Sécurité des Réseaux

Projet IpTables

Youri Monton, Victorien Derasse, Alexandre Bergiers, Monroe Samuel

8 décembre 2015

1 Introduction

Ce rapport fait état de notre travail sur le projet Iptables dans le cadre du cours de Sécurité des Réseaux donné par Madame Van Den Schrieck.

Il contiendra une explication des règles haut niveau implémentées, et notre stratégie de validation ainsi que leurs résultats.
En annexe seront également incluses les configurations des trois firewalls, ainsi que les scripts ou méthodologies de validation.

2 Pré-configurations et Environnement

Tout d'abord, ce projet a été réalisé via le labo Netkit fournit par Mme. Van Den Schrieck, tournant dans un environnement Centos 6 Securité virtualisé sous VmWare.

Ceci a un impact au niveau de la configuration initiale, le labo Netkit n'avait tout simplement pas accès à internet. Quelques petits points de configurations sont donc nécéssaires pour poursuivre l'implémentation de notre solution :

1. Dans la machine virtuelle, il faut déterminer sur quelle interface est liée le labo Netkit, elle s'apelle typiquement **nk_tap_user**.

2. Il faut également déterminer quelle adresse ip est assignée à cette interface, ici **10.0.1.15** .

3. Dans le **router** du labo Netkit, il faut définir sa route par défaut (gateway) sur l'adresse ip de l'interface nk_tap_user : **route add default gw 10.0.1.15**.

4. Il faut maintenant activer le NAT sur la Vm pour que le tout fonctionne, en déterminant au préalable sous quelle interface la VM elle-même est reliée à l'Internet (eth6) :

   — **iptables -t nat -I POSTROUTING 1 -o eth6 -j MASQUERADE**
   — **iptables -I FORWARD 1 -i nk_tap_user -j ACCEPT**
   — **echo "1" ¿ /proc/sys/net/ipv4/ip_forward**

Un ping 8.8.8.8 depuis router devrait maintenant fonctionner, et une implémentation des règles NAT au sein du réseau et des règles Firewall peut être commencée.

Un ensemble de règles de POSTROUTING et de PREROUTING sont indispensables pour autoriser le trafic à sortir et entrer dans le réseau.
Celles-ci sont définies dans la configuration de FW1 et sont basiquement, du POSTROUTING en Masquerade pour les éléments sortants, et un PREROUTING pour les éléments sortants à destination des services publiques de Paranoyak.

3 Règles de haut niveau

J'ai ici séparé les requirements par ensemble de machines et en me focalisant à chaque fois autour d'un Firewall.

3.1 FireWall 1

La partie NFS peut subir des problèmes si les machines sont lancées directement avec les scripts de configuration, je n'ai pas identifié les requirements nécéssaires au mouting NFS.

— Les éléments de la DMZ publique doivent être accessibles depuis l'extérieur, nouvelle connexion ou établie depuis l'extérieur, réponses pour des connexions établies depuis l'intérieur.

— Les machines de la DMZ Sandwich peuvent contacter l'extérieur et établir de nouvelles connexions
— HTTP(S) de la DMZ Sandwich doivent pouvoir accéder au serveur WEB
— R1 peut contacter Processor en SSH
— R1 et R2 peuvent utiliser le serveur SSH
— R1 et R2 peuvent accéder au serveur Web
— R1 et R2 peuvent accéder à http et https vers l'extérieur
— R1 et R2 peuvent accéder au serveur Mail interne
— R1 et R2 peuvent accéder à RSYNC
— R1 et R2 peuvent accéder à NFS
— R1 et R2 peuvent accéder au DNS extérieur, et au LDNS
— R1 et R2 peuvent accéder au FTP
— Le reste du traffic doit être jeté

3.2 FireWall 2

Une redirection du traffic http (nat) a été nécéssaire afin de mettre en place des proxies web transparents.

— Le serveur LDNS, HTTP(S), SMTP/IMAP doit être accessible par U1 et U2
— Jeter le reste

3.3 FireWall 3

— Autoriser une connexion en SSH depuis R1 vers Processor
— Autoriser une connexion en SSH depuis SSH vers Processor
— Autoriser Processor à accéder au FTP
— Jeter le reste

4 Conclusion

Ce projet était une expérience très intéressante, néanmoins un peu complexe vu la diversité des services qui parfois interagissent entre eux aux travers de protocoles différents.

Nous pensons cependant avoir réalisé une belle partie de ce qui était demandé, même si certains petits points restent non fonctionnels à cause de difficultés et d'une gestion du temps un peu hasardeuse.