POLYTECHNIQUE
MONTRÉAL

UNIVERSITÉ
D'INGÉNIERIE

INF4420a: Sécurité Informatique

Exercices 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

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 22) (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

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

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

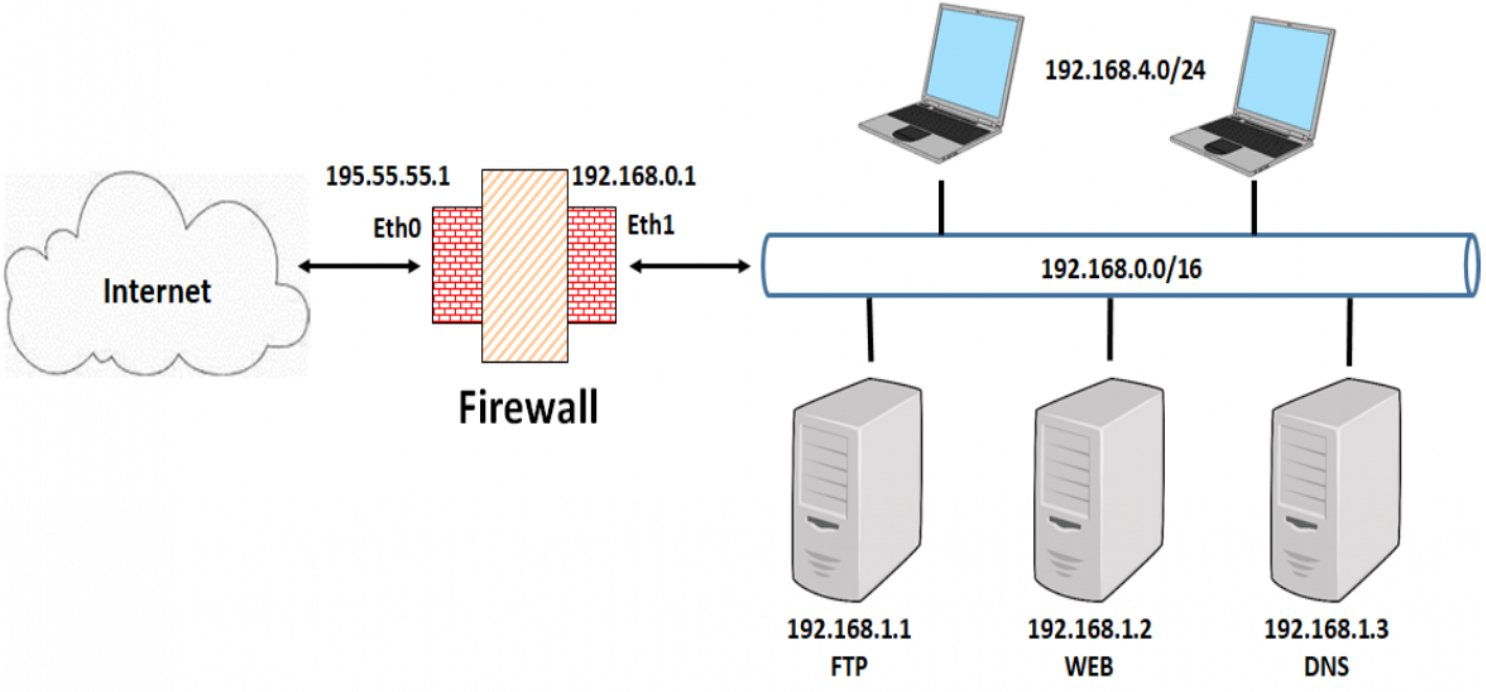
Exercice de réseau

- 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



Exercice de réseau

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

Exercice de réseau

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

- Question 4 : Pourquoi ?

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.

Exercice de réseau

- Ancienne config (page 1)

```
# 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 (page 2)

```
# 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 (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 -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

- 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