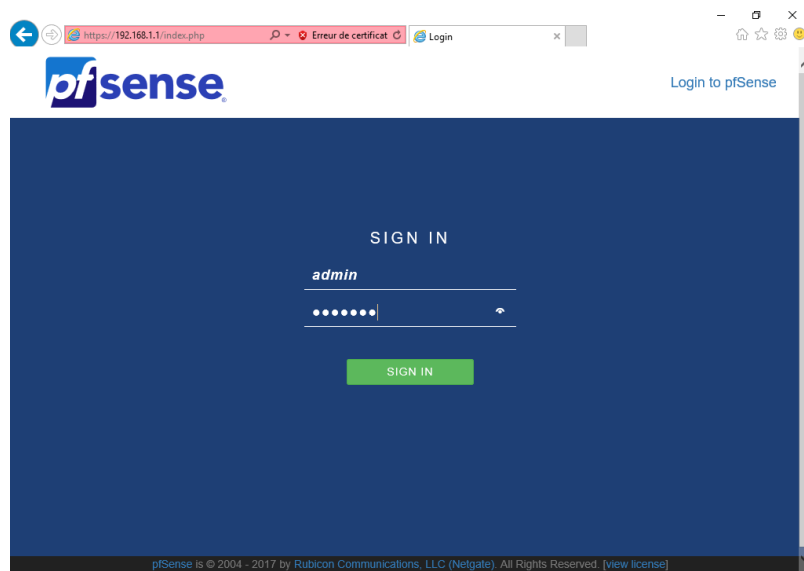


Tutoriel d'installation et configuration

De base PFSense bloque tout le trafic, pour accéder à l'interface web, le login est « admin » et le mot de passe est « PFSense ».



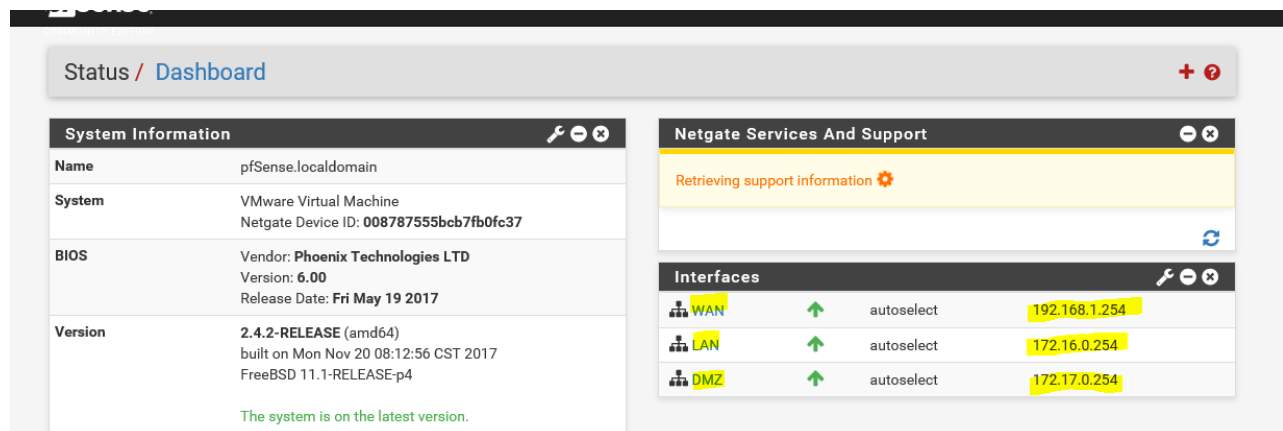
Ensuite, il faut assigner et allumer les différentes interfaces du PFSense (ici il y en a trois) et leurs mettre une description afin de s'y retrouver comme ci-dessous.

Voici les trois interfaces de notre maquette sur le PFSense :

WAN → 192.168.0.254 /24

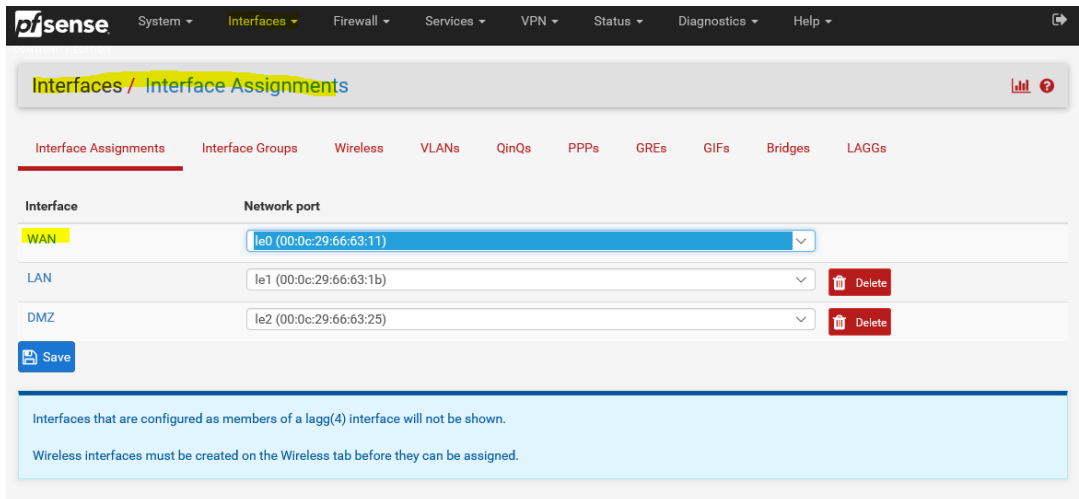
LAN → 172.16.0.254 /24

DMZ → 172.17.0.254 /24



Teddy BRUGUET - Personnel

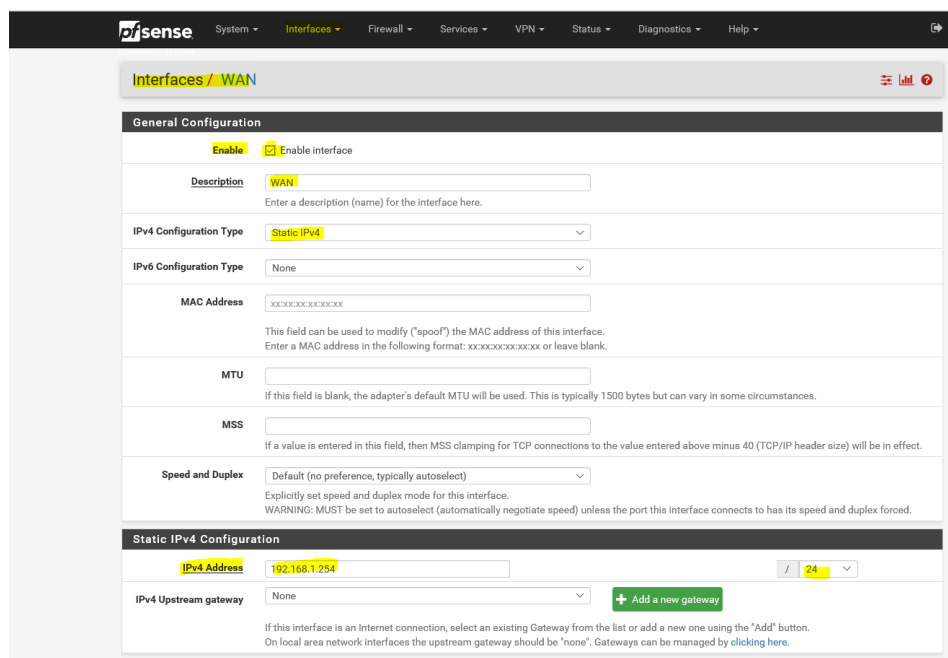
Pour configurer une interface, allez dans l'onglet « Interfaces » et « Assignments », ensuite choisissez l'interface que vous voulez configurer comme ci-dessous.



Comme sur l'image ci-dessous, il faut dans un premier temps, activer l'interface en cochant la case « Enable », dans description vous mettez le titre de l'interface en question (ici WAN).

Ensuite, vous devez lui attribuer une adresse IP, ici pour le Wan l'adresse IP est 192.168.1.254, après il vous suffit de sauvegarder les paramètres.

Vous devez répéter cette action sur les différentes interfaces et ensuite redémarrer votre PfSense afin que les modifications soient prises en compte.



Une fois vos interfaces actives, nous allons configurer le nat afin d'accéder à distance depuis un réseau extérieur les ressources suivantes :

- Serveur web = 172.17.0.1 sur le port 80.
- Serveur mail = 172.17.0.1 sur le port 25.

The screenshot shows the Mikrotik WinBox interface for configuring NAT Port Forwarding. The breadcrumb trail is Firewall / NAT / Port Forward. The configuration is set for 1:1 NAT, Outbound, and NPT. A table of rules is displayed with the following data:

Rules	Interface	Protocol	Source Address	Source Ports	Dest. Address	Dest. Ports	NAT IP	NAT Ports	Description	Actions
<input type="checkbox"/>	WAN	TCP	*	*	DMZ net	3389 (MS RDP)	172.17.0.1	3389 (MS RDP)		
<input type="checkbox"/>	WAN	TCP	*	*	DMZ address	25 (SMTP)	172.17.0.1	25 (SMTP)		
<input type="checkbox"/>	WAN	TCP	*	*	DMZ address	110 (POP3)	172.17.0.1	110 (POP3)		
<input type="checkbox"/>	WAN	TCP	*	*	DMZ net	3389 (MS RDP)	172.17.0.1	3389 (MS RDP)	Redirection de ports vers Bureau à distance vers SRV MAIL	
<input type="checkbox"/>	WAN	TCP	*	*	DMZ address	80 (HTTP)	172.17.0.1	80 (HTTP)		

At the bottom of the table, there are control buttons: Add (up arrow), Add (down arrow), Delete, Save, and Separator.

Nous allons ensuite créer des règles sur les différentes interfaces afin d'autoriser les différents trafics entre les machines.

Pour ajouter une règle il vous suffit de cliquer sur « Add » et de remplir les champs demandés, il vous faudra la source, le port à ouvrir, la destination le port dont il est question, et le protocole utilisé.

Voici les extraits de ma configuration PFSense en fonction de nos différentes interfaces.

Ci-dessous nos règles sur la partie WAN :

The screenshot shows the PFSense Firewall configuration page for the WAN interface. A dropdown menu is open, highlighting 'Rules'. Below the menu, there are tabs for Floating, WAN (selected), LAN, and DMZ. A table titled 'Rules (Drag to Change Order)' lists five NAT rules. At the bottom, there are buttons for Add, Add, Delete, Save, and Separator.

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/> ✓ 0/0 B	IPV4 TCP	*	*	172.17.0.1	80 (HTTP)	*	none		NAT	
<input type="checkbox"/> ✓ 0/0 B	IPV4 TCP	*	*	172.17.0.1	3389 (MS RDP)	*	none		NAT Redirection de ports vers Bureau à distane vers SRV MAIL	
<input type="checkbox"/> ✓ 0/0 B	IPV4 TCP	*	*	172.17.0.1	110 (POP3)	*	none		NAT	
<input type="checkbox"/> ✓ 0/0 B	IPV4 TCP	*	*	172.17.0.1	25 (SMTP)	*	none		NAT	
<input type="checkbox"/> ✓ 0/0 B	IPV4 TCP	*	*	172.17.0.1	3389 (MS RDP)	*	none		NAT	

Voici nos règles sur le LAN :

The screenshot shows the PFSense Firewall configuration page for the LAN interface. The 'LAN' tab is selected. A table titled 'Rules (Drag to Change Order)' lists four rules. At the bottom, there are buttons for Add, Add, Delete, Save, and Separator.

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
✓ 3 / 2.96 MiB	*	*	*	LAN Address	443 80	*	*		Anti-Lockout Rule	
<input type="checkbox"/> ✓ 0/0 B	IPV4 UDP	LAN net	*	172.17.0.1/24	110 (POP3)	*	none			
<input type="checkbox"/> ✓ 20 / 49 KiB	IPV4 *	LAN net	*	*	*	*	none		Default allow LAN to any rule	
<input type="checkbox"/> ✓ 0/0 B	IPV4 TCP	LAN net	*	172.17.0.1/24	25 (SMTP)	*	none			

Teddy BRUGUET - Personnel

Par exemple ici, pour la DMZ, nous avons ouvert l'accès aux comptes AD, DNS, MAIL, IIS.

De plus, tous les pings sont autorisés à travers l'interface de la DMZ.

The screenshot shows the Mikrotik WinBox interface for configuring Firewall Rules on the DMZ interface. The breadcrumb navigation is 'Firewall / Rules / DMZ'. Below the breadcrumb, there are tabs for 'Floating', 'WAN', 'LAN', and 'DMZ', with 'DMZ' being the active tab. The main area displays a table of rules titled 'Rules (Drag to Change Order)'. The table has columns for 'States', 'Protocol', 'Source', 'Port', 'Destination', 'Port', 'Gateway', 'Queue', 'Schedule', 'Description', and 'Actions'. There are 12 rules listed, each with a checkbox, a status indicator (green checkmark), and a data transfer amount. The rules are for various protocols (TCP, UDP, ICMP) and ports (25, 110, 3389, 1026, 1025, 135, 445, 53, 389, 88, 3268). The descriptions include 'smtp 25 mail', 'pop 110 pour mail', 'test pb rpc prof', 'test rpc', 'test pb RPC', 'port 445 test', 'Acces au DNS du LAN', 'Acces Annuaire LDAP Active Directory', 'Acces aux comptes AD', 'Acces au cataogue AD', and 'Permet de ping à partir de la DMZ'. At the bottom right, there are buttons for 'Add', 'Delete', 'Save', and 'Separator'.

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/> ✓ 0 / 0 B	IPv4 TCP	DMZ net	*	172.16.0.3	25 (SMTP)	*	none		smtp 25 mail	
<input type="checkbox"/> ✓ 0 / 0 B	IPv4 TCP	DMZ net	*	172.16.0.3	110 (POP3)	*	none		pop 110 pour mail	
<input type="checkbox"/> ✓ 0 / 0 B	IPv4 TCP	DMZ net	*	172.16.0.3	3389 (MS RDP)	*	none		test pb rpc prof	
<input type="checkbox"/> ✓ 0 / 0 B	IPv4 TCP	DMZ net	*	172.16.0.3	1026	*	none		test rpc	
<input type="checkbox"/> ✓ 0 / 0 B	IPv4 TCP	DMZ net	*	172.16.0.3	1025	*	none		test rpc	
<input type="checkbox"/> ✓ 1 / 18 KiB	IPv4 TCP	DMZ net	*	172.16.0.3	135	*	none		test pb RPC	
<input type="checkbox"/> ✓ 0 / 47 KiB	IPv4 TCP	DMZ net	*	172.16.0.3	445 (MS DS)	*	none		port 445 test	
<input type="checkbox"/> ✓ 0 / 6 KiB	IPv4 UDP	DMZ net	*	172.16.0.3/24	53 (DNS)	*	none		Acces au DNS du LAN	
<input type="checkbox"/> ✓ 0 / 22 KiB	IPv4 TCP/UDP	DMZ net	*	172.16.0.3/24	389 (LDAP)	*	none		Acces Annuaire LDAP Active Directory	
<input type="checkbox"/> ✓ 0 / 24 KiB	IPv4 TCP	DMZ net	*	172.16.0.3/24	88	*	none		Acces aux comptes AD	
<input type="checkbox"/> ✓ 0 / 0 B	IPv4 TCP	DMZ net	*	172.16.0.3/24	3268	*	none		Acces au cataogue AD	
<input type="checkbox"/> ✓ 0 / 0 B	IPv4 ICMP any	*	*	*	*	*	none		Permet de ping à partir de la DMZ	

Configuration réseau – routage

Ci-dessous, notre configuration pour le DHCP et les réseaux déclarés sur le routeur.

Routage

Routeur bas, réseaux déclarés :

(Protocole RIP)

- 10.0.0.0
- 172.16.0.0
- 192.168.10.0
- 192.168.20.0

DHCP:

Pool : Utilisateurs

Passerelle : 192.168.10.254

Start IP address : 192.168.10.1

End IP address : 192.168.10.50

Masque : 255.255.255.0

Vlan : 10

Pool : Visiteurs

Passerelle : 192.168.20.254

Start IP address: 192.168.20.1

End IP address: 192.168.20.50

Masque : 255.255.255.0

Vlan : 20