Contrôle d'accès : TP - Firewall

BLUEM Juliette - SEZNEC Lucas - MAIMBOURG Gaston

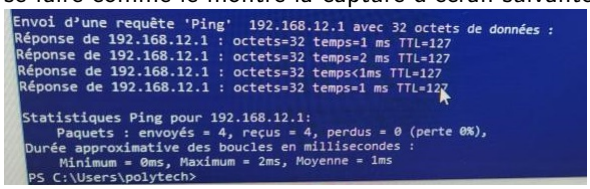
19 mai 2022

1 Introduction

Dans le cadre du cours de contrôle d'accès réseaux et authentification, nous réalisons ce TP sur les par-feu. Ce TP a pour but de nous faire manipuler de nouveaux équipements réseau dit de sécurité. En effet un pare feu permet de protéger un hôte sur un réseau en bloquant la totalité ou une partie des flux entrant sur l'hôte en question.

2 Filtrage de paquet avec les ACL

Les ACL (Access Control List) sont un mécanisme de contrôle d'accès à une ressource, désignant une liste d'adresses ou de ports autorisés ou interdits.
Afin de prendre en main ce mécanisme de contrôle d'accès, nous mettons en place une topologie très simple composée d'un routeur et de deux hôtes.
Lorsque que les IP des postes ainsi que les interfaces du router, sont configurées, la connexion entre H0 et H1 peut se faire comme le montre la capture d'écran suivante :



Nous mettons ensuite en place une ACL standart 10 pour bloquer tous les paquets dans le sens entrant de l'interface est. Maintenant, l'hôte ouest ne peut pas ping l'hôte est. Lorsqu'on lance un ping de l'hôte ouest vers l'hôte est, et que l'on observe le paquet sur Wireshark, on remarque que le paquet est bien bloqué car il ne peut pas atteindre sa destination.
Après avoir configuré une ACL standard 20 pour bloquer tous les paquets entrant dans l'interface Est, sauf si le paquet provient de l'hôte est, l'hôte ouest ne peut pas ping l'hôte est. En revanche, le contraire est possible.
La figure suivante montre la configuration finale de R0 où l'on remarque que l'interface 0 appartient au groupe ACL 20 en in et out. L'ACL 20 sert à tout refuser sauf ce qui provient de H1 :

3 Filtrage stateful

Nous allons maintenant déployer un PIX/ASA et observer du filtrage stateful. Ce filtrage dynamique de paquets permet de suivre l'état des sessions et d'adapter de manière dynamique les règles du pare-feu. L'amélioration par rapport au filtrage simple réside dans la conservation de la trace des sessions et des connexions dans des tables d'états internes au firewall.

3.1 Déploiement du Firewall

Les équipements plus récents comme les ASA proposent une fonction serveur DHCP par défaut pour protéger tout nouveau hôte qui se connecterait à la zone protégée par le firewall.
Nous mettons en place une topologie composée de deux hotes. Entre eux, un pare feu et un commutateur.
L'hôte H0 peut ping l'adresse de l'interface "inside" mais ne peut pas ping l'adresse de l'interface "outside". Il ne peut pas non-plus ping l'hôte H1.
Pourquoi les flux sont bloqués ? Le paquet est abandonné au moment où H1 souhaite répondre au ping de H0 mais que le pare feu bloque la réception de la réponse. Sur la figure suivante on observe bien que l'hôte H1 reçoit le paquet :

L'hôte H1 ne peut pas ping l'hôte H0 car H0 est protégé des pings par le firewall. Dans ce sens, le paquet est abandonné au moment où il traverse le firewall et que celui le bloque.
Voici notre table de routage du pare-feu :

```
ciscoasa# show route

Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 192.168.12.1 to network 0.0.0.0

C    192.168.12.0 255.255.255.0 is directly connected, outside
C    192.168.11.0 255.255.255.0 is directly connected, inside
S*   0.0.0.0 0.0.0.0 [1/0] via 192.168.12.1, outside
```

Le comportement par défaut du pare-feu est de protéger les hôtes de l'interface inside des paquets en provenance de l'interface outside, c'est pour cela que le ping ne fonctionne pas car la réponse est bloquée par le firewall et ne peut pas rentrer dans l'interface inside.

3.2 Class-map et Policy-map : filtrage et actions

Suite à un problème avec la commande "inspect icmp", nous n'avons pas pu effectuer cette partie du TP.

4 Placement du firewall

4.1 Notion de DMZ

Une DMZ est un sous-réseau physique ou logique qui expose une partie des ressources au réseau externe non-sécurisé. L'objectif est de restreindre l'accessibilité au strict nécessaire, en créant une zone tampon moins sécurisée. On trouve généralement des conceptions à un ou deux firewall.
Après avoir mit en place la topologie attendue, nous n'avons pas pu activer le paramètre de conservation d'inspection ICMP. Nous avons donc continué le TP sans prendre en compte cette configuration.
H2 ne peut pas atteindre le firewall lorsqu'il ping H0 et H0 n'arrive pas à atteindre H2. En effet, H2 traverse Routeur 0 mais n'atteint pas le firewall, il est comme bloqué dans le switch. H1, lui atteint le Routeur 0 mais ne le traverse pas. De l'autre coté, H1 ne traverse pas le firewall. H0 traverse le firewall mais reste comme h2 comme bloqué par le switch.
Nous n'identifions pas la source du problème, peut-être est-ce du au paramètre "inspect icmp" que nous ne pouvons pas mettre en place ?

5 Conclusion

Ce TP nous a appris le fonctionnement d'un pare-feu afin de protéger des équipements en bloquant certains types de paquets ainsi que l'utilité de mettre en place une DMZ pour séparer les équipements sensibles de ceux qui peuvent être exposés aux risques d'internet.