

M2L - Procédure détaillée de pfSense.

Console d'administration de l'appliance pfSense :

The screenshot shows the pfSense Status Dashboard. The top navigation bar includes System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, and Help. The main content area is divided into several sections:

- System Information:**
 - Name: pfSense.home.arpa
 - User: admin@10.10.20.1 (Local Database Fallback)
 - System: pfSense, Netgate Device ID: cbd222a672ee17b659b2
 - BIOS: Vendor: LENOVO, Version: FCKT46AUS, Release Date: Mon Dec 16 2013
 - Version: 2.7.2-RELEASE (amd64), built on Mon Mar 4 20:53:00 CET 2024, FreeBSD 14.0-CURRENT. A notification indicates that version 2.8.1 is available.
 - CPU Type: Intel(R) Core(TM) i5-4430S CPU @ 2.70GHz, 4 CPUs: 1 package(s) x 4 core(s), AES-NI CPU Crypto: Yes (inactive), QAT Crypto: No
 - Hardware crypto: Inactive
 - Kernel PTI: Enabled
 - MDS Mitigation: Inactive
 - Uptime: 50 Days 17 Hours 13 Minutes 53 Seconds
 - Current date/time: Thu Apr 2 7:48:39 CEST 2026
 - DNS server(s): 127.0.0.1, 8.8.8.8
 - Last config change: Mon Mar 16 16:36:37 CET 2026
 - State table size: 0% (194/599000)
 - MBUF Usage: 2% (20828/1000000)
- Netgate Services And Support:**
 - Contract type: Community Support, Community Support Only
 - NETGATE AND pfSense COMMUNITY SUPPORT RESOURCES**
 - Text: "If you purchased your pfSense gateway firewall appliance from Netgate and elected **Community Support** at the point of sale or installed pfSense on your own hardware, you have access to various community support resources. This includes the **NETGATE RESOURCE LIBRARY**."
 - Upgrade Your Support
 - Community Support Resources
 - Netgate Global Support FAQ
 - Official pfSense Training by Netgate
 - Netgate Professional Services
 - Visit Netgate.com
 - Alert: "If you decide to purchase a Netgate Global TAC Support subscription, you **MUST** have your **Netgate Device ID (NDI)** from your firewall in order to validate support for this unit. Write down your NDI and store it in a safe place. You can purchase TAC supports [here](#)."
- Interfaces:**

Interface	Speed	Mode	IP Address
WAN	↑	100baseTX <full-duplex>	172.16.1.190
LAN	↑	100baseTX <full-duplex>	10.10.20.1
DMZPUBLIQUE	↑	1000baseT <full-duplex>	192.168.0.6
- Snort Alerts:** (Section header visible)

Adressage logique des segments WAN / LAN / DMZ :

The screenshot shows the pfSense Interface Assignments page. The top navigation bar includes System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, and Help. The main content area is titled "Interfaces / Interface Assignments" and includes a sub-navigation menu with options like Interface Assignments, Interface Groups, Wireless, VLANs, QinQs, PPPs, GREs, GIFs, Bridges, and LAGGs.

The main table lists the interface assignments:

Interface	Network port	Action
WAN	re0 (44:37:e6:dc:dc:cd)	
LAN	bge0 (00:62:0b:08:ce:1c)	Delete
DMZpublique	bge1 (00:62:0b:08:ce:1d)	Delete
Available network ports:	bge2 (00:62:0b:08:ce:1e)	Add

A "Save" button is located at the bottom left of the page.

Règles de filtrages de pfSense :

Interface WAN

The screenshot shows the pfSense Firewall Rules configuration page for the WAN interface. The breadcrumb is "Firewall / Rules / WAN". The interface tabs are Floating, Tailscale, WAN (selected), LAN, DMZPUBLIQUE, and OpenVPN. The table below lists the rules for this interface.

<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✓ 0/0 B	IPv4 UDP	*	*	WAN address	1194 (OpenVPN)	*	none			
<input type="checkbox"/>	✓ 3/1.89 GiB	IPv4 *	*	*	*	*	*	none			
<input type="checkbox"/>	✓ 0/0 B	IPv4 ICMP any	*	*	*	*	*	none			

Buttons at the bottom: Add (up), Add (down), Delete, Toggle, Copy, Save, Separator.

Interface LAN

The screenshot shows the pfSense Firewall Rules configuration page for the LAN interface. The breadcrumb is "Firewall / Rules / LAN". The interface tabs are Floating, Tailscale, WAN, LAN (selected), DMZPUBLIQUE, and OpenVPN. The table below lists the rules for this interface.

<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✓ 0/32.21 MiB	*	*	*	LAN Address	443 80 22	*	*		Anti-Lockout Rule	
<input type="checkbox"/>	✓ 7/10.41 GiB	IPv4 *	*	*	*	*	*	none			
<input type="checkbox"/>	✓ 0/0 B	IPv4 ICMP any	*	*	*	*	*	none			
<input type="checkbox"/>	✓ ⚙️ 0/0 B	IPv4 ICMP any	*	*	*	*	LAN	none			

Buttons at the bottom: Add (up), Add (down), Delete, Toggle, Copy, Save, Separator.

Interface DMZ Publique :

The screenshot shows the pfSense Firewall Rules configuration page for the DMZPUBLIQUE interface. The breadcrumb is "Firewall / Rules / DMZPUBLIQUE". The interface tabs are Floating, Tailscale, WAN, LAN, DMZPUBLIQUE (selected), and OpenVPN. The table below lists the rules for this interface.

<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✓ 0/843.38 MiB	IPv4 *	*	*	*	*	*	none			
<input type="checkbox"/>	✓ 0/0 B	IPv4 ICMP any	*	*	*	*	*	none			

Buttons at the bottom: Add (up), Add (down), Delete, Toggle, Copy, Save, Separator.

Règle NAT outbound :

pfSense COMMUNITY EDITION System - Interfaces - Firewall - Services - VPN - Status - Diagnostics - Help -

Firewall / NAT / Outbound

Port Forward 1:1 **Outbound** NPt

Outbound NAT Mode

Mode

- Automatic outbound NAT rule generation. (IPsec passthrough included)
- Hybrid Outbound NAT rule generation. (Automatic Outbound NAT + rules below)
- Manual Outbound NAT rule generation. (AON - Advanced Outbound NAT)
- Disable Outbound NAT rule generation. (No Outbound NAT rules)

[Save](#)

Mappings

<input type="checkbox"/>	Interface	Source	Source Port	Destination	Destination Port	NAT Address	NAT Port	Static Port	Description	Actions
<input type="checkbox"/>	<input checked="" type="checkbox"/> WAN	172.16.99.16/28	*	*	*	WAN address	*	<input checked="" type="checkbox"/>		
<input type="checkbox"/>	<input checked="" type="checkbox"/> WAN	172.16.14.0/24	*	*	*	WAN address	*	<input checked="" type="checkbox"/>		
<input type="checkbox"/>	<input checked="" type="checkbox"/> WAN	172.16.13.0/24	*	*	*	WAN address	*	<input checked="" type="checkbox"/>		
<input type="checkbox"/>	<input checked="" type="checkbox"/> WAN	172.16.12.0/24	*	*	*	WAN address	*	<input checked="" type="checkbox"/>		
<input type="checkbox"/>	<input checked="" type="checkbox"/> WAN	172.16.11.0/24	*	*	*	WAN address	*	<input checked="" type="checkbox"/>		
<input type="checkbox"/>	<input checked="" type="checkbox"/> WAN	172.16.5.0/24	*	*	*	WAN address	*	<input checked="" type="checkbox"/>		
<input type="checkbox"/>	<input checked="" type="checkbox"/> WAN	172.16.2.224/27	*	*	*	WAN address	*	<input checked="" type="checkbox"/>		
<input type="checkbox"/>	<input checked="" type="checkbox"/> WAN	172.16.10.0/24	*	*	*	WAN address	*	<input checked="" type="checkbox"/>		
<input type="checkbox"/>	<input checked="" type="checkbox"/> WAN	192.168.2.0/29	*	*	*	WAN address	*	<input checked="" type="checkbox"/>		
<input type="checkbox"/>	<input checked="" type="checkbox"/> WAN	192.168.0.0/29	*	*	*	WAN address	*	<input checked="" type="checkbox"/>		
<input type="checkbox"/>	<input checked="" type="checkbox"/> WAN	10.10.20.0/29	*	*	*	WAN address	*	<input checked="" type="checkbox"/>		
<input type="checkbox"/>	<input checked="" type="checkbox"/> WAN	127.0.0.0/8	*	*	500 (ISAKMP)	WAN address	*	<input checked="" type="checkbox"/>	Auto created rule for ISAKMP - localhost to WAN	
<input type="checkbox"/>	<input checked="" type="checkbox"/> WAN	127.0.0.0/8	*	*	*	WAN address	*	<input checked="" type="checkbox"/>	Auto created rule - localhost to WAN	
<input type="checkbox"/>	<input checked="" type="checkbox"/> WAN	::1/128	*	*	500 (ISAKMP)	WAN address	*	<input checked="" type="checkbox"/>	Auto created rule for ISAKMP - localhost to WAN	
<input type="checkbox"/>	<input checked="" type="checkbox"/> WAN	::1/128	*	*	*	WAN address	*	<input checked="" type="checkbox"/>	Auto created rule - localhost to WAN	
<input type="checkbox"/>	<input checked="" type="checkbox"/> WAN	172.16.2.224/27	*	*	500 (ISAKMP)	WAN address	*	<input checked="" type="checkbox"/>	Auto created rule for ISAKMP - LAN to WAN	
<input type="checkbox"/>	<input checked="" type="checkbox"/> WAN	172.16.2.224/27	*	*	*	WAN address	*	<input checked="" type="checkbox"/>	Auto created rule - LAN to WAN	

Interface	Source	Source Port	Destination	Destination Port	NAT Address	NAT Port	Static Port	Description
✓ WAN	127.0.0.0/8 ::1/128 172.16.2.224/27 192.168.2.0/24 192.168.1.0/28 172.16.11.0/24 172.16.5.0/24 172.16.10.0/24 172.16.99.16/28 172.16.13.0/24 172.16.14.0/24 172.16.12.0/24 192.168.0.0/29 10.8.0.0/24	*	*	500	WAN address	*	✓	Auto created rule for ISAKMP
✓ WAN	127.0.0.0/8 ::1/128 172.16.2.224/27 192.168.2.0/24 192.168.1.0/28 172.16.11.0/24 172.16.5.0/24 172.16.10.0/24 172.16.99.16/28 172.16.13.0/24 172.16.14.0/24 172.16.12.0/24 192.168.0.0/29 10.8.0.0/24	*	*	*	WAN address	*	✗	Auto created rule
✓ LAN	127.0.0.0/8 ::1/128 172.16.2.224/27 192.168.2.0/24 192.168.1.0/28 172.16.11.0/24 172.16.5.0/24 172.16.10.0/24 172.16.99.16/28 172.16.13.0/24 172.16.14.0/24 172.16.12.0/24 192.168.0.0/29 10.8.0.0/24	*	*	500	LAN address	*	✓	Auto created rule for ISAKMP
✓ LAN	127.0.0.0/8 ::1/128 172.16.2.224/27 192.168.2.0/24 192.168.1.0/28 172.16.11.0/24 172.16.5.0/24 172.16.10.0/24 172.16.99.16/28 172.16.13.0/24 172.16.14.0/24 172.16.12.0/24 192.168.0.0/29 10.8.0.0/24	*	*	*	LAN address	*	✗	Auto created rule

Bonus, configuration VPN d'accès au réseau de mon infrastructure :

pfSense COMMUNITY EDITION System - Interfaces - Firewall - Services - VPN - Status - Diagnostics - Help

VPN / Tailscale / Settings

Tailscale is online.

Authentication Settings Status

Settings

Enable Enable Tailscale

Listen Port
UDP port to listen on for WireGuard and peer-to-peer traffic.

State Directory
Path to directory for storage of config state, certificates, and incoming files. WARNING: Changing this value will not move an existing configuration and will require reauthentication with the control server.

Keep Configuration Enable
With 'Keep Configuration' enabled (default), all package settings and the local Tailscale state cache will persist on install/de-install.

DNS

Accept DNS Accept DNS configuration from the control server.

Routing

Advertise Exit Node Offer to be an exit node for outbound internet traffic from the Tailscale network.

Accept Subnet Routes Accept subnet routes that other nodes advertise.

Notice Routes will be transformed into proper subnet start boundaries prior to validating and saving.

Advertised Routes	Administrative description (not parsed)	Action
<input type="text" value="10.10.20.0/24"/>	LAN pfSense	Delete
<input type="text" value="192.168.1.0/24"/>	Proxmox	Delete
<input type="text" value="172.16.2.0/24"/>	ESXI-LAN	Delete
<input type="text" value="192.168.2.0/24"/>	commutateur de niv 3	Delete
<input type="text" value="10.10.30.0/24"/>	Borne wifi	Delete
<input type="text" value="172.16.5.0/24"/>	VoIP	Delete
<input type="text" value="172.16.13.0/24"/>	vlan 13	Delete
<input type="text" value="172.16.14.0/24"/>	vlan 14	Delete

Subnet expressed using CIDR notation

Add

Logging

Syslog Logging Enable syslog output

Syslog Settings
Set the syslog logging priority. Set the syslog logging facility.