INF4420a: Sécurité Informatique

Exercices : Sécurité Réseau Partie 1

POLYTECHNIQUE MONTRÉAL
UNIVERSITÉ D'INGÉNIERIE

Exercice de réseau

- Exercice 1 : Configuration du pare-feu d'une petite entreprise

- Objectif :
  - Savoir définir une architecture de sécurité réseau pour une petite entreprise
  - Savoir configurer un pare-feu à état conformément à une politique de filtrage réseau

POLYTECHNIQUE MONTRÉAL
UNIVERSITÉ D'INGÉNIERIE

Exercice de réseau

- Exercice 1 : Configuration du pare-feu d'une petite entreprise
- La petite entreprise YLOP.com a déployé, sur son réseau privé 192.168.0.0/16, plusieurs serveurs
  - 3 serveurs FTP (port TCP 21) (192.168.1.1, 192.168.2.1, 192.168.3.1)
  - 3 serveurs WEB (port TCP 80) (192.168.1.2, 192.168.2.2, 192.168.3.2)
  - 3 serveurs DNS (port UDP 53) (192.168.1.3, 192.168.2.3, 192.168.3.3)
- Il y a environ 100 employés dans l'entreprise YLOP.com qui ont leurs adresses de 192.168.4.1 à 192.168.4.254

POLYTECHNIQUE MONTRÉAL
UNIVERSITÉ D'INGÉNIERIE

Exercice de réseau

- Exercice 1 : Configuration du pare-feu d'une petite entreprise

- L'entreprise YLOP.com a acheté une plage d'adresses publiques sur Internet
  - 195.55.55.0/29
- Vous venez d'être embauché en tant qu'administrateur de sécurité dans l'entreprise YLOP.com
- Vous avez en charge de proposer et configurer une architecture de sécurité pour l'entreprise YLOP.com

POLYTECHNIQUE MONTRÉAL
UNIVERSITÉ D'INGÉNIERIE

Exercice de réseau

- On vous demande d'écrire la table de port forwarding qui fera la liaison entre le réseau privé et Internet

- Question 1 : Est-ce que ce déploiement est possible ?
  - Oui
  - Non

Exercice de réseau

- Réponse question 1 : La réponse est oui !
  - Les adresses publiques demandées : 195.55.55.0/29

    /29 : 11111111. 11111111.11111111.11111000
  - deux adresses de ce sous-réseau sont réservées au sous-réseau lui-même et au broadcast et ne pouvant pas être utilisées pour numéroter une interface
  - $2^3 - 2 = 6$
  - Avec du NAT on va pouvoir assurer le déploiement !

Exercice de réseau

- Question 2 : Si la réponse est oui à la question 1, proposez votre solution de NAT dynamique et de port forwarding ?

Exercice de réseau

- Réponse question 2 :

IP publique	Port public	IP privée	Port Privé
195.55.55.1	21	192.168.1.1	21
195.55.55.1	80	192.168.1.2	80
195.55.55.1	53	192.168.1.3	53
195.55.55.2	21	192.168.2.1	21
195.55.55.2	80	192.168.2.2	80
195.55.55.2	53	192.168.2.3	53
195.55.55.3	21	192.168.3.1	21
195.55.55.3	80	192.168.3.2	80
195.55.55.3	53	192.168.3.3	53
195.55.55.1	> 1024 (PAT)	192.168.4.0/24	> 1024

POLYTECHNIQUE MONTRÉAL
UNIVERSITÉ D'INGÉNIERIE

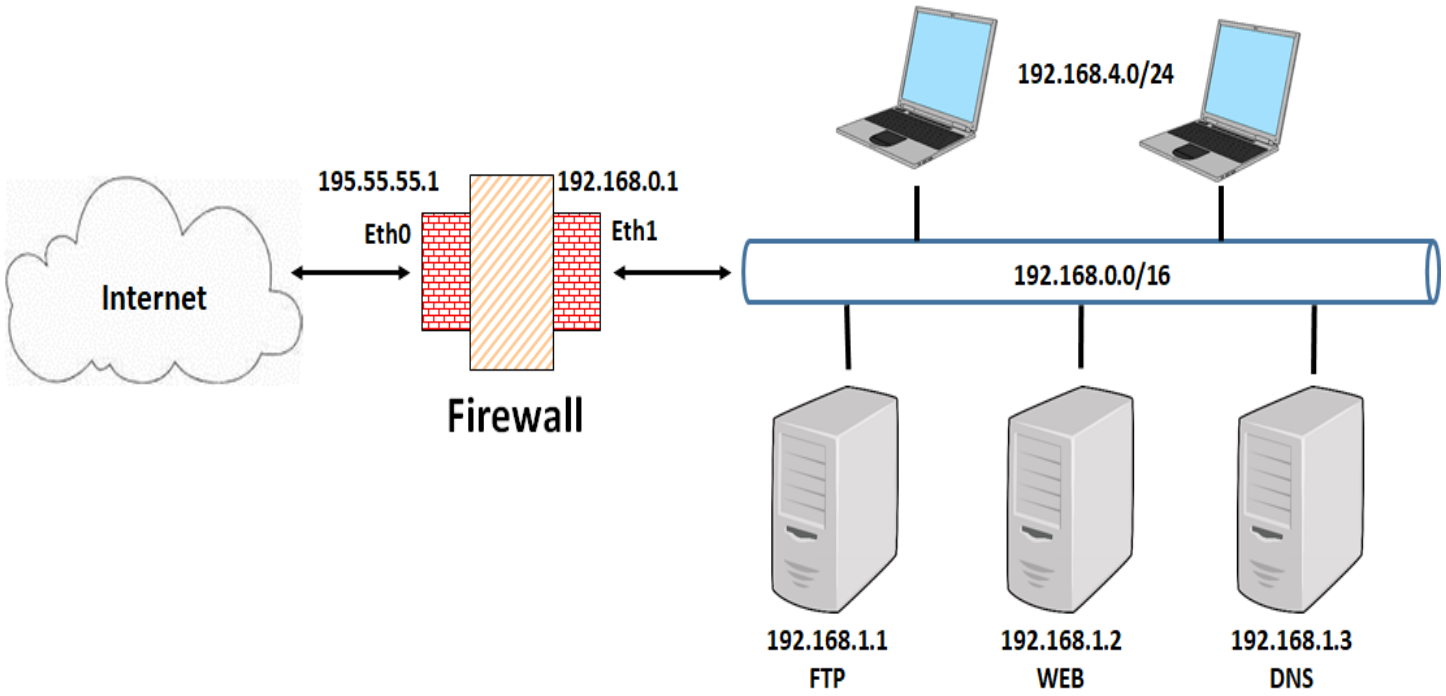
Exercice de réseau

- Sur son site de Montréal (adresse publique 195.55.55.1), l'entreprise YLOP.com a déployé
  - Les 3 serveurs d'adresses 192.168.1.1 (FTP), 192.168.1.2 (WEB) et 192.168.1.3 (DNS)
  - Les 100 employés (EMP)

- Pour assurer la sécurité du site de Montréal, YLOP.com a déployé un pare-feu Netfilter

Exercice de réseau

- Voici l'architecture de sécurité qui a été déployée chez YLOP.com



POLYTECHNIQUE MONTRÉAL
UNIVERSITÉ D'INGÉNIERIE

Exercice de réseau

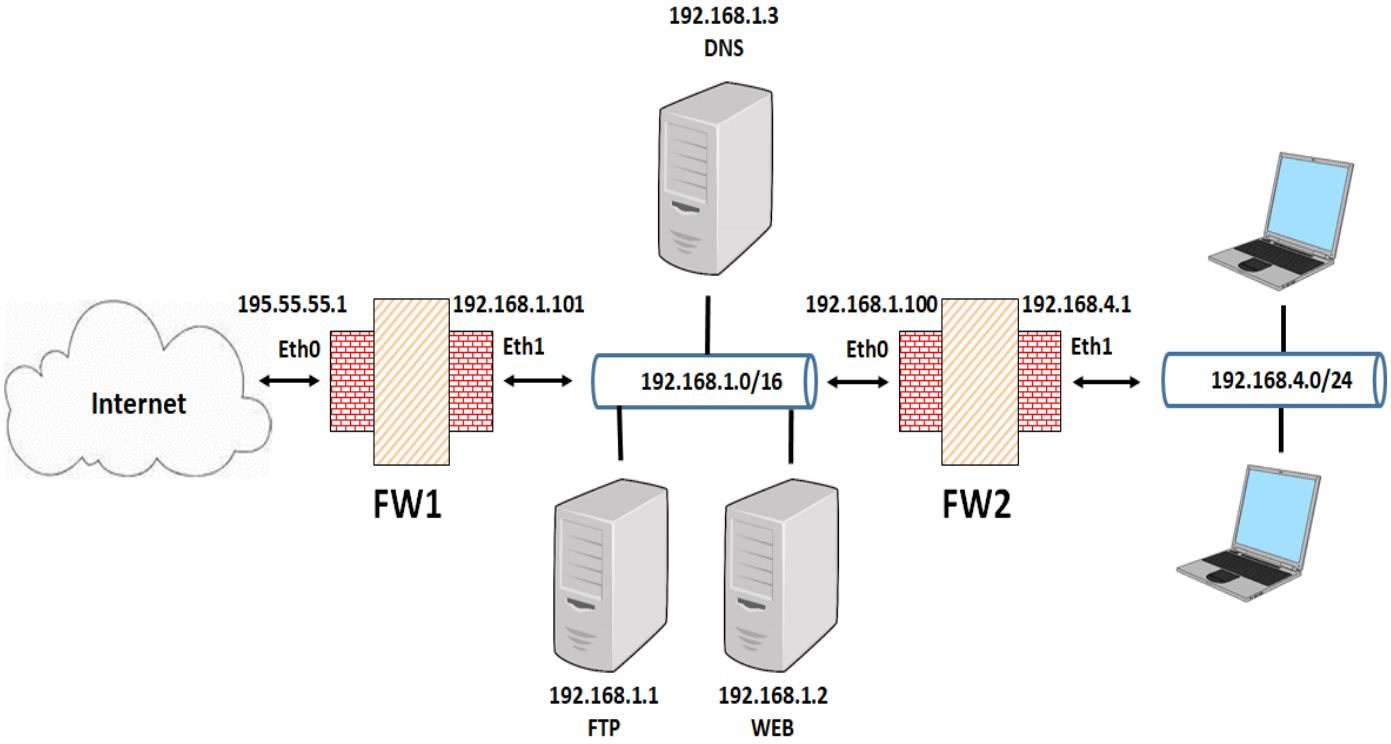
- Question 3 : Quelles recommandations faites-vous à YLOP.com pour améliorer cette architecture de sécurité ?

Exercice de réseau

- Réponse question 3 :
  - Vous proposez de créer une DMZ pour séparer les trois serveurs (WEB, FTP et DNS) du réseau privé des utilisateurs
  - Vous recommandez de changer l'architecture de sécurité :
    - Soit en achetant un deuxième pare-feu
    - Soit en ajoutant une troisième interface au pare-feu déjà existant

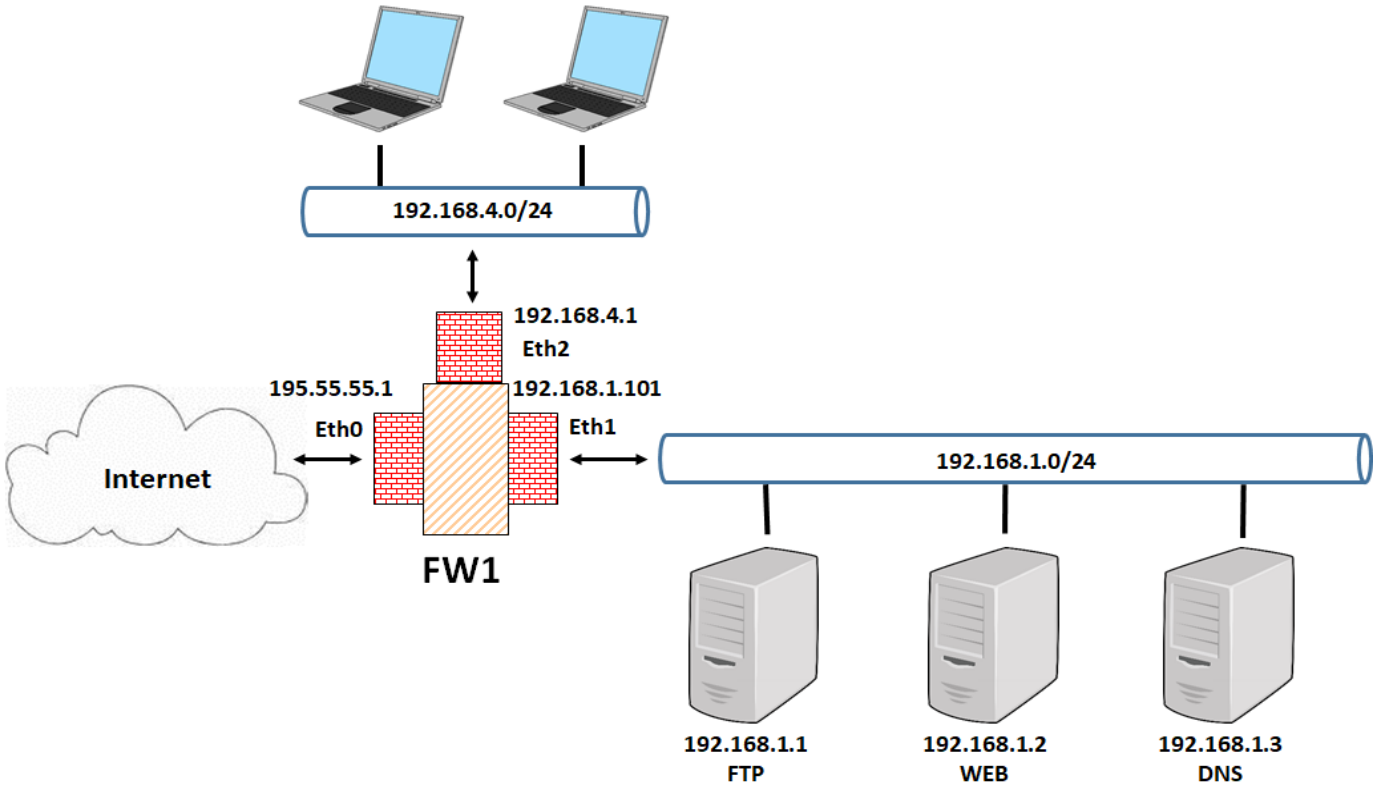
Exercice de réseau

- Réponse question 3 :
  - Solution 1 : Création d'une DMZ avec deux pare-feux



Exercice de réseau

- Réponse question 3 :
  - Solution 2 : Création d'une DMZ avec un seul pare-feu équipé de 3 interfaces réseau



POLYTECHNIQUE MONTRÉAL
UNIVERSITÉ D'INGÉNIERIE

Exercice de réseau

- Vous recommandez à votre direction la solution 1 avec deux pare-feux

- Question 4 : Pourquoi ?

Exercice de réseau

- Réponse question 4 :
- L'architecture avec deux firewalls est plus sécurisée
  - Si le FW1 tombe, l'attaquant devra ensuite attaquer le FW2 pour accéder au réseau privé
  - C'est encore mieux si on assure en plus une diversification fonctionnelle au niveau de ces 2 firewalls.
  - Performance ?
- Dans l'architecture avec 1 seul firewall
  - Si le firewall tombe, l'attaquant a accès à l'ensemble du réseau de l'entreprise (DMZ + réseau privé)
  - La configuration est moins aisée, plus de règles

Exercice de réseau

- En raison de restrictions budgétaires, c'est finalement la solution 2 avec un seul pare-feu et trois interfaces réseau qui est retenue

POLYTECHNIQUE MONTRÉAL
UNIVERSITÉ D'INGÉNIERIE

Exercice de réseau

- Vous avez maintenant la charge de corriger / mettre à jour la configuration de ce pare-feu conformément à la politique de filtrage suivante :
  - Les serveurs FTP, WEB et DNS doivent être accessibles depuis Internet
  - Les employés EMP doivent pouvoir accéder à Internet
  - Les employés EMP doivent pouvoir accéder aux serveurs de la DMZ
  - Les serveurs de la DMZ ne peuvent pas initier de sessions avec les employés EMP mais seulement répondre à leur requête.

POLYTECHNIQUE MONTRÉAL
UNIVERSITÉ D'INGÉNIERIE

Exercice de réseau

- Ancienne config

```
# set default closed policy
iptables -P INPUT DROP
iptables -P OUTPUT DROP
iptables -P FORWARD DROP

# network interfaces
EXTIF=eth0
INTIF=eth1
# addresses
EXTIP=195.55.55.1
FTP_SERVER=192.168.1.1
WEB_SERVER=192.168.1.2
DNS_SERVER=192.168.1.3
EMP_HOST=192.168.4.0/16

# accept packets on the local interface
iptables -A INPUT -i lo -j ACCEPT
iptables -A OUTPUT -o lo -j ACCEPT
```

Exercice de réseau

- Ancienne config

```
# the FTP server must be accessible from Internet
iptables -A FORWARD -i $EXTIF -o $INTIF -p tcp –d $FTP_SERVER --dport 21 -j ACCEPT

# the web server must be accessible from Internet
iptables -A FORWARD -i $EXTIF -o $INTIF -p tcp –d $WEB_SERVER --dport 80 -j ACCEPT

# the dns server must be accessible from Internet
iptables -A FORWARD -i $EXTIF -o $INTIF -p udp –d $DNS_SERVER --dport 53 -j ACCEPT
```

Exercice de réseau

- Ancienne config

```
# enable SNAT (MASQUERADE) functionality on External interface
iptables -t nat -A POSTROUTING -o $EXTIF -j MASQUERADE

# EMP must be able to access Internet
iptables -A FORWARD -i $INTIF -o $EXTIF –s $EMP_HOST –dport 80 -j ACCEPT
iptables -A FORWARD -i $INTIF -o $EXTIF –s $EMP_HOST –dport 443 -j ACCEPT
```

Exercice de réseau

- Question 5 : Corriger et mettre à jour la configuration du pare-feu conformément à l'architecture retenue et à la politique de filtrage

Exercice de réseau

- Réponse question 5 : nouvelle config (page 1)

```
# set default closed policy
iptables -P INPUT DROP
iptables -P OUTPUT DROP
iptables -P FORWARD DROP

# network interfaces
EXTIF=eth0
DMZIF=eth1
INTIF=eth2
# addresses
EXTIP=195.55.55.1
FTP_SERVER=192.168.1.1
WEB_SERVER=192.168.1.2
DNS_SERVER=192.168.1.3
EMP_HOST=192.168.4.0/24

# accept packets on the local interface
iptables -A INPUT -i lo -j ACCEPT
iptables -A OUTPUT -o lo -j ACCEPT
```

Exercice de réseau

- Réponse question 5 : nouvelle config (page 2)

```
# enable DNAT port translation from Internet to FTP server
iptables -t nat -A PREROUTING -i $EXTIF -p tcp –d --dport 21 -j DNAT --to-destination $FTP_SERVER:21

# enable DNAT port translation from Internet to web server
iptables -t nat -A PREROUTING -i $EXTIF -p tcp --dport 80 -j DNAT --to-destination $WEB_SERVER:80

# enable DNAT port translation from Internet to dns server
iptables -t nat -A PREROUTING -i $EXTIF -p udp --dport 53 -j DNAT --to-destination $DNS_SERVER:53

# the FTP server must be accessible from Internet
iptables -A FORWARD -i $EXTIF -o $DMZIF -p tcp --dport 21 -m state --state NEW, ESTABLISHED -j ACCEPT

# the web server must be accessible from Internet
iptables -A FORWARD -i $EXTIF -o $DMZIF -p tcp --dport 80 -m state --state NEW, ESTABLISHED -j ACCEPT

# the dns server must be accessible from Internet
iptables -A FORWARD -i $EXTIF -o $DMZIF -p udp --dport 53 -m state --state NEW, RELATED -j ACCEPT
```

Exercice de réseau

- Réponse question 5 : nouvelle config (page 3)

```
# enable SNAT (MASQUERADE) functionality on External interface
iptables -t nat -A POSTROUTING -o $EXTIF -j MASQUERADE

# EMP must be able to access Internet
iptables -A FORWARD -i $INTIF -o $EXTIF –s $EMP_HOST –dport 80 -m state --state NEW,ESTABLISHED -j ACCEPT
iptables -A FORWARD -i $INTIF -o $EXTIF –s $EMP_HOST –dport 443 -m state --state NEW,ESTABLISHED -j ACCEPT
```

443 === https

Exercice de réseau

- Réponse question 5 : nouvelle config (page 4)

```
# EMP must be able to access the DMZ
iptables -A FORWARD -i $INTIF -o $DMZIF –s $EMP_HOST –dport 80 -m state --state NEW,ESTABLISHED -j ACCEPT
iptables -A FORWARD -i $INTIF -o $DMZIF –s $EMP_HOST –dport 21 -m state --state RELATED -j ACCEPT
iptables -A FORWARD -i $INTIF -o $DMZIF –s $EMP_HOST –dport 53 -m state --state RELATED -j ACCEPT
```

Exercice de réseau

- Question 6 : Que devient la règle de la politique :
  - Les serveurs de la DMZ ne peuvent pas initier de sessions avec les employés EMP mais seulement répondre à leur requête

Exercice de réseau

- Réponse question 6 :
  - On pourrait ajouter la règle :

iptables -A FORWARD -i $DMZIF -o $INTIF -m state --state NEW –j DROP

  - Mais, c'est inutile car nous avons supposé que la politique était fermée par défaut
  - Tout ce qui n'est pas explicitement permis est implicitement interdit