

Mettre en place la sécurité d'une petite entreprise avec IPFire sur GNS3



Réalisé par : Karim maali



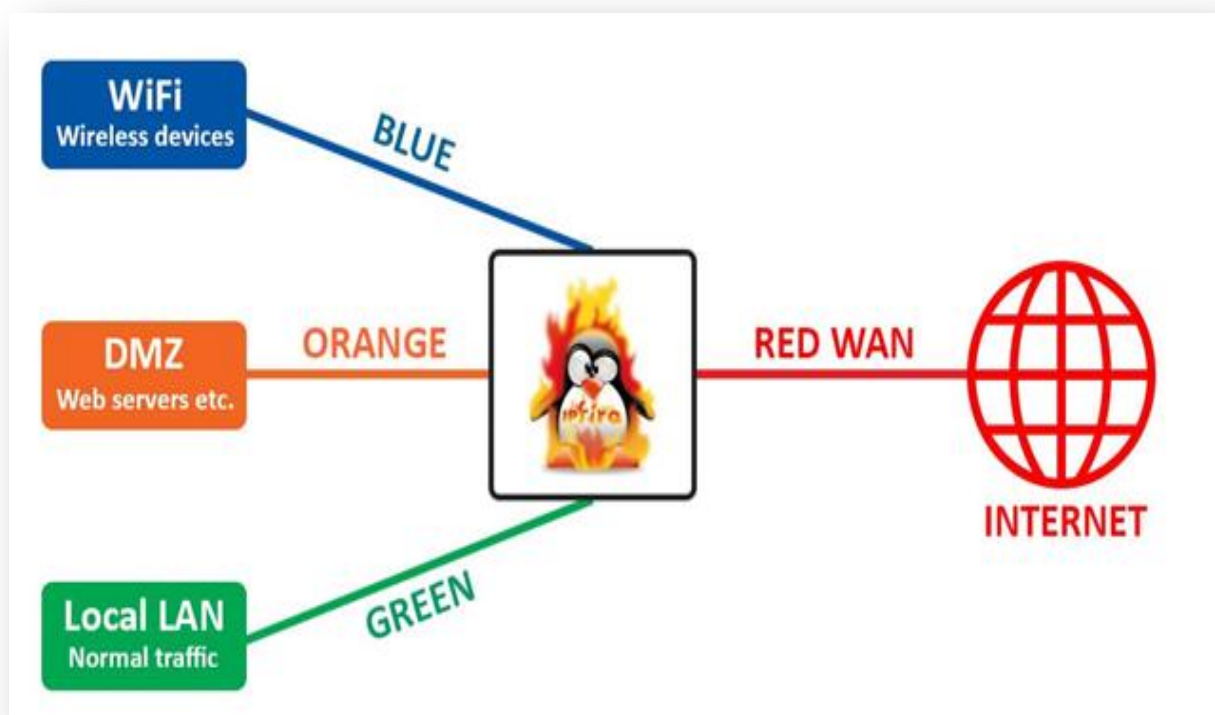
Introduction au pare-feu IPFire :

Le pare-feu IPFire est une solution open source puissante et flexible qui permet de protéger les réseaux contre les cyberattaques tout en offrant un contrôle avancé sur le trafic réseau. Conçu pour être facile à configurer et à utiliser, IPFire est une option idéale pour les petites et moyennes entreprises, ainsi que pour les utilisateurs domestiques soucieux de leur sécurité en ligne.



Principales caractéristiques d'IPFire

1. **Protection avancée** : IPFire utilise un moteur de pare-feu basé sur Netfilter (intégré au noyau Linux) pour filtrer le trafic réseau et appliquer des règles de sécurité personnalisées.
2. **Gestion simplifiée** : L'interface web intuitive permet de configurer rapidement le pare-feu, les règles de NAT, les zones réseau et bien plus encore.
3. **Support multi-zones** : IPFire divise le réseau en différentes zones de sécurité (Écarlate, Vert, Bleu et Orange) pour mieux contrôler les flux de données.
 - **Vert** : Réseau interne sécurisé.
 - **Rouge** : Connexion à Internet (zone non sécurisée).
 - **Bleu** : Réseau Wi-Fi.
 - **Orange** : DMZ (zone pour les serveurs accessibles depuis l'extérieur).



4. **Mise à jour régulière** : Les développeurs d'IPFire publient fréquemment des correctifs et des mises à jour de sécurité pour protéger contre les nouvelles menaces.
5. **Modules supplémentaires** : IPFire offre des fonctionnalités étendues via des add-ons, comme un serveur proxy, un système de détection/prévention des intrusions (IDS/IPS), et des outils pour la surveillance du trafic.



Avantages d'IPFire

- **Gratuit et open source** : Aucun coût de licence.
- **Flexibilité** : Convient à divers scénarios, que ce soit pour un domicile ou une entreprise.
- **Communauté active** : Une grande communauté d'utilisateurs et de développeurs qui contribuent à l'amélioration continue du projet.
- **Support matériel large** : Compatible avec une variété de matériels, y compris les appareils x86 et ARM.

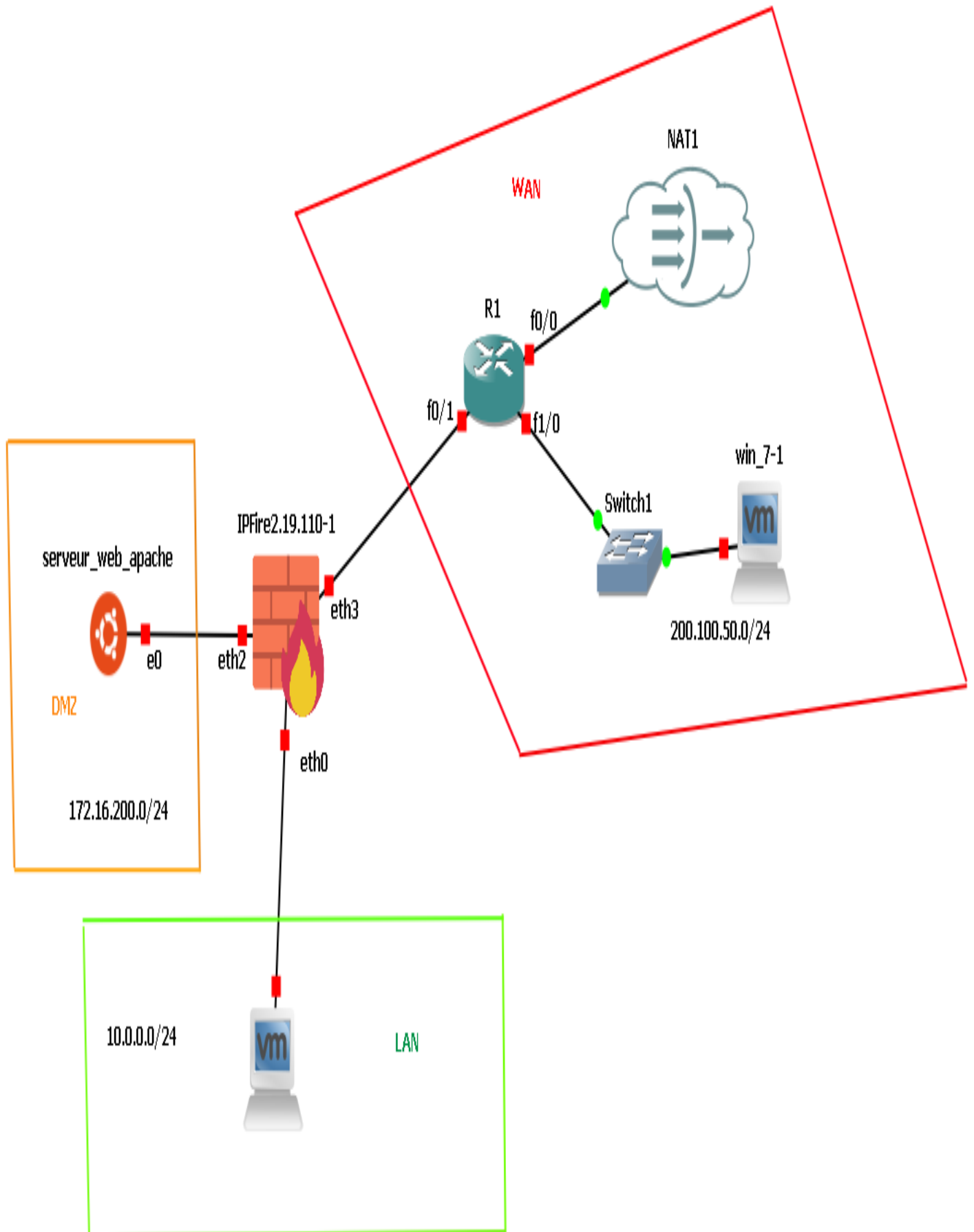


Cas d'utilisation d'IPFire

1. **Protection du réseau domestique** : Protéger les appareils connectés à Internet contre les cyberattaques.
2. **Sécurisation des petites entreprises** : Contrôle des accès Internet, surveillance du trafic et configuration des VPN pour les employés distants.
3. **Serveurs DMZ** : Hébergez des serveurs accessibles depuis Internet tout en isolant votre réseau interne.



Schéma du Projet :



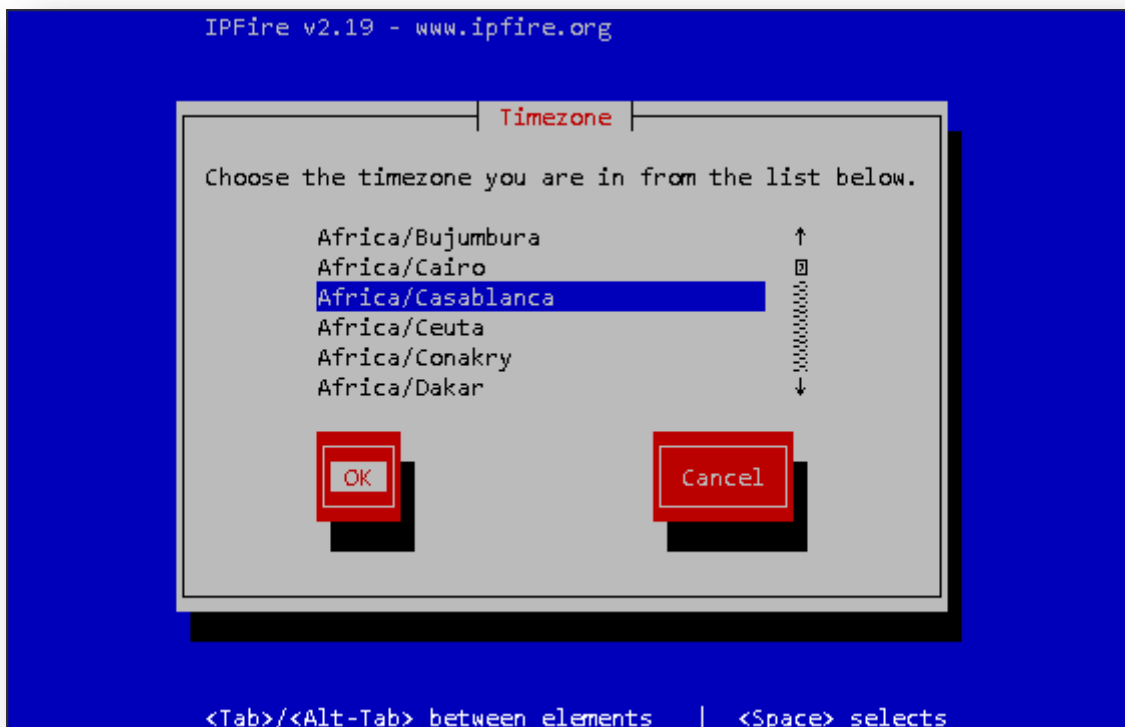


Installer IPFire: Étapes et Configuration

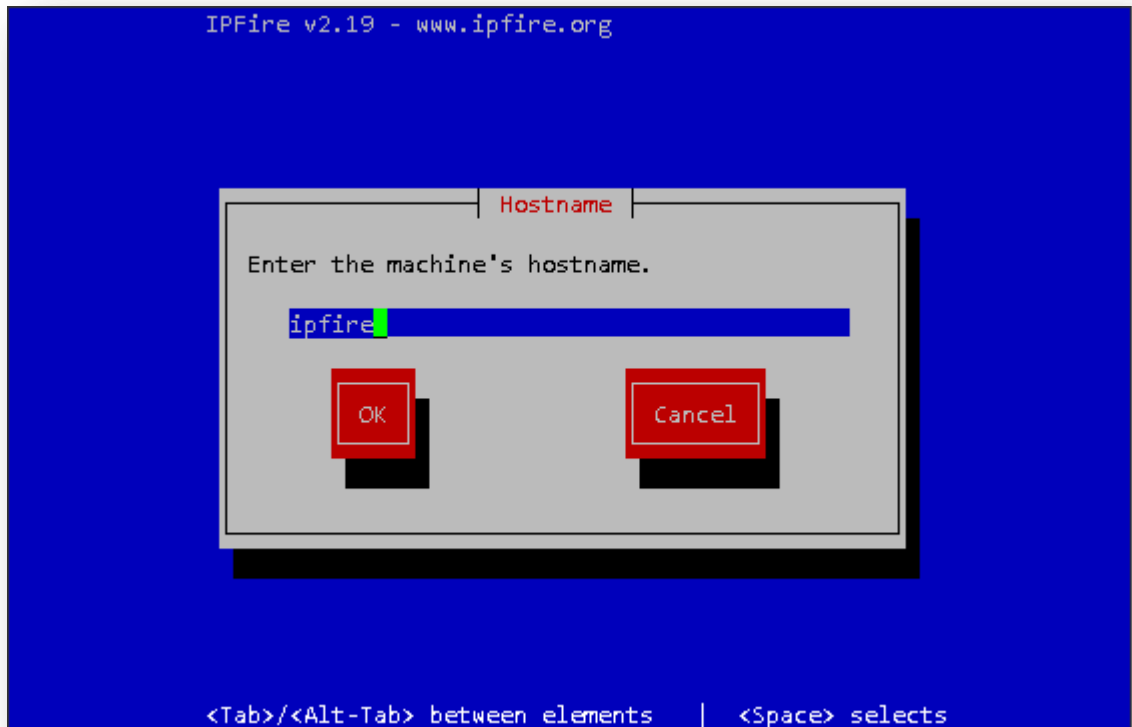
Sélectionnez le type de clavier que vous utilisez dans la liste ci-dessous. Et appuyez sur OK.



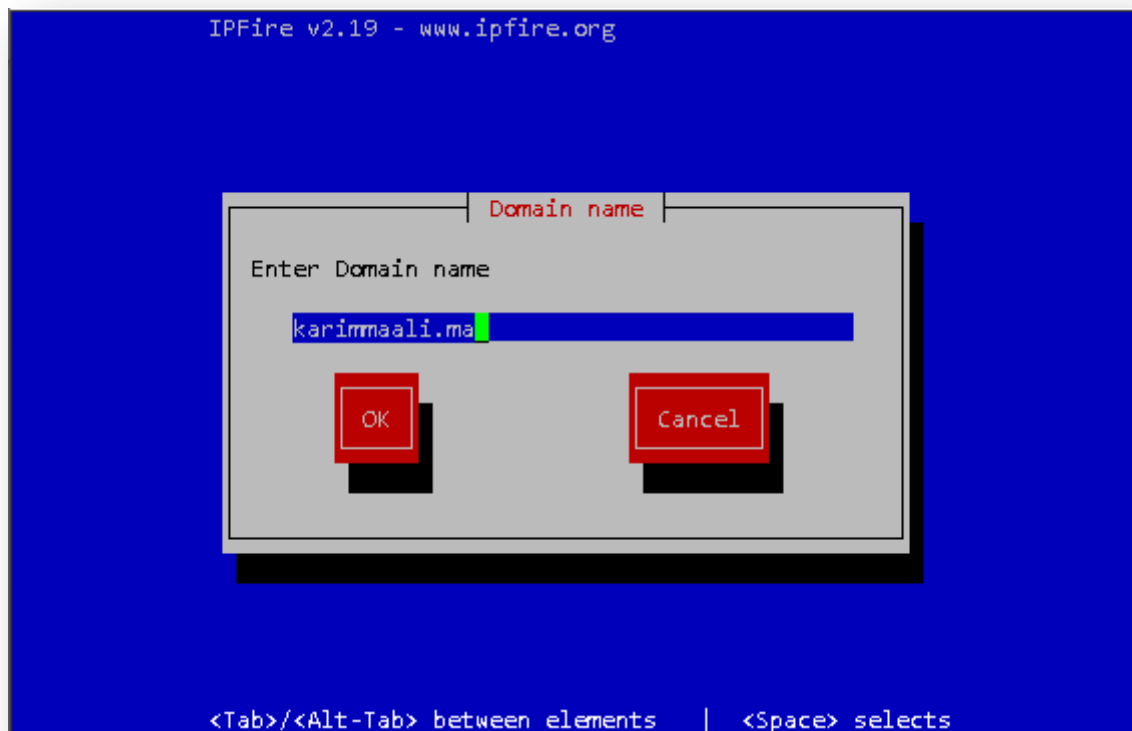
Choisissez le fuseau horaire dans lequel vous vous trouvez dans la liste ci-dessous.



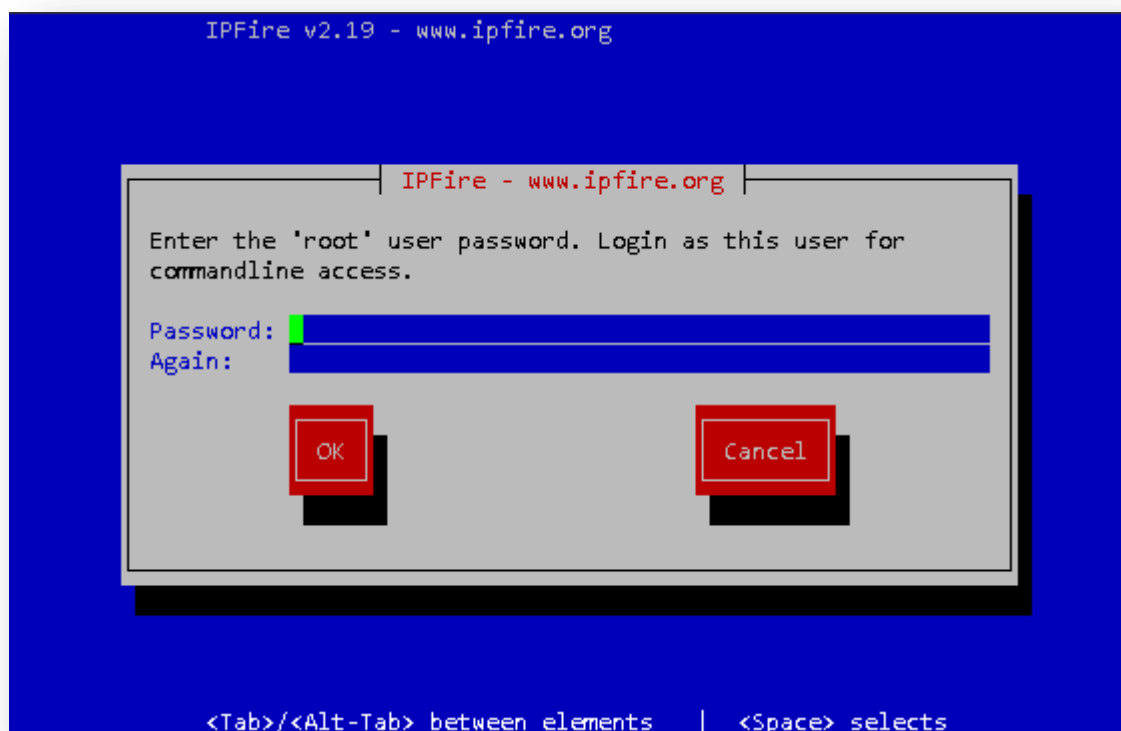
Entrez le nom d'hôte de la machine.



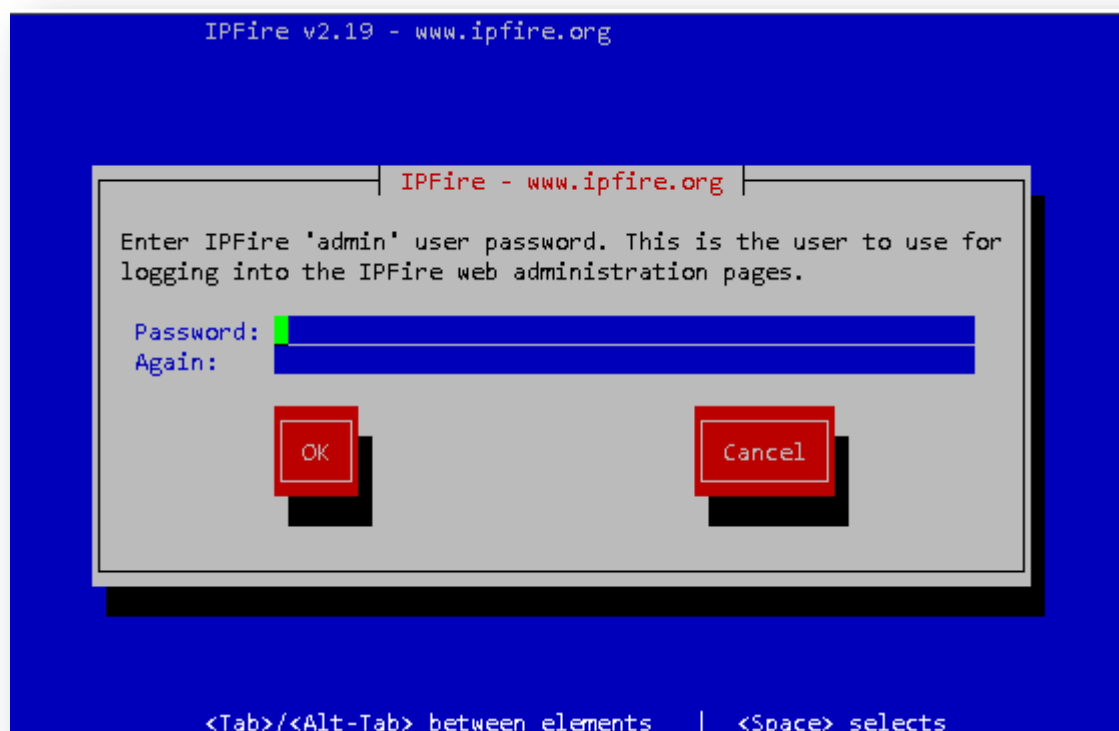
Entrez le nom de domaine



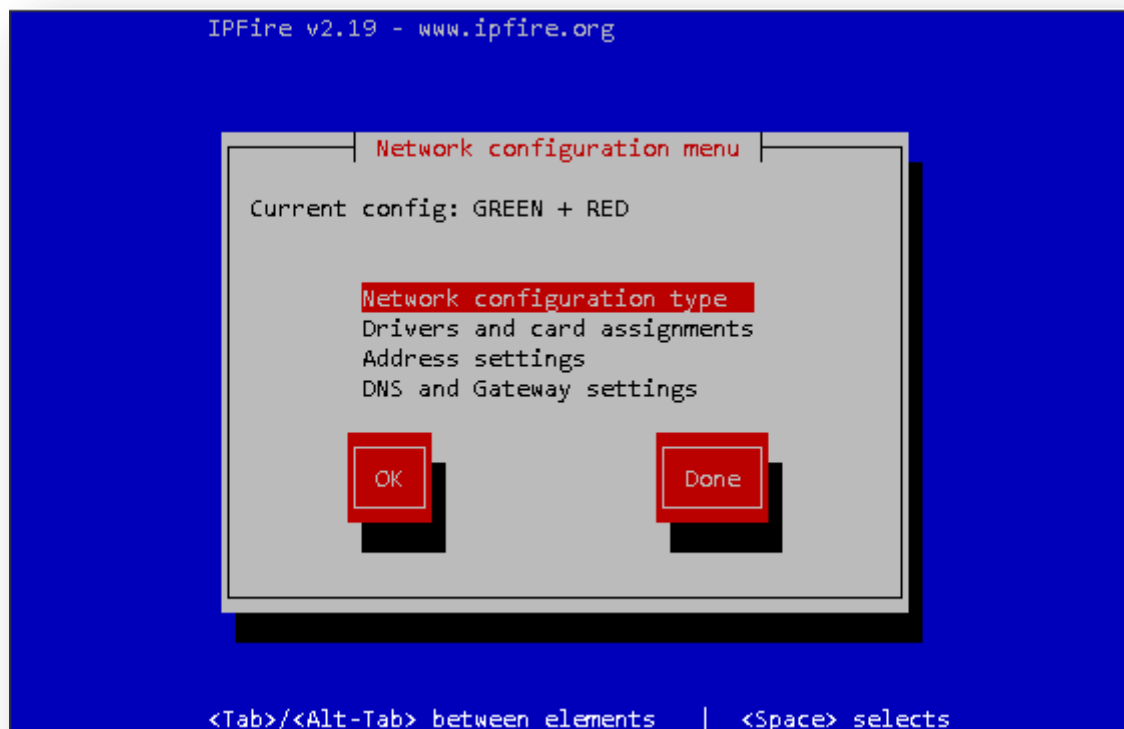
Saisissez le mot de passe de l'utilisateur « root ». Connectez-vous sous cet utilisateur pour accéder à la ligne de commande.



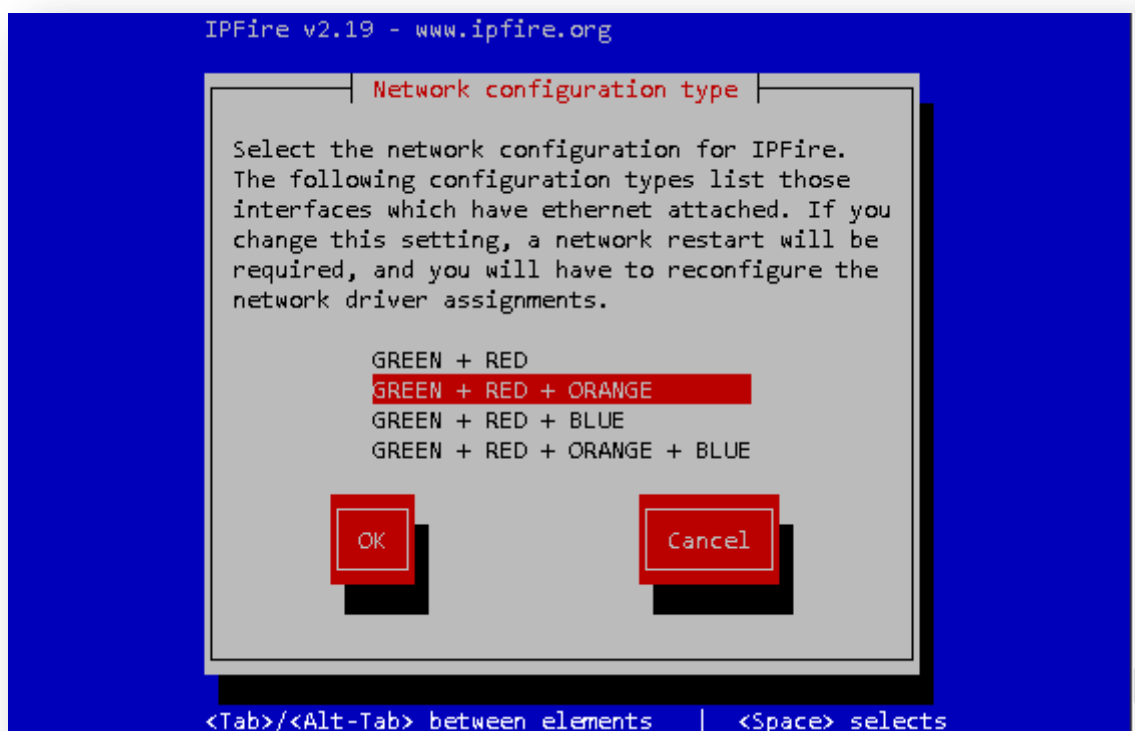
Saisissez le mot de passe de l'utilisateur « admin » d'IPFire. Il s'agit de l'utilisateur à utiliser pour se connecter aux pages d'administration Web d'IPFire.



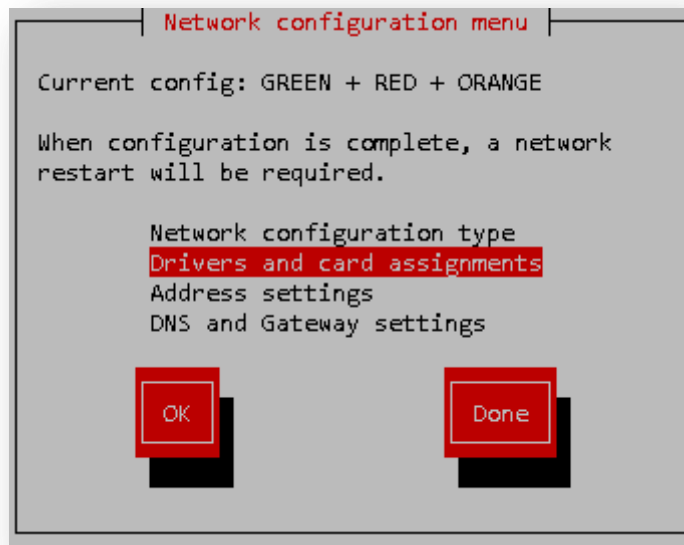
Type de configuration réseau



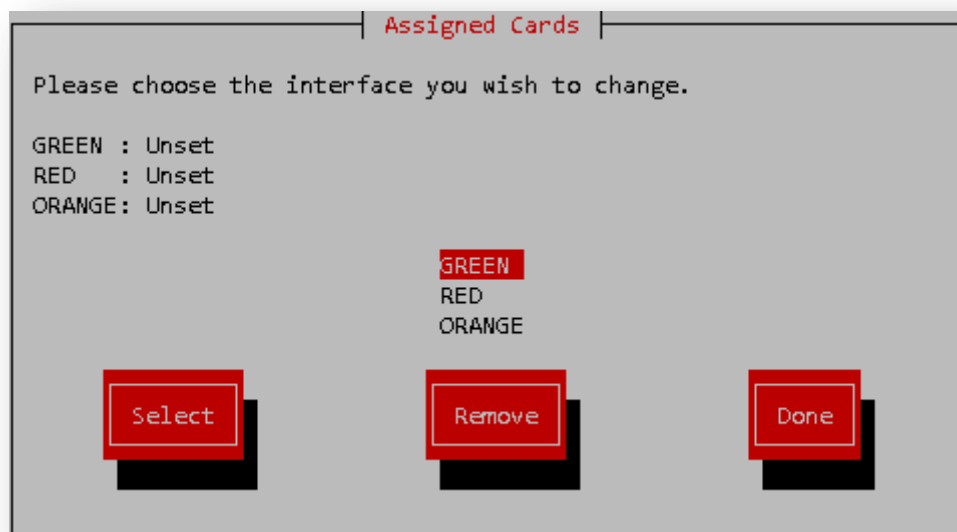
Spécifiez la configuration réseau pour IPFire. Choix selon vos besoins
Je choisirai VERT + ROUGE + ORANGE car je travaillerai avec le réseau DMZ



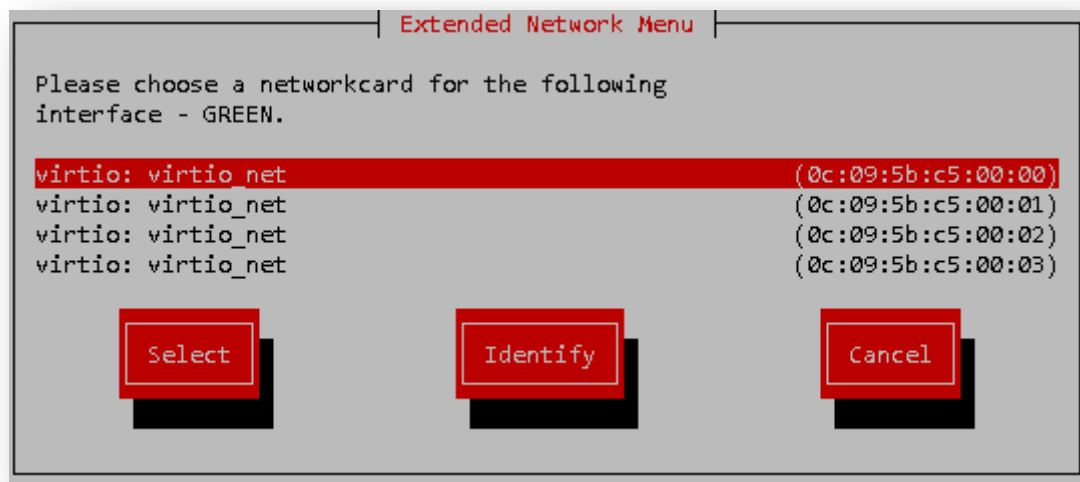
Vous devez maintenant sélectionner chaque couleur avec sa propre carte réseau.



Je choisirai la couleur verte pour le réseau interne de la carte, son propre réseau



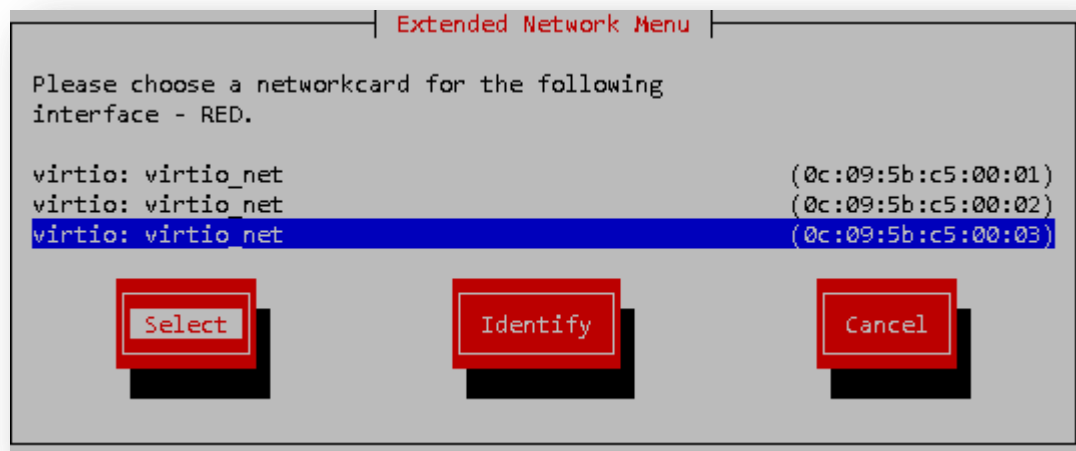
Veillez choisir une carte réseau pour l'interface suivante - **VERT**.



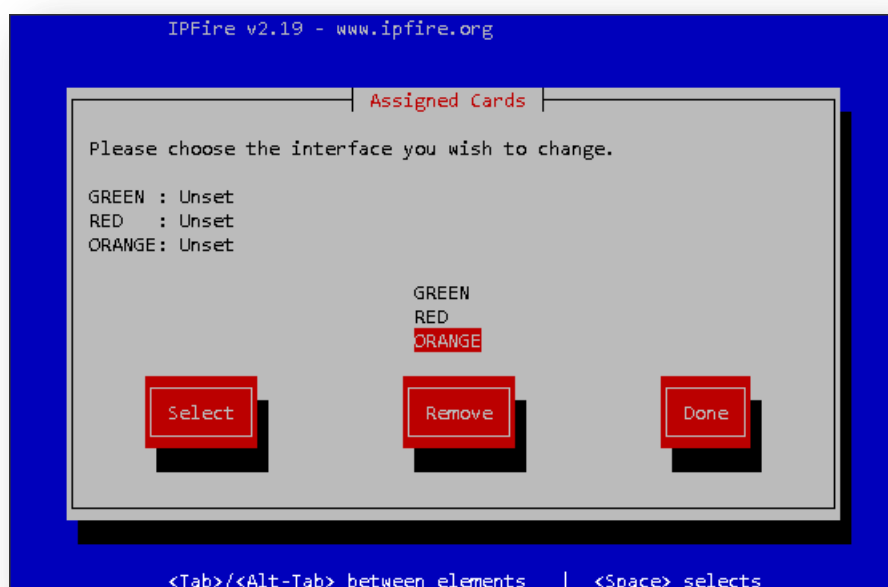
Je choisis la couleur **rouge** pour le réseau interne de la carte, son propre réseau.



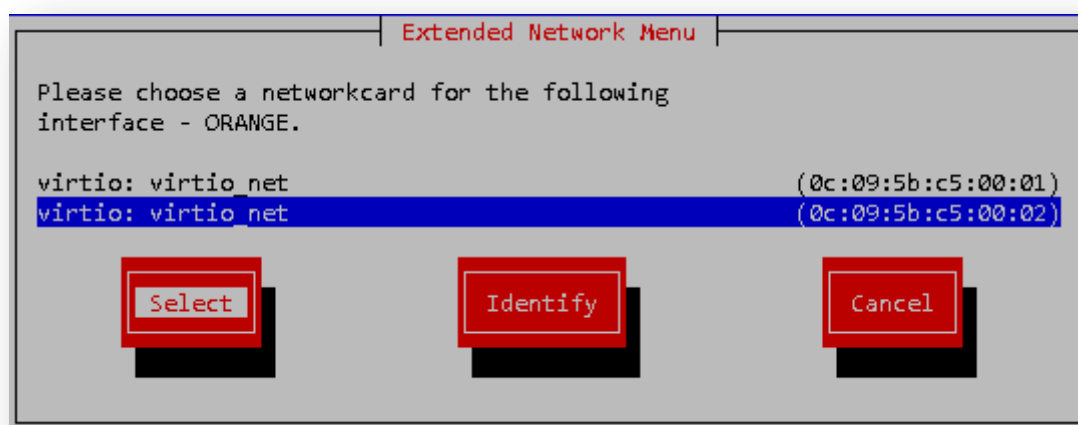
Veuillez choisir une carte réseau pour l'interface suivante -
rouge



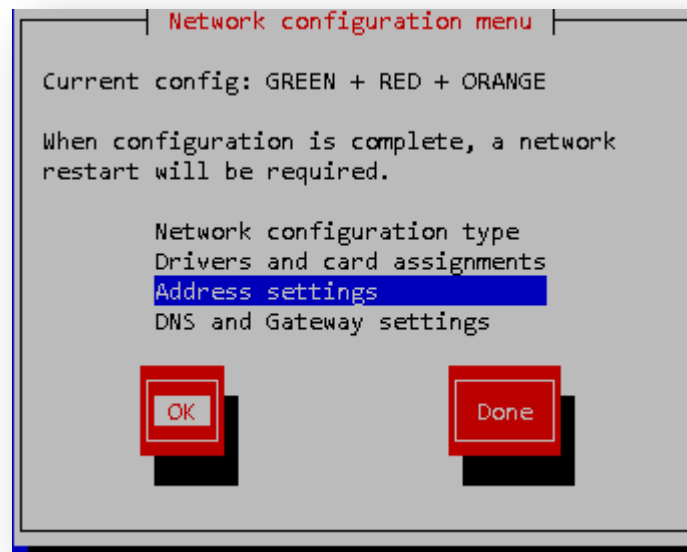
J'ai choisi l'orange pour réseau DMZ



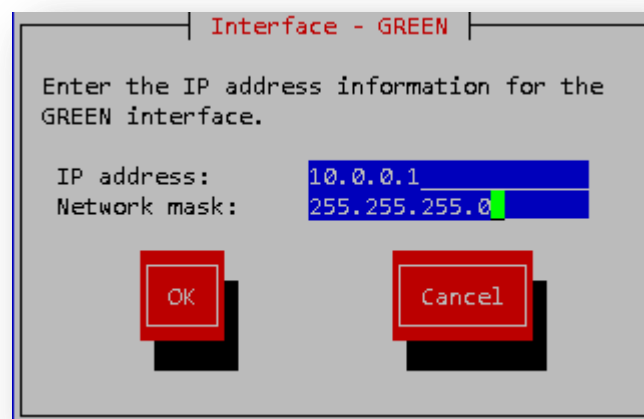
Veuillez sélectionner la carte réseau pour l'interface suivante -
Orange



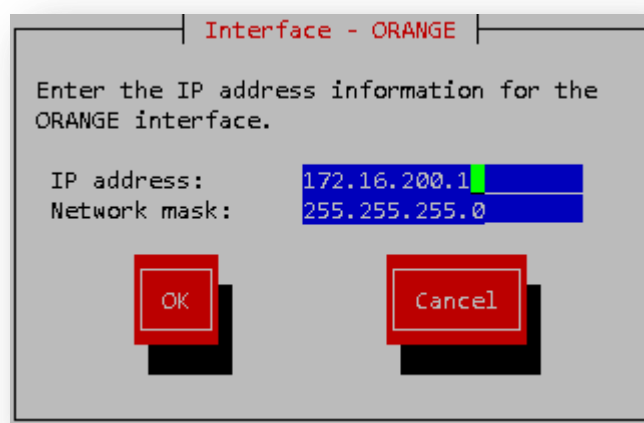
la configuration du adressage pour les interface



la configuration sur l'interface green (LAN)



la configuration sur l'interface orange (DMZ)



la configuration sur l'interface Rouge (WAN)

The screenshot shows a window titled "Interface - RED". Inside, it says "Enter the IP address information for the RED interface." There are three radio button options: "Static" (which is selected with an asterisk), "DHCP", and "PPP DIALUP (PPPoE, modem, ATM ...)". Below these, there are fields for "DHCP Hostname:" with the value "ipfire" and "Force DHCP MTU:". Further down, there are fields for "IP address:" with the value "84.0.0.1" and "Network mask:" with the value "255.255.255.254". At the bottom, there are two buttons: "OK" and "Cancel".

la configuration sur configure DNS et passerelle

The screenshot shows a window titled "Network configuration menu". It displays "Current config: GREEN + RED + ORANGE" and a warning: "When configuration is complete, a network restart will be required." Below this, there is a list of configuration steps: "Network configuration type", "Drivers and card assignments", "Address settings", and "DNS and Gateway settings" (which is highlighted with a blue background). At the bottom, there are two buttons: "OK" and "Done".

Saisissez les informations DNS et de passerelle. Ces paramètres sont utilisés uniquement avec une adresse IP statique (et DHCP si DNS est défini) sur l'interface RED.

L'adresse 84.0.0.2 de la passerelle se trouve sur le routeur connecté à l'interface rouge.

DNS and Gateway settings

Enter the DNS and gateway information. These settings are used only with Static IP (and DHCP if DNS set) on the RED interface.

Primary DNS: 8.8.8.8
Secondary DNS: 8.8.4.4
Default gateway: 84.0.0.2

OK Cancel

Activer le service DHCP pour l'interface verte

DHCP server configuration

Configure the DHCP server by entering the settings information.

☒ Enabled

Start address: 10.0.0.2
End address: 10.0.0.50
Primary DNS: 10.0.0.1
Secondary DNS: 8.8.8.8
Default lease (mins): 60
Max lease (mins): 120
Domain name suffix: karimaali.ma

OK Cancel

Le paramétrage est désormais terminé. Appuyez sur Entrée une dernière fois



IPFire va redémarrer pour vérifier que les configurations précédentes sont bien correctes. Patientez jusqu'à voir la demande de login en bas de l'écran.

Par défaut, les paramètres de connexion IPFire sont :

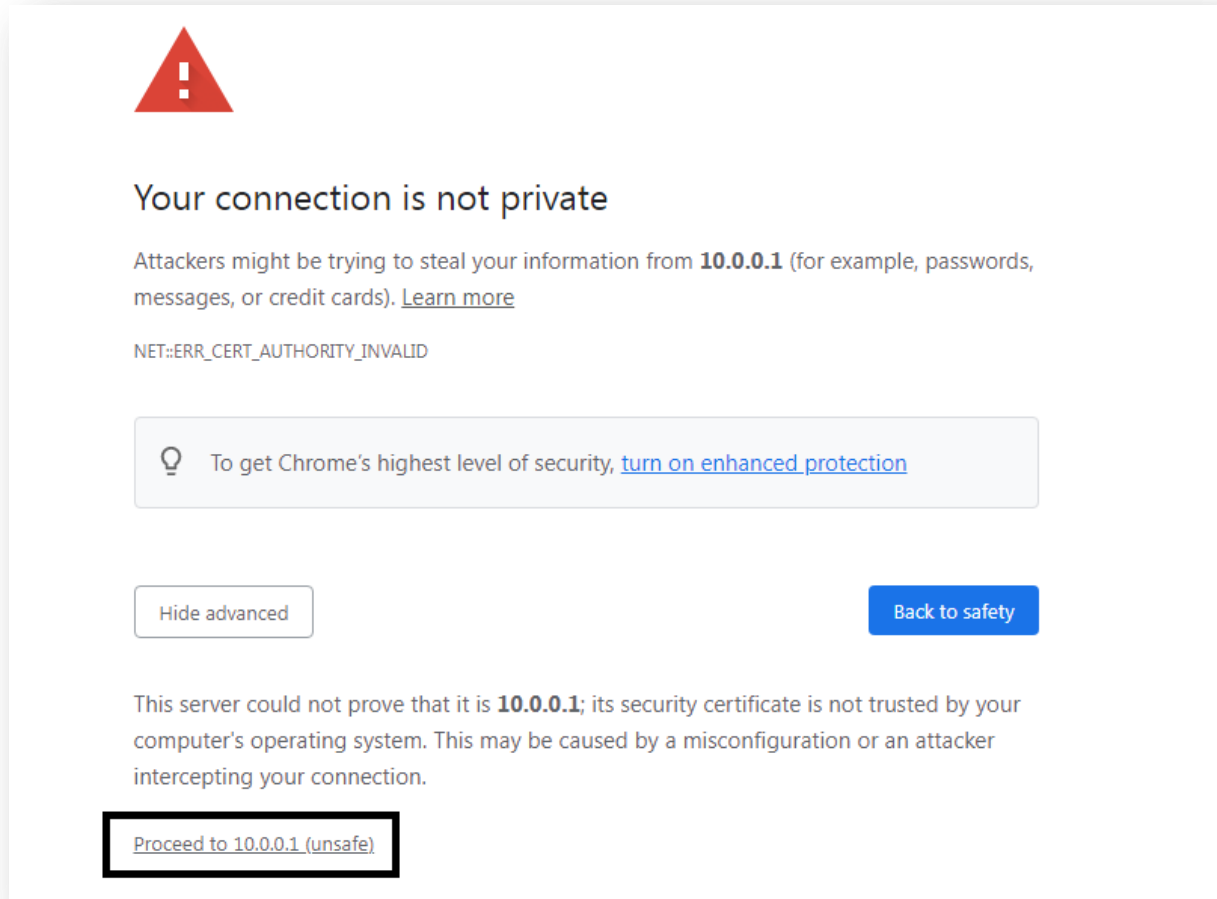
Nom d'utilisateur : root

Mot de passe : celui que vous avez spécifié lors de l'installation.

Depuis un autre poste sur le réseau local qui dispose bien d'une IP dans ce réseau (ip fixe ou dynamique attribuée pas un DHCP), ouvrez un navigateur internet et connectez vous à l'adresse suivante (en adaptant avec l'adresse IP que vous avez définie sur l'interface GREEN) :

<https://10.0.0.1:444>

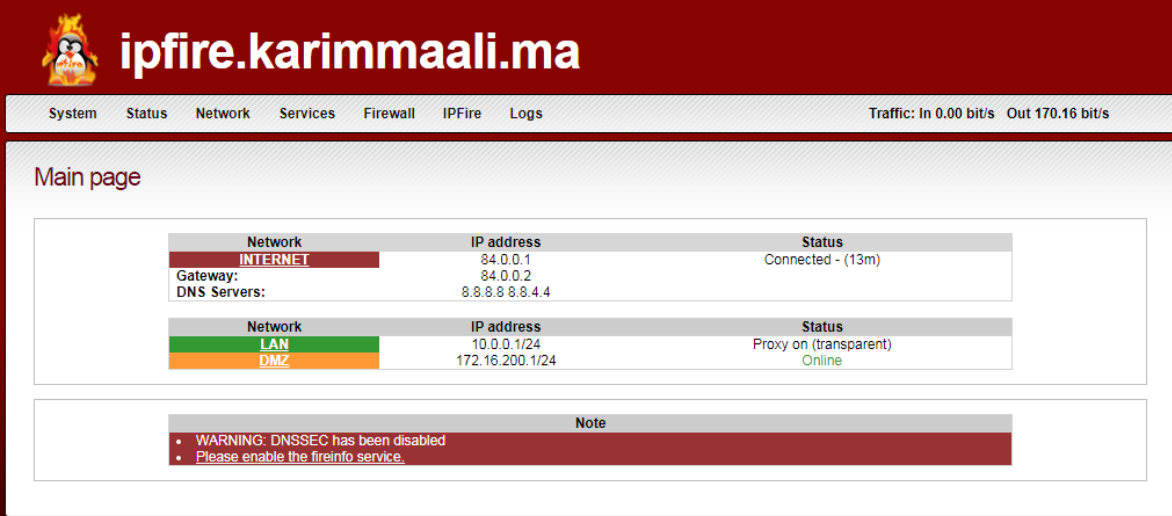
Si l'on vous dit que **la connexion n'est pas sécurisée**, no panic c'est normal on tente d'accéder à un site en HTTPS sans avoir de certificat valide. Cliquez sur Avancé puis sur « **Poursuivre vers IP (non sécurisé)** » (*La formulation peut varier selon le navigateur utilisé*).



Les identifiants de connexion à utiliser sont admin et le mot de passe que vous avez défini pour cet utilisateur.

A screenshot of a "Sign in" dialog box. The title is "Sign in" and the URL is "https://10.0.0.1:444". There are two input fields: "Username" with the text "admin" and "Password" with masked characters "*****". At the bottom right are two buttons: a blue "Sign in" button and a white "Cancel" button with a blue border.

Voici la page d'accueil du serveur IPfire :



The screenshot shows the IPfire web interface. At the top, there is a red header with the IPfire logo and the URL 'ipfire.karimmaali.ma'. Below the header is a navigation bar with links: System, Status, Network, Services, Firewall, IPFire, and Logs. On the right side of the navigation bar, it shows 'Traffic: In 0.00 bit/s Out 170.16 bit/s'. The main content area is titled 'Main page'. It contains two tables. The first table shows the 'INTERNET' network status: IP address 84.0.0.1, Gateway: 84.0.0.2, and DNS Servers: 8.8.8.8, 8.8.4.4. The status is 'Connected - (13m)'. The second table shows the 'LAN' and 'DMZ' network status: IP address 10.0.0.1/24 for LAN and 172.16.200.1/24 for DMZ. The status is 'Proxy on (transparent)' and 'Online'. At the bottom, there is a 'Note' section with a warning: 'WARNING: DNSSEC has been disabled. Please enable the fireinfo service.'



Configuration du Routeur R1 :

Interface	@IP	masque
F0/1	84.0.0.2	255.255.255.252
F1/0	200.100.50.1	255.255.255.0
F0/0	DHCP	DHCP

LA configuration :

```
interface FastEthernet0/1
ip address 84.0.0.2 255.255.255.252
ip nat inside
```

```
interface FastEthernet1/0
ip address 200.100.50.1 255.255.255.0
ip nat outside
```

```
interface FastEthernet0/0
ip address dhcp
ip nat outside
```

```
access-list 10 permit 10.0.0.0 0.0.0.255
ip nat inside source list 10 interface FastEthernet1/0
overload
```

```
ip dhcp pool R1
network 200.100.50.0 255.255.255.0
default-router 200.100.50.1
dns-server 8.8.8.8
```

```
ip route 10.0.0.0 255.255.255.0 84.0.0.1
ip route 172.16.200.0 255.255.255.0 84.0.0.1
```

Tester si le réseau interne 10.0.0.0/24 est autorisé à accéder à Internet **LAN-to-WAN**

```
C:\Users\karim>ping 8.8.8.8

Pinging 8.8.8.8 with 32 bytes of data:
Reply from 8.8.8.8: bytes=32 time=129ms TTL=126
Reply from 8.8.8.8: bytes=32 time=84ms TTL=126
Reply from 8.8.8.8: bytes=32 time=82ms TTL=126
Reply from 8.8.8.8: bytes=32 time=94ms TTL=126

Ping statistics for 8.8.8.8:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 82ms, Maximum = 129ms, Average = 97ms

C:\Users\karim>
```

Il doit également avoir accès au réseau 200.100.50.0/24 sur Internet. **LAN-to-WAN**

```
C:\Users\karim>ping 200.100.50.2

Pinging 200.100.50.2 with 32 bytes of data:
Reply from 200.100.50.2: bytes=32 time=42ms TTL=126
Reply from 200.100.50.2: bytes=32 time=28ms TTL=126
Reply from 200.100.50.2: bytes=32 time=27ms TTL=126
Reply from 200.100.50.2: bytes=32 time=27ms TTL=126

Ping statistics for 200.100.50.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 27ms, Maximum = 42ms, Average = 31ms

C:\Users\karim>
```

Désormais, tout le trafic réseau interne doit être bloqué. **WAN-to-LAN**

```
C:\Users\karim>ping 10.0.0.2

Pinging 10.0.0.2 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 10.0.0.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\Users\karim>_
```

DMZ-TO-LAN

```
karim@karim-virtual-machine:~$ ping 10.0.0.2
PING 10.0.0.2 (10.0.0.2) 56(84) bytes of data.
```

LAN-TO-DMZ

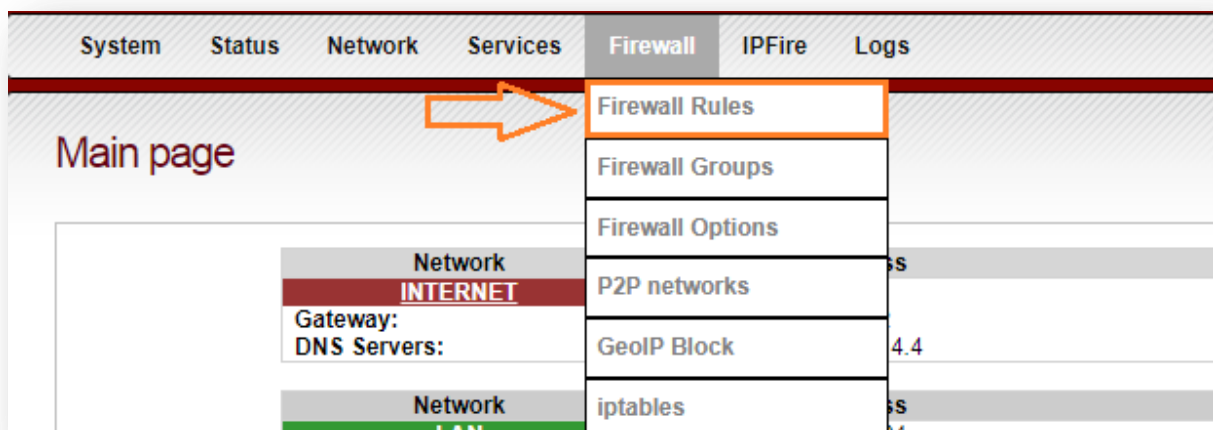
```
C:\Users\karim>ping 172.16.200.200

Pinging 172.16.200.200 with 32 bytes of data:
Reply from 172.16.200.200: bytes=32 time=1ms TTL=63
Reply from 172.16.200.200: bytes=32 time=3ms TTL=63
Reply from 172.16.200.200: bytes=32 time=2ms TTL=63
Reply from 172.16.200.200: bytes=32 time=1ms TTL=63

Ping statistics for 172.16.200.200:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 3ms, Average = 1ms
C:\Users\karim>_
```

Dans le cadre de la sécurisation de la zone démilitarisée (DMZ) et afin de n'autoriser que le trafic nécessaire, une politique de sécurité sera mise en place pour bloquer par défaut tous les protocoles transitant par la DMZ. Seul le protocole HTTP (**port 80**) sera autorisé, permettant ainsi le transfert des données nécessaires à la navigation web. L'objectif de cette politique est de réduire les risques de sécurité et de protéger les services disponibles dans la DMZ contre les attaques potentielles.

Dans le menu principal, sélectionnez **Règles de pare-feu**. (Firewall Rules)



Ajouter une nouvelle règle :



Précisez la source : Sélectionnez la zone : RED
(Internet)

Source

☐ Source address (MAC/IP address or network):

☒ Standard networks: RED

☐ GeoIP:

☐ Firewall: All

Destination: Sélectionnez la zone : Orange (DMZ)

Destination

☐ Destination address (IP address or network):

☒ Standard networks: ORANGE (172.16.200.0/24)

☐ GeoIP:

☐ Firewall: ORANGE (172.16.200.1)

Sélectionnez le protocole :

Sélectionnez le protocole : TCP.

Dans Port de destination, sélectionnez **Port 80**
(HTTP).

Action:

Sélectionnez Autoriser pour autoriser uniquement le
trafic.(accept)

Protocol

TCP




Source port:

Destination port: 80

☒ ACCEPT ☐ DROP ☐ REJECT

Sauvegarder la règle :

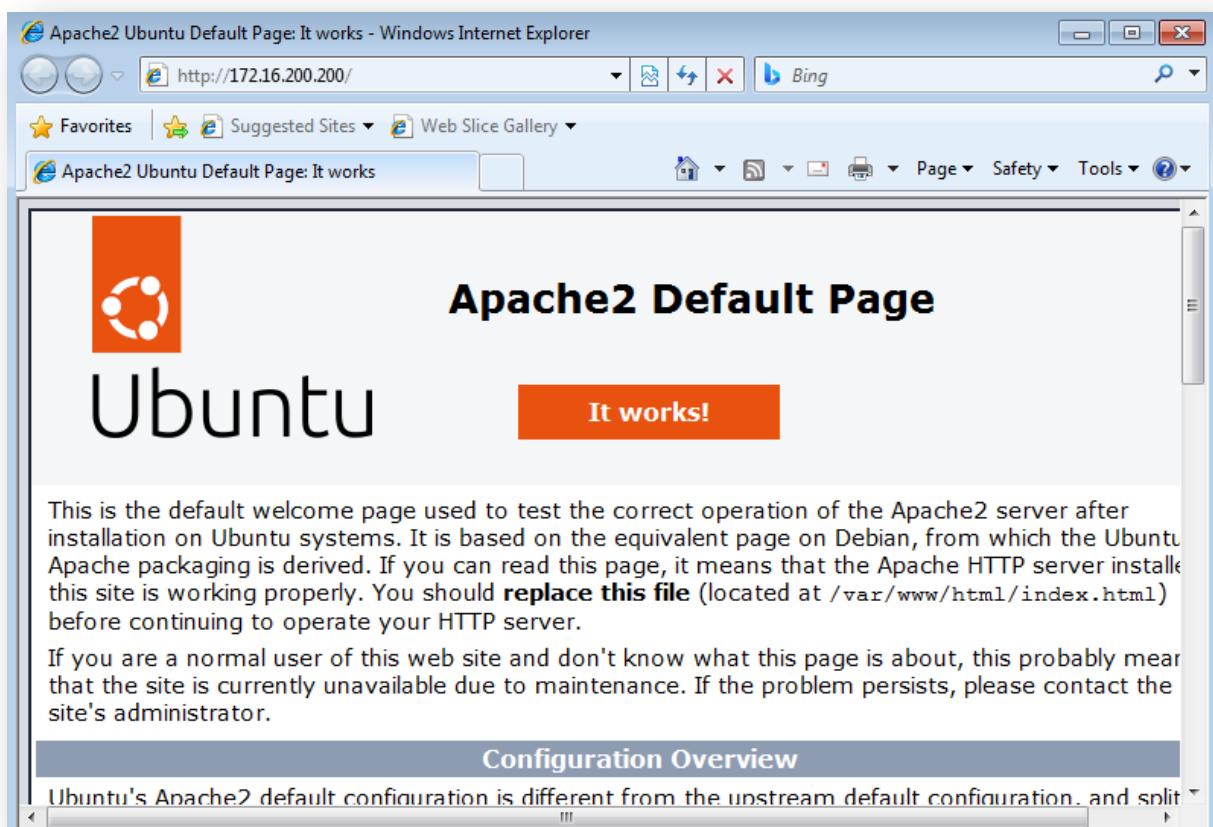
Firewall Rules

#	Protocol:	Source	Log	Destination	Action			
1	TCP	RED	<input type="checkbox"/>	ORANGE: 80	<input checked="" type="checkbox"/>			
GREEN		Internet (Allowed)		ORANGE (Allowed)				
ORANGE		Internet (Allowed)		GREEN (Blocked)				
Policy: Allowed								

Tests et ajustements supplémentaires :

Assurez-vous que cela fonctionne :

Essayez d'accéder au serveur dans la DMZ en utilisant HTTP depuis Internet.



Tous les protocoles sont bloqués sauf **HTTP**

```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\karim>ping 172.16.200.200

Pinging 172.16.200.200 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 172.16.200.200:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

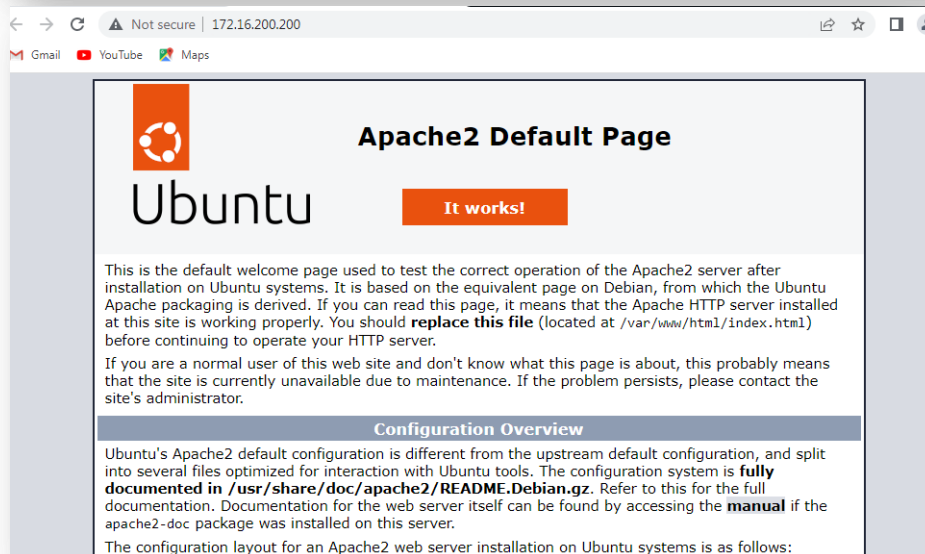
C:\Users\karim>_
```

Mais du *réseau interne* au réseau DMZ tous les protocoles sont autorisés **LAN-to-DMZ**

```
C:\Users\karim>ping 172.16.200.200

Pinging 172.16.200.200 with 32 bytes of data:
Reply from 172.16.200.200: bytes=32 time=81ms TTL=63
Reply from 172.16.200.200: bytes=32 time=1ms TTL=63
Reply from 172.16.200.200: bytes=32 time=2ms TTL=63
Reply from 172.16.200.200: bytes=32 time=3ms TTL=63

Ping statistics for 172.16.200.200:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 81ms, Average = 21ms
```



Tester les Ports du serveur pour la zone DMZ avec Nmap : Kali linux

```
(kali@kali)-[~]  
$ nmap 172.16.200.200  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-28 08:08 EST  
Nmap scan report for 172.16.200.200  
Host is up (0.31s latency).  
Not shown: 999 filtered tcp ports (no-response)  
PORT      STATE SERVICE  
80/tcp    open  http  
  
Nmap done: 1 IP address (1 host up) scanned in 35.65 seconds
```

IP vérifiée : 172.16.200.200.

L'hôte est en place.

Il y a 999 ports filtrés qui n'ont pas reçu de réponse.

Le port 80/TCP est ouvert et exécute HTTP.

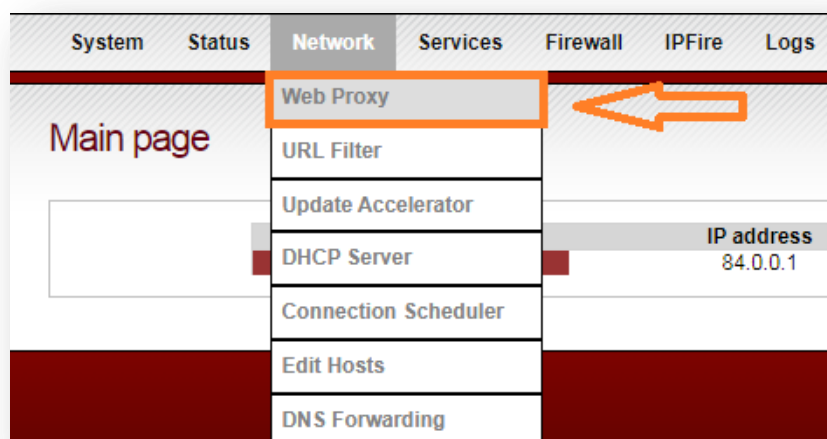
L'analyse a duré 35,65 secondes.

Les ports restants sont filtrés, ce qui signifie que le pare-feu a **bloqué** tous les protocoles sauf le Web.



CONFIGURATION DU PROXY WEB D'IPFIRE

Cliquez, dans le menu IPFire, sur « Réseau » - « Proxy web » • :



Activez les cases « Actif sur Green » et « Transparent sur Green » • Activez les cases « Filtre URL » et « Mise à jour de l'accélérateur »

Advanced Web Proxy

Common settings

Enabled on Green: ☒

Transparent on Green: ☒

Proxy port: * 800

Transparent port: * 3128

Visible hostname:

Error messages language: de

Error messages design: IPFire

Suppress version information: ☐

Squid cache version: [3.5.25]

Number of filter processes

Processes: * 10

URL filter

Enabled ☒

+ 8

Update accelerator

Enabled ☒

+ 7

Dans le bas de la fenêtre, cliquez le bouton « Sauvegarder et redémarrer » :

Save Save and Reload Save and Restart Clear Cache

* Required field

☐ **Activer le proxy pour le client :**

- Dans la section **Serveur proxy**, cochez l'option **Utiliser un serveur proxy pour votre réseau local (LAN)**.

☐ **Entrer les informations du proxy :**

-
-
- Dans le champ **Adresse**, saisissez l'adresse IP du proxy. (10.0.0.1)
- Dans le champ **Port**, entrez le numéro du port. (800)

☐ **Enregistrer les modifications :**

- Cliquez sur **OK** pour fermer la fenêtre des paramètres réseau.
- Cliquez à nouveau sur **OK** dans la fenêtre **Propriétés Internet**.

Local Area Network (LAN) Settings

Automatic configuration

Automatic configuration may override manual settings. To ensure the use of manual settings, disable automatic configuration.

☒ Automatically detect settings

☐ Use automatic configuration script

Address:

Proxy server

☒ Use a proxy server for your LAN (These settings will not apply to dial-up or VPN connections).

Address: 10.0.0.1 Port: 800 Advanced

☐ Bypass proxy server for local addresses

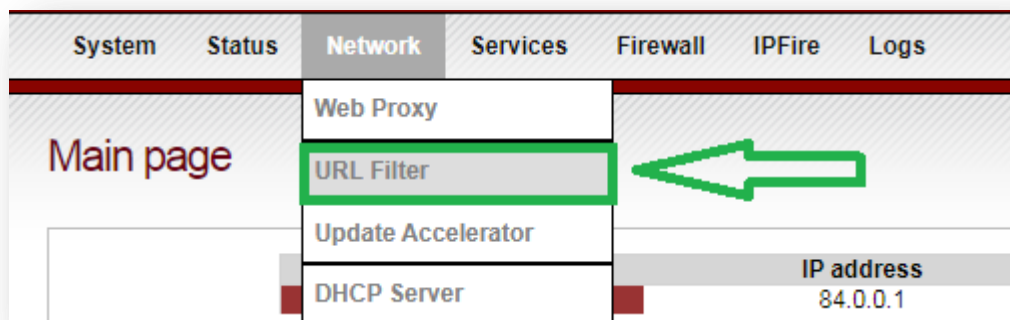
OK Cancel

❑ **Tester la connexion :**

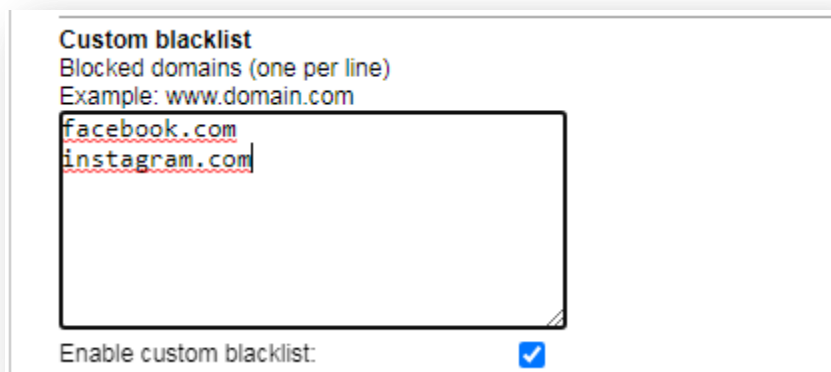
- Essayez d'accéder à un site web pour vérifier que le proxy fonctionne correctement.

Bloquer certains sites :

Cliquez ensuite sur le menu « Réseau » et « Filtrer le contenu URL »



Ajoutez les noms de domaine que vous souhaitez bloquer.



This site can't be reached

The webpage at <https://www.facebook.com/> might be temporarily down or it may have moved permanently to a new web address.

ERR_TUNNEL_CONNECTION_FAILED



This site can't be reached

The webpage at <https://www.instagram.com/> might be temporarily down or it may have moved permanently to a new web address.

ERR_TUNNEL_CONNECTION_FAILED

Il existe de nombreux avantages que vous pouvez découvrir avec la pratique.