HTTPS, TLS et certificats

Formation : BTS SIO — Option SISR

1. Rôle et fonctionnement

TLS protège la confidentialité et l'intégrité d'une connexion et permet d'authentifier le serveur à l'aide de son certificat. HTTPS associe HTTP à TLS. Dans le laboratoire, ces mécanismes concernent WAC, Guacamole et les services Web.

Un certificat contient notamment une identité, une période de validité et une clé publique. La clé privée correspondante reste confidentielle. Le navigateur vérifie le nom demandé, les dates et la chaîne de confiance.

2. Mise en œuvre

Choisir le nom DNS d'accès avant d'émettre le certificat. Définir les noms dans les extensions SAN, installer la chaîne nécessaire et protéger la clé privée. Un certificat utilisé via une IP doit couvrir cette IP ; couvrir uniquement un nom DNS ne suffit pas.

Un certificat auto-signé peut être employé dans une maquette avec une confiance explicitement maîtrisée. Le chiffrement ne garantit pas, à lui seul, que l'identité du serveur a été correctement vérifiée.

3. Vérification

```
openssl s_client -connect bastion.example.org:8443 -servername
bastion.example.org -verify_return_error
curl -I https://bastion.example.org:8443/guacamole/
```

Les noms `example.org` sont des exemples à remplacer par les noms réellement configurés. Contrôler l'émetteur, les dates, les SAN et le résultat de validation.

4. Dépannage

Erreur	Cause possible
Nom incompatible	URL différente des SAN
Autorité inconnue	Racine non approuvée ou chaîne incomplète
Certificat expiré	Renouvellement absent
Pas encore valide	Horloge incorrecte

Une option désactivant la vérification TLS peut aider à isoler un problème, mais ne constitue pas un critère de recette réussi. Vérifier le renouvellement et les dépendances à NTP.

5. Références

- IETF — TLS 1.3
- Microsoft — certificat WAC

From:
https://wiki.ewengadonnaud.xyz/ - **Base de savoir réseaux/cyber/devops**

Permanent link:
https://wiki.ewengadonnaud.xyz/doku.php?id=cyber:tls

Last update: **2026/10/18 01:23**