

20/09/2022

Mise en place d'une DMZ à différents niveaux

Atelier

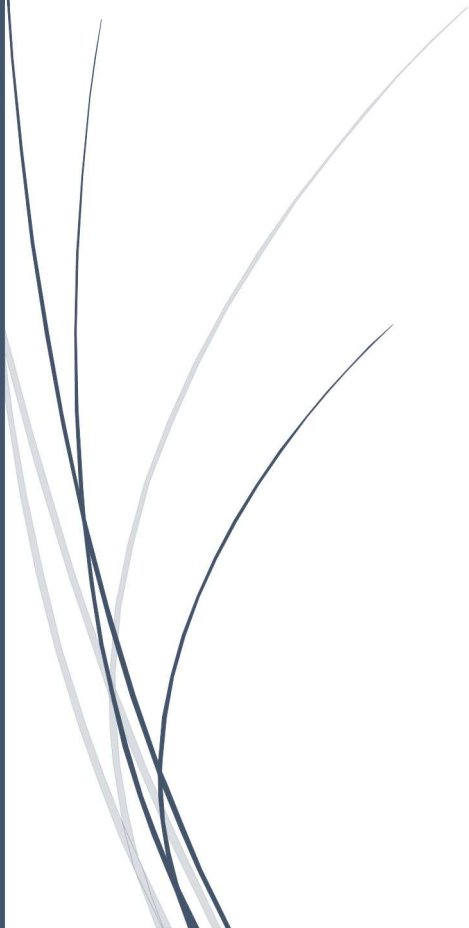




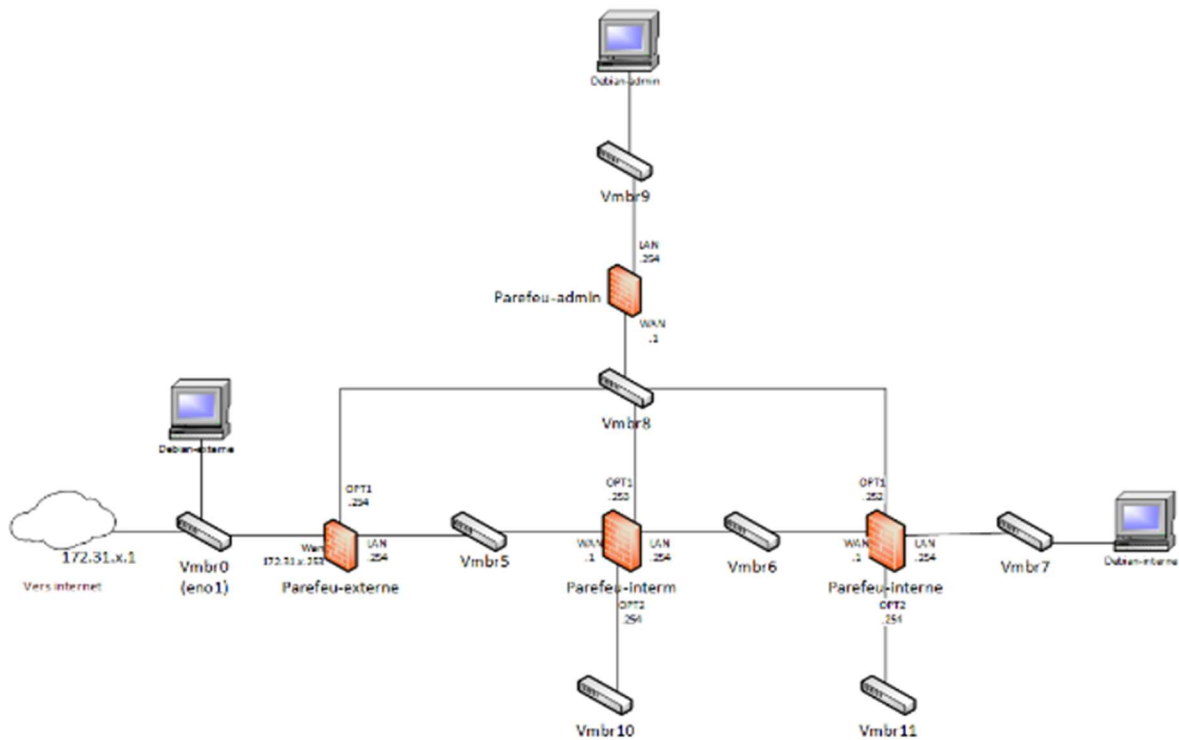
Table des matières

Travail à faire :.....	2
Ajout dan Proxmox :.....	3
Parametrage des PFs.....	4
Les manipulations Pfsense ADMIN.....	5
Les manipulations Pfsense AUTRES.....	6
Accès à Apache2.....	7

Travail à faire :

Dans ce TP nous allons créer une DMZ à plusieurs niveaux. Pour ce tp nous allons travailler avec un serveur Proxmox

Voilà à quoi cela va ressembler :



Réseaux IPs :

- parefeu-externe - parefeu-interm : 10.x.21.0/24
- parefeu-intermed - parefeu-interne : 10.x.20.0/24
- parefeu-interne-LAN : 10.x.18.0/24
- parefeu-interne-opt2 : 10.x.19.0/24
- parefeu-intermed-opt2 : 10.x.17.0/24
- parefeu-admin-wan : 10.x.2.0/24

Ajout dan Proxmox :

Il faudra ajouter des nouveaux VMBR afin de connecter nos nouvelles machines dessus.

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
vmbr1	Linux Bridge	Oui	Oui	Non
vmbr10	Linux Bridge	Oui	Oui	Non
vmbr11	Linux Bridge	Oui	Oui	Non
vmbr2	Linux Bridge	Oui	Oui	Non
vmbr5	Linux Bridge	Oui	Oui	Non
vmbr6	Linux Bridge	Oui	Oui	Non
vmbr7	Linux Bridge	Oui	Oui	Non
vmbr8	Linux Bridge	Oui	Oui	Non
vmbr9	Linux Bridge	Oui	Oui	Non

Il ne nous reste plus que a créer de nouvellement machines virtuel :

- 110 (TP4Pf-externe)
- 111 (TP4Pf-interm)
- 112 (TP4Pf-interne)
- 113 (TP4Pf-admin)
- 114 (TP4Debiane-externe)
- 115 (TP4Debian-admin)
- 116 (TP4Debian-interne)

Maintenant il ne nous reste juste a leur attribuer le vmbr a la bonne carte réseaux en respectant le schéma !!!

Machine Virtuelle 112 (TP4Pf-interne) sur le nœud proxmox13

Résumé	Ajouter	Supprimer	Éditer	Re-dimensionner le disque	Déplacer le disque	Revenir en arrière
Console	Mémoire	2.00 GiB				
Matériel	Processeurs	4 (1 sockets, 4 cores)				
Cloud-Init	BIOS	Défaut (SeaBIOS)				
Options	Affichage	Défaut				
Historique des tâches	Machine	Défaut (i440fx)				
Moniteur	Contrôleur SCSI	VirtIO SCSI				
Sauvegarde	Lecteur CD/DVD (ide2)	local:iso/pfSense-CE-2.6.0-RELEASE-amd64.iso,media=cdrom				
Réplication	Disque Dur (scsi0)	local-lvm:vm-112-disk-0,size=16G				
Snapshots	Carte réseau (net0)	virtio=72:CA:DE:45:E1:8D,bridge=vmbr6,firewall=1				
Parefeu	Carte réseau (net1)	virtio=6E:A0:4E:EB:88:4B,bridge=vmbr7,firewall=1				
Permissions	Carte réseau (net2)	virtio=5A:86:01:7F:D2:7B,bridge=vmbr8,firewall=1				
	Carte réseau (net3)	virtio=E2:0D:F7:85:6E:65,bridge=vmbr11,firewall=1				

Parametrage des PFs

Nous allons attribuer les adresses IP à l'interface de nos pare-feux en respectant le schéma.

Pour moi cela donne :

Pare-feu externe

```
WAN (wan)      -> vtnet0      -> v4: 172.31.13.253/24
LAN (lan)      -> vtnet1      -> v4: 10.13.21.254/24
OPT1 (opt1)    -> vtnet2      -> v4: 10.13.1.254/24
```

Pare-feu interm :

```
WAN (wan)      -> vtnet0      -> v4: 10.13.21.1/24
LAN (lan)      -> vtnet1      -> v4: 10.13.20.254/24
OPT1 (opt1)    -> vtnet2      -> v4: 10.13.1.253/24
```

Pare-feu interne :

```
WAN (wan)      -> vtnet0      -> v4: 10.13.20.1/24
LAN (lan)      -> vtnet1      -> v4: 10.13.18.254/24
OPT1 (opt1)    -> vtnet2      -> v4: 10.13.1.252/24
OPT2 (opt2)    -> vtnet3      -> v4: 10.13.19.254/24
```

Pare-feu admin :

```
WAN (wan)      -> vtnet0      -> v4: 10.13.1.1/24
LAN (lan)      -> vtnet1      -> v4: 10.13.2.254/24
```

Les manipulations Pfsense ADMIN

Pour commencer il faut désactiver le RFC1918 sur le WAN :

Reserved Networks

Block private networks and loopback addresses ☐

Blocks traffic from IP addresses that are reserved for private networks per RFC 1918 (10/8, 172.16/12, 192.168/16) and unique local addresses per RFC 4193 (fc00::/7) as well as loopback addresses (127/8). This option should generally be turned on, unless this network interface resides in such a private address space, too.

Vérifier si on n'utilise pas de route par défauts :

Gateways Static Routes Gateway Groups

Name	Default	Interface	Gateway	Monitor IP	Description	Actions
Save Add						

Default gateway

Default gateway IPv4: None
Select a gateway or failover gateway group to use as the default gateway.

Default gateway IPv6: None
Select a gateway or failover gateway group to use as the default gateway.

Save

Activer l'outbound-NAT sur l'interface WAN :

Firewall / NAT / Outbound

Port Forward 1:1 Outbound NAT

Outbound NAT Mode

Mode: ☒ Automatic outbound NAT rule generation. (IPsec passthrough included) ☐ Hybrid Outbound NAT rule generation. (Automatic Outbound NAT + rules below) ☒ Manual Outbound NAT rule generation. (AON - Advanced Outbound NAT) ☐ Disable Outbound NAT rule generation. (No Outbound NAT rules)

Save

Mappings

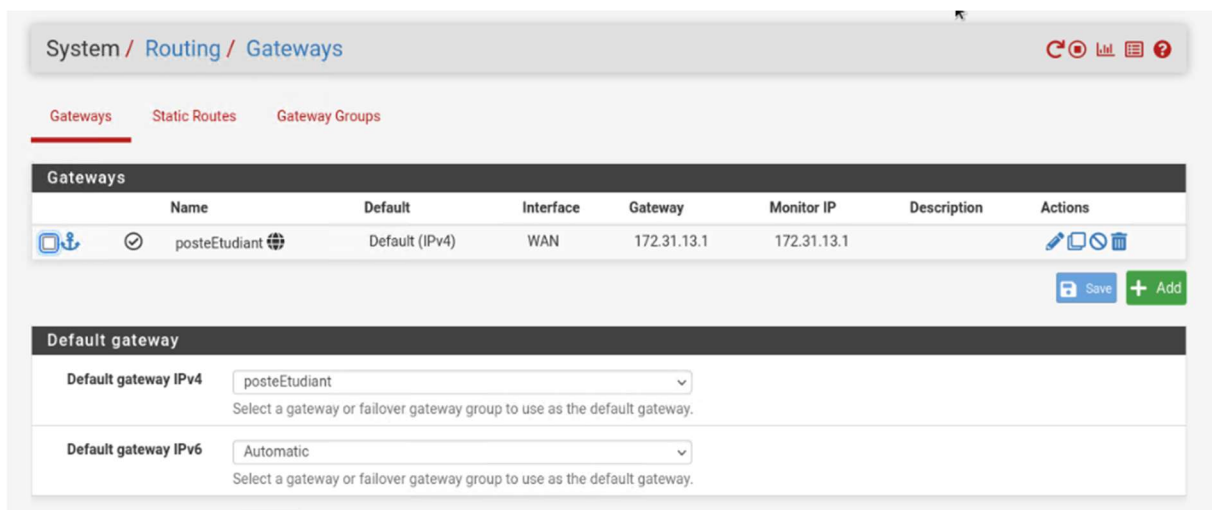
	Interface	Source	Source Port	Destination	Destination Port	NAT Address	NAT Port	Static Port	Description	Actions
<input checked="" type="checkbox"/>	WAN	any	*	*	*	WAN address	*			Save Add Delete

Les manipulations Pfsense AUTRES

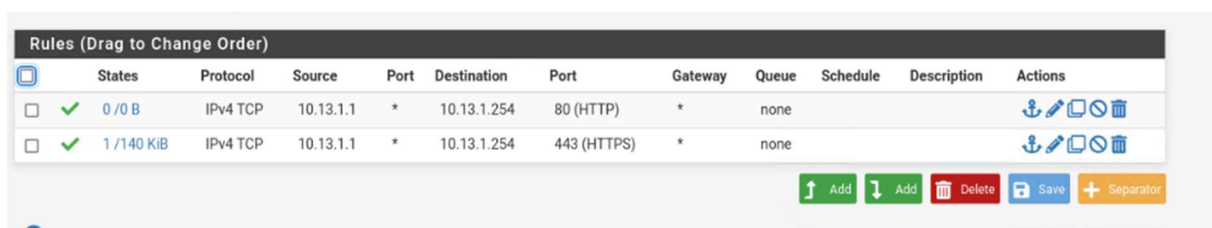
Grace à la Debian interne nous pouvoir paramétrer toute les autres PF mais il y aura un ordre à respecter afin de faire.

PF interne puis PF interm puis PF externe

Comme pour la PF admin il faudra désactiver le RFC1918 sur le WAN et mettre une passerelle par défauts :



Créer deux règles pour autoriser l'administrations du pf pare OPT1 :






Et après il reste plus que à couper l'administration par le réseau Lan :
Système > Advanced > Admin Access

Anti-lockout ☒ Disable webConfigurator anti-lockout rule

When this is unchecked, access to the webConfigurator on the LAN interface is always permitted, regardless of the user-defined firewall rule set. Check this box to disable this automatically added rule, so access to the webConfigurator is controlled by the user-defined firewall rules (ensure a firewall rule is in place that allows access, to avoid being locked out!) Hint: the "Set interface(s) IP address" option in the console menu resets this setting as well.




Accès à Apache2

Nous avons installé un serveur apache 2 dans le réseau opt2 de la pf-extérieur

<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	WAN	TCP	*	*	172.31.13.253	80 (HTTP)	10.13.21.1	80 (HTTP)	  
--------------------------	-------------------------------------	--------------------------	-----	-----	---	---	---------------	-----------	------------	-----------	---

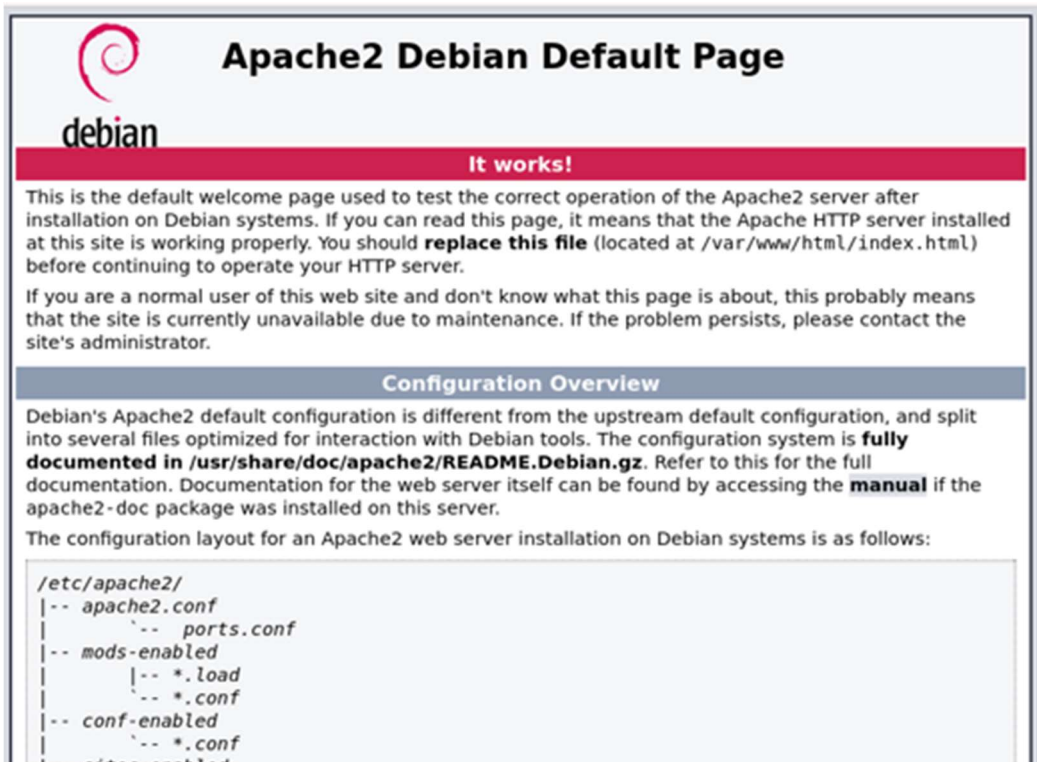
La règle a pour but de rediriger toute source visant l'interface WAN a être rediriger sur le WAN du PF intermédiaire.

On fait la même règle sur la PF-extérieur :

<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	WAN	TCP	*	*	WAN address	80 (HTTP)	10.13.17.10	80 (HTTP)	  
--------------------------	-------------------------------------	-------------------------------------	-----	-----	---	---	-------------	-----------	-------------	-----------	---

Même principe que pour l'autre.

Grace a cela on obtient cela sur ip 172.31.13.253 on obtient :



The screenshot shows the Apache2 Debian Default Page. At the top, there is a Debian logo and the title "Apache2 Debian Default Page". Below the title, a red banner says "It works!". The main text explains that this is the default welcome page used to test the correct operation of the Apache2 server after installation on Debian systems. It states that if you can read this page, it means that the Apache HTTP server installed at this site is working properly. It advises to replace this file (located at /var/www/html/index.html) before continuing to operate your HTTP server. It also mentions that if you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.

Below the main text, there is a section titled "Configuration Overview". It explains that Debian's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Debian tools. The configuration system is fully documented in /usr/share/doc/apache2/README.Debian.gz. It refers to this for the full documentation. Documentation for the web server itself can be found by accessing the manual if the apache2-doc package was installed on this server. It then states that the configuration layout for an Apache2 web server installation on Debian systems is as follows:

```
/etc/apache2/
|-- apache2.conf
|   |-- ports.conf
|-- mods-enabled
|   |-- *.load
|   |-- *.conf
|-- conf-enabled
|   |-- *.conf
|-- sites-enabled
```