HTTPS

Chiffrement des communications

Mise en place des certificats

Pour commencer, on installe SSL car c'est grâce à ça que l'on pourra générer un certificat :

```
apt-get install openssl
```

Ensuite, nous créons un dossier pour stocker nos certifcats, puis on s'y rends :

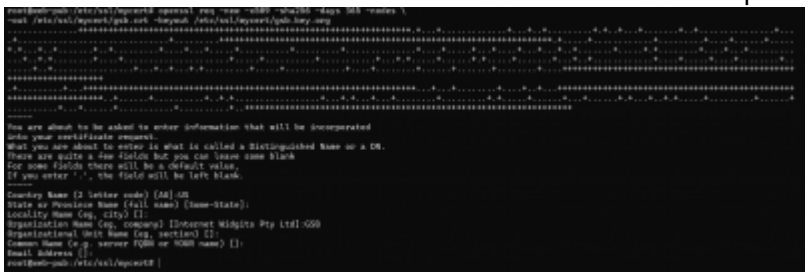
On crée ensuite un répertoire /etc/ssl/localcert pour stocker le certificat (auto-signé) et sa clé :

```
mkdir /etc/ssl/mycert
#il faudra s'y déplacer avec la commande cd
# cd  /etc/ssl/localcerts
```

Une fois dans le répertoire, on crée le certificat TLS.
Un certificat TLS (Transport Layer Security) est un élément crucial de la sécurité des communications sur Internet, assurant l'authenticité, l'intégrité et la confidentialité des données échangées entre les parties. Pour le créer on claque 2 commandes :

```
#on annonce le directory
DIR=/etc/ssl/mycert
Enfin, nous créons les deux certificats
#on crée le certificat
openssl req -new -x509 -sha256 -days 365 -nodes \
-out /etc/ssl/mycert/gsb.crt -keyout /etc/ssl/mycert/gsb.key.org
```

On nous demandera de rentrer des informations telles que le pays, la région, la ville, etc...



Modifications dans Apache

Il faut rajouter dans chaque Vhost un bloc pour le port 443. Adaption du virtuals.conf :

il faut ajouter dans chaque Vhost , un autre bloc 443 .

sisr2-usa:gsb.conf

sisr2-usa:usa.gsb.conf

sisr2-usa:cloud.usa.gsb.conf

sisr2-usa:wiki.usa.gsb.conf

Nb : wiki et nextcloud sont sur la 240

Une fois fais, on active le module SSL pour Apache et les Vhost SSL par défaut :

```
#activation de ssl pour apache
a2enmod ssl

#activation du vhost ssl par défaut
a2ensite default-ssl
```

On modifie le fichier /etc/apache2/sites-available/default-ssl.conf et on adapte, de la même manière, les directives suivantes :

Il faut mettre ici les bons chemins, à savoir :

- /etc/ssl/mycert/gsb.crt
- /etc/ssl/mycert/gsb.key.org

On vérifie que le port 443 est bien activé/en écoute (listen) :

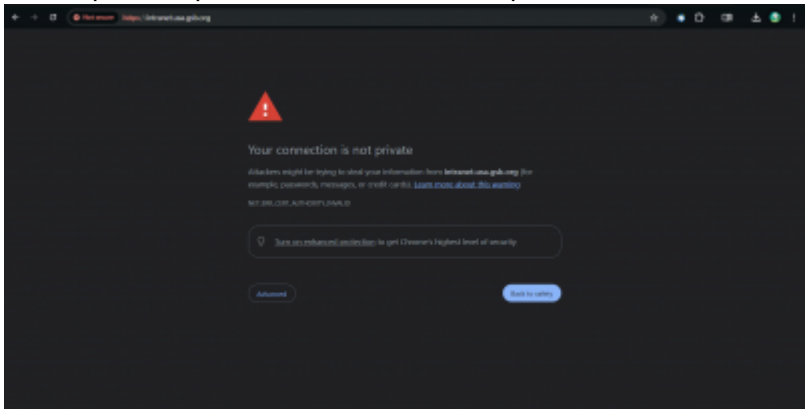
```
netstat -nat
```

```
tcp6       0      0 :::443                  :::*                    LISTEN
```

On redémarre apache :

```
systemctl restart apache2
```

On test avec un navigateur web (Chrome, Mozilla, Opera). Le navigateur nous affichera un énorme warning comme quoi le certificat est auto-signé (pas reconnu par une autorité). On accepte malgré les risque. On peut aussi le voir en cliquant sur “Non sécurisé” (fait depuis le navigateur Chrome) :



Cela nous renvoie directement sur la partie des certificats sécurisés :

FTPS

FTPS

Pour mettre en place le SSL/TLS pour proftp, nous devons d'abord créer la paire de clés RSA. Pour ce faire, Nous nous déplaçons donc dans le dossier ssl de proftpd puis nous utilisons la commande openssl

Il faut aller dans le dossier /etc/proftpd/

```
cd /etc/proftpd
```

Création du dossier SSL

```
mkdir ssl
```

Se déplacer dans le dossier </sxh>

```
cd ssl
```

♦ Génération du certificat ssl auto-signé et la clé : openssl req -x509 -nodes -days 365 -newkey rsa:2048 -out proftpd-rsa.pem -keyout proftpd-key.pem

Éditer le fichier /etc/proftpd/proftpd.conf et activer TLS en décommentant la ligne :

- # This is used for FTPS connections
- Include /etc/proftpd/tls.conf

```
  GNU nano 7.2                                                    /etc/proftpd/proftpd.co
#Include /etc/proftpd/ldap.conf
#Include /etc/proftpd/sql.conf

#
# This is used for FTPS connections
#
Include /etc/proftpd/tls.conf

#
# This is used for SFTP connections
#
#Include /etc/proftpd/sftp.conf

#
# This is used for other add-on modules
#
#Include /etc/proftpd/dnsbl.conf
#Include /etc/proftpd/geoip.conf
#Include /etc/proftpd/snmp.conf
```

Ensuite, nous activons le module tls dans le fichier /etc/proftpd/modules.conf. Il nous suffit de dé-commenter la ligne suivante :

```
  GNU nano 7.2                                                    /etc/proftpd/modules.conf
#
# This file is used to manage DSO modules and features.
#

# This is the directory where DSO modules reside

ModulePath /usr/lib/proftpd

# Allow only user root to load and unload modules, but allow everyone
# to see which modules have been loaded

ModuleControlsACLs insmod,rmmod allow user root
ModuleControlsACLs lsmod allow user *

#This is required only if you need to set IdentLookups on
#LoadModule mod_ident.c

LoadModule mod_ctrls_admin.c

# Install proftpd-mod-crypto to use this module for TLS/SSL support.
LoadModule mod_tls.c
# Even these modules depend on the previous one
#LoadModule mod_tls_fscache.c
#LoadModule mod_tls_shmcache.c
```

Pour finaliser la configuration, nous dé-commentons plusieurs lignes du fichier /etc/proftpd/tls.conf. On y active le TLS, spécifie l'emplacement des logs et des certificats et active des options.

```
  GNU nano 7.2                                                    /etc/proftpd/modules.conf
#
# This file is used to manage DSO modules and features.
#

# This is the directory where DSO modules reside

ModulePath /usr/lib/proftpd

# Allow only user root to load and unload modules, but allow everyone
# to see which modules have been loaded

ModuleControlsACLs insmod,rmmod allow user root
ModuleControlsACLs lsmod allow user *

#This is required only if you need to set IdentLookups on
#LoadModule mod_ident.c

LoadModule mod_ctrls_admin.c

# Install proftpd-mod-crypto to use this module for TLS/SSL support.
LoadModule mod_tls.c
# Even these modules depend on the previous one
#LoadModule mod_tls_fscache.c
#LoadModule mod_tls_shmcache.c
```

On redémarre proftpd

```
systemctl restart proftpd
```

On corrige les erreurs s'il y en a (on vérifie les fichiers de log si besoin). On vérifie ensuite en testant avec un client (compte std par exemple) FTP, FileZilla par exemple (c'est ce que j'utilise).

Test et verifications.