

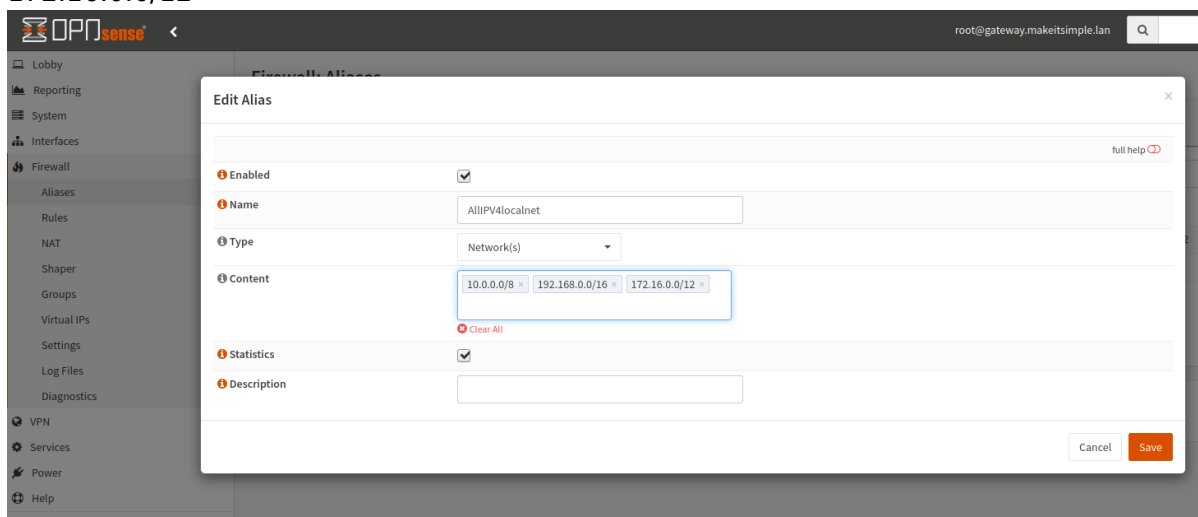
OPNSense - Règles de firewall pour un réseau invité

Créer au préalable les interfaces et le serveur DHCP

Configuration des règles

1. Dans Firewall → Aliases, nous allons d'abord créer un alias AllIPv4localnet qui va identifier tous les réseaux locaux pour les bloquer facilement. Mettez-y :

- 10.0.0.0/8
- 192.168.0.0/16
- 172.16.0.0/12



2. Dans Firewall → Rules → Guest créer les règles suivantes:

- DNS:
 - Protocol **IPv4 TCP/UDP**
 - Destination **8.8.8.8**
 - Port **53**
- HTTP:
 - Protocol **IPv4 TCP**
 - Destination **!AllIPv4localnet (AllIPv4localnet inversé)**
 - Port **80**
- HTTPS:
 - Protocol **IPv4 TCP**
 - Destination **!AllIPv4localnet (AllIPv4localnet inversé)**
 - Port **443**
- IMAP:
 - Protocol **IPv4 TCP**
 - Destination **!AllIPv4localnet (AllIPv4localnet inversé)**
 - Port **143**
- IMAPS:
 - Protocol **IPv4 TCP**
 - Destination **!AllIPv4localnet (AllIPv4localnet inversé)**
 - Port **993**

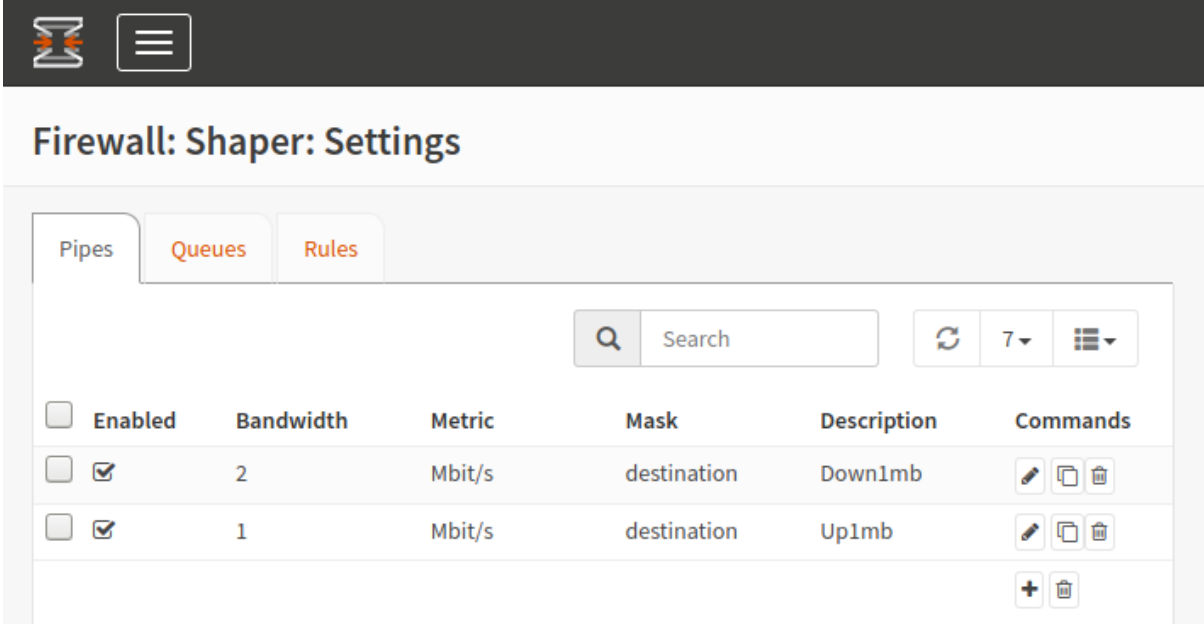
- POP3:
 - Protocol **IPv4 TCP**
 - Destination **!AllIPv4localnet (AllIPv4localnet inversé)**
 - Port **110**
- POP3S:
 - Protocol **IPv4 TCP**
 - Destination **!AllIPv4localnet (AllIPv4localnet inversé)**
 - Port **995**
- SMTP:
 - Protocol **IPv4 TCP**
 - Destination **!AllIPv4localnet (AllIPv4localnet inversé)**
 - Port **25**
- SMTPS:
 - Protocol **IPv4 TCP**
 - Destination **!AllIPv4localnet (AllIPv4localnet inversé)**
 - Port **465**
- Whatsapp1:
 - Protocol **IPv4 TCP**
 - Destination **!AllIPv4localnet (AllIPv4localnet inversé)**
 - Port **5222 - 5223**
- Whatsapp2:
 - Protocol **IPv4 TCP**
 - Destination **!AllIPv4localnet (AllIPv4localnet inversé)**
 - Port **5228**
- Teamviewer:
 - Protocol **IPv4 TCP&UDP**
 - Destination **!AllIPv4localnet (AllIPv4localnet inversé)**
 - Port **5938**
- Anydesk:
 - Protocol **IPv4 TCP**
 - Destination **!AllIPv4localnet (AllIPv4localnet inversé)**
 - Port **6568**

Firewall: Rules: LAN_GUEST Nothing selected







<input type="checkbox"/>	Protocol	Source	Port	Destination	Port	Gateway	Schedule	Description	
Automatically generated rules									
<input type="checkbox"/>	IPv4 TCP	*	*	10.0.0.232	8880	*	*		<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
<input type="checkbox"/>	IPv4 TCP/UDP	*	*	8.8.8.8	53 (DNS)	*	*	DNS	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
<input type="checkbox"/>	IPv4 TCP	*	*	!AllIPv4localnet	80 (HTTP)	*	*		<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
<input type="checkbox"/>	IPv4 TCP	*	*	!AllIPv4localnet	443 (HTTPS)	*	*		<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
<input type="checkbox"/>	IPv4 TCP	*	*	!AllIPv4localnet	143 (IMAP)	*	*		<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
<input type="checkbox"/>	IPv4 TCP	*	*	!AllIPv4localnet	993 (IMAP/S)	*	*		<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
<input type="checkbox"/>	IPv4 TCP	*	*	!AllIPv4localnet	110 (POP3)	*	*		<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
<input type="checkbox"/>	IPv4 TCP	*	*	!AllIPv4localnet	995 (POP3/S)	*	*		<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
<input type="checkbox"/>	IPv4 TCP	*	*	!AllIPv4localnet	25 (SMTP)	*	*		<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
<input type="checkbox"/>	IPv4 TCP	*	*	!AllIPv4localnet	465 (SMTP/S)	*	*		<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
<input type="checkbox"/>	IPv4 TCP	*	*	!AllIPv4localnet	5222 - 5223	*	*	Messenger and whatsapp	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
<input type="checkbox"/>	IPv4 TCP	*	*	!AllIPv4localnet	5228	*	*	Messenger and whatsapp	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>

Configuration du shaping

1. Dans Firewall → Shaper → Settings → Pipe créer
 - Une interface Down de 2Mb en mask=destination
 - Une interface Up de 1Mb en mask=destination




The screenshot shows the 'Firewall: Shaper: Settings' interface. It has three tabs: 'Pipes', 'Queues', and 'Rules'. The 'Queues' tab is active. At the top right, there is a search bar and a refresh button. Below is a table with columns: Enabled, Bandwidth, Metric, Mask, Description, and Commands. Two queues are listed: one with a bandwidth of 2 Mbit/s and description 'Down1mb', and another with a bandwidth of 1 Mbit/s and description 'Up1mb'. Both are enabled and have a mask of 'destination'.

Enabled	Bandwidth	Metric	Mask	Description	Commands
<input checked="" type="checkbox"/>	2	Mbit/s	destination	Down1mb	  
<input checked="" type="checkbox"/>	1	Mbit/s	destination	Up1mb	  

2. Dans Firewall → Shaper → Settings → Rules créer en mode advanced
 - Interface Wan / Interface 2: LAN_GUEST_PORTAL Direction IN Target Down2mb
 - Interface Wan / Interface 2: LAN_GUEST_PORTAL Direction Out Target Up1mb

Edit rule ✕

advanced mode full help 

Enabled

Sequence

Interface

Interface 2

Proto

Source ✕ Clear All

Invert source

Src-port

Destination ✕ Clear All

Invert destination

Dst-port

DSCP ✕ Clear All

Direction

Target

Description

From:
<https://wiki.makeitsimple.be/> - **makeITsimple wiki**

Permanent link:
<https://wiki.makeitsimple.be/doku.php?id=reseau:opnsense:firewall-guest&rev=1588446225>

Last update: **2021/06/20 09:42**

