

Je configure la carte réseau pour toutes les machines

Je modifie le serveur dns

```
GNU nano 7.2 /etc/bind/named.conf.options
options {
    directory "/var/cache/bind";

    // If there is a firewall between you and nameservers you want
    // to talk to, you may need to fix the firewall to allow multiple
    // ports to talk.  See http://www.kb.cert.org/vuls/id/800113

    // If your ISP provided one or more IP addresses for stable
    // nameservers, you probably want to use them as forwarders.
    // Uncomment the following block, and insert the addresses replacing
    // the all-0's placeholder.

    forwarders {
        172.16.10.20;
        172.16.20.21;
    };

    allow-query {192.168.0.0/16; 172.16.10.0/24; localnets;};
    //=====
    // If BIND logs error messages about the root key being expired,
    // you will need to update your keys.  See https://www.isc.org/bind-keys
    //=====
    dnssec-validation no;

    auth-nxdomain no;    # conform to RFC1035
    listen-on-v6 { any; };
};
```

Je vérifie qu'il n'y a pas d'erreur avec la commande systemctl bind9 status

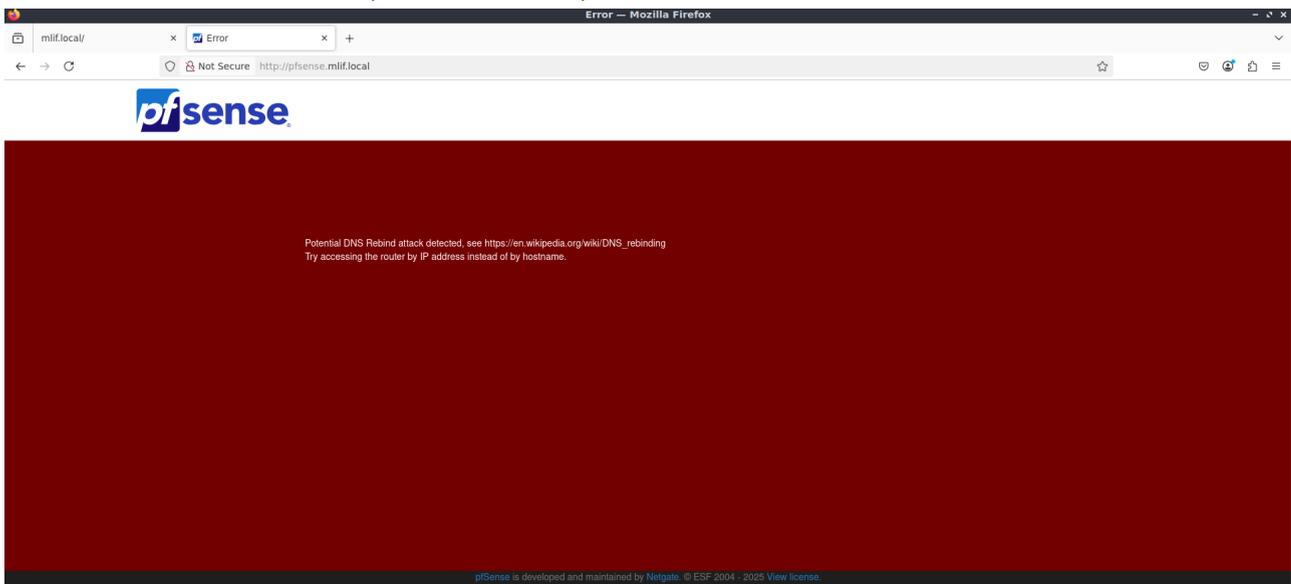
```
root@messagelab:~# systemctl restart bind9
root@messagelab:~# systemctl status bind9
● named.service - BIND Domain Name Server
   Loaded: loaded (/lib/systemd/system/named.service; enabled; preset: enabled)
   Active: active (running) since Fri 2025-09-12 16:39:11 CEST; 7s ago
     Docs: man:named(8)
  Main PID: 983 (named)
    Status: "running"
   Tasks: 4 (limit: 1097)
  Memory: 11.1M
     CPU: 23ms
   CGroup: /system.slice/named.service
           └─983 /usr/sbin/named -f -u bind

sept. 12 16:39:11 messagelab named[983]: zone 255.in-addr.arpa/IN: loaded serial 1
sept. 12 16:39:11 messagelab named[983]: zone 0.in-addr.arpa/IN: loaded serial 1
sept. 12 16:39:11 messagelab named[983]: zone 100.168.192.in-addr.arpa/IN: loaded serial 9
sept. 12 16:39:11 messagelab named[983]: zone localhost/IN: loaded serial 2
sept. 12 16:39:11 messagelab named[983]: zone 127.in-addr.arpa/IN: loaded serial 1
sept. 12 16:39:11 messagelab named[983]: zone 200.168.192.in-addr.arpa/IN: loaded serial 1
sept. 12 16:39:11 messagelab named[983]: zone mlif.local/IN: loaded serial 11
sept. 12 16:39:11 messagelab named[983]: all zones loaded
sept. 12 16:39:11 messagelab systemd[1]: Started named.service - BIND Domain Name Server.
sept. 12 16:39:11 messagelab named[983]: running
root@messagelab:~#
```

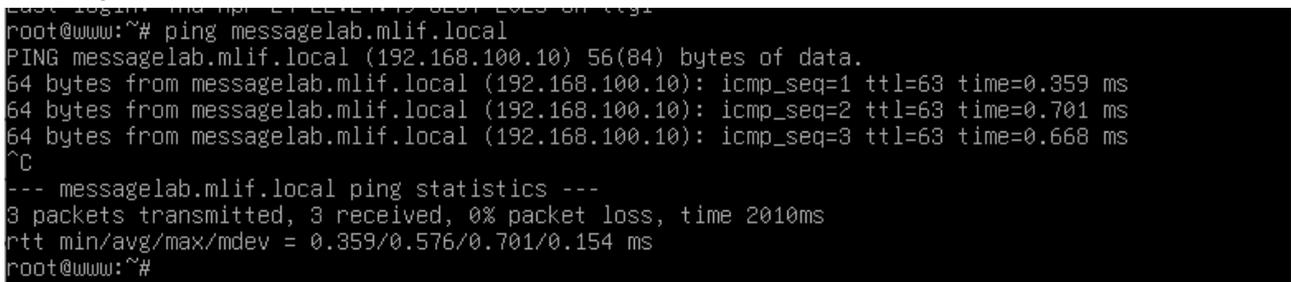
Je test un accès au serveur web



Je me rends sur PFSENSE (192.168.50.254)



Les ping fonctionnent



```
root@www:~# nslookup www.mlif.local
Server:      192.168.100.10
Address:     192.168.100.10#53

Name:   www.mlif.local
Address: 192.168.200.5
```

```
root@www:~# ping www.cisco.com
PING e2867.dsca.akamaiedge.net (2.20.10.35) 56(84) bytes of data:
64 bytes from a2-20-10-35.deploy.static.akamaitechnologies.com (2.20.10.35): icmp_seq=1 ttl=53 time=7.70 ms
64 bytes from a2-20-10-35.deploy.static.akamaitechnologies.com (2.20.10.35): icmp_seq=2 ttl=53 time=8.04 ms
64 bytes from a2-20-10-35.deploy.static.akamaitechnologies.com (2.20.10.35): icmp_seq=3 ttl=53 time=7.49 ms
^C
--- e2867.dsca.akamaiedge.net ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 7.490/7.743/8.042/0.227 ms
root@www:~#
```

Je me connecte sur le pfsense

WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.

Status / Dashboard

System Information	
Name	pf-firewall.mlif.local
User	admin@192.168.50.10 (Local Database)
System	VirtualBox Virtual Machine Netgate Device ID: 94bb399ae96f663a9d0a
BIOS	Vendor: Innatek GmbH Version: VirtualBox Release Date: Fri Dec 1 2006
Version	2.7.0-RELEASE (amd64) built on Wed Jun 28 03:53:34 UTC 2023 FreeBSD 14.0-CURRENT The system is on the latest version. Version information updated at Fri Sep 12 16:32:50 CEST 2025
CPU Type	AMD Ryzen 7 PRO 5750G with Radeon Graphics AES-NI CPU Crypto: Yes (inactive) QAT Crypto: No
Hardware crypto	Inactive
Kernel PTI	Disabled
MDS Mitigation	Inactive

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.	
<ul style="list-style-type: none">Upgrade Your SupportNetgate Global Support FAQNetgate Professional Services	<ul style="list-style-type: none">Community Support ResourcesOfficial pfSense Training by NetgateVisit 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.	

Je me rends sur l'onglet firewall puis Rules

WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.

Firewall / Rules / WAN

Floating: WAN LAN SRV DMZ

Rules (Drag to Change Order)											
<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
No rules are currently defined for this interface All incoming connections on this interface will be blocked until pass rules are added. Click the button to add a new rule.											

Buttons: Add, Add, Delete, Toggle, Copy, Save, Separator

pfSense is developed and maintained by Netgate. © ESP 2004 - 2025 View license.

Je supprime les règle DMZ

The screenshot shows the pSense Firewall Rules configuration page for the DMZ interface. At the top, there is a warning message: "WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager." Below this, the breadcrumb navigation is "Firewall / Rules / DMZ". There are tabs for "Floating", "WAN", "LAN", "SRV", and "DMZ", with "DMZ" being the active tab. A table titled "Rules (Drag to Change Order)" contains one rule with the following details:

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	0/5 KIB	IPv4 *	*	*	*	*	none			↓ ↑ Delete Toggle Copy Save + Separator

At the bottom of the page, it says "pSense is developed and maintained by Netgate. © ESF 2004 - 2025 View license."

Je supprime les règles lié au serveur

The screenshot shows the pSense Firewall Rules configuration page for the SRV interface. A green message box at the top states: "The changes have been applied successfully. The firewall rules are now reloading in the background. Monitor the filter reload progress." Below this, the breadcrumb navigation is "Firewall / Rules / SRV". There are tabs for "Floating", "WAN", "LAN", "SRV", and "DMZ", with "SRV" being the active tab. A table titled "Rules (Drag to Change Order)" is empty, with a message below it: "No rules are currently defined for this interface. All incoming connections on this interface will be blocked until pass rules are added. Click the button to add a new rule." At the bottom, there are buttons for "Add", "Delete", "Toggle", "Copy", "Save", and "Separator".

Je supprime les règles Clients

The screenshot shows the pSense Firewall Rules configuration page for the WAN interface. The breadcrumb navigation is "Firewall / Rules / WAN". There are tabs for "Floating", "WAN", "LAN", "SRV", and "DMZ", with "WAN" being the active tab. A table titled "Rules (Drag to Change Order)" is empty, with a message below it: "No rules are currently defined for this interface. All incoming connections on this interface will be blocked until pass rules are added. Click the button to add a new rule." At the bottom, there are buttons for "Add", "Delete", "Toggle", "Copy", "Save", and "Separator".

Suite a mes modifications , les pings ne fonctionnent plus

```
root@www:~# ping messagelab.mlif.local
^C
root@www:~# ping www.cisco.com
^C
root@www:~# _
```

STOP1

J'ai ajouté les aliases pour les adresses IP

IP Ports URLs All

Firewall Aliases IP			
Name	Values	Description	Actions
DEBIAN_TRAINING_DMZ	192.168.200.5		  
DEBIAN_TRAINING_SERVEUR	192.168.100.10		  
IPS_DNS_LYCEE	IP_DNS_LYCEE_1, IPS_DNS_LYCEE_2		  
IPS_DNS_LYCEE_2	172.16.10.21		  
IP_BLACKLIST_CLIENTS	192.168.50.20		  
IP_DNS_LYCEE_1	172.16.10.20		  
SRV_DNS	192.168.100.10		  
SRV_FTP	192.168.100.10		  
SRV_MAIL	192.168.100.10		  

 Add  Import



J'ai ajouté les aliasse concernant les ports

IP **Ports** URLs All

Firewall Aliases Ports

Name	Values	Description	Actions
PORT_DNS	53		  
PORT_IMAP	143		  
PORT_MAIL	PORT_IMAP, PORT_SMTP		  
PORT_SMTP	25		  
PORT_WEB	80, 443		  

 Add  Import

WARNING: The 'admin' account password is set to the default value. [Change the password in the User Manager.](#)

Firewall / Rules / DMZ   

Floating WAN LAN SRV **DMZ**

Rules (Drag to Change Order)

<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✓ 0/0 B	IPv4 UDP	DMZ net	*	SRV_DNS	53 (DNS)	*	none			  

 Add  Add  Delete  Toggle  Copy  Save  Separator



WARNING: The 'admin' account password is set to the default value. [Change the password in the User Manager.](#)

Firewall / Rules / LAN   

Floating WAN **LAN** SRV DMZ

Rules (Drag to Change Order)

<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✓ 1/2.23 MiB	*	*	*	LAN Address	80	*	*		Anti-Lockout Rule	
<input type="checkbox"/>	✗ 0/0 B	IPv4 UDP	IP_BLACKLIST_CLIENTS	*	SRV_DNS	53 (DNS)	*	none			  
<input type="checkbox"/>	✓ 9/12 KiB	IPv4 UDP	LAN net	*	SRV_DNS	53 (DNS)	*	none			  

 Add  Add  Delete  Toggle  Copy  Save  Separator



```
root@www:~#  
root@www:~# systemctl restart networking  
root@www:~#
```

R1 VALIDÉ

R2 VALIDÉ

Firewall / Rules / SRV

Floating WAN LAN **SRV** DMZ

Rules (Drag to Change Order)

<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✓	0/4 KiB	IPv4 UDP	SRV_DNS	*	IPS_DNS_LYCEE	53 (DNS)	*	none		

↑ Add ↓ Add Delete Toggle Copy Save + Separator

R3 VALIDÉ

Firewall / Rules / SRV

Floating WAN LAN **SRV** DMZ

The changes have been applied successfully. The firewall rules are now reloading in the background. Monitor the filter reload progress.

Rules (Drag to Change Order)

<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✓	0/0 B	IPv4 TCP	DEBIAN_TRAINING_DMZ	*	DEBIAN_TRAINING_DMZ	*	*	none		
<input type="checkbox"/>	✓	4/10 KiB	IPv4 UDP	SRV_DNS	*	IPS_DNS_LYCEE	53 (DNS)	*	none		

↑ Add ↓ Add Delete Toggle Copy Save + Separator

Firewall / Rules / LAN

Floating WAN **LAN** SRV DMZ

The changes have been applied successfully. The firewall rules are now reloading in the background. Monitor the filter reload progress.

Rules (Drag to Change Order)

<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✓	1/2.75 MiB	*	*	LAN Address	80	*	*		Anti-Lockout Rule	
<input type="checkbox"/>	✓	0/0 B	IPv4 TCP	LAN net	*	*	PORT_WEB	*	none	LE CLIENT ACCEDE A INTERNET	
<input type="checkbox"/>	✗	0/0 B	IPv4 UDP	IP_BLACKLIST_CLIENTS	*	SRV_DNS	53 (DNS)	*	none		
<input type="checkbox"/>	✓	2/194 KiB	IPv4 UDP	LAN net	*	SRV_DNS	53 (DNS)	*	none		

↑ Add ↓ Add Delete Toggle Copy Save + Separator

R4

STOP 2

Firewall / NAT / Port Forward ?

The changes have been applied successfully. The firewall rules are now reloading in the background.
[Monitor](#) the filter reload progress. ✕

Port Forward 1:1 Outbound NPT

Rules										
<input type="checkbox"/>	Interface	Protocol	Source Address	Source Ports	Dest. Address	Dest. Ports	NAT IP	NAT Ports	Description	Actions
<input type="checkbox"/>	<input checked="" type="checkbox"/> WAN	TCP	*	*	WAN address	PORT_WEB	192.168.200.5	PORT_WEB		

↑ Add ↓ Add 🗑 Delete 🔄 Toggle 💾 Save + Separator