COMPTE RENDU
Architecture virtualisée

Par Alexandre BEROT-ARMAND
BTS SIO 2
Lycée Louis PERGAUD

TABLE DES MATIERES

Introduction _____ 3
Creation d'une carte réseau sur proxmox _____ 4
Création, installation et préparation de la VM firewall _____ 5
Configuration de la VM Firewall _____ 6
Configuration du Firewall _____ 7
Preuve de fonctionnement _____ 8

INTRODUCTION

Le but de ce TP est de commencer à créer une infrastructure de base pour pouvoir travailler sur notre projet et plus précisément d'amener à la création d'une zone sécurisée pour pouvoir avoir une infrastructure protégée.

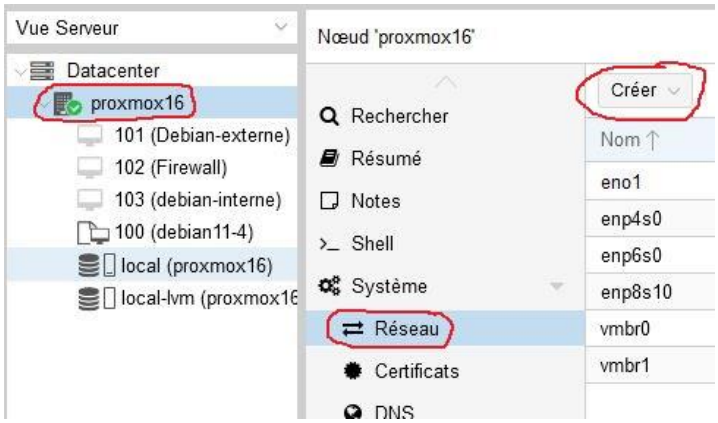
Ce compte rendu montrera comment réaliser un Firewall (ou pare-feu) sur l'hyperviseur Proxmox depuis la création des interfaces requises jusqu'au test final de fonctionnement.

CREATION D'UNE CARTE RESEAU SUR PROXMOX

J'ai commencé par créer une carte réseau sur Proxmox pour la future installation de la machine virtuelle Firewall.

En effet, cette deuxième interface est obligatoire pour séparer le flux extérieur du WAN qui est potentiellement dangereux (appelé Red) du flux interne du LAN qui n'a pas accès à l'extérieur sans passer par le Firewall (appelé Green).

Pour créer cette interface, il faut aller sur le serveur Proxmox, Onglet « réseau » et cliquer sur « créer » puis « créer un nouveau Bridge Linux » :



Finalement, il suffit de lui donner un nom (vmbr1 dans ce cas) puis appliquer la configuration.

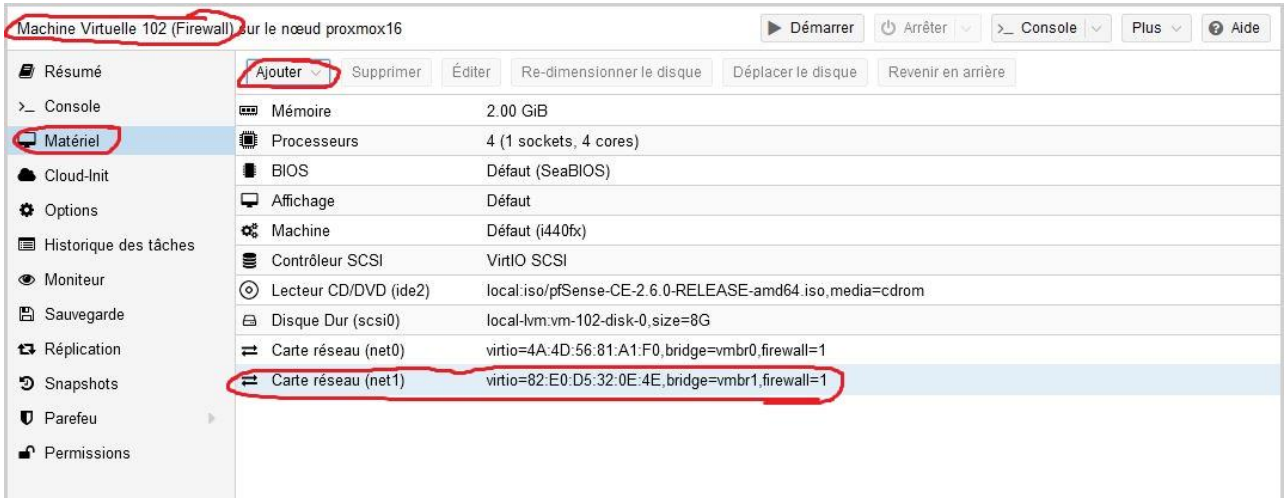
eno1	Carte réseau	Oui	Non	Non	
enp4s0	Carte réseau	Non	Non	Non	
enp6s0	Carte réseau	Non	Non	Non	
enp8s10	Carte réseau	Non	Non	Non	
vmbr0	Linux Bridge	Oui	Oui	Non	eno1
vmbr1	Linux Bridge	Oui	Oui	Non	

CREATION, INSTALLATION ET PREPARATION DE LA VM FIREWALL

Dans cette partie, j'ai créé une VM avec comme système d'exploitation Pfsense, un système d'exploitation qui sert à la mise en place de pare-feu.

Pour cela, il suffit de créer une VM (en haut à droite), puis lui donner un nom (Firewall ici).
Comme ISO, lui mettre Pfsense sous Linux puis lui ajouter un disque dur de 10 Go ainsi que 4 cœurs du CPU : il ne les utilisera pas tous en permanence.
2 Go de Ram est largement suffisant pour un Firewall.
On valide l'interface réseau puis on crée la VM.

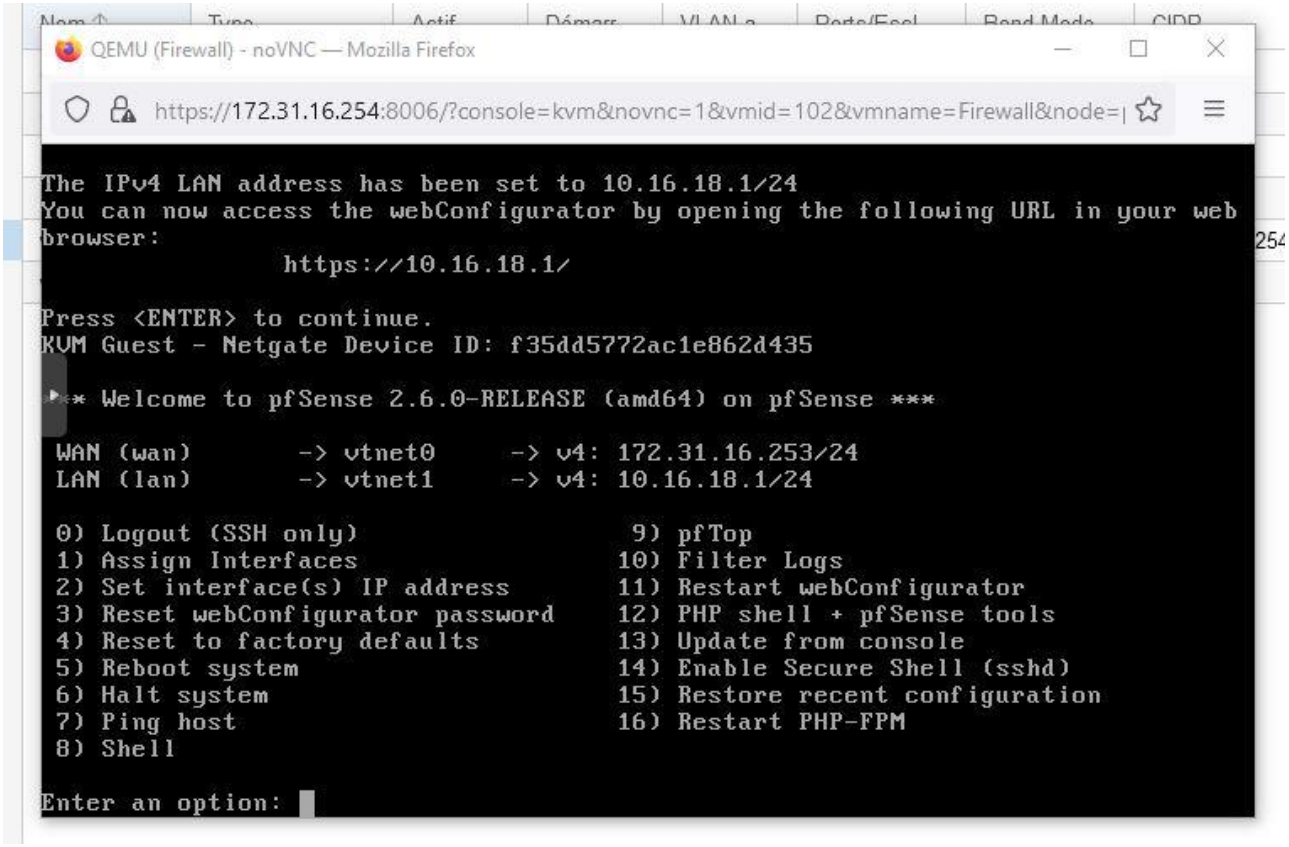
Ensuite il faut éteindre la VM. En effet, il n'y a qu'une seule interface réseau or il faut un WAN (vmbr0 ici) et le LAN sécurisé (vmbr1) : il faut donc lui rajouter l'interface créé précédemment.
Pour cela, il faut aller sur la VM, onglet « Matériel » et ajouter la « carte réseau vmbr1 » :



CONFIGURATION DE LA VM FIREWALL

Une fois la carte réseau ajoutée, il faut lancer la VM.

Après un temps de lancement, il va être demandé de configurer le Pfsense. Il suffit d'appuyer sur « 2 » et de mettre les adresses IP du WAN (sur l'interface du réseau externe) et du LAN (dans le réseau interne). Puis il faut redémarrer la machine :

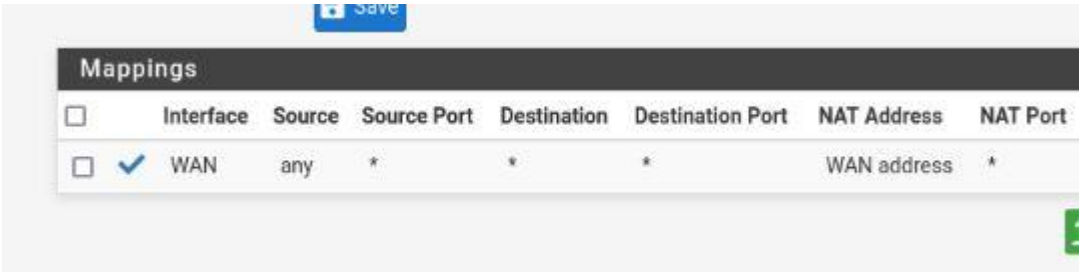


CONFIGURATION DU FIREWALL

La machine Firewall installée, il faut se connecter via une machine tierce au pare-feu.
Pour cela il faut créer (ou posséder) une machine virtuelle pour s'y connecter via une interface Web.
Dans mon cas, j'ai utilisé une machine Debian déjà prête avec une configuration pour avoir accès au réseau LAN sécurisé :

Puis nous nous connectons à l'interface du Firewall via le coté sécurisé (LAN) et nous configurons le Firewall pour faire une route :

Puis un NAT :



PREUVE DE FONCTIONNEMENT

Pour montrer le fonctionnement d'un Firewall, il suffit de prendre Wireshark et de faire un ping pour voir quelles sont les adresses AVANT le firewall et les adresses APRES le firewall. Dans ce cas de figure, voici le ping AVANT :

	Time	Source	Destination	Protocol	Length	Info
75	35.049632	10.16.18.10	8.8.8.8	ICMP	98	Echo (ping) request
76	35.064692	8.8.8.8	10.16.18.10	ICMP	98	Echo (ping) reply
77	36.050955	10.16.18.10	8.8.8.8	ICMP	98	Echo (ping) request
78	36.066941	8.8.8.8	10.16.18.10	ICMP	98	Echo (ping) reply
79	37.052211	10.16.18.10	8.8.8.8	ICMP	98	Echo (ping) request
80	37.083872	8.8.8.8	10.16.18.10	ICMP	98	Echo (ping) reply
81	38.054132	10.16.18.10	8.8.8.8	ICMP	98	Echo (ping) request
82	38.069434	8.8.8.8	10.16.18.10	ICMP	98	Echo (ping) reply

On voit bien la VM interne 10.16.18.10 qui ping vers 8.8.8.8 (donc un DNS de google).
Et voici le comportement des adresses APRES le Firewall :

396	102.136165	172.31.16.253	8.8.8.8	ICMP	98	Echo (ping) request
397	102.153647	8.8.8.8	172.31.16.253	ICMP	98	Echo (ping) reply
402	103.138158	172.31.16.253	8.8.8.8	ICMP	98	Echo (ping) request
403	103.162255	8.8.8.8	172.31.16.253	ICMP	98	Echo (ping) reply
408	104.139714	172.31.16.253	8.8.8.8	ICMP	98	Echo (ping) request
409	104.154420	8.8.8.8	172.31.16.253	ICMP	98	Echo (ping) reply
414	105.140860	172.31.16.253	8.8.8.8	ICMP	98	Echo (ping) request
415	105.155835	8.8.8.8	172.31.16.253	ICMP	98	Echo (ping) reply
420	106.142332	172.31.16.253	8.8.8.8	ICMP	98	Echo (ping) request

On voit bien que l'adresse IP de la Debian est masqué par le Firewall.