Voici une documentation formatée pour DokuWiki pour l'installation de TLS sur ProFTPD :

—

Configuration TLS sur ProFTPD

Cette documentation explique comment configurer TLS sur un serveur FTP avec ProFTPD.

Étape 1 : Préparer le dossier de configuration

1. Aller dans le dossier de configuration de ProFTPD :

```
cd /etc/proftpd/
```

1. Créer un dossier pour les fichiers SSL :

```
mkdir ssl
```

1. Se déplacer dans le dossier créé :

```
cd ssl/
```

Étape 2 : Générer le certificat SSL auto-signé et la clé

1. Exécuter la commande suivante pour créer un certificat et une clé :

```
openssl req -x509 -nodes -days 365 -newkey rsa:2048 -out proftpd-rsa.pem
-keyout proftpd-key.pem
```

1. **Options** :
    1. **-newkey rsa:2048** : Taille de la clé
    2. **-nodes** : Pas de phrase de passe
    3. **-days 365** : Durée de validité du certificat (1 an)
    4. **-out proftpd-rsa.pem** : Fichier de certificat
    5. **-keyout proftpd-key.pem** : Fichier de clé
2. Protéger la clé générée :

```
chmod 440 proftpd-key.pem
```

Étape 3 : Configurer ProFTPD pour utiliser TLS

1. Éditer le fichier de configuration principal `/etc/proftpd/proftpd.conf` et activer TLS en décommentant la ligne suivante :

```
Include /etc/proftpd/tls.conf
```

1. Éditer le fichier de configuration TLS `/etc/proftpd/tls.conf` et ajouter les paramètres suivants :

```
<IfModule mod_tls.c>
  TLSEngine on
  TLSLog /var/log/proftpd/tls.log
  TLSProtocol SSLv23
  TLSRSACertificateFile /etc/proftpd/ssl/proftpd-rsa.pem
  TLSRSACertificateKeyFile /etc/proftpd/ssl/proftpd-key.pem
  TLSOptions AllowClientRenegotiations
  TLSRequired on
  TLSRenegotiate required off
</IfModule>
```

Étape 4 : Redémarrer ProFTPD

1. Redémarrer le service pour appliquer les modifications :

```
/etc/init.d/proftpd restart
```

1. En cas d’erreur, lancer ProFTPD en mode manuel pour diagnostiquer :

```
proftpd
```

Étape 5 : Tester le serveur

1. **Avec `lftp` (client en ligne de commande) :**
    1. Installer `lftp` si nécessaire :

```
```

```
apt install lftp
```

1. Lancer le test interactif :

```
lftp
set ftp:ssl-allow true
set ssl:verify-certificate no
open 127.0.0.1
user std
```

1. **Avec FileZilla :**
    1. Ajouter un nouveau site dans le gestionnaire de sites et configurer la connexion en FTPES.

Étape 6 : Analyser les logs et le trafic réseau (optionnel)

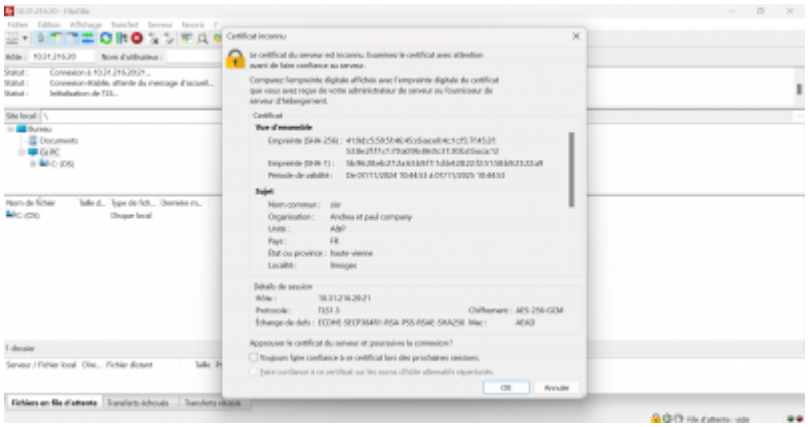
1. **Vérifier les logs :**
    1. Les logs TLS se trouvent dans `/var/log/proftpd/tls.log`.
2. **Analyser le trafic TLS avec tcpdump :**
    1. Pour capturer les paquets FTP :

```
tcpdump -n -i lo -X -s0 port 21
```

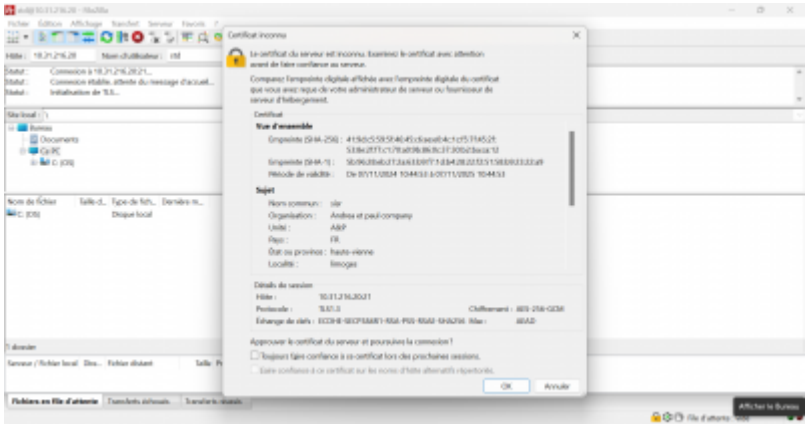
Tests

Nous devons maintenant tester les certificats et leur implémentations, pour ça on peut utiliser FileZilla.

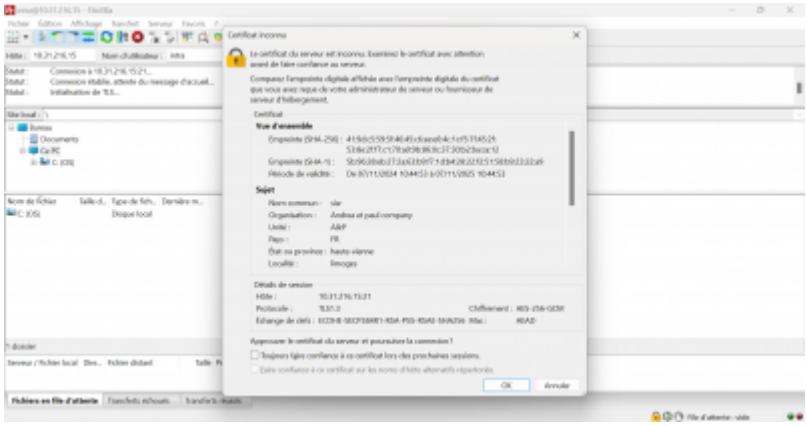
Anonymous



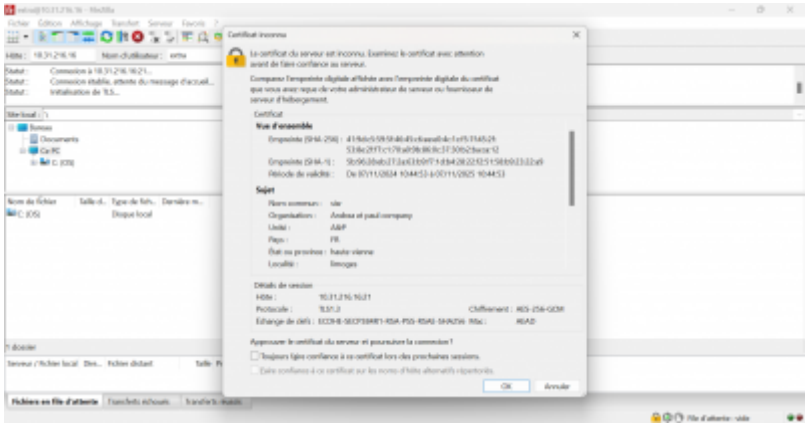
std



intra



extra



HTTPS

TLS (Transport Layer Security) est un protocole de sécurité conçu pour faciliter la confidentialité et la sécurité des données sur les communications Internet.

HTTPS(HyperText Transfert Protocole): c'est un protocole de communication et de transfert de fichiers entre un client et un serveur web. Le “S” signifie “Secure”: c'est la version sécurisée du protocole par le chiffrement et l'authentification. Open-SSL: C'est une boîte à outils de chiffrement qui permet de chiffrer les communications sur un réseau grâce au protocole TLS/SSL.

Création d'un certificat

Rendons nous sur le serveur web (10.31.208.80). Installons openssl :

```
apt update
apt install openssl
```

Nous devons créer un répertoire où seront stocké les certificats :

```
mkdir /etc/ssl/mycert/
```

Puis nous pouvons entrer la commande permettant de générer un certificat :

```
openssl req -new -x509 -sha256 -days 365 -nodes -out /etc/ssl/mycert/gsb.crt
-keyout /etc/ssl/mycert/gsb.key.org
```

•-req : Permet de créer et traiter les demandes de certificats. •-keyout : La clef •-out : Le certificat •-nodes : Pas de phrase de passe lors de l'utilisation pour le déverrouiller (no DES) •-days 365 : Correspondant à la durée de validité du certificat Lorsqu'on exécute cette commande, on nous demandera des informations de plus à compléter pour finaliser l'obtention du certificat:

```
Generating a RSA private key..............................++++
.....................................................++++
writing new private key to '/etc/ssl/mycert/gsb.key.org'
-----
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]:Haute-Vienne
Locality Name (eg, city) []:Limoche
Organization Name (eg, company) [Internet Widgits Pty Ltd]:PaulIndustrie
Organizational Unit Name (eg, section) []:
Common Name (e.g. server FQDN or YOUR name) []:www.paulindustrie.org
Email Address []:max.color87@gmail.com
```

Activation du VHost SSL par défaut d'Apache

Nous devons activer le VHost SSL par défaut d'Apache.

Pour cela on tape les commande :

```
a2ensite default-ssl
```

Pour nous assurer que ssl est bien activé :

```
cat /etc/apache2/sites-available/default-ssl.conf
```

Normalement ces lignes doivent être décommenté :

```
SSLEngine On → pour activer la fonction
SSLCertificateFile /etc/ssl/mycert/gsb.crt → préciser le chemin ou
l'emplacement vers le certificat
SSLCertificateKeyFile /etc/ssl/mycert/gsb.key.org → pour préciser
l'emplacement du
fichier contenant la clé
```

Puis pour finaliser on tape les commandes :

```
a2enmod ssl
systemctl restart apache2
```

Création des VHosts pour solutions

Notre objectif maintenant est de chiffrer la solution Nextcloud et la solution DokuWiki. Pour cela on se rend dans leurs VirtualHosts :

```
nano /etc/apache2/sites-available/dokuwiki.conf
```

Dans ce fichier nous allons rajouter un VirtualHost fonctionnant sur le port 443 :

```
<VirtualHost *:443>
 ServerAdmin webmaster@beaupeyrat.com
 ServerName docs.oceanie.gsb.org
 DocumentRoot /home/htdocs/dokuwiki-2024-02-06b
 ErrorLog /var/log/apache2/docs-error.log
 CustomLog /var/log/apache2/docs-access.log combined
 <Directory /home/htdocs/dokuwiki-2024-02-06b>
 Require all granted
 AllowOverride All
 </Directory>
 SSLEngine on
 SSLCertificateFile     /etc/ssl/mycert/gsb.crt
 SSLCertificateKeyFile  /etc/ssl/mycert/gsb.key.org
</VirtualHost>
```

De plus, on rajoute une ligne dans le VHost du port 80 pour lui dire de nous rediriger vers le port 443 :

```
<VirtualHost *:80>
```

```
 ServerAdmin webmaster@beaupeyrat.com
 ServerName docs.oceanie.gsb.org
 DocumentRoot /home/htdocs/dokuwiki-2024-02-06b
 ErrorLog /var/log/apache2/docs-error.log
 CustomLog /var/log/apache2/docs-access.log combined
 <Directory /home/htdocs/dokuwiki-2024-02-06b>
 Require all granted
 AllowOverride All
 </Directory>
 redirect permanent / https://docs.oceanie.gsb.org
</VirtualHost>
```

On fait la même chose avec NextCloud :

```
nano /etc/apache2/sites-available/nextcloud.conf
```

```
<VirtualHost *:80>
  DocumentRoot /home/htdocs/nextcloud
  ServerName  intranet.oceanie.gsb.org
  ErrorLog /var/log/apache2/intra-error.log
  CustomLog /var/log/apache2/intra-access.log combined

  <Directory /home/htdocs/nextcloud>
    Require all granted
    AllowOverride All
    Options FollowSymLinks MultiViews

    <IfModule mod_dav.c>
      Dav off
    </IfModule>
  </Directory>
 redirect permanent / https://docs.oceanie.gsb.org
</VirtualHost>

<VirtualHost *:443>
  DocumentRoot /home/htdocs/nextcloud
  ServerName  intranet.oceanie.gsb.org
  ErrorLog /var/log/apache2/intra-error.log
  CustomLog /var/log/apache2/intra-access.log combined

  <Directory /home/htdocs/nextcloud>
    Require all granted
    AllowOverride All
    Options FollowSymLinks MultiViews

    <IfModule mod_dav.c>
      Dav off
    </IfModule>
  </Directory>
 SSLEngine on
 SSLCertificateFile     /etc/ssl/mycert/gsb.crt
```

```
 SSLCertificateKeyFile  /etc/ssl/mycert/gsb.key.org
</VirtualHost>
```

```
systemctl restart apache2
```

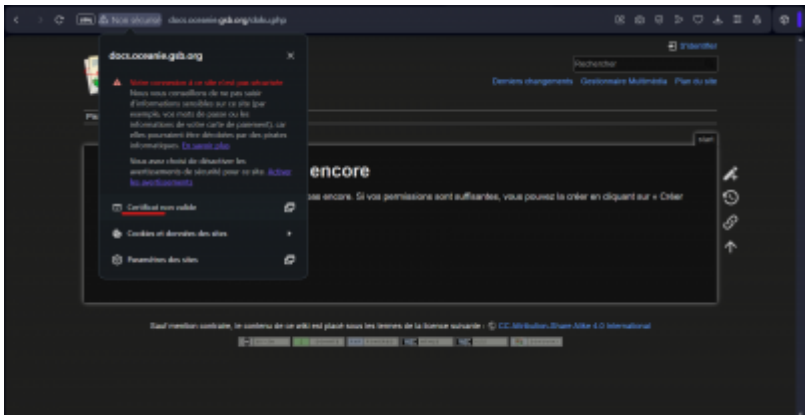
On recommence

Sur notre deuxième serveur web on refait la même chose (création du certificat etc...) pour le site gsb.org et oceanie.gsb.org.

Tests

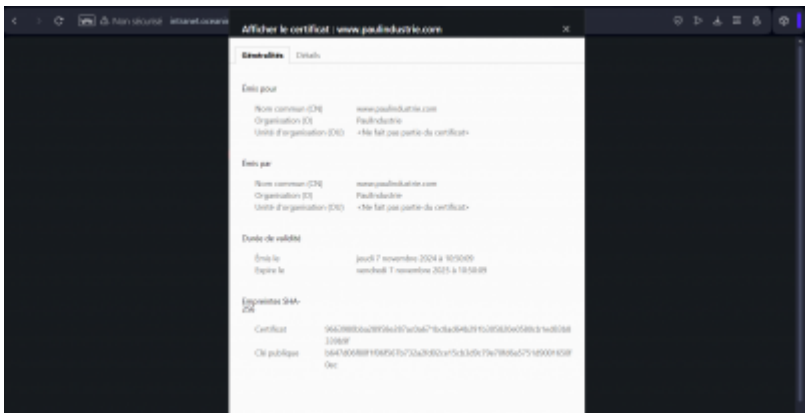
Pour tester ceci, on se rend sur les URLs de nos sites et on vérifie que les certificats sont présents.

DokuWiki



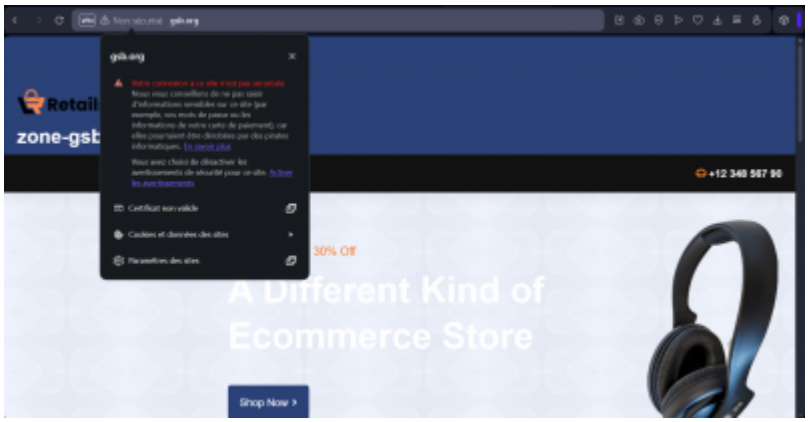
On voit bien qu'un certificat est présent sur cette page web (la page reste non-sécurisé car le certificat est auto-signé).

NextCloud



On peut même voir les détails du certificats.

gsb.org



oceanie.gsb.org