**TD Réseaux : sujet les Routeurs Filtrants**

## Description

|  |  |
| --- | --- |
| Propriétés | Description |
| **Intitulé** | Mettre en œuvre des règles de filtrage sur un routeur. |
| **Public concerné** | BTS Services informatiques aux organisations |
| **Matière** | SISR 3 – 4 – 5 |
| **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 filtrant |
| **Mots-clés** | Routeur filtrant, filtrage, firewall, pare-feu, Nat/Pat, DMZ |

## 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.

Le routeur d’accès distant (R1) est un routeur filtrant, il permet d’interdire certains flux et en autoriser d'autres. Vous êtes chargé d’implémenter dans le routeur R1 les règles définies par la politique de sécurité de l'entreprise.

Vous trouverez dans l’archive de l’exercice les éléments de référence du côté cours sur TCP/IP concernant le datagramme IP, les numéros de ports et de protocoles prédéfinis à connaître, la technique de filtrage de paquets.

Dans notre exercice, ce sont sur ces éléments que portent les filtres.

Vous trouverez en [annexe 1](#Annexe2) la structure schématique du nouveau réseau de l’entreprise

Vous trouverez en [annexe 2](#Annexe2), des exemples de règles précisant la syntaxe à utiliser.

On considère au départ de l'exercice qu'aucune règle n'est active sur le routeur et on utilisera l'annexe 3 pour rédiger ces règles.

Les règles de filtrage s'appliquent avant les règles NAT/PAT en sortie de l'interface et après les règles NAT/PAT en entrée d'interface.

## Les règles de filtrage s'appliquent donc toujours sur des adresses non substituées.

|  |
| --- |
| Travail à Réaliser |

En utilisant l'annexe 3, mettre en œuvre les règles de sécurités suivantes sur les interfaces du routeur R1 :

|  |  |
| --- | --- |
| A | Toutes les communications entre le poste195.115.100.2 et Internet sont autorisées. |
| B | Tous les flux depuis l'Intranet (le réseau local) vers la DMZ sont autorisés mais l'inverse n'est pas vrai. |
| C | Les serveurs HTTP du réseau 195.115.100.0 peuvent accéder à la base de données du poste 192.168.50.10, sur le port TCP 4523. |
| D | Le serveur 195.115.100.2 est un serveur "relais" pour les flux DNS et SMTP du réseau 192.168.50.0. Les communications SMTP et DNS sont autorisées entre les serveurs du réseau local et ceux de la DMZ. |
| E | On autorise les connexions SSH sur les postes de la DMZ à partir de l'Internet et de l'Intranet mais pas sur le réseau 192.168.50.0. |
| F | Les adresses réseaux autorisées à accéder aux "données partenaires" sont 195.83.0.0, 202.10.12.0 et 221.12.184.0 (qui correspondent aux adresses IP des réseaux des entreprises partenaires) |
| G | Le réseau 202.10.12.0 n'est pas autorisé à utiliser le service NNTP sur les données partenaires. |
| H | Il faut interdire tout trafic ICMP en provenance de l'extérieur. |

|  |
| --- |
| Annexes |

## Annexe 1 : Structure schématique du réseau d'une entreprise

Toutes les adresses du réseau 192.168.50.0/24 sont masquées par l'adresse publique du routeur.

## 

SGBD 192.168.50.10

195.115.100.1

**Réseau local 192.168.50.0/24**



195.115.100.2

HTTP - SMTP

DNS

Données publiques

HTTP – SMTP – NNTP - DNS

192.168.50.11

195.115.100.3

HTTP – NNTP

Données partenaires

192.168.50.1

Commutateur

100 Mbit/s

**Routeur R1**



213.152.47.9

**Internet**

35 postes

+ 3 imprimantes 192.168.50.100 à 192.168.50.150



**Zone démilitarisée – 195.115.100.0/28**

## Annexe 2 : Exemple de règles précisant la syntaxe à utiliser

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **No de règle** | **Interface**  **d'arrivée** | **Action** | **Adresse**  **Source** | **Port**  **source** | **Adresse**  **Destination** | **Port**  **destination** | **Protocole** | **Etat TCP** | **Description** |
| 1 | 195.115.100.1 | accepte | 195.115.100.2/32 | \* | \* | 53 | \* |  | accepte les connexions DNS sortantes |
| 2 | 213.152.47.9 | accepte | \* | 53 | 192.115.100.2/32 | \* | \* |  | accepte le retour DNS |
| 3 | 192.168.50.1 | bloque | 192.168.50.0/24 |  | \* |  | 1 (ICMP) |  | empêche le trafic ICMP sortant |
| 4 | 213.152.47.9 | bloque | \* |  | \* |  | 1  (ICMP) |  | empêche tout le trafic ICMP entrant de l'Internet |
| défaut | toutes | bloque | toutes | tous | toutes | tous | tous |  | Règle par défaut, tout ce qui n’est pas autorisé est interdit |

Ici les règles numéro 1 et 2 permettent au serveur DNS 195.115.100.2 de relayer les demandes DNS (il s'agit vraisemblablement d'un serveur cache).

La règle numéro 3 interdit tout trafic ICMP (émis ou en réponse) à partir de l'Intranet. Il s'agit d'interdire ici essentiellement un trafic ICMP entre la DMZ et l'Intranet puisque la règle 4 interdit le trafic ICMP en provenance de L'internet. Mais on évite aussi de fait un flux ICMP possible émis vers l'Internet.

La règle numéro 4 interdit tout trafic ICMP en provenance de l'Internet.

La règle "défaut" est la règle appliquée quand aucune autre règle n'est applicable.

Le routeur est SPI (stateful Inspection Packet) c'est à dire qu'il peut s'appuyer sur l'état TCP. Le routeur gère deux valeurs pour l'état TCP :

* nul ou non renseigné : l'état n'est pas testé par le routeur
* Établi : la connexion TCP est établie

Attention les règles sont appliquées dans l'ordre.

## Annexe 3 : Tableau à utiliser pour rédiger les règles

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **No de règle** | **Interface d'arrivée** | **Action** | **@Source** | **Port source** | **@Destination** | **Port destination** | **Protocole** | **Etat TCP** |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |