TP 8.1

ÉTUDE D'UN FIREWALL

OBJECTIFS

- Comprendre le fonctionnement d'un firewall et d'une DMZ ;
- Étudier les règles de filtrage et de translation entre réseaux privées et public.

PRÉ-REQUIS

- Système d'exploitation Linux, commandes de base.
- Protocoles TCP/IP.
- Principes de base du filtrage et de la translation d'adresse et de port.

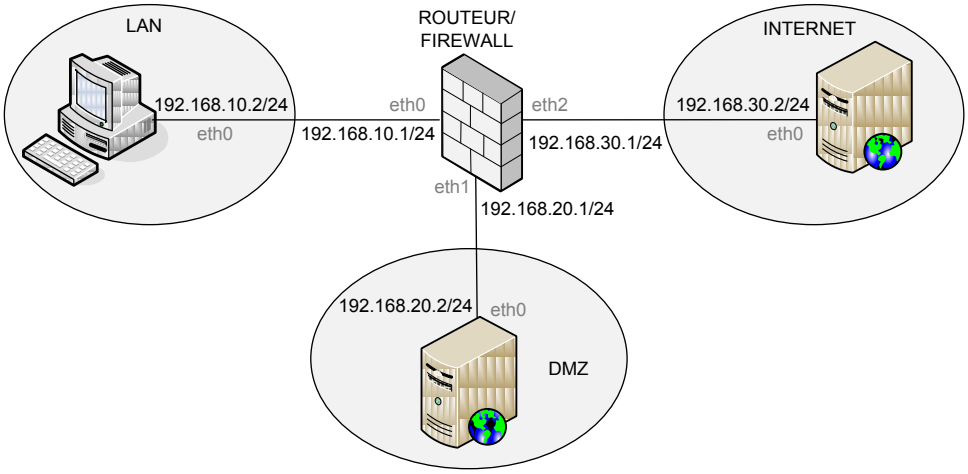
CONTEXTE

Vous devez disposer d'un PC possédant une distribution Linux (sur une partition spécifique, sur une clé USB *bootable* ou encore à l'aide d'un logiciel de virtualisation du type *VMware* ou *VirtualBox*). Le logiciel *wireshark* doit être installé sur votre système, le logiciel de virtualisation *Netkit* doit être installé sur la machine Linux.

a) Cahier des charges

L'objectif est de configurer un firewall permettant à une entreprise de filtrer les accès vers son réseau privé et de rendre accessible à partir d'Internet un serveur

web placé sur une zone neutre de type DMZ. Les adresses du réseau privé et du serveur web seront masquées. Le firewall utilisé fonctionne sous Linux avec les règles de filtrage *iptables*.
Pour simplifier, le réseau local privé est représenté par la machine LAN. L'extérieur est représenté par la machine INTERNET et le serveur web par la machine DMZ. L'accès entre les différentes machines est géré par le FIREWALL. Le schéma suivant présente l'architecture du réseau avec le plan d'adressage :



Le firewall doit répondre aux consignes suivantes :

- il autorise l'accès vers un serveur web d'Internet à partir du LAN ;
- il doit permettre le *ping* d'une machine vers une machine d'Internet (message *echo request*) ;
- il doit accepter en retour la réponse du *ping* (*echo reply*) ;
- il ne doit pas autoriser une demande de connexion à partir d'une machine venant d'Internet ;
- les machines du LAN ne doivent pas être visibles d'Internet ;
- les machines du LAN doivent pouvoir accéder au serveur web de l'entreprise localisé dans la DMZ ;
- une machine d'Internet doit pouvoir accéder au serveur web de la DMZ mais l'adresse de ce dernier doit être masquée de l'extérieur.

b) Mise en œuvre du routage sans sécurité

Le but de cette partie est de réaliser l'interconnexion des quatre machines en configurant leurs interfaces Ethernet, en activant le routage IP sur la machine FIREWALL et en configurant les tables de routage des machines sans contrôler les accès (pas de règle de filtrage particulière).

- Dans votre répertoire de travail, exécutez les commandes suivantes pour créer les quatre machines virtuelles sous *Netkit* et connecter les interfaces :

```
vstart LAN --eth0=A
vstart DMZ --eth0=B
vstart INTERNET --eth0=C
vstart FIREWALL --eth0=A -eth1=B -eth2=C
```

- Attribuez aux machines les adresses IP suivant votre plan d'adressage avec les masques adéquats (commande *ifconfig*). Dans la table de routage de chaque machine, rajoutez les lignes nécessaires (commande *route add*).
- Vérifiez à l'aide de la commande *ping* sur les que vous pouvez accéder de n'importe quelle machine à toutes les autres machines.
- Vérifiez sur la machine DMZ que le serveur web est opérationnel (commande */etc/init.d/apache2 restart*).
- À partir de la machine LAN, ouvrez un navigateur (éventuellement *lynx* en mode console) et connectez-vous au serveur web pour vérifier son fonctionnement.

c) Configuration par défaut du firewall

La commande *iptables* sous Linux permet de définir les règles de filtrage des flux en entrée ou en sortie sur le routeur/firewall (beaucoup de tutoriaux sur *iptables* existent sur Internet). Cette commande utilise trois chaînes :

- INPUT pour les paquets reçus sur une interface ;
- OUTPUT pour les paquets qui sont générés localement et qui sortent d'une interface ;
- FORWARD pour les paquets qui entrent par une interface et qui sortent par une autre.

Pour chaque chaîne, deux traitements sont possibles pour les paquets : ACCEPT ou DROP.

Quelques commandes de base :

- Pour afficher l'état courant du firewall : *iptables -L*
- Pour supprimer toutes les règles du firewall (sauf les règles par défaut) : *iptables -F*

- Pour définir la politique par défaut : *iptables -P regle -i interface option*
  Exemple : *iptables -P INPUT -i eth0 DROP* pour interdire par défaut tout flux en entrée sur l'interface ethernet numéro 0.
- Pour ajouter une nouvelle règle au firewall :

```
iptables -A regle -i interface -s @reseau/préfixe -d
@reseau/préfixe -p protocole -j option
```

Exemples

```
iptables -A INPUT -i eth0 -s 192.168.10.0/24 -d 192.168.20.0/24 80 -p
tcp -j ACCEPT
```

Cette commande accepte les flux en entrée de l'interface eth0 pour un flux venant du réseau IP source 192.168.10.0 avec le masque 255.255.255.0 (24 bits à "1") vers le réseau destination 192.168.20.0 et le port 80 pour le protocole TCP.

```
iptables -A FORWARD -s 192.168.10.0/24 -d 192.168.20.0/24 80 -p tcp
-j ACCEPT
```

Cette commande accepte le routage entre les réseaux IP 192.168.10.0 et 192.168.20.0 vers le port 80 pour le protocole TCP.

- Réalisez une configuration par défaut du firewall qui rejette tout flux dans les chaînes INPUT, OUTPUT et FORWARD (commande *iptables -P*). Vous pouvez utiliser un fichier script pour éviter d'avoir à saisir plusieurs fois les commandes.
- Vérifiez maintenant à l'aide de *pings* que les trois machines (LAN ,INTERNET et DMZ) ne peuvent plus communiquer.

d) Autorisation des *pings*

Le but de cette partie est de rajouter les règles sur le firewall pour autoriser les *pings* du LAN vers la DMZ.

- Ajoutez les règles de filtrage permettant d'accepter sur l'interface du firewall coté LAN un *ping* venant du LAN. Donnez les règles ajoutées.
- Exécutez votre script. Faites un *ping* à partir du PC LAN vers l'interface 192.168.10.1 et vérifiez que cela fonctionne.
- De la même façon ajoutez et testez les filtres pour autoriser les *pings* entre la DMZ et le firewall.

- Quelle chaîne devez vous modifier pour pouvoir pinger la DMZ à partir du LAN ? Effectuez la modification et testez.

e) Translation d'adresse

Le but de cette partie est de réaliser une translation pour toutes les adresses venant du LAN et allant vers la DMZ.

Dans le programme *iptables*, la table « *nat* » est utilisée pour les translations d'adresses. Comme pour le filtrage, cette table utilise trois chaînes :

- PREROUTING pour faire du DNAT (*Destination NAT*), la translation est réalisée sur l'adresse de destination avant le processus de routage. Exemple : pour un paquet entrant vers un serveur web interne et masqué, le routeur va remplacer sa propre adresse IP par l'adresse du serveur web.
- POSTROUTING utilisée à la sortie du routeur pour faire du SNAT (*Source NAT*), l'adresse source est masquée après le processus de routage. Exemple : un ordinateur local veut sortir sur Internet, le routeur va remplacer l'adresse IP du paquet émis en local par sa propre adresse.
- OUTPUT pour les paquets qui sont générés localement et qui sortent d'une interface.

Pour les deux premières chaînes, le traitement permettant de faire du masquage est noté MASQUERADE.

Exemple

```
iptables -t nat -A POSTROUTING -s 10.2.0.0/16 -d 10.3.0.0/16 -o eth2
-j MASQUERADE
```

Cette commande ajoute une règle dans la table de translation d'adresses *nat* du routeur qui opère après la décision de routage (*postrouting*) et qui masque (*masquerade*) le trafic provenant du réseau 10.2.0.0 et à destination du réseau 10.3.0.0. Ce dernier voit le trafic sortant de l'interface eth2 comme provenant uniquement du routeur.

- Ajoutez une règle sur le *firewall* permettant de faire de la translation d'adresse entre le PC LAN et la DMZ. Donnez la règle ajoutée et justifiez les options choisies (chaîne utilisée, *prerouting* ou *post routing*, politique *masquerade*…).
- Exécutez votre script.
- Sur DMZ, exécutez la commande *tcpdump –i eth1* pour réaliser une capture de trames. Sur LAN, tapez la commande *ping 192.168.20.2* .
- Donnez la séquence des trames obtenue sur DMZ avant et après la mise en place de la translation. Interprétez les résultats obtenus.

On souhaite maintenant permettre l'accès au serveur web de la DMZ pour les machines du LAN.

- Proposez les règles de filtrage pour la chaîne FORWARD permettant une connexion du LAN à destination du serveur web, sur son port d'écoute.
- Testez à l'aide d'un navigateur sur LAN que l'accès au serveur web fonctionne.

f) Filtrage entre LAN et INTERNET

Les machines du LAN ne doivent pas être directement visibles de l'Internet.

- Ajoutez les règles de filtrage pour accepter un *ping* et un accès à un serveur web situé sur internet. On réalisera une translation d'adresse pour toute machine ayant comme adresse source le réseau LAN et comme réseau destination le réseau INTERNET. Vérifiez les accès et la translation.

g) Filtrage entre DMZ et INTERNET

Le serveur web de la DMZ doit être accessible à partir de la machine INTERNET mais pas directement avec l'adresse192.168.20.2. À partir de la machine INTERNET, seule une connexion avec come URL : http://192.168.30.1 doit fonctionner. Pour cela, il faut mettre en place une translation d'adresse du réseau DMZ vers le réseau INTERNET et un *forwarding* de port pour que toute connexion HTTP venant d'INTERNET vers la machine 192.168.30.1 soit redirigée vers la machine 192.168.20.2, sur le port d'écoute du serveur web de la DMZ.

- Ajoutez les règles de filtrage *iptables* nécessaires pour réaliser la translation d'adresse et le *forwarding* de port (vous justifierez les options choisies : *prerouting* ou *post routing*, SNAT ou DNAT…).
- Testez la configuration sur la machine INTERNET avec un navigateur sur http://192.168.30.1.
- Analysez avec *tcpdump* les trames obtenues lors de la connexion http précédente sur le pc DMZ.