TD sécurité : Exonet N°54 bis - Routeur NAT/PAT

Description

Contexte de travail

L'entreprise SAGI externalisait ses serveurs HTTP, NNTP et SMTP pour l'Internet et l'extranet. Elle a décidé d'accueillir dans une zone démilitarisée ces serveurs. Ceci l'a conduit à revoir son architecture réseau et sa politique de sécurité.

Après avoir décidé dans un premier temps de créer une DMZ avec une adresse publique, l'administrateur décide d'utiliser aujourd'hui une adresse privée pour renforcer la sécurité.

Le routeur d'accès distant (R1) est un routeur filtrant, il permet d'interdire certains flux et en autoriser d'autres. Ce routeur prend aussi en charge la traduction d'adresses (NAT/PAT).

Les clients du réseau local ont un accès à Internet.

Vous trouverez en annexe 1 la structure schématique du nouveau réseau de l'entreprise.
Vous trouverez en annexe 2, des exemples de règles NAT/PAT appliquées par le routeur R1.
Vous trouverez en annexe 3 des exemples de règles de redirection appliquées par le routeur R1.

Travail à Réaliser

Première partie

1. Pourquoi le routeur R1 masque-t-il les adresses du réseau 192.168.50.0/24 ?
2. Expliquer le rôle des règles de l'annexe 3.
3. Le routage porte-t-il sur les adresses substituées ou sur les adresses réelles ?

Deuxième partie

1. Pourquoi n'utilise-t-on pas le port standard 80 pour rediriger vers le serveur http partenaire de nom prive.sagi.fr ?
2. Comment les clients http des partenaires doivent-ils adresser leur requête pour accéder au serveur http partenaire prive.sagi.fr?

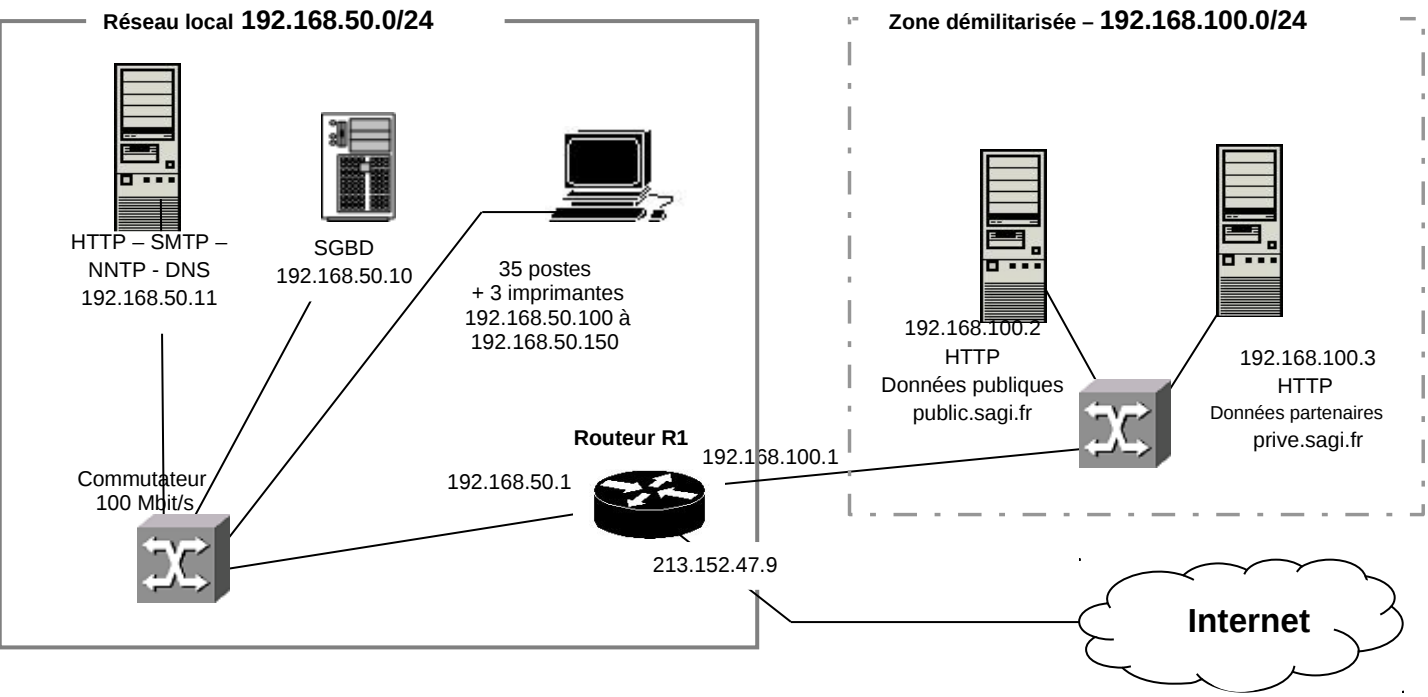
Troisième partie

L'administrateur décide d'appliquer une politique de sécurité plus restrictive. Il veut empêcher tout trafic entre l'Internet et l'Intranet. Pour cela il va mettre en place un Proxy HTTP sur un serveur d'adresse 192.168.100.4 dans la DMZ qui écoutera sur le port 8080. Tous les utilisateurs devront passer par ce Proxy.

1. Comment fonctionne un Proxy-HTTP et quel est son intérêt ?
2. Proposer une solution pour permettre aux postes de l'Intranet d'utiliser le Proxy-HTTP de façon transparente.
3. Rédiger le(s) règle(s) permettant cette solution.

Annexes

Annexe 1 : Structure schématique du réseau d'une entreprise



Annexe 2 : exemples de règles NAT/PAT

Le type NP (NAT/PAT) s'applique en sortie de l'interface et substitue l'adresse IP source et le port source privés par une adresse IP publique et un port public. Cette règle génère une entrée dans une table interne du routeur qui permettra de gérer la substitution inverse.

numéro	Interface	Type	protocole	Adresse publique	port public	adresse privée	port privé
1	213.152.47.9	NP	TCP	213.152.47.9	*	192.168.50.0/24	*
2	213.152.47.9	NP	TCP	213.152.47.9	*	192.168.100.0/24	*

Annexe 3 : exemples de règles de redirection

Le Type R (Redirection) s'applique en entrée de l'interface et substitue l'adresse IP destination et le port de destination publics par une adresse IP privée et un port privé. Cette règle génère une entrée dans une table interne du routeur qui permettra de gérer la substitution inverse.

numéro	Interface	Type	protocole	Adresse publique	port public	adresse privée	port privé
3	213.152.47.9	R	TCP	213.152.47.9	80	192.168.100.2	80
4	213.152.47.9	R	TCP	213.152.47.9	4500	192.168.100.3	80