Filtrage par Liste de Contrôle d'Accès (ACL)

ESIR - TD

2025

1 Objectifs

— Comprendre les mécanismes de filtrage IP.
— Concevoir et mettre en œuvre une politique de filtrage efficace.

1.1 Rappel de méthode

— Posséder une cartographie du réseau à jour.
— Identifier tous les besoins utilisateur et machine en termes d'entrée, de sortie et d'accès.
— Rassembler les machines par groupes ayant les mêmes besoins.
— Schématiser les flux d'entrée/sortie par un tableau à double entrées.
— Toujours réfléchir avec un papier et un crayon plutôt qu'avec un clavier.

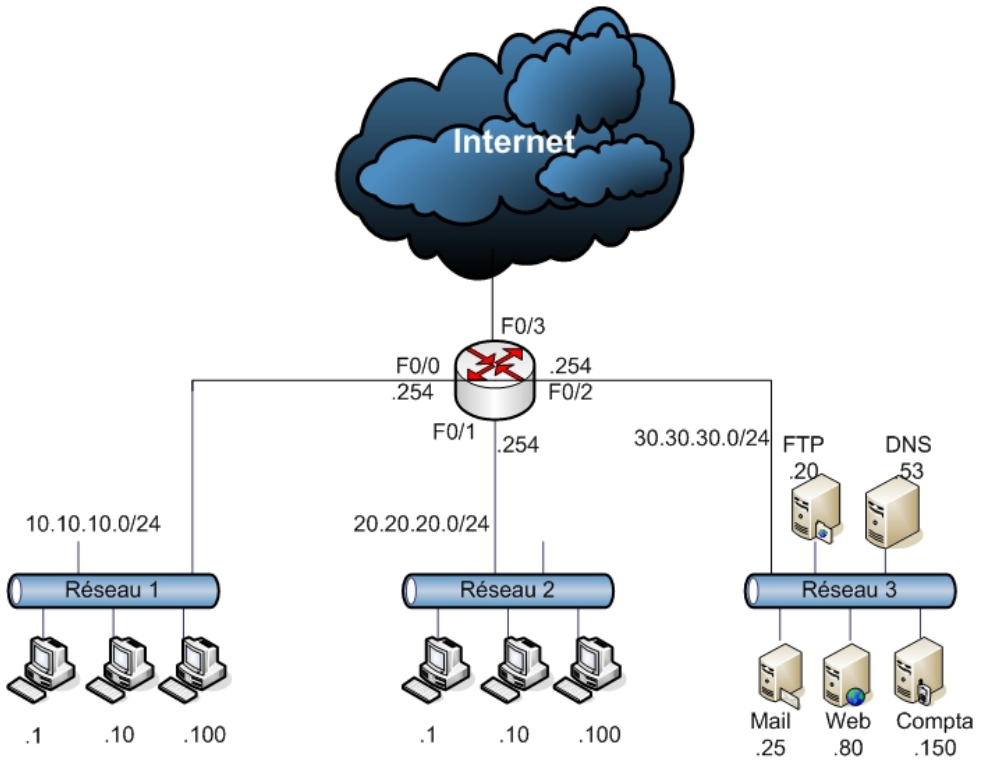
1.2 Rappel de fonctionnement

Deux décisions possibles : `permit` ou `deny`.
Les éléments de décision possibles sont :
— Adresse IP source.
— Adresse IP destination.
— Port Source.
— Port destination.
— Les Flags TCP : SYN, ACK, RST, etc.

Les règles sont évaluées séquentiellement jusqu'à en trouver une qui fonctionne, sinon on applique la politique par défaut (`deny` sur un Cisco).

Exercice 1

Soit la topologie réseau suivante :



1.3 Introduction

En fonction des cahiers des charges suivants :
Question 1 : Tracez sur un schéma les flux d'entrée/sortie.
Question 2 : Composez le tableau de flux puis écrivez les règles de filtrage.

1.4 Cahier des charges 1

— Fermez toutes les communications venant et à destination d'Internet.

1.5 Cahier des charges 2

— Les machines du sous-réseau 1 peuvent contacter le serveur cache DNS de l'entreprise.
— Le serveur DNS de l'entreprise peut consulter d'autres serveurs DNS sur Internet.
— Le sous-réseau 1 peut consulter un service HTTP sur Internet.

1.6 Cahier des charges 3

— Tout le monde a accès au serveur Web de l'entreprise.
— Les machines internes doivent pouvoir envoyer et recevoir du courrier (SMTP, POP3), le serveur de mail est dans le sous-réseau 3.

1.7 Cahier des charges 4

— Le sous-réseau 2 (comptabilité) est le seul à avoir accès au serveur de comptabilité (port 3012).
— Seule la machine de l'administrateur peut se connecter en SSH à tous les serveurs.

1.8 Cahier des charges 5

— Le sous-réseau 1 a accès au serveur FTP.

Question bonus : quelles améliorations pourraient être apportées pour améliorer la sécurité de cette architecture ?

Exercice 2

Contexte : l'entreprise *XYZ* vient de déployer un pare-feu (simpliste) sur son serveur web, mais elle a des doutes sur sa sécurité et son bon fonctionnement. On vous confie le fichier de configuration iptables correspondant. Grâce à vos connaissances en sécurité des réseaux et aux besoins identifiés ci-desssous, trouvez les 5 erreurs de configuration ou éléments manquants.

Les besoins identifiés :

— Autoriser l'accès au serveur web (HTTP, HTTPS, ...) ;
— Autoriser l'accès depuis le serveur à des API hébergés sur le web ;
— Autoriser l'accès SSH depuis la machine 192.168.1.42 ;

Question 1

A faire :

— Analyser le script et trouver les erreurs de configuration.
— Expliquer les risques associés à chaque erreur.
— Bonus : proposer une version sécurisée / fonctionnelle.

Fichier de configuration

```
#!/bin/bash

iptables -F
iptables -X

# Stackoverflow said:
iptables -P INPUT ACCEPT
iptables -P FORWARD ACCEPT
iptables -P OUTPUT ACCEPT

# Administration
iptables -A INPUT -p tcp --dport 22 -j ACCEPT

# Web
iptables -A INPUT -p tcp --dport 80 -j ACCEPT
iptables -A INPUT -p tcp --dport 443 -j ACCEPT

iptables -A OUTPUT -j ACCEPT
```

Bonus : question 2

Après vos retours, le fichier a été modifié et contient désormais l'extrait suivant :

```
#!/bin/bash

iptables -F
iptables -X

iptables -P INPUT DROP
iptables -P FORWARD DROP
iptables -P OUTPUT DROP

iptables -A INPUT -p udp --dport 53 -j ACCEPT
iptables -A INPUT -p tcp --dport 53 -j ACCEPT
```

Questions : cela est-il suffisant pour le fonctionnement attendu ?

2 Annexe

2.1 ACL DIRECTE (ou numérotée)

Commande pour placer une ACL sur une interface :

```
ip access-group {acl number | acl name} {in | out}
```

Commande pour ajouter une règle à une ACL :
`access-list acl_number autres_paramètres`
— `acl_number`
  — `<1-99>` IP standard access list
  — `<100-199>` IP extended access list
  — `<1100-1199>` Extended 48-bit MAC address access list
  — `<200-299>` Protocol type-code access list
  — `<700-799>` 48-bit MAC address access list

Exemple de syntaxe : cette ACL filtre les paquets provenant du réseau 172.16.1.0/24.

```
access-list 1 deny 172.16.1.0 0.0.0.255
```

Note importante : plusieurs règles peuvent s'appliquer sur la même ACL (avec le même *acl_ number*) dans l'ordre où elles sont écrites.

Lien vers la documentation (FR) : `https://www.cisco.com/c/fr_ca/support/docs/security/ios-firewall/23602-confaccesslists.html#toc-hId-1286187984`

2.2 Liste des principaux protocoles et ports associés

— 20 : ftp-data (TCP)
— 21 : ftp (TCP)
— 22 : ssh (TCP)
— 23 : telnet (TCP)
— 25 : smtp (TCP)
— 53 : domain (TCP/UDP)
— 69 : tftp (UDP)
— 80 : http (TCP)
— 110 : pop3 (TCP)
— 443 : https (TCP)