



ROUTEROS HIDDEN FEATURE TRICKS & IMPLEMENT SOCIAL WIFI ON MIKROTIK HOTSPOT.

ABOUT PRESENTER

- Mikrotik enthusiast. Since 2011
- MTCNA MTCRE /recently/
- Linux
- VoIP
- Erdenetsogt.d@gmail.com

OUTLINE

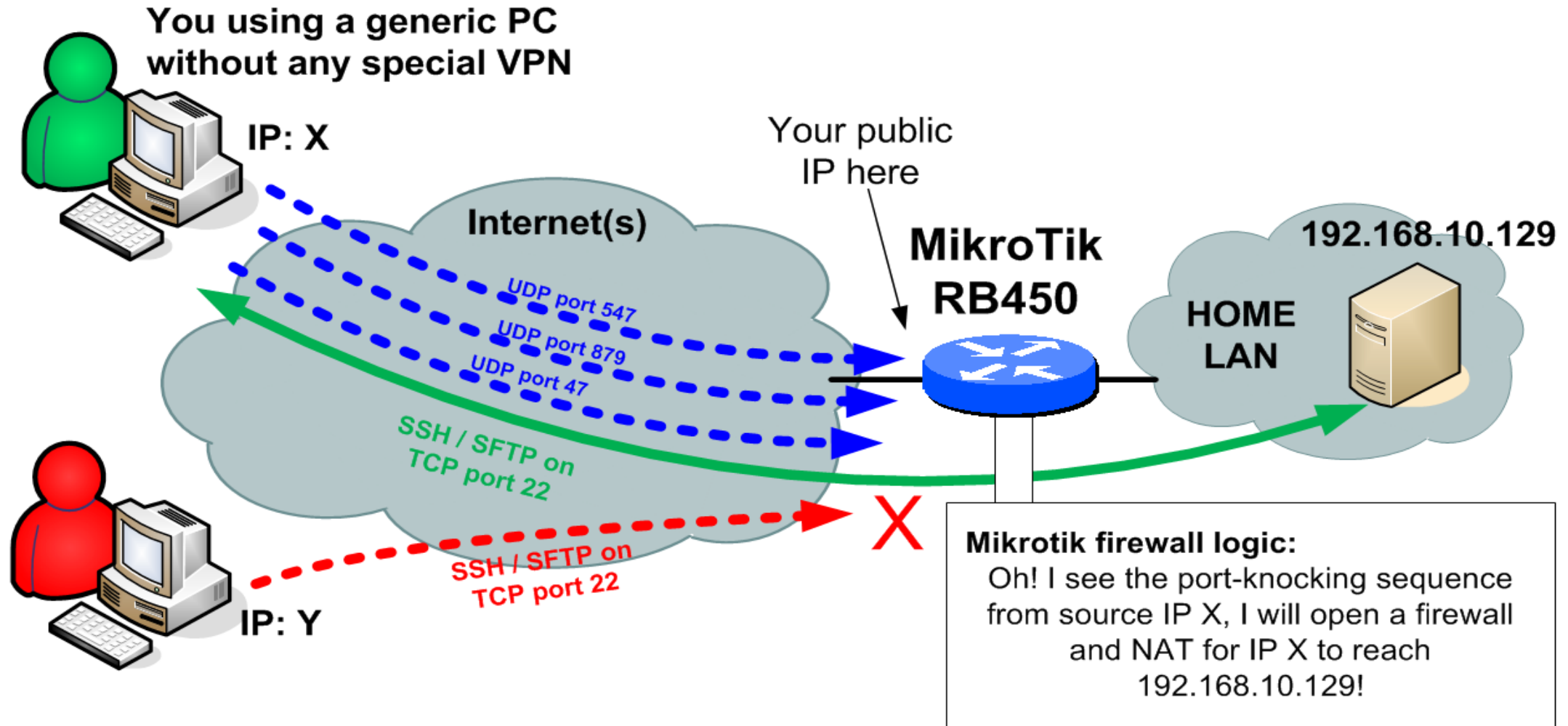
- Scripting
 - Control, Monitor with SMS
- Port knocking concept, usage
- Wan Aggregation
- Social WiFi login



PORT KNOCKING



EFFECTIVNESS



DEMONSTRATION

DEMONSTRATION OF PORT KNOCKING

FIREWALL TRICKS

- Brute force is a trial and error method used by application programs to decode encrypted data such as passwords

Jun/07/2017 15:45:50	memory	system, info, account	user admin logged in from 202.70.34.82 via telnet
Jun/07/2017 15:45:50	memory	system, info, account	user admin logged in from 202.70.34.82 via telnet
Jun/07/2017 15:46:04	memory	system, info	filter rule changed by admin
Jun/07/2017 15:46:04	memory	system, info	filter rule changed by admin
Jun/07/2017 15:46:17	memory	wireless, info	wlan1: data from unknown device 40:F3:08:2D:5E:97, sent deauth
Jun/07/2017 15:46:39	memory	system, error, critical	login failure for user fdsfsdfd from 202.70.34.82 via ssh
Jun/07/2017 15:46:43	memory	system, error, critical	login failure for user fdsfsdfd from 202.70.34.82 via ssh
Jun/07/2017 15:47:04	memory	system, error, critical	login failure for user root from 202.70.34.82 via ssh
Jun/07/2017 15:47:05	memory	system, error, critical	login failure for user root from 202.70.34.82 via ssh
Jun/07/2017 15:47:07	memory	system, error, critical	login failure for user root from 202.70.34.82 via ssh
Jun/07/2017 15:47:09	memory	system, error, critical	login failure for user root from 202.70.34.82 via ssh
Jun/07/2017 15:47:12	memory	wireless, info	wlan1: data from unknown device 40:F3:08:2D:5E:97, sent deauth

SSH BRUTE ATTACK STOP FIREWALL FILTER

```
conntrack off log off log-prefix=""
```

```
;;; SSH bruteforcers
```

```
chain=input action=drop protocol=tcp src-address-list=ssh_blacklist dst-port=22 log=no log-prefix=""
```

```
chain=input action=add-src-to-address-list connection-state=new protocol=tcp src-address-list=ssh_stage2  
address-list=ssh_blacklist address-list-timeout=1w3d dst-port=22 log=no log-prefix=""
```

```
chain=input action=add-src-to-address-list connection-state=new protocol=tcp src-address-list=ssh_stage1  
address-list=ssh_stage2 address-list-timeout=1m dst-port=22 log=no log-prefix=""
```

```
chain=input action=add-src-to-address-list connection-state=new protocol=tcp address-list=ssh_stage1  
address-list-timeout=1m dst-port=22 log=no log-prefix=""
```

D	ssh_blacklist	73.203.198.13	9d 15:12:12
D	ssh_blacklist	91.197.232.11	9d 23:30:18
D	ssh_blacklist	179.132.156.24	9d 21:55:46
D	ssh_blacklist	191.210.123.230	9d 15:04:07
D	ssh_blacklist	193.201.224.215	9d 22:05:04
X	salbanud10	172.16.11.0/24	

SCRIPTING

- Provides a method to automate tasks through the use of user defined scripts.
- Examples
 - Cable testing
 - Wan availability
 - Automated backup
 - Get health status /Using 3g modem/

AUTOMATIC BACKUP

- Create backup file
- Wait 10s
- Send e-mail with backup attachment
- Wait 30s
- Remove newly created backup file
- Send Log

The screenshot shows a Windows-style dialog box titled "Schedule <Daily_Backup>". It contains the following fields and controls:

- Name:** Daily_Backup
- Start Date:** Jun/11/2017
- Start Time:** 01:00:00 (with a dropdown arrow)
- Interval:** 1d 00:00:00
- Owner:** admin
- Policy:** A grid of checkboxes:
 - ☒ ftp, ☒ reboot
 - ☒ read, ☒ write
 - ☒ policy, ☒ test
 - ☒ password, ☒ sniff
 - ☒ sensitive, ☒ romon
 - ☐ dude
- Run Count:** 17
- Next Run:** Jun/12/2017 18:31:44
- On Event:** A text area containing:

```
:log warning "Backup Starting"
/system backup save name=daily dont-encrypt=yes
:delay 10s
:log warning "Sending to email"
/tool e-mail send file=daily.backup to=erdenetsogt.d@gmail.com
server=maxgroup.mn port=587 user=it_update@maxgroup.mn
password=XXXXXX from=it_update@maxgroup.mn subject=Backup
:delay 30s
/file remove daily.backup
:log warning "Backup Done!."
```
- Buttons:** OK, Cancel, Apply, Disable, Comment, Copy, Remove.
- Status:** enabled

CABLE TEST

Script <cabletest>

Name:

Owner:

Policy: ☒ ftp ☒ reboot
☒ read ☒ write
☒ policy ☒ test
☒ password ☒ sniff
☒ sensitive ☒ romon
☐ dude

Last Time Started:

Run Count:

Source:

```
:local link;  
/interface ethernet cable-test ether5 once do={  
:set link "$status";  
};  
if ($link = "no-link") do={  
/log error "Interface down!! Sending mail...."  
};
```

OK

Cancel

Apply

Comment

Copy

Remove

Run Script

32	memory	wireless, info	38:BC:1A:DB:62:9F, sent deauth
			WAN2: data from unknown device
			38:BC:1A:DB:62:9F, sent deauth
35	memory	wireless, info	38:BC:1A:DB:62:9F@WAN2: connected
50	memory	system, info	changed script settings by admin
52	memory	system, info	address list entry added by admin
55	memory	system, info	address list entry removed by admin
19	memory	system, info	changed script settings by admin
23	memory	system, info	address list entry added by admin
23	memory	script, error	Interface down!! Sending mail....
58	memory	wireless, info	38:BC:1A:DB:62:9F@WAN2: disconnected, extensive data loss
58	memory	wireless, info	WAN2: data from unknown device
			38:BC:1A:DB:62:9F, sent deauth
58	memory	wireless, info	WAN2: data from unknown device
			38:BC:1A:DB:62:9F, sent deauth
01	memory	wireless, info	38:BC:1A:DB:62:9F@WAN2: connected
26	memory	system, info, account	user admin logged in via local
15	memory	script, error	Interface down!! Sending mail....
13	memory	system, info	address list entry added by admin
36	memory	system, info, account	user admin logged out via local
14	memory	script, error	Interface down!! Sending mail....
08	memory	script, error	Interface down!! Sending mail....
09	memory	script, error	Interface down!! Sending mail....

CONTROL, MONITOR WITH SMS

- Determine usb port and modem
 - Enable SMS and Receive enabled
 - Check send sms
-
- Execute script via SMS
 - :cmd [secret] script [scriptname]



Terminal

```
/          Move up to base level
..         Move up one level
/command   Use command at the base level
[admin@MikroTik] > port print
Flags: I - inactive
#  DEVICE NAME      CHANNELS USED-BY  BAUD-RATE
0  1:2   usb1       4 sms tool      9600
[admin@MikroTik] >
```

SMS Settings

☒ Receive Enabled

Port: usb1

Channel: 0

Secret: ****

Allowed Number:

Keep Max SMS: 0

OK

Cancel

Apply

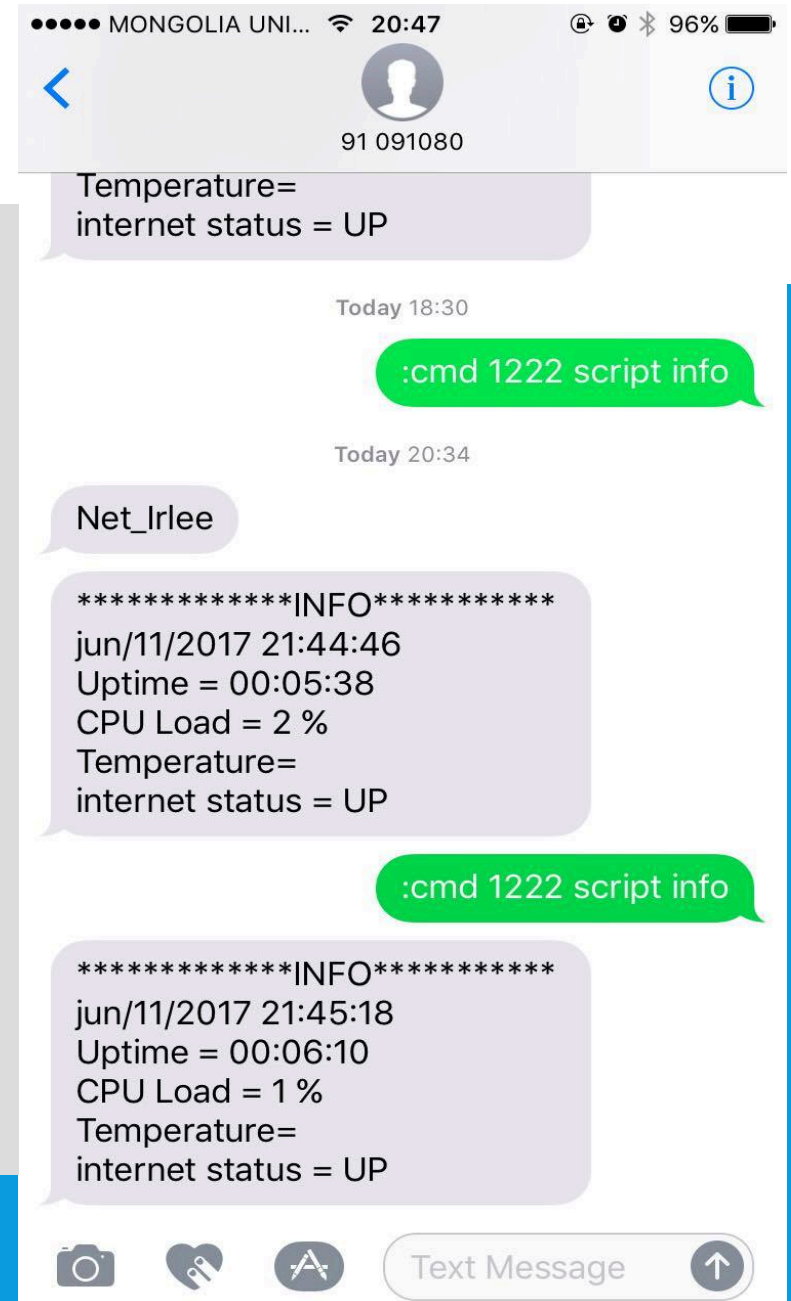
Inbox

Send SMS

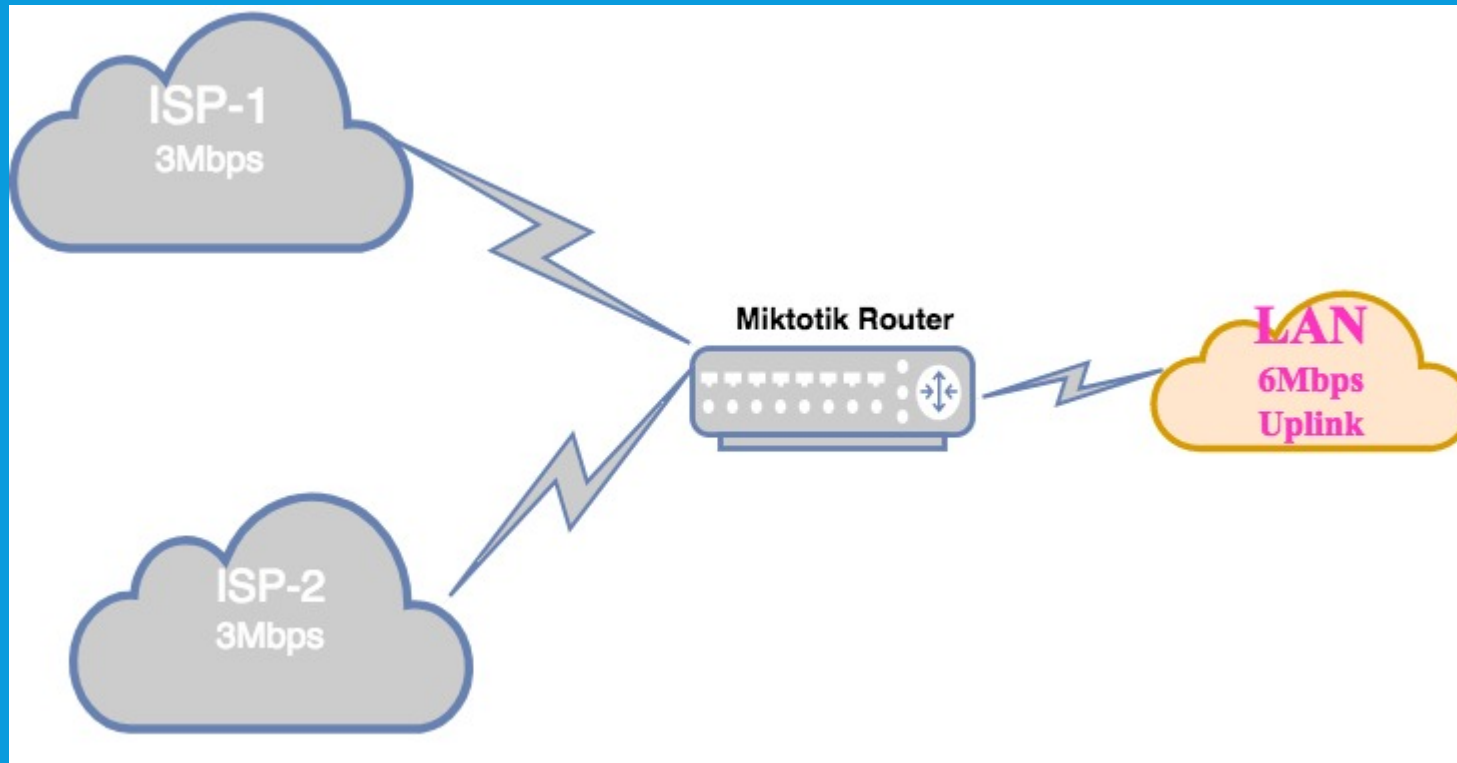
EXAMPLE

Source:

```
:local date;  
:local time;  
:set date [/system clock get date];  
:set time [/system clock get time];  
:local UPTIME [/system resource get uptime]  
:local CPU [/system resource get cpu-load]  
:local TEMPR [/sys health get temperature]  
:global STS;  
:if ([/ping 8.8.8.8 count=3] = 0) do {:set STS value=DOWN} else={:set STS value=UP}  
:local MSG "*****INFO*****"  
$date $time  
Uptime = $UPTIME  
CPU Load = $CPU %  
Temperature=$TEMPR  
internet status = $STS"  
/tool sms send port=usb1 channel=0 phone-number="88088391" message="$MSG"
```



WAN BONDING /AGGREGATE/



WAN BONDING CONCEPT

- ❖ Mark connection for input wan interfaces respectively
- ❖ Mark routing for output wan interfaces that matches connection
- ❖ Use PCC method for divide traffic
- ❖ Config route for marked routes

Safe Mode Session: 00:0C:42:BC:B5:2F

Quick Set

CAPsMAN

Interfaces

Wireless

Bridge

PPP

Switch

Mesh

IP

MPLS

Routing

System

Queues

Files

Log

Radius

Tools

New Terminal

LCD

MetaROUTER

Interface List

Interface Interface List Ethernet EoIP Tunnel IP Tunnel GRE Tunnel VLAN VRRP Bonding LTE

	Name	Type	Actual MTU	L2 MTU	Tx	Rx	Tx Packet (p/s)	Rx Packet (p/s)	FP Tx
R	WAN1	Ethernet	1500	1598	136.4 kbps	3.1 Mbps	254	290	122
R	WAN2	Wireless (Atheros AR9...	1500	1600	118.1 kbps	3.0 Mbps	252	252	
... defconf									
R	bridge-local	Bridge	1500	1598	6.3 Mbps	198.8 kbps	537	536	
RS	ether2-master	Ethernet	1500	1598	0 bps	0 bps	0	0	6.
S	ether3	Ethernet	1500	1598	0 bps	0 bps	0	0	
S	ether4	Ethernet							
RS	ether5	Ethernet							
S	ether6-master	Ethernet							
S	ether7	Ethernet							
S	ether8	Ethernet							
S	ether9	Ethernet							
S	ether10	Ethernet							
X	ppp-out1	PPP Client							

14 items (1 selected)

11% 1Gio.dat

Download status

Speed Limiter

Options on completion

<http://ovh.net/files/1Gio.dat>

Status Receiving data...

File size 1.000 GB

Downloaded 115.467 MB (11.27 %)

Transfer rate 786.145 KB/sec

Time left 19 min 59 sec

Resume capability Yes

<< Hide details

Pause

Cancel

DEMONSTRATION VIDEO GOES HERE

HOTSPOT

Benefits of Offering Free WiFi

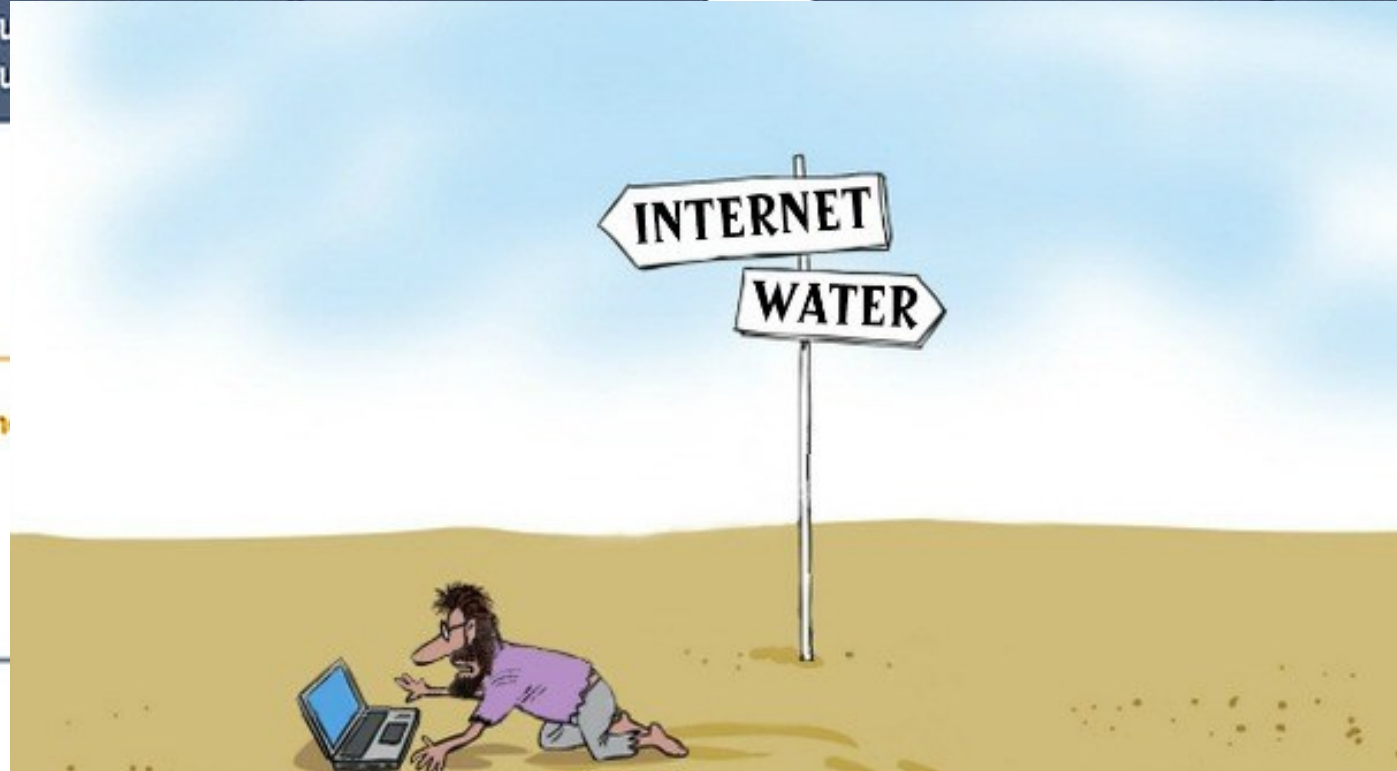
Which of the following best describes

you
you

Which of the following best describes

rior since

Spend
same time



1%

Spend
more
money

price
scape

EXAMPLES



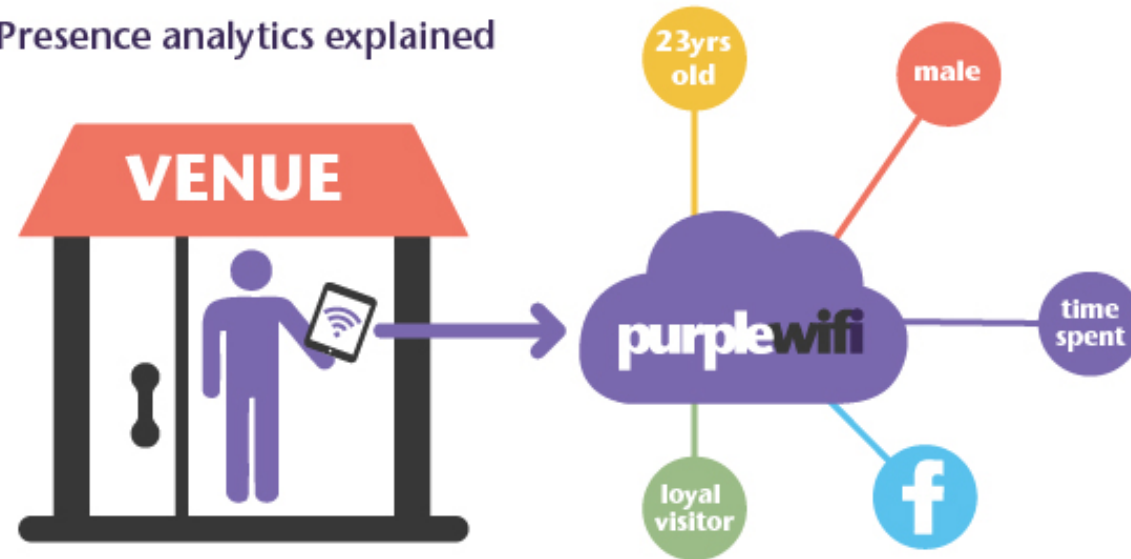
facebook

Facebook WiFi

Check In



Presence analytics explained



HOTPSOT + SOCIAL = MUTUAL BENEFIT


1. Configure RouterOS act as Hotspot server
2. Redirect request to external Captive portal
3. Set some walled gardens
4. Retrieve data from social service
5. AAA server authorize user able to access internet





DASHBOARD USER MANAGEMENT

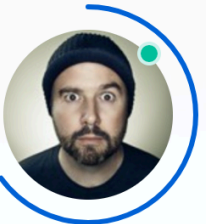
UMEGA

←

6


Hi, Matthew






Matthew Gonzalez
Designer
















MAIN

 Самбар

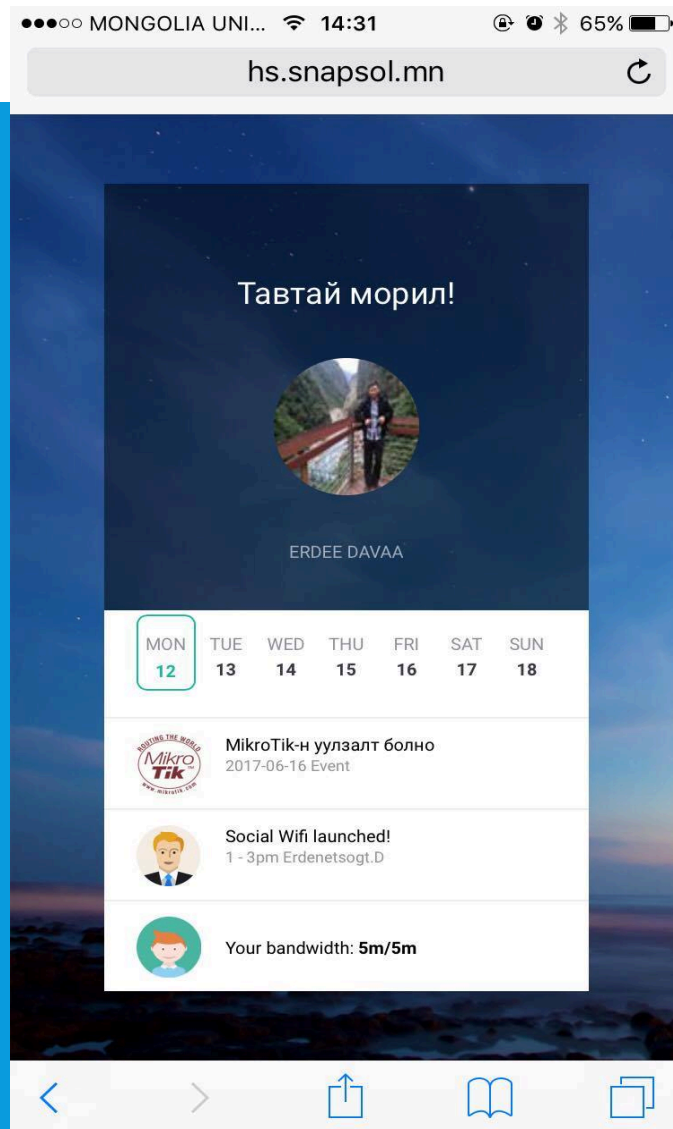
 Үйлчлүүлэгчид

Welcome to Radios System

Үйлчлүүлэгчдийн мэдээлэл

#	Хэрэглэгч	Имэйл	Сүүлд зочилсон	Нийт зочилсон	Status	...
1	 Dowell Dogood эрэгтэй	dowell.mn@gmail.com		0	Салсан	 
2	 Hottot Tottot эрэгтэй	gapu_online@yahoo.com	2017-04-17 13:17:07	1	Салсан	 
3	 Erdee Davaa эрэгтэй	erdenetsogt.d@gmail.com	2017-06-12 07:24:52	35	Идэвхитэй	 
4	 Tseegii Tselmeg эрэгтэй	tseegii.it@gmail.com	2017-06-10 21:47:23	19	Салсан	 
5	 Nomintsetseg Byambajav эмэгтэй	nomio2_b@yahoo.com	2017-06-11 23:11:15	13	Салсан	 

• <http://hs.snapsol.mn/dashboard/>



DEMONSTRATION:

SSID=RADIOS

LOGIN USING YOUR FB

THANK YOU

QUESTIONS &
SUGGESTION