

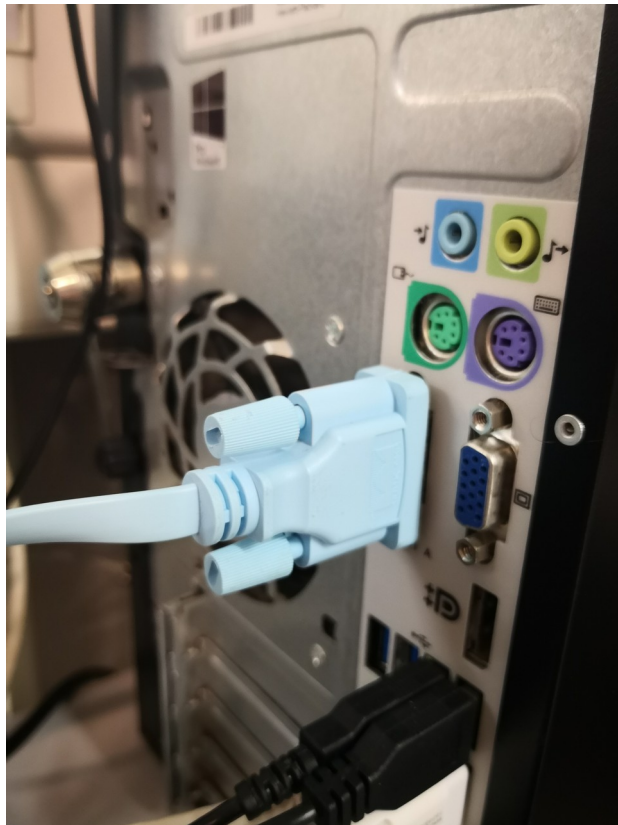
## Process de configuration de la borne Wifi Cisco(Sans sécurité)

Pour configurer la borne wifi cisco Aironet 1200 Series, vous devez relier le port console de la borne wifi et le port serial du pc entre eux à l'aide d'un câble console. Il faut aussi relier le port ethernet de la borne wifi au vlan qui lui est attribué (pour notre configuration nous avons utilisé le vlan 42 de notre salle de cours), et il faut aussi relier la carte réseau dédiée au réseau **bleu** d'ipfire à ce même vlan.

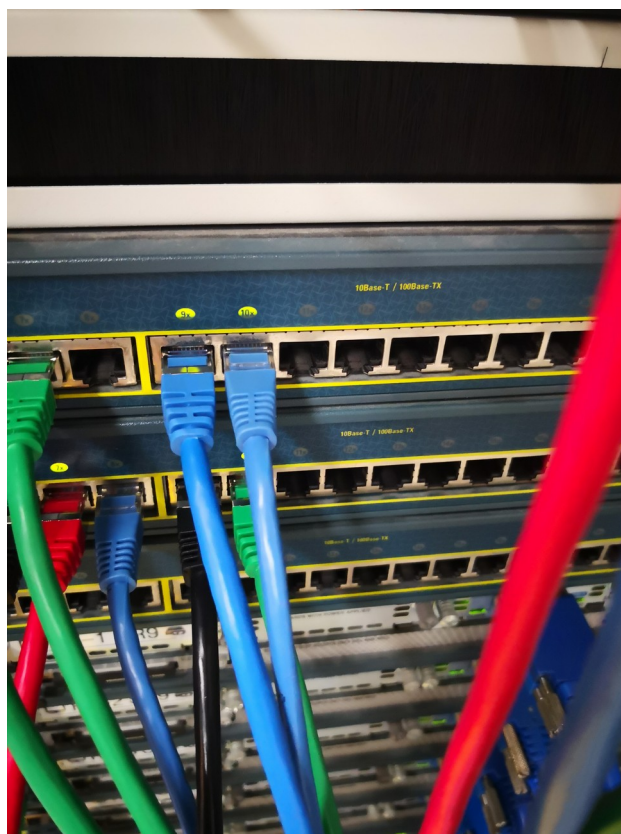
Port console de la borne wifi ci-dessous en bleu et port ethernet en jaune :



Port serial du pc ci-dessous en bleu clair :



Vlan 42 ci-dessous câblé en bleu :





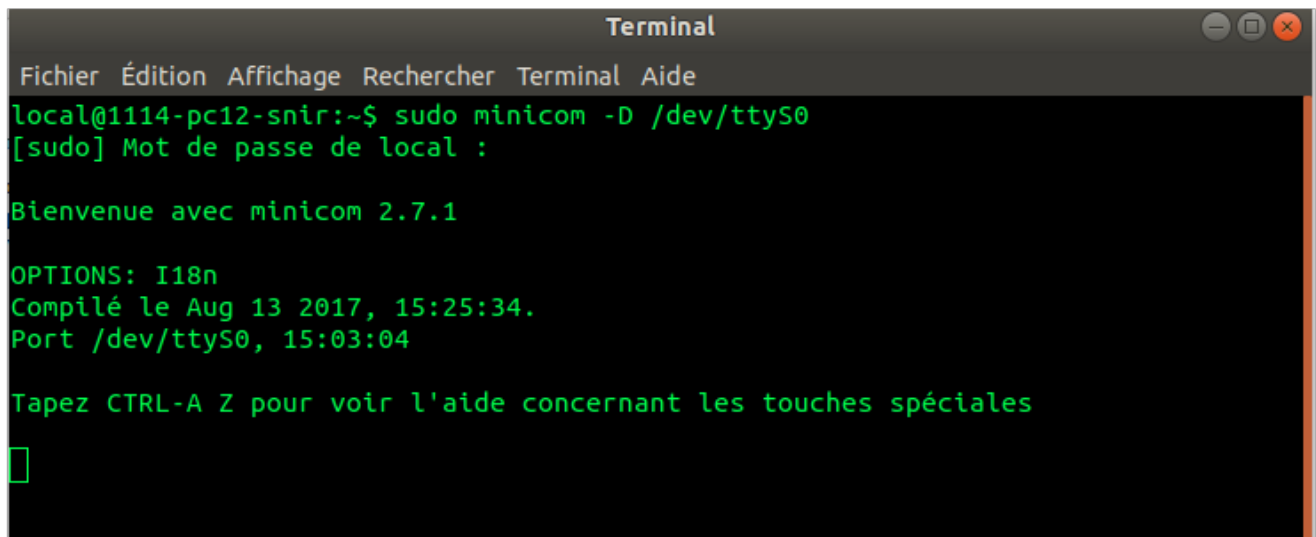
Carte réseau dédiée au réseau bleu du firewall ipfire (pastille bleu):



Une fois le câblage effectué, il faut ensuite se connecter à la borne wifi cisco pour la paramétrer.

Sous linux nous utilisons **Minicom** qui est un programme de communication serial pour accéder un équipement réseau ou sécurité par l'intermédiaire de son port console (Son alternative sous Windows est PuTTY).

Commande pour se connecter à la borne wifi avec minicom « `sudo minicom -D /dev/ttyS0`»:



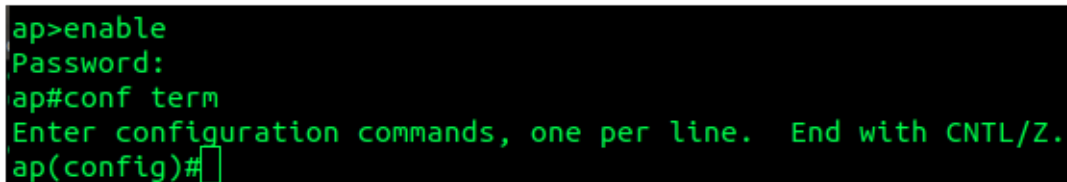
```
Terminal
Fichier Édition Affichage Rechercher Terminal Aide
local@1114-pc12-snr:~$ sudo minicom -D /dev/ttyS0
[sudo] Mot de passe de local :

Bienvenue avec minicom 2.7.1

OPTIONS: I18n
Compilé le Aug 13 2017, 15:25:34.
Port /dev/ttyS0, 15:03:04

Tapez CTRL-A Z pour voir l'aide concernant les touches spéciales
█
```

Ensuite on active les commandes privilégiées et on va passer en mode configuration. L'identifiant et le mot de passe par défaut est « **Cisco** ».



```
ap>enable
Password:
ap#conf term
Enter configuration commands, one per line.  End with CNTL/Z.
ap(config)#█
```

On va maintenant la nommer :

- `ap(config)#hostname ipfire`

On va maintenant configurer l'interface virtuelle controlant les interfaces fastEthernet et radio de la borne. Attention, il ne faudra jamais attribuer une adresse IP à l'interface fastEthernet ou l'interface radio. Seule la bvi doit en avoir une. Pour cela, en mode console, tapez les commandes suivantes :

```
ipfire#configure terminal
ipfire(config)#interface bvi1
ipfire(config-if)#ip address 192.168.1.2 255.255.255.0
ipfire(config-if)#no shutdown
ipfire(config-if)#^Z
ipfire#
```

Nous allons finir de configurer à minima la borne pour :

- qu'elle diffuse un SSID nommé ipfire
- que l'authentification soit la plus simple possible
- et qu'il n'y ait pas d'encryption lors de l'échange des données.

Les commandes sont donc les suivantes :

```
ipfire#configure terminal
ipfire(config)#dot11 ssid ipfire
ipfire(config-ssid)#authentication open
ipfire(config-ssid)#guest-mode
ipfire(config-ssid)#exit
ipfire(config)#interface dot11radio 0
ipfire(config-if)#ssid ipfire
ipfire(config-if)#no shutdown
ipfire(config-if)#^Z
```

Nous n'oublions pas de rajouter une porte de sortie vers d'autre réseau :

```
ipfire#configure terminal
ipfire(config)# ip default-gateway 192.168.1.1
ipfire(config)#^Z
```

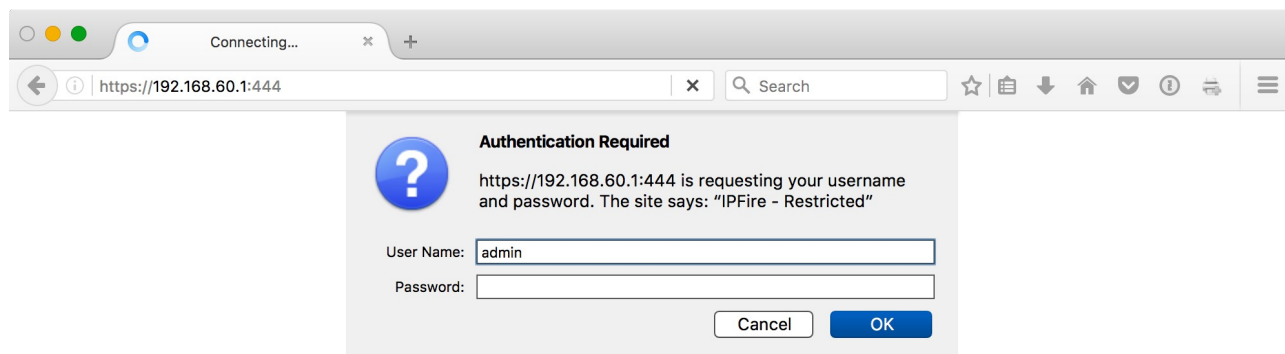
On fini en sauvegardant les paramètres :

```
ipfire#copy running-config startup-config
```

De base ipfire bloque l'accès à d'autre réseau à tous les périphériques du réseau bleu, il faut donc autoriser cette accès. Pour ce faire, il faut se connecter à l'interface utilisateur Web d'ipfire. L'interface utilisateur Web IPFire (également appelée interface Web ou webUI ou WUI) est une interface permettant de configurer IPFire.

Vous pouvez y accéder via un navigateur Web à partir de n'importe quel ordinateur du réseau **vert** . Une fois la connexion établie, il permet d'accéder à tous les paramètres et fonctionnalités d'IPFire.

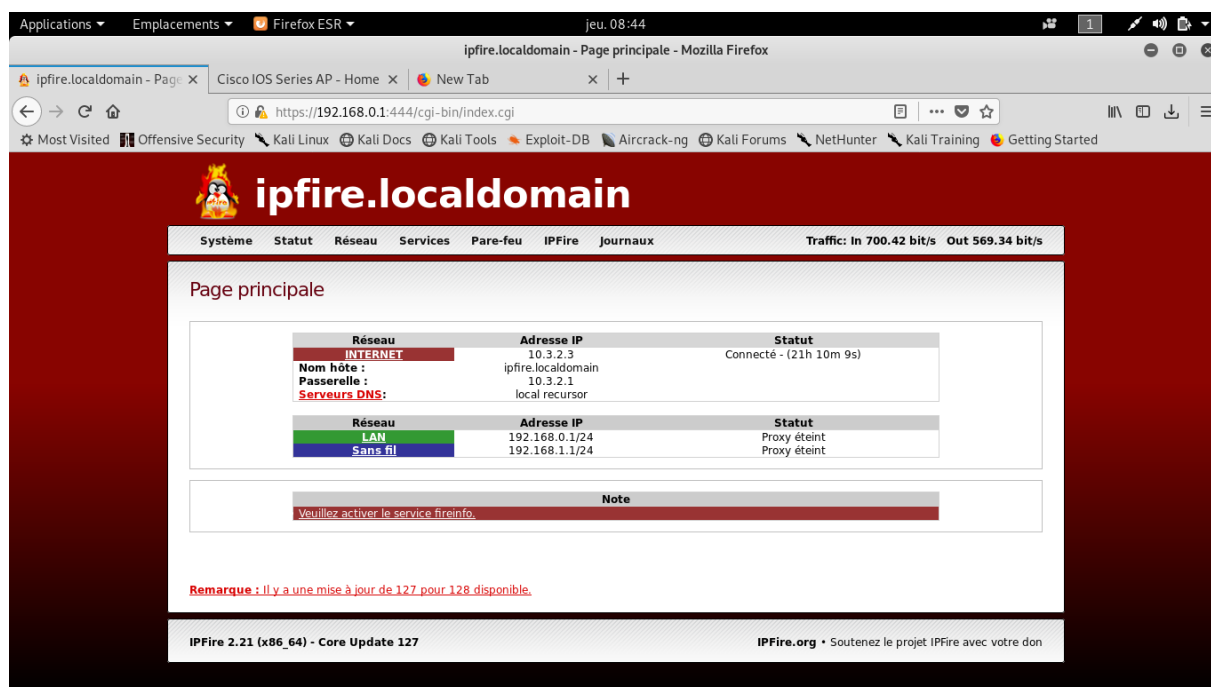
Par défaut, l'interface Web est à l' [adresse https://ipfire.localdomain:444](https://ipfire.localdomain:444) . Si vous utilisez un nom d'hôte ou un domaine différent, vous devrez l'utiliser ou y accéder facilement via l'adresse IP (par exemple, <https://192.168.0.1:444> ).



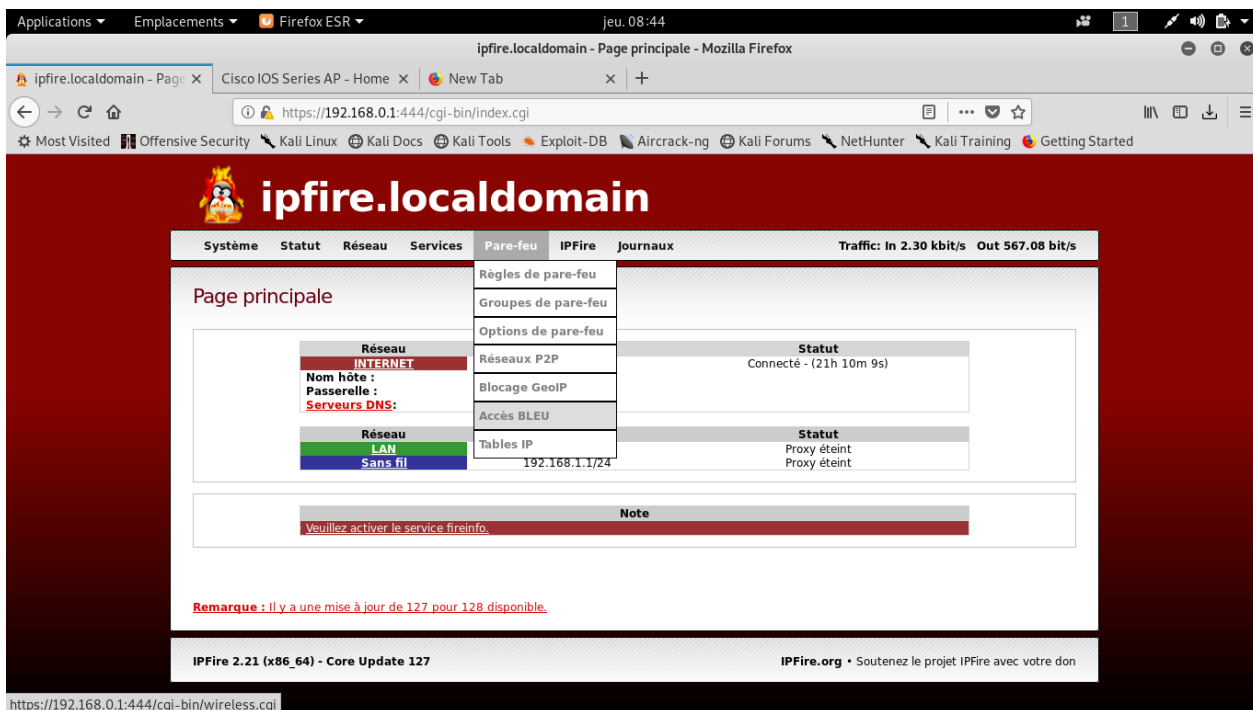
Votre navigateur Web affichera un avertissement «Certificat de sécurité auto-signé» lors de la tentative d'ouverture de l'interface Web. Vous devez accepter ce certificat pour pouvoir vous connecter!

Une fenêtre apparaîtra vous demandant votre nom d'utilisateur et votre mot de passe. Le nom d'utilisateur pour l'admission est **admin** et le mot de passe est celui qui a été saisi lors de la procédure d'installation du compte admin. (mot de passe : « admin »)

Une fois connecté, vous arrivez sur la page d'accueil.

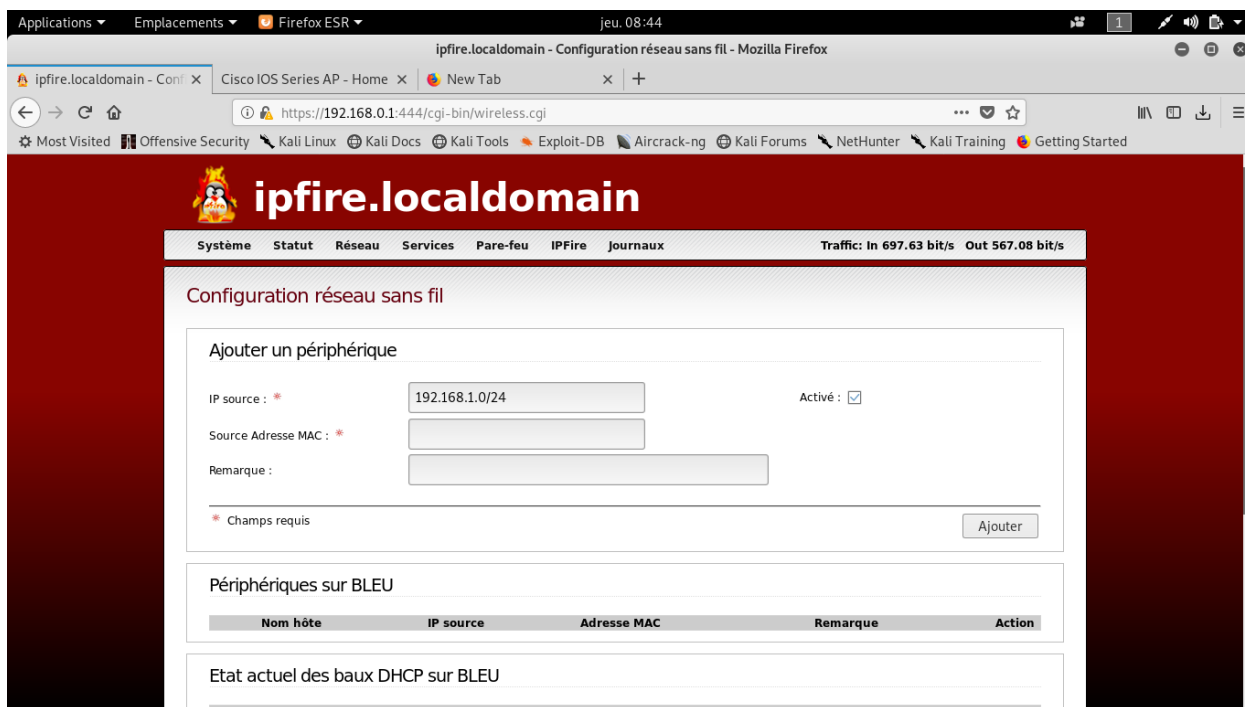


Ensuite, il faut se rendre dans l'onglet pare-feu et cliquer sur « Accès BLEU » :



The screenshot shows the IPFire web interface in a Mozilla Firefox browser. The address bar displays `https://192.168.0.1:444/cgi-bin/index.cgi`. The page title is "ipfire.localdomain - Page principale". The navigation menu includes "Système", "Statut", "Réseau", "Services", "Pare-feu", "IPFire", and "Journaux". The "Pare-feu" menu is expanded, showing options like "Règles de pare-feu", "Groupes de pare-feu", "Options de pare-feu", "Réseaux P2P", "Blocage GeoIP", "Accès BLEU", and "Tables IP". The "Accès BLEU" option is highlighted. The main content area shows the "Page principale" with a "Réseau" section displaying "INTERNET" and "LAN" networks. A "Statut" section shows "Connecté - (21h 10m 9s)". A "Note" section contains the message "Veuillez activer le service fireinfo." and a "Remarque" section mentions a update for version 127.

Sur la page qui s'affiche, il faut renseigner l'adresse réseau de Bleu avec son masque et cliquer sur activé puis ajouter:



The screenshot shows the IPFire web interface in a Mozilla Firefox browser. The address bar displays `https://192.168.0.1:444/cgi-bin/wireless.cgi`. The page title is "ipfire.localdomain - Configuration réseau sans fil". The navigation menu includes "Système", "Statut", "Réseau", "Services", "Pare-feu", "IPFire", and "Journaux". The "IPFire" menu is expanded, showing options like "Ajouter un périphérique", "Périphériques sur BLEU", and "Etat actuel des baux DHCP sur BLEU". The "Ajouter un périphérique" form is visible, with fields for "IP source" (192.168.1.0/24), "Source Adresse MAC", and "Remarque". The "Activé" checkbox is checked. A "Champs requis" message is displayed. The "Ajouter" button is visible. Below the form, the "Périphériques sur BLEU" section shows a table with columns: "Nom hôte", "IP source", "Adresse MAC", "Remarque", and "Action". The "Etat actuel des baux DHCP sur BLEU" section is also visible.

Applications ▾Emplacements ▾Firefox ESR ▾

jeu. 08:44

ipfire.localdomain - Configuration réseau sans fil - Mozilla Firefox

ipfire.localdomain - Conf

Cisco IOS Series AP - Home

New Tab

←→↻🏠

🔒📄🔗https://192.168.0.1:444/cgi-bin/wireless.cgi

⋮📧🌟

🔍📄📄📄

🔗🔗🔗🔗🔗🔗🔗🔗

⚙️ Most Visited📁 Offensive Security🐧 Kali Linux📄 Kali Docs🔗 Kali Tools🔥 Exploit-DB🔍 Aircrack-ng🌐 Kali Forums🔍 NetHunter🐧 Kali Training🔥 Getting Started

IP source : \*

Activé : ☐

Source Adresse MAC : \*

Remarque :

\* Champs requis

Ajouter

Périphériques sur BLEU

Nom hôte	IP source	Adresse MAC	Remarque	Action
	192.168.1.0/24	NONE		☑️✎🗑

Etat actuel des baux DHCP sur BLEU

Adresse IP	Adresse MAC	Nom hôte	Bail expiré (local time d/m/y)	
192.168.1.3	20:54:fa:12:8f:ac	HUAWEI_Mate_10_Pro-4fc8a5	21/03/2019 09:38:46	✎+
192.168.1.4	00:1b:d5:9f:68:36		20/03/2019 11:04:29	✎+
192.168.1.5	00:40:96:b2:50:f7		20/03/2019 11:21:59	✎+
192.168.1.6	80:a5:89:b4:d3:c3	SmKali	21/03/2019 09:36:04	✎+
192.168.1.7	84:9f:b5:26:f7:4a		20/03/2019 14:01:40	✎+
192.168.1.8	08:78:08:fd:00:2a	Galaxy-A5-2017	21/03/2019 09:25:58	✎+



En dernière étape, on effectue un ping vers le serveur dns de google 8.8.8.8 pour vérifier la connectivité :

```
ipfire#ping 8.8.8.8
```

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 8.8.8.8, timeout is 2 seconds:

!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 9/9/10 ms

```
ipfire#
```

Et on vérifie la connexion au point d'accès à l'aide d'un pc :

