Composants fodamentaux d'une archi sécurisée

12 décembre 2018

Cet examen dure 1h00. Les documents ne sont pas autorisés. Le barème est donné à titre indicatif.

---

1 Firewall

Question 1.1 (7 points)

Quelques lignes de /etc/services

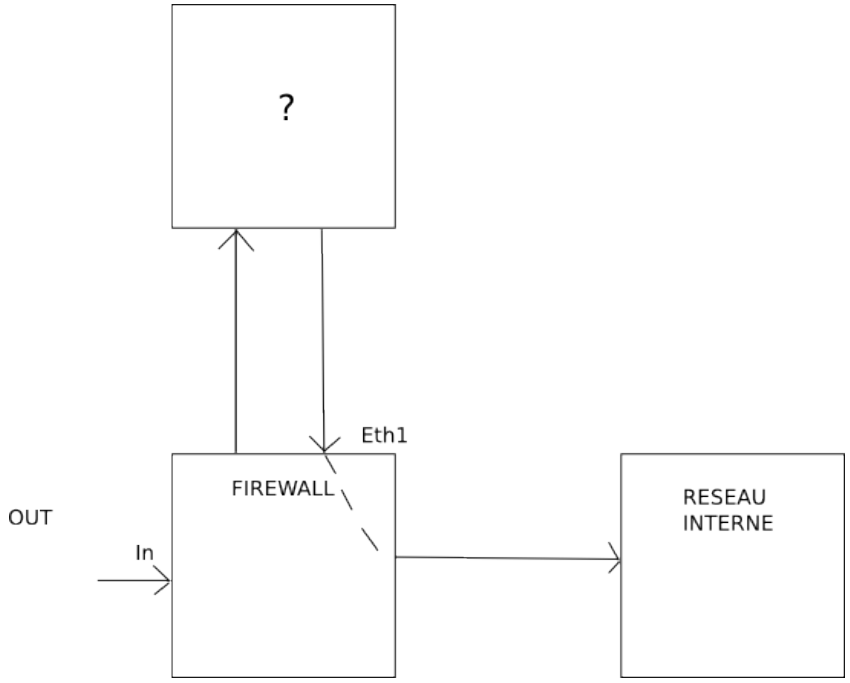
```
mysql   3306/tcp
http    80/tcp
https   443/tcp
ssh   22/tcp
```

Voici des règles IPtables configurées sur un firewall.

```
Chain INPUT (policy DROP)

target     prot opt source               destination
ACCEPT     all  --  anywhere             anywhere             ctstate
    RELATED,ESTABLISHED
ACCEPT     tcp  --  147.127.1.1          anywhere             ctstate
    NEW tcp dpt:ssh

Chain FORWARD (policy DROP)

target     prot opt source               destination
ACCEPT     all  --  anywhere             anywhere             ctstate
    RELATED,ESTABLISHED
ACCEPT     tcp  --  anywhere             192.168.80.1         ctstate
    NEW tcp dpt:http
ACCEPT     tcp  --  192.168.80.1         192.168.6.1          tcp dpt:
    mysql ctstate NEW
ACCEPT     tcp  --  192.168.1.1          192.168.6.1          tcp dpt:
    mysql ctstate NEW

Chain OUTPUT (policy DROP)

target     prot opt source               destination
ACCEPT     all  --  anywhere             anywhere             ctstate
    RELATED,ESTABLISHED
```

— Dessiner le schéma réseau correspondant à ces règles en nommant les éléments.
— Quel type de règles supplémentaires (3) pourriez-vous rajouter pour renforcer la sécurité de cette architecture ? (écrire rapidement la règle ou l'expliquer si vous ne connaissez pas la syntaxe, exemple : je veux que le trafic tcp sur le port 42 qui aille de a à b en passant par l'interface d'entrée x soit accepté)
— Quel est l'intérêt de travailler avec un firewall avec états ?
— Quel est l'inconvénient majeur de ce dernier ?

Question 1.2 (8 points)



On s'intéresse pour cet exercice uniquement du trafic provenant de l'extérieur du réseau.

iptables -A FORWARD -m conntrack –ctstate RELATED,ESTABLISHED -j ACCEPT

— Quel est l'intérêt de mettre ce genre de règles en début de configuration iptables ?
— Quelle différence faites-vous entre un IDP et un IPS ?
— Dans la configuration ci-dessus, tout le trafic ESTABLISHED,RELATED est accepté vers le réseau intérieur, en revanche le trafic "NEW" est redirigé vers l'élément noté ?. Le trafic provenant de Eth1 est accepté. Quel peut être le rôle de cet élément ?
— Quel est l'intérêt de réaliser une telle architecture ?
— Sur quelle table (filter,nat,mangle) doit-on travailler pour que le trafic NEW soit redirigé ? Ecrire la règle ou l'expliquer. Comment s'appelle ce mécanisme ?

2 VPN

Question 2.1 (5 points)

— Quelles sont les propriétés de sécurité offertes par IPsec en mode AH (3) ?
— Quelle propriété de sécurité supplémentaire est offerte par IPsec en mode ESP ?
— Quelle différence faites-vous entre le mode tunnel et transport ?
— Le quel utiliseriez-vous pour dialoguer d'un réseau d'entreprise vers un serveur web (public / extérieur) ? Pourquoi l'autre ne fonctionnerait pas ?
— Quel est pour vous l'avantage d'un point de vue de l'application d'utiliser un VPN plutôt qu'une connexion via ssh ?