Archi réseau:

Question 1:

Routeur pate Admin: 192.168.0.254

Réseau entre routeur et PF : 192.168.5.0/24
Routeur pate PF : 192.168.5.1
PF Pate Routeur : 192.168.5.254

Règle pare-feu accès admin sur SSH DMZ

IP Src | Port SRC | IP Dest | Port Dst | Proto

192.168.0.0/24 | Any | 201.203.203.[201 - 202 - 203 - 204] | 22 | TCP

Question 2 :

NAT : Substitution de l'@IP Src par l'@IP du pare-feu (équipement Natant)

Proxy : Substitution de la requête client au niveau applicatif par un requête énamant du proxy.

Règle pare-feu utilisateurs vers proxy:

192.168.1.0/24 | Any | 201.203.203.201 | 80 - 443 | TCP

Règle pare-feu Proxy vers Internet

201.202.203.201 | Any | Any | 80 - 443 | TCP

Ajout de la règle DNS pour la résolution du nom

En mode bourrin :)

Any | Any | 201202.203.203 | 53 | TCP-UDP

Question 3 Accès des clients vers DMZ:

Any | Any | 201.203.203.202 | 80 - 443 | TCP

Any | Any | 201.203.203.203 | 53 | TCP - UDP

Any | Any | 201.203.203.204 | 25 | TCP

Remarque : Les clients n'ont pas a utiliser le proxy

Detection d'intrusion

Question 1:

NIDS avec analyse du traffic en temps réel.

Question 2:

La sauvegarde du flux analysé sur espace de stockage interne.

Question 3:

Certif A:

L'utilisation de TLS/SSL empêche la lecture du flux, avec SSL le flux est chiffré.
L'installation du certificat serveur HTTP sur le NIDS permettra de déchiffrer le flux à destination du serveur web et donc de l'analyser.

IGC et certificat:

Proptio : Paul - CA : AC1

Utilisation : vérifier Signature mail

x509v3

Certif B:

2.1:

D = AC RAcine

E : CA Utilisateur

2.2: Relou à faire :S

Juste à regarder le titre de "Issuer" et "Suject" pour construire l'arbre

2.3:

Regarder les certif G et H " CRL" et faire correspondre les "Serial Number" de la CRL avec ceux des certif utilisateur