

solutions ISG
Impartition de services et gestion

Building MSP infrastructure with Mikrotik

Presented by | Jonathan Grenier
Solutions ISG

About me

- Network consultant at Solutions ISG specialized in Mikrotik
- MikroTik certified trainer
- MTCNA
- MTCRE
- 20 Years experience in IT

About Solutions ISG

- Founded in 2007
- Managed service provider and consulting firm
- Based in Montréal serving clients worldwide
- 213 active clients (trailing 12 months)

Introduction

As a managed service provider (MSP) we had multiple challenges in order to offer better support to our customers. This lead us through a few small projects and after a couple years of development brought us to a complete solution for our needs.

The goal of this presentation is to give you a functional and technical overview of our solution so you can see all the potential and advantages that Mikrotik RouterOS and RouterBOARD have to offer.

Solution requirement overview

- Accessibility
  Provide a simple and standard method to access client infrastructure. We also wanted to give our team efficient ways to work and the ability to multi-task.

- Security
  Protect our network and also our clients network against external and internal security threats. Provide the ability to keep an audit trail of users activity.

- Low cost
  Market competition lead us to find the most cost efficient way to deliver a solution. It is very important to provide the customer with better return on investment.

Solution requirement (accessibility)

- Possibility to access multiple clients at the same time
- Avoid subnet conflict (ex. Two clients with 192.168.0.0/24)
- Access for central monitoring console
- Simple deployment

Solution requirement (security)

- Web based authentication (webauth)
- Centralized user control
- Encrypted communication between sites
- Rules set per user and/or group
- Restricted client access

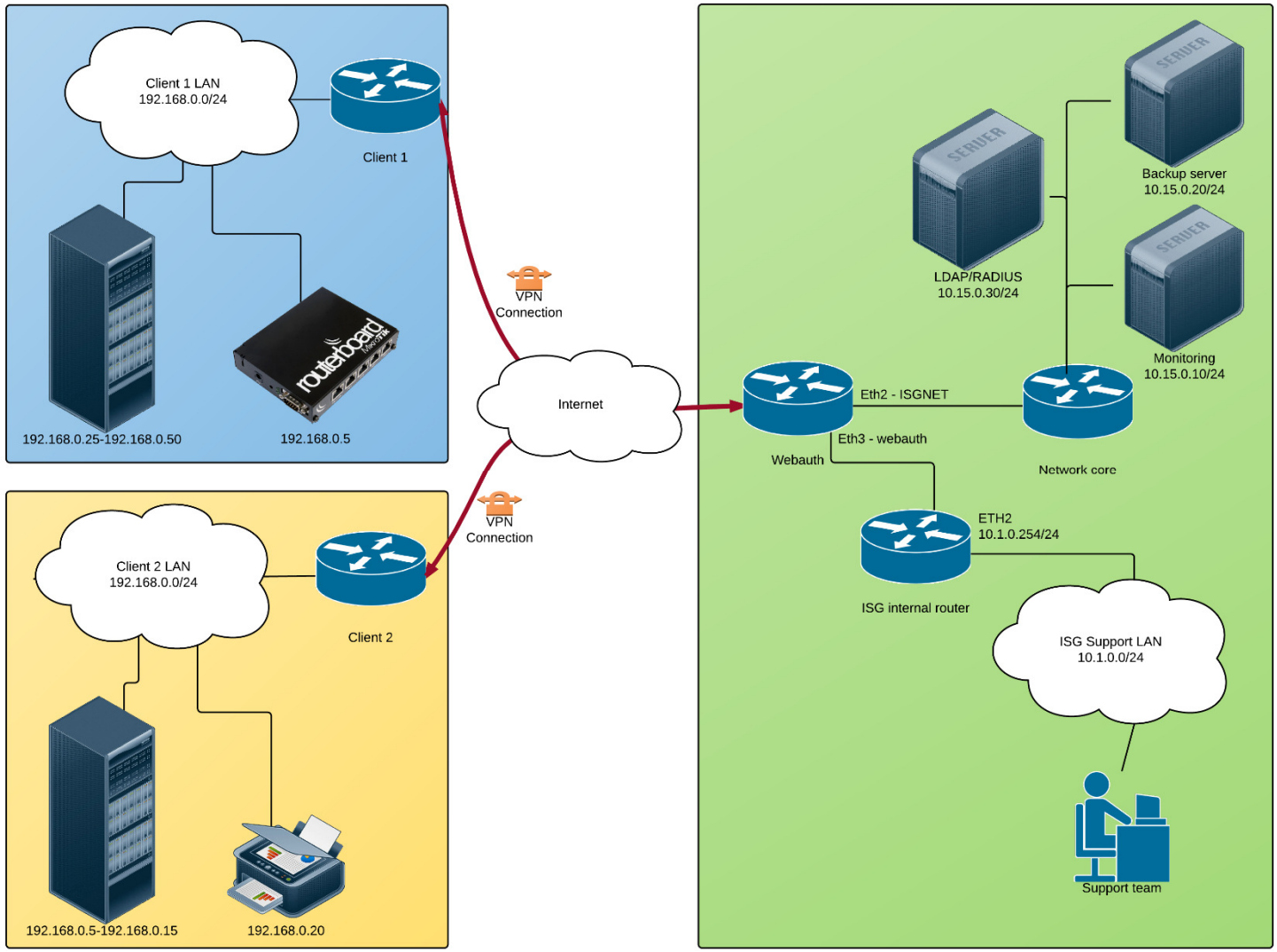
Solution requirement (financial)

- Low cost client device when dedicated equipment is required
- Maximize return on investment if already Mikrotik

Solution

- Use MikroTik products for their low total cost of ownership
- Tweak the hotspot to offer webauth functionality with Radius
- Site-to-Site VPN
- Use built-in firewall to control access from client and internal users
- Use built-in firewall to netmap client network to assigned subnet in our network, ISGNET
- Use OSPF for dynamic routing configuration in our network

Solution - diagram



Webauth

- Using the RouterOS hotspot functionality to a private network rather than the Internet
- Provide simple access control from internal network to customer.
- Provide the ability to log users activity
- Limit session time and concurrency

Webauth

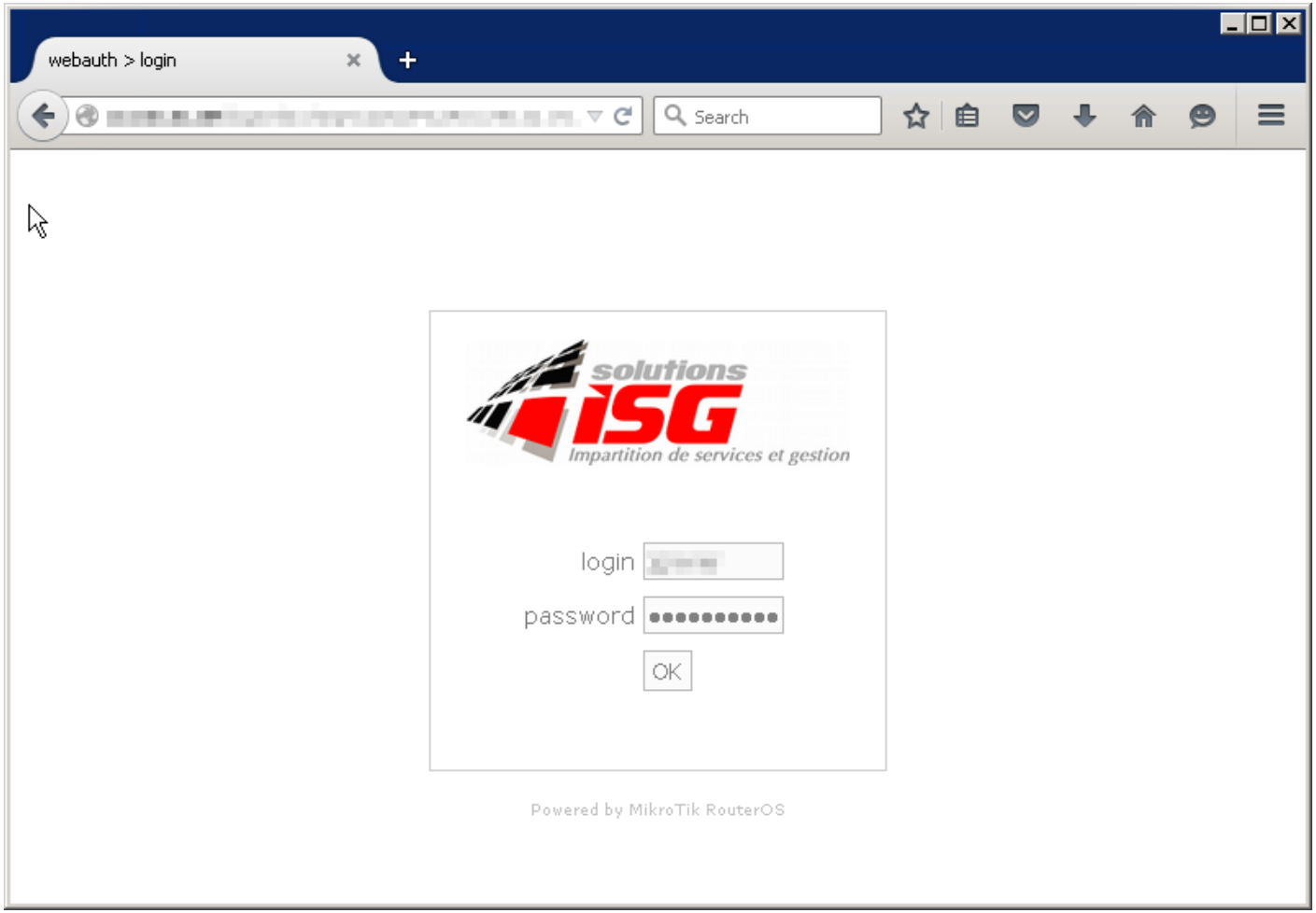
Sample configuration on RouterOS

```
/ip hotspot
add disabled=no idle-timeout=1d interface=ether3 \
    keepalive-timeout=1d name=webauth1 profile=webauth

/ip hotspot user profile
set [ find default=yes ] idle-timeout=none keepalive-timeout=1h \
    session-timeout=12h shared-users=1 status-autorefresh=1h

/ip hotspot profile
add html-directory=webauth login-by=http-pap name=webauth nas-port-type=\
    ethernet radius-accounting=no radius-default-domain=yul.isg.ca \
    use-radius=yes
```

Webauth


webauth > login
Search
solutions
ISG
Impartition de services et gestion
login
password
OK
Powered by MikroTik RouterOS

RADIUS

- Centralized user management
- Possible to revoke access from one central AD or LDAP

Sample configuration on RouterOS

```
/radius
add address=10.15.0.30 domain=isg.ca secret=pass2set service=hotspot
```

RADIUS

- Give the ability to have different user class using Mikrotik-Mark-Id RADIUS attribute

FreeRADIUS users configuration file sample:

```
DEFAULT LDAP-Group == netadmin, Service-Type == Login-User, NAS-Identifier == "yuls9r99"
        Mikrotik-Mark-Id = netadmin
```

Result in mangles:

```
38 D chain=hotspot action=mark-packet new-packet-mark=netadmin
     passthrough=yes src-address=10.1.0.100
39 D chain=hotspot action=mark-packet new-packet-mark=netadmin
     passthrough=yes src-address=10.1.0.100
```

Site-to-site VPN

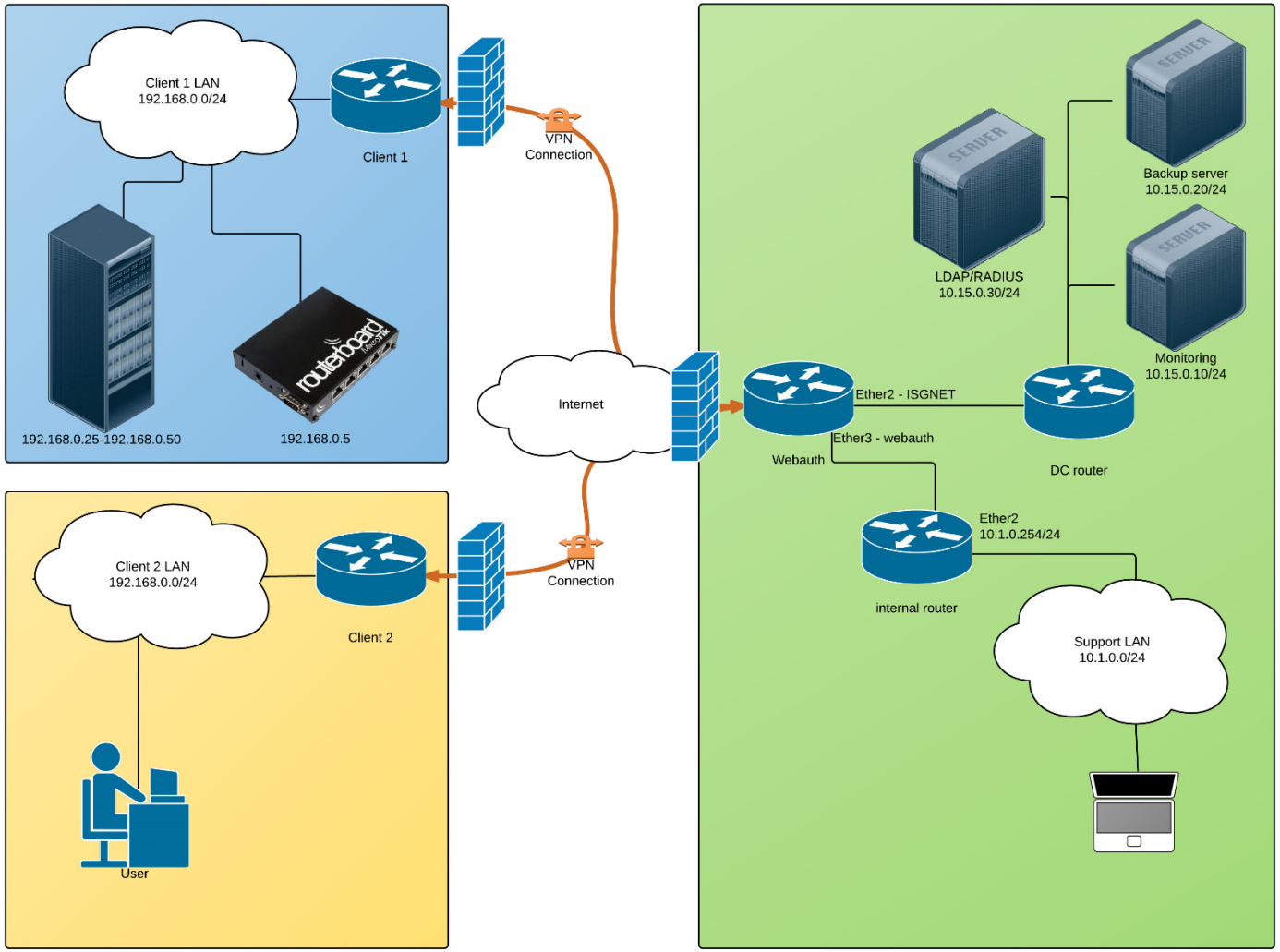
- RouterOS offers many options, the best suited for our application are IPSec and SSTP
- Provide permanent connectivity to client equipment which is required for monitoring and backups
- SSTP can be client initiated so it can be behind NAT and/or Firewall. It also works with dynamic public IPs.

Firewall

- On the client router, protect us from client accessing our network using SRCNAT and if required only open required services (backups, monitoring agents)

- On the webauth router, block client to see other clients or our internal network if there is a security breach between us and the client network.

Firewall - diagram



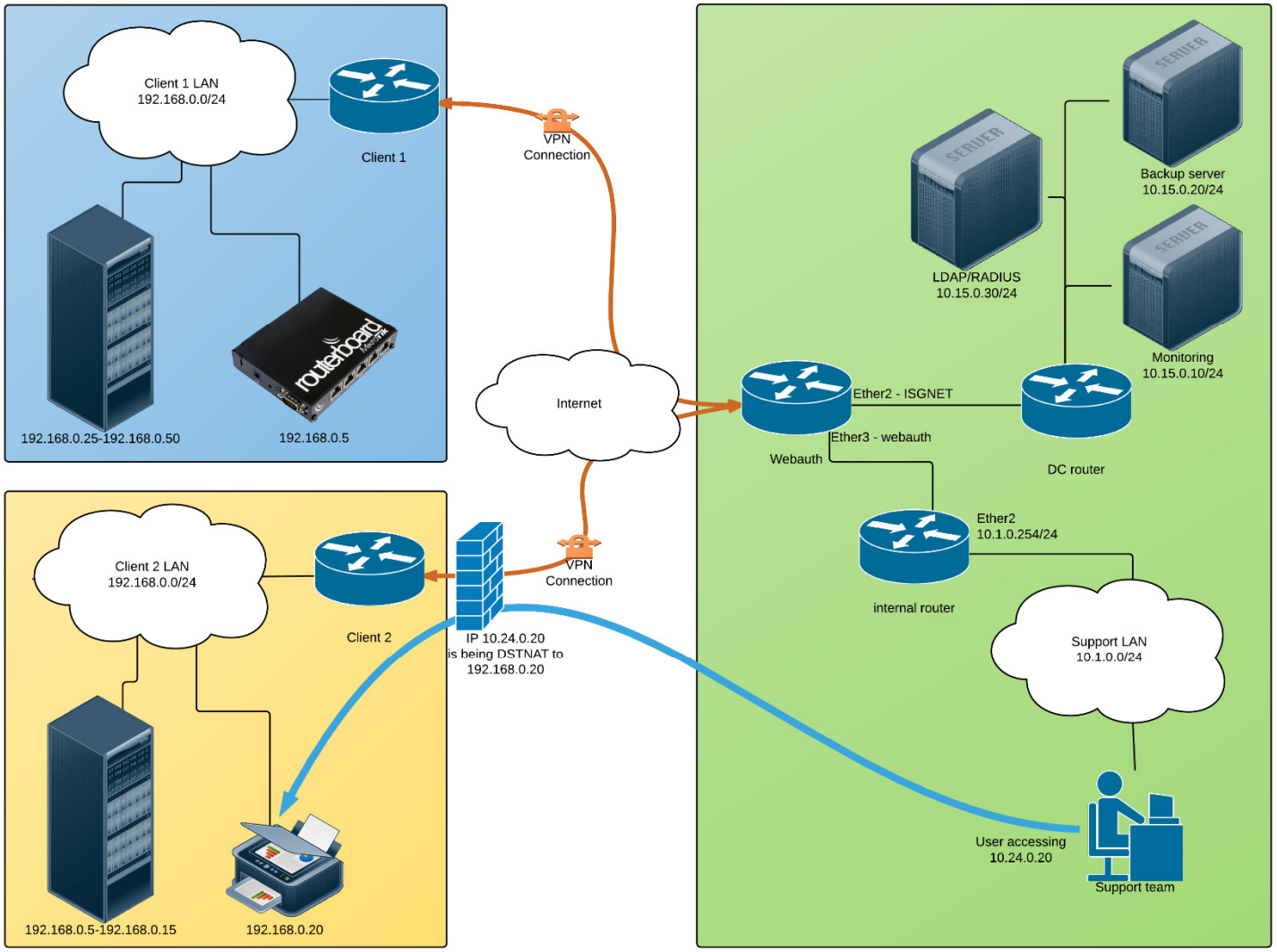
Netmap

- Netmap is a NAT action that creates a static 1:1 mapping of one set of IP addresses to another one
- Allows mapping from provider private IP to client private subnet (ex. 10.24.0.0/24 to 192.168.0.0/24)
- This is done on the client side router

Sample configuration of a Netmap:

```
/ip firewall nat
add action=netmap chain=dstnat comment=\
    "Netmapping 10.24.0.0/24 -> 192.168.0.0/24" disabled=no dst-address=\
    10.24.0.0/24 in-interface=yuls9r99 to-addresses=\
    192.168.0.0-192.168.0.255
```

NETMAP - diagram



OSPF

- Only on the provider side
- Dynamic network configuration in our network so when a client is added there is no need to reconfigure each router. This is particularly interesting when adding client who already has a subnet which is not in conflict and outside our standard ranges
- Give the ability to implement network redundancy

Conclusion

This solution has been a success for our daily operations and gave us the efficiency we were looking for. We've been using this model for more than 5 years. The technology has been proven stable and very economical to maintain.

The return on investment is great and for that, we have to thank Mikrotik for a great product line which enable us to make it a reality without breaking the bank!