Principe de noms de domaine

► Préambule

La navigation sur les sites web se fait à l'aide d'un navigateur qui est considéré comme le client, qui se connecte à un serveur qui lui fourni les informations à afficher.

Pour ce faire on utilise des noms de domaines afin de simplifier la tâche côté utilisateur. Il est plus simple de retenir un acronyme, une marque ou une appellation qu'une suite de chiffres définissant l'adresse IP du serveur.

FQDN : Fully Qualified Domain Name, en Français Nom de Domaine Pleinement Qualifié.

► Navigation

Pour se rendre sur un site Web en particulier, on tape son URL dans la barre d'adresse du navigateur. L'adresse est interprétée par le serveur DNS qui transforme le nom de domaine en adresse IP et le routeur prend le relais pour envoyer et recevoir les informations et le diriger vers les bonnes machines.

► Protocole de communication

Pour naviguer sur le Web on utiliser un protocole, le http ou HyperText Transfer Protocol. Aujourd'hui on a tendance à utiliser exclusivement la version sécurisé du protocole, à savoir : https.

La sécurisation se fait par un système de certificat de sécurité et le protocole de chiffrage SSL ou TLS.

► Le rôle du certificat SSL/TLS

Un certificat SSL/TLS est un fichier installé sur le serveur web qui contient :

• Une clé publique
• Des informations sur le site (nom de domaine, organisation, etc.)
• La signature d'une autorité de certification (CA)

► Ce certificat permet de :

1. Chiffrer les données échangées.
2. Authentifier l'identité du serveur auprès du client.

► Comment fonctionne une connexion HTTPS ?

Étape 1 – Le client demande une page HTTPS

Le navigateur de l'utilisateur demande une connexion sécurisée au serveur (https://monsite.com).

Étape 2 – Le serveur envoie son certificat

Le serveur web envoie son **certificat SSL/TLS** au client.

Étape 3 – Vérification du certificat

Le client vérifie :

- Que le certificat est **valide** (non expiré, pas révoqué)
- Que le certificat a été émis par une **autorité de certification reconnue**
- Que le **nom de domaine** correspond

Si un problème est détecté, l'utilisateur voit un **avertissement HTTPS**.

Étape 4 – Échange de clés et chiffrement (Handshake TLS)

- Le client génère une **clé de session** (clé symétrique) qu'il chiffre avec la **clé publique** du serveur (contenue dans le certificat).
- Le serveur déchiffre cette clé avec sa **clé privée**.
- À partir de là, **toute la communication est chiffrée** symétriquement avec la clé de session partagée.

Étape 5 – Échange sécurisé

Le client et le serveur communiquent en toute sécurité : les données sont **illisibles** pour un tiers.

► Pourquoi c'est sécurisé ?

- Chiffrement **asymétrique** (clé publique/privée) pour établir une session sécurisée.
- Chiffrement **symétrique** pour l'échange rapide des données.
- Authentification du serveur (et parfois du client dans les cas plus poussés).
- Protection contre les attaques de type "man-in-the-middle" (MITM).

► Comment est composée une adresse web (ou URL) ?

Une URL (Uniform Resource Locator) est composée de plusieurs parties :

1. Le protocole : http ou https
2. Le séparateur ://
3. Un sous-domaine nommé « www » qui n'est pas obligatoire mais qui est historiquement utilisé pour désigner les sites web. WWW : World Wide Web
4. Le nom de domaine, qui peut être une marque, un acronyme ou autre. Ce nom ne comportera jamais d'espace, de lettes accentuées ou de caractères spéciaux autres que ceux autorisés.
5. Une extension, .com / .fr / .org / .tv / … etc.
6. On retrouve ensuite ce qu'on appelle le chemin qui est spécifique au site web que vous consulté.

• Prenons un exemple :

https://www.exemple.com



Protocole | Sous-domaine | Nom de domaine | Extension

L'ensemble complet de l'URL est alors appelé FQDN.

Lorsque on tape une URL dans le navigateur et qu'on valide, la demande est transmise au serveur DNS (Domain Name System) qui s'occupe de transformer les noms de domaine en adresses IP et inversement.
La première chose qui est lue est l'extension, ensuite le nom de domaine et le sous-domaine.

Derrière le nom de domaine on retrouve généralement ce qu'on appelle le chemin.
Il s'agit de paramètre propre au serveur web qui affiche le site qui lui permet de savoir ce qu'il faut afficher.

Il existe plusieurs technologie pour afficher un site, dans la majorité des cas soit on affiche un site web dit statique donc avec un chemin qui se termine avec nom .html ou .htm.
Soit un site dit dynamique avec un chemin qui se termine avec un nom .php ou .asp.

D'autre sites n'ont tout simplement pas de nom spécifique et utilisent plutôt des codes.
Comme par exemple avec youtube ou on retrouve l'instruction « `watch?v=` » suivi de l'identifiant de la vidéo.

► Ports de communication

En utilisant le protocole http le port utilisé est toujours le port TCP 80.
En ce qui concerne le protocole https, le port utilisé est le port TCP 443.

Ceux-ci sont implicites lorsque vous utilisez http ou https.

Parfois, lorsque vous vous connectez à un serveur local ou distant il est nécessaire d'indiquer le port de communication, car celui-ci n'est pas réglé sur les ports standards.

Pour ce faire on ajoute du texte dans l'URL comme suit.

https://serveur-local:8000

Ici on interroge un site web ou interface web situé sur un serveur local sur le port TCP 8000 en utilisant le protocole sécurisé SSL/TLS.

A savoir qu'on peut très bien utiliser l'adresse IP au lieu du nom de domaine.

https://192.168.1.10:8000

Cette URL mène au même endroit dans notre exemple et interroge le même serveur.
En faisant cela on court-circuite juste le serveur DNS.

► RAPPEL ◄

Il existe 65535 ports en TCP et 65535 ports en UDP

TCP et UDP sont deux protocoles de communication de basse couche sur le modèle OSI et font partis de la pile TCP/IP.

Voir le cours sur le TCP/IP :

► Accès au cours. ◄