Exercice – Proxy - N°69

Énoncé

Un administrateur envisage de mettre en place un **serveur mandataire** (*proxy*) pour optimiser et contrôler les accès aux sites Web externes à l'entreprise depuis le réseau local. Les adresses du réseau local sont privées.

Un routeur ADSL connecte le réseau local à internet via un fournisseur d'accès à internet (FAI). Le service NAT (*Network Address Translator*) est installé sur ce routeur.
Aucun filtrage n'est actif sur le routeur, le FAI prend en charge la sécurité des accès.

L'administrateur hésite entre différentes solutions pour choisir l'emplacement de son serveur *proxy* sur le réseau. Son objectif est d'obliger les utilisateurs à passer par le service *proxy* pour accéder au *Web*. *Attention, passer par l'ordinateur **serveur proxy** ne veut pas dire forcément qu'on utilise le **service proxy**.*

Tous les utilisateurs ont la possibilité de modifier le paramétrage de leur navigateur Internet (passage par un *proxy* ou non, enregistrement de l'adresse du *proxy*). Pour des raisons organisationnelles, certains utilisateurs privilégiés ont les permissions suffisantes pour modifier le paramétrage IP de leur poste (adresse IP, adresse de la passerelle)

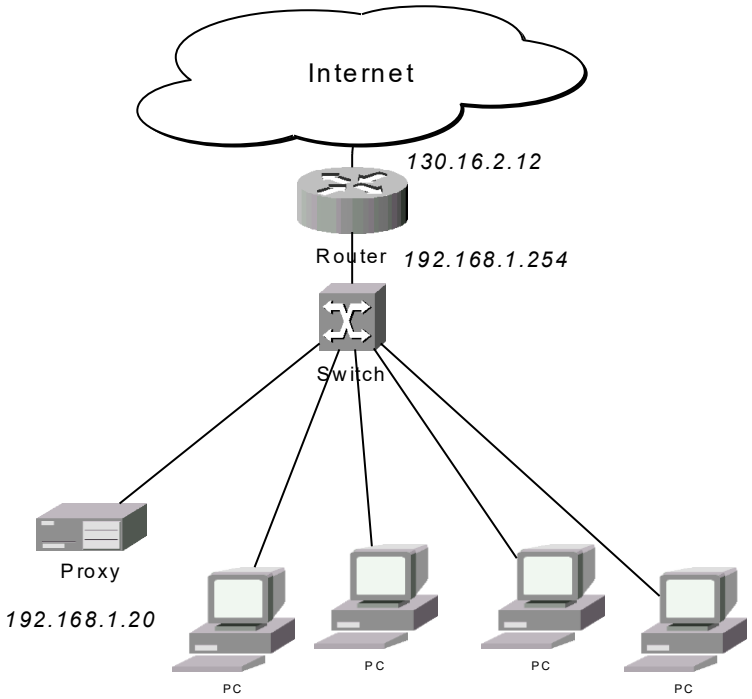
Les pages suivantes présentent différentes architectures envisagées pour faire en sorte que les utilisateurs passent par le service *proxy* pour accéder à Internet. Vous êtes chargé d'aider l'administrateur à choisir la meilleure solution.

Questions

Pour chacune des architectures présentées répondre aux questions suivantes :

- Le passage par le service *proxy* est-il obligatoire pour les **utilisateurs non privilégiés** ? Si non, que peut faire un **utilisateur non privilégié** pour contourner le service *proxy* ?
- Le passage par le service *proxy* est-il obligatoire pour les **utilisateurs privilégiés** ? Si non, que peut faire un **utilisateur privilégié** pour contourner le service *proxy* ?
- Pour chaque architecture proposée, modifier ou ajouter les règles de filtrage ou de translation d'adresses (NAT) afin d'empêcher le contournement du service *proxy*. Une méthode pour représenter les règles est proposée en **Annexe**.

Architecture 1



Postes appartenant au réseau 192.168.1.0
Le nombre de postes du schéma n'est pas représentatif.

Paramétrage actuellement en vigueur :

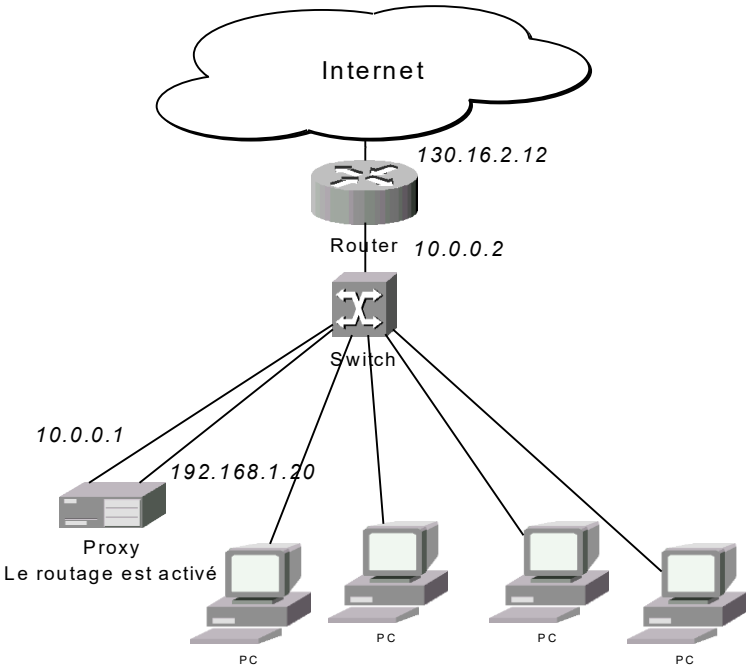
- Le routeur effectue la traduction de toutes les adresses (NAT) et n'a aucune règle de filtrage active.
- Les postes sont configurés avec le *routeur* 192.168.1.254 comme *passerelle par défaut.*
- Les navigateurs Internet sont paramétrés pour utiliser le *proxy* 192.168.1.20.

Annexe : Exemple de table de filtrage

Le routeur parcours la table de filtrage, dès qu'une règle s'applique elle est prise en compte et le parcours de la table s'arrête. Autrement dit : seule la première règle applicable rencontrée est exécutée. Par définition, tout ce qui n'est pas autorisé est interdit, ainsi si aucune règle ne s'applique, le paquet est refusé.

No de règle	Interface d'arrivée/sens	Action	Adresse Source	Port source	Adresse Destination	Port destination	Protocole	Description

Architecture 2



Postes appartenant au réseau 192.168.1.0

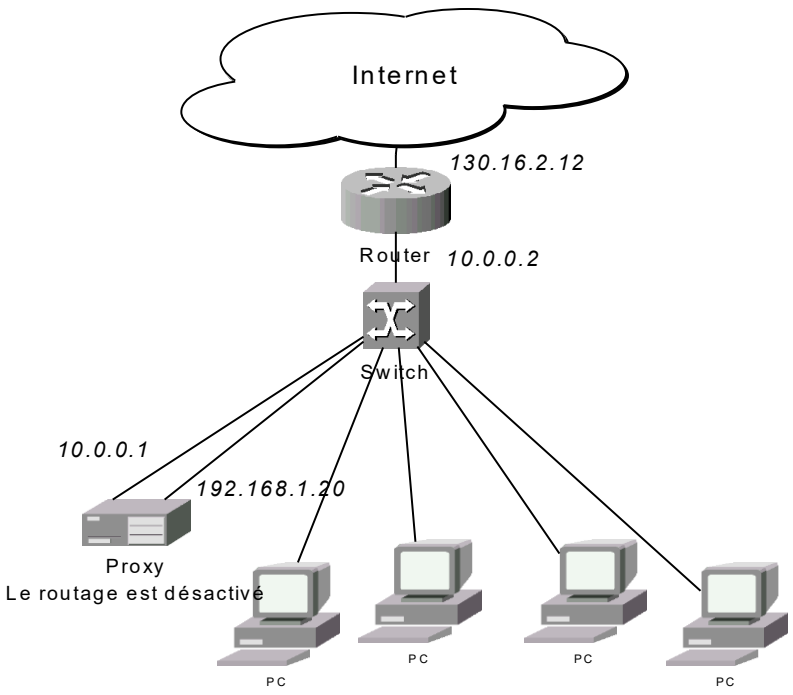
Le nombre de postes du schéma n'est pas représentatif.

Paramétrage actuellement en vigueur :

- Le routeur effectue la traduction de toutes les adresses (NAT) et n'a aucune règle de filtrage active
- Les postes sont configurés avec le *proxy* 192.168.1.20 comme *passerelle par défaut*.
- Les navigateurs Internet sont paramétrés pour utiliser le *proxy* 192.168.1.20.

No de règle	Interface d'arrivée/ sens	Action	Adresse Source	Port source	Adresse Destination	Port destination	Protocole	Description

Architecture 3



Postes appartenant au réseau 192.168.1.0
Le nombre de postes du schéma n'est pas représentatif.

Paramétrage actuellement en vigueur :

- Le routeur effectue la traduction de toutes les adresses (NAT) et n'a aucune règle de filtrage active
- Les postes n'ont pas de passerelle par défaut.
- Les navigateurs Internet sont paramétrés pour utiliser le *proxy* 192.168.1.20.

Remédiation : même règle de filtrage que l'architecture précédente

Annexe : Exemple de table de filtrage

Le routeur parcours la table de filtrage, dès qu'une règle s'applique elle est prise en compte et le parcours de la table s'arrête. Autrement dit : seule la première règle applicable rencontrée est exécutée. Par définition, tout ce qui n'est pas autorisé est interdit, ainsi si aucune règle ne s'applique, le paquet est refusé.

No de règle	Interface d'arrivée /sens	Action	Adresse Source	Port source	Adresse Destination	Port destination	Protocole	Description
1	130.16.2.12	accepte				80		accepte les connexions HTTP entrantes