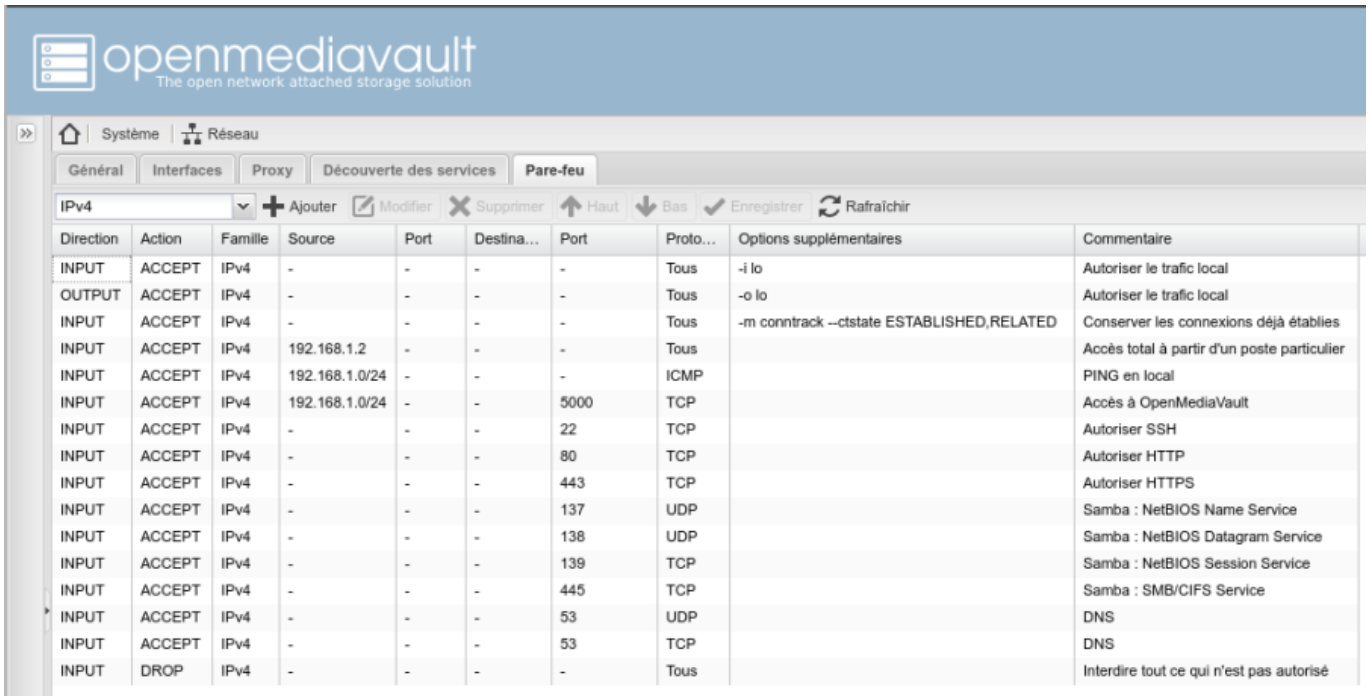
Parefeux sous OMV



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	Conserver 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 : Ontorise 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

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).

MISE À JOUR

La mise à jour permanente des paquets (logiciels) du Nas est la condition sine qua none d'une bonne sécurité. Elle est à faire régulièrement (une fois par semaine, voire quotidiennement dans le cas d'une vague de cyberattaques).

Cette mise à jour du système se fait dans Système/Update Management/Mises à jour. Il faut cocher l'ensemble des paquets et faire une Mise à niveau.

CONCLUSION

À ce stade, le NAS est accessible de façon sécurisée.

Il faudra ajouter des règles au pare-feu pour chaque nouveau service installé. Par exemple lors de l'installation de SAMBA pour le partage des fichiers (principale fonction d'un Nas).

On pourra renforcer la sécurité par la suite en :

- privilégiant l'accès au portail en HTTPS
- installant un antivirus
- désactivant le compte admin pour donner l'administration à un utilisateur dont l'identifiant sera plus neutre
- bloquant les tentatives infructueuses de connexion après un certain nombre d'échecs (via le pare-feu)

Doc Firewall OMV

Pare-feu

Cette table de données permet d'ajouter des règles iptables. Cela peut être utile si vous devez sécuriser l'accès à votre réseau local. Actuellement, il est uniquement possible d'ajouter des règles aux chaînes OUTPUT et INPUT dans la table de filtrage. La configuration pour charger les règles au démarrage ou au redémarrage du réseau est effectuée par l'unité systemd appelée openmediavault-firewall .

Conseil

- Pour éviter de vous retrouver bloqué pendant les tests, créez une commande cron à exécuter toutes les cinq minutes qui vide la chaîne OUTPUT/INPUT. N'oubliez pas de supprimer la tâche cron après le test :

```
/*/5 * * * * root /sbin/iptables -F INPUT && /sbin/iptables -F OUTPUT
```

- Avant d'ajouter la dernière règle pour tout rejeter, ajoutez une règle avant de tout rejeter, pour tout enregistrer. Cela vous aidera à comprendre pourquoi certaines règles ne fonctionnent pas. Le journal est enregistré dans dmesg ou syslog.

Conseil

Lorsque vous recherchez de l'aide, évitez de publier des captures d'écran du tableau de données. Cela est inutile car cela ne donne pas un aperçu complet de votre ensemble de règles de pare-feu. Utilisez plutôt :

```
$ iptables-save > /tmp/file.txt
```

From:
http://chanterie37.fr/fablab37110/ - **Castel'Lab le Fablab MJC de Château-Renault**

Permanent link:
http://chanterie37.fr/fablab37110/doku.php?id=start:raspberry:nas:firewall&rev=1736576374

Last update: **2025/01/11 07:19**