# Objectifs Pédagogiques

* Être capable d’identifier les protocoles de communications entre différents systèmes

# Travail à effectuer

Effectuez des recherches concernant les différents protocoles et normes listés ci-dessous.

Pour chaque protocole / norme, vous indiquerez au moins 3 sources différentes.

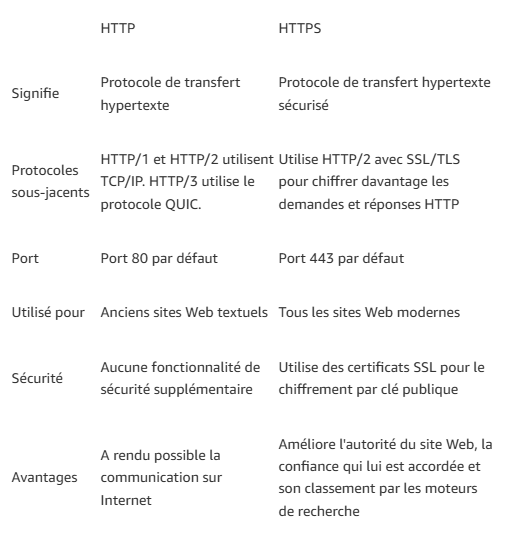
Une fois les recherches terminées, envoyez le document au formateur.

## HTTP et HTTPS (identifiez aussi les Port utilisé par ces protocoles)

* **MDN** : **Hypertext Transfer Protocol (HTTP) (ou protocole de transfert hypertexte en français)** est un protocole de [la couche application](https://fr.wikipedia.org/wiki/Couche_application) servant à transmettre des documents hypermédias, comme HTML. Il a été conçu pour la communication entre les navigateurs web et les serveurs web mais peut également être utilisé à d'autres fins. Il suit le modèle classique [client-serveur](https://fr.wikipedia.org/wiki/Client-serveur) : un client ouvre une connexion, effectue une requête et attend jusqu'à recevoir une réponse. Il s'agit aussi d'un [protocole sans état](https://fr.wikipedia.org/wiki/Protocole_sans_%C3%A9tat), ce qui signifie que le serveur ne conserve aucune donnée (on parle d'état) entre deux requêtes.

* **Amazon Web Service : Précision HTTPS (Hypertext Transfer Protocol Secure),** avantage donné à la sécurité, à l’autorité (priorité sur l’http pour les moteurs de recherches) et les performances (se chargent plus rapidement que le simple protocole http.
* **Wikipedia :** http déprécié par rapport au HTTPS pour les raisons de sécurité évoqués auparavant. HTTPS permet au visiteur de vérifier l'identité du [site web](https://fr.wikipedia.org/wiki/Site_web) auquel il accède, grâce à un [certificat](https://fr.wikipedia.org/wiki/Certificat_%C3%A9lectronique) d'[authentification](https://fr.wikipedia.org/wiki/Authentification) émis par une autorité tierce, réputée fiable (et faisant généralement partie de la [liste blanche](https://fr.wikipedia.org/wiki/Liste_blanche) des [navigateurs internet](https://fr.wikipedia.org/wiki/Navigateur_web) et des [systèmes d'exploitation](https://fr.wikipedia.org/wiki/Syst%C3%A8me_d%27exploitation)). Il garantit **théoriquement** la [confidentialité](https://fr.wikipedia.org/wiki/Confidentialit%C3%A9) et l'intégrité des données envoyées par l'utilisateur (notamment des informations entrées dans les [formulaires](https://fr.wikipedia.org/wiki/Formulaire)) et reçues du [serveur](https://fr.wikipedia.org/wiki/Serveur_informatique).

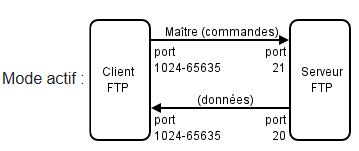
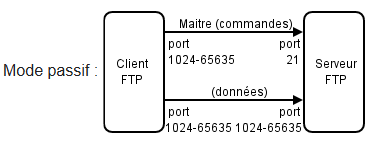
DATE CREATION HTTPS : 1994



## SMTP (identifiez aussi les Port utilisé par ce protocole)

* **AWS :** SMTP est l'abréviation de Simple Mail Transfer Protocol. Il s'agit d'un protocole de communication utilisé pour envoyer et recevoir des messages électroniques sur Internet. Les serveurs de messagerie et autres agents de transfert de messages (MTA) utilisent le protocole SMTP pour envoyer, recevoir et relayer des messages électroniques.
* **MDN : SMTP** (Simple Mail Transfer Protocol) est un [protocole](https://developer.mozilla.org/fr/docs/Glossary/Protocol) utilisé pour envoyer un nouveau courriel. Tout comme [POP3](https://developer.mozilla.org/fr/docs/Glossary/POP) et [NNTP](https://developer.mozilla.org/fr/docs/Glossary/NNTP), il s'agit d'un protocole piloté par une [machine d'état](https://developer.mozilla.org/fr/docs/Glossary/State_machine).   
  Le protocole est relativement simple. Les principales difficultés viennent du support des divers mécanismes d'authentification ([GSSAPI](http://fr.wikipedia.org/wiki/GSS-API), [CRAM-MD5](http://en.wikipedia.org/wiki/CRAM-MD5), [NTLM](http://fr.wikipedia.org/wiki/NT_Lan_Manager), MSN, AUTH LOGIN, AUTH PLAIN, etc.), de la gestion des réponses en cas d'erreurs, et de trouver un moyen de réagir en cas d'échec des mécanismes d'authentification.
* **Wikipedia :** PORT TCP 25 ou PORT 587

## FTP (identifiez aussi les Port utilisé par ce protocole)

* **MDN**: **FTP** (file transfer protocol) est un [protocole](https://developer.mozilla.org/fr/docs/Glossary/Protocol) réseau standard utilisé pour transférer des fichiers d'un [hôte](https://developer.mozilla.org/fr/docs/Glossary/Host) à un autre par Internet. De plus en plus, cependant, les équipes et les comptes d'hébergement n'autorisent pas le FTP et s'appuient plutôt sur un système de contrôle de version comme Git. Vous le trouverez toujours utilisé sur les anciens comptes d'hébergement, mais il est sûr de dire que FTP n'est plus considéré comme la meilleure pratique.
* **Wikipedia :** Port 21 (écoute) Port 20 (données par défaut). 2 utilisations différentes, mode actif et passif, ci-joint illustration :

## DNS (identifiez aussi le Port utilisé par ce protocole)

* **AWS** : Un système de noms de domaine, ou DNS, traduit les noms de domaine lisibles par l'homme (par exemple, www.amazon.com) en adresses IP lisibles par une machine (par exemple, 192.0.2.44). Deux types de DNS : DNS faisant autorité et DNS récursif.
* **Wikipedia**: Port 53. Associe les noms de domaines internet avec leurs adresses IP ou d’autres types d’enregistrement. Date de 1985.
* **MDN**: Même chose.

## SSL

* **MDN**: SSL (Secure Sockets Layer) est un protocole standard qui garantit que la communication entre deux applications informatiques est privée et sécurisée (ne peut être ni lue ni modifiée par des observateurs extérieurs). C'est la base du protocole [TLS](https://developer.mozilla.org/fr/docs/Glossary/TLS).
* **Wikipedia**: Le SSL est le prédécesseur du TLS. Il permet de satisfaire les objectifs de sécurité suivants : authentification du serveur (et optionnellement du client), confidentialité des données, l’intégrité des données.
* **AWS**: Les certificats sont utilisés dans un système cryptographique appelé « infrastructure à clé publique » (PKI, Public Key Infrastructure). L'infrastructure PKI permet à une partie d'établir l'identité d'une autre partie à l'aide de certificats si elles font toutes deux confiance à un tiers appelé « autorité de certification ». Les certificats SSL/TLS font donc office de cartes d'identité numériques pour sécuriser les communications réseau, établir l'identité des sites web sur Internet, ainsi que des ressources sur les réseaux privés.

## SSH (identifiez aussi le Port utilisé par ce protocole)

* **Wikipedia** : Port TCP/22. Secure Shell (SSH) est un [protocole de communication](https://fr.wikipedia.org/wiki/Protocole_de_communication) sécurisé. Le protocole de connexion impose un échange de [clés de chiffrement](https://fr.wikipedia.org/wiki/Cl%C3%A9_de_chiffrement) en début de connexion. Par la suite, tous les [segments](https://fr.wikipedia.org/wiki/Couche_transport) [TCP](https://fr.wikipedia.org/wiki/Transmission_Control_Protocol) sont authentifiés et chiffrés. Il devient donc impossible d'utiliser un [analyseur de paquets](https://fr.wikipedia.org/wiki/Analyseur_de_paquets) (*sniffer*) pour voir ce que fait l'utilisateur.  
  Le protocole SSH a été conçu avec l'objectif de remplacer les différents protocoles non chiffrés comme [rlogin](https://fr.wikipedia.org/wiki/Rlogin), [telnet](https://fr.wikipedia.org/wiki/Telnet), [rcp](https://fr.wikipedia.org/wiki/Rcp_(Unix)) et [rsh](https://fr.wikipedia.org/wiki/Rsh).
* **Evolyon**: SSH dispose d'un système d'authentification par nom d'utilisateur et mot de passe, contrairement à SSL. SSL utilise des certificats numériques et une infrastructure à clé publique. L'authentification n'a donc lieu que du côté serveur.
* **Cloudfare :** Possibilité de tunnellisation : dans le domaine des réseaux, la tunnellisation est une méthode permettant de faire transiter un paquet au travers d'un réseau en utilisant un protocole ou suivant un itinéraire qu'il ne pourrait normalement pas emprunter. La tunnellisation consiste à envelopper les paquets (Toutes les données qui traversent un réseau sont décomposées en morceaux plus petits ces morceaux sont appelés « paquet ») de données avec des informations supplémentaires, appelées en-têtes, afin de modifier leur destination. Les tunnels SSH ont recours à une technique appelée redirection de port pour transférer des paquets d'une machine à l'autre. La redirection de port est expliquée plus en détail ci-dessous.

## TCP et UDP

* **Wikipedia** : Dans le [modèle Internet](https://fr.wikipedia.org/wiki/Suite_des_protocoles_Internet), aussi appelé modèle TCP/IP, TCP est situé au-dessus de IP. Dans le modèle [OSI](https://fr.wikipedia.org/wiki/Mod%C3%A8le_OSI), il correspond à la [couche transport](https://fr.wikipedia.org/wiki/Couche_transport), intermédiaire de la [couche réseau](https://fr.wikipedia.org/wiki/Couche_r%C3%A9seau) et de la [couche session](https://fr.wikipedia.org/wiki/Couche_session). Les applications transmettent des flux de données sur une [connexion réseau](https://fr.wikipedia.org/wiki/Connexion_r%C3%A9seau). TCP découpe le flux d’[octets](https://fr.wikipedia.org/wiki/Octet) en *segments* dont la taille dépend de la [MTU](https://fr.wikipedia.org/wiki/Maximum_Transmission_Unit) du réseau sous-jacent ([couche liaison de données](https://fr.wikipedia.org/wiki/Couche_liaison_de_donn%C3%A9es)).
* **MDN** : **TCP (pour Transmission Control Protocol en anglais)** (ou « protocole de contrôle des transmissions ») est un [protocole](https://developer.mozilla.org/fr/docs/Glossary/Protocol) réseau qui permet à deux hôtes de se connecter et d'échanger des données. Le protocole TCP garantit la distribution des données et des **paquets dans l'ordre où ils ont été envoyés**. Vint Cerf et Bob Kahn, scientifiques du DARPA à l'époque, ont conçu TCP dans les années 70.  
  Le rôle de TCP est d'assurer la livraison fiable et sans erreur des paquets. TCP dispose d'un contrôle de concurrence, ce qui signifie que les requêtes initiales sont petites puis augmentent en taille en fonction des niveaux de bande passante que peuvent supporter les ordinateurs, les serveurs et le réseau.
* **Fortinet** : Le protocole TCP est l’une des normes de base qui définissent les règles d’Internet et est inclus dans les normes définies par l’Internet Engineering Task Force (IETF). Il s’agit de l’un des protocoles les plus couramment utilisés dans les communications numériques en réseau et il veille à la transmission des données de bout en bout.

## IP

* **Fortinet** : Le protocole IP est la méthode utilisée pour envoyer des données d’un appareil à un autre via Internet. Chaque appareil dispose d’une adresse IP qui l’identifie de manière unique et lui permet de communiquer et d’échanger des données avec d’autres appareils connectés à Internet.  Aujourd’hui, elle est considérée comme la norme pour une communication rapide et sécurisée directement entre les appareils mobiles.
* **Wikipedia :** pas fini
* **MDN :** Pas fini non plus…