istic Informatique Électronique

UNIVERSITÉ DE RENNES 1

SRES TP3

SSL

Master 2 Cybersécurité

2018 - 2019

Encadré par:
Gwenn FEUNTEUN

Réalisé par:
Manon DEROCLES
Alexis LE MASLE

Table des matières

Configurer un service HTTPS

Question 1:
Dans un répertoire temporaire, créez une autorité de certification (étape 3 et 4) avec les paramètres suivants :
• Clé RSA de 2048 bits (4096 seraient mieux, mais trop long à générer dans le cadre de ce TP) ;
• Valable 4 ans ;
• Country = FR, State = IEV, Locality = RENNES, Organization = ISTIC, Organizational Unit = SRES, Common Name = MonACPerso

Voici les deux commandes pour créer un certificat, créé la clé rsa puis crée le certificat avec cette clé générée.

Tout d'abord, on commence par générer l'autorité de certification.

```
openssl  openvt
derocles@derocles:~/Documents/SRES/TP3$ openssl genrsa -out ca.key 2048
Generating RSA private key, 2048 bit long modulus (2 primes)
.....................................+++++
.................................+++++
e is 65537 (0x010001)
derocles@derocles:~/Documents/SRES/TP3$ openssl req -x509 -new -days 1461 -key ca.key -out ca
.pem
Can't load /home/derocles/.rnd into RNG
140249817285056:error:2406F079:random number generator:RAND_load_file:Cannot open file:../cry
pto/rand/randfile.c:88:Filename=/home/derocles/.rnd
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:FR
State or Province Name (full name) [Some-State]:IEV
Locality Name (eg, city) []:RENNES
Organization Name (eg, company) [Internet Widgits Pty Ltd]:ISTIC
Organizational Unit Name (eg, section) []:SRES
Common Name (e.g. server FQDN or YOUR name) []:MonACPerso
Email Address []:
```

Création de l'autorité de certification

Question 2:
Créez un certificat serveur pour le site www.monsite.com , avec les mêmes caractéristiques.

On réalise les mêmes étapes pour créer un certificat client, pour le site www.monsite.com

```
Email Address []:
derocles@derocles:~/Documents/SRES/TP3$ openssl genrsa -out cert.key 2048
Generating RSA private key, 2048 bit long modulus (2 primes)
...+++++
.....................................................+++++
e is 65537 (0x010001)
derocles@derocles:~/Documents/SRES/TP3$ openssl req -new -days 1461 -key cert.key -out cert.csr
Ignoring -days; not generating a certificate
Can't load /home/derocles/.rnd into RNG
140504715264448:error:2406F079:random number generator:RAND_load_file:Cannot open file:../crypto/rand/randfile.c:
88:Filename=/home/derocles/.rnd
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:FR
State or Province Name (full name) [Some-State]:IEV
Locality Name (eg, city) []:RENNES
Organization Name (eg, company) [Internet Widgits Pty Ltd]:ISTIC
Organizational Unit Name (eg, section) []:SRES
Common Name (e.g. server FQDN or YOUR name) []:www.monsite.com
Email Address []:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
derocles@derocles:~/Documents/SRES/TP3$
```

Création du certificat

```
derocles@derocles:~/Documents/SRES/TP3$ openssl x509 -req -CAcreateserial -in cert.csr -CA ca.pem
CAkey ca.key -out cert.pem
Signature ok
subject=C = FR, ST = IEV, L = RENNES, O = ISTIC, OU = SRES, CN = www.monsite.com
Getting CA Private Key
```

Signature du certificat

Question 3:
Activez la prise en charge de HTTPS sur le service avec ce certificat.

Nous créeons un fichier *monsite.com* dans le dossier *etc/apache2/sites-available/* où nous mettons les configurations pour le port 80 (http) puis pour le port 443 pour le https.

```
 GNU nano 2.7.4                    Fichier : /etc/apache2/sites-available/monsite.com.conf

<VirtualHost *:80>
    ServerName monsite.com
    ServerAlias www.monsite.com
    ServerAdmin webmaster@monsite.com
    DocumentRoot /srv/web/monsite.com/www
        <Directory /srv/web/monsite.com/www>
                Options -Indexes +FollowSymLinks +MultiViews
                AllowOverride none
                Require all granted
        </Directory>
        ErrorLog /var/log/apache2/error.monsite.com.log
        CustomLog /var/log/apache2/access.monsite.com.log combined
</VirtualHost>

<VirtualHost *:443>
    ServerName monsite.com
    ServerAlias www.monsite.com
    ServerAdmin webmaster@monsite.com
    DocumentRoot /srv/web/monsite.com/www
        <Directory /srv/web/monsite.com/www>
                Options -Indexes +FollowSymLinks +MultiViews
                AllowOverride none
                Require all granted
        </Directory>
        # directives obligatoires pour TLS
        SSLEngine on
        SSLCertificateFile    /etc/letsencrypt/live/monsite.com/fullchain.pem
        SSLCertificateKeyFile   /etc/letsencrypt/live/monsite.com/privkey.pem
        Header always set Strict-Transport-Security "max-age=15768000"
        ErrorLog /var/log/apache2/error.monsite.com.log
        CustomLog /var/log/apache2/access.monsite.com.log combined
</VirtualHost>
```

Fichier de configuration de www.*monsite.com* pour apache2

Nous réussissons à nous connecter au port 80.

Succès de la connexion au port 80 sur le serveur

Nous réussissons également à nous connecter en https

Succès de la connexion au port 443 sur le serveur

Pour vérifier que nous possédons le bon certificat nous l' affichons sur le navigateur. C'est bien le certificat que nous avons créé.¶¶

Certificat présent lors de la connexion sur le navigateur en https

Configurer un service OpenVPN

Question 2:
Créez un certificat pour le serveur et un autre pour le client VPN (avec les CN respectifs « serveur » et « client »).

Pour générer un certificat SSL server pour openvpn (respectivement client) on utilise les commandes suivante:

```
istic-web:/etc/openvpn# openssl genrsa -out server.key 2048
ating RSA private key, 2048 bit long modulus
.....+++
65537 (0x010001)
```

```
root@istic-web:/etc/openvpn# openssl req -new -key server.key -out server.csr
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:FR
State or Province Name (full name) [Some-State]:IEV
Locality Name (eg, city) []:RENNES
Organization Name (eg, company) [Internet Widgits Pty Ltd]:ISTIC
Organizational Unit Name (eg, section) []:SRES
Common Name (e.g. server FQDN or YOUR name) []:vpnServer
Email Address []:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
root@istic-web:/etc/openvpn# openssl x509 -req -CAcreateserial -in cert.csr -CA
```

```
root@istic-web:/etc/openvpn# openssl x509 -req -CAcreateserial -in server.csr -C
A ca.pem -CAkey ca.key -out serveur.pem
Signature ok
subject=C = FR, ST = IEV, L = RENNES, O = ISTIC, OU = SRES, CN = vpnServer
Getting CA Private Key
```

Question 3:
Générez des paramètres Diffie-Hellman de 2048 bits dans dh2048.pem.

```
root@istic-vpn:/etc/openvpn# openssl genpkey -genparam -algorithm dh
-out dh2048.pem
.................+.........................+.........................
.+.....................................................+.+........+..
.....................................................................
.......................+.............+...........+.................
.....................................................................
.....................................................+.............
.........................+.................+..++*++*++*
```

```
-----BEGIN DH PARAMETERS-----
MIGHAoGBALFTeYpCdIRvWEpcP9XsiyfDJT53zDk3nFkwDNmEHSHeQiWJsp/zcVf2
CiB4pkOC5BGoUS/Ijm5ZKq9lDzwCk2sldI3Eo+wExFMlztS26eisgI0R9+BQ1IDY
HtYCNge7zFTXpjeVjiHGRli87pOdXhwdWMI+HKmytaUGhOLKh5CTAgEC
-----END DH PARAMETERS-----
```

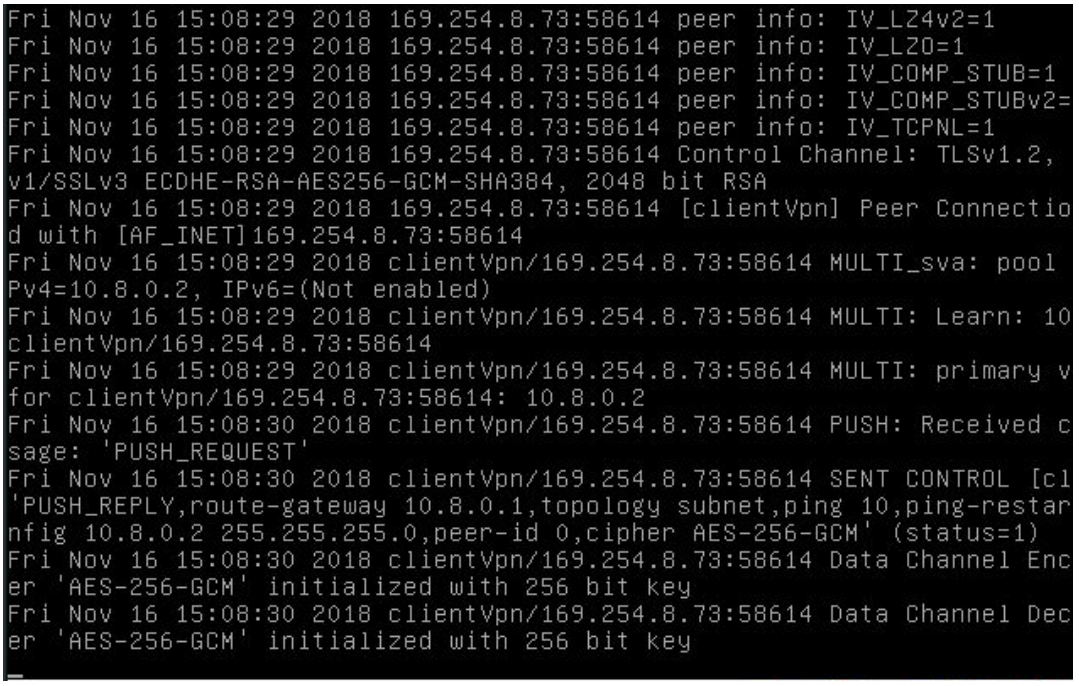
Question 4:
Mettez en place le serveur OpenVPN sur la machine serveur. Vous pourrez trouver un fichier de configuration déjà prêt dans le répertoire /usr/share/doc/openvpn/examples/sample-config-files/.
Copiez le fichier de configuration serveur d'exemple.

Question 5:
Mettez en place le serveur OpenVPN sur la machine cliente. Vous pourrez trouver un fichier de configuration déjà prêt dans le répertoire /usr/share/doc/openvpn/examples/sample-config-files/. Copiez le fichier de configuration client d'exemple

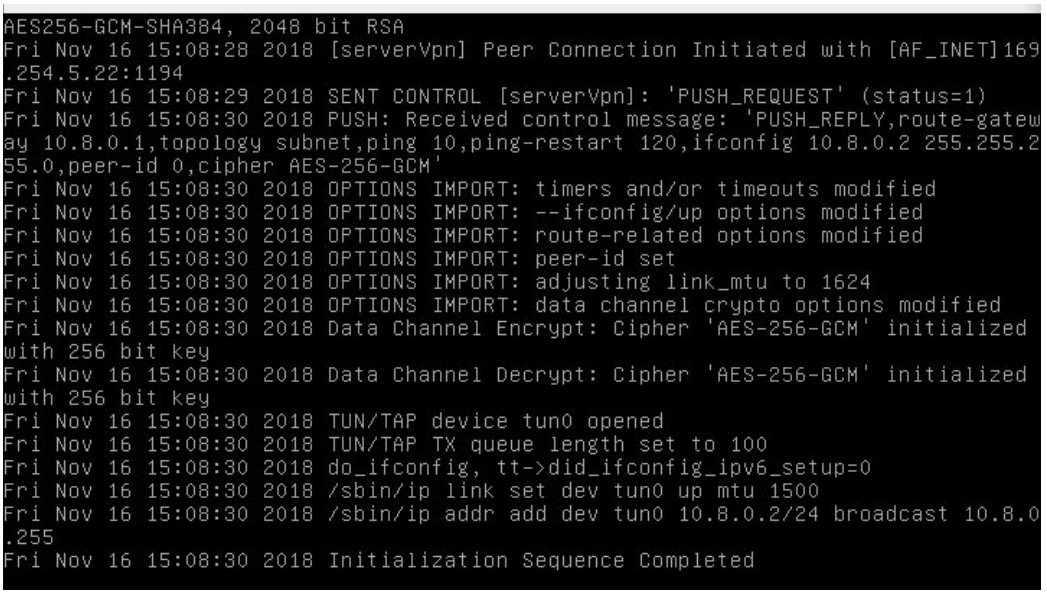
Question 6:
Lancez le serveur et le client pour établir la connexion VPN :

- **Sur le serveur : openvpn /etc/openvpn/server.conf**
- **Sur le client : openvpn /etc/openvpn/client.conf**

Mettez une machine en écoute avec netcat et connectez-vous avez l'autre en utilisant les adresses IP attribuées par le VPN, vous devez pouvoir vous échanger des messages.



Serveur VPN



Client VPN

Grâce aux commandes openvpn /etc/openvpn/server.conf et openvpn /etc/openvpn/client.conf, nous lançons le serveur VPN et le client associé. Ces captures d'écran nous montre que la liaison s'est bien faite entre les deux machines.