

Mettre en place des règles via Pfsense.

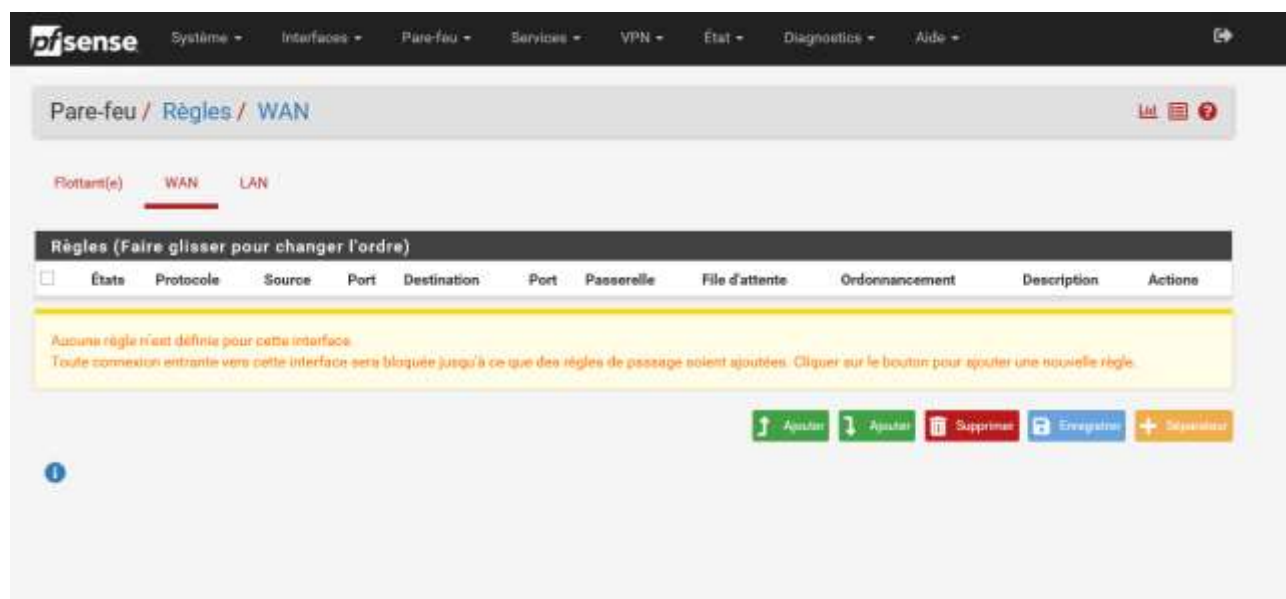
Table des matières

1. Les règles globales :	2
2. Les règles fines :	8

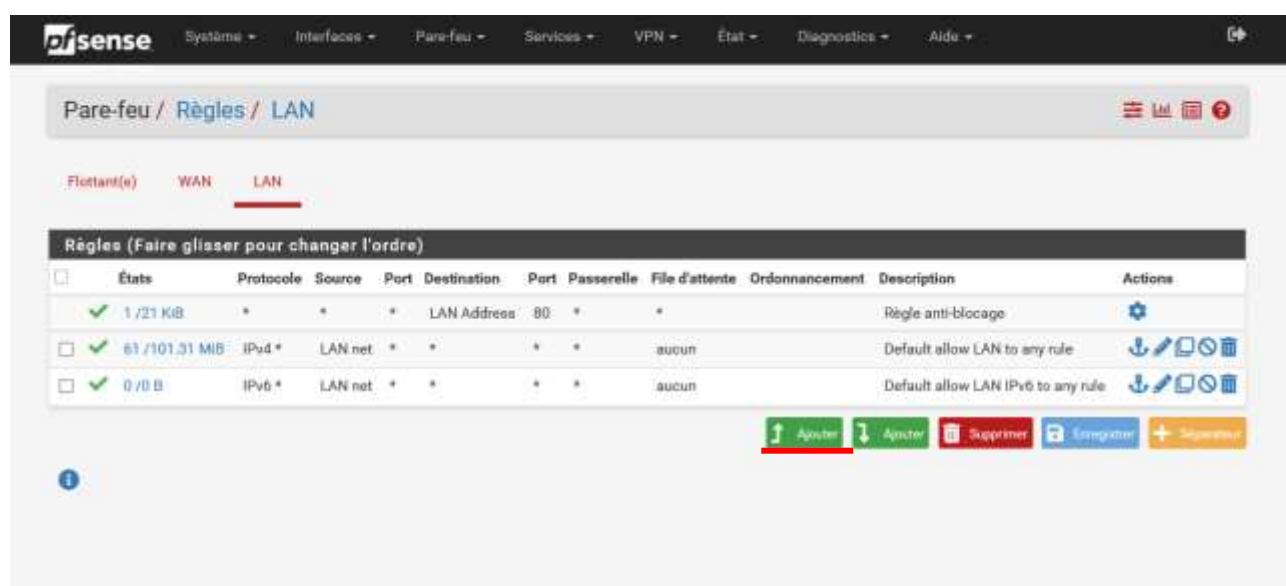
1. Les règles globales :

Vous pouvez définir les règles directement depuis le shell du système d'exploitation du pare-feu mais vous pouvez aussi le faire depuis l'interface graphique par le biais du webconfigurator que ce soit pour Pfsense ou bien Ipfire.

Nous allons mettre en place une règle générale simple qui permettra d'interdire le trafic sur les ports TCP et UDP en dehors du réseau local cela permettra d'interdire la navigation internet.



Le réseau WAN ne comporte aucune règle par défaut, nous allons configurer une nouvelle règle pour le réseau LAN qui lui comporte 3 règles par défaut.



Sélectionnez le réseau pour lequel vous souhaitez mettre en place une règle en l'occurrence le **réseau local (LAN)** et faites **Ajouter** pour créer une nouvelle règle.

Pare-feu / Règles / Modifier

Modifier la règle de Pare-Feu

Action	Autoriser Bloquer Rejeter
Désactivé	<input type="checkbox"/> Désactiver cette règle Choisissez cette option pour désactiver cette règle sans la supprimer de la liste.
Interface	LAN Choisissez l'interface d'où les paquets doivent provenir pour correspondre à cette règle.
Famille d'adresse	IPv4 Choisissez la version du protocole IP à laquelle cette règle s'applique.
Protocole	TCP Choisissez quel protocole IP cette règle devrait correspondre.

Aide : La différence entre bloquer et rejeter est qu'avec 'Rejeter', un paquet (TCP, RST ou ICMP port unreachable pour UDP) est retourné à l'expéditeur, alors qu'avec 'Bloquer', le paquet est supprimé silencieusement. Dans tous les cas, le paquet est supprimé.

Vous devez maintenant spécifier la règle à l'aide de la sémantique habituelle des pare-feu à savoir sur Pfsense :

- Autoriser le trafic
- Bloquer le trafic
- Rejeter le trafic (idem que bloquer mais avec suppression discrète du paquet interdit)

Mettez en place une règle de blocage sur l'interface LAN pour les protocoles TCP et UDP par exemple.

Pare-feu / Règles / Modifier

Modifier la règle de Pare-Feu

Action	Bloquer Choisissez que faire des paquets qui correspondent aux critères ci-dessous. Aide : La différence entre bloquer et rejeter est qu'avec 'Rejeter', un paquet (TCP, RST ou ICMP port unreachable pour UDP) est retourné à l'expéditeur, alors qu'avec 'Bloquer', le paquet est supprimé silencieusement. Dans tous les cas, le paquet est supprimé.
Désactivé	<input type="checkbox"/> Désactiver cette règle Choisissez cette option pour désactiver cette règle sans la supprimer de la liste.
Interface	LAN Choisissez l'interface d'où les paquets doivent provenir pour correspondre à cette règle.
Famille d'adresse	IPv4 Choisissez la version du protocole IP à laquelle cette règle s'applique.
Protocole	TCP/UDP Tous TCP UDP ICMP ESP AH GRE EoIP IPv6 IGMP PIM OSPF SCTP CARP PFSYNC
Source	Source Source Address

Presque jamais égale au port de destination. Dans la plupart des cas, ce

La règle suivante va permettre de bloquer toutes les connexions TCP et UDP entrantes et sortantes à partir du réseau local depuis n'importe quelles adresses IPv4 situées en dehors du réseau LAN.

Pare-feu / Règles / Modifier

Modifier la règle de Pare-Feu

Action Bloquer

Choisissez que faire des paquets qui correspondent aux critères ci-dessous:
Aide : La différence entre bloquer et rejeter est qu'avec 'Rejeter', un paquet (TCP, RST ou ICMP port unreachable pour UDP) est retourné à l'expéditeur, alors qu'avec 'Bloquer', le paquet est supprimé silencieusement. Dans tous les cas, le paquet est supprimé.

Désactiver ☐ Désactiver cette règle

Choisissez cette option pour désactiver cette règle sans la supprimer de la liste.

Interface LAN

Choisissez l'interface d'où les paquets doivent provenir pour correspondre à cette règle.

Famille d'adresse IPv4

Choisissez la version du protocole IP à laquelle cette règle s'applique.

Protocole TCP/UDP

Choisissez quel protocole IP cette règle devrait correspondre.

Dans une deuxième partie le pare-feu vous demande de préciser les **sources** et **destinations** concernant les flux que vous souhaitez autoriser ou interdire.

Source

Source ☐ Invert match

[Afficher les options avancées](#)

La plage de ports source d'une règle doit rester à sa valeur par défaut.

Destination ☐ Invert match

Plage de port de destination (autre)

Do: Personnalisé(e) À: Personnalisé(e)

Spécifiez le port destination ou la plage de port pour cette règle. Le champ « À » peut rester vide seulement si le filtre est sur un seul port.

Source Address: /

Destination Address: /

tout
Hôte ou alias unique
Réseau
Clients PPPoE
Clients L2TP
WAN net
WAN address
LAN net
LAN address

Vous pouvez spécifier des adresses réseaux ou bien aussi directement des plages de postes ou des postes en particulier, la syntaxe varie suivant le logiciel mais reste globalement similaire dans son ensemble.

Dans l'exemple ci-dessous, l'ensemble du réseau LAN est bloqué au niveau du trafic entrant et sortant à destination de n'importe quel autre poste en dehors du réseau LAN pour les protocoles TCP et UDP.

Source

Source ☐ Invert match LAN net Source Address /

[Afficher les options avancées](#)

La plage de ports source d'une connexion est généralement aléatoire et presque jamais égale au port de destination. Dans la plupart des cas, ce paramètre doit rester à sa valeur par défaut, any.

Destination

Destination ☐ Invert match tout Destination Address /

Plage de port de destination

De tout À tout

Personnalisé(e) Personnalisé(e)

Spécifiez le port destination ou la plage de port pour cette règle. Le champ « A » peut rester vide seulement si le filtre est sur un seul port.

Options additionnelles

Journalise ☐ Journaliser les paquets gérés par cette règle

Suggestion : Le pare-feu a un espace de journalisation limité. N'activez pas la journalisation de tout. Si vous faites beaucoup de journalisation considérez l'utilisation d'un serveur syslog distant (voir la page Statut : Journaux système : Paramètres).

Description

Une description est proposée ici pour aider l'administrateur. Un maximum de 52 caractères sera utilisé dans l'ensemble de règles et affiché dans le journal du pare-feu.

Options Avancées [Afficher les options avancées](#)

La nouvelle règle étant établie, appliquez les modifications afin que la règle soit prise en compte, parfois un certain temps est nécessaire avant la prise en compte du changement.

Pare-feu / Règles / LAN

La configuration de la règle de pare-feu a été modifiée. Ces modifications doivent être appliquées pour prendre effet. [✓ Appliquer les modifications](#)

Flottant(e) WAN LAN

Règles (Faire glisser pour changer l'ordre)

	États	Protocole	Source	Port	Destination	Port	Passerelle	File d'attente	Ordonnement	Description	Actions
<input checked="" type="checkbox"/>	2 / 163 KIB	*	*	*	LAN Address	80	*	*		Règle anti-blocage	
<input type="checkbox"/>	0 / 0 B	IPv4 TCP/UDP	LAN net	*	*	*	*	aucun			
<input type="checkbox"/>	44 / 105.35 MIB	IPv4 *	LAN net	*	*	*	*	aucun		Default allow LAN to any rule	
<input type="checkbox"/>	0 / 0 B	IPv6 *	LAN net	*	*	*	*	aucun		Default allow LAN IPv6 to any rule	

[Ajouter](#) [Ajouter](#) [Supprimer](#) [Enregistrer](#) [Réinitialiser](#)

Pare-feu / Règles / LAN

Les modifications ont été appliquées avec succès. Les règles du pare-feu sont en cours de rechargement en arrière-plan.
[Surveiller](#) le rechargement des filtres.

Flottant(e) WAN LAN

Règles (Faire glisser pour changer l'ordre)

	État	Protocole	Source	Port	Destination	Port	Passerelle	File d'attente	Ordonnement	Description	Actions
<input type="checkbox"/>	✓ 2 / 174 KB	*	*	*	LAN Address	80	*	*		Règle anti-blocage	
<input type="checkbox"/>	✗ 0 / 0 B	IPv4 TCP/UDP	LAN net	*	*	*	*	aucun			
<input type="checkbox"/>	✓ 25 / 115.20 MB	IPv4 *	LAN net	*	*	*	*	aucun		Default allow LAN to any rule	
<input type="checkbox"/>	✓ 0 / 0 B	IPv6 *	LAN net	*	*	*	*	aucun		Default allow LAN IPv6 to any rule	

↑ Ajouter ↓ Ajouter Supprimer Suspendre + Supprimer

Si la règle s'exécute correctement, il devrait être impossible de lancer la navigation internet depuis le serveur ou n'importe quel autre poste du réseau LAN.

Nous ne pouvons pas accéder à cette page

- Vérifier que l'adresse web <https://www.msn.com> est correcte
- [Rechercher ce site sur Bing](#)
- [Actualiser la page](#)

⌵ Informations

Résoudre les problèmes de connexion

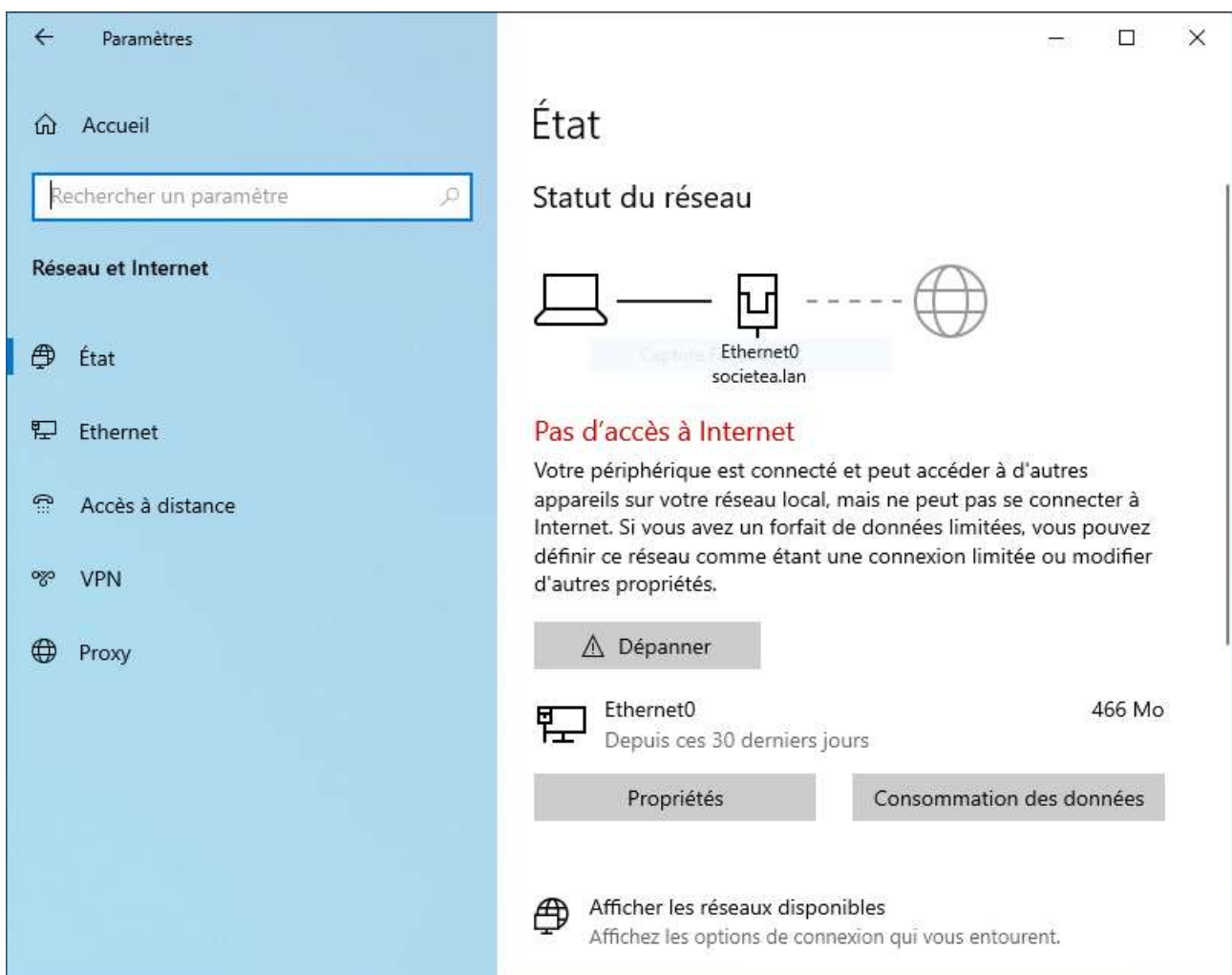
Le serveur en revanche est bien toujours connecté au réseau WAN, ce sont les protocoles TCP et UDP qui ont été bloqués.

```
Administrateur : Windows PowerShell
PS C:\Users\Administrateur> ping 1.1.1.1

Envoi d'une requête 'Ping' 1.1.1.1 avec 32 octets de données :
Réponse de 1.1.1.1 : octets=32 temps=74 ms TTL=127
Réponse de 1.1.1.1 : octets=32 temps=74 ms TTL=127
Réponse de 1.1.1.1 : octets=32 temps=83 ms TTL=127
Réponse de 1.1.1.1 : octets=32 temps=73 ms TTL=127

Statistiques Ping pour 1.1.1.1:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 73ms, Maximum = 83ms, Moyenne = 76ms
PS C:\Users\Administrateur>
```

Depuis un poste client, la connexion à Internet semble être coupée.



2. Les règles fines :

La règle de blocage de l'ensemble du flux depuis et vers le réseau local est une règle globale qui doit donc se placer vers la fin de la liste car sinon elle sera lue dès le début puis exécuter et les règles fines ne seront tout simplement pas lues et donc exécutées.

Une règle fine pourrait être par exemple d'autoriser un poste en particulier à avoir un trafic entrant et sortant en dehors du LAN, dans ce cas-là, la règle doit se placer devant les règles globales (il s'agit d'une exception aux règles globales).

Créer une nouvelle règle autorisant un poste client à avoir un flux TCP et UDP entrant et sortant à destination de n'importe quel réseau.

Pare-feu / Règles / Modifier

Modifier la règle de Pare-Feu

Action : Autoriser
Choisissez que faire des paquets qui correspondent aux critères ci-dessous.
Aide : La différence entre bloquer et rejeter est qu'avec 'Rejeter', un paquet (TCP, RST ou ICMP port unreachable pour UDP) est retourné à l'expéditeur, alors qu'avec 'Bloquer', le paquet est supprimé silencieusement. Dans tous les cas, le paquet est supprimé.

Désactivé : ☐ Désactiver cette règle
Choisissez cette option pour désactiver cette règle sans la supprimer de la liste.

Interface : LAN
Choisissez l'interface d'où les paquets doivent provenir pour correspondre à cette règle.

Famille d'adresse : IPv4
Choisissez la version du protocole IP à laquelle cette règle s'applique.

Protocole : TCP/UDP
Choisissez quel protocole IP cette règle devrait correspondre.

Spécifiez le poste client à l'aide de son adresse IP par exemple.

Source

Source : ☐ Invert match / Hôte ou alias unique / 192.168.0.37 /

Destination

Destination : ☐ Invert match / tout /

Plage de port de destination : tout /

Options additionnelles

Journaliser : ☐ Journaliser les paquets gérés par cette règle
Suggestion : Le pare-feu a un espace de journalisation limité. N'activez pas la journalisation de tout. Si vous faites beaucoup de journalisation considérez l'utilisation d'un serveur syslog distant (voir la page Statut : Journaux système : Paramètres).

Description :
Une description est proposée ici pour aider l'administrateur. Un maximum de 52 caractères sera utilisé dans l'ensemble de règles et affiché dans le journal du pare-feu.

Pare-feu / Règles / LAN

La configuration de la règle de pare-feu a été modifiée. Ces modifications doivent être appliquées pour prendre effet. ✓ Appliquer les modifications

Flottant(e) WAN LAN

Règles (Faire glisser pour changer l'ordre)

	États	Protocole	Source	Port	Destination	Port	Passerelle	File d'attente	Ordonnancement	Description	Actions
<input type="checkbox"/>	✓ 1 / 47 Kio	*	*	*	LAN Address	80	*	*		Règle anti-blocage	
<input type="checkbox"/>	✓ 0 / 0 B	IPv4 TCP/UDP	192.168.0.37	*	*	*	*	aucun			
<input type="checkbox"/>	✗ 0 / 172 Kio	IPv4 TCP/UDP	LAN net	*	*	*	*	aucun			
<input type="checkbox"/>	✓ 0 / 115.71 Mio	IPv4 *	LAN net	*	*	*	*	aucun		Default allow LAN to any rule	
<input type="checkbox"/>	✓ 0 / 0 B	IPv6 *	LAN net	*	*	*	*	aucun		Default allow LAN IPv6 to any rule	

↑ Ajouter ↓ Ajouter Supprimer Enregistrer + Séparer

La nouvelle règle doit se trouver au-dessus de la règle globale afin d'être lue et appliquée par le pare-feu.

Pare-feu / Règles / LAN

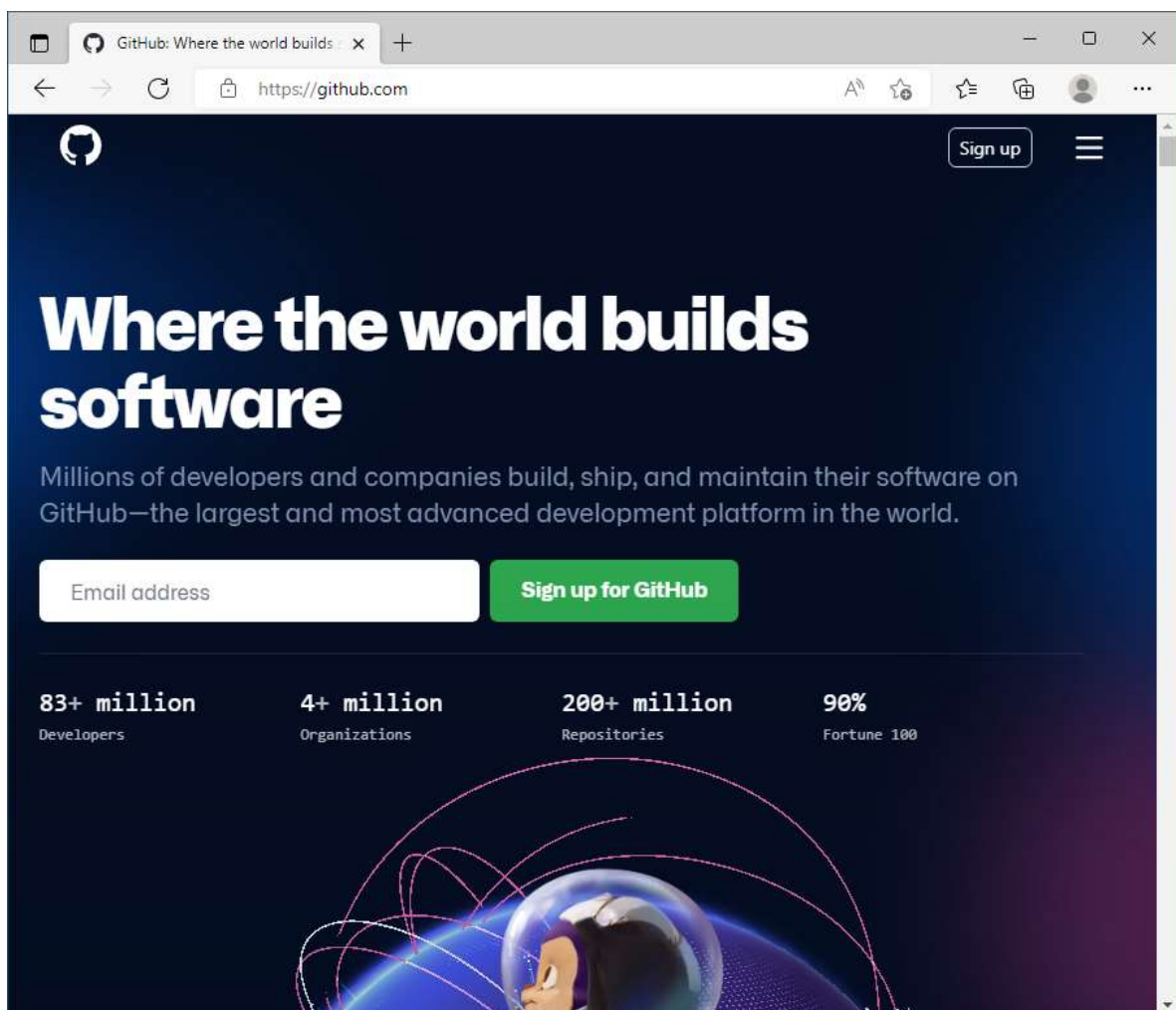
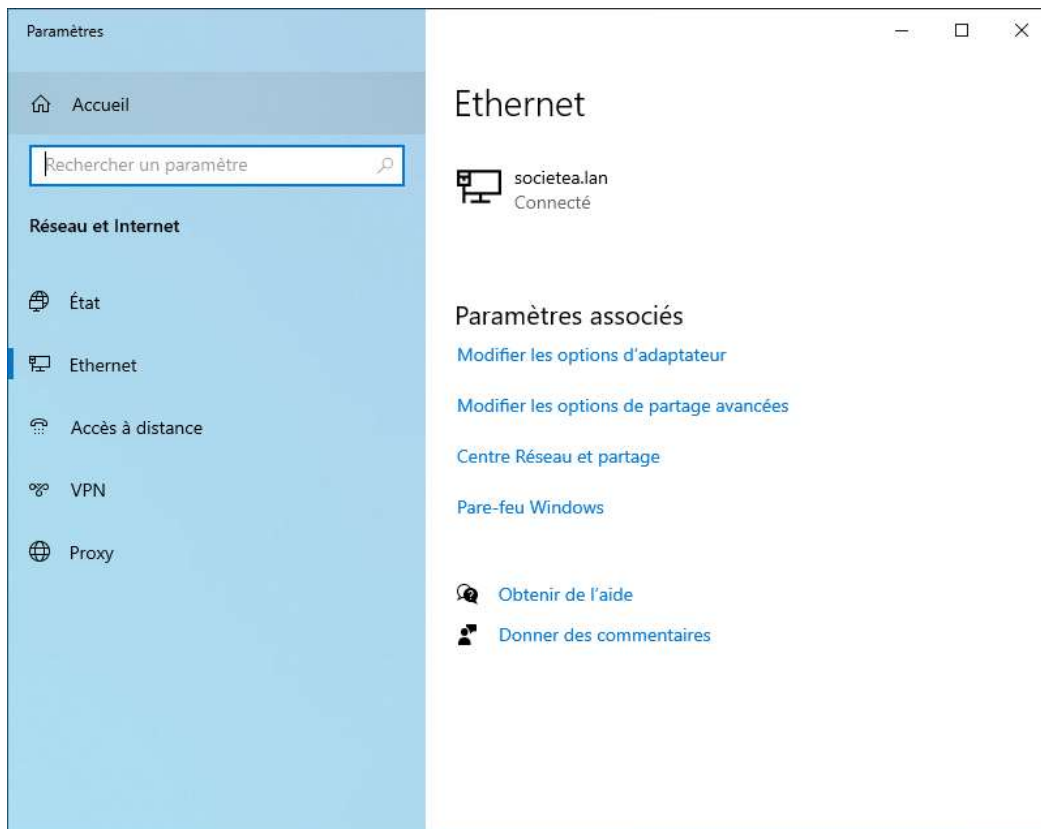
Flottant(e) WAN LAN

Règles (Faire glisser pour changer l'ordre)

	États	Protocole	Source	Port	Destination	Port	Passerelle	File d'attente	Ordonnancement	Description	Actions
<input type="checkbox"/>	✓ 0 / 70 Kio	*	*	*	LAN Address	80	*	*		Règle anti-blocage	
<input type="checkbox"/>	✓ 11 / 4.24 Mio	IPv4 TCP/UDP	192.168.0.37	*	*	*	*	aucun			
<input type="checkbox"/>	✗ 0 / 13 Kio	IPv4 TCP/UDP	LAN net	*	*	*	*	aucun			
<input type="checkbox"/>	✓ 0 / 115.71 Mio	IPv4 *	LAN net	*	*	*	*	aucun		Default allow LAN to any rule	
<input type="checkbox"/>	✓ 0 / 0 B	IPv6 *	LAN net	*	*	*	*	aucun		Default allow LAN IPv6 to any rule	

↑ Ajouter ↓ Ajouter Supprimer Enregistrer + Séparer

Après un court lap de temps, la règle devrait s'appliquer et le poste client devrait à nouveau récupérer la connexion à internet et pouvoir naviguer.



Si les clients pour lesquels vous allez mettre en place des règles spécifiques sont adressés dynamiquement, n'oubliez pas de mettre en place des réservations d'adresses IP sur le serveur DHCP sauf si les règles s'appliquent directement sur les adresses MAC des postes en question.

