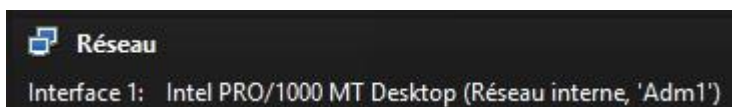
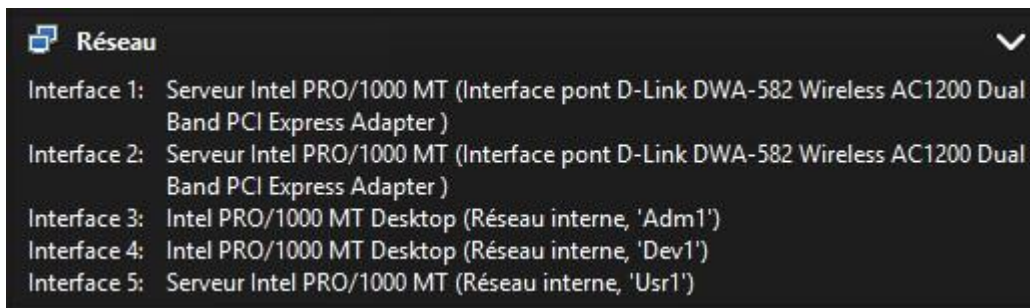


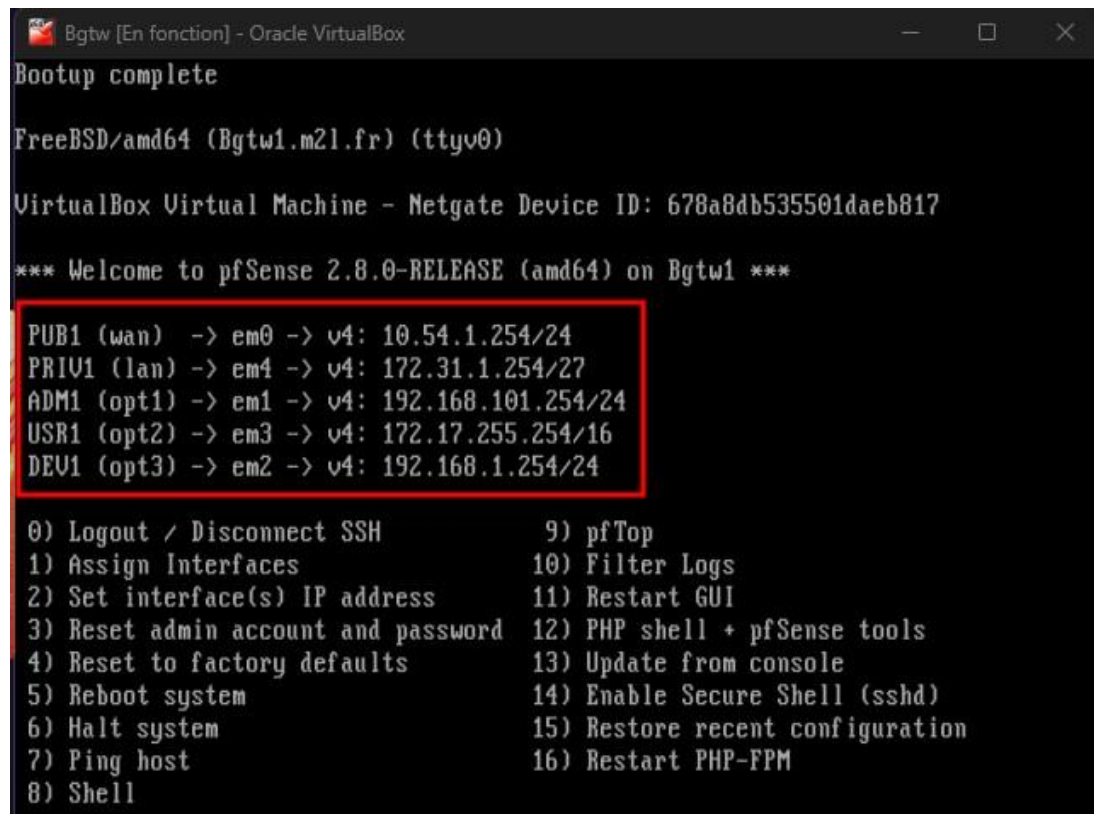
DOCUMENTATION BGTW

Installation des machines virtuelles :



Les cartes réseaux sont différent car je réalise les rendus chez moi.

Mise en place du routeur Bgtw :



```
Bgtw [En fonction] - Oracle VirtualBox
Bootup complete

FreeBSD/amd64 (Bgtw1.m21.fr) (ttyv0)

VirtualBox Virtual Machine - Netgate Device ID: 678a8db535501daeb817

*** Welcome to pfSense 2.8.0-RELEASE (amd64) on Bgtw1 ***


PUB1 (wan) -> em0 -> v4: 10.54.1.254/24
PRIV1 (lan) -> em4 -> v4: 172.31.1.254/27
ADM1 (opt1) -> em1 -> v4: 192.168.101.254/24
USR1 (opt2) -> em3 -> v4: 172.17.255.254/16
DEV1 (opt3) -> em2 -> v4: 192.168.1.254/24

0) Logout / Disconnect SSH          9) pfTop
1) Assign Interfaces                10) Filter Logs
2) Set interface(s) IP address     11) Restart GUI
3) Reset admin account and 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
```

D'abord nous avons ajouté les cartes réseaux 5 au total. Pour mettre en place le 5ème on devait utiliser un programme qui nous été fourni.

Il fallait faire attention à ne pas se tromper d'adresses IP pendant l'assignement. Sinon ça ne fonctionnera pas. Ensuite on utilise un Kali pour l'administrer.

Dashboard :


System ▾ Interfaces ▾ Firewall ▾ Services ▾ VPN ▾ Status ▾ Diagnostics ▾ Help ▾

Status / Dashboard

+

?

System Information

Name

Bgtw1.m2l.fr

User

admin@192.168.101.28 (Local Database)

Version

2.8.0-RELEASE (amd64)
built on Tue Aug 12 16:59:00 UTC 2025
FreeBSD 15.0-CURRENT
Error in version information

Uptime

00 Hour 46 Minutes 50 Seconds

Current date/time

Sat Feb 7 14:15:52 UTC 2026

DNS server(s)

- 192.168.51.254

Last config change

Fri Jan 16 15:25:40 UTC 2026

State table size

0% (24/96000)
Show states

MBUF Usage

1% (5334/1000000)

CPU usage

3%

Memory usage

31% of 968 MiB

SWAP usage

0% of 1024 MiB

Disks

Mount	Used	Size	Usage
/var	260K	41G	0% of 41G (zfs)
/	1.0G	42G	2% of 42G (zfs)

Interfaces

PUB1

↑

1000baseT <full-duplex>

10.54.1.254

PRIV1

↑

1000baseT <full-duplex>

172.31.1.254

ADM1

↑

1000baseT <full-duplex>

192.168.101.254

USR1

↑

1000baseT <full-duplex>

172.17.255.254

DEV1

↑

1000baseT <full-duplex>

192.168.1.254

Gateways

Name

RTT

RTTsd

Loss

Status

No gateways found.

Services Status



Service

Description

Action



dnsmasq

DNS Forwarder



kea-dhcp4

Kea DHCP Server

syslogd

System Logger Daemon

NTP Status

NTP Server is disabled

Installed Packages

No packages installed.






Packages may be added/managed here: [System -> Packages](#)

Status.Interfaces :

Status / Interfaces	
PUB1 Interface (wan, em0)	
Status	up
MAC Address	08:00:27:d9:39:24
IPv4 Address	10.54.1.254
Subnet mask IPv4	255.255.255.0
IPv6 Link Local	fe80::a00:27ff:fed9:3924%em0
MTU	1500
Media	1000baseT <full-duplex>
In/out packets	502/0 (125 KiB/0 B)
In/out packets (pass)	502/0 (125 KiB/0 B)
In/out packets (block)	28/0 (2 KiB/0 B)
In/out errors	0/0
Collisions	0
PRIV1 Interface (lan, em4)	
Status	up
MAC Address	08:00:27:da:d0:af
IPv4 Address	172.31.1.254
Subnet mask IPv4	255.255.255.224
IPv6 Link Local	fe80::a00:27ff:fed9:d0af%em4
MTU	1500
Media	1000baseT <full-duplex>
In/out packets	1424/0 (333 KiB/0 B)
In/out packets (pass)	1424/0 (333 KiB/0 B)
In/out packets (block)	62/0 (5 KiB/0 B)
In/out errors	0/0
Collisions	0
ADM1 Interface (opt1, em1)	
Status	up
MAC Address	08:00:27:65:87:dd
IPv4 Address	192.168.101.254
Subnet mask IPv4	255.255.255.0
IPv6 Link Local	fe80::a00:27ff:fe65:87dd%em1
MTU	1500
Media	1000baseT <full-duplex>
In/out packets	632/885 (150 KiB/668 KiB)
In/out packets (pass)	632/885 (150 KiB/668 KiB)
In/out packets (block)	0/1 (0 B/88 B)
In/out errors	0/0
Collisions	0
USR1 Interface (opt2, em3)	
Status	up
MAC Address	08:00:27:01:2f:de
IPv4 Address	172.17.255.254
Subnet mask IPv4	255.255.0.0
IPv6 Link Local	fe80::a00:27ff:fe01:2fde%em3
MTU	1500
Media	1000baseT <full-duplex>
In/out packets	0/0 (0 B/0 B)
In/out packets (pass)	0/0 (0 B/0 B)
In/out packets (block)	0/0 (0 B/0 B)
In/out errors	0/0
Collisions	0
DEV1 Interface (opt3, em2)	
Status	up
MAC Address	08:00:27:1f:4b:e0
IPv4 Address	192.168.1.254
Subnet mask IPv4	255.255.255.0
IPv6 Link Local	fe80::a00:27ff:fe1f:4be0%em2
MTU	1500
Media	1000baseT <full-duplex>
In/out packets	0/0 (0 B/0 B)
In/out packets (pass)	0/0 (0 B/0 B)
In/out packets (block)	0/5 (0 B/384 B)
In/out errors	0/0
Collisions	0

Voici les 5 cartes réseaux. Avec toutes les informations nécessaires.

Status.Services :

Status / Services			
Services			
Service	Description	Status	Actions
dnsmasq	DNS Forwarder	✓	   
kea-dhcp4	Kea DHCP Server	✓	   
syslogd	System Logger Daemon	✓	   

Service.Dns-forwarder :

Services / DNS Forwarder

General DNS Forwarder Options

Enable ☒ Enable DNS forwarder

Ignore System DNS

☐ Do not use system DNS servers

If this option is set the configured system DNS servers will be ignored and custom "server=" options must be used.

DNS Query Forwarding

☐ Query DNS servers sequentially

If this option is set pfSense DNS Forwarder (dnsmasq) will query the DNS servers sequentially in the order specified (System - General Setup - DNS Servers), rather than all at once in parallel.

☐ Require domain

If this option is set pfSense DNS Forwarder (dnsmasq) will not forward A or AAAA queries for plain names, without dots or domain parts, to upstream name servers. If the name is not known from /etc/hosts or DHCP then a "not found" answer is returned.

☐ Do not forward private reverse lookups

If this option is set pfSense DNS Forwarder (dnsmasq) will not forward reverse DNS lookups (PTR) for private addresses (RFC 1918) to upstream name servers. Any entries in the Domain Overrides section forwarding private "n.n.n.in-addr.arpa" names to a specific server are still forwarded. If the IP to name is not known from /etc/hosts, DHCP or a specific domain override then a "not found" answer is immediately returned.

Listen Port

53

The port used for responding to DNS queries. It should normally be left blank unless another service needs to bind to TCP/UDP port 53.

Interfaces

PRV1

ADM1

USR1

DEV1

Other IPv6 Link Local

Interface IPs used by the DNS Forwarder for responding to queries from clients. If an interface has both IPv4 and IPv6 IPs, both are used. Queries to other interface IPs not selected above are discarded. The default behavior is to respond to queries on every available IPv4 and IPv6 address.

Strict binding

☐ Strict interface binding

If this option is set, the DNS forwarder will only bind to the interfaces containing the IP addresses selected above, rather than binding to all interfaces and discarding queries to other addresses.

This option does NOT work with IPv6. If set, dnsmasq will not bind to IPv6 addresses.

Il faut l'activer et choisir les interfaces dont on veut l'appliquer.

Diagnostic.Routes :

IPv4 Routes						
Destination	Gateway	Flags	Uses	MTU	Interface	Expire
10.54.1.0/24	link#1	U	1	1500	em0	
10.54.1.254	link#7	UHS	3	16384	lo0	
127.0.0.1	link#7	UH	2	16384	lo0	
172.17.0.0/16	link#4	U	8	1500	em3	
172.17.255.254	link#7	UHS	9	16384	lo0	
172.31.1.224/27	link#5	U	4	1500	em4	
172.31.1.254	link#7	UHS	5	16384	lo0	
192.168.1.0/24	link#3	U	10	1500	em2	
192.168.1.254	link#7	UHS	11	16384	lo0	
192.168.101.0/24	link#2	U	6	1500	em1	
192.168.101.254	link#7	UHS	7	16384	lo0	

Diagnostics.Sockets :

IPv4 System Socket Information						
USER	COMMAND	PID	FD	PROTO	LOCAL	FOREIGN
root	php-fpm	65015	4	udp4	*:*	*:*
root	kea-dhcp4	82610	16	udp4	192.168.101.254:67	*:*
root	kea-dhcp4	82610	18	udp4	192.168.1.254:67	*:*
root	kea-dhcp4	82610	20	udp4	172.17.255.254:67	*:*
root	php-fpm	37290	4	udp4	*:*	*:*
root	syslogd	93711	10	udp4	*:514	*:*
root	nginx	56945	5	tcp4	*:80	*:*
root	nginx	56828	5	tcp4	*:80	*:*
root	nginx	56540	5	tcp4	*:80	*:*
nobody	dnsmasq	11105	4	udp4	*:53	*:*
nobody	dnsmasq	11105	5	tcp4	*:53	*:*
root	php-fpm	428	4	udp4	*:*	*:*
root	php-fpm	427	4	udp4	*:*	*:*
root	php-fpm	426	4	udp4	*:*	*:*

Firewall.nat.port-forward :

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
--------------------------	-----------	--------	-------------	-------------	------------------	-------------	----------	-------------	-------------	---------

[Add](#) [Add](#) [Delete](#) [Toggle](#) [Save](#)

Il faut désactiver le firewall outbound du côté Back Gateway.

Services.dhcp-server :

pfSense COMMUNITY EDITION System Interfaces Firewall Services VPN Status Diagnostics Help

Services / DHCP Server / Settings

Settings PUB1 PRIV1 ADM1 USR1 DEV1

General Settings

DNS Registration ☐ Enable DNS registration
Default DNS registration policy for DHCP server.
When checked, DHCP leases will automatically be registered with the DNS Resolver.

Early DNS Registration ☐ Enable early DNS registration
Default early DNS registration policy for DHCP server.
When checked, DHCP static mappings will automatically be pre-registered with the DNS Resolver.

Pub 1 :

Primary Address Pool	
Subnet	10.54.1.0/24
Subnet Range	10.54.1.1 - 10.54.1.254
Address Pool Range	<input type="text"/> From To
The specified range for this pool must not be within the range configured on any other address pool for this interface.	
Additional Pools	<input type="button" value="+ Add Address Pool"/>
If additional pools of addresses are needed inside of this subnet outside the above range, they may be specified here.	

Priv 1 :

Primary Address Pool	
Subnet	172.31.1.224/27
Subnet Range	172.31.1.225 - 172.31.1.254
Address Pool Range	<input type="text" value="192.168.1.100"/> From To <input type="text" value="192.168.1.199"/>
The specified range for this pool must not be within the range configured on any other address pool for this interface.	
Additional Pools	<input type="button" value="+ Add Address Pool"/>
If additional pools of addresses are needed inside of this subnet outside the above range, they may be specified here.	

Adm 1 :

Primary Address Pool	
Subnet	192.168.101.0/24
Subnet Range	192.168.101.1 - 192.168.101.254
Address Pool Range	<input type="text" value="192.168.101.10"/> From To <input type="text" value="192.168.101.200"/>
The specified range for this pool must not be within the range configured on any other address pool for this interface.	
Additional Pools	<input type="button" value="+ Add Address Pool"/>
If additional pools of addresses are needed inside of this subnet outside the above range, they may be specified here.	

Usr 1 :

Primary Address Pool	
Subnet	172.17.0.0/16
Subnet Range	172.17.0.1 - 172.17.255.254
Address Pool Range	<input type="text" value="172.17.1.10"/> From To <input type="text" value="172.17.1.200"/>
The specified range for this pool must not be within the range configured on any other address pool for this interface.	
Additional Pools	<input type="button" value="+ Add Address Pool"/>
If additional pools of addresses are needed inside of this subnet outside the above range, they may be specified here.	

Dev 1 :

Primary Address Pool

Subnet

192.168.1.0/24

Subnet Range

192.168.1.1 - 192.168.1.254

Address Pool Range

192.168.1.10

192.168.1.200

From

To

The specified range for this pool must not be within the range configured on any other address pool for this interface.





































Additional Pools

+ Add Address Pool

If additional pools of addresses are needed inside of this subnet outside the above range, they may be specified here.

Voici toutes les adresses IP et les plages de tous les réseaux.

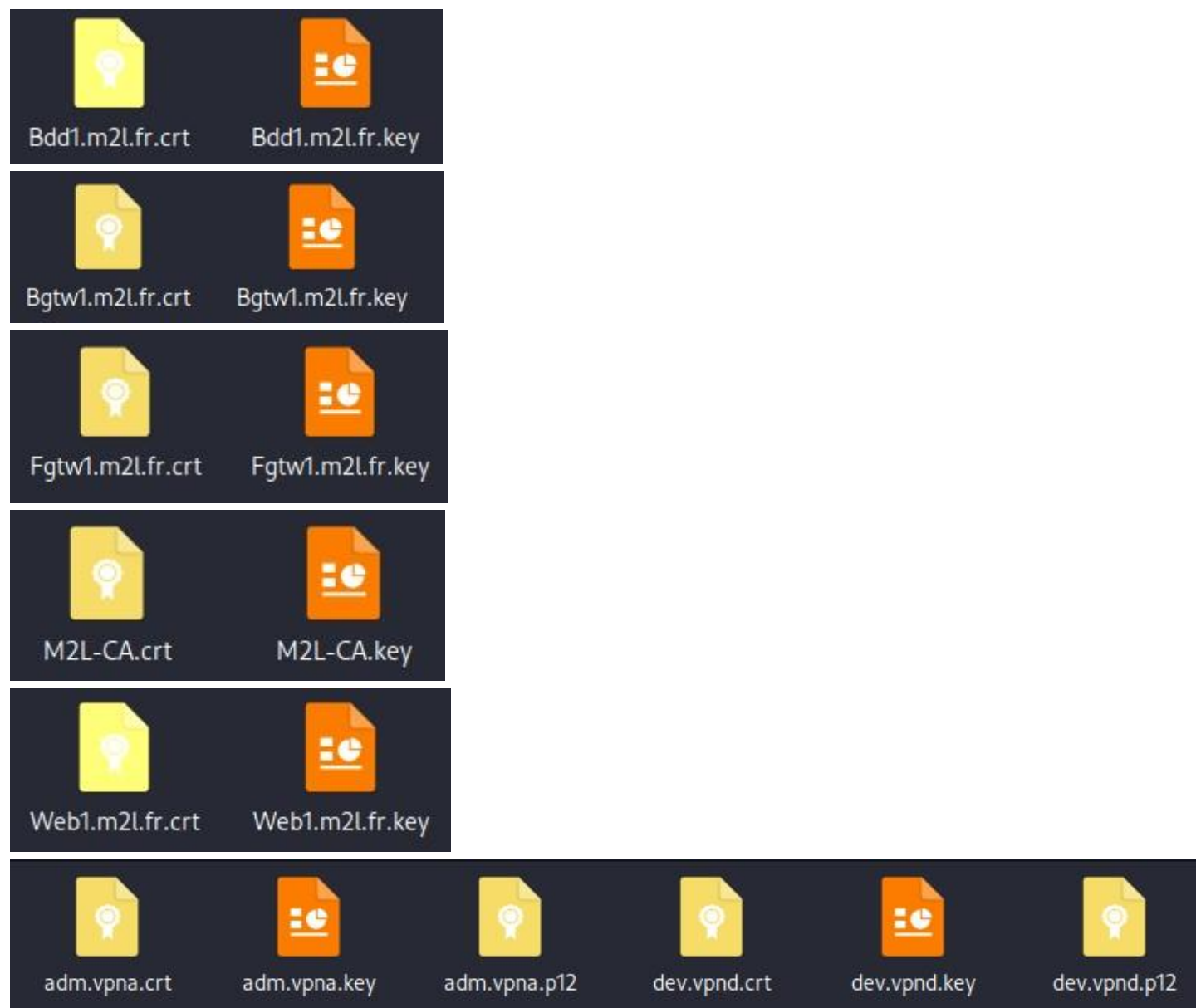
System.Certificats :

Bgtw1.m2l.fr Server Certificate CA: No Server: Yes	M2L-CA	CN=Bgtw1.m2l.fr Valid From: Sun, 14 Dec 2025 13:17:41 +0000 Valid Until: Wed, 12 Dec 2035 13:17:41 +0000	     
Fgtw1.m2l.fr Server Certificate CA: No Server: Yes	M2L-CA	CN=Fgtw1.m2l.fr Valid From: Sun, 14 Dec 2025 13:21:17 +0000 Valid Until: Wed, 12 Dec 2035 13:21:17 +0000	     
Bdd1.m2l.fr Server Certificate CA: No Server: Yes	M2L-CA	CN=Bdd1.m2l.fr Valid From: Sun, 14 Dec 2025 13:23:17 +0000 Valid Until: Wed, 12 Dec 2035 13:23:17 +0000	     
Web1.m2l.fr Server Certificate CA: No Server: Yes	M2L-CA	CN=Web1.m2l.fr Valid From: Sun, 14 Dec 2025 13:24:53 +0000 Valid Until: Wed, 12 Dec 2035 13:24:53 +0000	     
adm.vpna User Certificate CA: No Server: No	M2L-CA	CN=adm.vpna Valid From: Sun, 14 Dec 2025 13:27:09 +0000 Valid Until: Wed, 12 Dec 2035 13:27:09 +0000	     
dev.vpnd User Certificate CA: No Server: No	M2L-CA	CN=dev.vpnd Valid From: Sun, 14 Dec 2025 13:27:36 +0000 Valid Until: Wed, 12 Dec 2035 13:27:36 +0000	     

Et certificat d'autorité,

M2L-CA	✓	self-signed	6	CN=internal-ca Valid From: Sun, 14 Dec 2025 13:12:21 +0000 Valid Until: Wed, 12 Dec 2035 13:12:21 +0000	     
--------	---	-------------	---	---	---

Et voici tous les certificats :



Firewall.rules :

Pub 1 :

Firewall / Rules / PUB1

Floating PUB1 PRIV1 ADM1 USR1 DEV1

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✓	8/444 KiB	IPv4 *	*	*	*	*	none		TOUT PASSE	

Add Add Delete Toggle Copy Save Separator

Priv 1 :

Firewall / Rules / PRIV1

Floating PUB1 PRIV1 ADM1 USR1 DEV1

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	✓	0/1 KiB	*	*	PRIV1 Address	80	*	*		Anti-Lockout Rule	
<input type="checkbox"/>	✓	9/244 KiB	IPv4 *	*	*	*	*	none		TOUT PASSE	

Add Add Delete Toggle Copy Save Separator

Adm 1 :

Firewall / Rules / ADM1

Floating PUB1 PRIV1 ADM1 USR1 DEV1

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✓	1/1.15 MiB	IPv4 *	*	*	*	*	none		TOUT PASSE	

Add Add Delete Toggle Copy Save Separator

Usr 1 :

Firewall / Rules / USR1

Floating PUB1 PRIV1 ADM1 USR1 DEV1

Rules (Drag to Change Order)

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

Add Add Delete Toggle Copy Save Separator

Dev 1 :

Firewall / Rules / DEV1

Floating PUB1 PRIV1 ADM1 USR1 DEV1

Rules (Drag to Change Order)

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

Add Add Delete Toggle Copy Save Separator