

Master 2 SeCReTS 2010-2011  
Module ``Concepts de sécurité & réseaux''  
Examen – Partie 2

**Architecture réseau**

---

Consignes :

- 1h maximum ;
  - tout document autorisé ;
  - aucune communication ;
  - aucun accès à un ordinateur, une station de travail, un téléphone portable, une calculatrice, un PDA ou tout autre dispositif électronique, connectable ou non.
- 

**Architecture réseau (10 points)**

Les questions portent sur le schéma joint. On peut y observer 2 zones publiques, la DMZ (serveurs WWW, DNS et SMTP) et le Proxy, ainsi que 3 zones internes (Administrateurs, Utilisateurs et Serveurs intranet).

Sur le routeur et le pare-feu, le routage entre les interfaces est activé. Sur le pare-feu, tous les types de trafic sont interdits par défaut.

Dans le reste du sujet, lorsqu'on vous demande des règles de routage, vous les exprimerez sous la forme suivante (mot-clé any pour désigner toutes les adresses IP) :

permit ip <ip source> <masque source> <ip destination> <masque destination>

Pour exprimer des règles de filtrage, vous utiliserez la syntaxe de iptables.

1. Les administrateurs doivent pouvoir accéder au port 22 (SSH) des machines de la DMZ. Décrivez les règles de routage et de filtrage à mettre en place pour autoriser ces accès.
2. On souhaite donner un accès vers Internet aux utilisateurs, en passant par le Proxy présent dans l'architecture.
  - Donnez les règles de routage et de filtrage autorisant respectivement l'accès des utilisateurs vers le proxy et l'accès du proxy vers Internet.
3. Les serveurs de la DMZ doivent être accessibles pour les clients en provenance d'Internet. Donnez les règles de filtrage correspondantes.



