

Rapport routeur PfSense

1- Préparation

Le routeur est un routeur PfSense fonctionnant sous FreeBSD 12. Il possède 3 cartes réseaux. Une sur le Vlan SIO (WAN), une sur le Vlan LAN et un sur le Vlan DMZ.










Les adresses IP sont les suivantes :

```
WAN (wan)      -> vmx0      -> v4 : 172.31.200.1/16
LAN (lan)      -> vmx1      -> v4 : 172.17.255.254/16
DMZ (opt1)     -> vmx2      -> v4 : 192.168.17.254/24
```

La configuration sur interface web se fait sur le LAN grâce à l'url <http://172.17.255.254>.

L'adresse 172.31.200.1 sera l'IP publique pour accéder à l'interface du site web.

2- Les règles NAT

Rules												
<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Interface	Protocol	Source Address	Source Ports	Dest. Address	Dest. Ports	NAT IP	NAT Ports	Description	Actions
<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	WAN	TCP	*	*	WAN address	8080	172.17.0.4	80 (HTTP)	redirection vers sgbd	  
<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	WAN	TCP	*	*	WAN address	22 (SSH)	192.168.17.1	22 (SSH)	redirection srv web ssh	  
<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	WAN	TCP	*	*	WAN address	web	192.168.17.1	web	redirection serveur web	  

La première règle sert à rediriger l'adresse 172.31.200.1 et pointer vers l'adresse 172.17.0.4 du serveur de base de données, avec également une redirection de port en 8080. Pour accéder au serveur de base de données depuis l'extérieur depuis l'interface web, il faudra donc saisir <http://172.31.200.1:8080/phpmyadmin> pour y accéder.

La deuxième règle est une règle provisoire, permettant d'accéder au serveur web 192.168.17.1 en accès SSH, afin de permettre aux développeurs de déposer les fichiers sur le serveur web.

La troisième règle est la règle de redirection vers le serveur web. Un alias a été créé pour les ports 80 et 443. Le site web est donc accessible depuis l'extérieur grâce à l'url <http://172.31.200.1/infotools1>.

3- Les règles de Filtrage

Carte réseau WAN

Firewall / Rules / WAN

Floating **WAN** LAN DMZ

Rules (Drag to Change Order)

<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✓ 0 / 978 KiB	IPv4 TCP	*	*	192.168.17.1	web	*	none		NAT redirection serveur web	
<input type="checkbox"/>	✓ 0 / 5 KiB	IPv4 TCP	*	*	192.168.17.1	22 (SSH)	*	none		NAT redirection srv web ssh	
<input type="checkbox"/>	✓ 0 / 0 B	IPv4 TCP	*	*	172.17.0.4	80 (HTTP)	*	none		NAT redirection vers sgbd	

La première règle autorise toute les adresses IP à se diriger vers le serveur web 192.168.17.1 en HTTP et HTTPS.

La deuxième règle autorise toute les adresses IP à se diriger vers le serveur web en 192.168.17.1 en SSH.

La troisième règle autorise toute les adresses IP à se diriger vers le serveur de base de données 172.17.0.4 en HTTP.

Carte réseau LAN

Floating WAN **LAN** DMZ

Rules (Drag to Change Order)

<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✓ 3 / 1.92 MiB	*	*	*	LAN Address	80	*	*		Anti-Lockout Rule	
<input type="checkbox"/>	✓ 1 / 34.58 MiB	IPv4 UDP	172.17.0.5	*	LAN address	161 (SNMP)	*	none		requête SNMP dans le LAN	
<input type="checkbox"/>	✓ 0 / 8.98 MiB	IPv4 UDP	172.17.0.5	*	192.168.17.1	161 (SNMP)	*	none		Acces SNMP du Centreon vers le serveur web	
<input type="checkbox"/>	✓ 0 / 31.64 MiB	IPv4 TCP	172.17.0.6	*	192.168.17.1	22 (SSH)	*	none		Acces ssh SrvBackup vers SrvWeb	
<input type="checkbox"/>	✓ 9 / 57.60 MiB	IPv4 TCP/UDP	172.17.0.1	*	*	53 (DNS)	*	none		requetes DNS SrvAD sur le NET	
<input type="checkbox"/>	✓ 6 / 22.73 GiB	IPv4 TCP	LAN net	*	*	web	*	none		acces internet	
<input type="checkbox"/>	✓ 0 / 0 B	IPv4 TCP	*	*	192.168.17.1	80 (HTTP)	*	none		Acces LAN vers le serveur Web local	
<input type="checkbox"/>	✓ 1 / 6.89 MiB	IPv4 ICMP any	*	*	*	*	*	none		ping	

La première règle sert est une règle définit par défaut d'anti blocage

La deuxième règle permet au serveur Centreon de faire des requêtes SNMP dans le LAN

La troisième règle permet au serveur Centreon de faire des requêtes SNMP vers le Serveur Web

La quatrième règle permet au serveur de sauvegarde (172.17.0.6) d'accéder en SSH au serveur web afin de récupérer les fichiers à sauvegarder.

La cinquième règle permet au serveur AD/DNS/DHCP de faire des requêtes DNS sur le net.

La sixième règle permet à tout le réseau du Vlan LAN à accéder à internet.

La septième règle permet à tout le réseau du Vlan LAN à accéder au serveur web.

La dernière règle est une règle provisoire de test autorisant les requêtes ICMP sur tout le réseau LAN.

Carte réseau DMZ

Floating WAN LAN DMZ											
Rules (Drag to Change Order)											
<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✓ 0 /12.95 MiB	IPv4 TCP	192.168.17.1	*	*	*	*	none		Accès SrvWeb à internet	
<input type="checkbox"/>	✓ 0 /1000 B	IPv4 TCP	192.168.17.1	*	172.17.0.4	*	*	none		Serveur web interroge sgbd	
<input type="checkbox"/>	✓ 0 /0 B	IPv4 ICMP any	*	*	*	*	*	none			

La première règle permet au serveur web d'accéder à internet.

La deuxième règle permet au serveur web d'accéder au serveur de base de données.

La dernière règle est une règle provisoire de test autorisant les requêtes ICMP.