

1. Cours

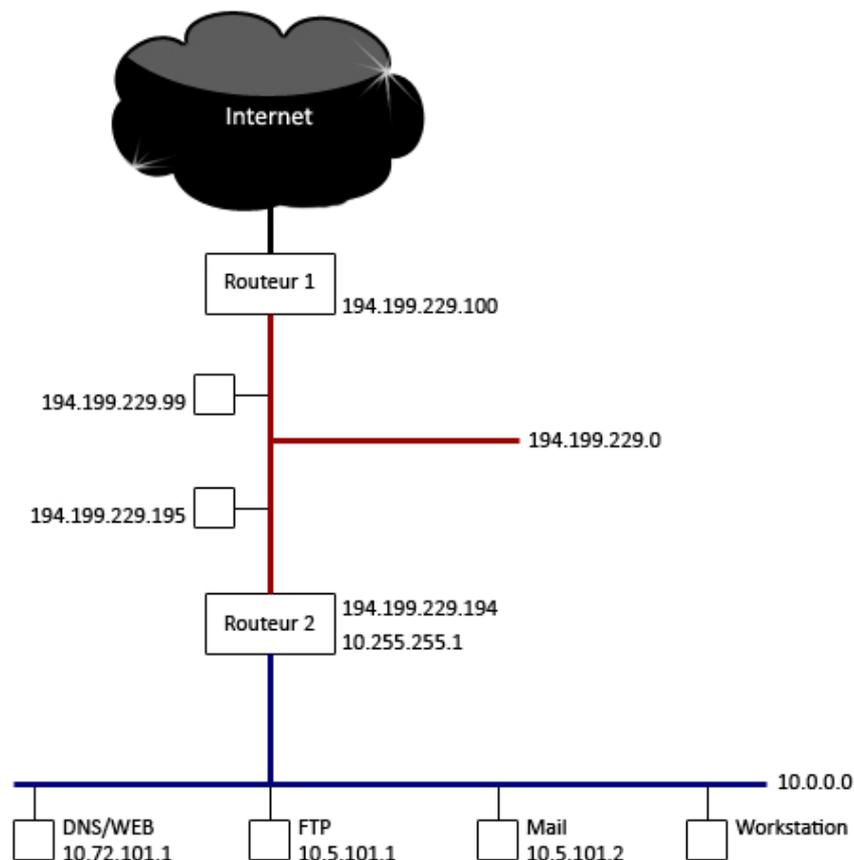
- a. Fonction d'un routeur filtrant : répète les paquets d'un côté et de l'autre des réseaux qu'il interconnecte laisse passer uniquement certains paquets, en fonction de règles prédéfinies par l'administrateur
- b. Un proxy est un dispositif qui permet de sécuriser un réseau (de niveau service). Il se comporte comme un serveur, qui fournira les services d'un autre serveur, en servant « d'intermédiaire »
- c. Un procédé cryptographique à clé asymétrique est une utilisation de 2 clés, une clé privée qui permet de décrypter, et une clé publique qui permet de crypter les messages. La transmission de message est cryptée.
- d. Un échange de « Diffie/Hellman » est basé sur le transfert, de données publiques, basées sur un calcul mathématique, qui ne peut être effectué qu'à partir de données privées. Manière d'échange de clés, sans qu'elles circulent en clair sur le réseau
L'intérêt est que l'on peut transférer des clés sans qu'elles soient en clair.
- e. Le spoofing est basé sur le principe de « man in the middle », il permet de se faire passer, au vu de 2 interlocuteurs, pour le poste distant à joindre.

2. Exercice de TD facile

- a. Le certificat CA authentifie la clé publique d'Alice, dans la mesure où le certificat contient la signature de la clé publique est signée par une autorité de certification.
- b. Eve ne peut pas falsifier la clé publique car elle n'est pas reconnue par l'autorité de confiance.
- c. L'autorité de certification est une entreprise qui valide les informations contenues dans un certificat. Ainsi on peut lui faire confiance lorsque l'on rencontre un certificat signé par celle-ci.

3. Exercice de TD

- a. Architecture



b. Tables de routage :

- Sur les machines de la DMZ :
 - ip r a default via 194.199.229.100
 - ip r a 10.0.0.0/8 via 194.199.229.194
 - ip r a 194.199.229.0/24 dev eth0
- Machines du réseau interne :
 - ip r a 10.0.0.0/8 dev eth0
 - ip r a default via 10.255.255.1

c. Non, elles ne peuvent pas, car l'adressage des machines internes est un adressage privé, et celui-ci n'est pas routable sur l'internet. La solution est d'installer un SNAT sur le routeur 2 (194.199.229.100).

d. Non, les machines de l'internet ne peuvent pas accéder aux services internes, pour les mêmes raisons. La solution est d'installer un DNAT sur le routeur 2 (194.199.229.194).

e. Uniquement le SNAT va intervenir (routeur 2).

Le paquet sortant aura l'IP « 194.199.229.194 ».

4. Exercice synthèse

- a. A
- b. B
- c. C
- d. D
- e. E
- f. F
- g. G
- h. H

5. Ingénierie de réseau

- a. A
- b. B
- c. C
- d. D