

Exonet N°9 – Proxy - NAT

Propriétés	Description
Intitulé long	Gestion des accès à internet depuis le réseau local.
Présentation de publication	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.
Date de publication	14-01-2003
Public concerné	BTS Services informatiques aux organisations
Matière	SISR2 – Conception des infrastructures réseaux
Compétences	Sécuriser une infrastructure réseau
Savoirs	Modèles de référence associés aux architectures réseaux
Objectifs	Évaluer et ajuster le niveau de sécurité demandé en analysant différentes architectures d'accès à internet.
Pré-requis	Routage, filtrage
Mots-clés	Proxy, Nat, routeur, filtrage, connexion internet
Auteur(es)	Roger SANCHEZ – relecture Eric Deschaintre

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)

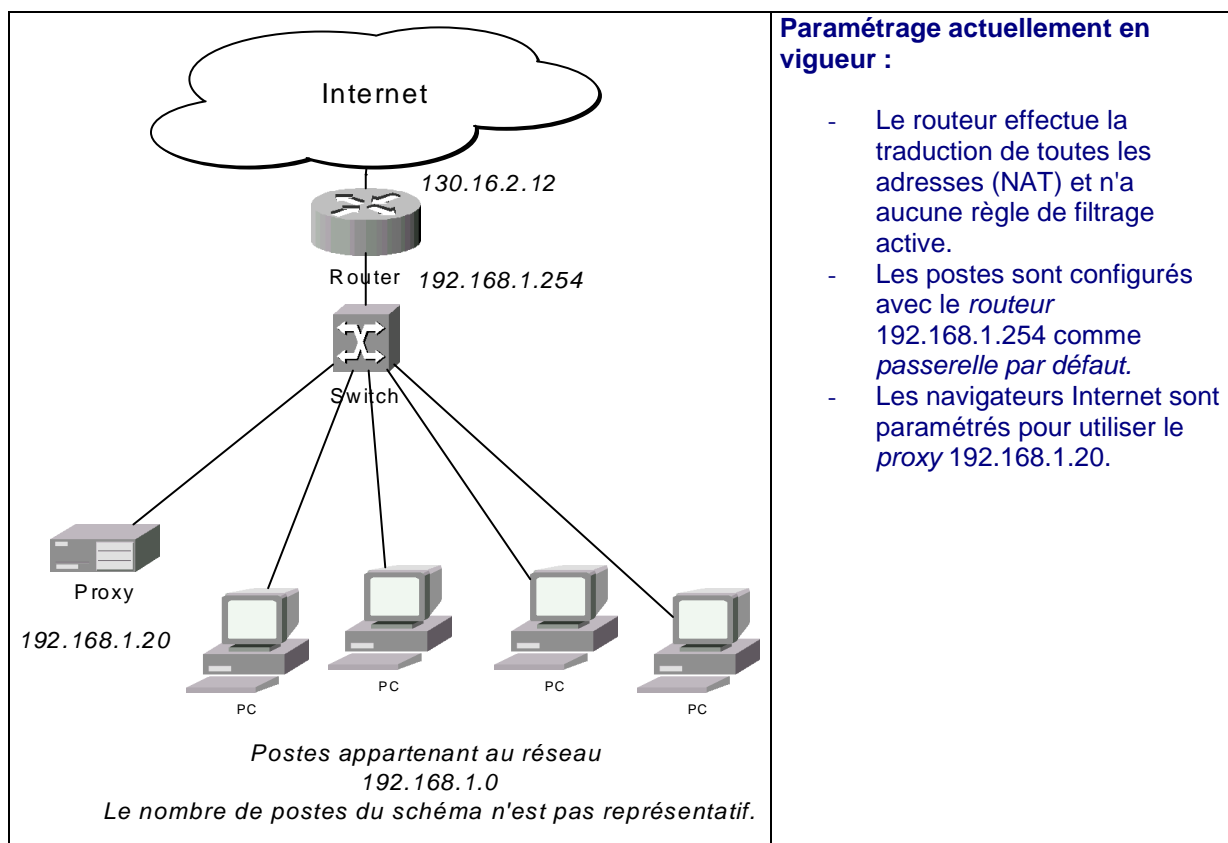
Les pages suivantes présentent différentes architectures envisagées pour faire en sorte que les utilisateurs passent par le service *proxy* pour accéder à Internet. Vous êtes chargé d'aider l'administrateur à choisir la meilleure solution.

Questions

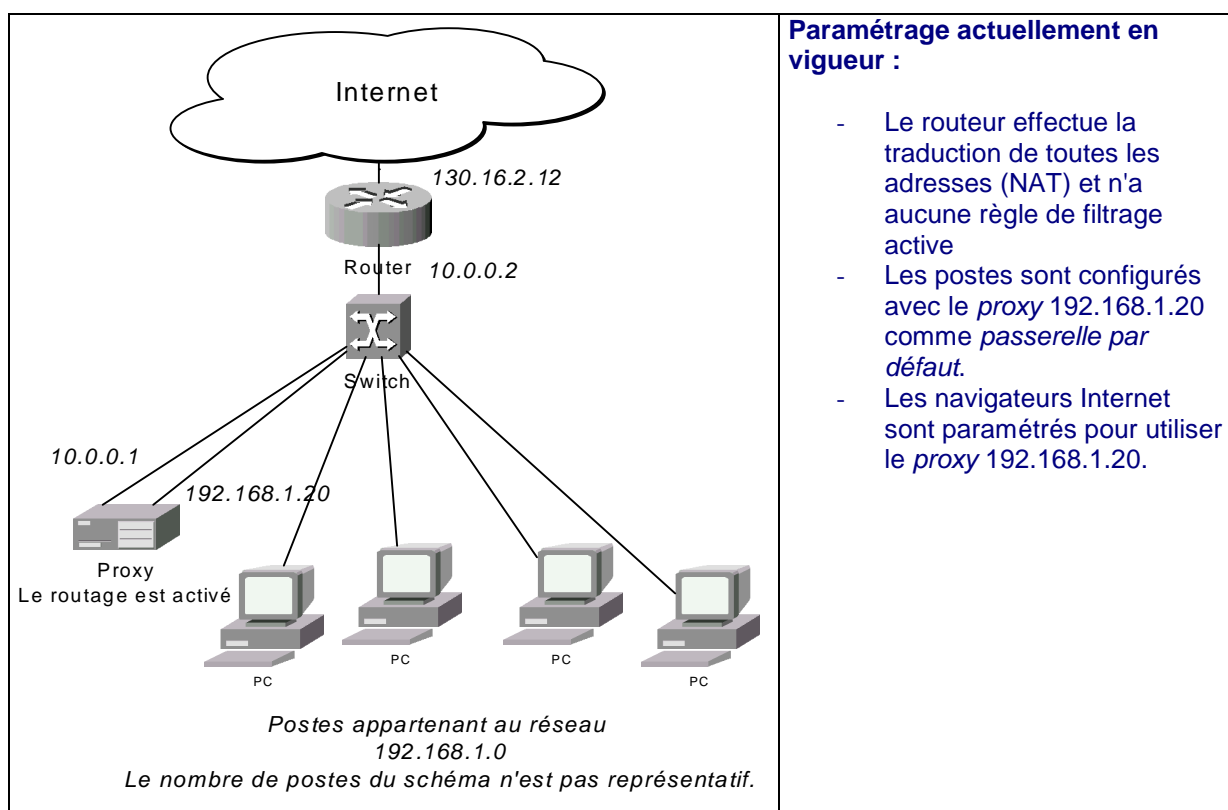
Pour chacune des architectures présentées répondre aux questions suivantes :

- 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**.

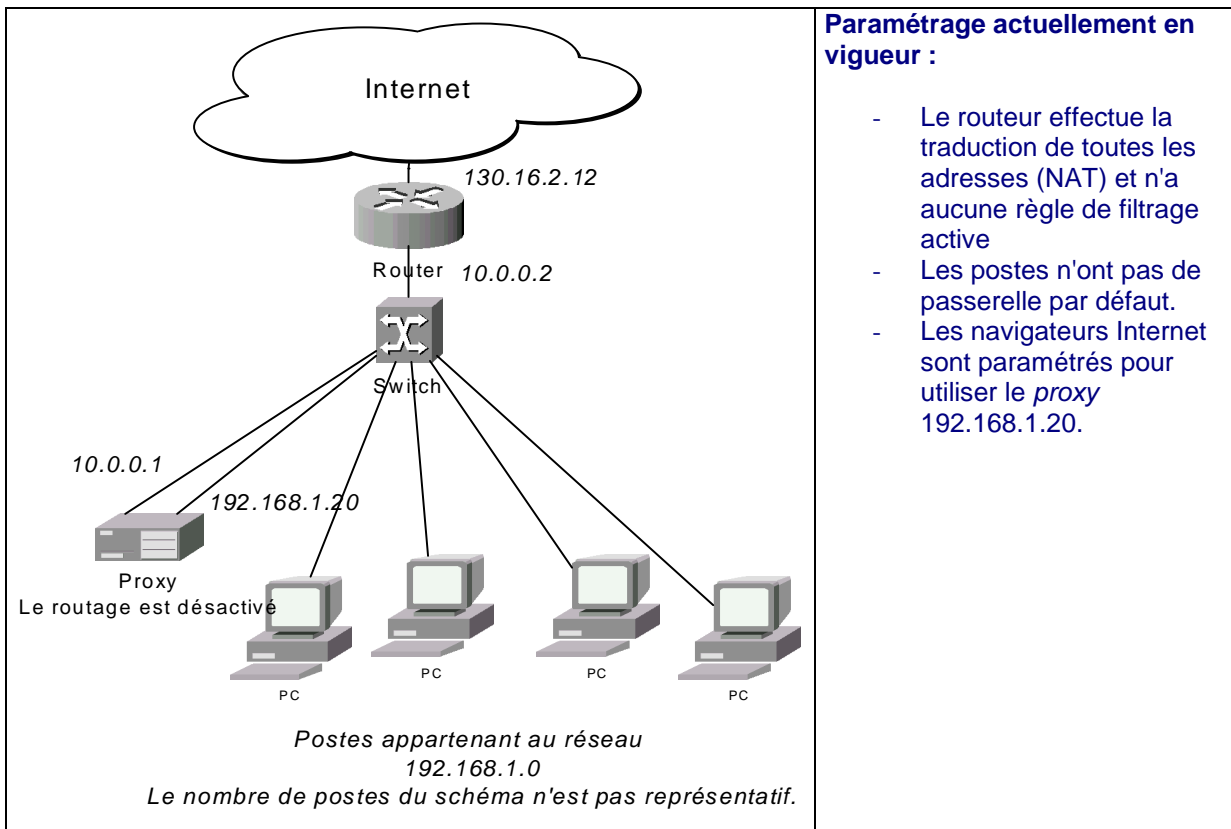
Architecture 1



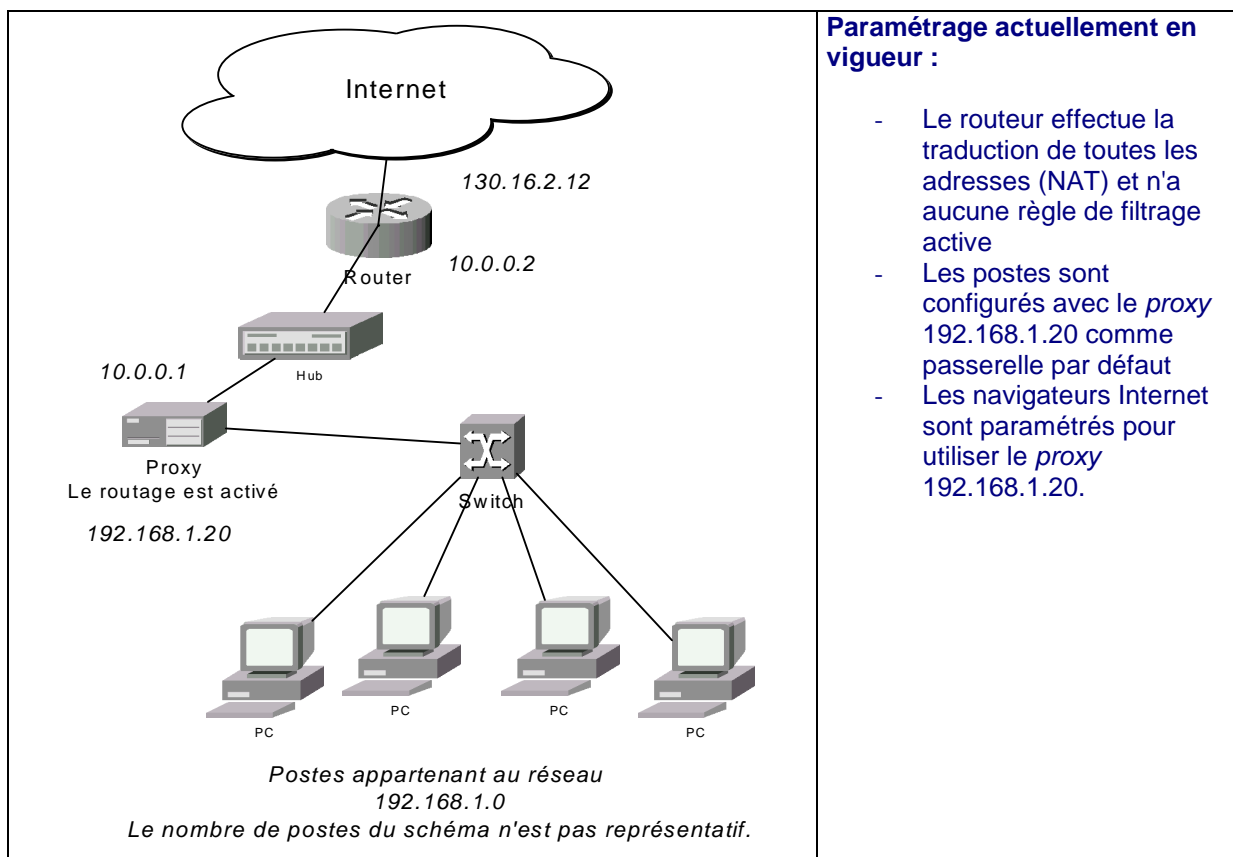
Architecture 2



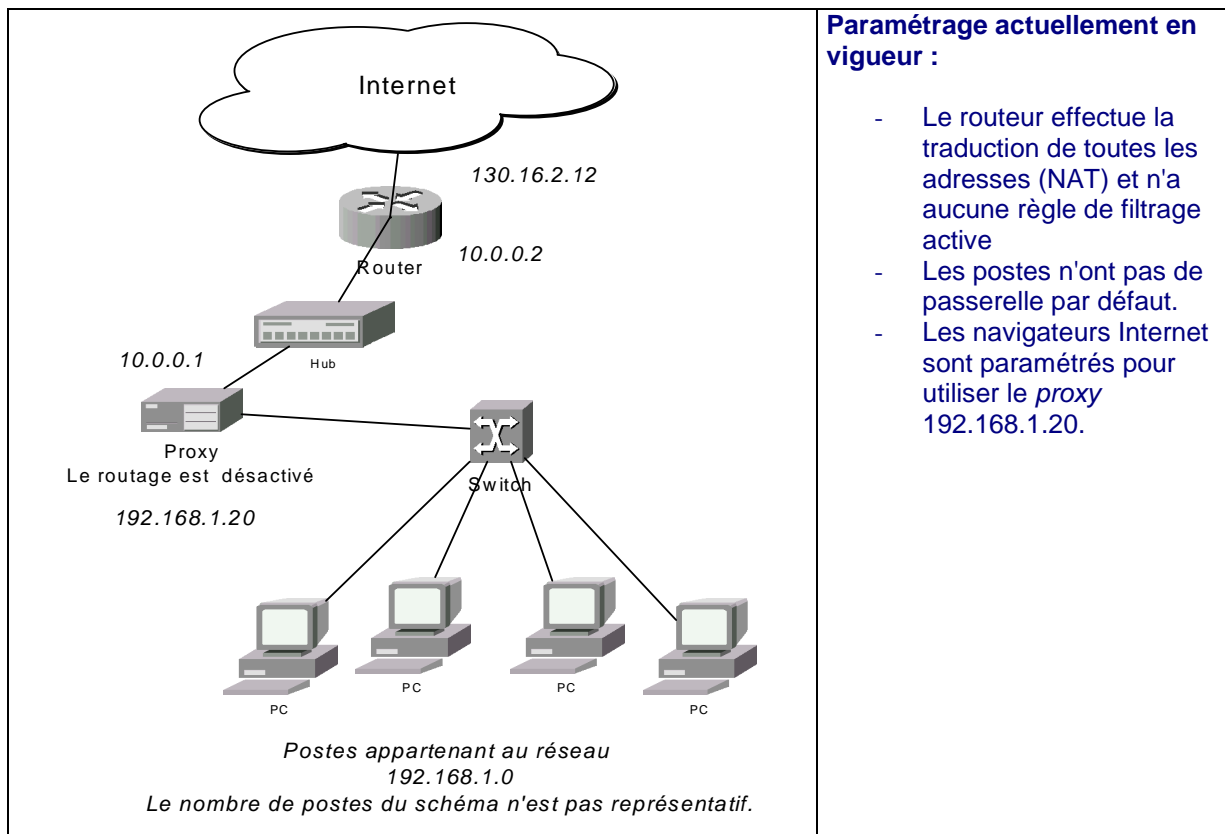
Architecture 3



Architecture 4



Architecture 5



Annexe : Exemple de table de filtrage

Le routeur parcourt 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	Action	Adresse Source	Port source	Adresse Destination	Port destination	Protocole	Description
1	130.16.2.12	accepte				80		accepte les connexions HTTP entrantes

Proposition de correction

Architecture 1

Tous les utilisateurs peuvent accéder directement à Internet sans passer par le service Proxy. Il suffit qu'ils n'indiquent pas le Proxy dans la configuration de leur navigateur. Ils ont accès directement au routeur qui translate toutes les adresses.

En ajoutant la règle de filtrage suivante au routeur Internet, on peut bloquer l'accès Web qui ne vient pas du Proxy.

N° de règle	Interface d'arrivée	Action	Adresse source	Port source	Adresse destination	Port destination
1	192.168.1.254	Accepte	192.168.1.20			

Ici on accepte tout ce qui vient du Proxy, celui-ci fait du NAT.

Architecture 2

Tous les utilisateurs peuvent accéder directement à Internet en utilisant le serveur utilisé comme routeur et non comme Proxy. Il suffit qu'ils n'indiquent pas le Proxy dans la configuration de leur navigateur. Le Proxy a la fonction routage activé, et est déclaré comme passerelle par défaut, donc sans modifier leur adresse IP, les utilisateurs auront accès au routeur Internet en utilisant le Proxy comme routeur intermédiaire et non comme Proxy.

Si le routeur Internet ne translate que les adresses en provenant du réseau 10.0.0.0, les utilisateurs non privilégiés n'accéderont pas à Internet.

Pour les utilisateurs privilégiés il faut rajouter la règle suivante sur le routeur Internet

N° de règle	Interface d'arrivée	Action	Adresse source	Port source	Adresse destination	Port destination
1	10.0.0.2	Accepte	10.0.0.1			

Architecture 3

Les utilisateurs non privilégiés ne peuvent pas contourner la fonction Proxy. Ils n'ont pas la même adresse réseau que le routeur Internet, qu'ils ne peuvent donc utiliser directement

Les utilisateurs privilégiés peuvent modifier leur configuration IP pour accéder au routeur Internet en contournant le Proxy.

On peut ne pas changer les règles du NAT sur le routeur Internet.
Mais il faut ajouter la règle proposée pour l'architecture précédente.

Architecture 4

Idem que pour l'architecture 2.

Architecture 5

Les utilisateurs non privilégiés ne peuvent pas contourner la fonction Proxy. Ils n'ont pas la même adresse réseau que le routeur Internet, qu'ils ne peuvent donc utiliser directement

Les utilisateurs privilégiés peuvent modifier leur configuration IP mais ils ne peuvent accéder directement au Routeur Internet. Il faut passer par la machine Proxy, or la fonction routage n'est pas activée, donc ils ne peuvent pas contourner le service Proxy.

Rien de supplémentaire n'est nécessaire.