



RouterOS en solution VPN

Philippe ROBERT

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

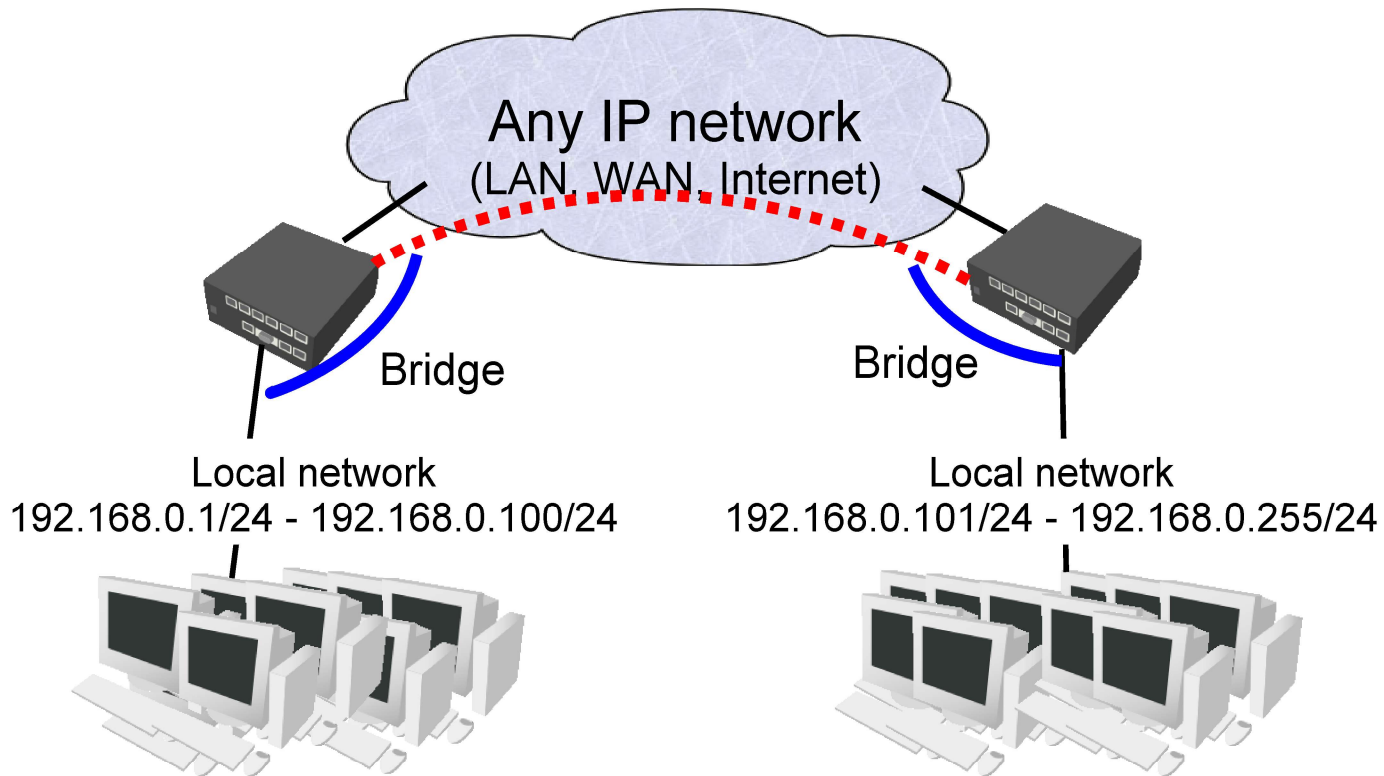
PPP: PPTP – L2TP – OPENVPN – SSTP – PPPoE

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 crée dynamiquement les règles IPSEC

Difficile de faire plus facile 😊

IPSEC - CONFIG

New Interface

General Status Traffic

Name: eoip-tunnel1

Type: EoIP Tunnel

MTU: [dropdown]

Actual MTU: [text]

L2 MTU: [text]

MAC Address: 02:CA:31:0D:3B:14

ARP: enabled

Local Address: 10.10.10.10

Remote Address: 10.11.11.11

Tunnel ID: 6

IPsec Secret: [masked]

Keepalive: [dropdown]

OK

Cancel

Apply

Disable

Comment

Copy

Remove

Torch

Clef partagée

IPSEC – Règles dynamiques

	Src. Address	Src. Port	Dst. Address	Dst. Port	Proto...	Action	Level	Tunnel
...	eosp 1							
D	10.10.10.10		10.11.11.11		47	encrypt	require	no
T	::/0		::/0		255 (...)	encrypt	require	no

2 items (1 selected)

Créé par simple
Ajout de la clef
IPSEC

	Address	Port	Propos...	Hash Al...	Encryption Al...
...	eosp 1				
D	10.11.11.11	500	obey	sha1	3des aes-128

1 item

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)

Chiffrement Matériel:

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: sécurée et fiable, actuellement en TCP
→ v7 proposera l'UDP 😊



LTE

Wireless Antenna
LTE antenna

60mbs down
30mbs up

Remplacement
de ligne ADSL



The image displays two screenshots of a 'Bandwidth Test' application window. The left window shows a test configuration for the 'lte2' interface. The test is set to 'receive' direction, with a 'Test To' of 195.154.49.61, 'Local UDP Tx Size' of 1500, and 'Remote UDP Tx Size' of 1500. The 'TCP Connection Count' is 30. The results show 'Local Tx Speed' and 'Remote Tx Speed' as 0 bps, and 'Remote Rx Speed' as 43.2 Mbps. The right window shows a test configuration for the IP address 195.154.49.61. The test is set to 'send' direction, with the same 'Test To' and UDP sizes. The results show 'Local Tx Speed' and 'Remote Tx Speed' as 15.7 Mbps, and 'Remote Rx Speed' as 0 bps. Both windows include a graph at the bottom showing Tx (blue) and Rx (red) activity over time.

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 -

Modem LTE:

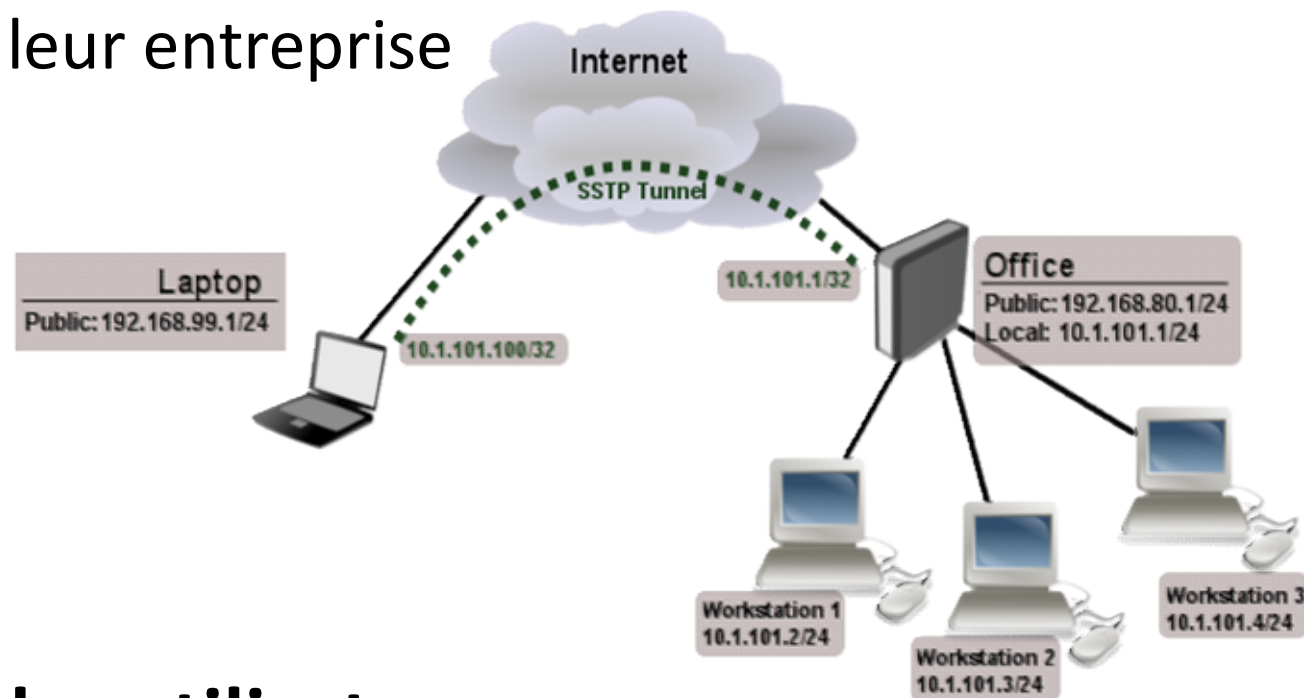
HUAWEI 909S

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

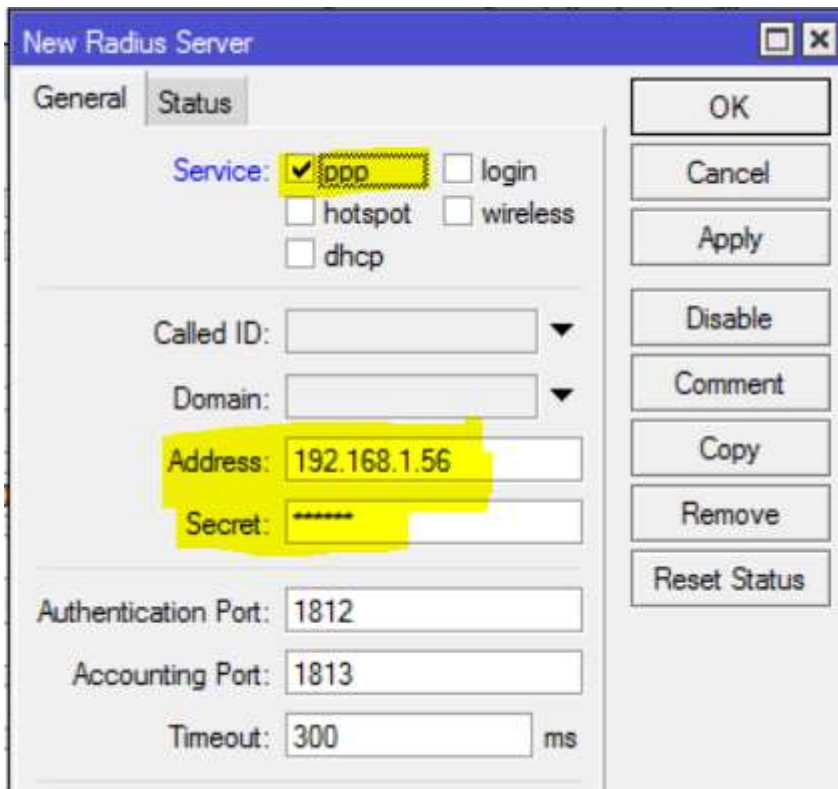
Authentification centralisée, redondance et liaison avec d'autres bases utilisateurs (ex.: Active Directory)

Notamment: FreeRADIUS, TekRADIUS, ...

RADIUS CONFIG

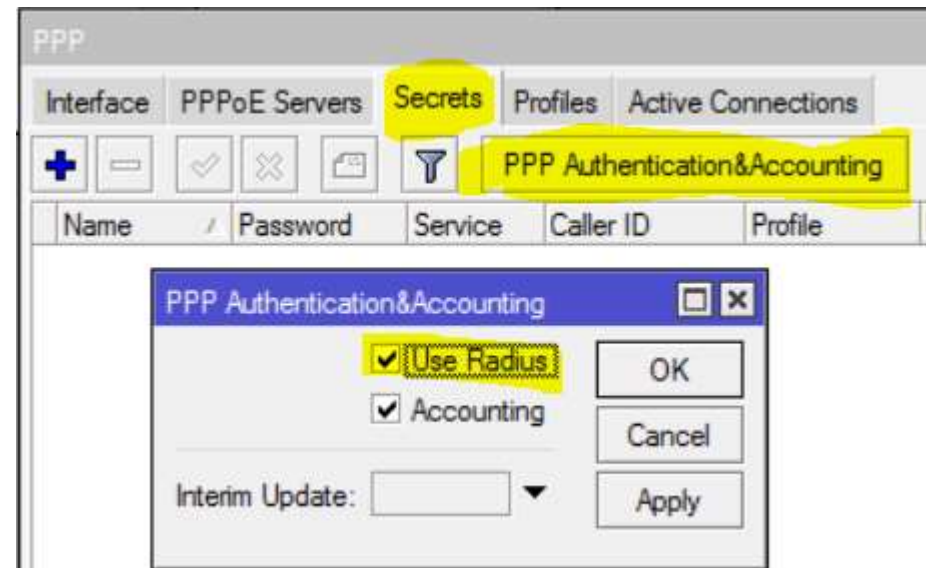
2 étapes:

Ajouter serveur radius



The 'New Radius Server' dialog box is shown with the 'General' tab selected. The 'Service' section has 'ppp' checked. The 'Address' field contains '192.168.1.56' and the 'Secret' field contains '*****'. The 'Authentication Port' is '1812', the 'Accounting Port' is '1813', and the 'Timeout' is '300 ms'. Buttons for 'OK', 'Cancel', 'Apply', 'Disable', 'Comment', 'Copy', 'Remove', and 'Reset Status' are visible on the right.

Configurer PPP pour l'utilisation du radius



The 'PPP' configuration window is shown with the 'Secrets' tab selected. A table lists 'PPP Authentication&Accounting' with a filter icon. A sub-dialog box 'PPP Authentication&Accounting' is open, showing 'Use Radius' and 'Accounting' checked. The 'Interim Update' field is empty. Buttons for 'OK', 'Cancel', and 'Apply' are visible.

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...

Wi Fi



Clavier automatique caché dans une clé USB ...



Sécurité

Authentification à 2 facteurs

Plusieurs exemples:

- Liste à biffer

041929

859642

460895

754812

332697

021754

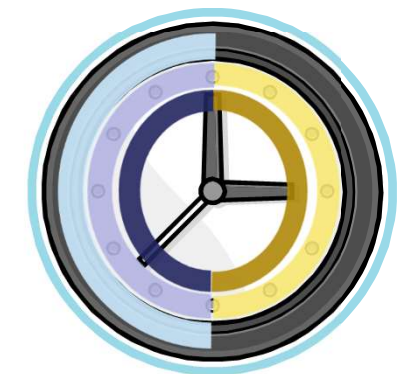
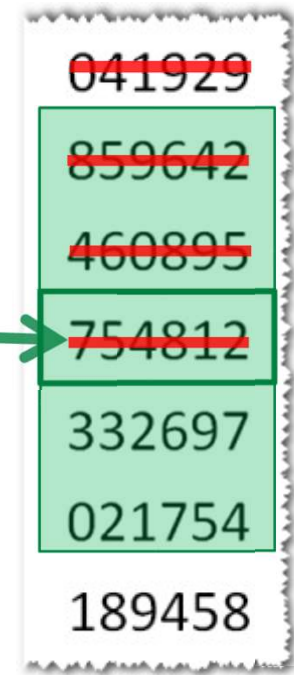
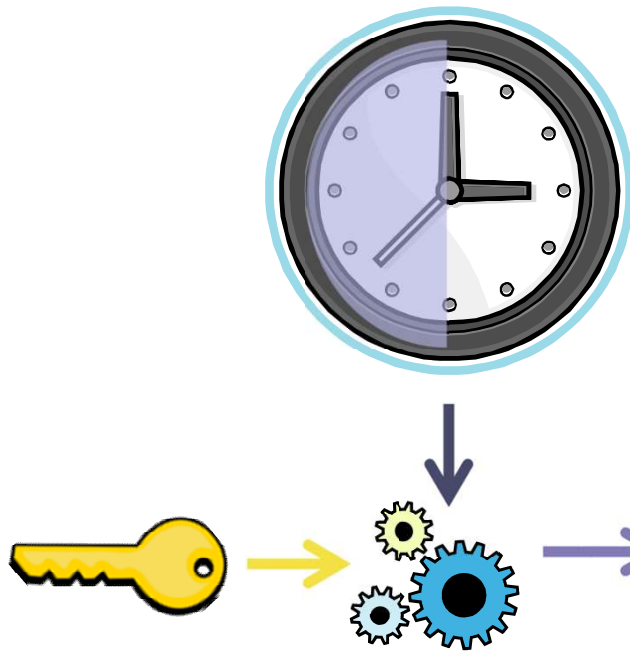
189458

TOTP

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

Utilisateur

Serveur



avantage:
pas de resynchronisation manuelle

Parade?

SecurID



Solutions propriétaires



OU

difficiles à implémenter



Réellement sécurée ?

SecurID

NSA BACKDOOR



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



Solution ?

Je rêve d'une banque solution qui soit:

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

Rêve ... Réalité!

Partie serveur:

<< **multiOTP** >> 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 ...

multiOTP

Certifié OATH:

une authentification forte universelle

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

Interopérabilité des produits

- Token matériel, logiciel multiplateforme

S y s C o®

Installation multiOTP

Configuration minime si vous utilisez déjà FreeRADIUS ou TekRADIUS

Et si ce n'est pas le cas:

- 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

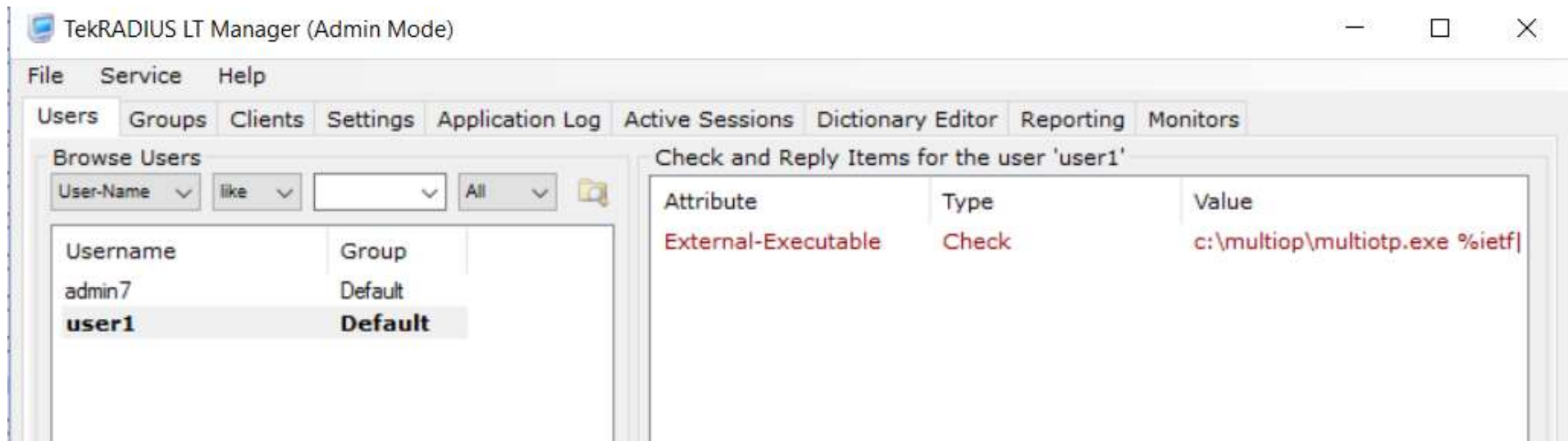
<http://wiki.freeradius.org/guide/multiOTP-HOWTO>

```
# 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



The screenshot shows the TekRADIUS LT Manager (Admin Mode) interface. The window title is "TekRADIUS LT Manager (Admin Mode)". The menu bar includes "File", "Service", and "Help". The main menu includes "Users", "Groups", "Clients", "Settings", "Application Log", "Active Sessions", "Dictionary Editor", "Reporting", and "Monitors".

The "Browse Users" section shows a search for "user1" with the following results:

Username	Group
admin7	Default
user1	Default

The "Check and Reply Items for the user 'user1'" section shows the following configuration:

Attribute	Type	Value
External-Executable	Check	c:\multiop\multiotp.exe %ietf

Interface multiOTP

Page web création utilisateur:

Génération du QR code
pour client Smartphone:



multiOTP web administration console
the open source strong authentication library
multiOTP 4.3.2.5 2015-07-15
Web service is ready 2016-04-15 15:01:02

Logout

[+] Change admin password
[+] Import new hardware tokens
[+] List of hardware token
[-] **Add a new user**

Username:

Email address:

Mobile phone (SMS):

With prefix PIN: yes no

Specific prefix PIN:

Select a token:

Token type:

Add this user

[+] Resync a user
[+] Check a user

List of users

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 connexion 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 **multiOTP** à cette configuration, on obtient un ensemble fiable, sécurisée, facile à mettre en place et à un coût défiant toute concurrence

Philippe ROBERT - p.robert@engitech.ch