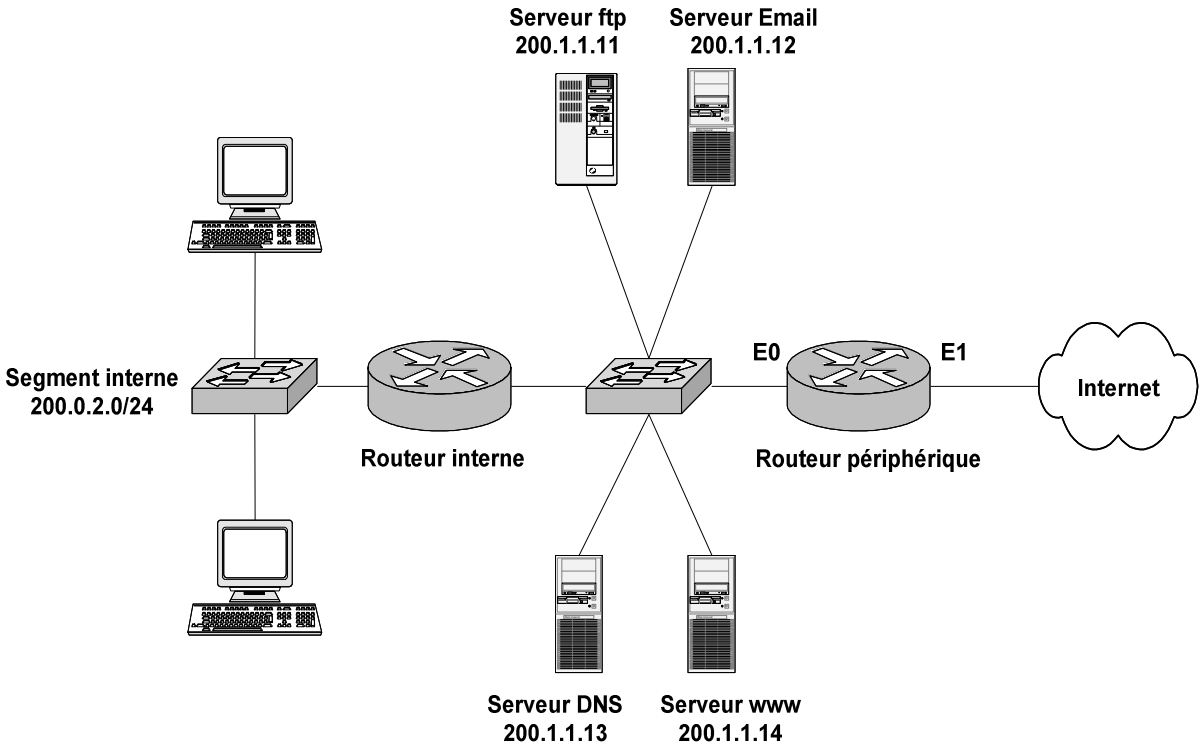
TD n°4
Les listes de contrôle d'accès
(notions avancées)

Exercice 1 *ACLs étendues*



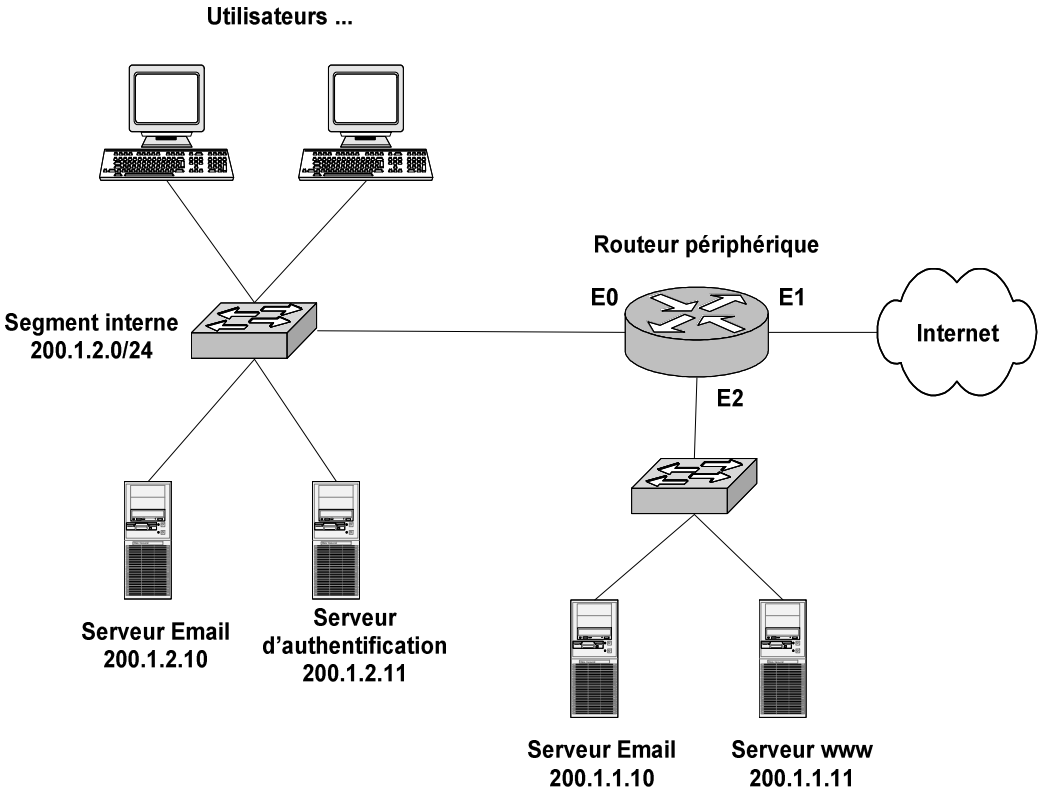
La configuration du routeur périphérique est la suivante :

```
access-list 100 permit tcp any host 200.1.1.14 eq 80                    (1)
access-list 100 permit udp any host 200.1.1.13 eq 53                    (2)
access-list 100 permit tcp any host 200.1.1.12 eq 25                    (3)
access-list 100 permit tcp any eq 25 host 200.1.1.12 established
access-list 100 permit tcp any host 200.1.1.11 eq 21                    (4)
access-list 100 permit tcp any host 200.1.1.11 eq 20                    (5)
access-list 100 permit tcp any eq 80 200.0.2.0 0.0.0.255 established    (6)
access-list 100 permit udp any eq 53 200.0.2.0 0.0.0.255                (7)
access-list 100 deny ip any any                                         (8)

interface Ethernet1
        ip access-group 100 in
```

1. Expliquez le rôle de chacune des lignes

Exercice 2 *ACLs étendues*



Le cahier des charges est le suivant :

- les internautes doivent avoir accès au serveur WEB 200.1.1.11
- les internautes doivent avoir accès au serveur SMTP 200.1.1.10
- le serveur SMTP 200.1.1.10 de la DMZ doit pouvoir transmettre des emails au serveur SMTP interne 200.1.2.10, mais seul ce trafic doit être autorisé de la DMZ vers le réseau interne
- les utilisateurs internes doivent pouvoir envoyer des requêtes DNS
- les utilisateurs internes doivent avoir accès aux deux serveurs de la DMZ
- les utilisateurs internes doivent avoir accès aux services TCP de l'Internet

1. Proposez la rédaction de deux ACLs qui permettent d'obtenir exactement ce fonctionnement :
    - une côté Internet en entrée
    - une en entrée du réseau interne

Exercice 3 *ACL dynamiques*

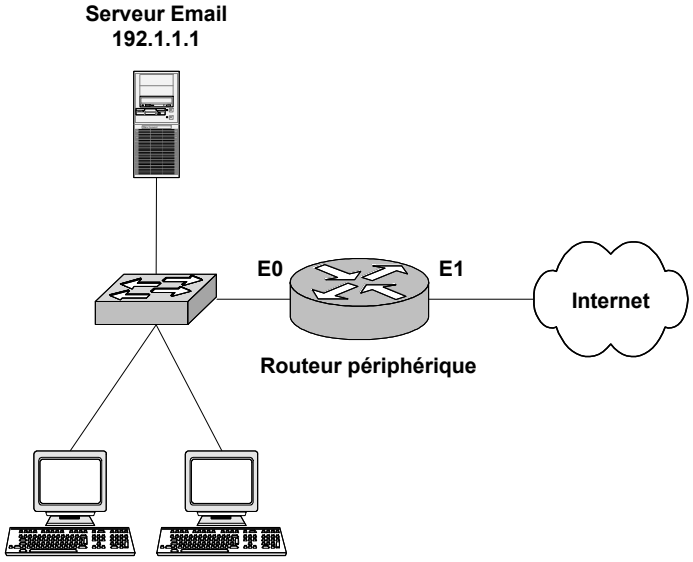
1. Quelle est l'utilité d'une ACL dynamique ?
2. Quel en est le principe de fonctionnement ?
3. Pourquoi ces ACL permettent-elles d'améliorer la sécurité du réseau ?
4. Que doit faire un Internaute malveillant pour « passer au travers » d'une ACL dynamique ?

Exercice 4 *ACL dynamiques*

```
username toto password tutu
interface Serial0
 ip address 172.18.23.2 255.255.255.0
 ip access-group 101 in
access-list 101 dynamic mytestlist timeout 120 permit ip any any
line vty 0
login local
autocommand access-enable timeout 5
```

1. Quels utilisateurs pourront entrer sur le réseau après s'être identifiés ?
2. Un essai montre que le fonctionnement n'est pas satisfaisant. Pouvez-vous proposer une modification ?
3. On désire que l'utilisateur autorisé ne puisse entrer sur le réseau que depuis le poste utilisant l'adresse IP 195.206.51.27. Comment modifiez-vous l'ACL ?
4. La situation de la question 3. est-elle réaliste ?
5. Identifiez les deux principales situations qui permettent à un poste client de sembler avoir une adresse IP publique ?
6. Discutez de l'utilisation des ACL dynamiques dans chaque cas
7. Quels sont les deux moyens de restreindre les adresses IP autorisée à se connecter ?
8. Discutez des avantages des deux stratégies
9. Quelle technique voisine des ACLs dynamiques apporte quelques améliorations ?

Exercice 5 *CBAC*

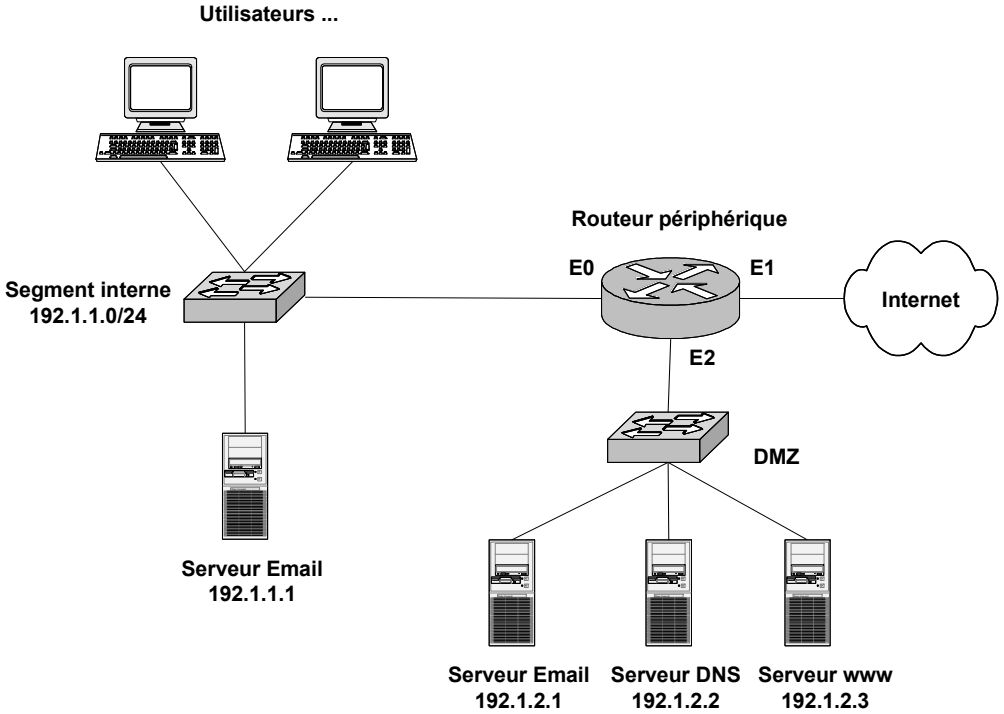


Le cahier des charges est le suivant :

- tous les utilisateurs internes doivent pouvoir utiliser Internet
- le trafic réponse aux requêtes internes doit rentrer
- les internautes doivent pouvoir atteindre le serveur email
- tout le reste doit être interdit

1. Proposez la rédaction d'une ACL qui permette d'obtenir exactement ce fonctionnement

Exercice 6 *CBAC*



La configuration du routeur périphérique est la suivante :

```
Router(config)#ip access-list extended internal_acl
Router(config-ext-nacl)#permit tcp host 192.1.1.1 host 192.1.2.1 eq smtp          (1)
Router(config-ext-nacl)#deny tcp any any eq pop                                   (2)
Router(config-ext-nacl)# deny tcp any any eq smtp                                 (2)
Router(config-ext-nacl)# deny ip host 192.1.1.1 any                               (3)
Router(config-ext-nacl)#permit ip any any                                         (4)
Router(config-ext-nacl)#exit
Router(config)#
Router(config)#ip inspect name internal_CBAC smtp audit-trail on                  (5)
Router(config)#ip inspect name internal_CBAC ftp
Router(config)#ip inspect name internal_CBAC http
Router(config)#ip inspect name internal_CBAC realaudio
Router(config)#ip inspect name internal_CBAC tcp
Router(config)#ip inspect name internal_CBAC udp
Router(config)#ip inspect name internal_CBAC icmp
Router(config)#
Router(config)#ip access-list extended DMZ_ACL
Router(config-ext-nacl)#permit tcp host 192.1.2.1 any eq smtp                     (6)
Router(config-ext-nacl)#permit udp host 192.1.2.2 any eq dns                      (7)
Router(config-ext-nacl)#exit
Router(config)#
Router(config)# ip inspect name DMZ_CBAC smtp audit-trail on                      (8)
Router(config)# ip inspect name DMZ_CBAC http
Router(config)# ip inspect name DMZ_CBAC tcp
Router(config)# ip inspect name DMZ_CBAC udp
Router(config)#
Router(config)# ip access-list extended external_acl
Router(config-ext-nacl)#permit tcp any host 192.1.2.1 eq smtp                     (9)
Router(config-ext-nacl)#permit tcp any host 192.1.2.2 eq dns
Router(config-ext-nacl)#permit tcp any host 192.1.2.3 eq http
Router(config-ext-nacl)#exit
Router(config)#
Router(config)# ip inspect name external_CBAC smtp audit-trail on                 (10)
```

```
Router(config)# ip inspect name external_CBAC ftp
Router(config)# ip inspect name external_CBAC http
Router(config)# ip inspect name external_CBAC realaudio
Router(config)# ip inspect name external_CBAC tcp
Router(config)# ip inspect name external_CBAC udp
Router(config)# ip inspect name external_CBAC icmp
Router(config)#
Router(config)# interface ethernet0                                    (11)
Router(config-if)# descrition internal network
Router(config-if)# ip access-group internal_acl in
Router(config-if)# ip inspect internal_CBAC in
Router(config-if)# exit
Router(config)#
Router(config)# interface ethernet2                                    (12)
Router(config-if)# descrition DMZ
Router(config-if)# ip access-group DMZ_acl in
Router(config-if)# ip inspect DMZ_CBAC in
Router(config-if)# exit
Router(config)#
Router(config)# interface ethernet1                                    (13)
Router(config-if)# descrition external network
Router(config-if)# ip access-group external_acl in
Router(config-if)# exit
Router(config)# ip inspect tcp synwait-time 15                         (14)
Router(config)# ip inspect tcp idle time 120
Router(config)# ip inspect udp idle-time 20
```

1. Expliquez le rôle de chacune des lignes

Exercice 7 *Smurf attack*

Sur un routeur, vous trouvez l'ACL suivante :

```
access-list 100 pemit icmp any any echo
access-list 100 pemit icmp any any echo-reply
access-list 100 pemit ip any any

interface serial0
 ip access-group in
```

1. Quel est l'effet de cette ACL ?

Intrigué, vous lancez la commande ***show access-list 100***, en voici le résultat :

```
Routeur 2500# show access-list 100
        Extended IP access list 100
        pemit icmp any any echo  (13 matches)
        pemit icmp any any echo-reply  (15001 matches)
        pemit ip any any  (105 matches)
```

2. A la lumière de ces informations, pouvez-vous dire à quoi sert l'ACL ?
3. Expliquez le principe d'une attaque de type « smurf » en faisant un schéma.

Réponses

Exercice 1 :

(1) N'importe qui peut atteindre le port TCP 80 du serveur web 200.1.1.14
(2) N'importe qui peut atteindre le port UDP 53 du serveur DNS 200.1.1.13
(3) La première commande autorise n'importe qui à envoyer un email sur le port TCP 25 du serveur SMTP 200.1.1.12.
La deuxième commande autorise le serveur SMTP interne à envoyer des email à l'extérieur et à recevoir les réponses
(4) N'importe qui peut atteindre le port TCP 21 du serveur FTP 200.1.1.11
(5) Permet aux internautes d'utiliser le port FTP DATA (20) du serveur FTP 200.1.1.11.
Remarque : on autorise les connexions sur le port 20, sans vérifier qu'il y a une connexion de contrôle sur le port 21 qui lui correspond. C'est un risque pour la sécurité. Pour éviter cela, il faudrait utiliser le CBAC.
(6) Autorise les réponses des serveurs WWW externes. L'option *established* oblige le routeur à tenir compte des informations de session de TCP.
(7) Autorise les réponses des serveurs DNS externes
(8) Facultatif, permet de voir le nombre de fois que cette ligne est utilisée en faisant *show ip access-list 100*

Exercice 2 :

Il faut 2 ACLs : une côté Internet en entrée, une en entrée du réseau interne

access-list 100 deny ip any 200.1.2.10 0.0.0.1
(1) on interdit tout le trafic Internet d'atteindre le serveur email interne et le serveur d'authentification ; lien avec (5) et (6)
access-list 100 permit tcp any host 200.1.1.11 eq 80
(2) accès au serveur WEB
access-list 100 permit tcp any host 200.1.1.10 eq 25
(3) accès au serveur SMTP
access-list 100 permit tcp any eq 25 host 200.1.1.10 established
(4) autorisation des réponses aux mails envoyés par 200.1.1.10 aux serveurs emails externes
access-list 100 permit tcp any 200.1.2.0 0.0.0.255 established
(5) on laisse passer les réponses aux requêtes des utilisateurs internes (sauf à destination du serveur mail interne et du serveur d'authentification, bloquées par (1))
access-list 100 permit udp any eq 53 200.1.2.0 0.0.0.255
(6) autorise les réponses DNS cers les utilisateurs internes (utile car DNS utilise UDP et n'est donc pas concerné par (5))
access-list 100 deny ip any any

interface ethernet 1
ip access-group 100 in

access-list 101 deny ip any host 200.1.2.11
(7) rien ne passe vers le serveur d'authentification
access-list 101 permit tcp any 200.1.2.0 0.0.0.255 established

(8) on laisse passer les réponses aux requêtes des utilisateurs internes, utile car on coupe le trafic qui pourrait venir de la DMZ

access-list 101 permit udp any eq 53 200.1.2.0 0.0.0.255

(9) on autorise les réponses DNS

access-list 101 permit tcp host 200.1.1.10 host 200.1.2.10 eq 25

(10) autorise le serveur SMTP externe à accéder au serveur SMTP interne

access-list 101 permit tcp host 200.1.1.10 eq 25 host 200.1.2.10 established

(11) autorise le serveur SMTP externe à répondre au serveur SMTP interne

access-list 101 deny ip any any

interface ethernet 0
ip access-group 101 out

Exercice 3 :

1. permet de résoudre le pb de l'authentification
2. avant de se voir autoriser l'accès par ajout d'une instruction dans l'ACL d'entrée, l'utilisateur doit fournir un identifiant et un mdp
3. elles permettent d'identifier l'utilisateur lui-même, et pas seulement son adresse IP
4. il doit connaître un nom d'utilisateur et un mdp valide, par exemple en observant le paquet qui les contient à l'ouverture de la session par le bon utilisateur. Il faut donc prendre la précaution de crypter ces données pour la transmission

Exercice 4 :

1. a priori, tous ceux qui se sont authentifiés
2. l'entrée dynamique est la seule :
   - l'ACL est vide tant que l'utilisateur ne s'est pas authentifié
   - l'unique entrée est donc le *deny any any* par défaut
   - or pour s'authentifier, il doit faire un *telnet* sur le routeur
   - l'identification est impossible (session telnet interdite), l'ACL dynamique ne servira jamais
   - en fait, rien ne peut entrer sur ce réseau
   - il faut autoriser l'accès telnet :
     access-list 101 permit tcp any host 172.18.23.2 eq telnet
3. *access-list 101 permit tcp host 195.206.51.27 host 172.18.23.2 eq telnet*
4. utilisateur a rarement une adresse IP publique a lui, cette situation est assez peu réaliste
5. connexion depuis l'intérieur d'un réseau d'entreprise : l'utilisateur a une adresse IP privée, et cette adresse est translatée par le firewall sur une adresse publique. L'adresse publique visible est donc celle utilisée par le firewall, ce n'est pas forcément toujours la même, mais elle appartient à un pool d'adresses qui lui est toujours le même.
   connexion depuis le domicile : c'est le fournisseur d'accès qui attribue à l'utilisateur une adresse publique par DHCP. Cette adresse est considérée comme aléatoire
6. Dans le premier cas, on peut utiliser les ACLs dynamiques, mais l'utilisateur pourra être identifié, mais on est obligés d'accepter toutes les adresses IP que le firewall utilise pour la translation
   Dans le second cas, l'utilisation des ACLs dynamiques est impossible
7. première méthode : en filtrant l'accès telnet dans la partie fixe de l'ACL

deuxième méthode : en filtrant dans l'unique entrée dynamique de l'ACL

8. première méthode : on peut autoriser n'importe quels groupes d'adresses IP, mais l'entrée dynamique est alors du style :
   access-list 101 dynamic mytestlist timeout 120 permit ip any any
   Cela rend le réseau vulnérable pendant que cette instruction est utilisée !
   Deuxième méthode : la vulnérabilité est limitée au champ des adresses IP autorisées, mais ce champ n'est défini que par l'unique entrée dynamique de l'ACL.
9. c'est le proxy d'authentification :
   - l'authentification telnet est remplacée par un serveur http
   - l'authentification se fera obligatoirement par un serveur déporté (Radius)
   - plusieurs entrées dynamiques peuvent être ajoutées

Exercice 5 :

```
Router(config)#ip access-list extended external_acl
Router(config-ext-nacl)#permit tcp any host 192.1.1.1 eq smtp
Router(config-ext-nacl)#deny ip any any
Router(config-ext-nacl)#exit
Router(config)#ip inspect name CBAC smtp
Router(config)#ip inspect name CBAC tftp
Router(config)#ip inspect name CBAC ftp
Router(config)#ip inspect name CBAC http
Router(config)#ip inspect name CBAC realaudio
Router(config)#ip inspect name CBAC tcp
Router(config)#ip inspect name CBAC udp
Router(config)#ip inspect name CBAC icmp
Router(config)#ip inspect tcp idle-time 300
Router(config)#interface ethernet 1
Router(config-if)#ip inspect CBAC out
Router(config-if)#ip access-group external_acl in
```

Exercice 6

Voir le cours et les autres exercices !

Exercice 7

1. Cette ACL n'a aucun effet sur le flux IP, ce qui ne veut pas dire qu'elle ne sert à rien !
2. On peut voir que le routeur a envoyé 13 demandes d'echo ping, mais qu'il en a reçu 15001 ! Ce n'est pas normal, il aurait du en recevoir à peu près le nombre qu'il a demandé.
   Dans ce cas, l'ACL est utilisée comme sonde de mesure sur un type de flux particulier. On utilise cette technique pour vérifier un flux, quand on a des soupçons d'attaque particulière.
3. un hacker envoie une demande d'echo ping vers un broadcast réseau, en utilisant une @IP source fausse : celle de sa cible. Toutes les machines du réseau destination vont répondre à la machine source en même temps, provoquant un déni de service par afflux trop important de message vers cette machine