COMPTE RENDU
Mise en place DMZ

Par Alexandre BEROT-ARMAND
BTS SIO 2
Lycée Louis PERGAUD

TABLE DES MATIERES

INTRODUCTION

Ce TP suit le TP d'architecture virtualisée et a pour intérêt de créer une DMZ (Zone démilitarisée) à 1 niveau (donc une couche de protection).

Le but d'une DMZ est d'avoir une zone derrière le firewall qui N'EST PAS dans le réseau interne mais qui est accessible depuis l'extérieur.

La DMZ n'a pas accès au réseau interne donc votre architecture protégée : le firewall et votre ordinateur de travail restent sécurisés, mais votre site web est accessible depuis internet.

Pour ce TP, nous allons recréer une carte réseau (vmbr2) dans Proxmox pour créer le réseau de la DMZ dans le firewall. Je n'ai pas inclus cette étape puisque j'ai déjà expliqué la méthodologie dans le premier TP. De même pour le serveur Web qui n'est qu'une simple machine Debian avec un serveur Apache installé.

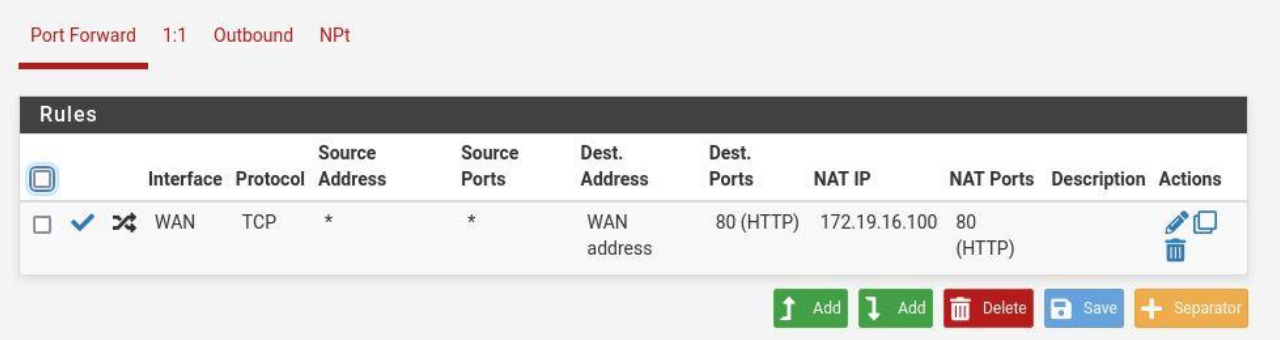
Ce compte rendu aura pour but de montrer la configuration du routeur.

CONFIGURATION DU PAT

Une fois la carte réseau créée et le serveur Apache installé dans ce nouveau réseau, il faut pouvoir y avoir accès via l'extérieur du firewall.

Pour des raisons de sécurité, il est préférable de laisser l'adresse du firewall comme IP frontale puisque c'est l'adresse la mieux protégée du réseau. Il est donc préférable de faire une redirection de port (PAT pour Port Adress Translation) vers le serveur Apache pour qu'en cas de requête via le port 80 (http), ce soit le pare-feu qui s'occupe de diriger la requête vers le serveur.

Pour cela, nous utilisons la Debian déjà dans le réseau interne pour se connecter au firewall. Nous allons ensuite dans les configurations NAT coté Port Forward pour créer une nouvelle règle :



Cette règle va simplement faire la redirection des requêtes sur le port 80 sur l'adresse du routeur (coté WAN donc extérieur, bien entendu) vers le serveur Apache de la DMZ.

DESACTIVATION DE LA REGLE RFC 1918

Pour la suite, il va falloir supprimer la règle RFC 1918 qui empêche les réseaux privés de passer le firewall.

Pour cela, il suffit d'aller dans la configuration de l'interface WAN via la Debian interne et de décocher la ligne « Block private networks and loopback addresses » :

Maintenant que la règle est désactivée, l'accès est possible via l'extérieur.

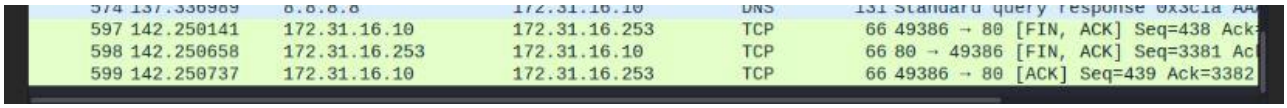
N.B. : puisque que les tests sont faits depuis des machines sur le même Proxmox, cette règle n'était pas utile à désactiver.

PREUVE DE FONCTIONNEMENT

Il est facile de vérifier que cela fonctionne puisqu'il suffit de prendre une machine du coté externe au firewall et de tenter de se connecter à la passerelle externe du firewall (qui ne répond pas s'il n y'a pas de redirection) :

La page d'Apache2 s'affiche, donc la redirection a bien lieu sur la DMZ.

On peut d'ailleurs voir le passage en regardant les trames de vmbr0 :



Ainsi que celle de vmbr2 du côté de la DMZ :