RouterOS
en solution VPN

Philippe ROBERT

ENGITECH
SOLUTIONS INFORMATIQUES

Orateur

Philippe ROBERT – p.robert@engitech.ch

MCTNA . MTCRE . MTCTCE . MTCUME . MTCWE . MTCINE
certifié comme formateur MikroTik depuis 2013

(Microsoft – VMware – Citrix certifications)

ENGITECH S.A. , Genève – Suisse

consulting, formation et distribution des produits MikroTik,

gestion serveurs, datacenter, réseau wifi, voip ….

Projets

- Support infra réseau:

  ISP – WISP – VPN

- Installations:

  WIFI – VPN …

- LTE

VPN ?

2 principaux types:

Site à Site: GRE – IPIP – EOIP

PPP: PPTP – L2TP – OPENVPN – SSTP – PPPoE

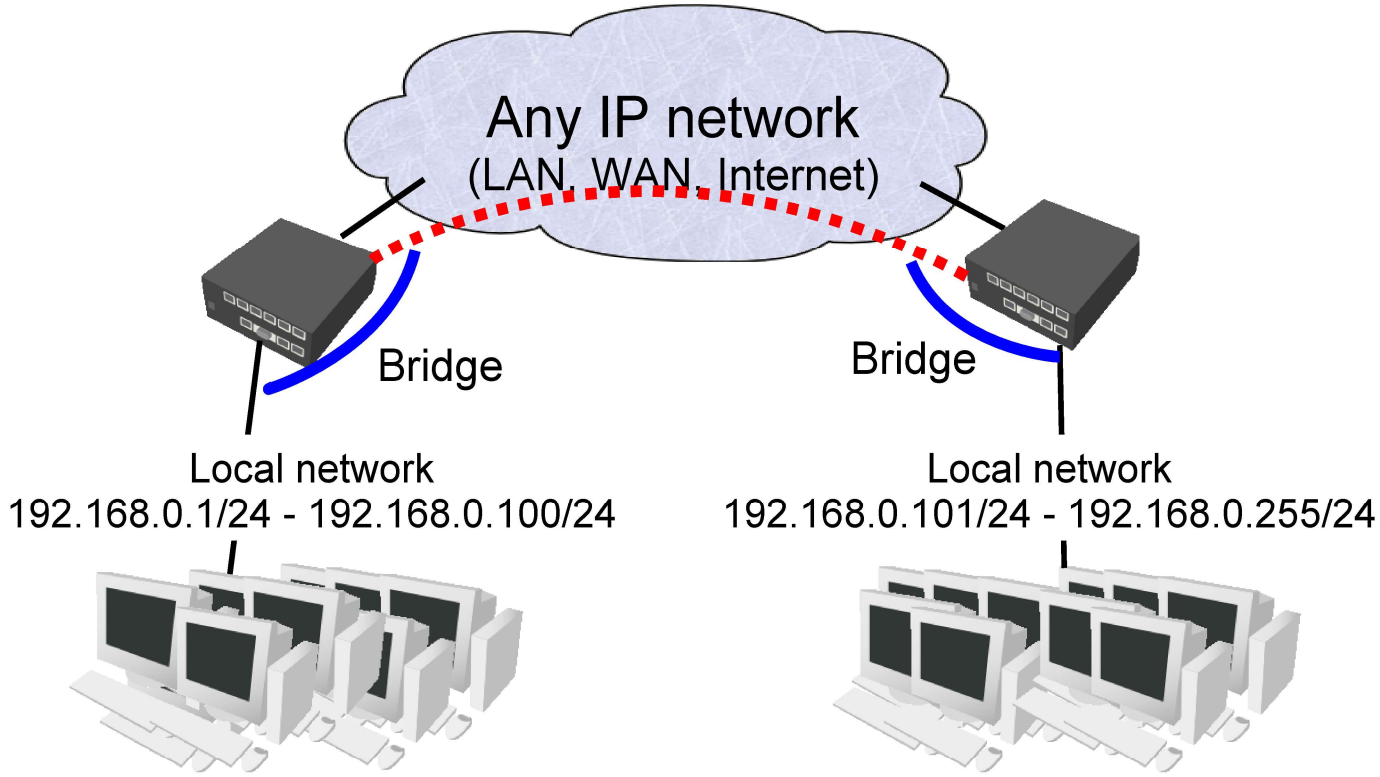
Sans oublier: MPLS , VPLS , IPSEC , CAPSMAN ….

RouterOS a vraiment de multiples possibilités

EOIP

Implémentation Propriétaire de MikroTik

Contrairement à GRE peut être mis en Bridge



EOIP

Fiable et performant, existe aussi en IPv6

IPv6 est disponible aussi pour GRE et IPIP

Et la sécurité ?

-> IPSEC

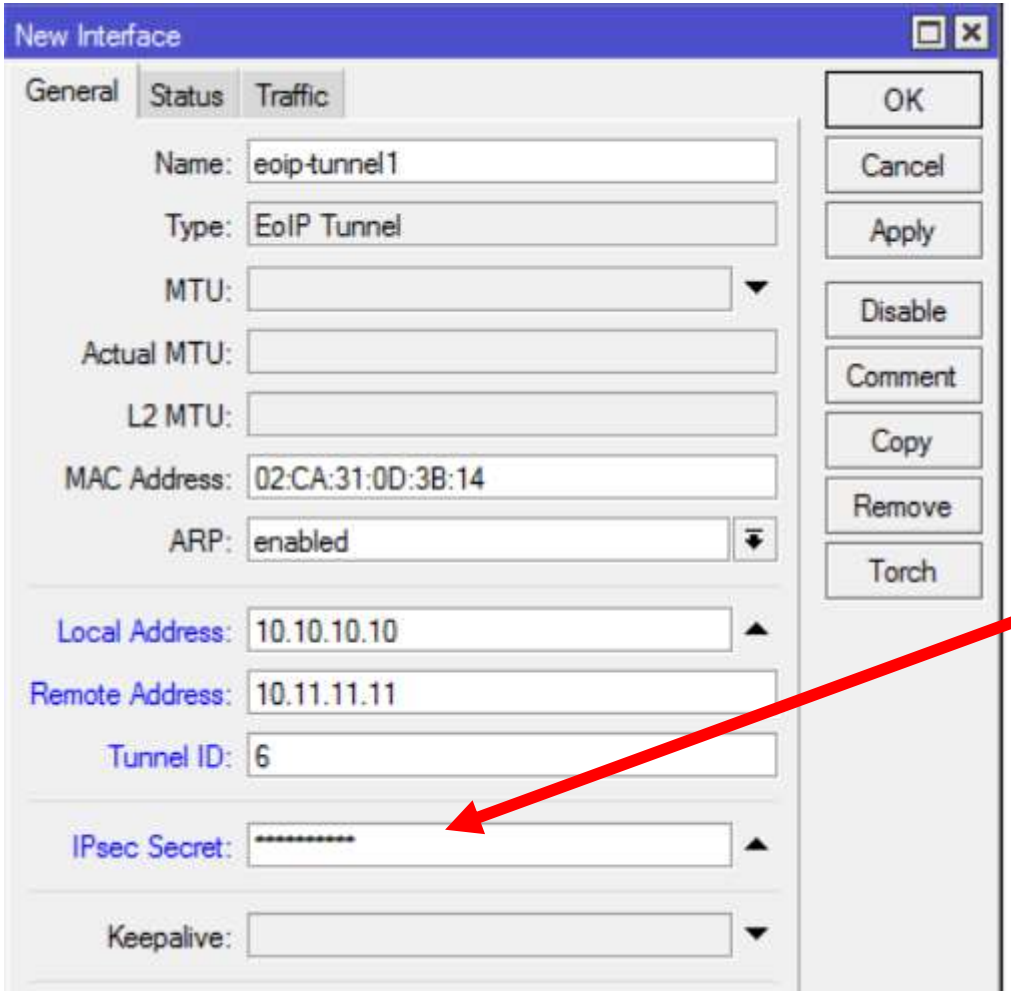
IPSEC

Depuis la version 6.30
-> entrez la clef partagée - 1 clic et IPSEC est activé

Liaison chiffrée IPSEC en moins de 2min.
RouterOS créé dynamiquement les règles IPSEC

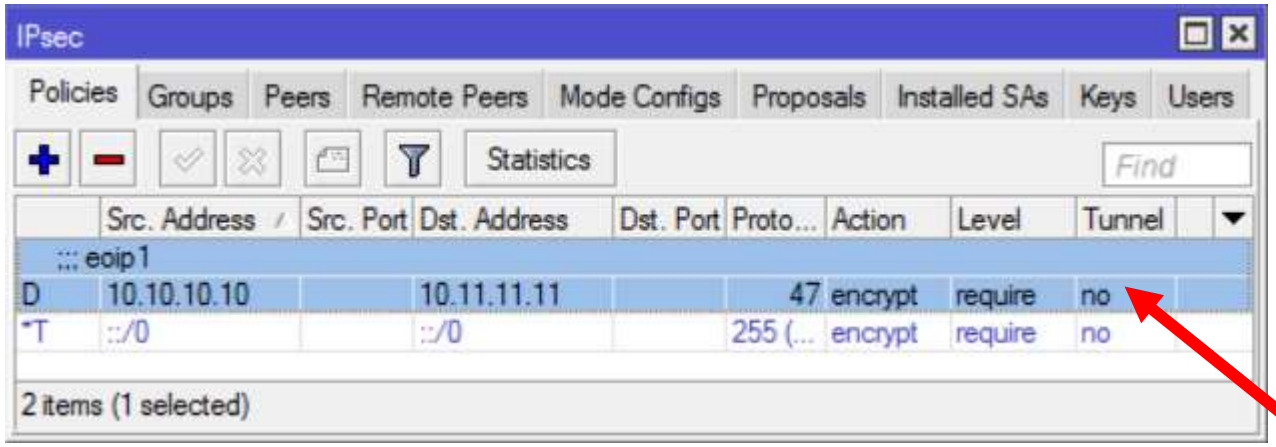
Difficile de faire plus facile ☺

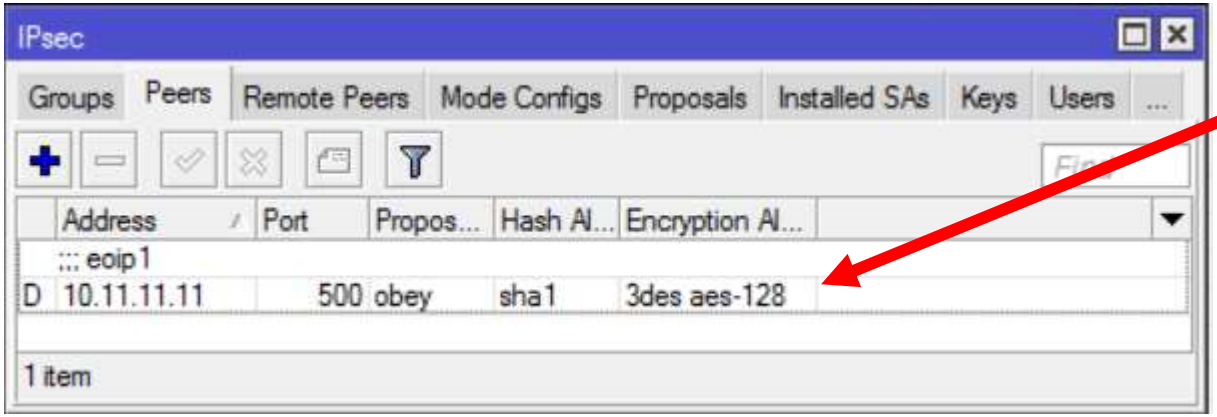
IPSEC - CONFIG



Clef partagée

IPSEC – Règles dynamiques





Créé par simple
Ajout de la clef
IPSEC

IPSEC pour tous

Identique pour:

EOIP

GRE

IPIP

Et aussi leurs versions IPv6

ainsi que pour L2TP / IPSEC

IPSEC - Performance

RB2011= 20mb/s

CCR1036 = 1500mb/s (mtu 1500)

<u>Chiffrement Matériel:</u>

RB1100AHX2

RB850GX2

Tous les CCR…

En v7: RB3011

PPP

PPtP: à utiliser uniquement pour sa compatibilité

SSTP: pratique pour la connection des clients Windows

L2TP: la seule implémentation actuelle de MikroTik sur UDP

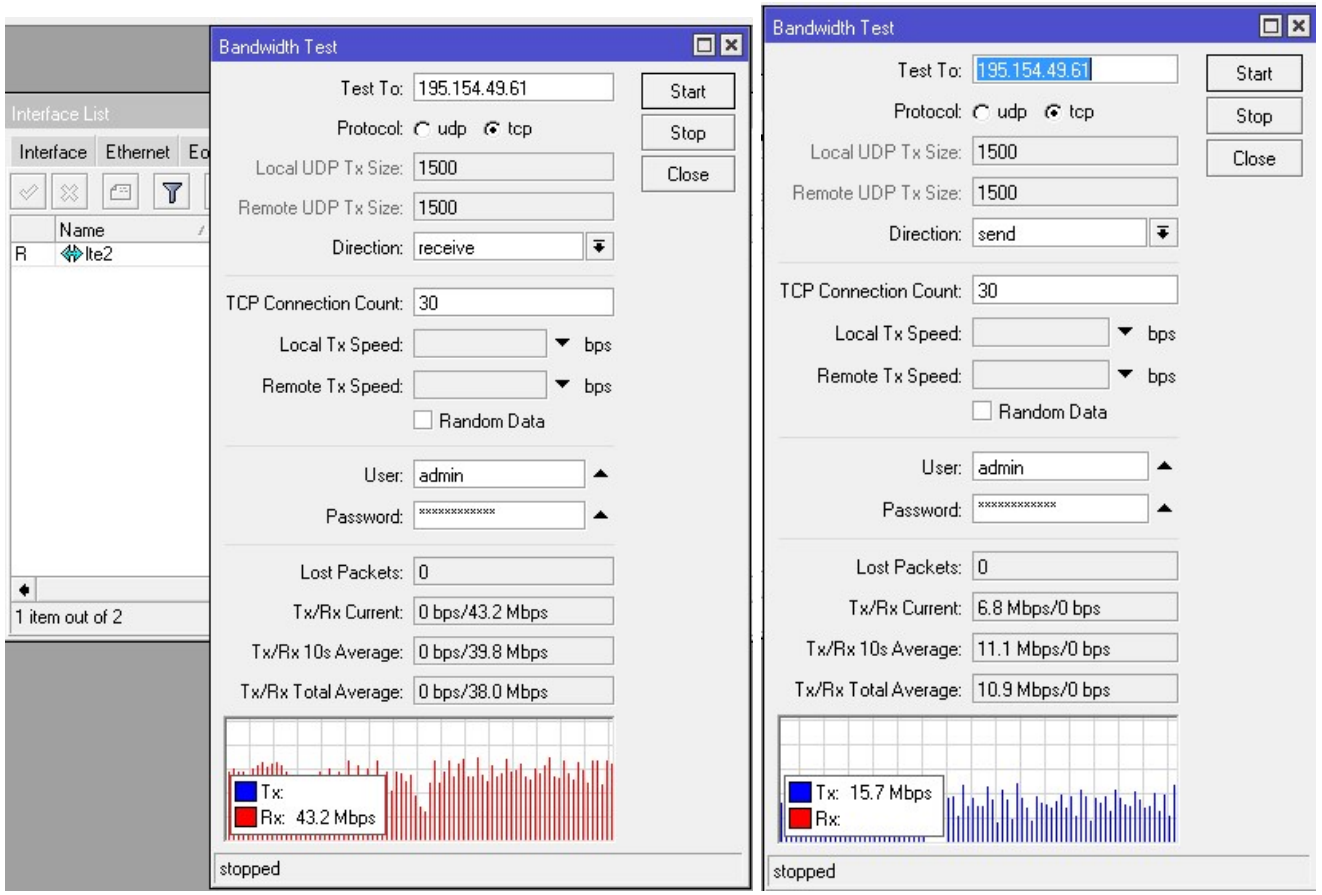
OpenVPN: sécure et fiable, actuellement en TCP
–> v7 proposera l'UDP ☺

LTE

Wireless Antenna
LTE antenna

60mbs down
30mbps up

Remplacement
de ligne ADSL

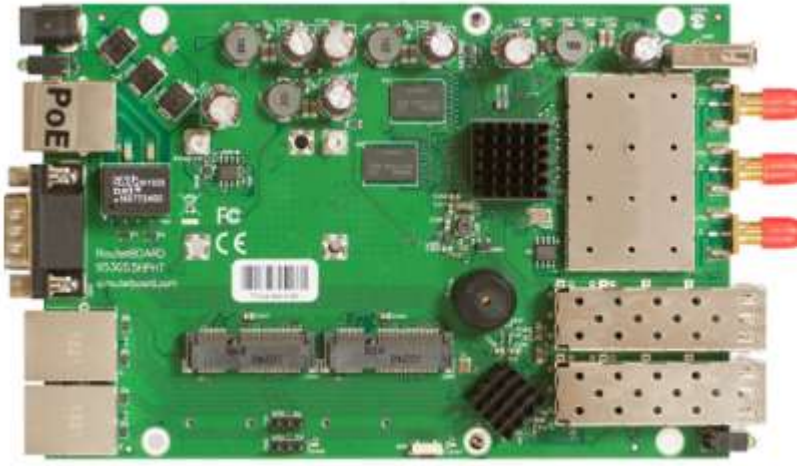


LTE

Utilisation de **L2TP** pour connexion à point central à haute vitesse:

- Fournir des services (adresse IP public)
- Limité effet de QOS du service provider

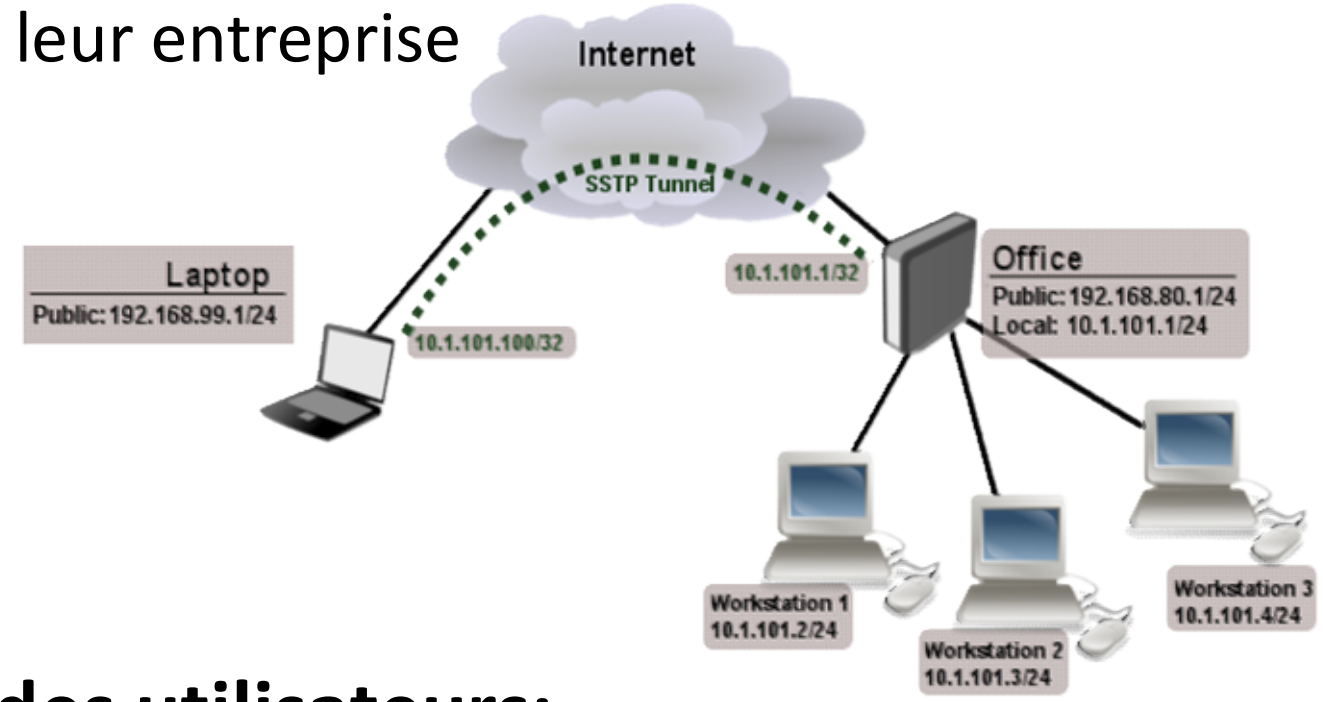
Utilisation de RB953G
Puissance CPU et connectivité -



<u>Modem LTE:</u>
HUAWEI 909S
WIRELESS INSTRUMENTS D15G2

PPP – Vpn clients

La majorité des installations réalisées servent à connecter des utilisateurs distants à l'infrastructure réseau de leur entreprise



Gestion des utilisateurs:

PPP Secrets -> propre à chaque routeur …

RADIUS

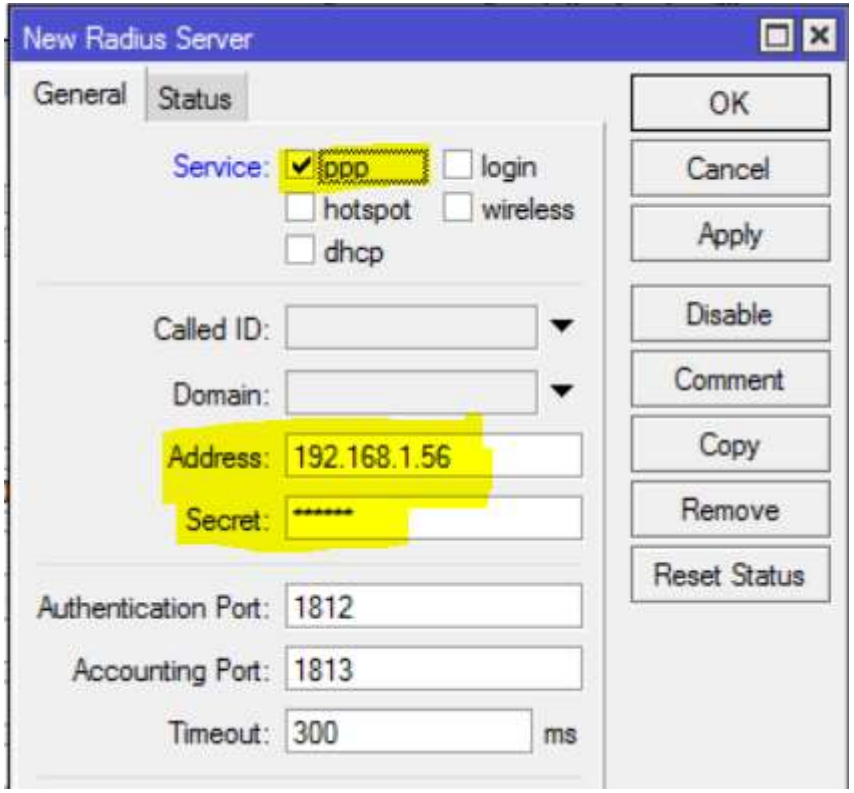
Authentification centralisée, redondance et liaison avec d'autres bases utilisateurs (ex.: Active Directory)

Notamment: FreeRADIUS, TekRADIUS, …

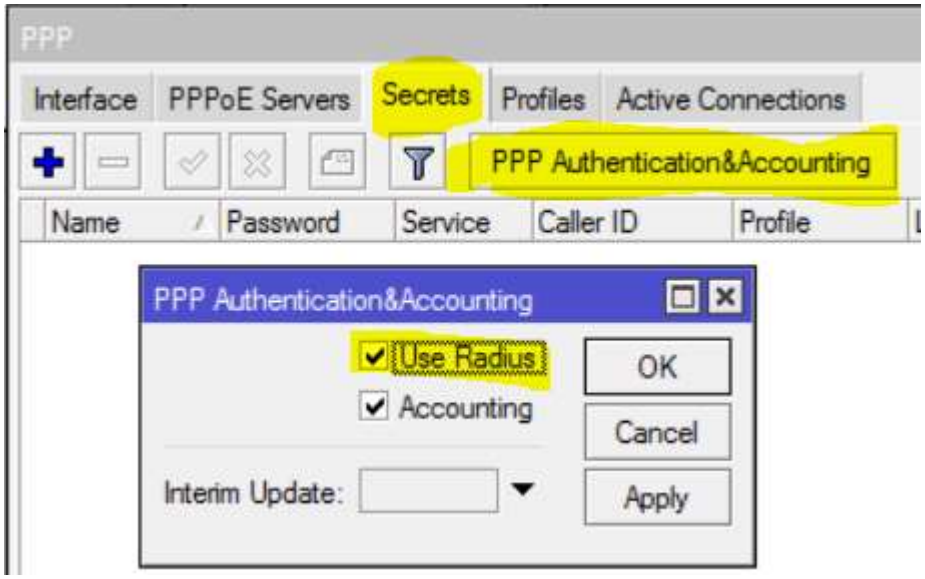
RADIUS CONFIG

2 étapes:

Ajouter serveur radius



Configurer PPP pour l'utilisation du radius



Authentification…

La majorité des solutions PPP
s'appuient sur une combinaison
Utilisateur / Mot de passe

Une combinaison unique … et toujours identique

Le rêve des ***keylogger***.

Keylogger – logiciel ou matériel

Malware mais aussi espions matériels peuvent exister

Keylogger sans fil…

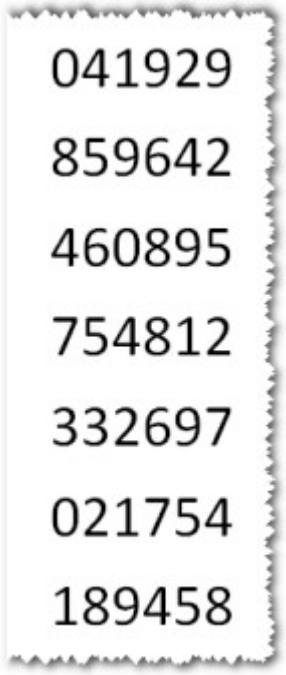
Clavier automatique caché dans une clé USB …

Sécurité

Authentification à 2 facteurs

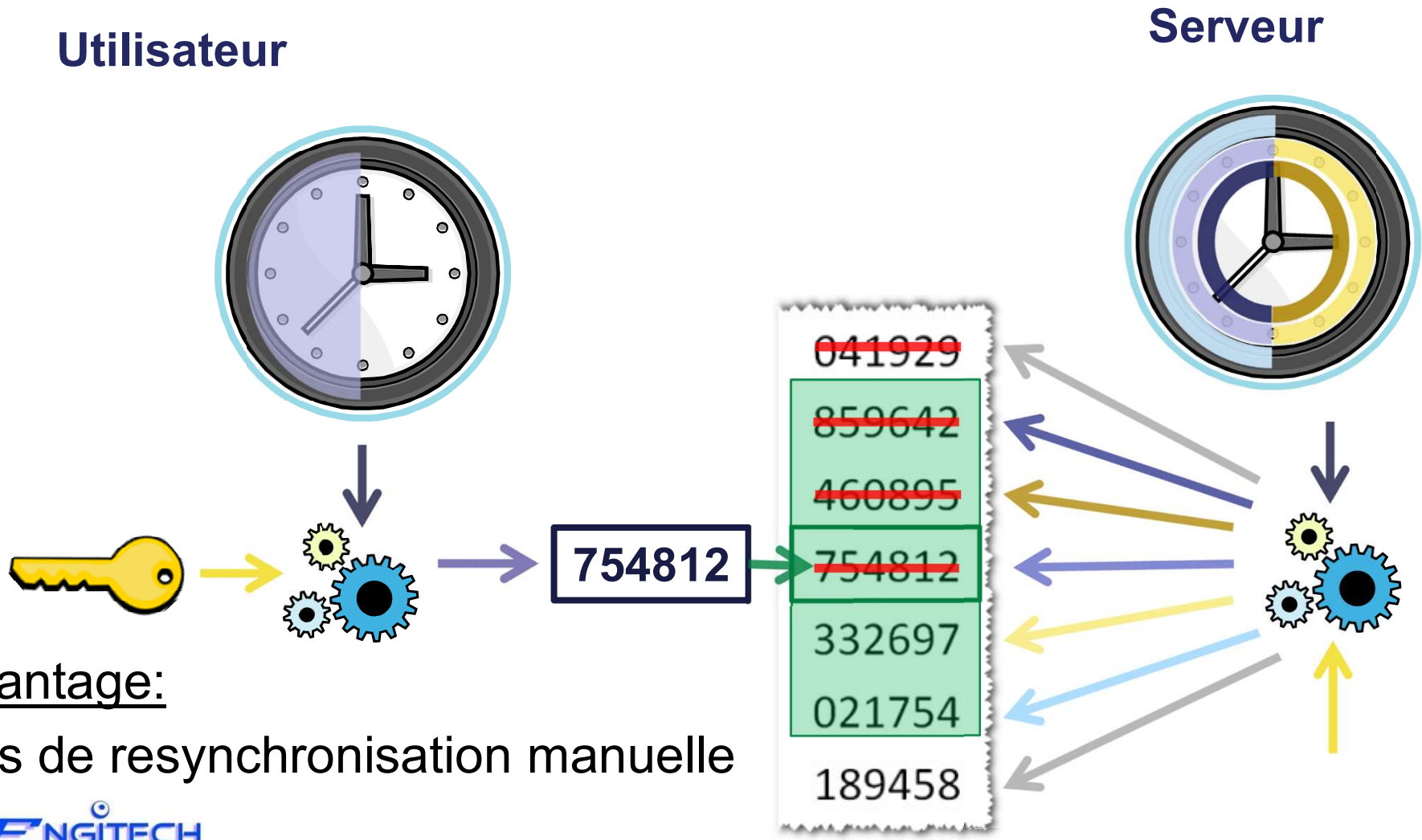
Plusieurs exemples:

- Liste à biffer



TOTP

L'algorithme change le mot de passe toutes les 30s



avantage:

pas de resynchronisation manuelle

SecurID

Parade?

Solutions propriétaires

OU

difficiles à implémenter

Réellement sécure ?

SecurID

NSA BACKDOOR

https://en.wikipedia.org/wiki/RSA_Security#Relationship_with_NSA

Solution ?

Je rêve d'une ~~banque~~ solution qui soit:

- Sécure …. réellement
- Facile à mettre en place
- D'un coût abordable
- Sans OGM ... Sans NSA
- Et pourquoi pas une solution OpenSource ? …

Rêve … Réalité!

Partie serveur:

<< **multi*OTP*** >> www.multiotp.net

Solution OpenSource qui s'interface avec FreeRADIUS et TekRADIUS pour une authentification à 2 facteurs

Partie cliente:

Chaque Smartphone inclus un client TOTP

Android: FreeOTP ; Windows: Authenticator …

multi*OTP*

Certifié OATH:

une authentification forte universelle

https://openauthentication.org/oath-certified-products/

Interopérabilité des produits

- Token matériel, logiciel multiplateforme

SysCo®

Installation multi*OTP*

Configuration minime si vous utilisez déjà FreeRADIUS ou TekRADIUS

<u>Et si ce n'est pas le cas:</u>

- Images **VMware** ou pour **Raspberry PI** disponible!
  déjà préconfigurées avec une interface web dédiée

En quelques minutes seulement vous avez amélioré la sécurité de vos accès distants

Exemple FreeRADIUS

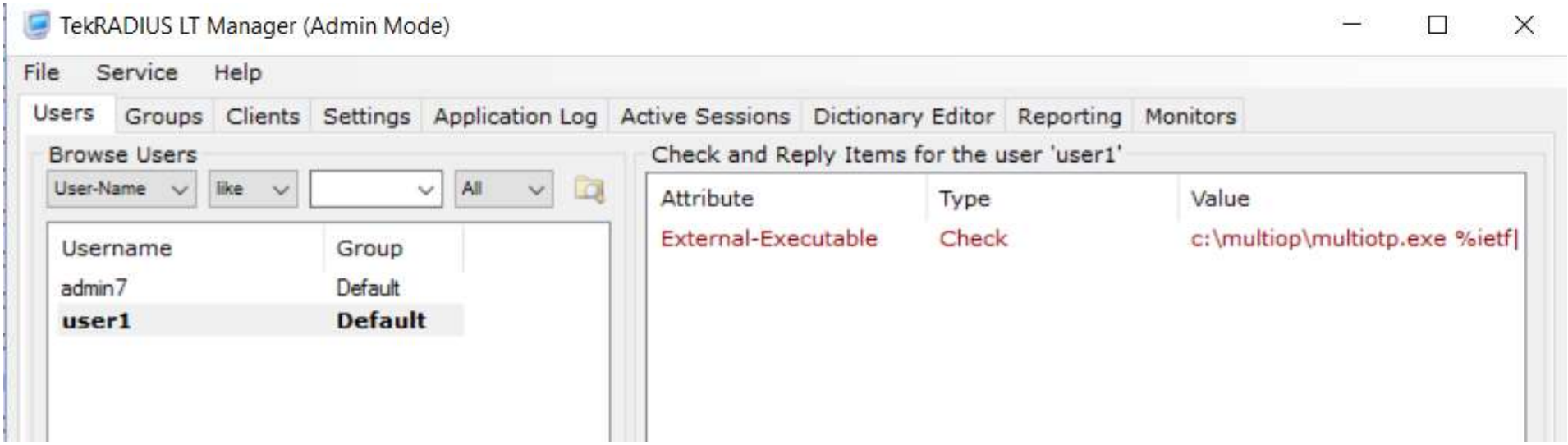
http://wiki.freeradius.org/guide/multiOTP-HOWTO

```
# Exec module instance for multiOTP
# Replace '/path/to' with the actual path to the multiotp.php file
exec multiotp {
        wait = yes
        input_pairs = request
        output_pairs = reply
        program = "/path/to/multiotp.php %{User-Name} %{User-Password} -request-nt-key -src=%{Packet-Src-IP-Address} -chap-challenge=%{CHAP-Challenge} -chap-password=%{CHAP-Password} -ms-chap-challenge=%{MS-CHAP-Challenge} -ms-chap-response=%{MS-CHAP-Response} -ms-chap2-response=%{MS-CHAP2-Response}"
        shell_escape = yes
}
```

Exemple TekRADIUS

Dans le monde windows, multiOTP est fourni sous la forme d'un executable: «multiotp.exe»

Utilisation dans des scripts sans aucun soucis

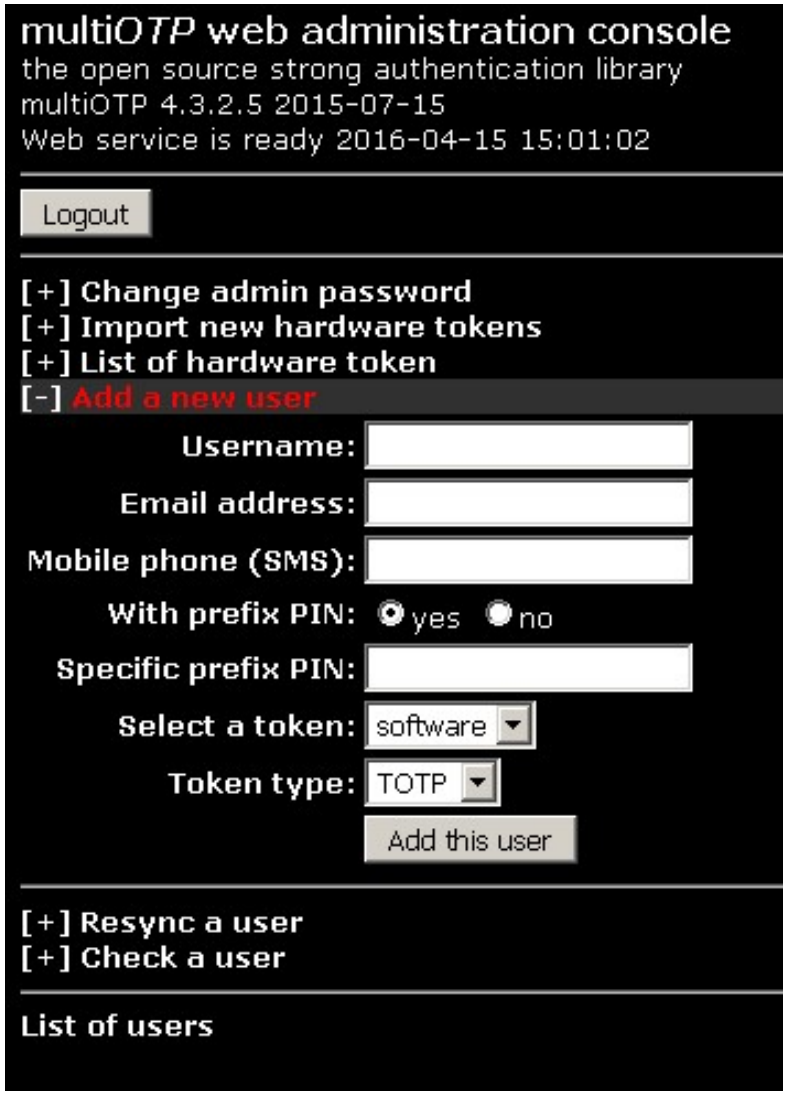


Interface multi*OTP*

Page web création utilisateur:

Génération du QR code

pour client Smartphone:



Démo

Création d’un utilisateur et connection vpn SSTP

Coût Licences

Les licences P1 (45$) – P10 (95$) – PU (250$) n'ont pas de limitation sur le nombre de connection VPN

Level	**0**	**1**	**3**	**4 (45$)**	**5 (95$)**	**6 (250$)**
EoIP - GRE	24h	1	illimité	illimité	illimité	illimité
PPPoE	24h	1	200	200	500	illimité
PPTP – SSTP L2TP	24h	1	200	200	500	illimité
OVPN	24h	1	200	200	illimité	illimité

Conclusion

- **MikroTik** a réalisé une configuration aisée du chiffrement **IPSEC** pour de nombreux protocoles
- Grâce à ses multiples possibilités, répond aux différents besoins
- **RouterOS** lié à un serveur **RADIUS** permet une gestion centralisée et redondante des utilisateurs distants
- En ajoutant **multi*OTP*** à cette configuration, on obtient un ensemble fiable, sécure, facile à mettre en place et à un coût défiant toute concurrence

Philippe ROBERT - p.robert@engitech.ch