Universidad Nacional de Rosario
Instituto Politécnico Superior
"General San Martín"

Conexión de Redes Extendidas

Laboratorio PKI y red VPN

Barletta, Luciano - Canut, Iker - Mondino, Georgina

19 de Junio 2019

Resumen

En este informe se explica como crear tu propia Autoridad de Certificación (CA), junto a los certificados y claves para un servidor OpenVPN y multiples clientes. Luego se explica como crear una red simple VPN.

6ºAño Informática

1. Crear tu propia Autoridad de Certificación. Generar certificados y claves para un servidor OpenVPN y múltiples clientes.

1.1. Teoría básica

El primer paso para configurar el OpenVPN es establecer un PKI (Public key Infrastructure). Un PKI consiste de:

- Un certificado separado (Clave pública) y una clave privada para el servidor y cada cliente.
- Un certificado de autoridad "Master" y una clave que se usan para firmar cada uno de los certificados servidor - cliente.

OpenVPN soporta autenticación bidireccional. Esto significa que el cliente verifica la autenticidad del servidor y viceversa, antes de establecer confianza mutua.
Ambos, cliente y servidor, verifican la autenticidad del otro ente verificando que el certificado haya estado firmado por el master CA (Autoridad de Certificación), para luego testear la información del header del certificado (ya autorizado).

Este modelo tiene varias implementaciones valiosas desde el punto de vista del VPN, como pueden ser:

- El server solo necesita su propio certificado y clave, no necesita saber el certificado de cada uno de los clientes que se quieran conectar.
- El server solo acepta clientes cuyos certificados hayan sido firmados por el master CA; y como el servidor puede hacer esta verificación sin la necesidad de acceder a la clave privada, la misma puede residir en una computadora distinta, incluso en una sin conexión.
- Si una clave privada se ve comprometida, puede ser deshabilitada al agregar su certificado al CRL (certificate revocation list).

1.2. Como generar la Autoridad de Certificación Maestra (junto a su Certificado y Clave):

Para la gestión de PKI, en este informe usaremos easy-rsa2. Si no está instalado en su computadora, se puede encontrar en el siguiente link:

https://github.com/OpenVPN/easy-rsa-old

Primero abrimos una terminal, para luego movernos hasta el subdirectorio easy-rsa. Generalmente está en **/usr/share/doc/packages/openvpn**. Se recomienda copiar esta carpeta a otro directorio para evitar sobreescrituras.

Luego editamos el archivo llamado **vars**, poniendo valores a KEY_COUNTRY, KEY_PROVINCE, KEY_CITY, KEY_ORG, y KEY_EMAIL. No se debe dejar ninguno en blanco.

Después inicializamos el PKI.

. ./vars
./clean-all
./build-ca

El comando **build-ca** va a crear el Certificado y la clave de la Autoridad de Certificación, invocando el comando openssl interactivo.

1.3. Como generar el certificado y la clave para el Servidor:

A continuación, ejecutamos el siguiente comando:

./build-key-server server

Cuando se pregunte por el **Common Name**, se puede escribir **server**. Luego, a las dos preguntas, "Sign the certificate? [**y/n**]" y "1 out of 1 certificate requests certified, commit? [**y/n**]" se le debe responder afirmativamente.

1.4. Como generar el certificado y la clave el cliente:

Para generar la información del cliente 1, ejecutamos:

./build-key client1

En el caso de que se quiera generar la información de varios clientes, basta con ejecutar la instrucción con distintos parámetros, como por ejemplo:

./build-key client2
./build-key client3

Y si se quiere proteger las claves de los clientes, se debe especificar en el **build-key-pass** script.

1.5. Como generar los parámetros Diffie Hellman:

Desde la terminal corremos la siguiente instrucción:

./build-dh

El output esperado es:

ai:easy-rsa # ./build-dh
Generating DH parameters, 1024 bit long safe prime, generator 2
This is going to take a long time
.....+.....
.....+.....+.....+.....
.....

1.6. Archivos claves:

Ahora las llaves y certificados se encuentran en el subdirectorio **keys**. En la siguiente tabla se especifican los archivos más relevantes.

Filename	Needed By	Purpose	Secret
ca.crt	server + all clients	Root CA certificate	NO
ca.key	key signing machine only	Root CA key	YES
dhn.pem	server only	Diffie Hellman parameters	NO
server.crt	server only	Server Certificate	NO
server.key	server only	Server Key	YES
client1.crt	client1 only	Client1 Certificate	NO
client1.key	client1 only	Client1 Key	YES
client2.crt	client2 only	Client2 Certificate	NO
client2.key	client2 only	Client2 Key	YES
client3.crt	client3 only	Client3 Certificate	NO
client3.key	client3 only	Client3 Key	YES

1.7. Próximos pasos:

Pero ¿No debería ser posible configurar la PKI sin un canal seguro preexistente? Y la respuesta es sí. En este ejemplo, por simplicidad, se generaron todas las claves en el mismo lugar. Pero las cosas se pueden hacer de otra manera, por ejemplo generando los certificados y claves de los clientes en el servidor, los clientes podrían haber generado sus propias claves privadas localmente y luego enviar una solicitud de firma de certificado (CSR) a la máquina de firma de claves. A su vez, la máquina de firma de claves podría procesar la CSR y devolver el certificado firmado al cliente. Esto se podría lograr sin necesidad de que el archivo secreto **.key** salga del disco de la máquina en la que se generó.

2. Crear tu propia red VPN

2.1. Configuración del servidor:

Para comenzar con la configuración de la red VPN, nos dirigimos a **/usr/share/doc/openvpn/exa**
config-files/ y luego corremos :

gunzip server.conf.gz

Una vez hecho esto, abrimos el archivo **server.conf** y buscamos la linea de **ca**, **crt**, **key** y **dh**, escribiendo las rutas de dichos archivos. También debemos anotar la dirección de la red para luego cargarla en el cliente. Guardamos los cambios y ejecutamos la siguiente instrucción:

openvpn server.conf

2.2. Configuración del servidor:

Del lado del cliente, nos dirigimos nuevamente a la misma carpeta, pero en este caso editamos el archivo **client.conf**, agregando las direcciones de **ca**, **crt** y **key**. Además de esto, se debe reemplazar la linea que dice **remote-server** con la red que se usó en el lado del servidor. Luego guardamos y ejecutamos el siguiente comando:

openvpn client.conf

2.3. Conclusiones

Con esto, queda configurada una red VPN simple entre un servidor y un cliente, pero facilmente se puede expandir a varios usuarios.