

[Aller au contenu](#)

SSL / TLS

♦ Premièrement, installation d'openssl :

```
1 | apt-get install openssl
```

♦ Ensuite on créer le répertoire

```
1 | mkdir /etc/ssl/localcerts
```

♦ Pour continuer on a créer un certificat :

```
1 | root@http-pub:~# openssl req -new -x509 -sha256 -days 365 -nodes -out /etc/ssl/localcerts/gsb.crt -keyo
```

♦ Explications :

- REQ permet de créer et traiter les demandes de certificats.
 - NEW permet de générer la demande de certificat.
 - NODES désactive le chiffrement de la clé privé.
 - KEYOUT donne le nom ou le fichier ou la clé privée sera crée.
 - OUT nom du fichier de sortie (cela correspond au certificat).
 - DAYS nombre de jour ou le certificat est valide.
-

- ♦ On obtient ça :

```
-----BEGIN CERTIFICATE-----
MIIDrTCCApWgAwIBAgIUcxA7R0jZ8tLarCVxfuvnrhNM1mswDQYJKoZIhvcNAQEL
BQAwZjELMAkGA1UEBhMCRLiExEzARBgNVBAgMC1NvbWUtU3RhdGUxITAfBgNVBAoM
GE1udGVybmV0IFdpZGdpdHMgUHR5IEEx0ZDEfMB0GCsQGSIB3DQEJARYQYWRTaW5n
QGdtYWlsLmNvbTAeFw0yMTE5MDkxMDE5NDRaFw0yMjExMDkxMDE5NDRaMGYxCzAJ
BgNVBAYTAkZSMRMwEQYDVQIDApTb211LVN0YXR1MSEwHwYDVQQKDBhJbnRlcm5l
dCBXaWRnaXRzIFB0eSBMDGQxH2AdBgkqhkiG9w0BCQEWEGFkbWluZ0BnbWFPbC5j
b20wggeiMA0GCsQGSIB3DQEBAAUAA4IBDwAwggEKAoIBAQPdPrHI7zDe0IPKktWd+
l4xUkzEbVQkk/L76nZsh3XGrTNePZqyrS/SHtt5eNDS97ZzhNWU051fgj9Nn+/M0
uo1e8qsg6vpVRUWs/bInydGJhvkDY7zgrONFLvpRbCH66B2pq4F8cDsoKX4jjx6h
SCMRXUWMuhd9V5mKesY9RusYNX4LMX2dBvEKsg5Cm08Ykc8sAd4NHs1Kfdx2hoBR
AsZHmKYLl+/d9fi4NzSNsxEZmsp1gckCNAQZ11cTMdkYTIqLvHLMmw9zKydwHUBW
3OUJa1Fh6kgXPjDEmFPWnsByGxorsrHYVK/Pyn8+v7784b6uv4u3I/E1GoUmgzrc
Pu9bAgMBAAGjUzBRMB0GA1UdDgQWBQBk1IgFgSkE+pehluAcDNjY86wxXjAfBgNV
HSMEGDAWgBQk1IgFgSkE+pehluAcDNjY86wxXjAPBgNVHRMBAf8EBTADAQH/MA0G
CSqGSIb3DQEBEwUAA4IBAQB3PGLYP0kvFu4o0cVuxbeu1abm6UJxmJ6TDyQFR+Ev
Inujzg0KoiIsEZobSe/fwAMSSNWctcCoz6ZML3DV1vS0o5ilr7Y4Dao+yXI5je4W
nr4MDQIIPxgrmSMwz0M3GubkRaXDI40XZ4TfRHHb0CXD70Awk1XXpbtibZyDXhe4
BAhRc7GNJqQCCFYc/h6ZqPB8xiyw3wBrtnub/WAqbLLu5Sx0MeKKA092RKYv7g2n
irqT8objco/yMHLsh+akAv0QE8Xx/hkf5hdm2Tc9B91dciFinAaw7usH/IeVpH3c
MwMb6SgxcIN7QF7JYSSi/nPXxxf1xiLzKi3MFTTZDvNn
-----END CERTIFICATE-----
```

- ♦ Cette clé va être stockée dans /etc/ssl/localcerts/

- ♦ Vérification :

```
root@http-pub:/etc/ssl/localcerts# ls
gsb.crt  gsb.key.org
```

Adaptation des Vhosts et de la configuration d'Apache

- ♦ Pour chaque VirtualHost il a fallut les modifier de la sorte :

```
1 <VirtualHost *:443>
2     DocumentRoot /home/htdocs/afrique.gsb.org/www/wiki
3     ServerName doc.afrique.gsb.org
4     ServerAlias wiki.afrique.gsb.org
5
6     # Autres directives ici
7     <Directory /home/htdocs/afrique.gsb.org/www/wiki>
8         Require all granted
9     </Directory>
10    # Fichier de log
11    ErrorLog /var/log/apache2/www-error.log
12    CustomLog /var/log/apache2/www-access.log combined
13
14
15    ServerAdmin webmaster@gsb.org
16
17    SSLCertificateFile /etc/ssl/localcerts/gsb.crt
18    SSLCertificateKeyFile /etc/ssl/localcerts/gsb.key.org
19
20
```

```
21 | </VirtualHost>
```

Il faut penser à laisser l'ancien virtualHost c'est-à-dire qu'il faut rajouter ce bloc en **★dessous★**.

♦ Quand c'est fait on fait **a2enmod ssl**.

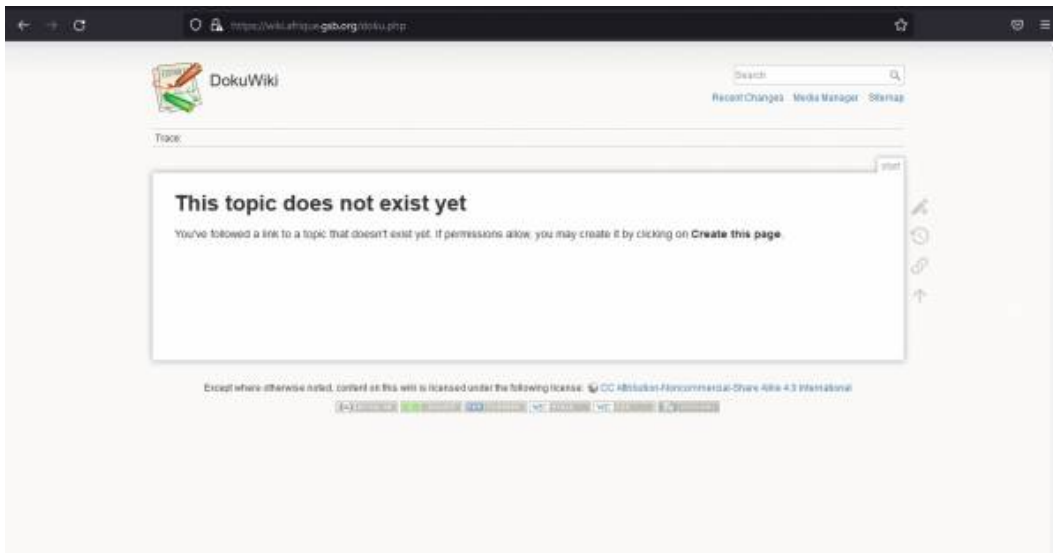
La commande a2enmod permet d' **activer** un module.

♦ On redémarre avec **systemctl restart apache2**.

♦ On test avec **netstat -nat**.

```
root@http-pub:/etc/ssl/localcerts# netstat -nat
Connexions Internet actives (serveurs et établies)
Proto Recv-Q Send-Q Adresse locale Adresse distante Etat
tcp 0 0 0.0.0.0:22 0.0.0.0:* LISTEN
tcp 0 224 10.31.248.80:22 10.187.20.188:58448 ESTABLISHED
tcp6 0 0 :::80 :::* LISTEN
tcp6 0 0 :::22 :::* LISTEN
tcp6 0 0 :::443 :::* LISTEN
root@http-pub:/etc/ssl/localcerts#
```

Test



TLS over FTP avec ProFTPD

- ♦ Il faut aller dans le dossier /etc/proftpd/

```
1 | cd /etc/proftpd/
```

- ♦ Création du dossier SSL

```
1 | mkdir ssl
```

- ♦ Se déplacer dans le dossier

```
1 | cd ssl
```

♦ Génération du certificat ssl auto-signé et la clé :

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

♦ Puis protéger la clé

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

Chmod 440 correspond à :

	Owner Rights (u)	Group Rights (g)	Others Rights (o)
Read (4)	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Write (2)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Execute (1)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

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

```
1 | # This is used for FTPS connections
2 | Include /etc/proftpd/tls.conf
```

♦ Éditer le fichier /etc/proftpd/tls.conf

```
1 | <IfModule mod_tls.c>
2 | #
3 | TLSEngine on
4 | TLSLog /var/log/proftpd/tls.log
```

```
5 | TLSProtocol SSLv23
6 | #
7 | TLSRSACertificateFile /etc/proftpd/ssl/proftpd-rsa.pem
8 | TLSRSACertificateKeyFile /etc/proftpd/ssl/proftpd-key.pem
9 | #
10 | TLSRequired on
11 | TLSRenegotiate required off
12 | </IfModule>
```

♦ Se déplacer dans /etc/proftpd/modules.conf :

→ Et décommenter la deuxième ligne ci-dessous

```
1 | # Install proftpd-mod-crypto to use this module for TLS/SSL support.
2 | LoadModule mod_tls.c
```

♦ Installer proftpd-mod-crypto :

```
1 | apt-get install proftpd-mod-crypto
```

♦ Il faut redémarrer proftpd :

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

```
root@ftp-pub:/# systemctl restart proftpd
root@ftp-pub:/#
```

Tester le serveur avec un client en mode commande :

♦ Installation de LFTP :

```
1 | apt install lftp
```

Test en mode interactif :

```
root@ftp-pub:/# lftp
lftp :~> set ftp:ssl-allow true
lftp :~> set ssl:verify-certificate no
lftp :~> open 127.0.0.1
lftp 127.0.0.1:~> user std
Mot de passe :
lftp std@127.0.0.1:~> l
Commande ambiguë « l ».
lftp std@127.0.0.1:~> ls
-rw-r--r-- 1 root root      6 Oct 18 14:06 ftpdocs.txt
lftp std@127.0.0.1:/> bye
root@ftp-pub:/# lftp 127.0.0.1 èu std
lftp 127.0.0.1:~> lftp 127.0.0.1 -u std
Mot de passe :
lftp std@127.0.0.1:~> █
```

Avec filezilla :

♦ Voici les logs afficher dans /var/log/proftpd/tls.log après s'être connecté sur le serveur avec filezilla :

```
root@ftp-pub:/# cat /var/log/proftpd/tls.log
2021-11-09 13:01:51,252 mod_tls/2.9[1121]: TLS/TLS-C requested, starting TLS handshake
2021-11-09 13:01:51,285 mod_tls/2.9[1121]: TLSv1.3 connection accepted, using cipher TLS_AES_256_GCM_SHA384 (256 bits)
2021-11-09 13:12:20,522 mod_tls/2.9[1155]: TLS/TLS-C requested, starting TLS handshake
2021-11-09 13:12:20,547 mod_tls/2.9[1155]: TLSv1.3 connection accepted, using cipher TLS_AES_256_GCM_SHA384 (256 bits)
2021-11-09 13:12:23,026 mod_tls/2.9[1155]: Protection set to Private
2021-11-09 13:12:23,073 mod_tls/2.9[1155]: client reused TLS session for data connection
2021-11-09 13:12:23,073 mod_tls/2.9[1155]: TLSv1.3 data connection accepted, using cipher TLS_AES_256_GCM_SHA384 (256 bits, resumed session)
root@ftp-pub:/#
```

♦ Voici le certificat après s'être connecté sur le serveur avec filezilla :



Capture de trames

Pour commencer on install tcpdump :

```
1 | apt-get install tcpdump
```

Commande pour lancer une capture de trame :

```
1 | sudo tcpdump -n -i enp1s0 -s0 port 21 -w (nom).pcap
```

Il faut se connecter au serveur sur filezilla et actualiser pour avoir la trame.

Réponse du serveur après avoir lancé une analyse TLS :

```
root@ftp-pub:~# tcpdump -n -i enp1s0 -X -s0 port 21 -w tcp.pcap
tcpdump: listening on enp1s0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
^C38 packets captured
38 packets received by filter
0 packets dropped by kernel
```

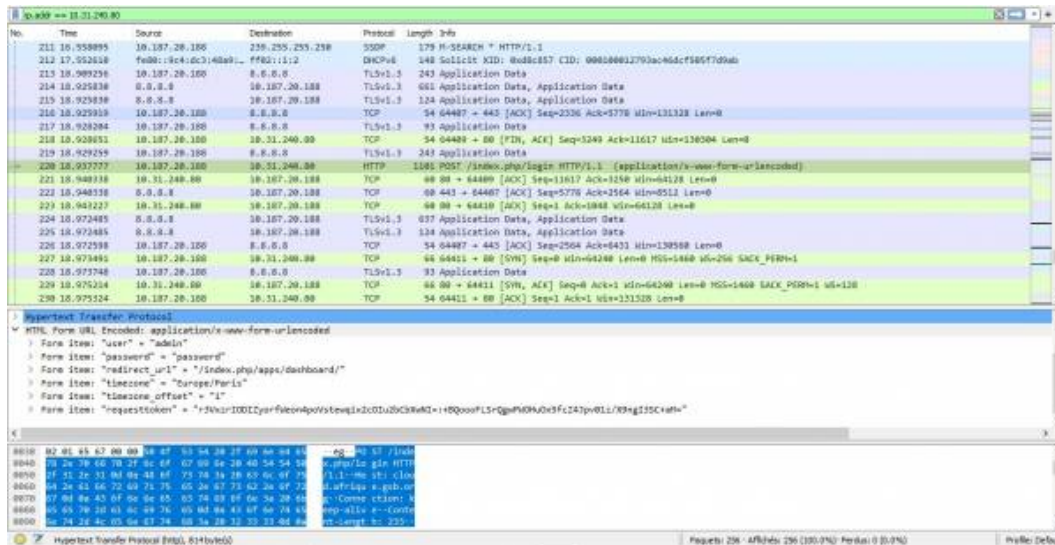
Réponse du serveur après avoir lancé une analyse sans TLS (ne pas oublier se connecter sur filezilla sans utiliser TLS):


```

root@ftp-pub:/home/ftpdocs# tcpdump -n -i enp1s0 -X -s0 port 21 -w tcp2.pcap
tcpdump: listening on enp1s0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
^C119 packets captured
119 packets received by filter
0 packets dropped by kernel

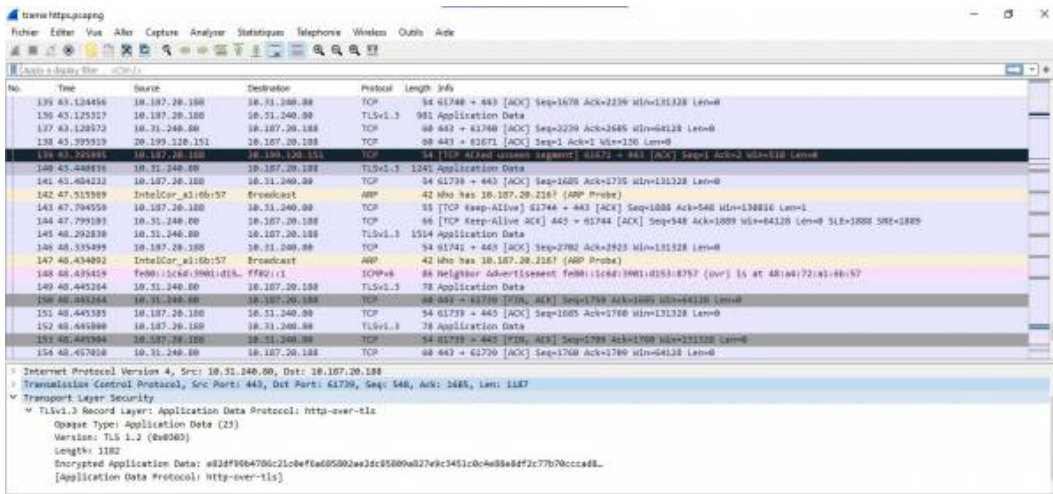
```

Voici, sur Wireshark l'analyse d'une trame HTTP :



On peut voir ici que l'identifiant et le mot de passe sont en clair.

Voici, sur Wireshark l'analyse d'une trame HTTPS :



On voit ici la ligne Encrypted Application qui nous indique que tout à été chiffré.

Commande pour lancer une capture de trame :

```
1 | sudo tcpdump -n -i lo -X -s0 port 21 -w (nom).pcap
```

Il faut se connecter au serveur sur filezilla et actualiser pour avoir la trame.

Il faut vérifier que la connexion sur filezilla utilise TLS

Réponse du serveur après avoir lancé une analyse TLS :

```
> Frame 7: 91 bytes on wire (728 bits), 91 bytes captured (728 bits) on interface 0
> Ethernet II, Src: RealtekU_a7:80:02 (52:54:00:a7:80:02), Dst: IntelCor_5b:4f:60 (00:13:20:5b:4f:60)
> Internet Protocol Version 4, Src: 10.31.248.20, Dst: 10.187.20.181
> Transmission Control Protocol, Src Port: 21, Dst Port: 51230, Seq: 52, Ack: 11, Len: 37
> File Transfer Protocol (FTP)
  > 234 AUTH TLS exécuté avec succès\r\n
    Response code: Security data exchange complete (234)
    Response arg: AUTH TLS exécuté avec succès
    [Current working directory: ]
```

```
0000 00 13 20 5b 4f 60 52 54 00 a7 80 02 08 00 45 00  .. [O]RT .....E.
0010 00 4d ce 39 40 00 40 06 4a ce 0a 1f f8 14 0a bb  .M.9@.@.].
0020 14 b5 00 15 c8 1e e4 69 53 b8 9d c1 72 55 50 18  ....i S...rUP.
0030 01 f6 21 e3 00 00 32 33 34 20 41 55 54 48 20 54  .!...23 4 AUTH T
0040 4c 53 20 65 78 c3 a9 63 75 74 c3 a9 20 61 76 65  LS ex..c ut.. ave
0050 63 20 73 75 63 63 c3 a8 73 0d 0a  c succ... s..
```

Commande pour lancer une capture de trame :

```
1 | sudo tcpdump -n -i lo -s0 port 21 -w (nom).pcap
```

Il faut se connecter au serveur sur filezilla et actualiser pour avoir la trame.

Il faut vérifier que la connexion sur filezilla n'utilise pas TLS

Réponse du serveur après avoir lancé une analyse TLS :

1	0.000000	10.187.20.181	10.31.248.20	TCP	66 61741 → 21 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
2	0.000055	10.31.248.20	10.187.20.181	TCP	66 21 → 61741 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM=1 WS=128
3	0.003591	10.187.20.181	10.31.248.20	TCP	60 61741 → 21 [ACK] Seq=1 Ack=1 Win=131328 Len=0
4	0.041456	10.31.248.20	10.187.20.181	FTP	105 Response: 220 ProFTPD Server (Debian) [::ffff:10.31.248.20]
5	0.092849	10.187.20.181	10.31.248.20	TCP	60 61741 → 21 [ACK] Seq=1 Ack=52 Win=131328 Len=0
6	1.462364	10.187.20.181	10.31.248.20	FTP	64 Request: USER std
7	1.462416	10.31.248.20	10.187.20.181	TCP	54 21 → 61741 [ACK] Seq=52 Ack=11 Win=64256 Len=0
8	1.462802	10.31.248.20	10.187.20.181	FTP	80 Response: 331 Mot de passe requis pour std
9	1.466812	10.187.20.181	10.31.248.20	FTP	69 Request: PASS password
10	1.466869	10.31.248.20	10.187.20.181	TCP	54 21 → 61741 [ACK] Seq=86 Ack=26 Win=64256 Len=0
11	1.593948	10.31.248.20	10.187.20.181	FTP	88 Response: 230 Utilisateur std authentifié
12	1.598554	10.187.20.181	10.31.248.20	FTP	60 Request: SYST

> Frame 9: 60 bytes on wire (552 bits), 60 bytes captured (552 bits)

> Ethernet II, Src: IntelCor_5b:4f:60 (00:13:20:5b:4f:60), Dst: RealtekU_a7:80:02 (52:54:00:a7:80:02)

> Internet Protocol Version 4, Src: 10.187.20.181, Dst: 10.31.248.20

> Transmission Control Protocol, Src Port: 61741, Dst Port: 21, Seq: 11, Ack: 86, Len: 15

> File Transfer Protocol (FTP)

[Current working directory:]

0000 52 54 00 a7 80 02 00 13 20 5b 4f 60 00 00 45 00 RT..... [0'--E-

0010 00 37 6a 89 40 00 7e 06 70 94 0a bb 14 b5 0a 1f -7j @-- p-----

0020 f8 14 f1 2d 00 15 d3 56 39 d5 d0 c8 13 d8 50 18 ----V 9-----P-

0030 02 00 32 9b 00 00 50 41 53 53 20 70 63 73 73 77 --2---PA SS passw

0040 5f 72 66 0d 0a 00 00 00 00 00 00 00 00 00 00 end-

On peut voir ici que l'identifiant et le mot de passe sont en clair.