

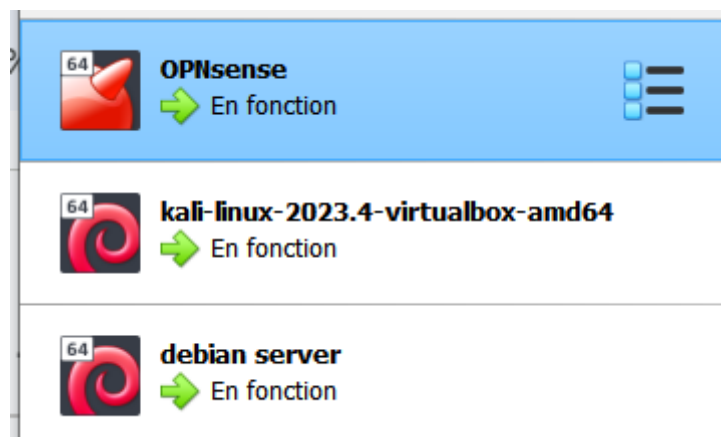
Rapport Stage

SOMMAIRE

1. Test d'un serveur web apache 2
2. Création d'un serveur reverse proxy
3. Test d'un certificat sur plusieurs noms de domaine
4. Migration OPNSense virtualbox vers VMWare
5. Ajout serveur web clients sur OPNSense

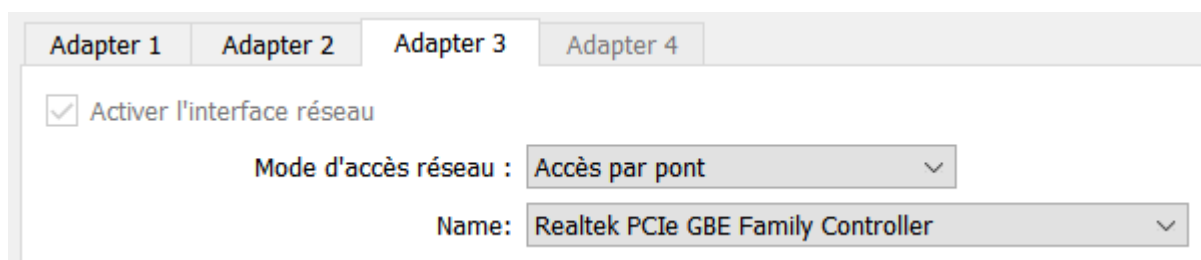
Je vais mettre en place un serveur web apache2 avec un pare-feu opnsense à l'aide de virtualbox. L'objectif final est de remplacer un pfsense par un opnsense sur vmware qui gère des sites internet de clients afin de pouvoir mettre un certificat sur plusieurs noms de domaines d'où l'intérêt de mettre en place un serveur reverse proxy.

-Vm nécessaire
Opnsense
Kali
Debian serveur



-Interface nécessaire
LAN en accès par pont brancher sur le cable ethernet
WAN sur la carte wifi
LAN SECURE en réseau interne

-Positionnement et configuration des interfaces sur chaque vm
OPNsense:
*LAN 10.0.0.176/24 en DHCP



*WAN 192.168.6.70/24 en DHCP

Adapter 1	Adapter 2	Adapter 3	Adapter 4
<input checked="" type="checkbox"/> Activer l'interface réseau			
Mode d'accès réseau : Accès par pont			
Name: Intel(R) Centrino(R) Advanced-N 6235			

*LAN SECURE 192.168.1.1/24 en static

Adapter 1	Adapter 2	Adapter 3	Adapter 4
<input checked="" type="checkbox"/> Activer l'interface réseau			
Mode d'accès réseau : Réseau interne			
Name: lan			

KALI:

IP 192.168.1.100

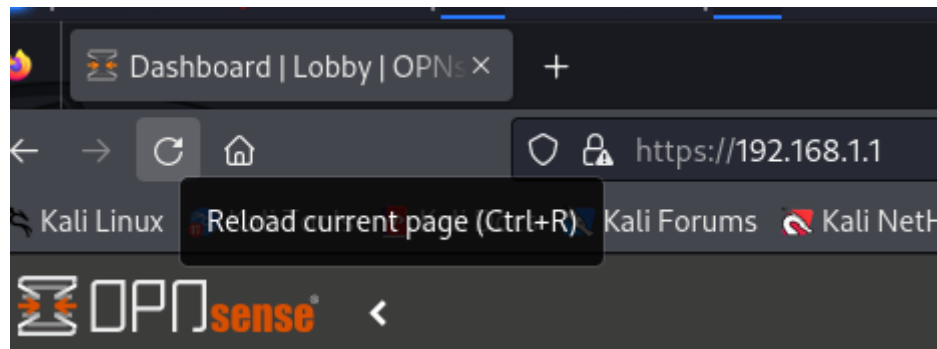
Adapter 1	Adapter 2	Adapter 3	Adapter 4
<input checked="" type="checkbox"/> Activer l'interface réseau			
Mode d'accès réseau : Réseau interne			
Name: lan			

Debian serveur:

IP 192.168.1.101

Adapter 1	Adapter 2	Adapter 3	Adapter 4
<input checked="" type="checkbox"/> Activer l'interface réseau			
Mode d'accès réseau : Réseau interne			
Name: lan			

Maintenant sur Kali on va pouvoir accéder à l'interface web de l'opnsense avec l'adresse du LAN SECURE qui est 192.168.1.1



Nous allons mettre une règle sur le LAN SECURE du pare-feu opnsense qui va nous permettre la bonne communication de kali et debian serveur qui finissent en 100 et en 101 vers n'importe quelle adresse, cela va nous être utile pour communiquer avec internet et ainsi installer apache2.

Firewall, rules, opt1:

<input type="checkbox"/>	Protocol	Source	Port	Destination	Port	Gateway	Schedule
<input type="checkbox"/>							
<input type="checkbox"/>	IPv4 *	OPT1 net	*	*	*	*	*

Depuis kali nous pouvons ping google:

```
(kali㉿kali)-[~]  
$ ping 8.8.8.8  
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.  
64 bytes from 8.8.8.8: icmp_seq=1 ttl=115 time=13.7 ms  
64 bytes from 8.8.8.8: icmp_seq=2 ttl=115 time=9.93 ms  
64 bytes from 8.8.8.8: icmp_seq=3 ttl=115 time=9.24 ms
```

De même depuis debian serveur:

```
root@debian-server:/home/user# ping 8.8.8.8  
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.  
64 bytes from 8.8.8.8: icmp_seq=1 ttl=115 time=10.7 ms  
64 bytes from 8.8.8.8: icmp_seq=2 ttl=115 time=10.2 ms  
64 bytes from 8.8.8.8: icmp_seq=3 ttl=115 time=10.2 ms  
64 bytes from 8.8.8.8: icmp_seq=4 ttl=115 time=9.77 ms
```

Il nous reste plus qu'à procéder à l'installation d'apache2 sur debian serveur.

La première étape est de se mettre en mode root en tapant sudo su et se connecter avec les codes de l'opnsense login root et password root.

```
user@debian-server:~$ sudo su
[sudo] password for user:
```

```
root@debian-server:/home/user#
```

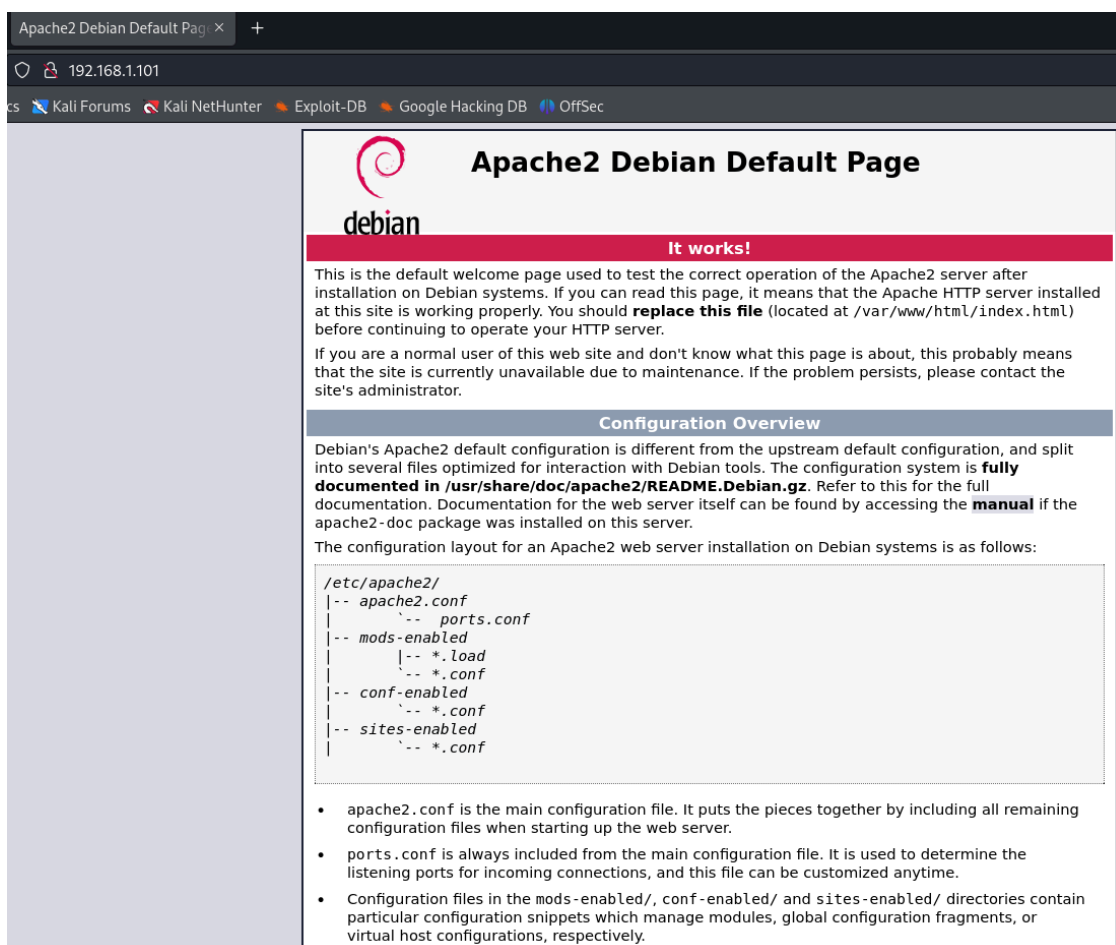
Ensuite il faut lancer un apt update pour mettre à jour les paquets. Une mise à jour se lancera.

```
root@debian-server:/home/user# apt update
```

Une fois fini on peut installer apache 2 en tapant apt install apache2

```
root@debian-server:/home/user# apt install apache2
```

Une fois l'installation terminée on peut désormais accéder au site apache2 depuis la kali grâce à l'ip du debian serveur qui a été attribué en DHCP donc 192.168.1.101



Apache2 Debian Default Page

192.168.1.101

Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

Apache2 Debian Default Page

debian

It works!

This is the default welcome page used to test the correct operation of the Apache2 server after installation on Debian systems. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should **replace this file** (located at `/var/www/html/index.html`) before continuing to operate your HTTP server.

If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.

Configuration Overview

Debian's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Debian tools. The configuration system is **fully documented in `/usr/share/doc/apache2/README.Debian.gz`**. Refer to this for the full documentation. Documentation for the web server itself can be found by accessing the **manual** if the `apache2-doc` package was installed on this server.

The configuration layout for an Apache2 web server installation on Debian systems is as follows:

```
/etc/apache2/
|-- apache2.conf
|   |-- ports.conf
|-- mods-enabled
|   |-- *.load
|   |-- *.conf
|-- conf-enabled
|   |-- *.conf
|-- sites-enabled
|   |-- *.conf
```

- `apache2.conf` is the main configuration file. It puts the pieces together by including all remaining configuration files when starting up the web server.
- `ports.conf` is always included from the main configuration file. It is used to determine the listening ports for incoming connections, and this file can be customized anytime.
- Configuration files in the `mods-enabled/`, `conf-enabled/` and `sites-enabled/` directories contain particular configuration snippets which manage modules, global configuration fragments, or virtual host configurations, respectively.

2.Création d'un serveur reverse proxy

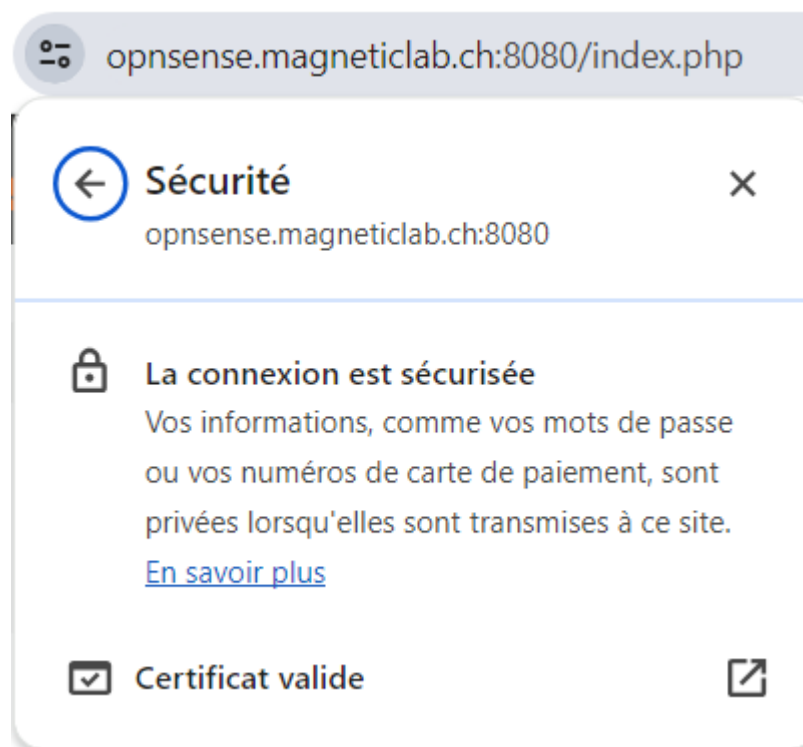
Avant de mettre en place le reverse proxy il faut sécuriser la zone dmz et mettre en place un certificat valide. Pour cela nous allons commencer par mettre en place des règles sur le opt1. Le pare feu écoutera sur le port 80 et 433 pour rediriger vers apache2 sur WAN en TCP

<input type="checkbox"/>		IPv4 TCP	*	*	This Firewall	80 (HTTP)	*	*	reverse proxy			
<input type="checkbox"/>		IPv4 TCP	*	*	This Firewall	443 (HTTPS)	*	*	reverse proxy			
<input type="checkbox"/>		IPv4 TCP/UDP	OPT1 net	*	OPT1 address	53 (DNS)	*	*	autoriser l'accès au serveur DNS			
<input type="checkbox"/>		IPv4 TCP/UDP	OPT1 net	*	*	53 (DNS)	*	*	Bloquer l'accès à tout les autres serveurs DNS			
<input type="checkbox"/>		IPv4 *	OPT1 net	*	! MonServeur	*	*	*	Autoriser l'accès à internet et bloquer l'accès à tous les réseaux locaux			

Ensuite nous allons utiliser un certificat fournit par infomaniac avec notre nom de domaine magneticlab un qui sera opnsense.magneticlab.ch qui nous permettra d'accéder au parefeu depuis le web et le second qui nous servira pour utiliser le reverse proxy donc nous rediriger sur apache 2 est ilias.magneticlab.ch

Ajout du certificat sur opnsense grâce à la clé publique et à la clé privé qui nous à été fourni

.magneticlab.ch	external	CN=.magneticlab.ch	Valid From:	Tue, 23 May 2023 00:00:00 +0000
CA: No, Server: Yes			Valid Until:	Sat, 22 Jun 2024 23:59:59 +0000

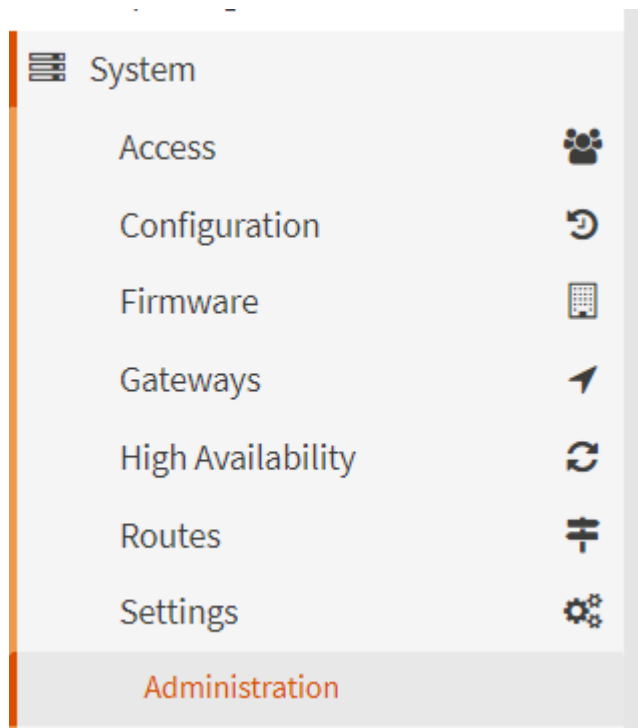


Nous allons maintenant mettre en place un reverse proxy à l'aide du plugin caddy.

Système, firmware, plugin

os-caddy (installed)	1.4.4	106KiB	3	os-caddy-plugin	Easy to configure Reverse Proxy based on Caddy with Automatic HTTPS and Dynamic DNS
----------------------	-------	--------	---	-----------------	---

Une fois installé nous allons mettre le port TCP sur 8080 sur lequel le pare-feu écoutera sur le web et utiliser le certificat magneticlab pour la suite sur caddy.



Web GUI

Protocol ☐ HTTP ☒ HTTPS

SSL Certificate

SSL Ciphers

HTTP Strict Transport Security ☐ Enable HTTP Strict Transport Security

TCP port

HTTP Redirect ☒ Disable web GUI redirect rule

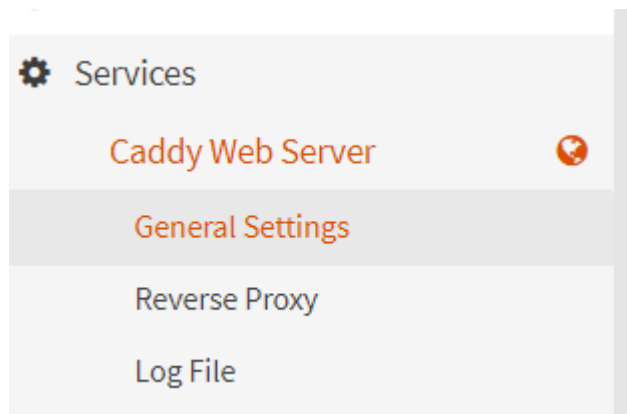
Login Messages ☐ Disable logging of web GUI successful logins

Session Timeout

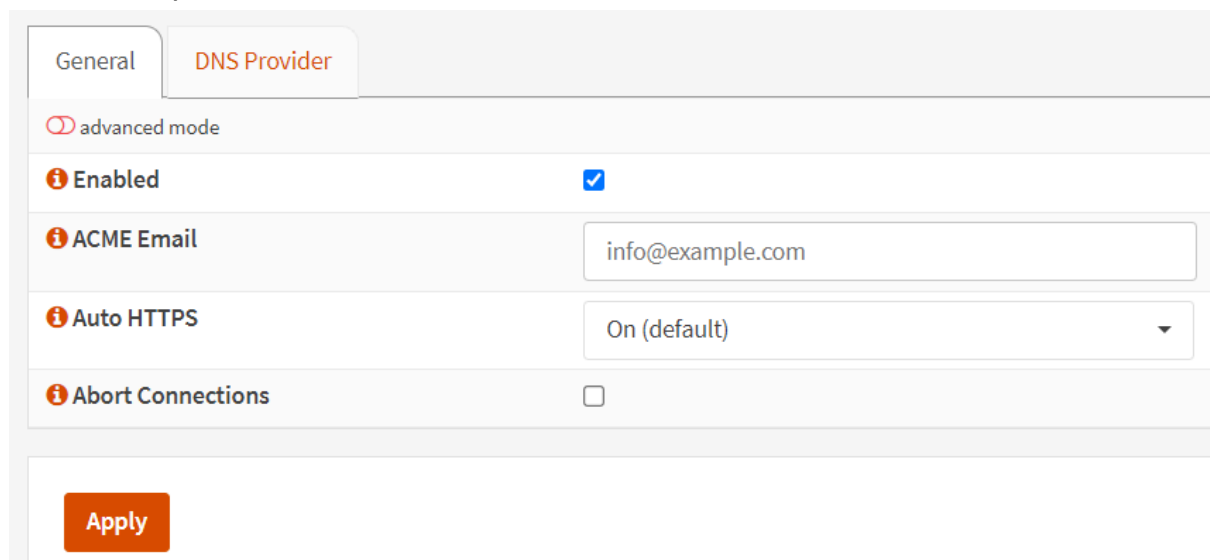
DNS Rebind Check ☐ Disable DNS Rebinding Checks

Alternate Hostnames
Alternate Hostnames for DNS Rebinding and HTTP_REFERER Checks

Nous pouvons désormais mettre en place le reverse proxy



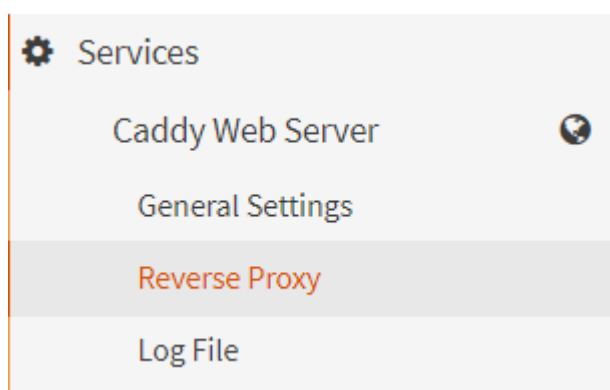
Ici il faut cliquer sur enabled

A screenshot of the 'DNS Provider' settings page. The page has two tabs: 'General' and 'DNS Provider' (active). Below the tabs is a section for 'advanced mode' with a toggle switch. The main settings are: 'Enabled' (checked), 'ACME Email' (info@example.com), 'Auto HTTPS' (On (default)), and 'Abort Connections' (unchecked). An 'Apply' button is at the bottom left.

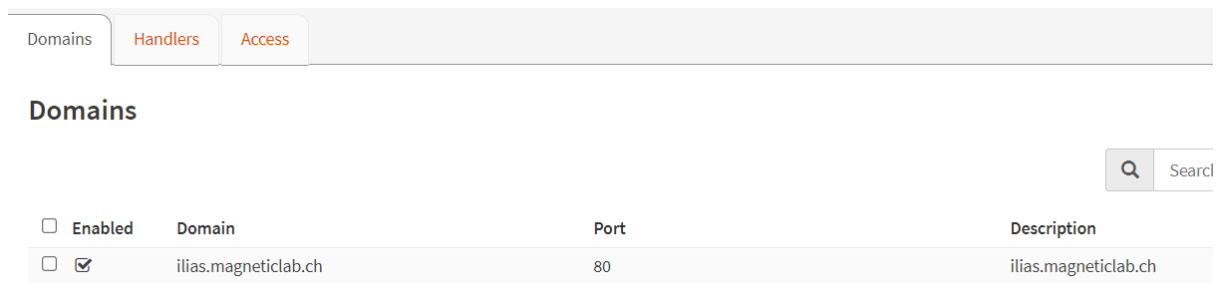
DNS Provider	
advanced mode	
Enabled	<input checked="" type="checkbox"/>
ACME Email	info@example.com
Auto HTTPS	On (default)
Abort Connections	<input type="checkbox"/>

Apply

—>



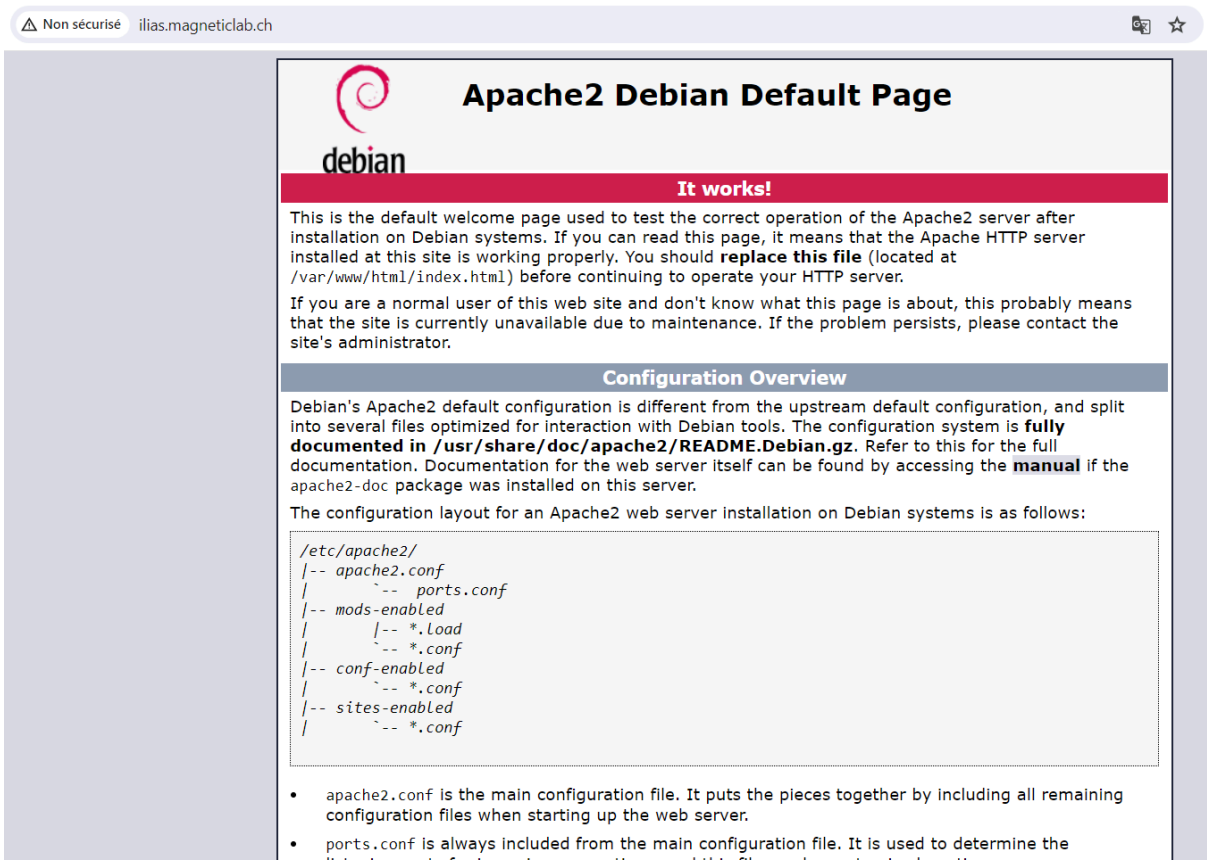
Il faut mettre le domaine qui nous redirigera sur apache2 par la suite qui est `ilias.magneticlab.ch` et qui écoute sur le port 80.



Et pour finir dans le gestionnaire de domaine il faut préciser sur quelle adresse le nom de domaine `ilias.magneticlab.ch` doit être redirigé et dans notre cas c'est l'adresse d'apache 2 qui est `192.168.1.100`.



Maintenant si on met `ilias.magneticlab.ch` en `http` qui est le port 80 sur un navigateur web quelconque on est bien redirigé sur `apache2`.



On peut remarquer que cette redirection n'est pas sécurisée c'est sécurisée uniquement sur `opnsense.magneticlab.ch` le pare feu `opnsense`.

Type	Answer	Server	Query time
A	opnsense.magneticlab.ch. 3600 IN A 84.75.242.109	62.2.17.60	32 msec

<input type="checkbox"/>		IPv4	OPT1 net	*	*	53 (DNS)	*	*	Bloquer l'accès à tout les autres serveurs DNS				
<input type="checkbox"/>		IPv4 *	OPT1 net	*	! MonServeur	*	*	*	Autoriser l'accès à internet et bloquer l'accès à tous les réseaux locaux				

3. Test d'un certificat valide sur plusieurs noms de domaine







Pour cela nous allons générer un nouveau nom de domaine gratuit sur un site internet qu'on a nommé xefi-ne.ch. Ce nouveau domaine sera remplacé par le certificat magneticlab mais le nom du site qui nous redigirera sur apache2 sera toujours ilias.magneticlab.ch grâce à une fonctionnalité proposée par caddy qui est le https automatique qui s'appelle let's encrypt et à chaque fois qu'on va ajouter un serveur web sur caddy let's encrypt nous proposera un site sécurisée avec un certificat valide.

The screenshot shows the 'DNS Provider' tab in the Caddy web server configuration. The 'General' tab is also visible. The 'advanced mode' toggle is turned on. The 'Enabled' checkbox is checked. The 'ACME Email' field is set to 'fred@magneticlab.ch'. The 'Auto HTTPS' dropdown is set to 'On (default)'. The description for 'Auto HTTPS' states: 'Select the auto HTTPS option. "On" (default) creates automatic certificates using Let's Encrypt or ZeroSSL without needing any configuration.'

Cette fonctionnalité nous crée un certificat automatique avec let's encrypt en https en et cela va nous permettre de sécuriser notre serveur web apache 2 grâce au second nom de domaine créé précédemment. Sa permet donc de shooter le ports 80

Il faut ajouter le nouveau nom de domaine dans reverse proxy

The screenshot shows the 'Domains' tab in the Caddy web server configuration. The 'Domains' section is active. The table below lists the domains configured for the reverse proxy.

Enabled	Domain	Port	Description	Commands
<input checked="" type="checkbox"/>	ilias.magneticlab.ch		ilias.magneticlab.ch	  
<input checked="" type="checkbox"/>	*.xefi-ne.ch		xefi-ne.ch	  

Dans le handlers il faut faire de même ajouter le nouveau nom de domaine mais également sur quel serveur il doit pointer donc apache2 qui est 192.168.1.100

Domains

Handlers

Access

Handlers

Q

Search

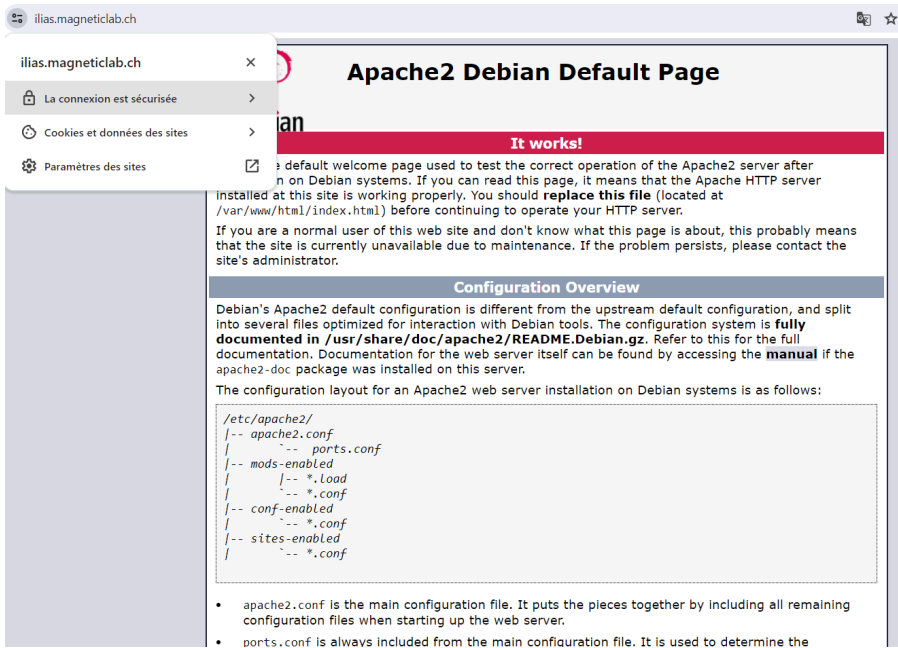
↺

7

▼

<div><input type="checkbox"/> Enabled</div>	Domain	Submain	Handle Path	Backend Domain	Backend Port	Description	Comm
<div><input type="checkbox"/> <input checked="" type="checkbox"/></div>	ilias.magneticlab.ch	None		192.168.1.100			<div><div></div><div></div></div>
<div><input type="checkbox"/> <input checked="" type="checkbox"/></div>	xefi-ne.ch	None		192.168.1.100			<div><div></div><div></div></div>

La connexion est bien sécurisée en https



Émis pour

Nom commun (CN)	ilias.magneticlab.ch
Organisation (O)	<Ne fait pas partie du certificat>
Unité d'organisation (OU)	<Ne fait pas partie du certificat>

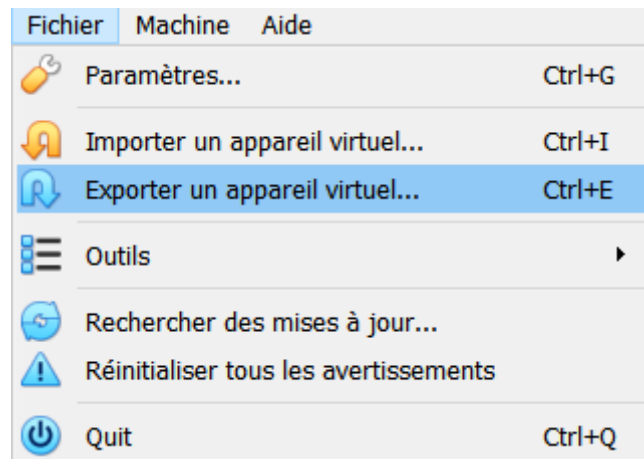
Émis par

Nom commun (CN)	R3
Organisation (O)	Let's Encrypt
Unité d'organisation (OU)	<Ne fait pas partie du certificat>

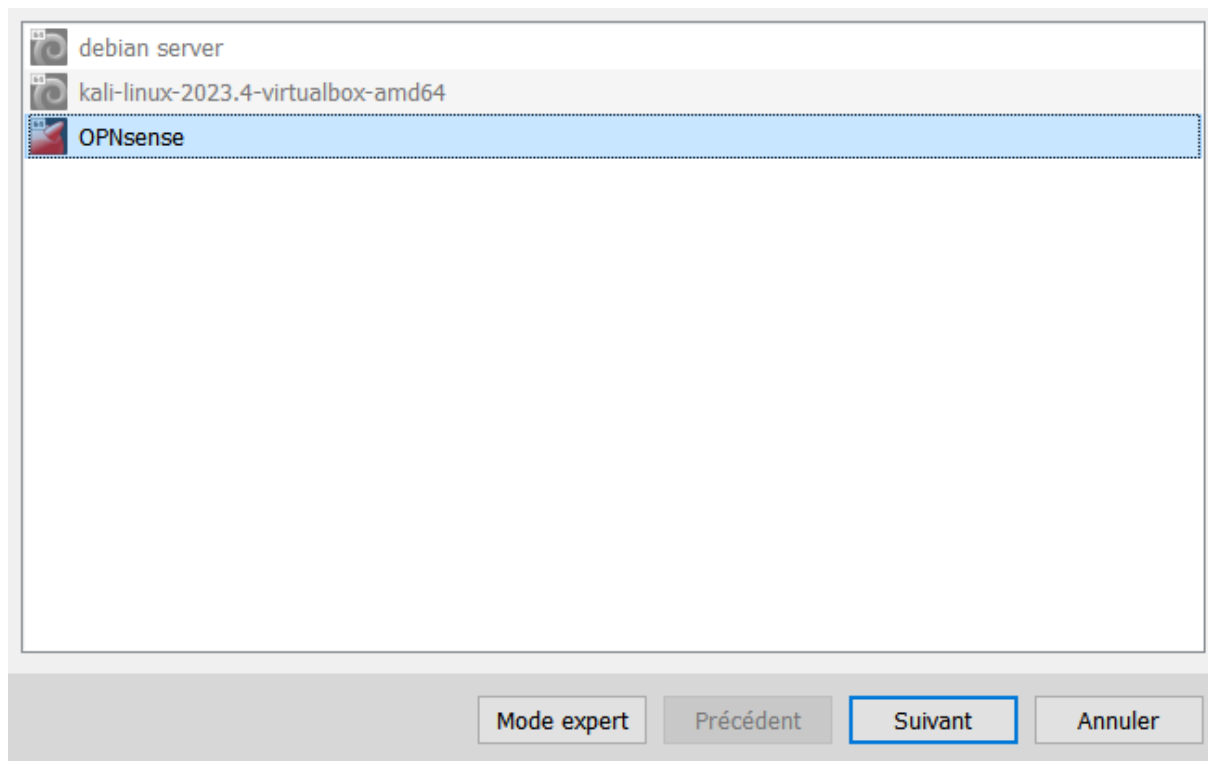
4.Migration OPNSense virtualbox vers VMWare

Le reverse proxy est fonctionnel et il est maintenant temps de migrer la configuration de l'opnsense du virtualbox vers nos serveurs sur vmware.

En haut à gauche



Sélectionner la vm



Sélectionnez ou on veut que la machine soit exporter pour ma part cela sera sur une clefs USB et en format OVF et non OVA pour des problème de compatibilité lors de l'importation, Suivant et finish

Format settings

Choisissez un nom de fichier pour exporter le dispositif virtuel.

Le **format Open Virtualization** ne prend en charge que les extensions **ovf** ou **ova**.
Si vous utilisez l'extension **ovf**, plusieurs fichiers seront écrits séparément.
Si vous utilisez l'extension **ova**, tous les fichiers seront combinés en un seul fichier au format Open Virtualisation Archive.

Le **format Oracle Cloud Infrastructure** supporte l'exportation vers des serveurs cloud distants seulement.
Le disque virtuel principal de chaque machine sélectionnée sera téléversé sur le serveur distant.

Format : Open Virtualization Format 1.0

Please choose a filename to export the virtual appliance to. Besides that you can specify a certain amount of options which affects the size and content of resulting archive.

Fichier : E:\OPNsense.ovf

Politique d'adresse MAC : Supprimer toutes les adresses MAC de l'interface réseau

Aditionnellement : ☒ Écrire un fichier manifeste
☐ Inclure les fichiers d'image ISO

Précédent Suivant Annuler

Ensuite on clique sur créer enregistrer une machine virtuelle et déployer une machine virtuelle à partir d'un fichier OVF

Nouvelle machine virtuelle

1 Sélectionner un type de création

2 Sélectionner des fichiers OVF et VMDK

3 Sélectionner un stockage

4 Contrats de licence

5 Options de déploiement

6 Paramètres supplémentaires

7 Prêt à terminer

Sélectionner un type de création

Comment voulez-vous créer une machine virtuelle ?

Créer une machine virtuelle

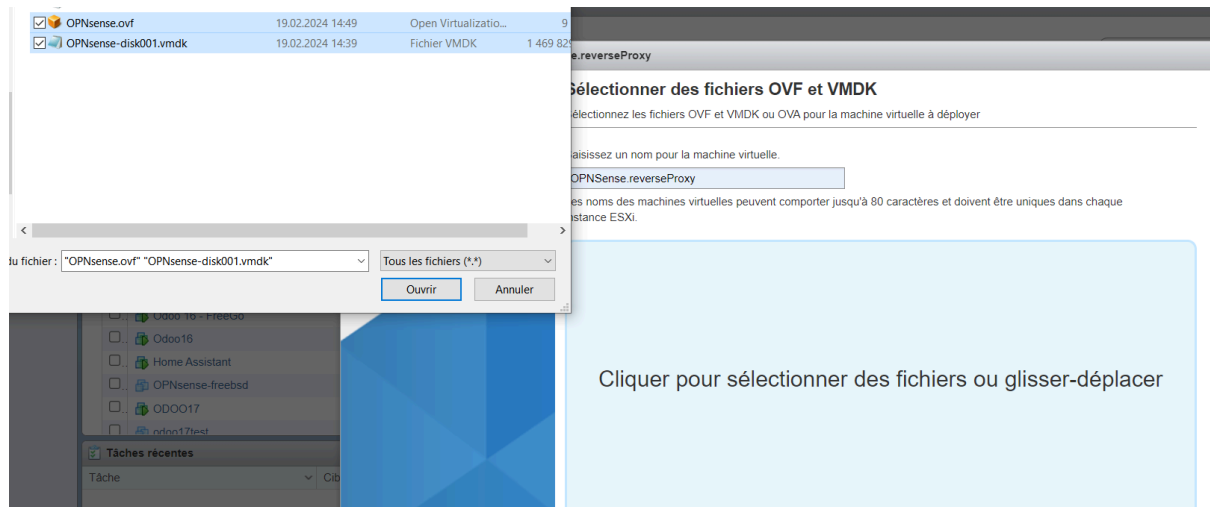
Déployer une machine virtuelle à partir d'un fichier OVF o...

Enregistrer une machine virtuelle existante

Cette option vous guide tout au long du processus de création d'une machine virtuelle à partir de fichiers OVF et VMDK.

Précédent Suivant Terminer Annuler

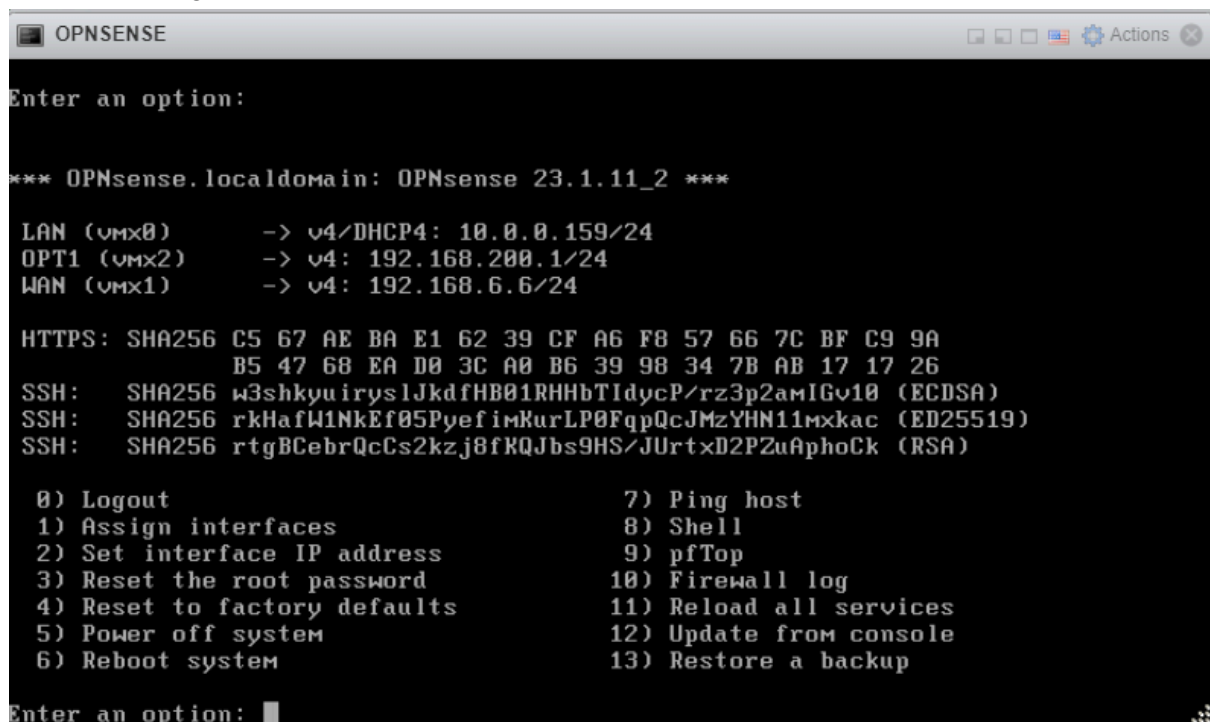
Pour finir on vient récupérer le fichier ovf avec son image disque et on fait suivant jusqu'à que l'importation se fasse






La machine à bien été importer

	OPNsense.reverseProxy		Normale	6,78 Go	FreeBSD (64 bits)	Inconnu	123 MHz	1,96 Go
--	-----------------------	--	---------	---------	-------------------	---------	---------	---------

Nouvelle config vmware



▶  Adaptateur réseau 1	VM Network
▶  Adaptateur réseau 2	UPC WAN
▶  Adaptateur réseau 3	OPNsense LAN SECURE

le 192.168.6.70 qui correspondait au wan n'arrivait pas à communiquer avec le routeur ce qui rendait l'accès au pare-feu depuis le web avec le nom de domaine opnsense.magneticlab.ch impossible, nous avons également changer le port d'écoute sur 8443.



5. Ajout serveur web clients sur OPNSense

Pour finir ce projet nous allons ajouter 2 serveurs web odoo que certains de nos clients utilisent grâce à caddy qui va nous rediriger dessus avec de nouvelles adresses qui ont été attribué sur les serveurs ubuntu de VMWare, il s'agit d'odoo14e et odoo15 en .magneticlab.ch qui rappelons le, représente notre nom de domaine.

Voici la configuration finale du pare feu

```
LAN (vmx0)      -> v4/DHCP4: 10.0.0.159/24
OPT1 (vmx2)     -> v4: 192.168.200.1/24
WAN (vmx1)      -> v4: 192.168.6.6/24
```

Pour faire ceci voici toutes les étapes:

-Ouvrir le serveur odoo14e sur vmware

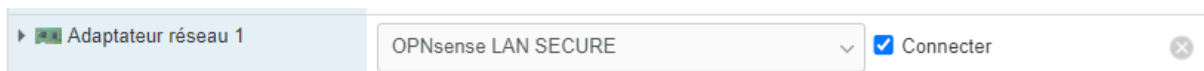


-Supprimer les cartes réseau du PFSense et ajouter celle de l'OPNSense qui correspond à la DMZ et par la suite sur les serveurs on aura une ip attribué sur ubuntu en 192.168.200. quelques choses qui nous servira à rediriger les sites internet sur caddy comme expliqué précédemment



```
m1ab@odoo14e:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
4: ens224: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000
    link/ether 00:0c:29:0c:ba:8e brd ff:ff:ff:ff:ff:ff
    inet 192.168.200.101/24 brd 192.168.200.255 scope global dynamic ens224
        valid_lft 6404sec preferred_lft 6404sec
```



-Même chose sur odoo15



```
m1ab@odoo15:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
2: ens160: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000
    link/ether 00:50:56:a6:a2:52 brd ff:ff:ff:ff:ff:ff
    inet 192.168.200.102/24 brd 192.168.200.255 scope global dynamic ens160
        valid_lft 4141sec preferred_lft 4141sec
```

-Ajout des 2 sites sur caddy

Services, Reverse proxy, Domains

<input type="checkbox"/>	<input checked="" type="checkbox"/>	odoo14e.magneticlab.ch		odoo14e.magneticlab.ch	  
<input type="checkbox"/>	<input checked="" type="checkbox"/>	odoo15.magneticlab.ch		odoo15.magneticlab.ch	  

Services, Reverse proxy, Handlers

<input type="checkbox"/>	<input checked="" type="checkbox"/>	odoo14e.magneticlab.ch	none	192.168.200.101	  
<input type="checkbox"/>	<input checked="" type="checkbox"/>	odoo15.magneticlab.ch	none	192.168.200.102	  

Il faut aussi changer la zone DNS de notre domaine magneticlab sur infomaniak en mettant l'ip externe du wan de l'OPNSense en 84.175.242.109 afin d'être bien rediriger sur sites, si on met l'ip externe du PFSense on aura un message d'erreur parce qu'on a supprimés les cartes réseau du PFSense sur les serveurs ubuntu et donc la redirection ne pourra pas se faire correctement.

Quelques choses comme ça

Not Found

The requested URL `/proprietary-software.html` was not found on this server.

Apache/2.4.10 (Debian) Server at localhost Port 80

Résultat:

Odoo14e sécurisée avec un certificat valide

odoo14e.magneticlab.ch/web/database/selector

odoo

anglais

français

Google Translate

CDF
CDF2
CDF2023
ISP-2022-12-01
ISP-270122
ISP13102022
MLAB2
mlab-sh-aout
mlab-sh-sept
mlab150822

Manage databases

Odoo15 sécurisée avec un certificat valide

odoo15.magneticlab.ch/web/database/selector



ALLOA-COPY-03-08
COMMUNITY
FMSTORES
HSOLUTIONS310323
HSOLUTIONS140723
HV
MAIN-27-10
MLAB-15-PROD
MLAB-30-01-2023
MLAB20.02.2023
MPR-DEMO
ODOO-EV
POS-DEMO
TEST-ODOO-SCHOOL
TEST-XEFI-MODULE
ott

.. 1 1 1

