

Le pare-feu intégré de Proxmox

Quelques informations

Ports utilisés par Proxmox

- Web interface: **8006** (TCP, HTTP/1.1 over TLS)
- VNC Web console: **5900-5999** (TCP, WebSocket)
- SPICE proxy: **3128** (TCP)
- sshd (used for cluster actions): **22** (TCP)
- rpcbind: **111** (UDP)
- sendmail: **25** (TCP, outgoing)
- corosync cluster traffic: **5405-5412** UDP
- live migration (VM memory and local-disk data): **60000-60050** (TCP)

Trois niveaux de pare-feu

1. Pare-feu du Datacenter
2. Pare-feu des nœuds (nodes)
3. Pare-feu des machines virtuelles et conteneurs

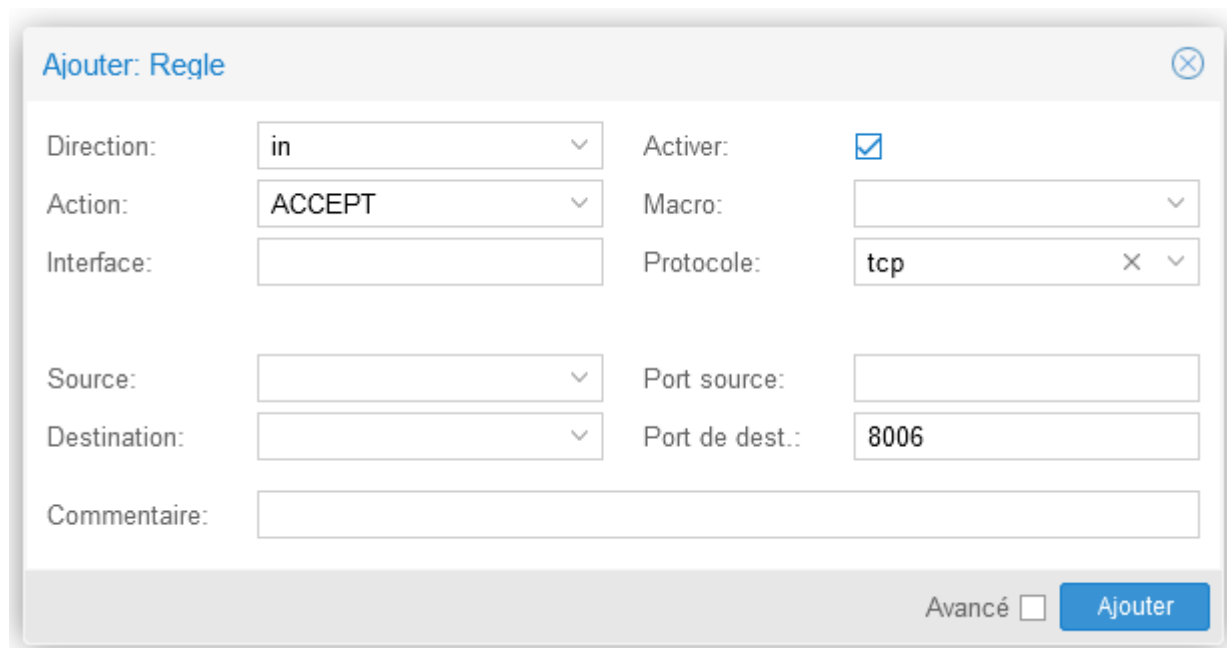
1 - Créer des règles pour le Datacenter avant d'activer le pare-feu

Pour ajouter des règles :

Datacenter ==> **Parefeu** ==> **[Ajouter]**

Règles à créer

Attention ! il y a des règles à créer avant l'activation du pare-feu :



The screenshot shows a dialog box titled "Ajouter: Règle" with a close button in the top right corner. The dialog contains the following fields:

Direction:	in	Activer:	<input checked="" type="checkbox"/>
Action:	ACCEPT	Macro:	
Interface:		Protocole:	tcp
Source:		Port source:	
Destination:		Port de dest.:	8006
Commentaire:			

At the bottom right, there is an "Avancé" checkbox (unchecked) and a blue "Ajouter" button.

Pour autoriser le port **8006** en **TCP** pour le portail WEB d'administration de Proxmox.
Ne pas oublier de cocher **activer**.

Ajouter: Règle ✕

Direction: Activer:

Action: Macro:

Interface: Protocole: ✕

Source: Port source:

Destination: Port de dest.:

Commentaire:

Avancé Ajouter

Pour autoriser le port **22** en **TCP** pour l'accès en **SSH**.
Ne pas oublier de cocher **activer**.

<input type="button" value="Ajouter"/> <input type="button" value="Copier"/> <input type="button" value="Insérer: Groupe de sécurité"/> <input type="button" value="Supprimer"/> <input type="button" value="Éditer"/>												
	On	Type	Action	Macro	Interface	Protoc...	Source	S.Port	Destination	D.Port	Niveau de j...	Commentaire
☰ 0	<input checked="" type="checkbox"/>	in	ACCEPT			tcp				22	nolog	
☰ 1	<input checked="" type="checkbox"/>	in	ACCEPT			tcp				8006	nolog	

Je peux voir mes règles.

2 - Activation du pare-feu pour le Datacenter

Lorsque toutes vos règles sont activées, vous pouvez maintenant activer le pare-feu en vous rendant dans :

Datacenter ==> **Parefeu** ==> **Options**
Sélectionnez **Parefeu** ==> **[Editer]**

Éditer: Parefeu ✕

Parefeu:

OK
Reset

Cochez **Parefeu** puis cliquez **[OK]**.

Éditer	
Parefeu	Oui
eatables	Oui
Limite de journal	Défaut (enable=1,rate1/second,burst=5)
Politique d'entrée	DROP
Politique de sortie	ACCEPT

Le pare-feu est bien activé.

Par défaut, tout ce qui entre est rejeté, tout ce qui sort est accepté.

3 - Création d'un groupe de sécurité depuis le Datacenter

Les groupes de sécurité permettent de regrouper plusieurs règles de pare-feu en une seule règle. Ils sont créés uniquement dans la zone « **Datacenter** ».
Exemple « *ServeurWEB* » avec les ports (22, 80, 443, etc.).

Datacenter ==> **Parefeu** ==> **Groupe de sécurité**

Cliquez sur **Créer**, donnez un nom.

Vous pouvez sélectionner ce groupe et cliquez sur [**Ajouter**] dans la partie droite pour commencer à ajouter toutes les règles de pare-feu.

Groupe: <input type="button" value="Créer"/> <input type="button" value="Supprimer"/> <input type="button" value="Éditer"/>		Regles: <input type="button" value="Ajouter"/> <input type="button" value="Copier"/> <input type="button" value="Supprimer"/> <input type="button" value="Éditer"/>			
Groupe ↑	Commentaire	On	Type	Action	Macro
serveurweb	HTTP HTTPS SSH				

Ajouter: Règle ✕

Direction: Activer:

Action: Macro:

Protocole:

Source: Port source:

Destination: Port de dest.:

Commentaire:

Avancé Ajouter

Ma règle pour le port **80** http, **Activer** est coché, je clique sur **[Ajouter]**, faire la même chose ensuite **pour le port 443 HTTPS**.

Ajouter: Règle ✕

Direction: Activer:

Action: Macro:

Protocole:

Source: Port source:

Destination: Port de dest.:

Commentaire:

Avancé Ajouter

Les paramètres pour le **SSH** (port 22) en utilisant une **macro** de configuration.

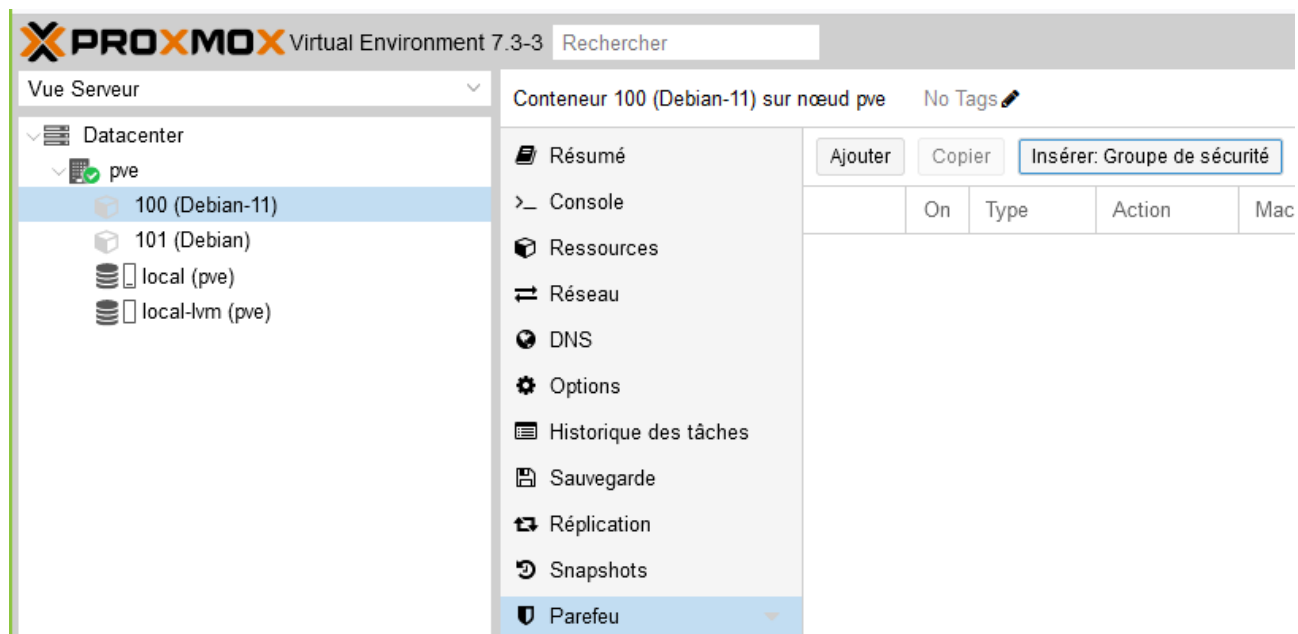
Groupe: Créer Supprimer Éditer		Regles: Ajouter Copier Supprimer Éditer										
Groupe ↑	Commentaire		On	Type	Action	Macro	Protoc...	Source	S.Port	Destination	D.Port	Niveau de j...
serveurweb	HTTP HTTPS SSH	☰ 0	<input checked="" type="checkbox"/>	in	ACCEPT	SSH						nolog
		☰ 1	<input checked="" type="checkbox"/>	in	ACCEPT		tcp				443	nolog
		☰ 2	<input checked="" type="checkbox"/>	in	ACCEPT		tcp				80	nolog

Le résultat.

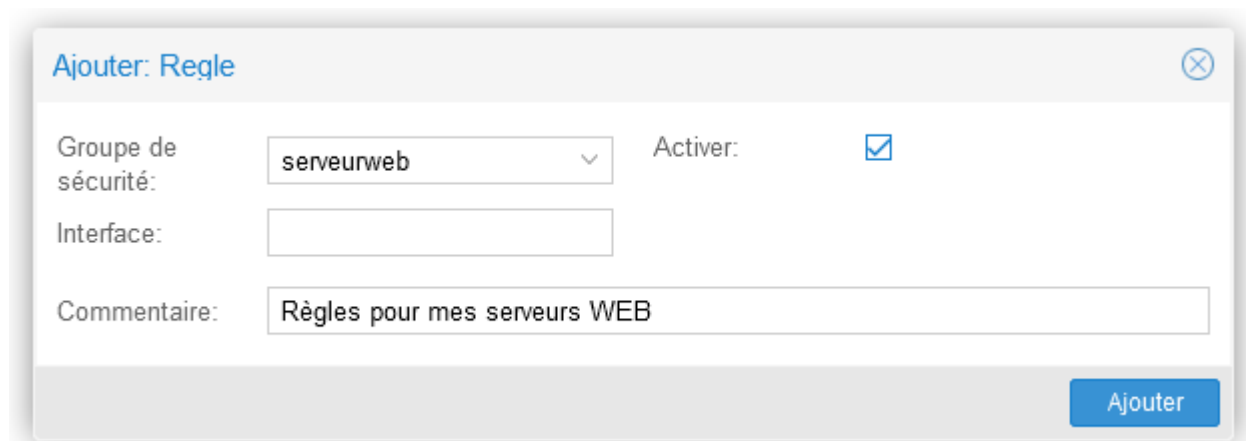
4 - Activation d'un groupe de sécurité pour une machine

Pour les règles

Rendez-vous dans la partie **Parefeu** de votre machine virtuelle et cliquez sur **[Insérer: Groupe de sécurité]**.

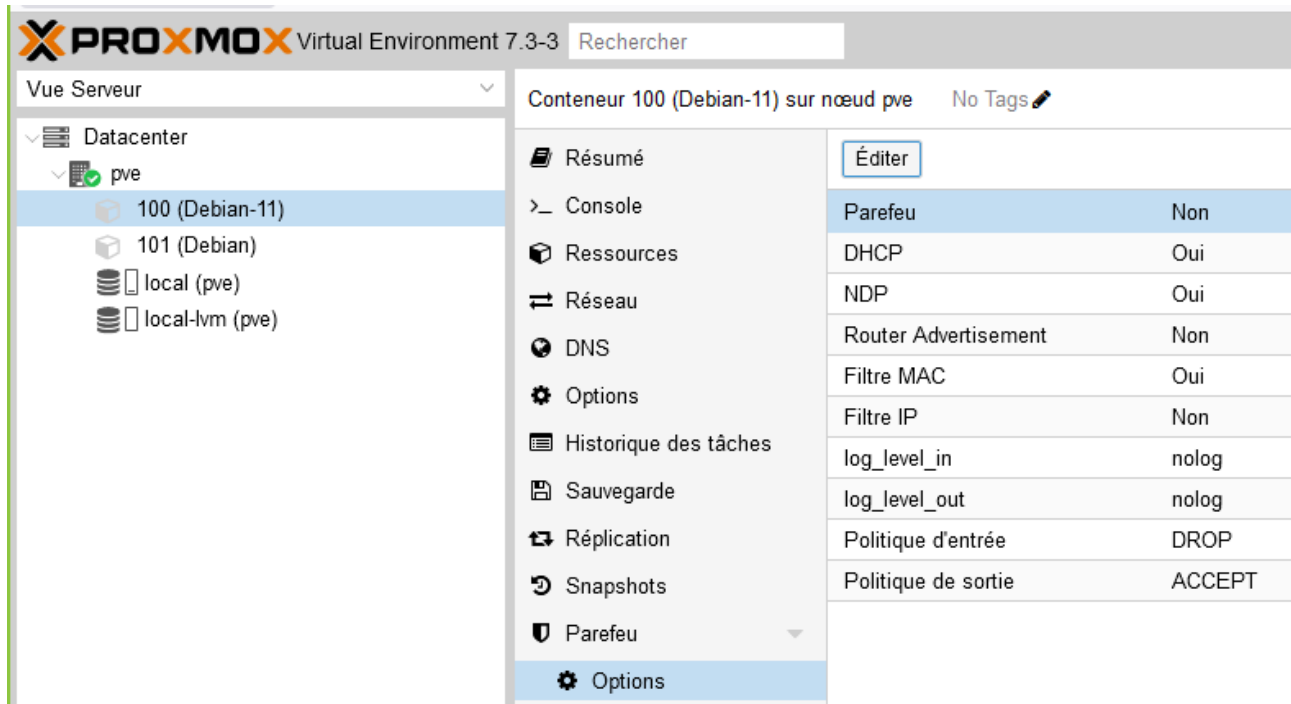


Choisissez le **groupe de sécurité** qui vous convient et cochez **Activer**.



Cliquez sur **[Ajouter]**.

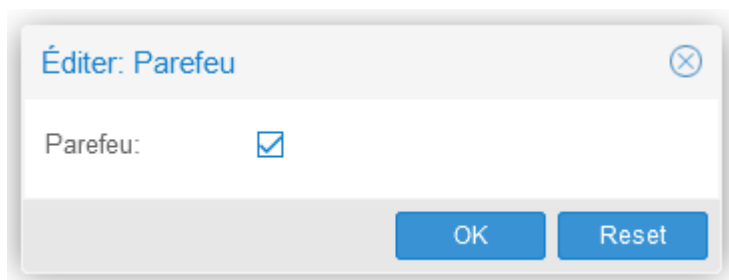
5 - Activer le pare-feu d'une machine



The screenshot shows the Proxmox VE interface for a container named '100 (Debian-11)'. The left sidebar shows the navigation tree with 'Datacenter' > 'pve' > '100 (Debian-11)' selected. The main area displays the 'Options' menu for the container, with 'Options' selected. The 'Options' panel shows a table of firewall settings:

Setting	Value
Parefeu	Non
DHCP	Oui
NDP	Oui
Router Advertisement	Non
Filtre MAC	Oui
Filtre IP	Non
log_level_in	nolog
log_level_out	nolog
Politique d'entrée	DROP
Politique de sortie	ACCEPT

Sélectionnez la **machine** ==> **Parefeu** ==> **Options** ==> Sélectionnez **Parefeu** ==> [Éditer]



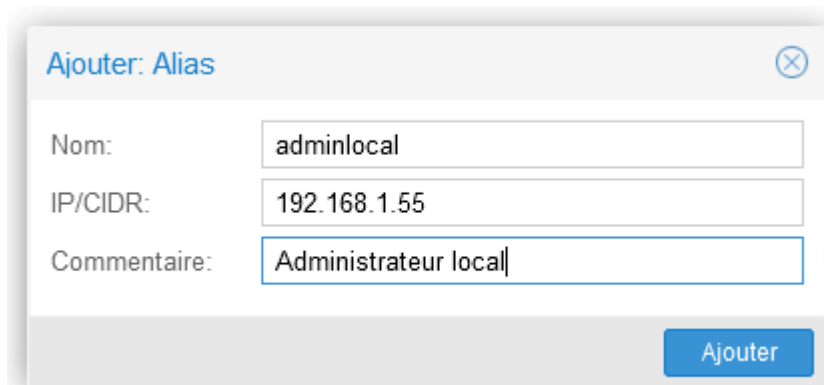
The dialog box 'Éditer: Parefeu' has a checkbox for 'Parefeu:' which is checked. At the bottom, there are 'OK' and 'Reset' buttons.

Cochez **Parefeu** ==> [OK]

6 - Alias

Alias va permettre de nommer les IP ou les plages d'IP à utiliser dans le pare-feu.

Datacenter ==> **Parefeu** ==> **Alias** ==> [Ajouter]



The dialog box 'Ajouter: Alias' contains three input fields: 'Nom:' with the value 'adminlocal', 'IP/CIDR:' with the value '192.168.1.55', and 'Commentaire:' with the value 'Administrateur local'. An 'Ajouter' button is at the bottom right.

Saisissez vos paramètres puis cliquez sur **[Ajouter]**.

Ajouter Supprimer Éditer		
Nom ↑	IP/CIDR	Commentaire
adminlocal	192.168.1.55	Administrateur local

On peut ajouter une plage d'adresse IP avec le CIDR (par exemple 192.168.1.0/24).

Lors de la création d'une règle on peut utiliser un alias en Source.

7-IPSet

Règles de pare-feu qui correspondent aux adresse IP ou aux sous-réseaux IP.

Exemple : IPSet nommé « Admin ».

Peuvent être créés dans les niveaux de pare-feu (Datacenter, VM et conteneurs).

Permet de créer des listes blanches et des listes noires d'adresses IP.

Datacenter ==> Parefeu ==> IPSet ==> [Créer]

Nommez l'IPSet ==> **[OK]**

Cliquez sur l'IPSet ==> **[Ajouter]** à droite.

Créer: IP/CIDR

IP/CIDR: adminlocal x v nomatch:

Commentaire:

Nom ↑	Commentaire
adminlocal	Administrateur local

Créer

IP/CIDR: Ajouter Supprimer Éditer		
	IP/CIDR	Commentaire
1	192.168.1.0/24	
2	192.168.1.55	
3	adminlocal	

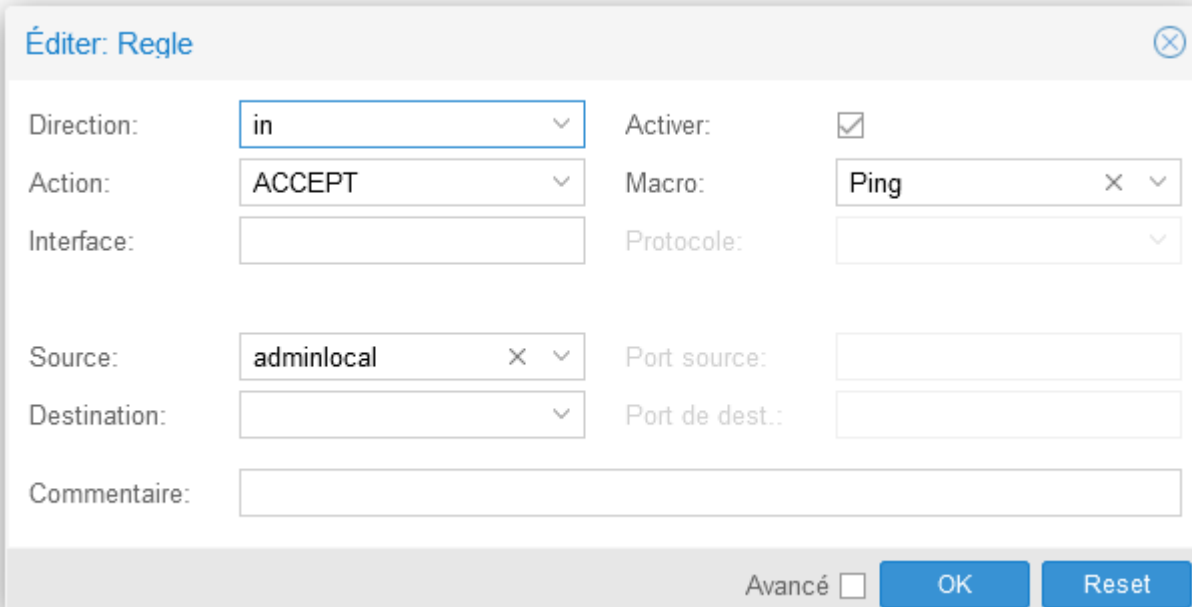
Juste pour l'exemple, on peut ajouter une plage d'adresse IP avec le CIDR (ici /24), une adresse IP, un alias.

Lors de la création d'une règle on peut utiliser un IPSet en Source.

8-Règles pour une machine virtuelle ou un conteneur

Exemple pour autoriser le ping (protocole ICMP).

On sélectionne la machine ==> **Parefeu** ==> **[Ajouter]**



Éditer: Règle

Direction: Activer:

Action: Macro:

Interface: Protocole:

Source: Port source:

Destination: Port de dest.:

Commentaire:

Avancé

Saisir les paramètres, j'utilise la macro **Ping**, ne pas oublier de cocher **Activer**.

Comme source, j'ai mis l'alias **adminlocal** qui correspond à l'IP de mon PC sur le réseau local.

En lignes de commande

Les fichiers que l'on crée pour les machines se trouvent dans **/etc/pve/firewall**

On peut les afficher sans les modifier avec la commande **cat nom_du_fichier**.

En console, il est possible de désactiver le pare-feu.

Éditez le fichier de configuration **/etc/pve/firewall/cluster.fw** et remplacez la valeur **1** par **0**.

```
[OPTIONS]
enable: 1
```

Plus d'informations

<https://pve.proxmox.com/wiki/Firewall>

<https://blog.waccabac.com/gestion-du-pare-feu-de-proxmox-ve-4/>

<https://doc.ataxya.net/books/proxmox-ve/page/securisation-basique-de-son-proxmox>

Mis à jour le 19/03/2023