

Question 1 : http/https

Indiquez les 2 services essentiels apportés par https vis à vis de http ?

Question 2 portail captif

Qu'appelle-t-on un portail captif ? Rappeler son mode de fonctionnement.

Après avoir lu la presse¹, Alice a décidé de ne plus se connecter que sur des sites en https. Elle se connecte depuis un lieu où le passage par un portail captif authentifiant est imposé pour toute connexion au WeB. Expliquez :

- Si la décision d'Alice a un impact sur le bon fonctionnement du portail captif
- si l'existence du portail captif a un impact sur le soucis d'Alice de ne pas voir ses données espionnées ?

Question 3 https/Tor/rien

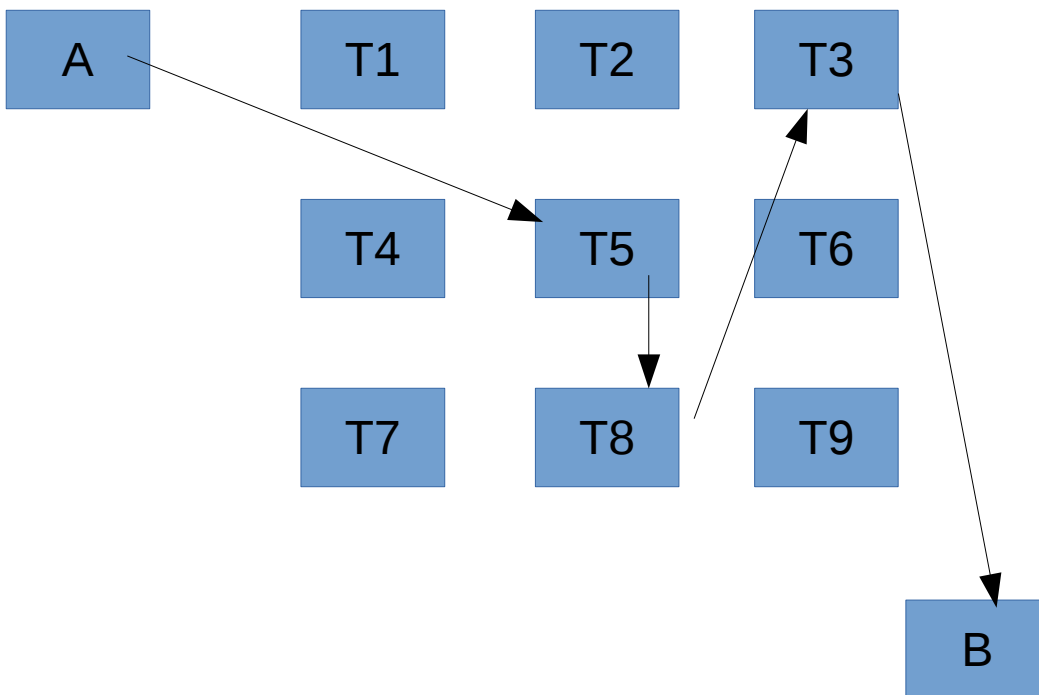
A (Alice) souhaite se connecter sur le serveur B (Bob). Comparez les propriétés de 4 modes de connexion en matière de sécurité et de confidentialité :

- connexion directe de A sur B en http
- connexion directe de A sur B en https
- connexion de A sur B en http via TOR (cf premier schéma)
- connexion de A sur B en https via TOR (cf second schéma)

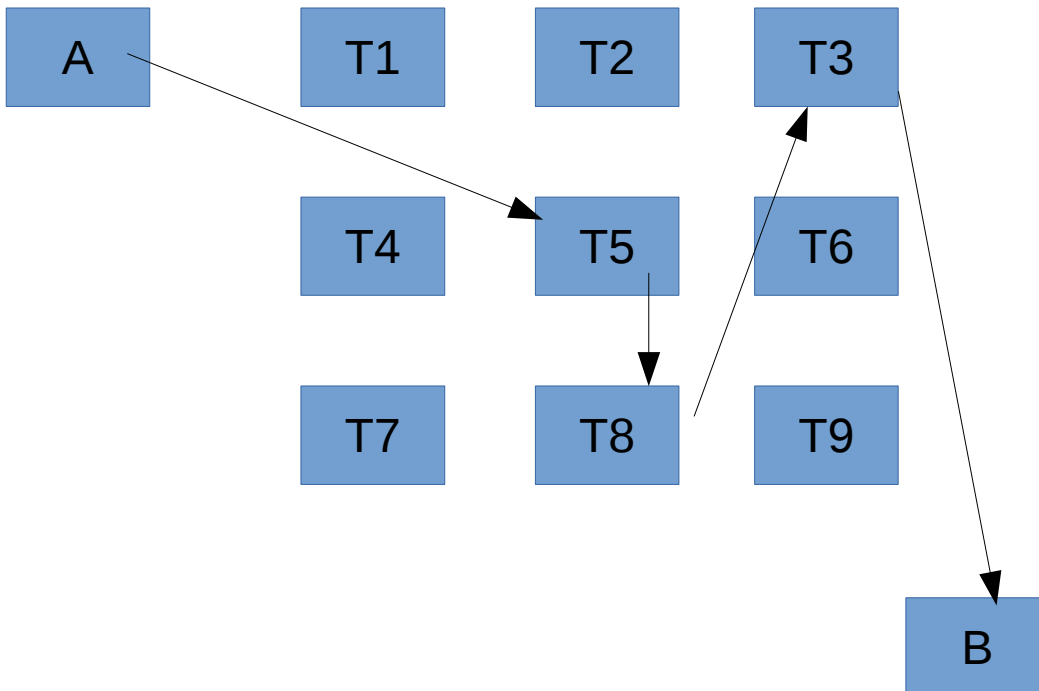
vous indiquerez pour chaque scénario : quelles parties de la connexion sont chiffrées, ce que sait chaque intermédiaire de la source du paquet, du contenu du paquet, de la destination du paquet. Pour TOR, vous pourrez utiliser les 2 schémans suivants (à rendre avec votre copie) :

1 Par exemple: 6 juin 2016: reflets.info, "[Qosmos et le gouvernement Français, très à l'écoute du Net dès 2009](https://reflets.info/qosmos-et-le-gouvernement-francais-tres-a-lecoute-du-net-des-2009/)" <https://reflets.info/qosmos-et-le-gouvernement-francais-tres-a-lecoute-du-net-des-2009/>

connexion en http via TOR:



connexion en https via TOR:



Question 4 reverse proxy

Qu'est-ce qu'un reverse proxy ? quel rôle a-t-il ?

Question 5

Définissez les termes suivants:

- DMZ
- machine bastion
- non répudiation
- authentification forte

Question 6

répondez à 2 des 3 questions suivantes :

- qu'est-ce qu'une attaque Man In The Middle (MiM) ?
- en vous appuyant sur un exemple, expliquez la différence entre données et métadonnées
- qu'est-ce qu'un certificat ? on pourra indiquer ce qu'a un certificat de plus qu'une simple clef publique)

Question 7

On considère le réseau de la société THEBEST qui est constitué des éléments suivants :

Serveurs :

- Serveur de fichiers interne ; adresse 172.30.32.13 /255.255.255.0
- commutateur 3com

Postes de travail

- Poste de travail 1 : secrétaire : Windows seven pro 172.30.32.51 / 255.255.255.0
- - Poste de travail 2 : directeur : Windows seven pro 172.30.32.52 / 255.255.255.0
- - Poste de travail 3 : comptable : Windows seven pro 172.30.32.53 / 255.255.255.0
- commutateur 3com

serveurs accessibles de l'extérieur :

- Serveur DNS ; Windows serveur 2003 ;adresse 172.30.32.3 / 255.255.255.0
- Serveur WEB internet Linux Debian & Apache ;adresse 172.30.32.4 / 255.255.255.0

Routeur accès internet

Votre travail :

- Critiquer l'architecture réseau de l'entreprise d'un point de vue sécurité
- Proposer une architecture réseau plus conforme à l'état de l'art en matière de sécurité. A cet effet, vous pourrez ajouter les éléments réseaux nécessaires (coupe feu, ...) et créer autant de réseau que cela vous semble nécessaire.