INTELLIGENT MANAGEMENT ROUTER FOR ENTERPRISES

Mikrotik User Meeting in MONGOLIA
Content

1. Overview
2. WAN connectivity
3. Security & Firewall
4. User management
5. Redundancy
6. L4 load-balancer
7. Advanced bandwidth management & QoS
8. SmartUPS
9. Powerful troubleshooting and network analysis
10. Monitoring and alerting
11. Extra features (API and scripting)
1. Overview

RouterOS is the powerful router operating system including necessary features like routing, firewall, bandwidth management, wireless access point, backhaul link, hotspot gateway, VPN server, MPLS node, load-balancer and many more. There are plenty of possibilities and advantages which are not mentioned in this presentation. In this presentation, tried to cover only popular and useful use cases for enterprises.

RouterOS fits in **Software-Defined** approach which supports X86 machine and virtualization including VirtualBox 5, VMWare ESXi/Workstation/Fusion, Qemu, Hyper-V on Windows Server 2012, Citrix XenServer, Microsoft Azure and Amazon Web Services (AWS) and as well as OpenFlow standard.

Following common challenges of enterprise networking can be overcome with RouterOS solution.

- Overall network load (throughput) is under 10GE but requires **flexible** networking features like advanced QoS, load-balanced redundant network, traffic filtering, security etc...
- Proof of Concept **without** additional **cost** – Use existing hardware as software router
- Do I really pay for appropriate internet usage – Data traffic **analysis**
- **QoI** (Quality of Investment) – Cost efficient but easily scalable solution based on the current requirement (**Economy of scale**)
2. WAN connectivity

- Main internet connection (MobiNet Leased Line)
- VPN (Virtual Private Network)
- Backup connection (MobiNet Leased Line Economy)
- Mobile WAN

**VPN**

- IPSec (Site-to-Site, Site-to-Host)
- OpenVPN
- L2TP (+IPSec)
- PPTP (GRE+MPPE128)
- SSTP (+IPSec, SSL)
- GRE, EoIP, IPIP tunnels

**Main internet**

- Static IP (IPv4, IPv6)
- Dynamic routing (BGP, OSPF)

**Backup internet**

- PPPoE

**Mobile WAN**

- 3G (USB)
- 4G/LTE (USB)
- WiFi (802.11n/ac)
MobiNet Leased Line as main internet connection with static IP configuration:

```
[Mobinet@lab] > /ip address add address=202.21.X.2/29 interface=ether1 disabled=no
[Mobinet@lab] > /ip route add dst-address=0.0.0.0/0 gateway=202.21.X.1 distance=1 check-gateway=arp disabled=no
[Mobinet@lab] > /ip firewall nat add chain=srcnat out-interface=ether1 action=masquerade disabled=no
```

VPN – PPTP (network-to-network) example:

```
[Mobinet@lab] > /ip address add address=10.0.0.1/29 interface=ether2 disabled=no
[Mobinet@lab] > /interface pptp-client add name=VPN_int user=test password=test \
[Mobinet@lab] > connect-to=10.0.0.2 add-default-route=no disabled=no
[Mobinet@lab] > /ip route add dst-address=192.168.15.0/24 gateway=VPN_int disabled=no
```
- MobiNet LL Economy as backup internet connection

```bash
[Mobinet@lab] > /interface pppoe-client add name=2nd_wan user=123 password=123 \
[Mobinet@lab] > default-route-distance=2 use-peer-dns=yes interface=ether2 disabled=no 
[Mobinet@lab] > /ip firewall nat add chain=srcnat out-interface=2nd_wan action=masquerade disabled=no 

# Use backup internet connection efficiently. Simplest example to separate traffic by organizational units:
[Mobinet@lab] > /ip firewall mangle add chain=prerouting src-address=192.168.2.0/24 \\ 
[Mobinet@lab] > action=mark-routing new-routing-mark=Fin_dep disabled=no 
[Mobinet@lab] > /ip route add dst-address=0.0.0.0/0 gateway=2nd_wan distance=1 routing-mark=Fin_dep check-gateway=ping 
[Mobinet@lab] > /ip route add dst-address=0.0.0.0/0 gateway=202.21.X.1 distance=2 routing-mark=Fin_dep disabled=no
```

- Mobile WAN – 4G USB modem configuration example  
  [https://wiki.mikrotik.com/wiki/Supported_Hardware](https://wiki.mikrotik.com/wiki/Supported_Hardware)

```bash
[Mobinet@lab] > /interface lte set [find] name=mobile_wan apn=internet disabled=no 
[Mobinet@lab] > /ip dhcp-client add default-route-distance=3 interface=mobile_wan disabled=no 
[Mobinet@lab] > /ip firewall nat add chain=srcnat out-interface=mobile_wan action=masquerade disabled=no 
```
3. Security & Firewall

- RouterOS is can not be gateway antivirus or WAF in standalone way. But basic security protections can be achieved by itself. Also possible to support your advanced firewall appliances to save it`s resource.

  - Basic firewall
    
    ```bash
    [Mobinet@lab] > /ip firewall address-list add list=local address=192.168.1.0/24 disabled=no
    [Mobinet@lab] > /ip firewall address-list add list=local address=192.168.2.0/24 disabled=no
    [Mobinet@lab] > /ip firewall filter add chain=forward connection-state=invalid action=drop
    [Mobinet@lab] > /ip firewall filter add chain=forward connection-state=established action=accept
    [Mobinet@lab] > /ip firewall filter add chain=forward connection-state=related action=accept
    [Mobinet@lab] > /ip firewall filter add chain=forward src-address-list=local action=accept
    [Mobinet@lab] > /ip firewall filter add chain=forward action=drop
    ```

  - Permit VPN in firewall
    
    ```bash
    [Mobinet@lab] > /ip firewall filter add chain=forward in-interface=VPN_int action=accept place-before=1
    ```

  - Make sure your router is not an open DNS server
    
    ```bash
    [Mobinet@lab] > /interface list add name=wan_list
    [Mobinet@lab] > /interface list member add list=wan_list interface=ether1
    [Mobinet@lab] > /interface list member add list=wan_list interface=2nd_wan
    [Mobinet@lab] > /ip firewall raw add chain=prerouting protocol=udp dst-port=53 \ in-interface-list=wan_list action=drop disabled=no
    [Mobinet@lab] > /ip firewall raw add chain=prerouting protocol=tcp dst-port=53 \ in-interface-list=wan_list action=drop disabled=no
    ```

  - Disable unnecessary access to the router
    
    ```bash
    [Mobinet@lab] > /ip service {disable api; disable api-ssl; disable ftp; disable www; \ disable www-ssl; disable ssh; disable telnet}
    ```
Some useful firewall rules

# Identify syn_flood DOS attack
[Mobinet@lab] > /ip firewall filter add chain=input in-interface-list=wan_list connection-limit=100,32 \
[Mobinet@lab] > protocol=tcp tcp-flags=syn action=add-src-to-address-list address-list=blacklist \
[Mobinet@lab] > address-list-timeout=30m

# Identify port scanners
[Mobinet@lab] > /ip firewall filter add chain=input in-interface-list=wan_list psd=21,3s,3,1 \
[Mobinet@lab] > protocol=tcp action=add-src-to-address-list address-list=blacklist address-list-timeout=1d

# Mitigate blacklisted internet sources
[Mobinet@lab] > /ip firewall raw add chain=prerouting src-address-list=blacklist action=drop disabled=no

# Identify Spammers inside the local network to prevent public IP listed in global black lists
[Mobinet@lab] > /ip firewall filter add chain=forward in-interface-list=wan_list connection-limit=30,32 \
[Mobinet@lab] > limit=30/1m,0:packet protocol=tcp dst-port=25,587,465 action=add-src-to-address-list \
[Mobinet@lab] > address-list=spam address-list-timeout=1d
[Mobinet@lab] > /ip firewall raw add chain=prerouting protocol=tcp dst-port=25,587,465 src-address-list=spam \
[Mobinet@lab] > action=drop disabled=no

For more useful rules and ideas please visit to the link https://wiki.mikrotik.com/wiki/Firewall
4. User management

- Secure your local area network that every host should have registration and known as company staff
- Simple example on DHCP to lease IP only to the known host and block manual IP configuration on hosts

```bash
[Mobinet@lab] > /ip dhcp-server lease add mac-address=00:01:AB:CD:EF:23 address=192.168.1.10
[Mobinet@lab] > /ip dhcp-server set [find] address-pool=static-only add-arp=yes
[Mobinet@lab] > /interface ethernet set ether1 arp=reply-only
```

- This prevents unauthorized hosts to communicate with router/gateway, but those hosts still have layer2 access to the local network. To be more secure, Layer2 access switches can have port based authentication. Routerboard CRS switches can achieve it with less cost (Low TCO)

- Same Layer 2 protection should apply to the company`s private wireless network.

```bash
[ Mobinet@lab ] > /interface wireless access-list add mac-address=00:01:AB:CD:EF:23 interface=local_wireless /
[ Mobinet@lab ] > vlan-mode=no-tag comment=Otgoo
[ Mobinet@lab ] > /interface wireless set local_wireless default-authentication=no default-forwarding=no
```
- An other option of internal user management is Hostpot
- Enterprises like Hotels, can have single WiFi-mesh infrastructure to authenticate both staffs and guests
- Based on credentials, staffs connects to the secure private network and guests connects to the advertised hotspot. Even guest can connect to the internet without credential, just CONTINUE button
- This setup can align with wired (Ethernet) network too
- Hotspot is something easy to configure with SETUP option

- More advanced **user management** can be covered by User manager package of RouterOS and 3rd party Radius server.
5. Redundancy

- Hardware and WAN connectivity redundancy in single office

```
[Mobinet@R1] > /interface vrrp add name=vrwap_lan vrid=111 priority=253 interval=1s
[Mobinet@R1] > preemption-mode=yes disabled=no interface=ether2
[Mobinet@R1] > /ip address add address=192.168.1.2/24 disabled=no interface=ether2
[Mobinet@R1] > /ip address add address=192.168.1.1/24 disabled=no interface=vrwap_lan

[Mobinet@R2] > /interface vrrp add name=vrwap_lan vrid=111 priority=252 interval=1s
[Mobinet@R2] > preemption-mode=no disabled=no interface=ether2
[Mobinet@R2] > /ip address add address=192.168.1.3/24 disabled=no interface=ether2
[Mobinet@R2] > /ip address add address=192.168.1.1/24 disabled=no interface=vrwap_lan
```
5. Redundancy

- Hardware and WAN connectivity redundancy with backup datacenter
  - Same mechanism can be applied. VRRP on the WAN interfaces
  - Branch hosts can access to the mission critical services (servers) anytime even main datacenter has issue (Application layer redundancy should be implemented on servers)
  - VPN connection type can be anything like IPSec or PPP
  - **Load-balancing** is possible in both cases
6. L4 load-balancer

- Web service load balancing with no server quantity limitation.
- Routers will handle **L4 load balancing**.
- Router detects not only Web servers network issue but also HTTP service (port 80, 443). If something happen with Server N, router will exclude this server from load balancing list automatically. Auto switching time will be depending on server quantity and frequency to check
  - Switching test \[\text{server}_\text{qty} \times 5 \text{ sec} + 4 \text{ seconds}\]
- Each router can act as other one if something happens with router itself. This is standard automatic VRRP protocol switches within 2 seconds.
- Router will manage **L4 firewall** functionality. Servers don`t need to handle IP firewall separately.
- Limitation: Can not act as WAF /Web application firewall/
- VRRP will be configured exactly same method as previous
- Load-balancing forwarding and scripting sections will be same for both R1 and R2 routers

/ip firewall nat add chain=dstnat dst-address=202.21.X.15 protocol=tcp dst-port=80,443 \ per-connection-classifier=src-address-and-port:3/0 action=dst-nat to-address=172.16.0.10 comment=loadbalance_s1 
/ip firewall nat add chain=dstnat dst-address=202.21.X.15 protocol=tcp dst-port=80,443 \ per-connection-classifier=src-address-and-port:3/1 action=dst-nat to-address=172.16.0.11 comment=loadbalance_s2 
/ip firewall nat add chain=dstnat dst-address=202.21.X.15 protocol=tcp dst-port=80,443 \ per-connection-classifier=src-address-and-port:3/2 action=dst-nat to-address=172.16.0.12 comment=loadbalance_s3
- Check TCP port 443 with fetch
  (In order to show friendly, script parameters are not in correct syntax format. Please copy source section in the winbox)

```plaintext
/system script add name=s1_fetch source=
  /file remove [find name=testfile.10];
  /tool fetch "https://172.16.0.10/test.txt" dst-path=testfile.10 mode=https port=443;
  /ip dns static add address=0.0.0.1 name=s1;
  /ip dns static add address=0.0.0.1 name=s2;
  /ip dns static add address=0.0.0.1 name=s3;
  /ip dns static add address=0.0.0.1 name=s0;
  /ip dns static add address=0.0.0.1 name=z;
/system script add name=s2_fetch source=
  /file remove [find name=testfile.11];
  /tool fetch "https://172.16.0.11/test.txt" dst-path=testfile.11 mode=https port=443;
  /ip dns static add address=0.0.0.1 name=s1;
  /ip dns static add address=0.0.0.1 name=s2;
  /ip dns static add address=0.0.0.1 name=s3;
  /ip dns static add address=0.0.0.1 name=s0;
  /ip dns static add address=0.0.0.1 name=z;
/system script add name=s3_fetch source=
  /file remove [find name=testfile.12];
  /tool fetch "https://172.16.0.12/test.txt" dst-path=testfile.12 mode=https port=443;
  /ip dns static add address=0.0.0.1 name=s1;
  /ip dns static add address=0.0.0.1 name=s2;
  /ip dns static add address=0.0.0.1 name=s3;
  /ip dns static add address=0.0.0.1 name=s0;
  /ip dns static add address=0.0.0.1 name=z;
```

/system script add name=s_status_check source=
if ([/file print count-only where name=testfile.10]=1) do=
/log info "172.16.0.10 is ok"; /ip dns static set [find where name=s1] comment=1;} else={/log info "172.16.0.10 is down";
/ip dns static set [find where name=s1] comment=0;
} if ([/file print count-only where name=testfile.11]=1) do=
/log info "172.16.0.11 is ok"; /ip dns static set [find where name=s2] comment=1;} else={/log info "172.16.0.11 is down";
/ip dns static set [find where name=s2] comment=0;
} if ([/file print count-only where name=testfile.12]=1) do=
/log info "172.16.0.12 is ok"; /ip dns static set [find where name=s3] comment=1;} else={/log info "172.16.0.12 is down";
/ip dns static set [find where name=s3] comment=0;

/system script add name=update_balancer source=
:global s1 [/ip dns static get [find where name=s1] comment];
:global s2 [/ip dns static get [find where name=s2] comment];
:global s3 [/ip dns static get [find where name=s3] comment];
:global s0 ($s1+$s2+$s3);
:global z 0;
if ($s1=1) do=
/ip firewall nat set [find where comment=loadbalance_s1] disabled=no per-connection-classifier="src-address-and-port:$s0/$z";
:global z ($z+1)} else={
/ip firewall nat set [find where comment=loadbalance_s1] disabled=yes};

:if ($s2=1) do=
/ip firewall nat set [find where comment=loadbalance_s2] disabled=no per-connection-classifier="src-address-and-port:$s0/$z";
:global z ($z+1)} else={
/ip firewall nat set [find where comment=loadbalance_s2] disabled=yes};

:if ($s3=1) do=
/ip firewall nat set [find where comment=loadbalance_s3] disabled=no per-connection-classifier="src-address-and-port:$s0/$z";
:global z ($z+1)} else={
/ip firewall nat set [find where comment=loadbalance_s3] disabled=yes};
- Tested log in real environment

16:32:44 script,info STARTED
16:32:46 info fetch: file "testfile.10" downloaded
16:32:56 info fetch: file "testfile.12" downloaded
16:32:59 script,info 172.16.0.10 is ok
16:32:59 system,info static dns entry changed by load-balancer
16:32:59 script,info 172.16.0.11 is down
16:32:59 system,info static dns entry changed by load-balancer
16:32:59 script,info 172.16.0.12 is ok
16:33:00 system,info static dns entry changed by load-balancer
16:33:02 system,info nat rule changed by load-balancer
16:33:02 system,info nat rule changed by load-balancer
16:33:02 system,info nat rule changed by load-balancer
16:33:02 script,info FINISHED
7. Advanced bandwidth management & QoS

- Utilize available bandwidth **efficiently**
- **Real-time** equal bandwidth distribution among available hosts in the office
- Destination based different **QoS management**
- Application **classification** and its QoS
Example of MIX (Mongolian InterExchange) traffic classification

```
[Mobinet@lab] > /ip firewall address-list add list=MIX_ISP address=202.131.224.0/19 disabled=no
[Mobinet@lab] > /ip firewall mangle add chain=prerouting src-address-list=MIX_ISP action=mark-packet \\ new-packet-mark=mix_down
[Mobinet@lab] > /ip firewall mangle add chain=postrouting dst-address-list=MIX_ISP action=mark-packet \\ new-packet-mark=mix_up
[Mobinet@lab] > /queue simple add name=Mongolian_Interexchange(MIX) packet-mark=mix_up,mix_down max-limit=1G/1G \\ target=0.0.0.0/0
```

- If your hardware has enough RAM, increase your queue sizes. It helps to drop less packets when traffic amount reaches limits at peak hours

```
[Mobinet@lab] > /queue type set default-small pfifo-limit=1000
[Mobinet@lab] > /queue type set pcq-download-default pcq-limit=5000 pcq-total-limit=200000
```
8. SmartUPS

- RouterOS supports APC SmartUPS series smart signaling protocol over USB and Serial interfaces
- Alert power-outage, safe hibernate router when battery capacity become low

SUA750ICH

SC420i

SMT1500i
9. Powerful troubleshooting and network analysis

- MTR including both trace route and ping
- ARP ping, IPScan “/tool traceroute 202.131.224.2”

![Traceroute screenshot](image)
- Real-time connection tracking

![Firewall Tracking Table]

<table>
<thead>
<tr>
<th>Src. Address</th>
<th>Dst. Address</th>
<th>Peplpy Src. Address</th>
<th>Peplpy Dst. Address</th>
<th>Protocol</th>
<th>Connecti...</th>
<th>Timeout</th>
<th>TCP State</th>
<th>Orig./Repl. Rate</th>
<th>Orig./Repl. Bytes</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.88.123</td>
<td>203.0.113.123</td>
<td>192.168.88.123</td>
<td>203.0.113.123</td>
<td>6 (tcp)</td>
<td>23:39:55 established</td>
<td>415 bps/1256 bps</td>
<td>67 KB/12.5 KB</td>
<td></td>
<td></td>
</tr>
<tr>
<td>192.168.88.124</td>
<td>203.0.113.124</td>
<td>192.168.88.124</td>
<td>203.0.113.124</td>
<td>6 (tcp)</td>
<td>23:39:55 established</td>
<td>0 bps/0 bps</td>
<td>6 KB/0.2 KB</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

MobiNet
Powered by MobiCom
- Real-time traffic torching

<table>
<thead>
<tr>
<th>Bin...</th>
<th>Prot...</th>
<th>Src...</th>
<th>VLAN Id</th>
<th>DSCP</th>
<th>Tx Rate</th>
<th>Rx Rate</th>
<th>Tx Pack</th>
<th>Rx Pack</th>
</tr>
</thead>
<tbody>
<tr>
<td>800 (p)</td>
<td>6 tcp</td>
<td>192.168.88.203.57017</td>
<td>216.58.197.112.80 (http)</td>
<td>11.3 Mbps</td>
<td>285.5 kbps</td>
<td>552</td>
<td>503</td>
<td></td>
</tr>
<tr>
<td>600 (p)</td>
<td>6 tcp</td>
<td>192.168.88.203.57019</td>
<td>216.58.197.112.80 (http)</td>
<td>10.1 Mbps</td>
<td>237.0 kbps</td>
<td>656</td>
<td>449</td>
<td></td>
</tr>
<tr>
<td>600 (p)</td>
<td>6 tcp</td>
<td>192.168.88.203.57015</td>
<td>216.58.197.112.80 (http)</td>
<td>4.7 Mbps</td>
<td>113.3 kbps</td>
<td>402</td>
<td>226</td>
<td></td>
</tr>
<tr>
<td>600 (p)</td>
<td>6 tcp</td>
<td>192.168.88.203.57010</td>
<td>216.58.197.112.80 (http)</td>
<td>2.5 Mbps</td>
<td>53.1 kbps</td>
<td>226</td>
<td>112</td>
<td></td>
</tr>
<tr>
<td>600 (p)</td>
<td>6 tcp</td>
<td>192.168.88.203.57021</td>
<td>216.58.197.112.80 (http)</td>
<td>2.3 Mbps</td>
<td>52.2 kbps</td>
<td>201</td>
<td>99</td>
<td></td>
</tr>
<tr>
<td>600 (p)</td>
<td>6 tcp</td>
<td>192.168.88.253.60804</td>
<td>192.168.88.1.8291 (winbox)</td>
<td>2.0 Mbps</td>
<td>46.4 kbps</td>
<td>181</td>
<td>86</td>
<td></td>
</tr>
<tr>
<td>800 (p)</td>
<td>17 (...)</td>
<td>192.168.88.158.52652</td>
<td>239.255.255.1900</td>
<td>139.6 kbps</td>
<td>3.3 kbps</td>
<td>15</td>
<td>11</td>
<td></td>
</tr>
<tr>
<td>800 (p)</td>
<td>17 (...)</td>
<td>192.168.88.222.63232</td>
<td>31.13.95.36.443 (ftp)</td>
<td>106 kbps</td>
<td>528 kbps</td>
<td>1</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>800 (p)</td>
<td>17 (...)</td>
<td>192.168.88.253.6240</td>
<td>192.168.1.11.12.161 (smtp)</td>
<td>0 bps</td>
<td>960 bps</td>
<td>0</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>800 (p)</td>
<td>17 (...)</td>
<td>192.168.88.253.6240</td>
<td>192.168.123.129.161 (smtp)</td>
<td>0 bps</td>
<td>960 bps</td>
<td>0</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>600 (p)</td>
<td>17 (...)</td>
<td>192.168.88.158.52652</td>
<td>192.168.88.158.52652</td>
<td>113 kbps</td>
<td>1.3 kbps</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>600 (p)</td>
<td>17 (...)</td>
<td>192.168.88.222.63232</td>
<td>31.13.95.36.443 (ftp)</td>
<td>0 bps</td>
<td>688 bps</td>
<td>0</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>800 (p)</td>
<td>17 (...)</td>
<td>192.168.88.158.52652</td>
<td>192.168.88.158.52652</td>
<td>0 bps</td>
<td>688 bps</td>
<td>0</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>600 (p)</td>
<td>17 (...)</td>
<td>192.168.88.222.63232</td>
<td>31.13.95.36.443 (ftp)</td>
<td>0 bps</td>
<td>688 bps</td>
<td>0</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>600 (p)</td>
<td>17 (...)</td>
<td>192.168.88.158.52652</td>
<td>192.168.88.158.52652</td>
<td>0 bps</td>
<td>688 bps</td>
<td>0</td>
<td>1</td>
<td></td>
</tr>
</tbody>
</table>

Total Tx Rate: 33.4 Mbps
Total Rx Rate: 798.6 kbps
Total Tx Packets: 2,839
Total Rx Packets: 1,501
- Packet sniffer
- Supports TZSP stream to export output to the wireshark host
10. Monitoring and alerting

- Small but useful tool “Graphing”. It graphs and stores queue and interfaces traffic usage.
- Basic monitoring protocols SNMP, NetFlowV9
- E-mail alerting and SMS alerting with USB 3G/4G modem
- Bandwidth test server and client functionality that generates real data. Client supports Windows machine
- Netwatch monitors defined hosts by ICMP and can take any action based on UP/DOWN event. Simple example:

  [Mobinet@lab] > /tool netwatch add host=192.168.1.10 interval=5s timeout=100ms down-script="/tool e-mail send server=202.131.224.27 port=25 from=lab@mobinet.mn to=otgonkhuu@mobinet.mn subject=video_processing_gone_down"
11. Extra features (API and scripting)

RouterOS Script and API features enables plenty of possibilities and advantages.

- Auto provisioning like create/remove automatic rules
- Automatically register local users which connected to CRM/ERP
- In a hotel possible to integrate into hotel CRM and create hotspot client with necessary policy.
- Broad range of network automation
- Act as SMS-to-Email server
- One-time password for networking access
- On-Demand speed booster
- Network based advertisement system
- Many more...

WIKI.MIKROTIK.COM
FORUM.MIKROTIK.COM
THANK YOU

Otgonkhuu.A
otgonkhuu@mobinet.mn
June 16, 2017. MobiNet LLC