Formation mini-routeurs

...

lionofminirouteurs & frazewtf

Sponsorisé par :

- beaucoup trop de schémas dsl
- lovali la meilleure sur PS

Mariage de mon meilleur pote

Formation mini-routeur

Wi-Fi : entre science et magie noire

Murs de la Maisel être comme

ArchéologIPP

Historique à MiNET

Il faut remonter au 29 Septembre 2017 pour voir un début de solution à ce problème:

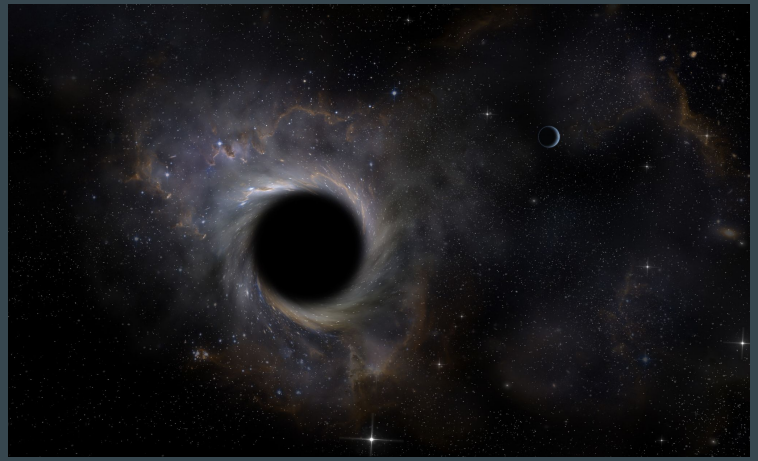
```
2) Pour les adhérents qui ont des connexions de merde, on propose un
service de location (sous caution à définir) des E3000 et de mini
routeur TP Link pour couvrir les trous de couverture. Dessus on flash un
firmware OpenWRT qui diffusera le SSID MiNET. Soit on relie la borne au
Radius MiNET pour rajouter une borne, soit on diffuse le SSID en
autorisant que les adresses MAC de l'adhérent sur la borne. (moins bien
car il peut avoir des nouveaux appareils et ça sera chiant à optimiser)
3) Sur plusieurs années, on met les mini routeurs TP Link avec des
OpenWRT flashé dans TOUTES les chambres des adhérents. Ça va être bagdad
mais c'est la solution qui nous permet de rester concurrentiel au niveau
débit.

Sowarks, mail sur équipe, 29 Sept 2017
```

Ah parce que tu pensais qu'une diapo suffisait ?

On leur a exposé notre idée de l'utilisation de mini-routeur pour completer notre couverture wifi, que l'on proposerait à nos adhérents. Ils ont ajouté à cela que eux aussi devrait sans doute à l'avenir utiliser des plus petits points d'accès (c'est ce qui se fait de plus en plus), même si leur couverture actuelle reste à priori satisfaisante.

varens 2018



En parallèle, pour gérer les zones mal couvertes, la solution des mini-routeurs a été proposée. Il s'agirait de mettre à disposition des mini-routeurs aux étudiants logeant dans ces zones, en échange d'une caution par chèque que l'on n'encaisserai pas. Les cautions sont un peu chiantes à gérer, mais ça reste jouable, le problème reste les étudiants étrangers qui n'ont pas de chéquier... De plus, il faudrait aussi rajouter cette option dans adhx. Va donc falloir bosser sur adh6.

On a un mini-routeur dans le local, un tp-link TL-WR810N (doc ici : https://static.tp-link.com/res/down/doc/TL-WR810N(EU_V1_UG.pdf) qui coûte dans les 30 euros environ. On peut donc effectuer des tests, sur sa portée dans une chambre adhérente, dans les chambres voisines, etc... Nous auront accès à des chambres pendant le recâblage u3 (qui se passe pendant les vacances d'avril), on pourra donc effectuer tous les tests nécessaires à ce moment, notamment par rapport aux différentes configurations possibles sur lesquelles on a commencé à réfléchir.

abracadabrastoral 2018

Toujours pas bg

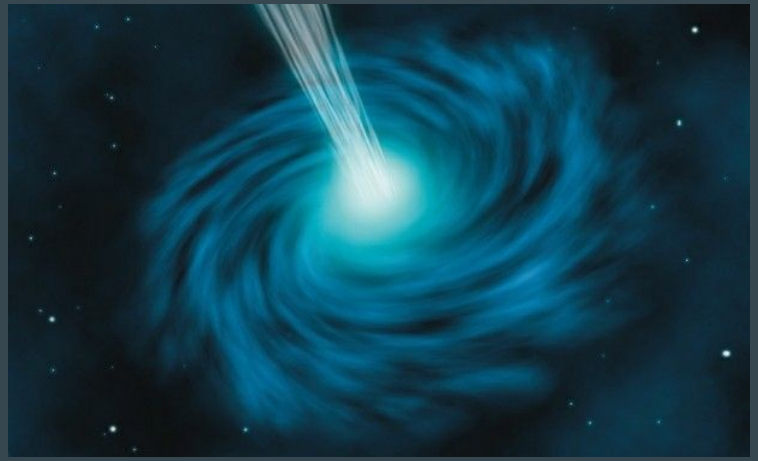
13 Projets menés dans l'immédiat

— Projets routeurs (Diabord, Gabery, Littlewillow) **Cahier des charges à établir**
Acheter plein de mini-routeurs afin de se constituer un stock (avantage, on pourra mettre le logo MiNET dessus) *Sourire niais et content de François*

littlewillow 2019

(j'ai soigné la transi tavu)

frazew 2019



Cependant, le routeur en question (TL-WR902AC -> https://www.amazon.fr/TP-Link-Routeur-Répéteur-Ethernet-TL-WR902AC/dp/B01MY...) n'est manifestement plus fabriqué. J'ai donc cherché des alternatives et le choix final semble s'orienter vers le routeur suivant : GL-AR750 (https://www.alibaba.com/product-detail/GL-AR750-5-8Ghz-802-3af_60627231927....). Une liste (probablement non exhaustive) des avantages :

- 2.4GHz et 5GHz

- OpenWRT (!)

- PoE (ce qui veut dire que potentiellement on a juste à filer le routeur, le mec branche et hop ça marche)

- Possibilité éventuellement en négociant de mettre le logo MiNET dessus (pas obligatoire, mais il faut bien reconnaître que c'est stylé)

Allez j'arrête

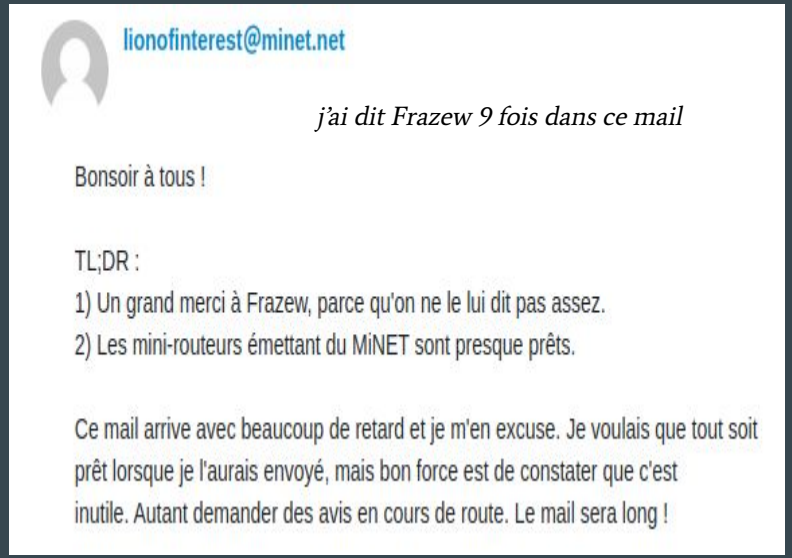
Yo,

Spoilers, ça risque d'être un peu long, donc si vous avez la flemme, il y a toujours le TL;DR juste là :

TL;DR: suite au stage d'Alex (diabord) de cet été, une infra de test parallèle à l'infra wifi actuelle a été mise en place pour NATer chaque adhérent derrière sa propre IP publique en Wifi (on a récupéré le 157.159.192.0/22 de la DISI, oui oui). Parallèlement, le développement des mini-routeurs a (beaucoup) avancé, mais là je peux pas TL;DR il faut lire, désolé.

Bon, comme c'est long, on va faire en plusieurs parties. @1A @2A svp prenez le temps de lire et bombardez moi de questions s'il le faut ;)

frazew 2019



lionoftocard 2021

(comment ça j'ai pas mis de trou noir ici ???)

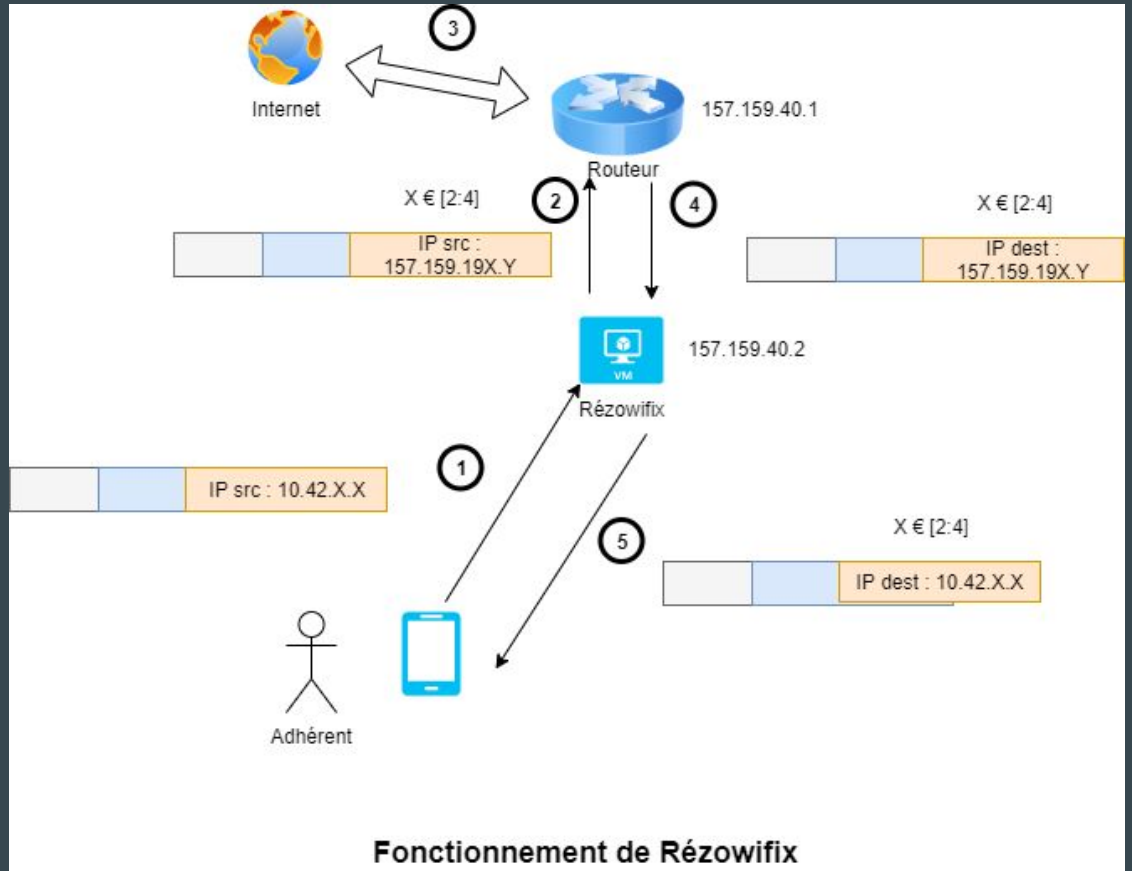
Définitions et rappels

Notions importantes - VxLAN

Rappel : VLAN

Notions importantes - Rézowifix

Rappel : NAT



Fonctionnement de Rézowifix

Notions importantes - Wireguard

Rappel : VPN

Lezgo résumé rapide

Nos acteurs principaux (p’tit partenariat la RE ?)

OS basé sur du Linux
Open Source
Idéal pour les systèmes embarqués
Ultra modulable et customizable

Constructeur de routeurs, de MINI routeurs
Large éventail de routeurs faciles à prendre en main
Routeurs basés sur du OpenWRT

Virgin mini-routeur

Bébou pas configuré

Crée un réseau privé, n'importe qui peut faire du partage de compte

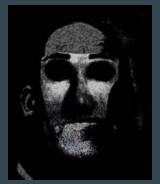
Le mot de passe par défaut du pannel admin...

Compliqué de monitorer

Un réseau privé par mini-routeur

Virgin mini-routeur

Bébou pas configuré



Crée un réseau privé, n'importe qui peut faire du partage de compte

Le mot de passe par défaut du pannel admin...

Compliqué de monitorer

Un réseau privé par mini-routeur

Chad mini-routeur

Émet "du MiNET" & attribue les mêmes IPs

Ne sert QUE de relais au trafic

Mot de passe généré aléatoirement

Monitoré (tqt)

Bébou pimpé

Service rendu à la communauté

Bébou pas configuré

Réseau privé

ne peut pas
se connecter

IP en 192.168.8.X

Bébou pimpé

Réseau MiNET

peut se connecter

IP en 10.42.X.X

L’infra de zéro

Un mini-routeur, qui va où ?

Cahier des charges

Bébou

- En tant qu'adhérent je veux avoir une bonne co wifi dans ma chambre en branchant bébou
- En tant qu'adhérent voisin je veux pouvoir me connecter à bébou sans que mon voisin h4ck mon trafic
- En tant qu'adhérent je veux pouvoir utiliser les interwebs en me connectant à bébou
- En tant qu'adhérent je veux pas changer la configuration wifi sur mon tel pour me co à bébou

Cahier des charges

Bébou

- En tant qu'adhérent je veux avoir une bonne co wifi dans [illegible] en branchant bébou
- En tant qu'adhérent voisin je veux pouvoir me connecter à bébou [illegible] mon voisin h4ck mon trafic
- En tant qu'adhérent je veux pouvoir utiliser les interwebs en me connectant à bébou
- En tant qu'adhérent je veux pas changer la configuration wifi [illegible] mon tel pour me co à bébou

HARDWARE PERFORMANT

WIREGUARD

VxLAN

RADIUS

Wireguard & VxLAN

Pourquoi il faut sécuriser ?

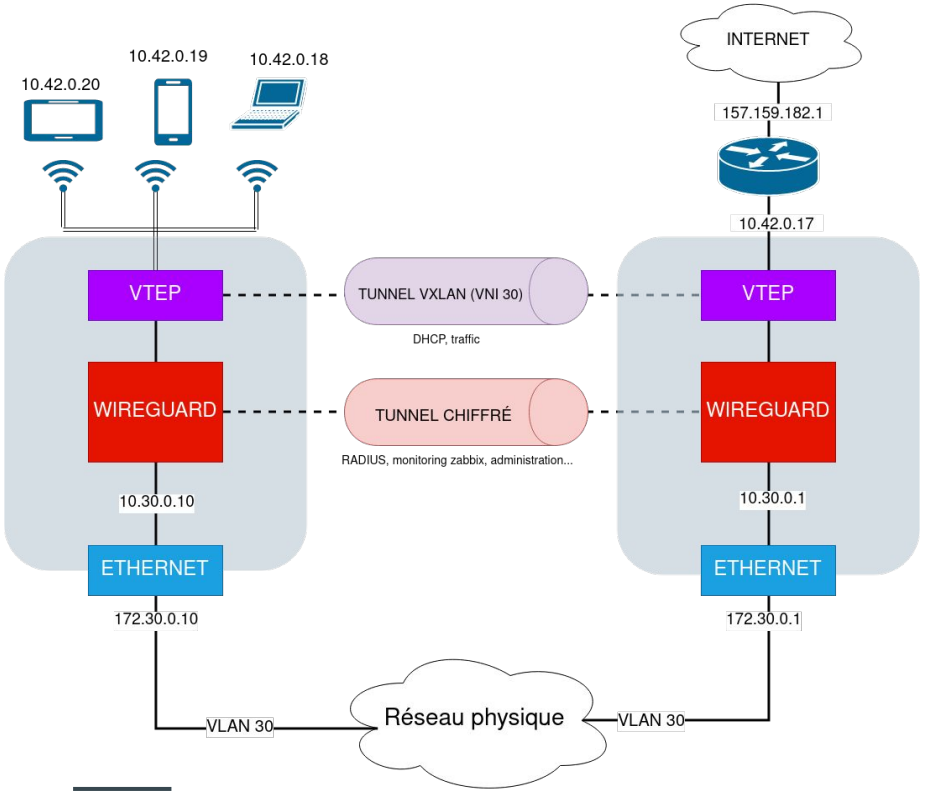
```
switchport voice vlan 30
switchport authentication multi-auth
mab
```

Comment on sécurise alors ?

Un bel oignon: encapsulations successives

Physique
Ethernet VLAN 30 *(séparation logique)*
IP VLAN 30 *(172.30.0.16)*
IP Wireguard *(10.30.0.16)*
VxLAN *(encapsulation UDP)*
Traffic adhérent *(Ethernet, IP, TCP/UDP)*

Résumé intermédiaire



Cahier des charges (le retour)

Bébou

- En tant qu'adhérent je veux avoir une bonne co wifi dans [illegible] en branchant bébou
- En tant qu'adhérent voisin je veux pouvoir me connecter à b[illegible] mon voisin h4ck mon trafic
- En tant qu'adhérent je veux pouvoir utiliser les interwebs en [illegible]ectant à bébou
- En tant qu'adhérent je veux pas changer la configuration wifi [illegible] mon tel pour me co à bébou

HARDWARE PERFORMANT

WIREGUARD

VxLAN

RADIUS

Hardware performant

Les sets d’instructions

Un SoC (System on Chip)

Un “vrai” processeur

(Court) cours d'assembleur ptdr

Pour UN SEUL round AES

```
procedure Round(State,ExpandedKey[i])
    SubBytes(State);
    ShiftRows(State);
    MixColumns(State);
    AddRoundKey(State,ExpandedKey[i]);
end procedure
```

De la soustraction, multiplication, XOR, addition, utilisation de la stack etc = **PLEIN D'INSTRUCTIONS**

Avec un set d'instructions dédié

`AESENC`: Perform one round of an AES encryption flow

Mesures concrètes

	Protocole d'authentification, hashing, chiffrement	**Débit sur le processeur embarqué**
OpenVPN	RSA / Courbes elliptiques SHA AES	~ 35Mbps
IPSec	RSA / PSK SHA AES	~ 25Mbps
Wireguard	Courbes elliptiques BLAKE2s ChaCha20	~ 50Mbps

Le cassiopus où on a essayé de faire un meilleur hardware

Cahier des charges (le retour encore)

Bébou

- En  dhérent je veux avoir une bonne co wi xe en branchant bébou

HARDWARE PERFORMANT

- En tant qu'adhérent voisin je veux pouvoir me connecter à b pas mon voisin h4ck mon trafic

WIREGUARD

- En tant qu'adhérent je veux pouvoir utiliser les interwebs en r nectant à bébou

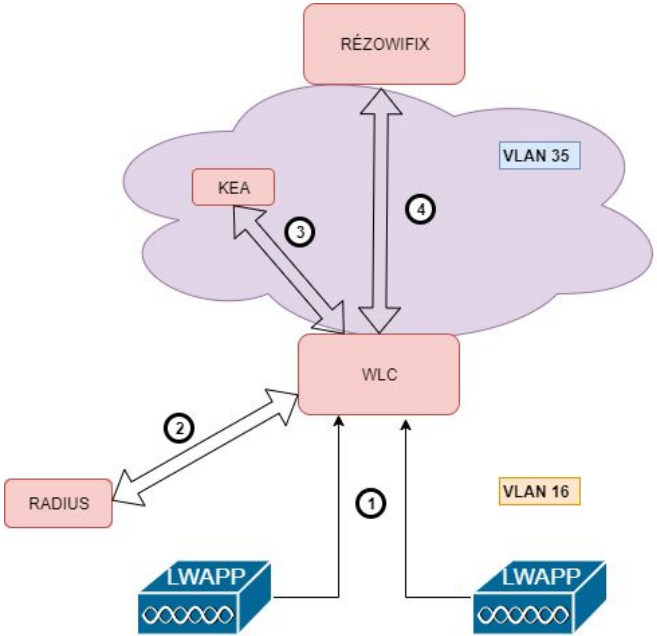
VxLAN

- En tant qu'adhérent je veux pas changer la configuration wi sur mon tel pour me co à bébou

RADIUS

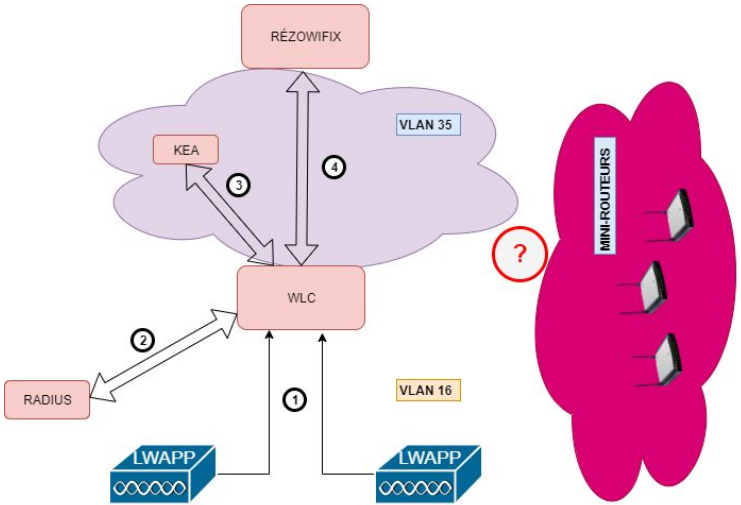
RADIUS & NAT

On a une infra wifi qui existe déjà...



L'infra Wifi "normale"

Comment on vient se brancher dessus ?



where mini-routeur??
where wireguard??
where vxlan??

C’est parti, lovali veut se connecter à MiNET

Le routeur diffuse du MiNET

VLAN 102

authentifie

RADIUS

C’est hors de question d’avoir une comm directe entre les deux

connexion

EAP
MSCHAP-V2
lovali a bien lu les tutos

Si seulement...
Si seulement on avait une passerelle qui a une patte dans le 102 et qui gère le Wi-Fi

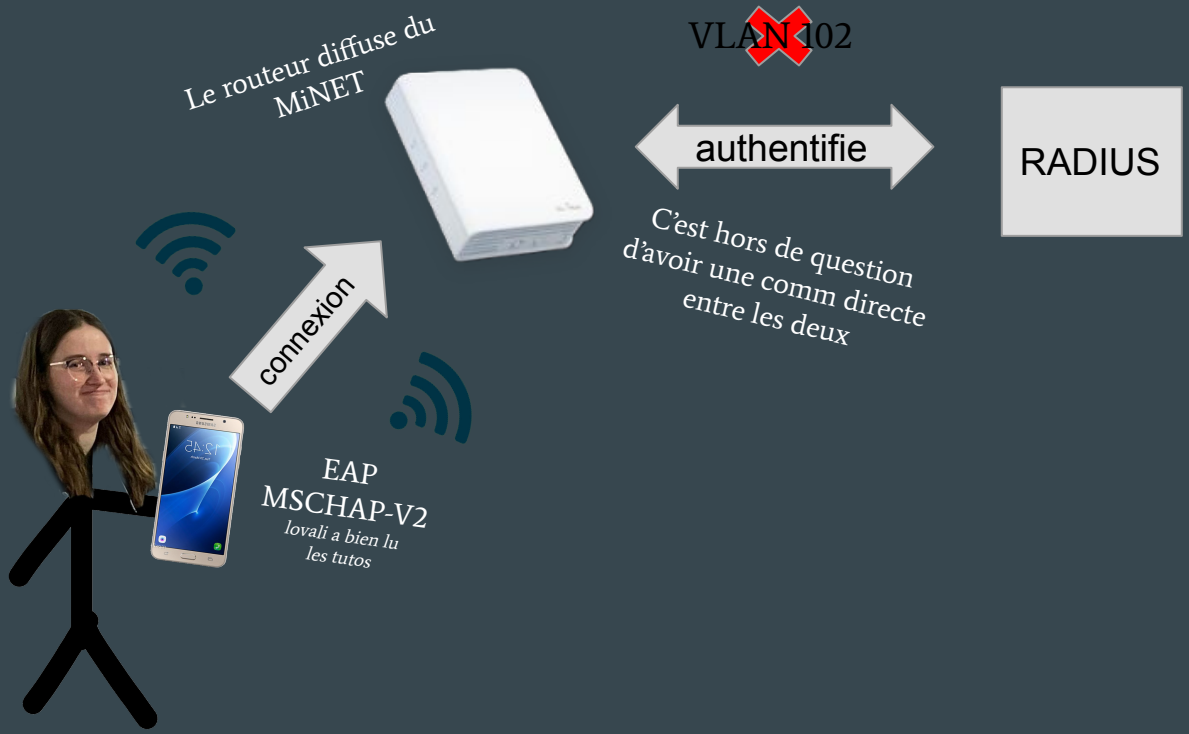
Avec qui les mini-routeurs doivent dialoguer ?

- Rézowifix est le usual suspect :
  - Il a une patte dans le 102, il peut joindre radius.
  - Il a une patte dans le 35, il peut joindre kea.
  - Il gère déjà le NAT, donc on est vraiment dans le thème Wi-Fi.

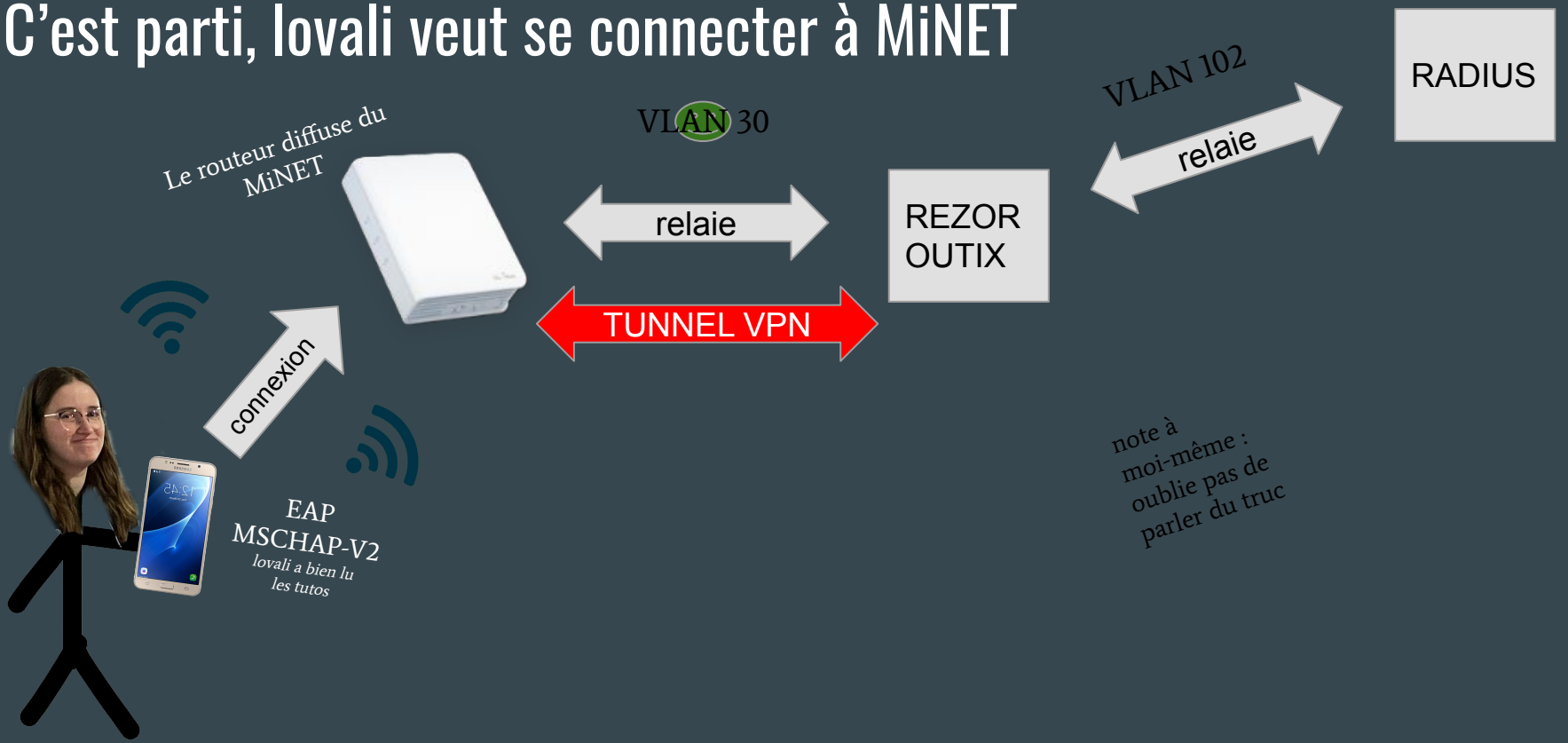
- Cependant :
  - C'est quand même mieux de séparer le trafic des mini-routeurs de celui des adhérents.

- **Solution : création de Rézoroutix.**

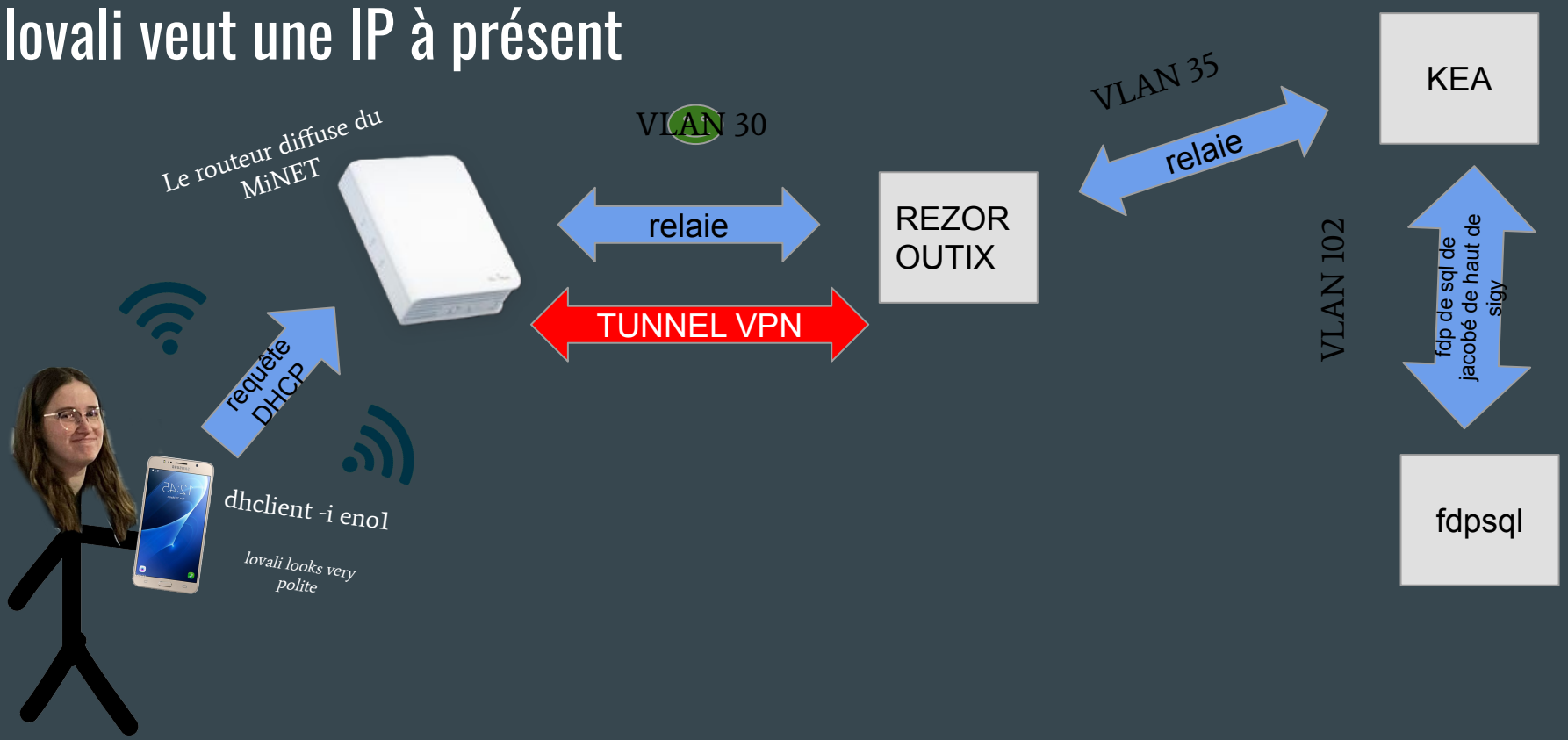
C’est parti, lovali veut se connecter à MiNET



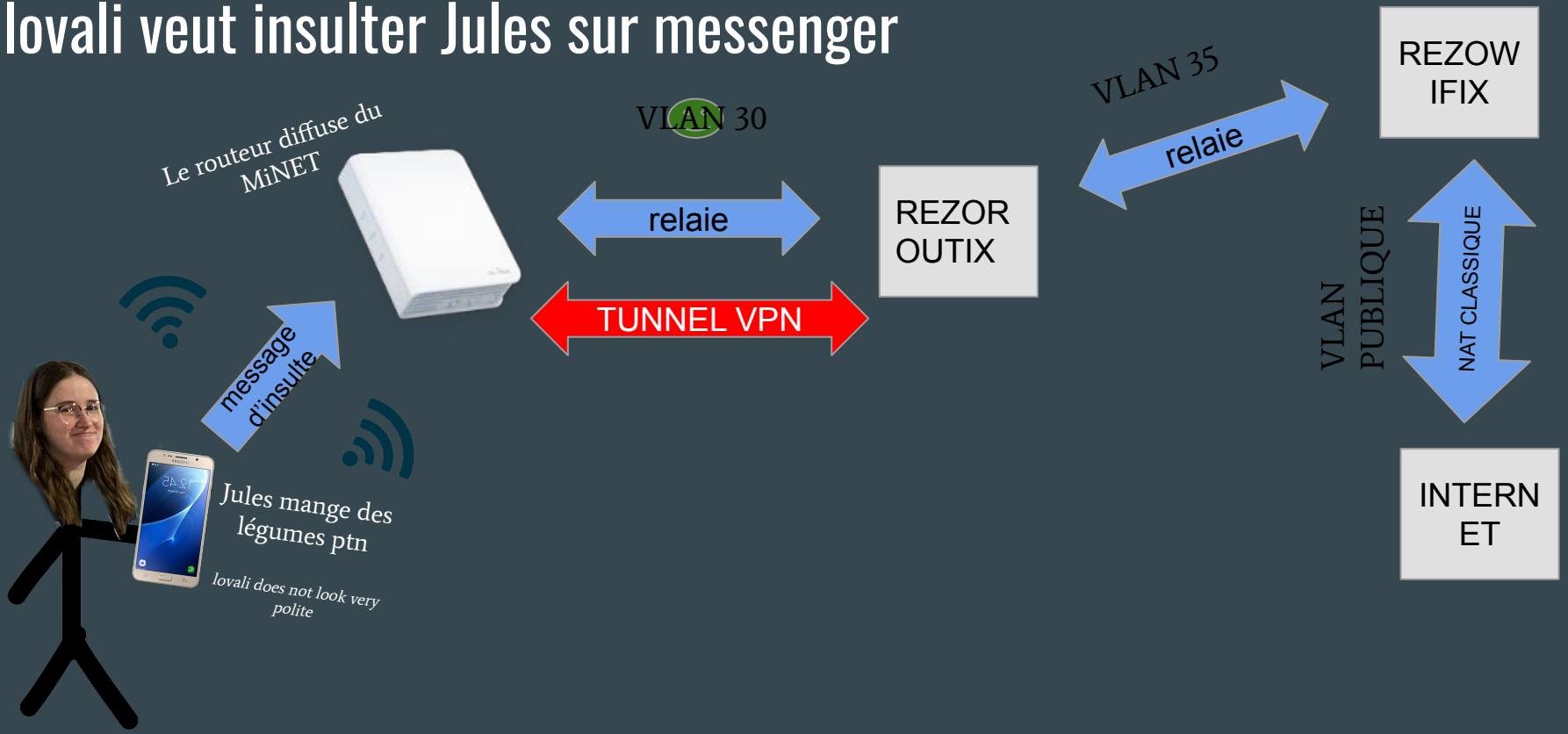
C’est parti, lovali veut se connecter à MiNET



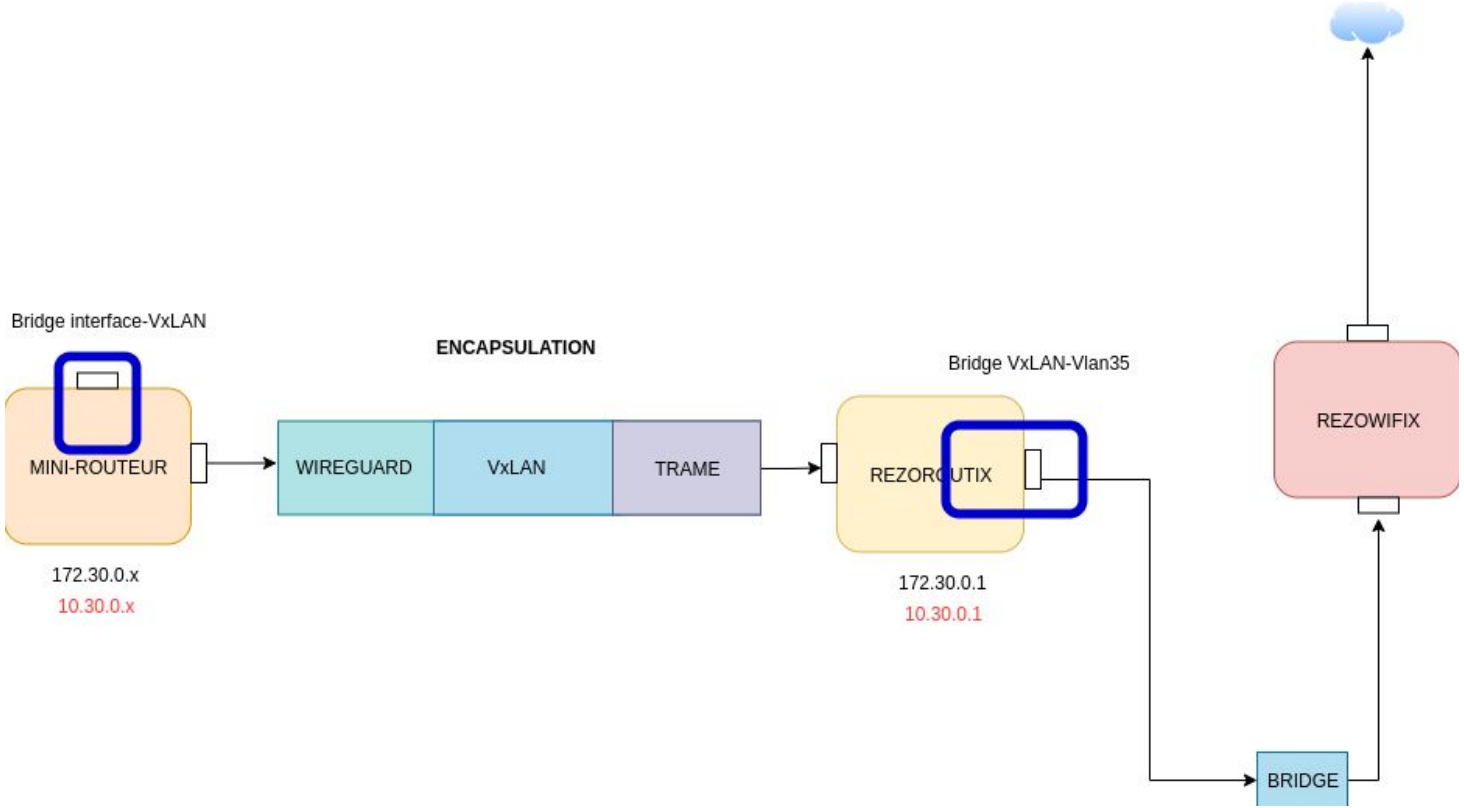
lovali veut une IP à présent



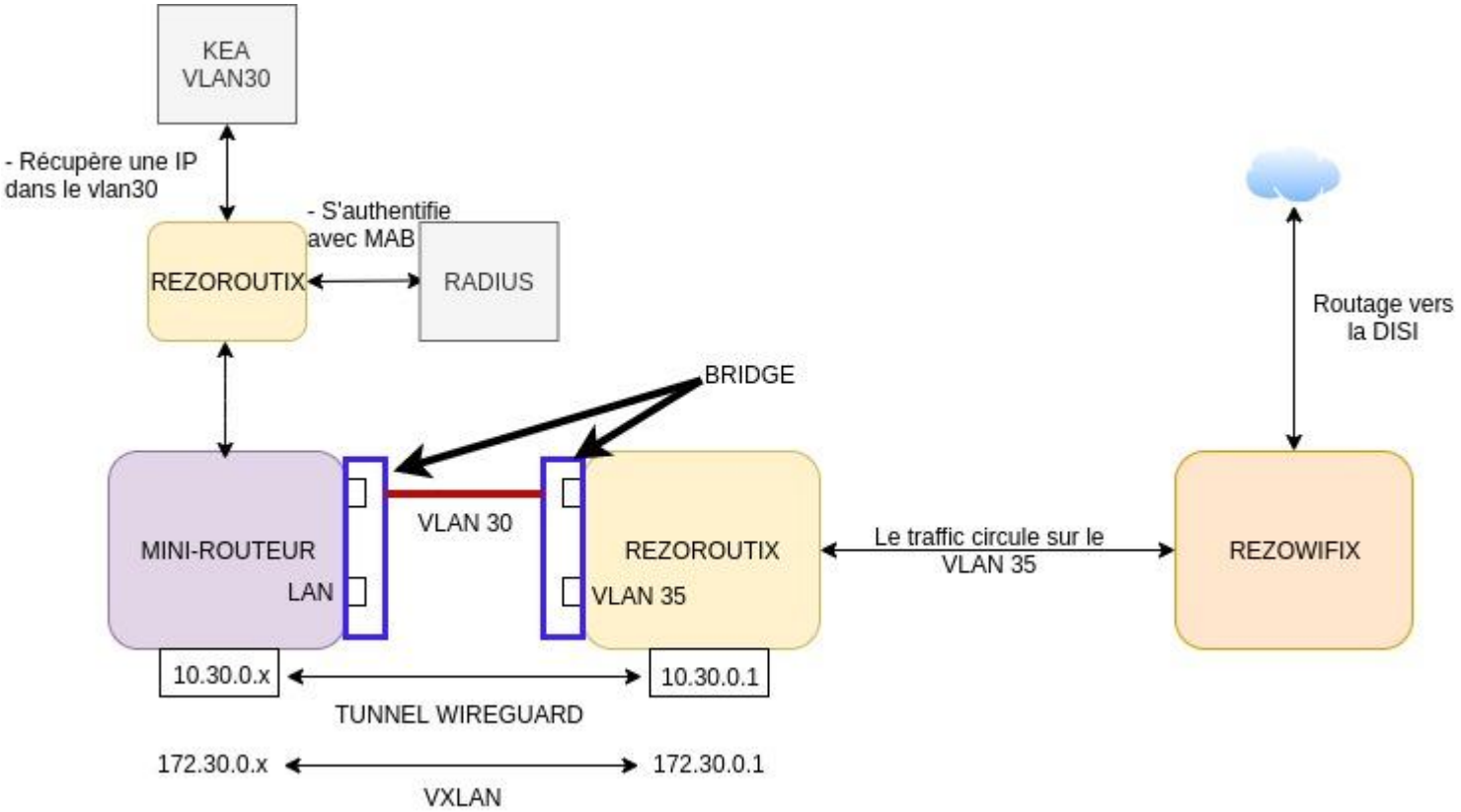
lovali veut insulter Jules sur messenger



Récapitulatif - small picture



Récapitulatif - big picture



Automatisation des mini-routeurs

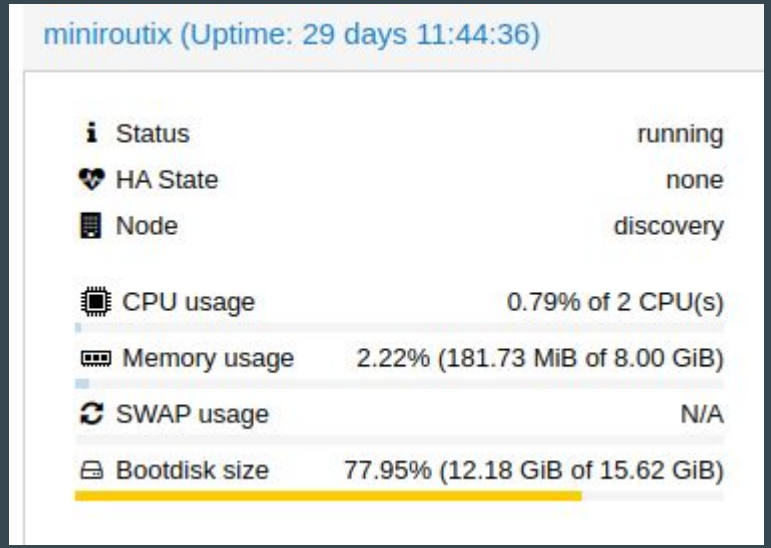
Vous pensiez que le plus dur était passé ?

On est pas au bout de nos peines.

- On a géré la partie réseau.
- Maintenant, les mini-routeurs à proprement parler.
  - Comment on les configure ?
  - Comment on les gère ?
  - Comment on keep track of them yeah english you know

Tu racontes ta vie, on fait comment concrètement ?

Première étape : créer un environnement de développement.



Voilà pourquoi y aura pas de TP

Seconde étape : choisir les paquets que l'on veut télécharger.

```
#
# Automatically generated file; DO NOT EDIT.
# OpenWrt Configuration
#
CONFIG_MODULES=y
CONFIG_HAVE_DOT_CONFIG=y
# CONFIG_TARGET_sunxi is not set
# CONFIG_TARGET_apm821xx is not set
# CONFIG_TARGET_ath25 is not set
CONFIG_TARGET_ar71xx=y
# CONFIG_TARGET_ath79 is not set
# CONFIG_TARGET_brcm2708 is not set
```

```
# CONFIG_PACKAGE_kmod-veth is not set
CONFIG_PACKAGE_kmod-vxlan=y
CONFIG_PACKAGE_kmod-wireguard=y
```

Les deux packages qui changent tout

Tu racontes ta vie, on fait comment concrètement ?

Troisième étape : insérer des configurations manuellement.

```
config wifi-iface
        option device 'radio0'
        option mode 'ap'
        option isolate '1'
        option encryption 'wpa2'
        option auth_secret 'bonjourjesuisleminirouteur'
        option auth_server '10.30.0.2'
        option network 'wlan'
        option ieee80211r '1'
        option mobility_domain 'e8aa'
        option ft_over_ds '1'
        option ft_psk_generate_local '1'
        option ssid 'MiNET_test'
```

```
config interface 'wg0'
        option proto 'wireguard'
        option private_key 'IKbdF6qQ87qfginrOCJSkMkTHj
        option mtu '1500'
        option ipaddr '10.30.0.11'
        option netmask '10.30.0.0/16'
```

Quatrième étape : y a plus qu'à !

make le firmware, et on est bon

Il est l'heure de la réflexion

- Projet plus **DENSE** que ce ratio.
- A vocation à être manipulé par des potits 1A.
- A vocation à être manipulé par n'importe qui en fait.
- Test grandeur nature peu concluant/insuffisant

Tu es : **vieux MiNET**
-> c'est tellement trivial que je ne vais pas faire de docu t'as cru quoi mdr.

Tu es : **visionnaire**
-> on va écrire de la docu, et il faut que le système soit le plus facile à utiliser.

Je déconne mais imagine quand même

Ça vous rappelle un truc les 2A ?

Ce qu'on doit pouvoir faire

Avoir un système clic-clic.

- Avantage : compréhensible
- Inconvénient : qui veut être mon cobaye ?

Faire des màj à distance

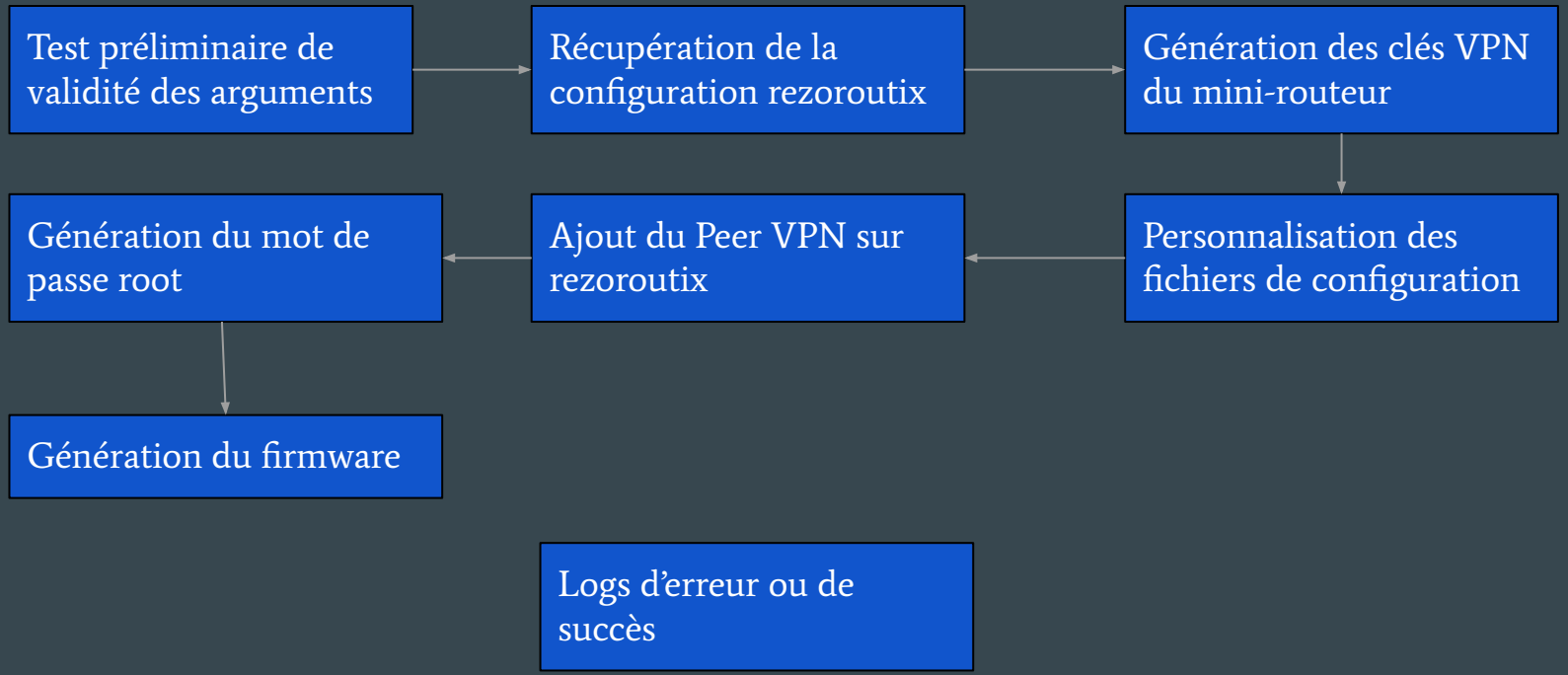
- Avantage : tu veux vraiment màj 100 MR à la main ?
- Inconvénient : faut pas se louper, et faut prévenir

Générer des firmwares.

- Avantage : utilisé
- Inconvénient : comme dit plus haut.

Ce que j'ai fait : automatiser la génération du firmware

- Script en Bash !



Ce que je fais : mettre à jour à distance.

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum.

http://192.168.102.118:8080 cependant, c'est moche mais oklm

Ce qu'il faudra faire : aller se faire foutre

- Injecter la config du port automatiquement chez l'adhérent qui demande un mini-routeur
- Ne pas se suicider
- La documentation (nuit du wiki, petit date au local hein vaktas et seberus ?)
- Ce qui a été dit précédemment
- Changer la gamme de routeurs utilisés


je sui a laeropor bisouuuu je manvol

Brouillon des trucs à caser

- Routeur, réseau privé vs notre solution
- OpenWRT
- Miniroutix lol xptdr
  - Hm je sèche
- TP ?
  - Je pense qu'une génération de firmware, c'est mort parce que ça prend bcp bcp bcp trop de taille
  - Leur préparer un firmware, et qu'ils le bidouillent un peu ?
  - Ils peuvent flasher une image ça peut-être marrant