

Parefeux sous OMV

Direction	Action	Famille	Source	Port	Destina...	Port	Proto...	Options supplémentaires	Commentaire
INPUT	ACCEPT	IPv4	-	-	-	-	Tous	-i lo	Autoriser le trafic local
OUTPUT	ACCEPT	IPv4	-	-	-	-	Tous	-o lo	Autoriser le trafic local
INPUT	ACCEPT	IPv4	-	-	-	-	Tous	-m conntrack --ctstate ESTABLISHED,RELATED	Conservier les connexions déjà établies
INPUT	ACCEPT	IPv4	192.168.1.2	-	-	-	Tous		Accès total à partir d'un poste particulier
INPUT	ACCEPT	IPv4	192.168.1.0/24	-	-	-	ICMP		PING en local
INPUT	ACCEPT	IPv4	192.168.1.0/24	-	-	5000	TCP		Accès à OpenMediaVault
INPUT	ACCEPT	IPv4	-	-	-	22	TCP		Autoriser SSH
INPUT	ACCEPT	IPv4	-	-	-	80	TCP		Autoriser HTTP
INPUT	ACCEPT	IPv4	-	-	-	443	TCP		Autoriser HTTPS
INPUT	ACCEPT	IPv4	-	-	-	137	UDP		Samba : NetBIOS Name Service
INPUT	ACCEPT	IPv4	-	-	-	138	UDP		Samba : NetBIOS Datagram Service
INPUT	ACCEPT	IPv4	-	-	-	139	TCP		Samba : NetBIOS Session Service
INPUT	ACCEPT	IPv4	-	-	-	445	TCP		Samba : SMB/CIFS Service
INPUT	ACCEPT	IPv4	-	-	-	53	UDP		DNS
INPUT	ACCEPT	IPv4	-	-	-	53	TCP		DNS
INPUT	DROP	IPv4	-	-	-	-	Tous		Interdire tout ce qui n'est pas autorisé

Configuration du pare-feu sur OMV:

La configuration du pare-feu se fait dans Système / Réseau / Pare-feu.

Rappel(exemple) : Réseau local 192.168.1.0/24 - IP du Nas 192.168.1.18.

Ci-dessous, vous trouverez un réglage de base du pare-feu. Nous étendrons les règles par la suite. Vérifiez bien vos règles (lignes) avant de les valider. Une erreur peut provoquer le verrouillage de la machine

- Règle 1 : On autorise le loopback en entrée
- Règle 2 : On autorise le loopback en sortie
- Règle 3 : On conserve les connexions établies en entrée
- Règle 4 : On donne tous les accès au PC utilisé par la configuration d'OMV (IP de mon poste : 192.168.1.2). On pourra supprimer cette ligne quand on sera certain d'avoir bien vérifié toutes les règles du firewall.
- Règle 5 : On autorise le PING (protocole ICMP) à partir de toute machine du réseau local.
- Règle 6 : On autorise l'accès à OMV à partir de toute machine du réseau local (port 80 remplacé par 5000)
- Règle 7 : On autorise l'accès en SSH à partir de toute machine du réseau local dans Système / Administration Web)
- Règle 8 et 9 : On autorise les requêtes HTTP et HTTPS si on a conservé l'accès sur les ports 80 et 443 pour un serveur web
- Règle 10 à 13 : On autorise le partage de fichier SAMBA
- Règle 14 et 15 : On autorise les requêtes DNS (port 53 en TCP et UDP)
- Règle 16 : On interdit tout le reste (ce qui n'est pas autorisé)

La règle 1 est prioritaire sur la règle 2, la 2 sur la 3 et ainsi de suite.

ACCEPT permet d'accepter un paquet si la règle est vérifiée DROP rejette un paquet sans message d'erreur si la règle est vérifiée REJECT rejette avec un retour d'un message d'erreur à l'expéditeur si la règle est vérifiée

ATTENTION : Pour les deux premières règles (Ne pas casser les connexions établies), une ancienne

Last
update:
2025/01/11 07:12 start:raspberrry:nas:firewall <https://magenealogie.chanterie37.fr/www/fablab37110/doku.php?id=start:raspberrry:nas:firewall&rev=1736575928>

configuration avec l'état “-state RELATED” est toujours sur internet, or cette option peut permettre l'ouverture de port non désirée sur votre machine par un attaquant. L'option “RELATED” est à utiliser avec prudence (source <https://doc.ubuntu-fr.org/iptables>).

From:
<https://magenealogie.chanterie37.fr/www/fablab37110/> - **Castel'Lab le Fablab MJC de Château-Renault**

Permanent link:
<https://magenealogie.chanterie37.fr/www/fablab37110/doku.php?id=start:raspberrry:nas:firewall&rev=1736575928>

Last update: **2025/01/11 07:12**

