQ+IZQQ=

# IPs (con máscara) que puede tener el cliente que se conecte con esta llave,
# pudiera usarse por ejemplo para un cliente que se conecte por 2 VPN
```

```
AllowedIPs = 172.16.0.2/32
```

Ahora apoyándonos en `systemd` y `wg-quick` podemos habilitar el servidor e iniciarlo:

```
# systemctl enable wg-quick@empresa
# systemctl start wg-quick@empresa
```

Podemos ver que se ha creado la interfaz con:

```
# ip a
...
12: empresa: <POINTOPOINT,NOARP,UP,LOWER_UP> mtu 1420 qdisc noqueue state UNKNOWN group default qlen 1000
link/none
inet 10.11.2.1/24 scope global empresa
   valid_lft forever preferred_lft forever
...
```

O mejor aun para ver todas las interfaces de WireGuard con sus clientes:

```
# wg
interface: empresa
  public key: teRk63YIGMHoaDCxS6xxwRd91oek2e378a+X6zunTy8=
  private key: (hidden)
  listening port: 51820

peer: R2G89C5dpuEOrU9IEzVuuoP3liQzsdnsUyY+cQ+IZQQ=
  allowed ips: 172.16.0.2/32
```

Ahora vamos a configurar a un cliente. Importante decir que WireGuard por ahora no tiene soporte en algo que no sea Linux (la implementación oficial) o Windows (por un port en user-space). Esto es debido a que para otras plataformas habría que implementar el driver en el *kernel-space* por el rendimiento superior, ver más.

Para configurar un cliente en Debian, instalamos los mismos paquetes y creamos un fichero de configuración en el mismo lugar:

```
# Definición de la Interfaz
```

```
[Interface]

# IP de cliente que tiene que coincidir con el permitido en el servidor
Address = 172.16.0.2/32

# Llave privada generada al igual que la del servidor con 'wg genkey'
PrivateKey = 2EHAW9zRKq8OH9Nq7ljF+QiIXPF3WlIs4mF6PFj6In4=

# Si queremos establecer un DNS
DNS = 172.16.0.1

# Definición del servidor al cual conectarse
[Peer]

# Se define la llave pública de dicho servidor
PublicKey = teRk63YIGMHoaDCxS6xxwRd91oek2e378a+X6zunTy8=

# En este apartado se define los IPs que enrutarán por esta interfaz,
# como se puede ver en este caso son todas, es decir, sería la puerta
# de enlace por defecto
AllowedIPs = 0.0.0.0/0

# Dirección del servidor de WireGuard
Endpoint = 10.0.0.1:51820

# Esto define un intervalo en segundos que WireGuard envía un paquete
# nulo para "mantener viva" la conección. Esto es útil en casos de NAT
# para que el firewall mantenga el mismo IP asociado a la conección.
PersistentKeepalive = 25
```

y el procedimiento es el mismo que para el servidor. Ya con esto tenemos un buen servidor de VPN, como pueden observar, el procedimiento es extremadamente sencillo comparado con las otras 2 propuestas.

Categoría

1. Ciberseguridad

2. Servidores

Etiquetas

1. CiberSeguridad
2. VPN
3. WireGuard

Fecha de creación
abril 2018
Autor
h3r3t1c