

260823-Le réglage du pare-feu Portmaster

Portmaster — la découverte réseau et le NAS maison

Poste `julie` (`DESKTOP-B7J2KGP`), Windows 10. Installation de **Safing Portmaster 2.2.1** le **22/08/2026 à 10:58**, réglage le **23/08/2026**.

Portmaster est un pare-feu applicatif qui s'insère au niveau **WFP** via son pilote `portmaster-kext.sys`. Il **double** le pare-feu Windows et c'est lui qui tranche : inutile d'aller chercher du côté de Defender.

Élément	Valeur
Version	2.2.1 (éditeur <code>safing</code>)
Service	<code>PortmasterCore</code> , démarrage automatique
Binaires	<code>C:\Program Files\Portmaster</code>
Données et journaux	<code>C:\ProgramData\Portmaster</code>
API locale	<code>http://127.0.0.1:817</code>

1. Le symptôme, et ce qui n'était pas en cause

Plus aucune découverte réseau sur le poste : le NAS Synology maison (`192.168.1.17`, `\\NASMAISON`) n'apparaissait plus dans le volet **Réseau** de l'Explorateur.

Le premier réflexe — soupçonner le réseau ou le NAS — était **faux**. Tout répondait :

Contrôle	Résultat
Poste	192.168.1.26/24, passerelle et DNS 192.168.1.1
Ping 192.168.1.17	répond
MAC du NAS	00-11-32-9C-8E-C9 — OUI Synology
Ports TCP	445, 139, 22, 80 ouverts (5000/5001 fermés)
Résolution du nom	NASMAISON → NASMAISON.local = 192.168.1.17, par mDNS
Lecteur A: → \\NASMAISON\foxy	monté et lisible, 55 entrées

Leçon : l'accès n'a jamais été rompu, seule la découverte l'était. Distinguer les deux dès le départ fait gagner beaucoup de temps.

Détail annexe, non symptomatique : \\192.168.1.17\foxy échoue alors que \\NASMAISON\foxy fonctionne. L'identifiant Windows est enregistré sous la cible NASMAISON (utilisateur juxjux), pas sous l'adresse IP — comportement normal de cmdkey.

2. Le diagnostic

La preuve est dans le journal de Portmaster, C:\ProgramData\Portmaster\logs\2026-08-22_10-57-46.log :

```
2026-08-23 07:12:50 filter: connection AUTORITE NT\SERVICE LOCAL:
C:\Windows\System32\svchost.exe:12184 <- 192.168.1.17
dropped: inbound connections blocked
```

svchost.exe PID 12184 héberge le service SSDPSRV (Découverte SSDP) — identifié par Get-CimInstance Win32_Service -Filter "ProcessId=12184".

Cadence des rejets : 05:56, 06:11, 06:26, 06:42, 06:57, 07:12 — toutes les ~15 minutes, soit exactement le rythme des annonces SSDP périodiques du NAS.

Répartition des 1 802 blocages du même motif :

Source	Occurrences	Destinataire
92.184.113.225	441	syncthing.exe
192.168.1.26 (le poste lui-même)	421	—
192.168.1.1 (Livebox)	330	—
192.168.1.17 (NAS)	249	SSDPSRV
192.168.1.19	153	—

Source	Occurrences	Destinataire
IPv6 globales 2a01:cb1c:...	~80	syncthing.exe, SSDPSRV

À noter : le trafic **sortant** passait bien (287 requêtes SSDP acceptées vers 239.255.255.250:1900). Le poste interrogeait, mais les annonces du NAS, qui arrivent en **entrant non sollicité**, étaient jetées.

3. La cause

Le réglage `filter/blockInbound` — « Force Block Incoming Connections » — **activé par défaut** à l'installation.

Sa propre description est sans ambiguïté : « *Is stronger than Rules* ». Aucune règle entrante ne peut le contourner, ce qui explique qu'aucun réglage fin ne suffisait tant qu'il restait coché.

État des réglages liés au moment du diagnostic :

Clé	Valeur	Rôle
<code>filter/blockInbound</code>	<code>True</code> (défaut)	la cause
<code>filter/defaultAction</code>	<code>permit</code> (défaut)	action si aucune règle ne correspond
<code>filter/serviceEndpoints</code>	<code>[]</code>	Incoming Rules, vides
<code>filter/blockLAN</code>	<code>False</code> (défaut)	non impliqué

4. La configuration retenue

Incoming Rules, **dans cet ordre impératif** :

Ordre	Menu	Champ
1	Allow	Localhost
2	Allow	LAN
3	Block	*

puis **décocher** *Force Block Incoming Connections*.

Localhost, LAN et Internet sont des **mots-clés de portée** reconnus par Portmaster, au même titre qu'une adresse ou un CIDR. Les utiliser vaut mieux que d'écrire 192.168.1.0/24 : la portée suit

le réseau, la règle ne devient jamais caduque.

Variante resserrée

Si l'on veut n'ouvrir que le strict nécessaire à la découverte, plutôt que tout le LAN — cela laisse notamment les partages administratifs C\$, D\$, E\$ et le RPC fermés y compris depuis le réseau local :

Menu	Champ	Rôle
Allow	Localhost	boucle locale
Allow	LAN UDP/1900	SSDP — les annonces du NAS
Allow	LAN UDP/3702	WS-Discovery
Allow	LAN TCP/5357	WSDAPI, l'échange qui construit l'icône
Block	*	tout le reste

Pour Syncthing en direct sur le LAN, ajouter avant le Block : LAN TCP/22000 , LAN UDP/22000 , LAN UDP/21027 .

5. Les pièges — à ne pas redécouvrir

1. Incoming Rules est invisible en mode Simple. filter/serviceEndpoints est de niveau expert (ExpertiseLevel 1), tandis que filter/endpoints (Outgoing Rules) est de niveau user — d'où l'impression trompeuse que seules les règles sortantes existent. Basculer l'interface sur Advanced Interface : sélecteur en haut à droite de la fenêtre, ou Settings → User Interface → UI Mode. Les réglages masqués restent actifs.

2. Ne jamais taper le + ou le - dans le champ de la règle. Le menu Allow/Block fournit déjà le signe. Saisir + LAN produit ++ LAN et déclenche :

```
Invalid Value: validation of filter/serviceEndpoints failed:
entry #1 did not match validation regex
```

La regex de validation est :

```
^(\\+|\\-) (! +)?[A-z0-9\\.\\:\\-\\*/]+( [A-z0-9\\*]+(/[A-z0-9]+(\\-[A-z0-9\\+])?)?)?( +#.\\*)?
```

Le `+` n'appartient pas à la classe de caractères qui suit le signe. La syntaxe `+ LAN / - *` est celle du **fichier de configuration**, pas de l'interface graphique.

3. `Block *` sans `Allow Localhost` au-dessus casse la boucle locale. Constaté en direct :

```
07:43:31 firefox.exe <- 127.0.0.1 dropped: denied by rule: matches *
07:43:18 syncthing.exe <- 127.0.0.1 changed from accepted to dropped
07:43:18 steam.exe <- 127.0.0.1 changed from accepted to dropped
07:43:18 dasHost.exe <- ::1 changed from accepted to dropped
```

L'interface Syncthing sur `127.0.0.1:8384` est tombée en timeout. Portmaster **ré-évalue les connexions déjà établies** et les coupe à chaud. Sur une machine de travail, une grande part du trafic légitime passe par la boucle locale.

Piège dans le piège : **l'API de Portmaster s'auto-exempte** et continue de répondre — elle ne sert donc pas de témoin pour détecter la panne.

4. L'ordre des règles fait tout. Évaluation de haut en bas, la première correspondance l'emporte. `Block *` doit être la **dernière** ligne. Les flèches à gauche de chaque ligne permettent de réordonner.

5. `filter/defaultAction` vaut `permit`. Une liste de règles sans `Block *` final **n'est pas restrictive** : tout ce qui ne correspond à aucune règle est autorisé. Décocher *Force Block Incoming* sans poser ce garde-fou ouvre la machine — point critique compte tenu de l'IPv6 (section 6).

6. L'API locale ment par omission. `GET http://127.0.0.1:817/api/v1/config/options` répond à n'importe quel processus, mais ne renvoie que les **définitions et les valeurs par défaut** : le champ `Value` reste vide même pour un réglage effectivement modifié, ce qui fait croire à tort que rien n'a été enregistré. Les endpoints qui exposent l'état réel (`/api/v1/sync/settings/export`) répondent :

```
403 The requesting process is not authorized to access the Portmaster API.
```

Vérifier par le journal, jamais par l'API.

7. Le profil réseau Windows n'a pas eu à être modifié. Il est resté sur **Public** et la découverte fonctionne. L'hypothèse initiale — passer en Privé et redémarrer `FDResPub` et `upnphost` — s'est révélée inutile. Ne pas y consacrer de temps.

6. IPv6 — le point de sécurité

Ce poste possède des adresses **IPv6 globales routables** : `2a01:cb1c:833b:d00:4958:51b1:629a:a6b4` et `2a01:cb1c:833b:d00:28cb:cac8:3621:d7d0` (préfixe Orange, obtenu par *Router Advertisement*).

En IPv6 il n'y a pas de NAT. La Livebox ne fait pas écran comme en IPv4 : Portmaster est la seule barrière. Ce que le poste expose au réseau :

Port	Processus
445	SMB — partages <code>ADMIN\$</code> , <code>C\$</code> , <code>D\$</code> , <code>E\$</code> , <code>IPC\$</code>
135 + 49664-49675	RPC (<code>lsass</code> , <code>wininit</code> , <code>spoolsv</code> , <code>services</code>)
5357	WSDAPI
22000	Syncthing
27036	Steam

La portée `LAN` **ne couvre pas** ces adresses globales — elles sont classées `Global`, pas `LAN`. Le `Block *` les refuse donc, ce qui est le comportement voulu.

Conséquence assumée : les liens **Syncthing directs en IPv6 restent bloqués**. Sans impact aujourd'hui, la synchronisation passant par le hub VPS (`syncthing-vps`, `tcp-client` vers `51.77.141.54:22000`). Pour les rétablir, ajouter `2a01:cb1c:833b:d00::/64` au-dessus du `Block *` — en sachant que **ce préfixe peut changer au redémarrage de la Livebox** et rendre la règle caduque sans le moindre signal.

7. Vérification

État constaté après réglage :

Portée	Verdict
<code>127.0.0.1 / ::1</code>	accepté — <code>scope matches Localhost</code>
LAN (<code>192.168.1.x</code> , <code>fe80::</code>)	accepté — <code>scope matches LAN</code> , 8 acceptations NAS, zéro rejet
IPv6 globales <code>2a01:cb1c:...</code>	rejeté — <code>denied by rule: matches *</code>

- Interface Syncthing `127.0.0.1:8384` : **HTTP 200**
- `A:` → `\\NASMAISON\foxy` : accessible, 55 entrées
- `fdPHost`, `SSDPSRV`, `FDResPub`, `upnphost` : les quatre `Running`

Commande de contrôle, à relancer si le NAS redisparaît :

```
grep "192.168.1.17" /c/ProgramData/Portmaster/logs/*.log | tail -20
```

Attendu :

```
svchost.exe:12184 <- 192.168.1.17  accepted: allowed by rule: scope matches LAN
dasHost.exe:3608  to nasmaison. (192.168.1.17)  accepted
```

dasHost.exe est le *Device Association Host* : le voir dialoguer avec nasmaison., c'est littéralement l'icône du NAS en train de se construire dans l'Explorateur.

Si l'on lit dropped: inbound connections blocked, c'est que *Force Block Incoming Connections* a été réactivé.

8. Chronologie

Horodatage	Événement
22/08 10:58	Installation de Portmaster 2.2.1
22/08 → 23/08	Découverte réseau muette, ~1 800 blocages entrants silencieux
23/08 ~05:45	Diagnostic : NAS joignable, seule la découverte est cassée
23/08 ~07:30	Cause identifiée — filter/blockInbound et les annonces SSDP
23/08 07:41	Allow LAN posé, Force Block Incoming décoché → NAS visible
23/08 07:43	Block * ajouté → boucle locale coupée , Syncthing GUI en timeout
23/08 07:45	Allow Localhost ajouté en tête → état final correct
23/08 07:46	Vérification des trois niveaux, conforme

9. Références

- CLAUDE.md — section « Portmaster (pare-feu applicatif) sur julie », insérée le 23/08/2026
- Journal Portmaster : C:\ProgramData\Portmaster\logs\
- Aide intégrée à Portmaster : la syntaxe complète des règles (portées, domaines, pays, AS, listes de filtrage, protocoles et ports) est dans l'infobulle des champs *Outgoing Rules* et *Incoming Rules*