

Chapitre 12 – Nouvelle passerelle de sécurité PfSense

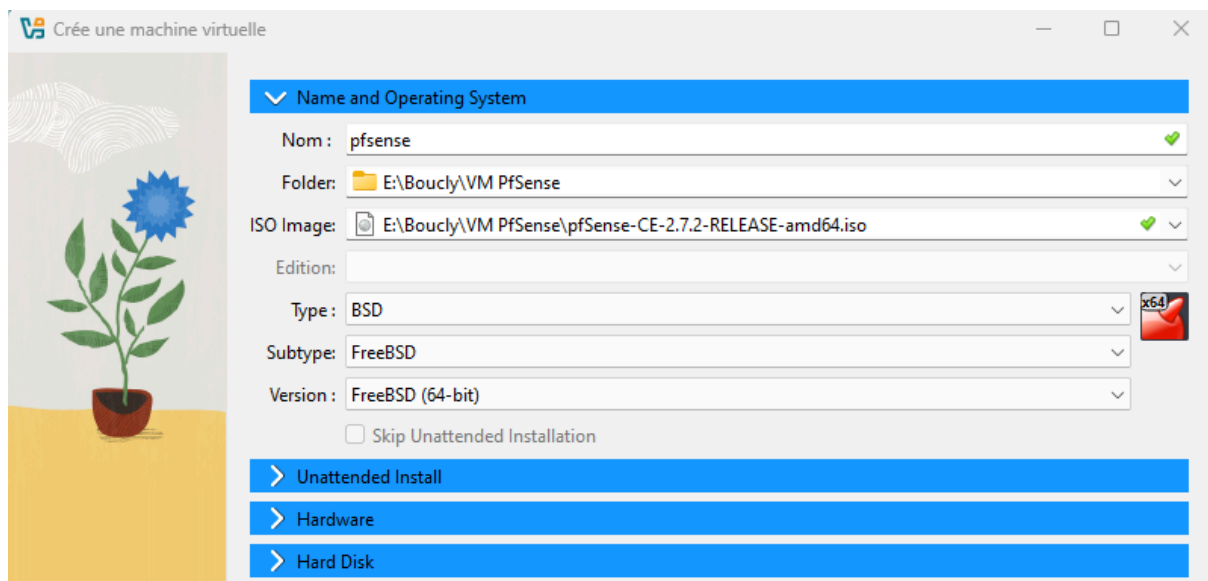
1. Création de la VM PfSense.....	2
2. Installation du serveur PfSense.....	3
3. Configuration des cartes réseau.....	8
4. Configuration générale depuis la Web GUI.....	13
5. Accès à la Web GUI depuis l'interface WAN.....	20
6. Port forwarding.....	22
7. Mise en place du split DNS.....	28

1. Création de la VM PfSense.

- RAM : 2 Go ; HD : 32 Go
- Iso : pfSense-CE-2.7.2-RELEASE-amd64

<https://provya.net/?d=2024/05/28/10/37/02-installer-pfsense#telecharger-pfsense>
<https://repo.ialab.dsu.edu/pfsense/>

- 3 NIC à l'instar de la machine US3 :
 - em0 : accès pont
 - em1 : réseau interne (DMZ)
 - em2 : réseau interne (LAN)



2. Installation du serveur PfSense.

```
pfSense Installer
-----
Copyright and distribution notice
-----
Copyright and Trademark Notices.

Copyright 2004-2016. Electric Sheep Fencing, LLC ("ESF").
All Rights Reserved.

Copyright 2014-2023. Rubicon Communications, LLC d/b/a Netgate
("Netgate").
All Rights Reserved.

All logos, text, and content of ESF and/or Netgate, including underlying
HTML code, designs, and graphics used and/or depicted herein are
protected under United States and international copyright and trademark
laws and treaties, and may not be used or reproduced without the prior
express written permission of ESF and/or Netgate.

"pfSense" is a registered trademark of ESF, exclusively licensed to
Netgate, and may not be used without the prior express written
permission of ESF and/or Netgate. All other trademarks shown herein are
----- 26%
[Accept]
```

```
pfSense Installer
-----
Welcome
-----
Welcome to pfSense!

Install      Install pfSense
Rescue Shell Launch a shell for rescue operations
Recover config.xml Recover config.xml from a previous install

-----
< OK >      <Cancel>
```

pfSense Installer

Partitioning

How would you like to partition your disk?

A uto (ZFS)	G uided Root-on-ZFS
A uto (UFS)	Guided UFS Disk Setup
M anual	Manual Disk Setup (experts)
S hell	Open a shell and partition by hand

< **D**K > <Cancel>

To use ZFS with less than 8GB RAM, see <https://wiki.freebsd.org/ZFSTuningGuide>

pfSense Installer

ZFS Configuration

Configure Options:

>>> Install	P roceed with Installation
T Pool Type/Disks:	stripe: 0 disks
- Rescan Devices	*
- Disk Info	*
N Pool Name	pfSense
4 Force 4K Sectors?	YES
E Encrypt Disks?	NO
P Partition Scheme	GPT (BIOS)
S Swap Size	1g
M Mirror Swap?	NO
W Encrypt Swap?	NO

<**S**elect> <Cancel>

---[Use alnum, arrows, punctuation, TAB or ENTER]---

Create ZFS boot pool with displayed options

pfSense Installer

ZFS Configuration

Select Virtual Device type:

stripe	Stripe - No Redundancy
mirror	Mirror - n-Way Mirroring
raid10	RAID 1+0 - n x 2-Way Mirrors
raidz1	RAID-Z1 - Single Redundant RAID
raidz2	RAID-Z2 - Double Redundant RAID
raidz3	RAID-Z3 - Triple Redundant RAID

< OK > <Cancel>

[Press arrows, TAB or ENTER]

[1+ Disks] Striping provides maximum storage but no redundancy

pfSense Installer

ZFS Configuration

[] ada0 VBOX HARDDISK

< OK > < Back >

pfSense Installer

```
-----ZFS Configuration-----
Last Chance! Are you sure you want to destroy
the current contents of the following disks:

ada0

-----< YES > < NO >-----
[Press arrows, TAB or ENTER]
```

pfSense Installer

```
-----Archive Extraction-----
base.txz [ █ 9% ]
Extracting distribution files...

-----Overall Progress-----
[ █ 9% ]
```

4544 files read @ 2272.0 files/sec.

pfSense Installer

```
Complete
Installation of pfSense complete!
Would you like to reboot into the
installed system now?

[Reboot]    [Shell ]
```

```
done.
Starting CRON... done.
pfSense 2.7.2-RELEASE amd64 20231206-2010
Bootup complete

FreeBSD/amd64 (pfSense.home.arpa) (ttyv0)
VirtualBox Virtual Machine - Netgate Device ID: a843c7ac70ddd82260dc
*** Welcome to pfSense 2.7.2-RELEASE (amd64) on pfSense ***

WAN (wan)      -> em0          -> v4/DHCP4: 172.17.5.9/16
LAN (lan)      -> em1          -> v4: 192.168.1.1/24

0) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults   13) Update from console
5) Reboot system              14) Enable Secure Shell (sshd)
6) Halt system                15) Restore recent configuration
7) Ping host                  16) Restart PHP-FPM
8) Shell

Enter an option: █
```

3. Configuration des cartes réseau.

```
done.
Starting CRON... done.
pfSense 2.7.2-RELEASE amd64 20231206-2010
Bootup complete

FreeBSD/amd64 (pfSense.home.arpa) (ttyv0)
VirtualBox Virtual Machine - Netgate Device ID: a843c7ac70ddd82260dc
*** Welcome to pfSense 2.7.2-RELEASE (amd64) on pfSense ***

WAN (wan)      -> em0      -> v4/DHCP4: 172.17.5.9/16
LAN (lan)      -> em1      -> v4: 192.168.1.1/24

0) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults  13) Update from console
5) Reboot system              14) Enable Secure Shell (sshd)
6) Halt system                 15) Restore recent configuration
7) Ping host                   16) Restart PHP-FPM
8) Shell
```

```
Enter an option: 1
```

```
Valid interfaces are:
```

```
em0      08:00:27:e3:39:18   (up) Intel(R) Legacy PRO/1000 MT 82540EM
em1      08:00:27:e4:e0:cf   (up) Intel(R) Legacy PRO/1000 MT 82540EM
em2      08:00:27:65:71:6d (down) Intel(R) Legacy PRO/1000 MT 82540EM
```

```
Do VLANs need to be set up first?
```

```
If VLANs will not be used, or only for optional interfaces, it is typical to say no here and use the webConfigurator to configure VLANs later, if required.
```

```
Should VLANs be set up now [y|n]? n
```

```
say no here and use the webConfigurator to configure VLANs later, if required.
```

```
Should VLANs be set up now [y|n]? n
```

```
If the names of the interfaces are not known, auto-detection can be used instead. To use auto-detection, please disconnect all interfaces before pressing 'a' to begin the process.
```

```
Enter the WAN interface name or 'a' for auto-detection
```

```
(em0 em1 em2 or a): em0
```

```
Enter the LAN interface name or 'a' for auto-detection
```

```
NOTE: this enables full Firewalling/NAT mode.
```

```
(em1 em2 a or nothing if finished): em2
```

```
Enter the Optional 1 interface name or 'a' for auto-detection
```

```
(em1 a or nothing if finished): em1
```

```
The interfaces will be assigned as follows:
```

```
WAN -> em0
```

```
LAN -> em2
```

```
OPT1 -> em1
```

```
Do you want to proceed [y|n]? y
```

```
OPT1 -> em1
Do you want to proceed [y/n]? y
Writing configuration...done.
One moment while the settings are reloading... done!
VirtualBox Virtual Machine - Netgate Device ID: a843c7ac70ddd82260dc

*** Welcome to pfSense 2.7.2-RELEASE (amd64) on pfSense ***

WAN (wan)      -> em0      -> v4/DHCP4: 172.17.5.9/16
LAN (lan)      -> em2      -> v4: 192.168.1.1/24
OPT1 (opt1)    -> em1      ->

0) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults  13) Update from console
5) Reboot system              14) Enable Secure Shell (sshd)
6) Halt system                 15) Restore recent configuration
7) Ping host                   16) Restart PHP-FPM
8) Shell
```

```
Enter an option: 2
```

```
Available interfaces:
```

```
1 - WAN (em0 - dhcp, dhcp6)
2 - LAN (em2 - static)
3 - OPT1 (em1)
```

```
Enter the number of the interface you wish to configure: 2
```

```
Configure IPv4 address LAN interface via DHCP? (y/n) n
```

```
Enter the new LAN IPv4 address. Press <ENTER> for none:
> 192.168.3.254
```

```
Subnet masks are entered as bit counts (as in CIDR notation) in pfSense.
e.g. 255.255.255.0 = 24
     255.255.0.0   = 16
     255.0.0.0     = 8
```

```
Enter the new LAN IPv4 subnet bit count (1 to 32):
> 24
```

```
For a WAN, enter the new LAN IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
>
```

```
Configure IPv6 address LAN interface via DHCP6? (y/n) n
```

```
Enter the new LAN IPv6 address. Press <ENTER> for none:
>
```

```
Do you want to enable the DHCP server on LAN? (y/n) n
```

```
Do you want to enable the DHCP server on LAN? (y/n) n
Disabling IPv4 DHCPD...
Disabling IPv6 DHCPD...
```

```
Do you want to revert to HTTP as the webConfigurator protocol? (y/n) n
```

```
Please wait while the changes are saved to LAN...
Reloading filter...
Reloading routing configuration...
DHCPD...
```

```
The IPv4 LAN address has been set to 192.168.3.254/24
You can now access the webConfigurator by opening the following URL in your web
browser:
```

```
https://192.168.3.254/
```

```
Press <ENTER> to continue.
```

```
The IPv4 LAN address has been set to 192.168.3.254/24
You can now access the webConfigurator by opening the following URL in your web
browser:
```

```
https://192.168.3.254/
```

```
Press <ENTER> to continue.
```

```
VirtualBox Virtual Machine - Netgate Device ID: a843c7ac70ddd82260dc
```

```
*** Welcome to pfSense 2.7.2-RELEASE (amd64) on pfSense ***
```

```
WAN (wan)      -> em0      -> v4/DHCP4: 172.17.5.9/16
LAN (lan)      -> em2      -> v4: 192.168.3.254/24
OPT1 (opt1)   -> em1      ->
```

```
0) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults 13) Update from console
5) Reboot system             14) Enable Secure Shell (sshd)
6) Halt system               15) Restore recent configuration
7) Ping host                 16) Restart PHP-FPM
8) Shell
```

```
Enter an option: 2
```

```
Available interfaces:
```

```
1 - WAN (em0 - dhcp, dhcp6)
2 - LAN (em2 - static)
3 - OPT1 (em1)
```

```
Enter the number of the interface you wish to configure: 3
```

```
Enter the new OPT1 IPv4 address. Press <ENTER> for none:
> 192.168.2.254

Subnet masks are entered as bit counts (as in CIDR notation) in pfSense.
e.g. 255.255.255.0 = 24
     255.255.0.0   = 16
     255.0.0.0     = 8

Enter the new OPT1 IPv4 subnet bit count (1 to 32):
> 24

For a WAN, enter the new OPT1 IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
>

Configure IPv6 address OPT1 interface via DHCP6? (y/n) n

Enter the new OPT1 IPv6 address. Press <ENTER> for none:
>

Do you want to enable the DHCP server on OPT1? (y/n) n
Disabling IPv4 DHCPD...
Disabling IPv6 DHCPD...

Do you want to revert to HTTP as the webConfigurator protocol? (y/n) n
```

```
The IPv4 OPT1 address has been set to 192.168.2.254/24
You can now access the webConfigurator by opening the following URL in your web
browser:
```

```
https://192.168.2.254/
```

```
Press <ENTER> to continue.
```

```
VirtualBox Virtual Machine - Netgate Device ID: a843c7ac70ddd82260dc
```

```
*** Welcome to pfSense 2.7.2-RELEASE (amd64) on pfSense ***
```

```
WAN (wan)      -> em0      -> v4/DHCP4: 172.17.5.9/16
LAN (lan)      -> em2      -> v4: 192.168.3.254/24
OPT1 (opt1)    -> em1      -> v4: 192.168.2.254/24
```

```
0) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults   13) Update from console
5) Reboot system              14) Enable Secure Shell (sshd)
6) Halt system                15) Restore recent configuration
7) Ping host                  16) Restart PHP-FPM
8) Shell
```

```
Enter an option: 2
```

```
Available interfaces:
```

```
1 - WAN (em0 - dhcp, dhcp6)
2 - LAN (em2 - static)
3 - OPT1 (em1 - static)
```

```
Enter the number of the interface you wish to configure: 1
```

```
Configure IPv4 address WAN interface via DHCP? (y/n) n
```

Réseau SIO : 172.17.0.0/16 ; GW : 172.17.250.2

```
Configure IPv4 address WAN interface via DHCP? (y/n) n
Enter the new WAN IPv4 address. Press <ENTER> for none:
> 172.17.101.1
Subnet masks are entered as bit counts (as in CIDR notation) in pfSense.
e.g. 255.255.255.0 = 24
     255.255.0.0   = 16
     255.0.0.0    = 8
Enter the new WAN IPv4 subnet bit count (1 to 32):
> 16
For a WAN, enter the new WAN IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
> 172.17.250.2
Should this gateway be set as the default gateway? (y/n) y

Configure IPv6 address WAN interface via DHCP6? (y/n) n
Enter the new WAN IPv6 address. Press <ENTER> for none:
>
Do you want to enable the DHCP server on WAN? (y/n) n
Disabling IPv4 DHCPD...
Disabling IPv6 DHCPD...
Do you want to revert to HTTP as the webConfigurator protocol? (y/n) n

The IPv4 WAN address has been set to 172.17.101.1/16
Press <ENTER> to continue.
VirtualBox Virtual Machine - Netgate Device ID: a843c7ac70ddd82260dc
*** Welcome to pfSense 2.7.2-RELEASE (amd64) on pfSense ***
WAN (wan)      -> em0      -> v4: 172.17.101.1/16
LAN (lan)     -> em2      -> v4: 192.168.3.254/24
OPT1 (opt1)   -> em1      -> v4: 192.168.2.254/24
```

4. Configuration générale depuis la Web GUI.

Nous accédons à l'interface Web de PfSense depuis le LAN avec UD1. Nous accédons également à l'interface Web de PfSense depuis le LAN avec UD1 :

Annuler **Filaire** **Appliquer**

Détails Identité **IPv4** IPv6 Sécurité

Méthode IPv4

Automatique (DHCP) Réseau local seulement

Manuel Désactiver

Partagée avec d'autres ordinateurs

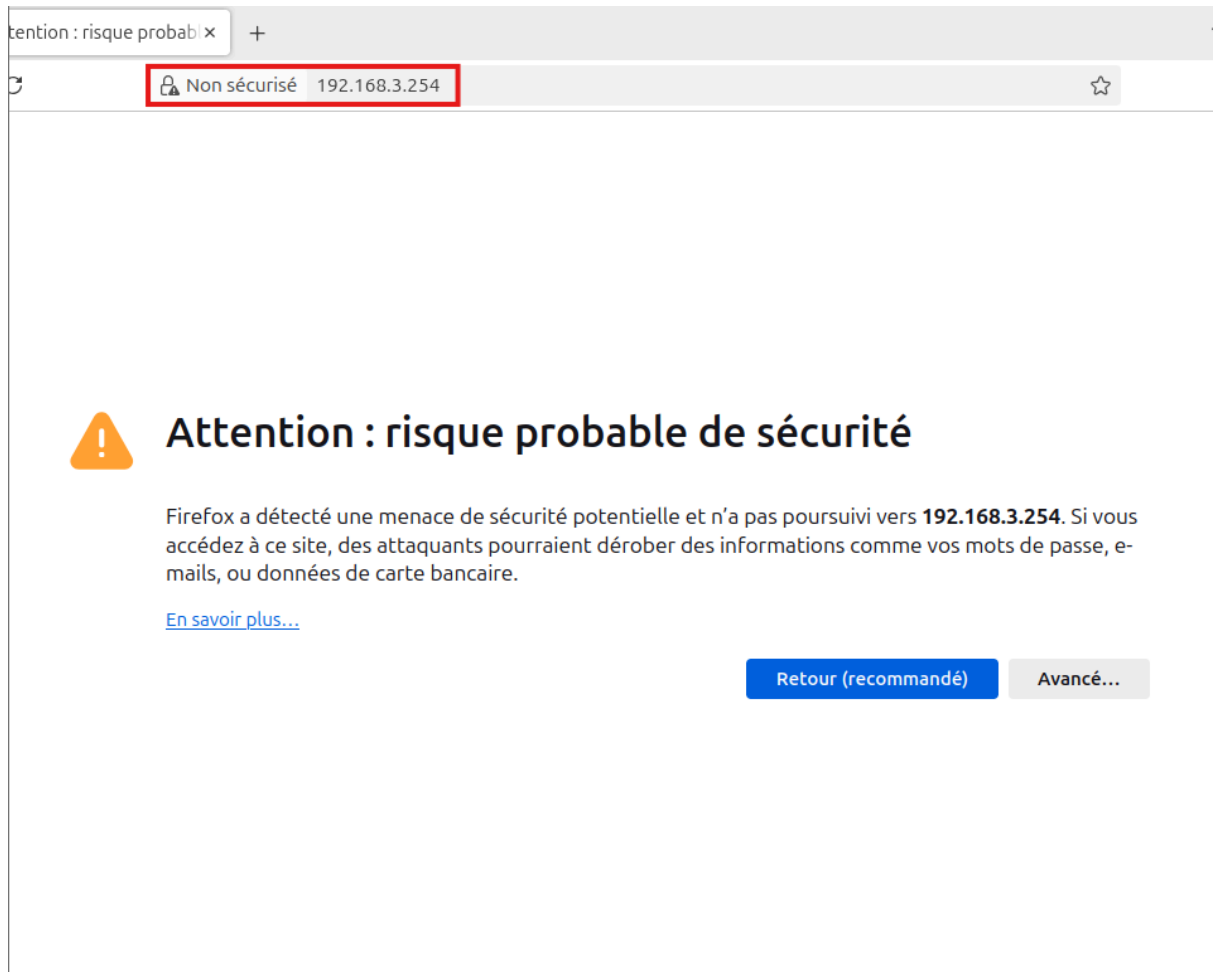
Adresses

Adresse	Masque de réseau	Passerelle	
192.168.3.11	255.255.255.0	192.168.3.254	

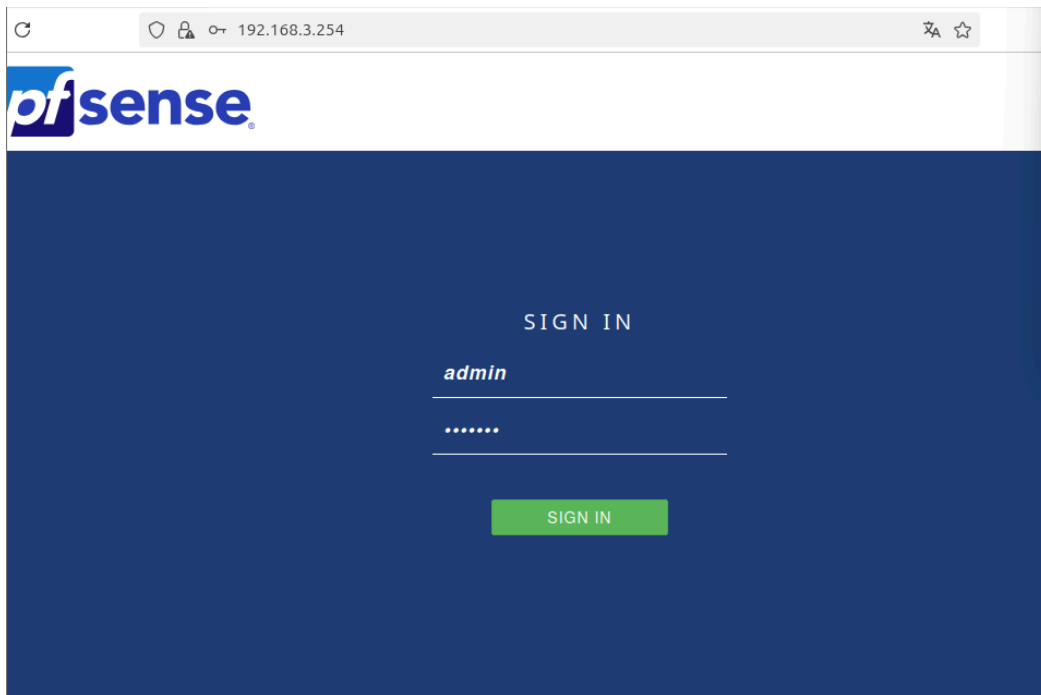
DNS Automatique

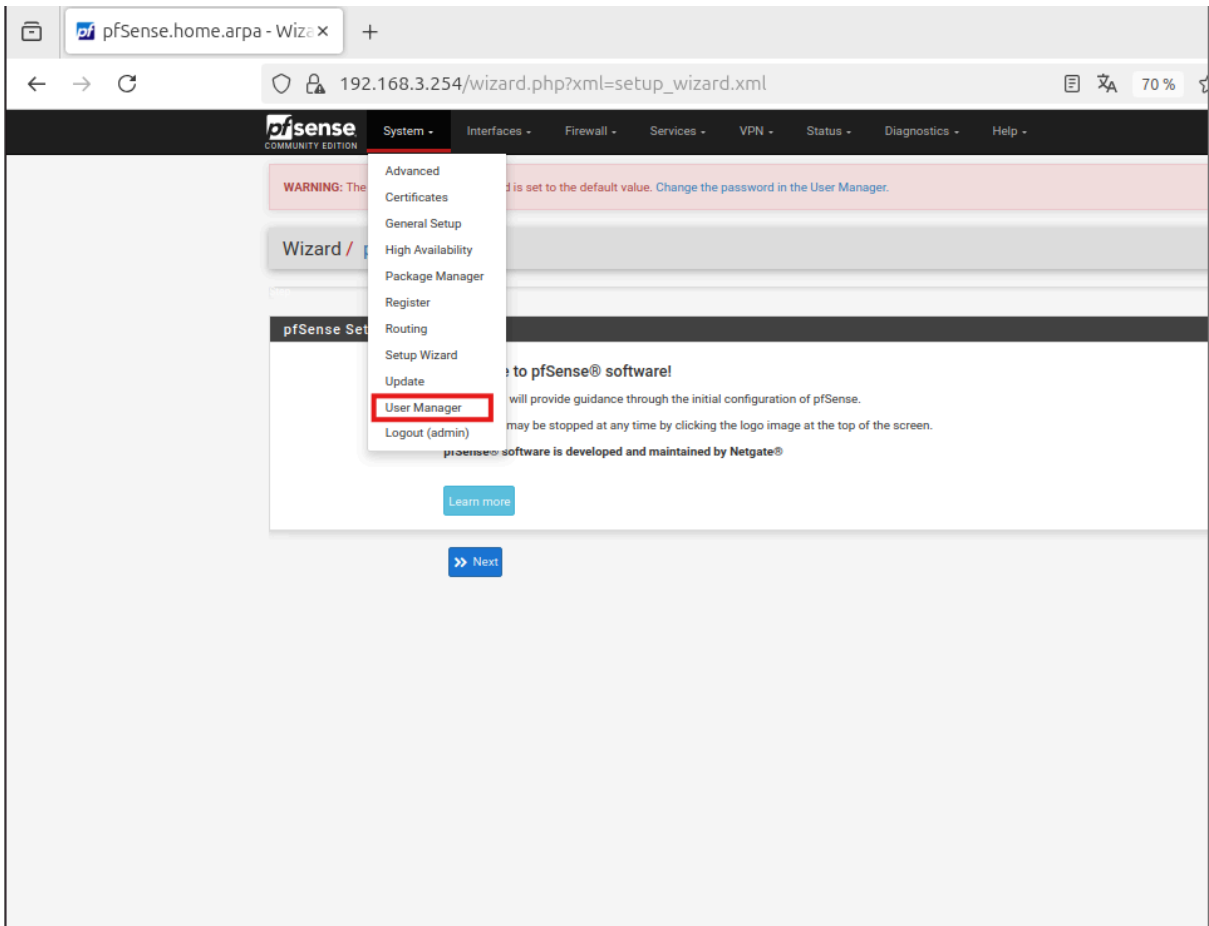
192.168.2.1

Séparer les adresses IP avec des virgules




Login : admin ; mot de passe : pfsense






System / User Manager / Users

Users Groups Settings Authentication Servers

Users					
	Username	Full name	Status	Groups	Actions
<input type="checkbox"/>	admin	System Administrator	✓	admins	

+ Add  Delete

Nous modifions le mot de passe du compte admin : Azerty0 (pas de capture mais le mdp a été sauvegardé)

System / User Manager / Users / Edit

Users Groups Settings Authentication Servers

User Properties

Defined by	SYSTEM
Disabled	<input type="checkbox"/> This user cannot login
Username	admin
Password	*****
Full name	System Administrator <small>User's full name, for administrative information only</small>
Expiration date	<input type="text"/> <small>Leave blank if the account shouldn't expire, otherwise enter the expiration date as MM/DD/YYYY</small>

Status **Dashboard**

System Information

Name	pfSense.home.arpa
User	admin@192.168.3.11 (Local Database)
System	VirtualBox Virtual Machine Netgate Device ID: a843c7ac70ddd82260dc
BIOS	Vendor: innotek GmbH Version: VirtualBox Release Date: Fri Dec 1 2006
Version	2.7.2-RELEASE (amd64) built on Wed Dec 6 20:10:00 UTC 2023 FreeBSD 14.0-CURRENT <i>Unable to check for updates</i>
CPU Type	AMD Ryzen 9 5950X 16-Core Processor 2 CPUs: 1 package(s) x 2 core(s) AES-NI CPU Crypto: Yes (inactive) QAT Crypto: No
Hardware crypto	Inactive
Kernel PTI	Disabled
MDS Mitigation	Inactive
Uptime	00 Hour 22 Minutes 46 Seconds
Current date/time	Thu Apr 24 9:50:02 UTC 2025
DNS server(s)	• 127.0.0.1
Last config change	Thu Apr 24 9:47:40 UTC 2025
State table size	0% (250/198000) Show states
MBUF Usage	0% (4318/1000000)
Load average	0.22, 0.21, 0.17
CPU usage	1%

Netgate Services And Support

Contract type **Community Support**
Community Support Only

NETGATE AND pfSense COMMUNITY SUPPORT RESOURCES

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](#).

You also may upgrade to a Netgate Global Technical Assistance Center (TAC) Support subscription. We're always on! Our team is staffed 24x7x365 and committed to delivering enterprise-class, worldwide support at a price point that is more than competitive when compared to others in our space.

- [Upgrade Your Support](#)
- [Community Support Resources](#)
- [Netgate Global Support FAQ](#)
- [Official pfSense Training by Netgate](#)
- [Netgate Professional Services](#)
- [Visit Netgate.com](#)

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

WAN	↑	1000baseT <full-duplex>	172.17.101.1
LAN	↑	1000baseT <full-duplex>	192.168.3.254
OPT1	↑	1000baseT <full-duplex>	192.168.2.254

System / General Setup

System

Hostname	<input type="text" value="pfSense"/>
Name of the firewall host, without domain part.	
Domain	<input type="text" value="sio-exupery.fr"/>
Domain name for the firewall.	

Do not end the domain name with '.local' as the final part (Top Level Domain, TLD). The 'local' TLD is widely used by mDNS (e.g. Avahi, Bonjour, Rendezvous, Airprint, Airplay) and some Windows systems and networked devices. These will not network correctly if the router uses 'local' as its TLD. Alternatives such as 'home.arpa', 'local.lan', or 'mylocal' are safe.

DNS Server Settings

DNS Servers	<input type="text" value="192.168.2.1"/>	<input type="text" value=""/>	
Address	Enter IP addresses to be used by the system for DNS resolution. These are also used for the DHCP service, DNS Forwarder and DNS Resolver when it has DNS Query Forwarding enabled.	Hostname	Enter the DNS Server Hostname for TLS Verification in the DNS Resolver (optional).
Add DNS Server	<input type="button" value="+ Add DNS Server"/>		
DNS Server Override	<input checked="" type="checkbox"/> Allow DNS server list to be overridden by DHCP/PPP on WAN or remote OpenVPN server If this option is set, pfSense will use DNS servers assigned by a DHCP/PPP server on WAN or a remote OpenVPN server (if Pull DNS option is enabled) for its own purposes (including the DNS Forwarder/DNS Resolver). However, they will not be assigned to DHCP clients.		
DNS Resolution Behavior	<input type="text" value="Use remote DNS Servers, ignore local DNS"/>		

By default the firewall will use local DNS service (127.0.0.1, DNS Resolver or Forwarder) as the first DNS server when possible, and it will fall back to remote DNS servers otherwise. Use this option to choose alternate behaviors.

Localization

Timezone	<input type="text" value="Europe/Paris"/>
Select a geographic region name (Continent/Location) to determine the timezone for the firewall. Choose a special or "Etc" zone only in cases where the geographic zones do not properly handle the clock offset required for this firewall.	
Timeservers	<input type="text" value="2.pfsense.pool.ntp.org"/>
Use a space to separate multiple hosts (only one required). Remember to set up at least one DNS server if a host name is entered here!	
Language	<input type="text" value="French"/>
Choose a language for the webConfigurator	
Disable dragging	<input type="checkbox"/> Disable dragging of firewall/NAT rules Disables dragging rows to allow selecting and copying row contents and avoid accidental changes.
Login page color	<input type="text" value="Dark Blue"/>
Choose a color for the login page	
Login hostname	<input type="checkbox"/> Show hostname on login banner

Interfaces / WAN (em0)

Static IPv4 Configuration

IPv4 Address /

IPv4 Upstream gateway [+ Add a new gateway](#)

If this interface is an Internet connection, select an existing Gateway from the list or add a new one using the "Add" button.
On local area network interfaces the upstream gateway should be "none".
Selecting an upstream gateway causes the firewall to treat this interface as a **WAN type interface**.
Gateways can be managed by [clicking here](#).

Reserved Networks

Block private networks and loopback addresses

Blocks traffic from IP addresses that are reserved for private networks per RFC 1918 (10/8, 172.16/12, 192.168/16) and unique local addresses per RFC 4193 (fc00::/7) as well as loopback addresses (127/8). This option should generally be turned on, unless this network interface resides in such a private address space, too.

Block bogon networks

Blocks traffic from reserved IP addresses (but not RFC 1918) or not yet assigned by IANA. Bogons are prefixes that should never appear in the Internet routing table, and so should not appear as the source address in any packets received. This option should only be used on external interfaces (WANs), it is not necessary on local interfaces and it can potentially block required local traffic. Note: The update frequency can be changed under System > Advanced, Firewall & NAT settings.

[Save](#)

The WAN configuration has been changed.
The changes must be applied to take effect.
Don't forget to adjust the DHCP Server range if needed after applying.

[Apply Changes](#)

Visualisation de la règle de translation existante. Que permet-elle ?

pfSense COMMUNITY EDITION

Système - Interfaces - Pare-feu - Services - VPN - État -

État / Tableau de bord

Informations système

Nom pfSense.s

Alias
IPs virtuels
NAT
Plannings
Règles

Pare-feu / NAT / Sortant

Transfert de port 1:1 **Sortant** NPt

Mode NAT sortant

Mode Création automatique de règles NAT sortantes. (IPsec passthrough inclu) Création hybride de règles NAT sortantes. (NAT sortant automatique + règles ci-dessous) Création manuelle de règles NAT sortantes. (NSA - NAT sortant avancée) Désactiver la création de règles NAT sortantes. (Aucune règle NAT sortant)

[Enregistrer](#)

Mappages

Interface	Source	Port source	Destination	Port destination	Adresse NAT	Port NAT	Port statique	Description	Actions
<input type="checkbox"/>									
Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter
Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter
Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter
Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter
Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter
Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter
Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter
Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter
Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter
Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter
Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter
Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter
Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter
Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter
Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter
Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter
Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter
Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter
Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter
Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter
Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter
Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter
Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter
Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter
Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter
Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter
Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter
Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter
Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter
Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter
Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter
Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter
Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter
Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter
Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter
Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter
Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter
Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter
Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter
Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter
Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter
Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter
Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter
Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter
Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter
Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter
Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter
Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter
Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter
Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter
Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter
Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter
Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter
Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter
Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter
Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter
Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter
Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter
Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter
Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter
Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter
Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter
Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter
Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter
Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter
Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter
Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter
Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter
Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter
Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter
Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter
Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter
Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter
Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter
Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter
Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter
Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter
Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter
Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter
Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter
Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter
Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter	Ajouter
Ajouter	Ajouter								

Cette règle NAT permet aux machines des réseaux 192.168.2.0/24,192.168.3.0/24, d'accéder à Internet, en traduisant leur adresse IP source vers l'adresse IP publique du routeur sur l'interface WAN.

Visualisez les règles de pare-feu existantes concernant l'interface LAN. Que permettent-elles ?

The screenshot shows the Mikrotik WinBox interface for Firewall Rules on the LAN interface. The 'Règles' table is highlighted with a red box. The table has the following columns: États, Protocole, Source, Port, Destination, Port, Passerelle, File d'attente, Ordonnement, Description, and Actions.

États	Protocole	Source	Port	Destination	Port	Passerelle	File d'attente	Ordonnement	Description	Actions
✓	1/195 KiB	*	*	LAN Address	443	*	*	*	Règle anti-blocage	⚙️
✓	161/43 KiB	IPv4 *	LAN subnets	*	*	*	aucun	*	Default allow LAN to any rule	📄 🗑️ 🔄 📄 🗑️
✓	0/0 B	IPv6 *	LAN subnets	*	*	*	aucun	*	Default allow LAN IPv6 to any rule	📄 🗑️ 🔄 📄 🗑️

Buttons at the bottom: Ajouter (up), Ajouter (down), Supprimer, Toggle, Copier, Enregistrer, Séparateur.

Elle permet à tous les appareils du réseau LAN de communiquer librement avec n'importe quelle destination, interne ou externe provenant des ports : 443 (HTTPS) et 80 (HTTP).

Consultez les règles pour les interfaces OPT1 et WAN. Qu'en déduisez-vous ?

The screenshots show the Mikrotik WinBox interface for Firewall Rules on the OPT1 and WAN interfaces. Both interfaces show a message: 'Aucune règle n'est définie pour cette interface. Toute connexion entrante vers cette interface sera bloquée jusqu'à ce que des règles de passage soient ajoutées. Cliquer sur le bouton pour ajouter une nouvelle règle.'

Buttons at the bottom of each screenshot: Ajouter (up), Ajouter (down), Supprimer, Toggle, Copier, Enregistrer, Séparateur.

Nous allons appliquer des règles plus tard pour permettre un filtrage

5. Accès à la Web GUI depuis l'interface WAN.

Modification du port de l'interface Web d'administration de Pfsense.

Systeme / Avancé / Accès administrateur

Accès administrateur Pare-feu et NAT Mise en réseau Divers Ajustements Systèmes Notifications

webConfigurator

Protocole HTTP HTTPS (SSL/TLS)

Certificat SSL/TLS

Port TCP

Nombre maximal de processus

Activation de l'accès à l'interface web depuis WAN (réseau 172.17.0.0/16).

Pare-feu / Règles / WAN

Flottant(e) WAN LAN OPT1

Règles (Faire glisser pour changer l'ordre)

Etats	Protocole	Source	Port	Destination	Port	Passerelle	File d'attente	Ordonnement	Description	Actions
-------	-----------	--------	------	-------------	------	------------	----------------	-------------	-------------	---------

Aucune règle n'est définie pour cette interface
Toute connexion entrante vers cette interface sera bloquée jusqu'à ce que des règles de passage soient ajoutées. Cliquez sur le bouton pour ajouter une nouvelle règle.

Ajouter Ajouter Supprimer Toggle Copier Enregistrer Séparateur

Pare-feu / Règles / Modifier

Modifier la règle de Pare-Feu

Action

Désactivé Désactiver cette règle

Interface

Famille d'adresse

Protocole

Source

Source Invert match /

Afficher les options avancées

Destination

Destination Invert match Tous Destination Address / / v

Plage de port de destination (autre) v 44443 (autre) v 44443

De Personnalisé(e) À 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 Administration depuis WAN

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

Enregistrer

Pare-feu / Règles / WAN 📄 📑 ?

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 OPT1

Règles (Faire glisser pour changer l'ordre)

<input type="checkbox"/>	États	Protocole	Source	Port	Destination	Port	Passerelle	File d'attente	Ordonnement	Description	Actions
<input type="checkbox"/>	✓	0/0 B	IPv4 TCP	172.17.0.0/16	*	*	44443	*	aucun	Administration depuis WAN	📄 📑 🗑️ 🔄 📄 📄 📄

↑ Ajouter
↓ Ajouter
🗑️ Supprimer
🔄 Toggle
📄 Copier
📄 Enregistrer
+ Séparateur

← → ↻ ⚠ Non sécurisé https://172.17.101.1:44443 🔍 ☆ 🌐


Login to pfSense

SIGN IN

admin

•••••

SIGN IN

6. Port forwarding.

Port forwarding : on souhaite que les flux arrivant sur l'interface WAN à destination des ports 80, 443 et 53 soient redirigés vers le serveur web DS2 figurant dans la DMZ.

The screenshot shows the Mikrotik WinBox interface for configuring port forwarding. The top navigation bar includes 'Système', 'Interfaces', 'Pare-feu', 'Services', 'VPN', 'État', 'Diagnostics', and 'Aide'. The breadcrumb trail is 'Pare-feu / NAT / Transfert de port'. A table of rules is visible, with 'Transfert de port' selected. Below the table, the 'Ajouter' button is highlighted with a red box. The 'Modifier l'entrée de redirection' form is shown below, with several fields highlighted in red: 'Destination' (set to 'WAN address'), 'Plage de port de destination' (set to 'HTTP' for both 'Du port' and 'Au port'), 'IP de redirection cible' (set to '192.168.2.1'), and 'Port de redirection cible' (set to 'HTTP').

Pare-feu / NAT / Transfert de port

Transfert de port 1:1 Sortant NPt

Règles

Interface	Protocole	Adresse source	Ports source	Adresse de destination	Ports dest.	IP NAT	Ports NAT	Description	Actions
									Ajouter, Supprimer, Toggle, Enregistrer, Séparateur

Pare-feu / NAT / Transfert de port / Modifier

Modifier l'entrée de redirection

Désactivé Désactiver cette règle

Pas de RDR (NOT) Désactiver la redirection pour le trafic vérifié par cette règle
Cette option est rarement nécessaire. Ne pas l'utiliser sans avoir connaissances des implications.

Interface WAN
Choisir l'interface à laquelle cette règle s'applique. Dans la plupart des cas, "WAN" est spécifié.

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

Protocole TCP
Choisir à quel protocole cette règle devrait correspondre. En général, "TCP" est spécifié.

Source [Afficher les options avancées](#)

Destination Inverser les critères. WAN address
Type: Adresse/masque

Plage de port de destination
Du port: HTTP, Au port: HTTP
Personnalisé(e) Personnalisé(e)
Spécifier le port ou le groupe de port pour la destination du paquet pour ce mapping. Le champ "tous" est laissé vide seulement si un seul port est mappé.

IP de redirection cible Address or Alias 192.168.2.1
Type: Adresse
Enter the internal IP address of the server on which to map the ports. e.g.: 192.168.1.12 for IPv4
In case of IPv6 addresses, in must be from the same "scope", i.e. it is not possible to redirect from link-local addresses scope (fe80:*) to local scope (::1)

Port de redirection cible HTTP
Port: Personnalisé(e)
Spécifiez le port sur la machine qui a l'adresse IP entrée ci-dessous. Dans le cas d'un groupe de port, spécifiez le port de début du groupe (le port de fin sera calculé automatiquement).
Ceci est habituellement identique avec la partie "Depuis le port" spécifiée ci-dessus.

Description
 Une description peut être saisie ici à des fins de référence administrative (non analysée).

Pas de synchronisation XMLRPC Ne pas synchroniser automatiquement avec les autres membres CRAP
 Ceci empêche la règle sur Maître de se synchroniser automatiquement avec les autres membres CARP. Cela n'empêche PAS que la règle soit écrasée sur l'Esclave.

Réflexion NAT

Association des Règle de filtre
 Visionner la règle de filtrage

Information de règle

Créé 4/24/25 16:28:48 par admin@192.168.3.11 (Local Database)

Mis à jour 4/24/25 16:28:48 par admin@192.168.3.11 (Local Database)

Pare-feu / NAT / Transfert de port

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.

Transfert de port 1:1 Sortant NPt

Règles

<input type="checkbox"/>	Interface	Protocole	Adresse source	Ports source	Adresse de destination	Ports dest.	IP NAT	Ports NAT	Description	Actions
<input type="checkbox"/>	<input checked="" type="checkbox"/> WAN	TCP	*	*	WAN address	80 (HTTP)	192.168.2.1	80 (HTTP)	Redirection vers serveur HTTP dans la DMZ	<input type="button" value="Ajouter"/> <input type="button" value="Ajouter"/> <input type="button" value="Supprimer"/> <input type="button" value="Toggle"/> <input type="button" value="Enregistrer"/> <input type="button" value="Séparateur"/>

Pare-feu / NAT / Transfert de port

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.

Transfert de port 1:1 Sortant NPt

Règles

<input type="checkbox"/>	Interface	Protocole	Adresse source	Ports source	Adresse de destination	Ports dest.	IP NAT	Ports NAT	Description	Actions
<input type="checkbox"/>	<input checked="" type="checkbox"/> WAN	TCP	*	*	WAN address	443 (HTTPS)	192.168.2.1	443 (HTTPS)	Redirection vers serveur HTTPS dans la DMZ	<input type="button" value="Ajouter"/> <input type="button" value="Ajouter"/> <input type="button" value="Supprimer"/> <input type="button" value="Toggle"/> <input type="button" value="Enregistrer"/> <input type="button" value="Séparateur"/>
<input type="checkbox"/>	<input checked="" type="checkbox"/> WAN	TCP	*	*	WAN address	53 (DNS)	192.168.2.1	53 (DNS)	Redirection vers serveur DNS dans la DMZ	<input type="button" value="Ajouter"/> <input type="button" value="Ajouter"/> <input type="button" value="Supprimer"/> <input type="button" value="Toggle"/> <input type="button" value="Enregistrer"/> <input type="button" value="Séparateur"/>
<input type="checkbox"/>	<input checked="" type="checkbox"/> WAN	UDP	*	*	WAN address	53 (DNS)	192.168.2.1	53 (DNS)	Redirection vers serveur DNS dans la DMZ (UDP)	<input type="button" value="Ajouter"/> <input type="button" value="Ajouter"/> <input type="button" value="Supprimer"/> <input type="button" value="Toggle"/> <input type="button" value="Enregistrer"/> <input type="button" value="Séparateur"/>
<input type="checkbox"/>	<input checked="" type="checkbox"/> WAN	TCP	*	*	WAN address	80 (HTTP)	192.168.2.1	80 (HTTP)	Redirection vers serveur HTTP dans la DMZ	<input type="button" value="Ajouter"/> <input type="button" value="Ajouter"/> <input type="button" value="Supprimer"/> <input type="button" value="Toggle"/> <input type="button" value="Enregistrer"/> <input type="button" value="Séparateur"/>

Pare-feu / Règles / WAN

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 OPT1

Règles (Faire glisser pour changer l'ordre)

<input type="checkbox"/>	États	Protocole	Source	Port	Destination	Port	Passerelle	File d'attente	Ordonnement	Description	Actions
<input type="checkbox"/>	✓	0/454 KIB	IPv4 TCP	172.17.0.0/16	*	WAN address	44443	*	aucun	Administration depuis WAN	
<input type="checkbox"/>	✓	0/0 B	IPv4 TCP	*	*	192.168.2.1	80 (HTTP)	*	aucun	NAT Redirection vers serveur HTTP dans la DMZ	
<input type="checkbox"/>	✓	0/0 B	IPv4 UDP	*	*	192.168.2.1	53 (DNS)	*	aucun	NAT Redirection vers serveur DNS dans la DMZ (UDP)	
<input type="checkbox"/>	✓	0/0 B	IPv4 TCP	*	*	192.168.2.1	53 (DNS)	*	aucun	NAT Redirection vers serveur DNS dans la DMZ	
<input type="checkbox"/>	✓	0/0 B	IPv4 TCP	*	*	192.168.2.1	443 (HTTPS)	*	aucun	NAT Redirection vers serveur HTTPS dans la DMZ	

Ajouter Ajouter Supprimer Toggle Copier Enregistrer Séparateur

(J'ai modifié la première en conséquence que j'avais oublié en destination "WAN address").

Création de deux IP virtuels pour les redirections http et https.

Pare-feu / IPs virtuels

Adresse IP virtuelle

Adresse IP virtuelle	Interface	Type	Description	Actions

Pare-feu / IPs virtuels / Modifier

Modifier l'IP virtuelle

Type Alias IP CARP Mandataire (proxy) ARP Autre

Interface WAN

Type d'adresse Adresse unitaire

Adresse(s) 172.17.101.2 / 16
Le masque doit être le masque de sous-réseau du réseau. Il ne spécifie pas une plage CIDR.

Mot de passe d'IP virtuelle Virtual IP Password Virtual IP Password
Entrez le mot de passe du groupe VHID. Confirmer



Groupe VHID 1
Entrez le nom du groupe VHID qui sera partagé.

Fréquence d'annonce 1 0
Base Biais
La fréquence à laquelle cette machine effectue ses annonces. Autrement, la plus petite combinaison des valeurs de la grappe déterminera le maître.

Description Pour redirection serveur Web DMZ
Une description peut être saisie ici à des fins de référence administrative (non analysée).

Enregistrer





Pare-feu / IPs virtuels ?

Adresse IP virtuelle				
Adresse IP virtuelle	Interface	Type	Description	Actions
172.17.101.2/16	WAN	Alias IP	Pour redirection serveur Web DMZ	 

[+ Ajouter](#)

Pare-feu / IPs virtuels ?

Les modifications ont été appliquées avec succès. ✕

Adresse IP virtuelle				
Adresse IP virtuelle	Interface	Type	Description	Actions
172.17.101.2/16	WAN	Alias IP	Pour redirection serveur Web DMZ	 
172.17.101.3/16	WAN	Alias IP	Pour redirection serveur https DMZ	 

[+ Ajouter](#)

Modification des règles de redirection.

Pare-feu / NAT / Transfert de port / Modifier ?

Modifier l'entrée de redirection

Désactivé Désactiver cette règle

Pas de RDR (NOT) Désactiver la redirection pour le trafic vérifié par cette règle
Cette option est rarement nécessaire. Ne pas l'utiliser sans avoir connaissances des implications.

Interface
Choisir l'interface à laquelle cette règle s'applique. Dans la plupart des cas, "WAN" est spécifié.

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

Protocole
Choisir à quel protocole cette règle devrait correspondre. En général, "TCP" est spécifié.

Source [Afficher les options avancées](#)

Destination Inverser les critères. /
Adresse/masque

Plage de port de destination
Du port Personnalisé(e) Au port Personnalisé(e)
Spécifier le port ou le groupe de port pour la destination du paquet pour ce mapping. Le champ "tous" est laissé vide seulement si un seul port est mappé.

IP de redirection cible
Type Adresse
Enter the internal IP address of the server on which to map the ports. e.g.: 192.168.1.12 for IPv4
 In case of IPv6 addresses, it must be from the same "scope",
 i.e. it is not possible to redirect from link-local addresses scope (fe80:*) to local scope (::1)

Port de redirection cible
Port Personnalisé(e)
Spécifiez le port sur la machine qui a l'adresse IP entrée ci-dessous. Dans le cas d'un groupe de port, spécifiez le port de début du groupe (le port de fin sera calculé automatiquement).
 Ceci est habituellement identique avec la partie "Depuis le port" spécifiée ci-dessus.

Interface WAN
Choisir l'interface à laquelle cette règle s'applique. Dans la plupart des cas, "WAN" est spécifié.

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

Protocole TCP
Choisir à quel protocole cette règle devrait correspondre. En général, "TCP" est spécifié.

Source [Afficher les options avancées](#)

Destination Inverser les critères. 172.17.101.3 (Pour redirection serveur https DMZ) / Adresse/masque

Plage de port de destination Du port: HTTPS, Au port: HTTPS
Spécifier le port ou le groupe de port pour la destination du paquet pour ce mapping. Le champ "tous" est laissé vide seulement si un seul port est mappé.

IP de redirection cible Address or Alias: 192.168.2.9, Type: Adresse
Enter the internal IP address of the server on which to map the ports. e.g.: 192.168.1.12 for IPv4
In case of IPv6 addresses, it must be from the same "scope", i.e. it is not possible to redirect from link-local addresses scope (fe80*) to local scope (::1)

Port de redirection cible Port: HTTPS, Type: Personnalisé(e)
Spécifiez le port sur la machine qui a l'adresse IP entrée ci-dessous. Dans le cas d'un groupe de port, spécifiez le port de début du groupe (le port de fin sera calculé automatiquement).
Ceci est habituellement identique avec la partie "Depuis le port" spécifiée ci-dessus.

Pare-feu / NAT / Transfert de port

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.](#)

Transfert de port 1:1 Sortant NPt

Règles	Interface	Protocole	Adresse source	Ports source	Adresse de destination	Ports dest.	IP NAT	Ports NAT	Description	Actions
<input type="checkbox"/>	WAN	TCP	*	*	172.17.101.3	443 (HTTPS)	192.168.2.9	443 (HTTPS)	Redirection vers serveur HTTPS dans la DMZ	
<input type="checkbox"/>	WAN	TCP	*	*	WAN address	53 (DNS)	192.168.2.1	53 (DNS)	Redirection vers serveur DNS dans la DMZ	
<input type="checkbox"/>	WAN	UDP	*	*	WAN address	53 (DNS)	192.168.2.1	53 (DNS)	Redirection vers serveur DNS dans la DMZ (UDP)	
<input type="checkbox"/>	WAN	TCP	*	*	172.17.101.2	80 (HTTP)	192.168.2.1	80 (HTTP)	Redirection vers serveur HTTP dans la DMZ	

[Ajouter](#) [Ajouter](#) [Supprimer](#) [Toggle](#) [Enregistrer](#) [Séparateur](#)

(J'ai également modifier la règle avec https d'où j'avais fais une erreur sur l'IP NAT qui était de 192.168.2.9)

Modification de l'adresse du serveur DNS de notre machine physique.

Propriétés de : Protocole Internet version 4 (TCP/IPv4) X

Général Configuration alternative

Les paramètres IP peuvent être déterminés automatiquement si votre réseau le permet. Sinon, vous devez demander les paramètres IP appropriés à votre administrateur réseau.

Obtenir une adresse IP automatiquement

Utiliser l'adresse IP suivante :

Adresse IP :

Masque de sous-réseau :

Passerelle par défaut :

Obtenir les adresses des serveurs DNS automatiquement

Utiliser l'adresse de serveur DNS suivante :

Serveur DNS préféré :

Serveur DNS auxiliaire :

Valider les paramètres en quittant

Avancé...

OK Annuler

7. Mise en place du split DNS.

Le serveur DNS DS2.sio-exupery.fr, situé dans la DMZ, doit indiquer une adresse IP du serveur Web différente en fonction de la source de la requête qui lui est adressée : celle-ci proviendra soit de l'extérieur soit du réseau LAN. Vous allez utiliser pour cela la notion de vue.

```
GNU nano 7.2 /etc/bind/named.conf
// Fichier de configuration générale pour le DNS avec vues.
acl lans {
    192.168.2.0/24;
    192.168.3.0/24;
};

options {
    forward only;
    forwarders { 80.10.246.2; };
    auth-nxdomain no;
};

//Zones de la vue interne

view "interne" {
    match-clients { lans; };
    allow-recursion {lans; };
};
```

```
root@DS2: ~#cat /etc/bind/named.conf.default-zones >> /etc/bind/named.conf
```

```
// prime the server with knowledge of the root servers
//zone "." {
//    type hint;
//    file "/usr/share/dns/root.hints";
//};

// be authoritative for the localhost forward and reverse zones, and for
// broadcast zones as per RFC 1912

zone "localhost" {
    type master;
    file "/etc/bind/db.localhost";
};

zone "127.in-addr.arpa" {
    type master;
    file "/etc/bind/db.127";
};

zone "0.in-addr.arpa" {
    type master;
    file "/etc/bind/db.0";
};

zone "255.in-addr.arpa" {
    type master;
    file "/etc/bind/db.255";
};
```

```
//notre zone vue de l'intérieur

zone "sio-exupery.fr" IN {
    type master;
    file "/var/cache/bind/internals/db.sio-exupery.fr";
    allow-update { none; };
};

zone "2.168.192.in-addr.arpa" IN {
    type master;
    file "/var/cache/bind/internals/rev.sio-exupery.fr";
    allow-update { none; };
};
};
```

```
// zones de la vue externe

zone "sio-exupery.fr" IN {
    type master;
    file "/var/cache/bind/externals/db.sio-exupery.fr";
    allow-update { none; };
};

zone "2.168.192.in-addr.arpa" IN {
    type master;
    file "/var/cache/bind/externals/rev.sio-exupery.fr";
    allow-update { none; };
};
};
```

Création des deux répertoires externes et internes dans `/var/cache/bind/`.

```
root@DS2: ~#mkdir /var/cache/bind/externals/
root@DS2: ~#mkdir /var/cache/bind/internals/
root@DS2: ~#cd /var/cache/bind
root@DS2: /var/cache/bind#ls -l
total 24
-rw-rw-r-- 1 root bind 554 11 avril 19:04 db.sio-exupery.fr
drwxr-xr-x 2 root root 4096 24 avril 17:38 externals
drwxr-xr-x 2 root root 4096 24 avril 17:38 internals
-rw-rw-r-- 1 bind bind 221 25 mars 17:44 managed-keys.bind
-rw-rw-r-- 1 bind bind 2438 25 mars 17:43 managed-keys.bind.jnl
-rw-rw-r-- 1 root bind 201 11 avril 19:06 rev.sio-exupery.fr
root@DS2: /var/cache/bind#
```


Copie des fichiers `db.sio-exupery.fr` et `rev.sio-exupery.fr` existants.

```
root@DS2: ~#cp /var/cache/bind/db.sio-exupery.fr /var/cache/bind/externals/
root@DS2: ~#cp /var/cache/bind/db.sio-exupery.fr /var/cache/bind/externals/
root@DS2: ~#cp /var/cache/bind/rev.sio-exupery.fr /var/cache/bind/externals/
root@DS2: ~#cp /var/cache/bind/rev.sio-exupery.fr /var/cache/bind/externals/
root@DS2: ~#
```

Attribution de ces fichiers de zone au groupe `bind` afin de les rendre accessibles au démon.

```
root@DS2: ~#chgrp bind /var/cache/bind/*
root@DS2: ~#chmod 664 /var/cache/bind/*
root@DS2: ~#chmod 664 /var/cache/bind/externals/*
root@DS2: ~#chmod 664 /var/cache/bind/internals/*
root@DS2: ~#
```

Nous Testons www.sio-exupery.fr, projet1.sio-exupery.fr et secu.sio-exupery.fr depuis notre machine hôte puis depuis depuis UD1/DD1 ou WIN11.



Ce site est inaccessible


192.168.4.10 a mis trop de temps à répondre.

Voici quelques conseils :

- Vérifier la connexion
- Vérifier le proxy et le pare-feu
- Exécutez les diagnostics réseau de Windows

ERR_CONNECTION_TIMED_OUT

[Actualiser](#) [Détails](#)



Ce site est inaccessible

192.168.4.9 a mis trop de temps à répondre.

Voici quelques conseils :

- Vérifier la connexion
- Vérifier le proxy et le pare-feu
- Exécutez les diagnostics réseau de Windows

ERR_CONNECTION_TIMED_OUT

[Actualiser](#) [Détails](#)