Exonet N°54 : Routeur filtrant

Description

Propriétés	Description
Intitulé long	Mettre en oeuvre des règles de filtrage sur un routeur.
Public concerné	BTS Services informatiques aux organisations
Matière	Architecture matérielle des systèmes informatiques
Compétences	Configurer les éléments d'interconnexion permettant d'établir des périmetres de sécurité
Savoirs	Modéles 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
Auteur(es)	Roger SANCHEZ (avec la participation importante et précieuse de Valérie Emin et Daniel Regnier)
Version	v 2.0
Date de publication	20 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.
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 la structure schématique du nouveau réseau de l'entreprise
Vous trouverez en annexe 2, 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

Première partie :

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.

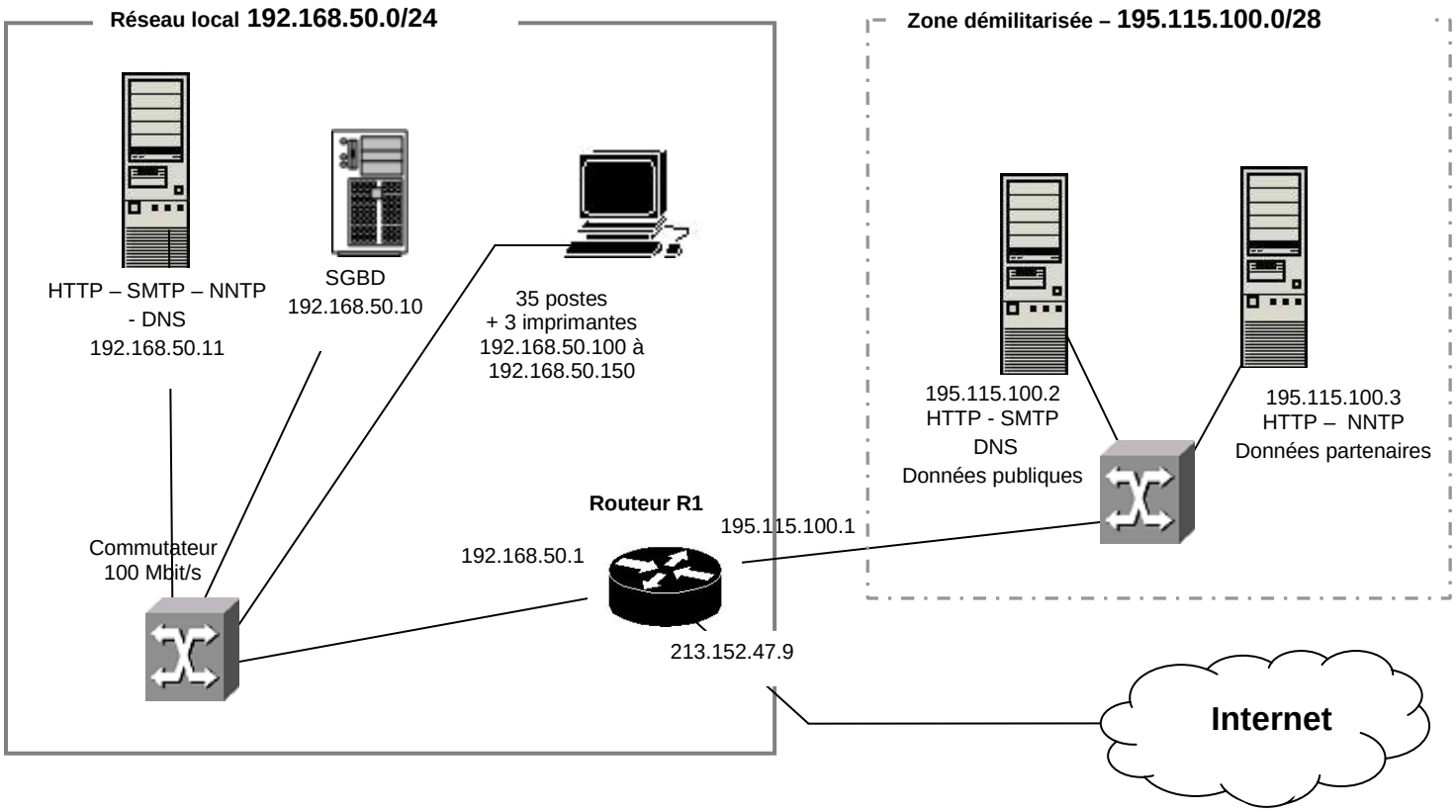
Deuxième partie :

L'administrateur veut autoriser les utilisateurs du réseau local à accéder à Internet. Mais il souhaite éviter toute tentative de connexion TCP à partir d'Internet vers le réseau local.

1. Comment peut-on détecter une tentative de connexion TCP ?
2. Compléter les règles de filtrage pour permettre la communication http et https des clients du réseau local sans autoriser les connexions TCP en provenance d'Internet et à destination du réseau local.

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.

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	Adresse Source	Port source	Adresse Destination	Port destination	Protocole	Etat TCP

Proposition de correction

Première partie

Aucune règle n'étant définie commençons par interdire tout, la politique de sécurité ainsi appliquée est "Tout ce qui n'est pas autorisé est interdit".

No de règle	Interface d'arrivée	Action	Adresse Source	Port source	Adresse Destination	Port destination	Protocole	Etat TCP
défaut	toutes	bloque	toutes	tous	toutes	tous	tous	

Appliquons la règle A :
Toutes les communications entre le poste195.115.100.2 et Internet sont autorisées.

No de règle	Interface d'arrivée	Action	Adresse Source	Port source	Adresse Destination	Port destination	Protocole	Etat TCP
2	213.152.47.9	accepte	*	*	195.115.100.2/32	*	*	
3	195.115.100.1	accepte	195.115.100.2/32	*	*	*	*	
défaut	toutes	bloque	toutes	tous	toutes	tous	tous	

Il faut écrire une règle pour l'aller et une pour le retour.
Remarque : Le poste 195.115.100.2 devient un poste très vulnérable. Il faut veiller à supprimer tous les services non nécessaires, tout compilateur .etc. Il faut aussi vérifier périodiquement les fichiers de "log" et contrôler qu'aucun nouveau programme n'a été installé et que les programmes existant n'ont pas été modifiés.

Règle B :
Tous les flux de l'Intranet (le réseau local) vers la DMZ sont autorisés mais l'inverse n'est pas vrai.

No de règle	Interface d'arrivée	Action	Adresse Source	Port source	Adresse Destination	Port destination	Protocole	Etat TCP
2	213.152.47.9	accepte	*	*	195.115.100.2/32	*	*	
3	195.115.100.1	accepte	195.115.100.2/32	*	*	*	*	
11	192.168.50.1	accepte	192.168.50.0/24	*	195.115.100.0/28	*	*	
défaut	toutes	bloque	toutes	tous	toutes	tous	tous	

Remarque : on autorise ici le flux entre le réseau local et la DMZ pour faciliter l'écriture des règles suivantes. On considère de fait qu'il n'y a pas de danger en provenance du réseau local ce qui est discutable. Ceci dit, il n'y a aucun flux en retour d'ouvert donc le danger est extrêmement limité.

Appliquons la règle C
Les serveurs HTTP du réseau 195.115.100.0 peuvent accéder à la base de données du poste 192.168.50.10. Le retour est rendu possible par la règle 11.

No de règle	Interface d'arrivée	Action	Adresse Source	Port source	Adresse Destination	Port destination	Protocole	Etat TCP
2	213.152.47.9	accepte	*	*	195.115.100.2/32	*	*	
3	195.115.100.1	accepte	195.115.100.2/32	*	*	*	*	
11	192.168.50.1	accepte	192.168.50.0/24	*	195.115.100.0/28	*	*	
21	195.115.100.1	accepte	195.115.100.2/32	*	192.168.50.10/32	4523	TCP	
22	195.115.100.1	accepte	195.115.100.3/32	*	192.168.50.10/32	4523	TCP	
défaut	toutes	bloque	toutes	tous	toutes	tous	tous	

Il n'y a pas de problème d'ordre avec les règles précédentes puisqu'on accepte les paquets dans chaque cas.
Remarque : Les règles 2 et 3 vont permettre à des internautes de se connecter aux données publiques et les règles 11 et 12 vont permettre aux serveurs http de se connecter aux bases de données qui sont dans une zone moins vulnérable.

Règle 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
Remarque: Il ne s'agit pas ici d'autoriser les postes du réseau 192.168.50.0 à utiliser les services DNS et SMTP de la DMZ mais uniquement la communication entre les serveurs. En fait, on a placé dans la DMZ des "relais" DNS (serveur cache) et SMTP (anti-spam et anti-virus) pour éviter toute communication directe entre le serveur DNS et SMTP de l'Intranet (192.168.50.11) et Internet. Le serveur DNS et SMTP de l'Intranet est donc client du serveur DNS et SMTP de la DMZ et lui même est client pour les serveurs DNS et SMTP de l'Internet (ce qui explique les numéros de port dans les règles). Les règles 2 et 3 permettent l'échange de ce serveur avec l'Internet.

Par rapport aux règles précédentes il n'y a pas de problème d'ordre. Les demandes DNS et SMTP du serveur local sont ici gérées par la règle 11. Les retours sont rendus possibles par les règles 31 et 32.

No de règle	Interface d'arrivée	Action	Adresse Source	Port source	Adresse Destination	Port destination	Protocole	Etat TCP
2	213.152.47.9	accepte	*	*	195.115.100.2/32	*	*	
3	195.115.100.1	accepte	195.115.100.2/32	*	*	*	*	
11	192.168.50.1	accepte	192.168.50.0/24	*	195.115.100.0/28	*	*	
21	195.115.100.1	accepte	195.115.100.0/28	*	192.168.50.10/32	4523	TCP	
22	195.115.100.1	accepte	195.115.100.3/32	*	192.168.50.10/32	4523	TCP	
31	195.115.100.1	accepte	195.115.100.2/32	53	192.168.50.11/32	*	*	
32	195.115.100.1	accepte	195.115.100.2/32	25	192.168.50.11/32	*	TCP	
défaut	toutes	bloque	toutes	tous	toutes	tous	tous	

Règle E

On autorise les connexions SSH sur les postes de la DMZ mais pas sur le réseau 192.168.50.0.

No de règle	Interface d'arrivée	Action	Adresse Source	Port source	Adresse Destination	Port destination	Protocole	Etat TCP
2	213.152.47.9	accepte	*	*	195.115.100.2/32	*	*	
3	195.115.100.1	accepte	195.115.100.2/32	*	*	*	*	
11	192.168.50.1	accepte	192.168.50.0/24	*	195.115.100.0/28	*	*	
21	195.115.100.1	accepte	195.115.100.0/28	*	192.168.50.10/32	4523	TCP	
22	195.115.100.1	accepte	195.115.100.3/32	*	192.168.50.10/32	4523	TCP	
31	195.115.100.1	accepte	195.115.100.2/32	53	192.168.50.11/32	*	*	
32	195.115.100.1	accepte	195.115.100.2/32	25	192.168.50.11/32	*	TCP	
41	195.115.100.1	accepte	195.115.100.0/28	22	*	*	TCP	
42	213.152.47.9	accepte	*	*	195.115.100.0/28	22	TCP	
défaut	toutes	bloque	toutes	tous	toutes	tous	tous	

L'ordre par rapport aux précédentes règles importe peu. On ne crée pas de règle d'interdiction puisqu'on a la règle par défaut. Il faudrait 2 règles pour autoriser à partir d'Internet et de l'Intranet mais la règle 11 autorise implicitement le flux SSH en provenance de l'Intranet. La règle 42 autorise le flux SSH en provenance d'Internet. La règle 41 autorise les flux SSH en retour.

Règle F

Les adresses réseaux autorisées à accéder aux "données partenaires" sont 195.83.0.0/24, 202.10.12.0/24 et 221.12.184.0/24 (qui correspondent aux adresses IP des réseaux des entreprises partenaires).
On va créer une règle pour chaque entreprise mais générale pour tous les services, il faut donc impérativement ici, encore une fois, avoir un serveur sur lequel on n'a installé que les services utiles (pas de compilateur qui traîne) et qui est vérifié régulièrement. Il faut prévoir une règle pour chaque retour.

No de règle	Interface d'arrivée	Action	Adresse Source	Port source	Adresse Destination	Port destination	Protocole	Etat TCP
2	213.152.47.9	accepte	*	*	195.115.100.2/32	*	*	
3	195.115.100.1	accepte	195.115.100.2/32	*	*	*	*	
11	192.168.50.1	accepte	192.168.50.0/24	*	195.115.100.0/28	*	*	
21	195.115.100.1	accepte	195.115.100.0/28	*	192.168.50.10/32	4523	TCP	
22	195.115.100.1	accepte	195.115.100.3/32	*	192.168.50.10/32	4523	TCP	
31	195.115.100.1	accepte	195.115.100.2/32	53	192.168.50.11/32	*	*	
32	195.115.100.1	accepte	195.115.100.2/32	25	192.168.50.11/32	*	TCP	
41	195.115.100.1	accepte	195.115.100.0/28	22	*	*	TCP	
42	213.152.47.9	accepte	*	*	195.115.100.0/28	22	TCP	
51	213.152.47.9	accepte	195.83.0.0/24	*	195.115.100.3/32	*	*	
52	213.152.47.9	accepte	202.10.12.0/24	*	195.115.100.3/32	*	*	
53	213.152.47.9	accepte	221.12.184.0/24	*	195.115.100.3/32	*	*	
54	195.115.100..1	accepte	195.115.100.3/32	*	195.83.0.0/24	*	*	
55	195.115.100..1	accepte	195.115.100.3/32	*	202.10.12.0/24	*	*	
56	195.115.100..1	accepte	195.115.100.3/32	*	221.12.184.0/24	*	*	
défaut	toutes	bloque	toutes	tous	toutes	tous	tous	

Règle G
Le réseau 202.10.12.0/24 n'est pas autorisé à utiliser le service NNTP sur les données partenaires.

Ici il y a un problème d'ordre par rapport aux règles précédentes. Cette règle doit être placée avant la 52 (ici elle a le numéro 50).

No de règle	Interface d'arrivée	Action	Adresse Source	Port source	Adresse Destination	Port destination	Protocole	Etat TCP
2	213.152.47.9	accepte	*	*	195.115.100.2/32	*	*	
3	195.115.100.1	accepte	195.115.100.2/32	*	*	*	*	
11	192.168.50.1	accepte	192.168.50.0/24	*	195.115.100.0/28	*	*	
21	195.115.100.1	accepte	195.115.100.0/28	*	192.168.50.10/32	4523	TCP	
22	195.115.100.1	accepte	195.115.100.3/32	*	192.168.50.10/32	4523	TCP	
31	195.115.100.1	accepte	195.115.100.2/32	53	192.168.50.11/32	*	*	
32	195.115.100.1	accepte	195.115.100.2/32	25	192.168.50.11/32	*	TCP	
41	195.115.100.1	accepte	195.115.100.0/28	22	*	*	TCP	
42	213.152.47.9	accepte	*	*	195.115.100.0/28	22	TCP	
50	213.152.47.9	bloque	202.10.12.0/24	*	195.115.100.3/32	119	*	
51	213.152.47.9	accepte	195.83.0.0/24	*	195.115.100.3/32	*	*	
52	213.152.47.9	accepte	202.10.12.0/24	*	195.115.100.3/32	*	*	
53	213.152.47.9	accepte	221.12.184.0/24	*	195.115.100.3/32	*	*	
54	195.115.100..1	accepte	195.115.100.3/32	*	195.83.0.0/24	*	*	
55	195.115.100..1	accepte	195.115.100.3/32	*	202.10.12.0/24	*	*	
56	195.115.100..1	accepte	195.115.100.3/32	*	221.12.184.0/24	*	*	
défaut	toutes	bloque	toutes	tous	toutes	tous	tous	

Règle H
Il faut interdire tout trafic ICMP en provenance de l'extérieur.

Il n'y a rien à faire si on pense que la règle par défaut est suffisante. Mais elle ne l'est pas à cause des règles 2 et 3. Il faut donc une nouvelle règle.

No de règle	Interface d'arrivée	Action	Adresse Source	Port source	Adresse Destination	Port destination	Protocole	Etat TCP
1	213.152.47.9	bloque	*	*	*	*	ICMP	
2	213.152.47.9	accepte	*	*	195.115.100.2/32	*	*	
3	195.115.100.1	accepte	195.115.100.2/32	*	*	*	*	
11	192.168.50.1	accepte	192.168.50.0/24	*	195.115.100.0/28	*	*	
21	195.115.100.1	accepte	195.115.100.0/28	*	192.168.50.10/32	4523	TCP	
22	195.115.100.1	accepte	195.115.100.3/32	*	192.168.50.10/32	4523	TCP	
31	195.115.100.1	accepte	195.115.100.2/32	53	192.168.50.11/32	*	*	
32	195.115.100.1	accepte	195.115.100.2/32	25	192.168.50.11/32	*	TCP	
41	195.115.100.1	accepte	195.115.100.0/28	22	*	*	TCP	
42	213.152.47.9	accepte	*	*	195.115.100.0/28	22	TCP	
50	213.152.47.9	bloque	202.10.12.0/24	*	195.115.100.3/32	119	*	
51	213.152.47.9	accepte	195.83.0.0/24	*	195.115.100.3/32	*	*	
52	213.152.47.9	accepte	202.10.12.0/24	*	195.115.100.3/32	*	*	

53	213.152.47.9	accepte	221.12.184.0/24	*	195.115.100.3/32	*	*	
54	195.115.100..1	accepte	195.115.100.3/32	*	195.83.0.0/24	*	*	
55	195.115.100..1	accepte	195.115.100.3/32	*	202.10.12.0/24	*	*	
56	195.115.100..1	accepte	195.115.100.3/32	*	221.12.184.0/24	*	*	
défaut	toutes	bloque	toutes	tous	toutes	tous	tous	

Récapitulatif avec précision des règles de sécurité mises en œuvre.

No de règle	Interface d'arrivée	Action	Adresse Source	Port source	Adresse Destination	Port destination	Protocole	Etat TCP
1 (H)	213.152.47.9	bloque	*	*	*	*	ICMP	
2 (A)	213.152.47.9	accepte	*	*	195.115.100.2/32	*	*	
3 (A)	195.115.100.1	accepte	195.115.100.2/32	*	*	*	*	
11 (B)	192.168.50.1	accepte	192.168.50.0/24	*	195.115.100.0/28	*	*	
21 (C)	195.115.100.1	accepte	195.115.100.0/28	*	192.168.50.10/32	4523	TCP	
22 (C)	195.115.100.1	accepte	195.115.100.3/32	*	192.168.50.10/32	4523	TCP	
31 (D)	195.115.100.1	accepte	195.115.100.2/32	53	192.168.50.11/32	*	*	
32 (D)	195.115.100.1	accepte	195.115.100.2/32	25	192.168.50.11/32	*	TCP	
41 (E)	195.115.100.1	accepte	195.115.100.0/28	22	*	*	TCP	
42 (E)	213.152.47.9	accepte	*	*	195.115.100.0/28	22	TCP	
50 (G)	213.152.47.9	bloque	202.10.12.0/24	*	195.115.100.3/32	119	*	
51 (F)	213.152.47.9	accepte	195.83.0.0/24	*	195.115.100.3/32	*	*	
52 (F)	213.152.47.9	accepte	202.10.12.0/24	*	195.115.100.3/32	*	*	
53 (F)	213.152.47.9	accepte	221.12.184.0/24	*	195.115.100.3/32	*	*	
54 (F)	195.115.100..1	accepte	195.115.100.3/32	*	195.83.0.0/24	*	*	
55 (F)	195.115.100..1	accepte	195.115.100.3/32	*	202.10.12.0/24	*	*	
56 (F)	195.115.100..1	accepte	195.115.100.3/32	*	221.12.184.0/24	*	*	
défaut	toutes	bloque	toutes	tous	toutes	tous	tous	

Deuxième partie :

1. L'ouverture de connexion TCP est basée sur trois échanges :

SYN // Le client demande la connexion
SYN, ACK // le serveur accepte la connexion
ACK. // La connexion est établie

Ces échanges utilisent les drapeaux (flag) de l'entête TCP. En basculant le bit correspondant au drapeau à 1.
La fermeture d'une connexion est détectée par l'entête TCP "FIN, ACK " envoyée par le client.

Remarque : UDP n'est pas un protocole travaillant en mode connecté, les routeurs essaient cependant d'identifier des séquences d'échange UDP en mettant en "relation" grâce à un temporisateur des échanges comportant le même quadruplet [IP source, Port Source, IP destination, Port Destination].
Des techniques similaires de mise en relation peuvent être utilisées avec ICMP ou FTP qui modifie son port en cours d'échange.

2. Ces nouvelles règles (60 à 63) constitueront la règle de sécurité I.

No de règle	Interface d'arrivée	Action	Adresse Source	Port source	Adresse Destination	Port destination	Protocole	Etat TCP
1 (H)	213.152.47.9	bloque	*	*	*	*	ICMP	
2 (A)	213.152.47.9	accepte	*	*	195.115.100.2/32	*	*	
3 (A)	195.115.100.1	accepte	195.115.100.2/32	*	*	*	*	
11 (B)	192.168.50.1	accepte	192.168.50.0/24	*	195.115.100.0/28	*	*	
21 (C)	195.115.100.1	accepte	195.115.100.0/28	*	192.168.50.10/32	4523	TCP	
22 (C)	195.115.100.1	accepte	195.115.100.3/32	*	192.168.50.10/32	4523	TCP	
31 (D)	195.115.100.1	accepte	195.115.100.2/32	53	192.168.50.11/32	*	TCP	
32 (D)	195.115.100.1	accepte	195.115.100.2/32	25	192.168.50.11/32	*	TCP	
41 (E)	195.115.100.1	accepte	195.115.100.0/28	22	*	*	TCP	
42 (E)	213.152.47.9	accepte	*	*	195.115.100.0/28	22	TCP	

50 (G)	213.152.47.9	bloque	202.10.12.0/24	*	195.115.100.3/32	119	*	
51 (F)	213.152.47.9	accepte	195.83.0.0/24	*	195.115.100.3/32	*	*	
52 (F)	213.152.47.9	accepte	202.10.12.0/24	*	195.115.100.3/32	*	*	
53 (F)	213.152.47.9	accepte	221.12.184.0/24	*	195.115.100.3/32	*	*	
54 (F)	195.115.100..1	accepte	195.115.100.3/32	*	195.83.0.0/24	*	*	
55 (F)	195.115.100..1	accepte	195.115.100.3/32	*	202.10.12.0/24	*	*	
56 (F)	195.115.100..1	accepte	195.115.100.3/32	*	221.12.184.0/24	*	*	
60 (I)	192.168.50.1	accepte	192.168.50.0/24	*	*	80	TCP	
61 (I)	213.152.47.9	accepte	*	80	192.168.50.0/24	*	TCP	établi
62 (I)	192.168.50.1	accepte	192.168.50.0/24	*	*	443	TCP	
63 (I)	213.152.47.9	accepte	*	443	192.168.50.0/24	*	TCP	établi
défaut	toutes	bloque	toutes	tous	toutes	tous	tous	