Documentation Technique

Mise en place du chiffrement TLS sur Asterisk avec téléphones Cisco SPA303

Serveur : Debian 11 | Asterisk | TLS/SRTP

1. Prérequis et préparation

1.1 Vérification de la structure de répertoires

Créer les répertoires nécessaires pour stocker les certificats :

```
mkdir -p /etc/asterisk/keys/ca
mkdir -p /etc/asterisk/keys/server
mkdir -p /etc/asterisk/certificats/u1101
mkdir -p /etc/asterisk/certificats/u1102
mkdir -p /etc/asterisk/certificats/u1201
mkdir -p /etc/asterisk/certificats/u1202
```

2. Création de l'Autorité de Certification (CA)

Toutes les commandes suivantes sont à exécuter dans /etc/asterisk/keys/ca/

```
cd /etc/asterisk/keys/ca
```

2.1 Création de la clé CA

⚠ *Le mot de passe demandé sera nécessaire pour signer les certificats. Ne pas l'oublier !*

```
openssl genrsa -des3 -out ca.key 4096
```

2.2 Création du certificat CA

```
openssl req -new -x509 -days 365 -key ca.key -out ca.crt
```

Remplir les informations demandées (Country, Organization, etc.)

3. Création des certificats du serveur Asterisk

Toutes les commandes suivantes sont à exécuter dans /etc/asterisk/keys/server/

```
cd /etc/asterisk/keys/server
```

3.1 Création de la clé du serveur

```
openssl genrsa -out key.pem 2048
```

3.2 Création de la demande de certificat

```
openssl req -new -key key.pem -out req-srv.csr
```

3.3 Signature du certificat par la CA

```
openssl x509 -req -days 365 -in req-srv.csr -CA ../ca/ca.crt -CAkey
../ca/ca.key -set_serial 01 -out srv.crt
```

3.4 Fusion de la clé et du certificat

Le fichier asterisk.pem contiendra à la fois la clé et le certificat :

```
cat key.pem > asterisk.pem
cat srv.crt >> asterisk.pem
```

4. Création des certificats utilisateurs

4.1 Utilisateur u1101 (Josias)

```
cd /etc/asterisk/certificats/u1101
openssl genrsa -out key.pem 2048
openssl req -new -key key.pem -out req-u1101.csr
openssl x509 -req -days 365 -in req-u1101.csr -CA
/etc/asterisk/keys/ca/ca.crt -CAkey /etc/asterisk/keys/ca/ca.key
-set_serial 02 -out cert-u1101.crt
cat key.pem > cert-u1101.pem
cat cert-u1101.crt >> cert-u1101.pem
```

4.2 Utilisateur u1102 (Lucas)

```
cd /etc/asterisk/certificats/u1102
openssl genrsa -out key.pem 2048
openssl req -new -key key.pem -out req-u1102.csr
openssl x509 -req -days 365 -in req-u1102.csr -CA
/etc/asterisk/keys/ca/ca.crt -CAkey /etc/asterisk/keys/ca/ca.key
-set_serial 03 -out cert-u1102.crt
cat key.pem > cert-u1102.pem
cat cert-u1102.crt >> cert-u1102.pem
```

4.3 Utilisateur u1201 (Rayan)

```
cd /etc/asterisk/certificats/u1201
openssl genrsa -out key.pem 2048
openssl req -new -key key.pem -out req-u1201.csr
openssl x509 -req -days 365 -in req-u1201.csr -CA
/etc/asterisk/keys/ca/ca.crt -CAkey /etc/asterisk/keys/ca/ca.key
-set_serial 04 -out cert-u1201.crt
cat key.pem > cert-u1201.pem
cat cert-u1201.crt >> cert-u1201.pem
```

4.4 Utilisateur u1202 (Gala)

```
cd /etc/asterisk/certificats/u1202
openssl genrsa -out key.pem 2048
openssl req -new -key key.pem -out req-u1202.csr
openssl x509 -req -days 365 -in req-u1202.csr -CA
/etc/asterisk/keys/ca/ca.crt -CAkey /etc/asterisk/keys/ca/ca.key
-set_serial 05 -out cert-u1202.crt
cat key.pem > cert-u1202.pem
cat cert-u1202.crt >> cert-u1202.pem
```

5. Configuration de sip.conf

```
nano /etc/asterisk/sip.conf
```

5.1 Section [general]

Ajouter ou modifier les lignes suivantes dans la section [general] :

```
transport = tls
tlsenable = yes
tlsbindaddr = 0.0.0.0:5061
tlscertfile = /etc/asterisk/keys/server/asterisk.pem
tlscafile = /etc/asterisk/keys/ca/ca.crt
tlsdontverifyserver = yes
```

5.2 Modification du fichier users.conf

Ouvrir le fichier users.conf :

```
nano /etc/asterisk/users.conf
```

Dans la section [general], ajouter les deux lignes suivantes :

```
[general]
transport = tls
encryption = yes
```

> ⚠ *Ces paramètres dans [general] s'appliquent à tous les utilisateurs. Sans eux, les appels ne seront pas chiffrés même si TLS est activé sur le serveur.*

6. Modification de la version TLS

```
nano /etc/ssl/openssl.cnf
```

Trouver et modifier la ligne suivante :

```
MinProtocol = TLSv1.2     →     MinProtocol = TLSv1.0
```

7. Redémarrage d'Asterisk

```
systemctl restart asterisk
```

```
systemctl status asterisk
```

⚠ *Vérifier que le service est bien en état 'active (running)'*

8. Configuration des téléphones Cisco SPA303

8.1 Accès à l'interface web

Depuis un navigateur, accéder à l'adresse IP du téléphone :

```
http://<adresse_ip_du_telephone>
```

Cliquer sur Admin Login puis Advanced.

8.2 Étape 1 - Menu User > Supplementary Services

Dans le sous-menu Supplementary Services du menu User :

```
Secure Call Setting  →  yes
```

Cliquer sur Submit All Changes.

8.3 Étape 2 - Menu Phone > Supplementary Services

Dans le sous-menu Supplementary Services du menu Phone :

```
Secure Call Serv.  →  yes
```

Cliquer sur Submit All Changes.

8.4 Étape 3 - Menu SIP > SIP Parameters

Dans le sous-menu SIP Parameters du menu SIP :

```
SRTP Method  →  s-descriptor
```

Cliquer sur Submit All Changes.

8.5 Étape 4 - Menu EXT > SIP Settings

Dans le sous-menu SIP Settings associé au menu EXT de l'utilisateur concerné (EXT1, EXT2 ou EXT3) :

```
SIP Transport  →  TLS
SIP Port       →  5061
```

⚠ *Le port SIP passe de 5060 (non chiffré) à 5061 (TLS) automatiquement.*

Cliquer sur Submit All Changes.

9. Vérification du chiffrement avec Wireshark

9.1 Lancer une capture réseau

Depuis un PC sur le même réseau, ouvrir Wireshark et lancer une capture sur l'interface réseau.

9.2 Filtres à appliquer

```
tcp.port == 5061        (signalisation TLS)
udp.port == 5004        (voix RTP/SRTP)
```

9.3 Résultats attendus

- Paquets TLSv1 sur le port 5061 → signalisation chiffrée ✅
- Paquets SRTP → voix chiffrée ✅
- Absence de SIP en clair → chiffrement actif ✅

⚠ *Si vous voyez du RTP en clair, le chiffrement de la voix n'est pas actif. Vérifier le paramètre encryption=yes dans sip.conf.*