

Exonet N°54 bis : Routeur NAT/PAT

Description

Propriétés	Description
Intitulé long	Mettre en oeuvre des règles de NAT/PAT et de redirection sur un routeur.
Présentation	On reprend le contexte de travail de l'exonet 54 pour l'adapter à un contexte plus actuel : réseau local protégé, DMZ privée et accès internet.
Public concerné	BTS Services informatiques aux organisations
Matière	SISR2 – Conception des infrastructures réseaux
Compétences	Configurer les éléments d'interconnexion permettant d'établir des périmètres de sécurité
Savoirs	Modèles de référence associés aux architectures réseaux
Objectifs	Fixer les règles d'un routeur NAT/PAT
Mots-clés	Routeur filtrant, filtrage, Nat/Pat, Redirection de port, Proxy, Proxy transparent, DMZ
Auteur(es)	Roger SANCHEZ (avec la participation importante et précieuse de Daniel Regnier et Valérie Emin)
Version	v 1.0
Date de publication	26 février 2006

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?

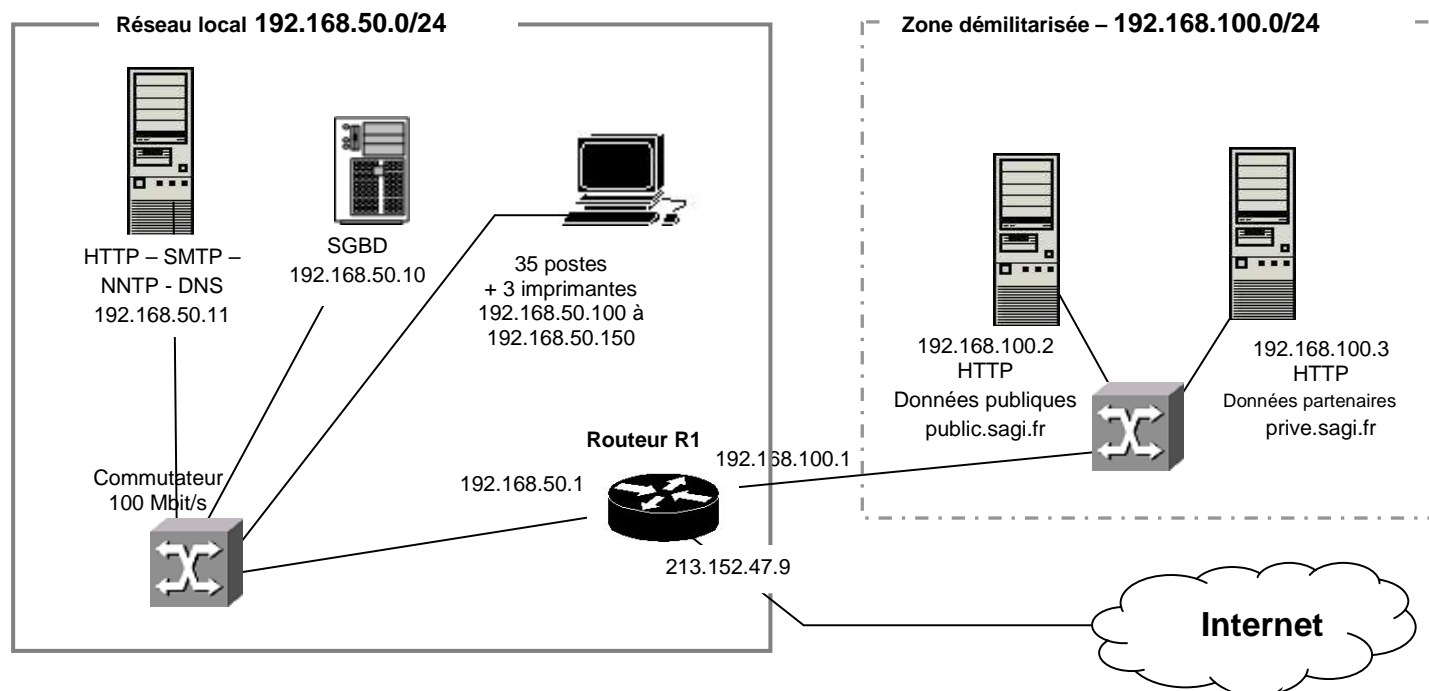
Troisième partie

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

Proposition de correction

Première partie :

1. La RFC 1918 stipule que les adresses de classe C 192.168.x.x sont des adresses privées qui ne peuvent être routées sur Internet, il faut donc les substituer par une adresse publique (ici l'adresse publique du routeur).
2. Les règles de l'annexe 3 redirigent vers les serveurs http de la DMZ les paquets dont l'entête TCP comporte les ports de destination précisés. L'adresse IP de destination qui est l'adresse publique du routeur sera substituée par l'adresse privée précisée. Le port de destination sera lui aussi substitué si cela est nécessaire. Ces substitutions sont faites avant d'entrer dans le processus de routage et de filtrage.
3. Le processus de routage utilise l'adresse de destination d'un paquet pour prendre sa décision de routage. Cette décision ne peut être prise sur les adresses substituées car celles-ci ne correspondent pas aux adresses réelles du réseau local. Les règles suivantes sont donc appliquées :
 - On substitue en entrée de l'interface les adresses et les ports de destination par les adresses et les ports privés. Cette substitution se fait avant le processus de routage et de filtrage qui va donc porter sur les adresses réelles.
 - On substitue en sortie de l'interface les adresses et les ports sources par les adresses et les ports publics. Cette substitution se fait après le processus de routage et de filtrage qui a donc porté sur les adresses réelles.

Deuxième partie

1. Il faut différencier les ports des serveurs. En effet une requête DNS sur public.sagi.fr ou prive.sagi.fr renvoie l'adresse IP publique du routeur. On ne peut donc pas avoir deux fois le même port associé à la même adresse IP publique, car il est impossible de rediriger correctement la requête vers le serveur correspondant. On laisse ici les données publiques sur le port 80 (port standard du protocole http) mais on change le port http des données partenaires.
2. Les clients des partenaires doivent connaître ces numéros de port (il faut saisir le numéro de port dans l'URL.) ex: HTTP://prive.sagi.fr:4500

Remarque : on peut mettre en œuvre une solution basée sur les hôtes virtuels (Virtual Host). Dans ce cas la redirection se fait au niveau d'un des serveurs http, par exemple le serveur standard. Cette solution permet de ne pas spécifier le port dans l'URL.

Troisième partie :

1. Le terme français pour désigner un Proxy est mandataire, c'est-à-dire celui à qui on confie un travail. Les proxys sont des relais. Ils jouent le rôle de serveur pour le client, et de client pour le serveur. Ils peuvent analyser les données dans le contexte de l'application et appliquer des filtres (sites interdits « blacklist », audit, etc.). Dans une configuration minimum un proxy http mettra en cache les pages HTML visitées optimisant ainsi leur utilisation. Un proxy peut permettre d'éviter les connexions directes depuis un réseau interne vers Internet. Sans routeur, il permet le partage de l'accès à Internet avec une interface publique.
2. Deux solutions sont possibles :
 - Configurer tous les navigateurs Internet pour paramétrer le Proxy. Cette solution n'est pas transparente et peut être contournée par les postes.
 - Rediriger en entrée de l'interface 192.168.50.1 tout paquet avec l'adresse du port destination 80 vers le Proxy 192.168.100.4. C'est la technique dite du "**Proxy transparent**". Il faut bien sûr que le Proxy le permette c'est le cas de la plupart des Proxy du marché.

numéro	Interface	Type	protocole	Adresse publique	port public	adresse privée	port privé
5	192.168.50.1	R	TCP	*	80	192.168.100.4	8080

Ici les requêtes http à partir du réseau local sont redirigées vers le proxy situé dans la DMZ. Le Proxy agira ensuite en tant que client Internet il utilisera donc un port client supérieur à 1024 pour ses échanges. Il n'y aura donc pas de confusion avec les échanges des serveurs de la DMZ.

Pour plus de sécurité il faudrait supprimer la règle 1 du NAT/PAT qui masque les adresses des postes du réseau local et leur permet l'accès à Internet.