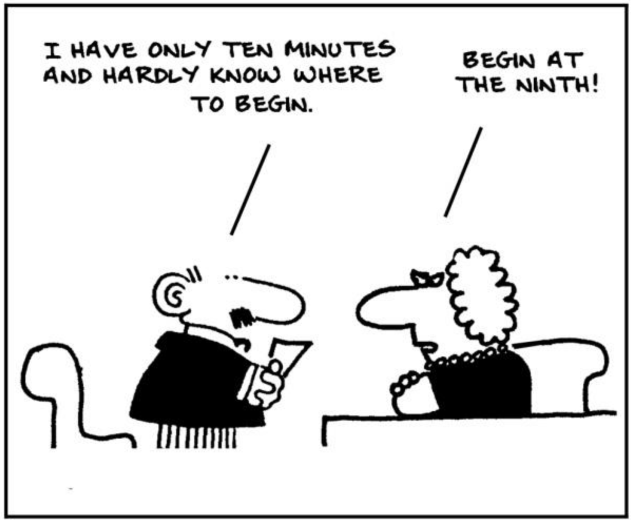
MikroTik User Meeting
Larnaca, Cyprus, 12th of June 2015

Hotspot using social accounts



Ionas Iona

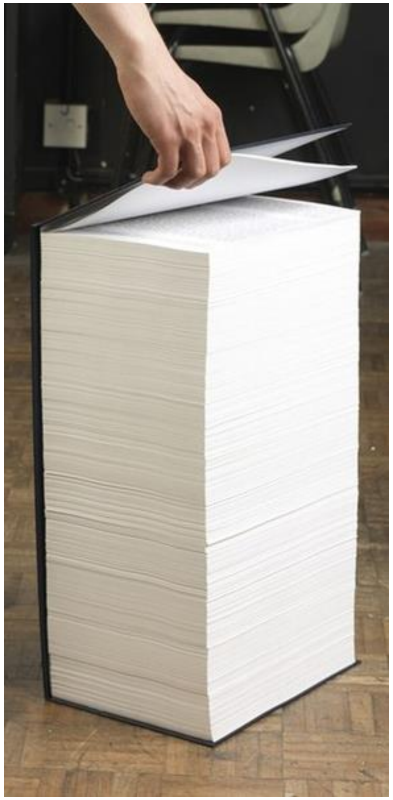
About me

Company	:	JoinMyWifi
Position	:	Co-founder, Chief Technical Officer (CTO)
Product	:	Wifi Marketing Software
Telephone number	:	+357 70009434
Email	:	ionas@joinmywifi.com
Website	:	http://www.joinmywifi.com
CV	:	http://www.joinmywifi.com/IonasCV.pdf
Education	:	National Technical University of Athens (Ethniko Metsovio Polytecnhio) Electrical & Computer Engineering department BSc & MSc in Computer Science, class of 2009
MikroTik certified	:	MTCNA, MTCWE, MTCTCE, MTCUME
MikroTik consultant	:	http://www.mikrotik.com/consultants/europe/cyprus
Hotspot presentation	:	http://www.joinmywifi.com/HotspotMUM.pdf

"I don't want yes-men around me. I want everyone to tell the truth, even if it costs them their jobs." *Samuel Goldwyn*

Agenda

- Why use MikroTik
- Hotspot concepts
- Hotspot on router vs. access points
- Pages on server vs. router
- Security issues
- Walled garden configuration
- JoinMyWifi platform
- Live demo



Configurations tested on RouterOS v6.27

Why use MikroTik

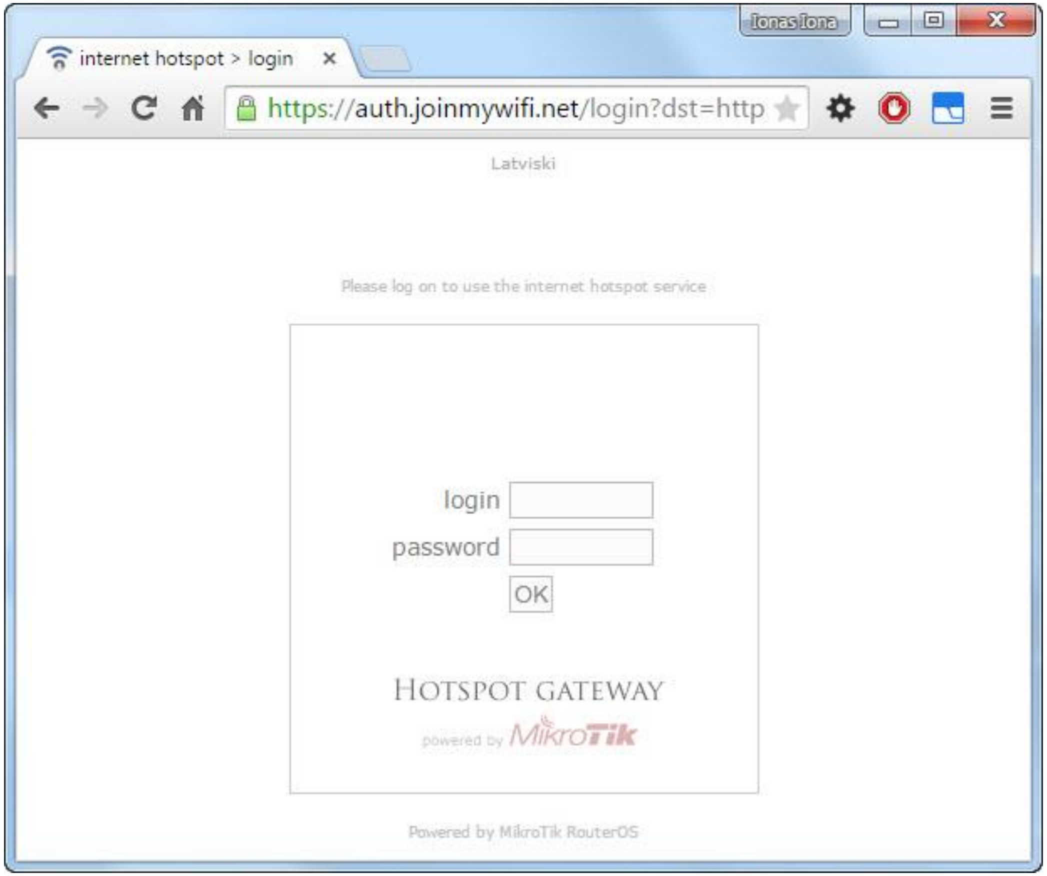
- Features we utilize with hotspot
  - Layer-7 firewall with content filtering
  - Dynamic bandwidth allocation (using PCQ)
  - Prioritize traffic (QoS)
  - Transparent web proxy (http traffic caching)
  - Transparent DNS server
  - VLAN (multiple SSIDs)
  - openVPN (secure connection with server)
  - Simple Network Management Protocol (SNMP)
  - Value for money

Hotspot concepts (1/2)

- Hotspot
  - Provides authentication for wired/wireless clients, via captive portal, before accessing the internet
- Captive portal
  - A special web-page (e.g. a login web-page) or a series of web-pages that are shown to unauthenticated users, to provide means of authentication. Only authenticated users gain full access to the internet. Unauthenticated users gain access only to the internet resources that are specified in the walled garden
- Walled garden
  - Specifies which HTTP and HTTPS resources can be accessed by unauthenticated users

Hotspot concepts (2/2)

- Default MikroTik hotspot's login web-page



Ionas Iona

internet hotspot > login

https://auth.joinmywifi.net/login?dst=http

Latviski

Please log on to use the internet hotspot service

login

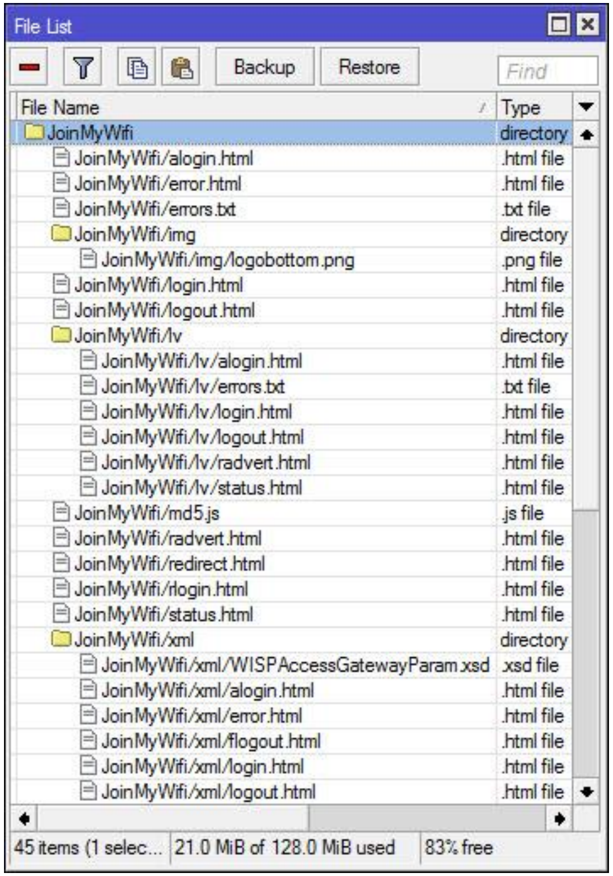
password

OK

HOTSPOT GATEWAY

powered by MikroTik

Powered by MikroTik RouterOS



File List

File Name	Type
JoinMyWifi	directory
JoinMyWifi/alogin.html	.html file
JoinMyWifi/error.html	.html file
JoinMyWifi/errors.txt	.txt file
JoinMyWifi/img	directory
JoinMyWifi/img/logobottom.png	.png file
JoinMyWifi/login.html	.html file
JoinMyWifi/logout.html	.html file
JoinMyWifi/lv	directory
JoinMyWifi/lv/alogin.html	.html file
JoinMyWifi/lv/errors.txt	.txt file
JoinMyWifi/lv/login.html	.html file
JoinMyWifi/lv/logout.html	.html file
JoinMyWifi/lv/radvert.html	.html file
JoinMyWifi/lv/status.html	.html file
JoinMyWifi/md5.js	.js file
JoinMyWifi/radvert.html	.html file
JoinMyWifi/redirect.html	.html file
JoinMyWifi/rlogin.html	.html file
JoinMyWifi/status.html	.html file
JoinMyWifi/xml	directory
JoinMyWifi/xml/WISPAccessGatewayParam.xsd	.xsd file
JoinMyWifi/xml/alogin.html	.html file
JoinMyWifi/xml/error.html	.html file
JoinMyWifi/xml/flogout.html	.html file
JoinMyWifi/xml/login.html	.html file
JoinMyWifi/xml/logout.html	.html file

45 items (1 selec... 21.0 MiB of 128.0 MiB used 83% free

Hotspot on router vs. access points (APs)

- We recommend hotspot on router
  - Centralized management
  - Advanced operating system
  - Less hardware required (Large enterprises require many APs for wifi coverage)
  - No need to replace/reconfigure current infrastructure
  - Easier/faster deployment
  - Cost effective

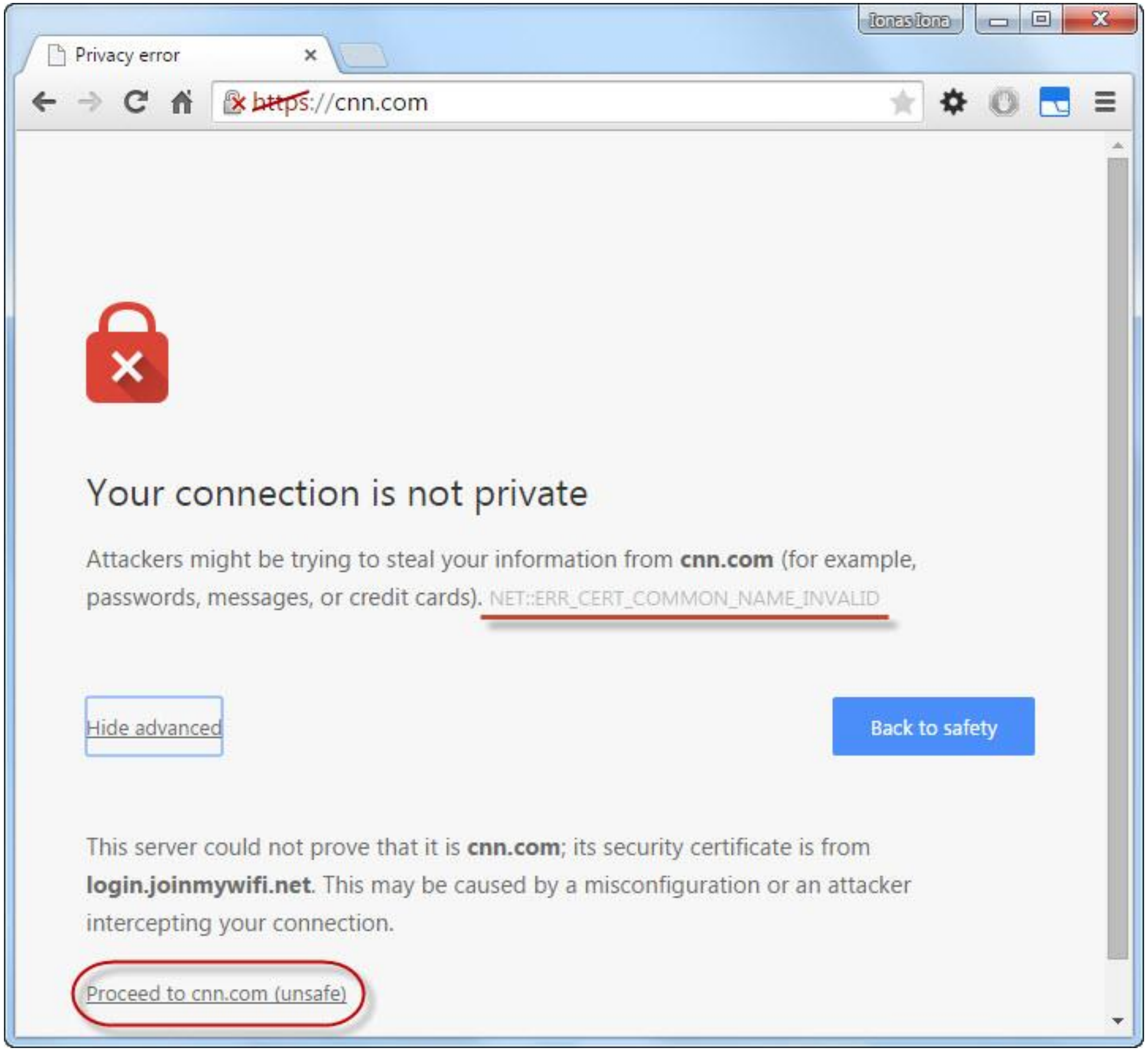
Pages on server vs. router

- We recommend pages on server. Although this approach lacks in speed, the benefits are described below
  - No need for massive updates on routers when new versions of the software are released
  - No need for router update when a client decides to change platform configuration
  - Almost all pages reside in one domain (avoiding cross side scripting issues)
  - Pages are created dynamically – Flexibility to customize pages for each user specifically
  - Source code is more manageable
  - Painless debugging
  - Smooth transition to global scale

Security issues (1/5)

- For security reasons we highly recommend to use HTTPS for ALL traffic between clients-routers-servers
- Man in the middle attack
  - When an unauthenticated user tries to visit an HTTPS site e.g. https://cnn.com the router redirects the user to the hotspot login page e.g. https://login.joinmywifi.net and sends hotspot's certificate (issued for login.joinmywifi.net), which doesn't match the certificate the browser expects (issued for cnn.com), so the browser produces a certificate error

Security issues (2/5)



Your connection is not private

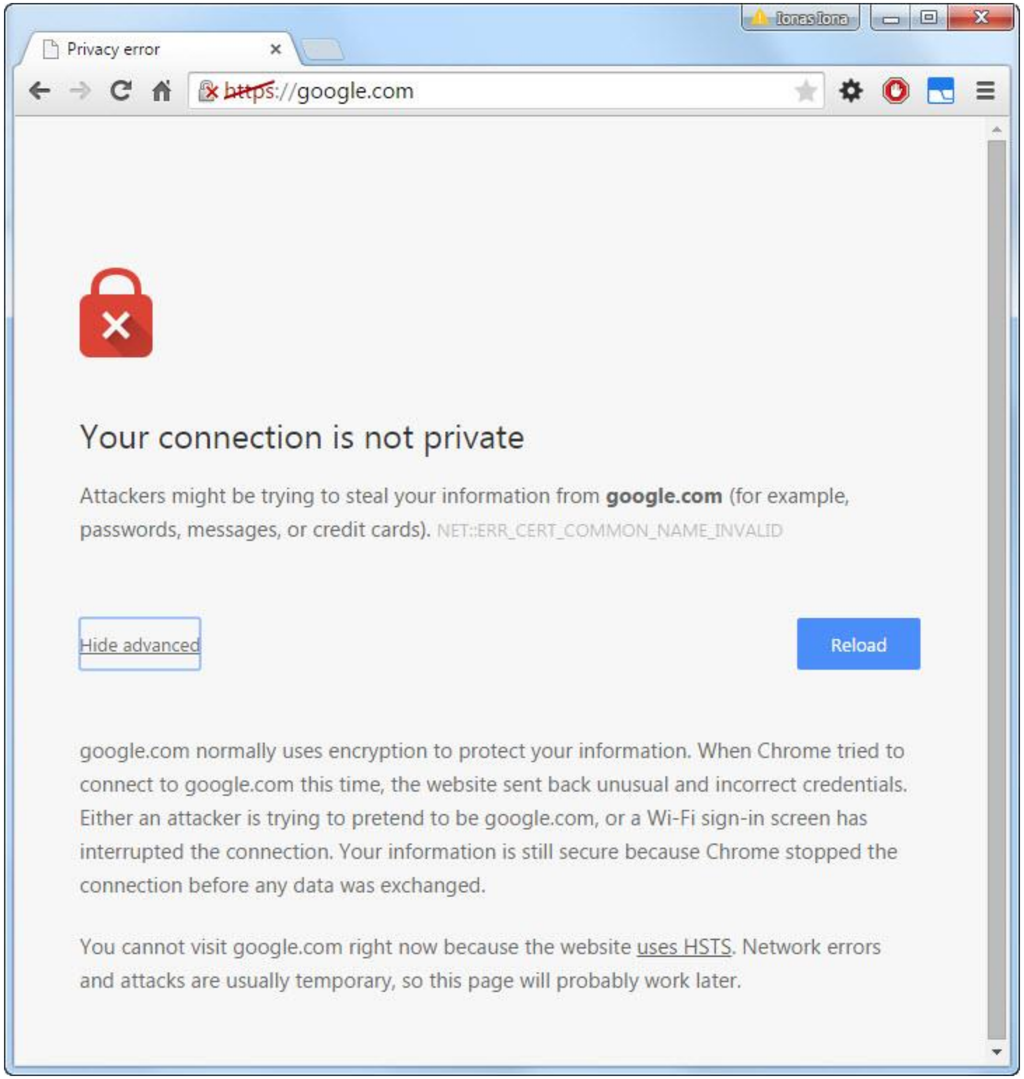
Attackers might be trying to steal your information from **cnn.com** (for example, passwords, messages, or credit cards). NET::ERR_CERT_COMMON_NAME_INVALID

This server could not prove that it is **cnn.com**; its security certificate is from **login.joinmywifi.net**. This may be caused by a misconfiguration or an attacker intercepting your connection.

Security issues (3/5)

- When such error is produced browsers give the option for proceeding anyway, except when a site is using HTTP Strict Transport Security (HSTS) and the specific browser supports it
  - for example, Chrome and Opera don’t give the option for proceeding when you try to access the below websites
    - https://google.com
    - https://youtube.com
    - https://github.com
  - but give you the option to proceed for the below websites
    - https://cnn.com
    - https://bbc.com
  - it is rare to come across this issue using Internet Explorer, Safari, Mozilla Firefox and Android browsers

Security issues (4/5)



Your connection is not private

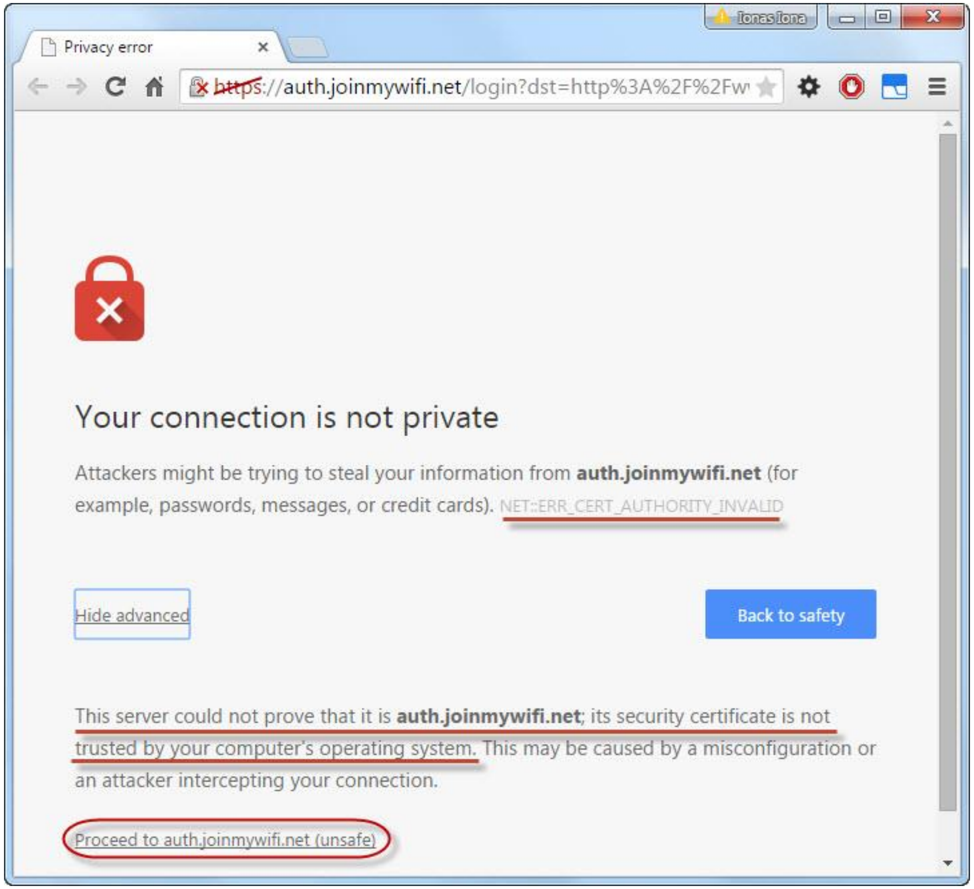
Attackers might be trying to steal your information from **google.com** (for example, passwords, messages, or credit cards). NET::ERR_CERT_COMMON_NAME_INVALID

google.com normally uses encryption to protect your information. When Chrome tried to connect to google.com this time, the website sent back unusual and incorrect credentials. Either an attacker is trying to pretend to be google.com, or a Wi-Fi sign-in screen has interrupted the connection. Your information is still secure because Chrome stopped the connection before any data was exchanged.

You cannot visit google.com right now because the website uses HSTS. Network errors and attacks are usually temporary, so this page will probably work later.

Security issues (5/5)

- Self-signed certificates will cause browsers to produce certificate authority errors, so we recommend buying certificates from trusted certification authorities (e.g. Comodo, Symantec). When such error is produced, all browsers give the option for proceeding anyway


Ionas Iona
Privacy error
~~https~~://auth.joinmywifi.net/login?dst=http%3A%2F%2Fw
Hide advanced
Back to safety
Proceed to auth.joinmywifi.net (unsafe)

Your connection is not private

Attackers might be trying to steal your information from **auth.joinmywifi.net** (for example, passwords, messages, or credit cards). NET::ERR_CERT_AUTHORITY_INVALID

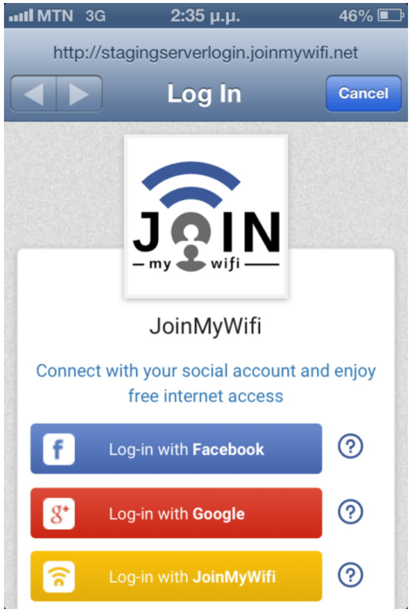
This server could not prove that it is **auth.joinmywifi.net**; its security certificate is not trusted by your computer's operating system. This may be caused by a misconfiguration or an attacker intercepting your connection.

Walled garden configuration (1/5)

- Captive portal detection
  - The moment a modern device gets connected to a network it tries to access some internet resources
    - if it receives the expected packages it assumes that you have connection to the internet
    - otherwise it assumes that you are connected to a hotspot and as a result, it pops up the default or a pseudo browser in order to follow the authentication procedure
- Problems arising when devices detect captive portal
  - Android OS devices (default pop up: Android browser)
    - if the user doesn’t authenticate successfully within a small amount of time, the device gets disconnected from the network automatically (on some Android versions)
  - iOS/OS X devices (default pop up: Safari pseudo browser)
    - if by accident the user closes the pseudo browser the device gets disconnected from the network automatically
    - if the pseudo browser tries to open a web-page inside the normal browser before the authentication process is completed the network connection is lost
    - sometimes the pseudo browser closes unexpectedly before the user completes the authentication process and thus the network connection is lost
    - the pseudo browser doesn’t save cookies so the user has to write his credentials every single time

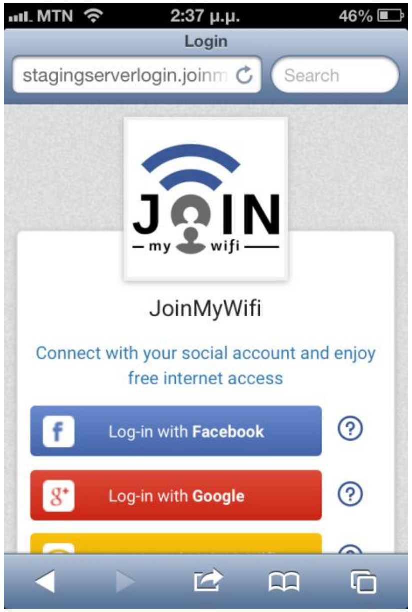
Walled garden configuration (2/5)

- One way to avoid the issues previously mentioned is to “disable” the captive portal detection. This is done by tricking each OS to assume that it has internet access, just by white listing each specific resource it searches for in the walled garden
  - The drawback of this solution is that each user will have to open a browser manually and try to visit a website for the captive portal to load



Connect with your social account and enjoy free internet access

Pseudo browser



Connect with your social account and enjoy free internet access

Default browser (Safari)

Walled garden configuration (3/5)

- Internet resources (domains) different devices are trying to access for captive portal detection
  - Android OS devices (default pop up: Android browser)
    - clients3.google.com
    - gstatic.com
  - iOS/OS X devices (default pop up: Safari pseudo browser)
    - airport.us
    - apple.com
    - apple.com.edgekey.net
    - appleiphonecell.com
    - captive.apple.com
    - gsp1.apple.com
    - ibook.info
    - itools.info
    - thinkdifferent.us
  - Windows OS devices (default pop up: IE browser)
    - ipv6.msftncsi.com
    - ipv6.msftncsi.com.edgesuite.net
    - microsoft.com
    - msftncsi.com (Windows checks if DNS server resolves this domain correctly)
    - msftncsi.com.edgesuite.net
    - teredo.ipv6.microsoft.com
    - teredo.ipv6.microsoft.com.nsatc.net

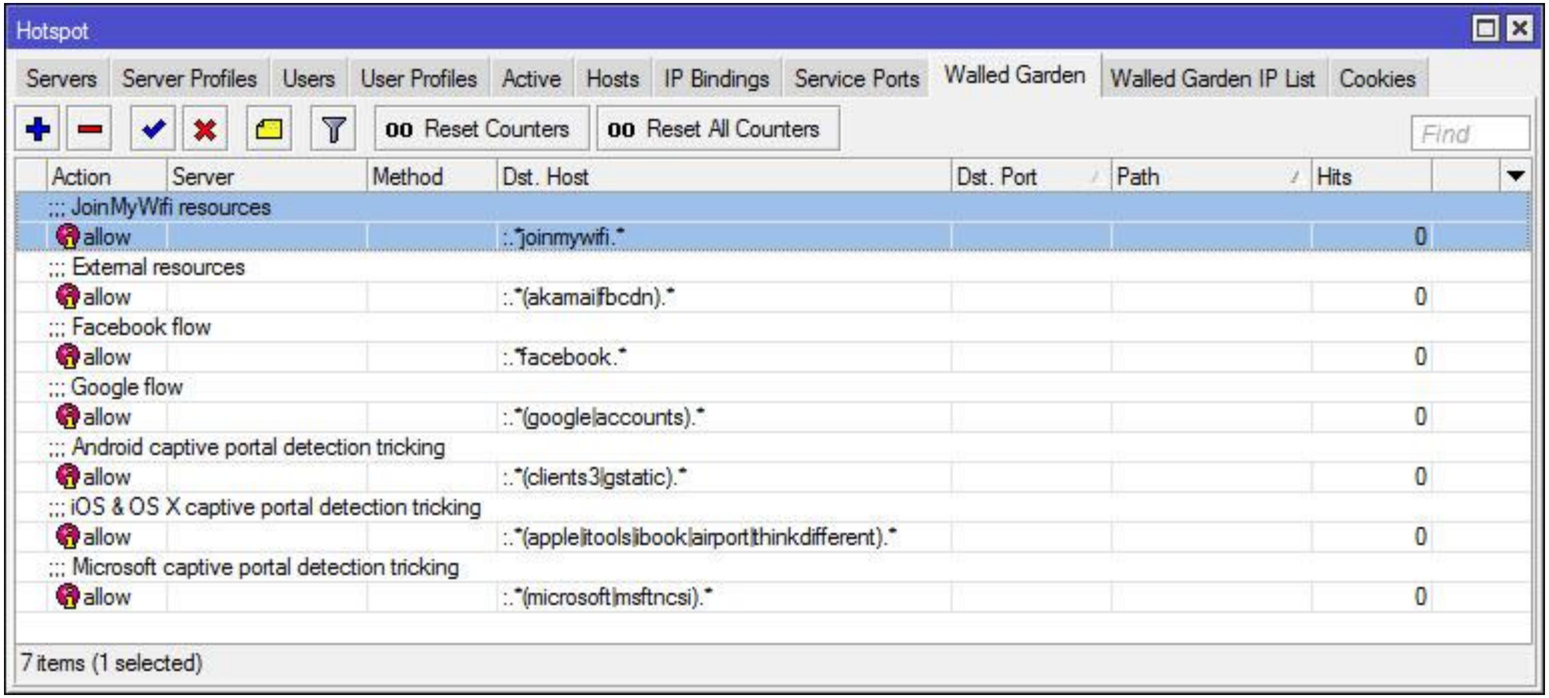
Walled garden configuration (4/5)

- If you want to provide the users the option to authenticate using their social accounts (e.g. Facebook, Google, Instagram, Twitter) you will have to white list all the internet resources (domains) needed for the authentication flow
  - Facebook flow
    - facebook.com
    - Akamai resources
    - Fbcdn resources
  - Google flow
    - accounts.google.com
    - apis.google.com
    - google.com
    - googleapis.com
    - googleusercontent.com
    - l.google.com
  - JoinMyWifi flow
    - JoinMyWifi resources
- The drawback of this approach is that once you white list those above a user will have access to Facebook and Google without the need of logging in

Walled garden configuration (5/5)

Walled garden configuration (using POSIX)

```
/ip hotspot walled-garden
add comment="JoinMyWifi resources" dst-host=":.*joinmywifi.*"
add comment="External resources" dst-host=":.*(akamai|fbcdn).*"
add comment="Facebook flow" dst-host=":.*facebook.*"
add comment="Google flow" dst-host=":.*(google|accounts).*"
add comment="Android captive portal detection tricking" dst-host=":.*(clients3|gstatic).*"
add comment="iOS & OS X captive portal detection tricking" dst-host=":.*(apple|itools|ibook|airport|thinkdifferent).*"
add comment="Microsoft captive portal detection tricking" dst-host=":.*(microsoft|msftncsi).*"
```

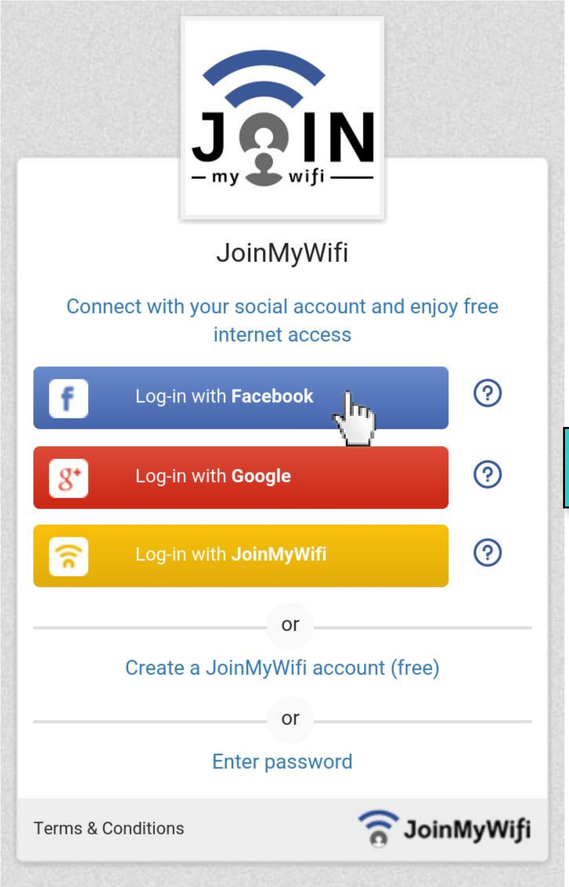


Action	Server	Method	Dst. Host	Dst. Port	Path	Hits
;;; JoinMyWifi resources						
allow			:.*joinmywifi.*			0
;;; External resources						
allow			:.*(akamai|fbcdn).*			0
;;; Facebook flow						
allow			:.*facebook.*			0
;;; Google flow						
allow			:.*(google|accounts).*			0
;;; Android captive portal detection tricking						
allow			:.*(clients3|gstatic).*			0
;;; iOS & OS X captive portal detection tricking						
allow			:.*(apple|itools|ibook|airport|thinkdifferent).*			0
;;; Microsoft captive portal detection tricking						
allow			:.*(microsoft|msftncsi).*			0

7 items (1 selected)

JoinMyWifi platform - beta version (1/4)

- Hotspot on MikroTik router with external pages (pages on server). Example of Log-in with Facebook flow



JoinMyWifi

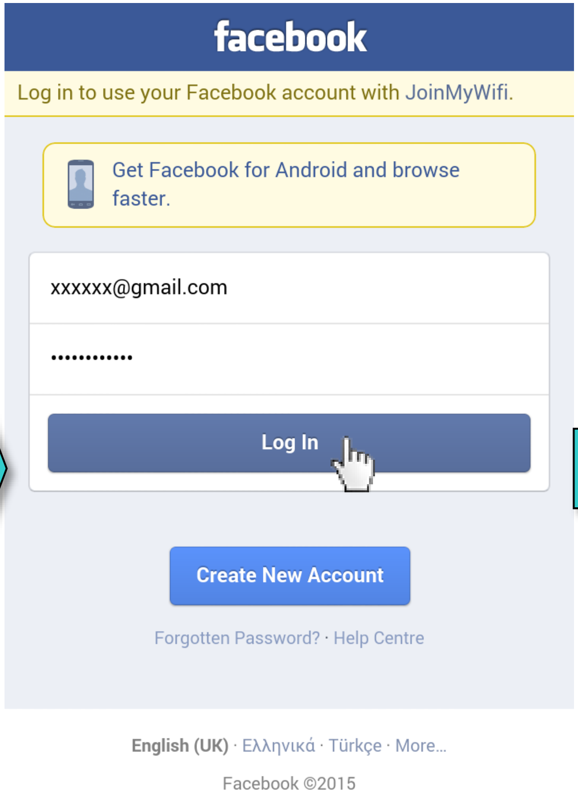
Connect with your social account and enjoy free internet access

Create a JoinMyWifi account (free)

Enter password

Terms & Conditions

Page resides on JoinMyWifi's servers



Log in to use your Facebook account with JoinMyWifi.

Get Facebook for Android and browse faster.

xxxxxx@gmail.com

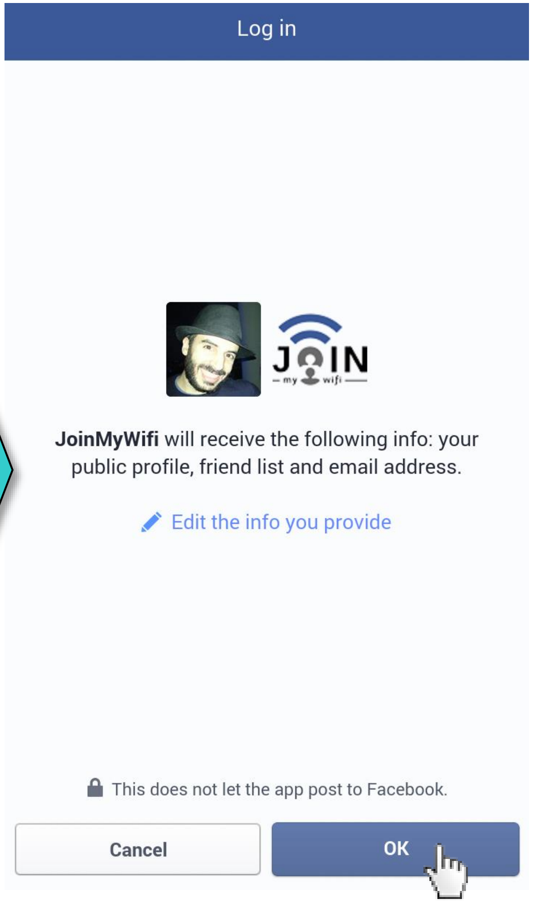
••••••••••••

Forgotten Password? · Help Centre

English (UK) · Ελληνικά · Türkçe · More...

Facebook ©2015

Page resides on Facebook 's servers



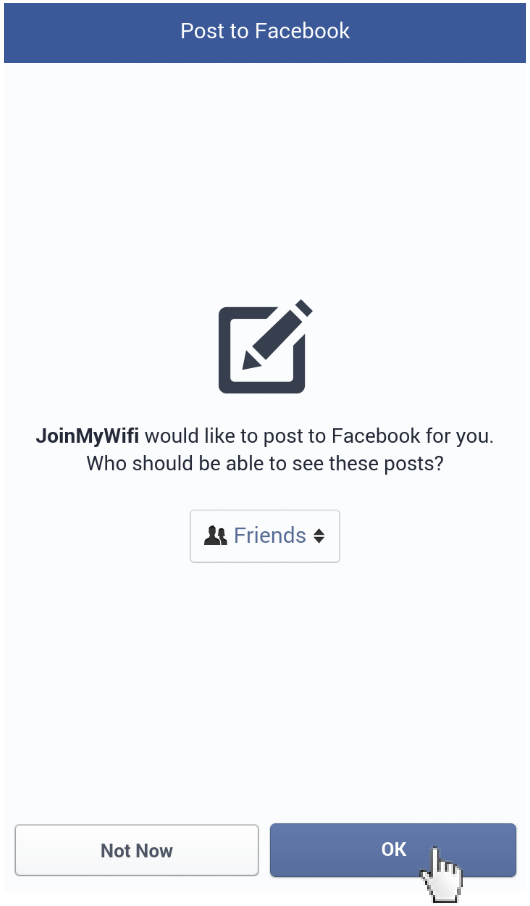
JoinMyWifi will receive the following info: your public profile, friend list and email address.

Edit the info you provide

This does not let the app post to Facebook.

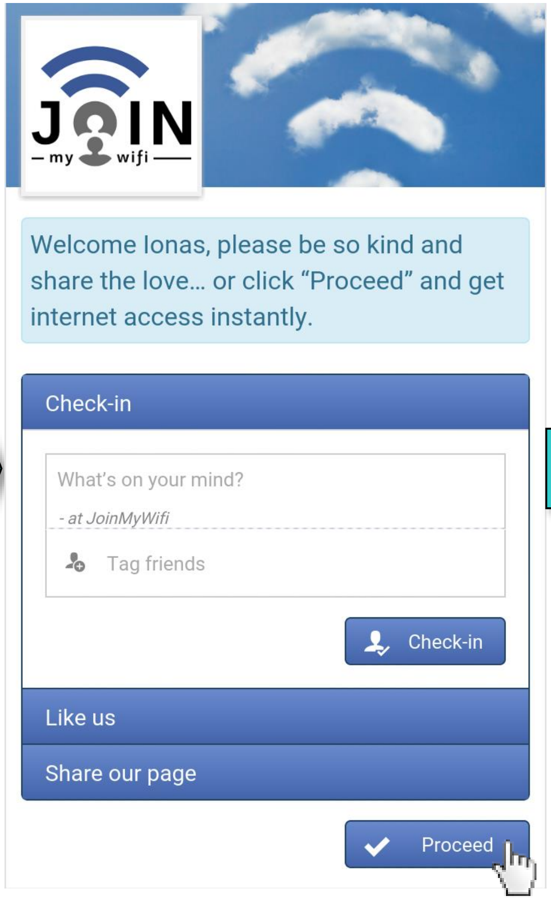
Page resides on Facebook 's servers
Shown only the first time of a user's login

JoinMyWifi platform - beta version (2/4)



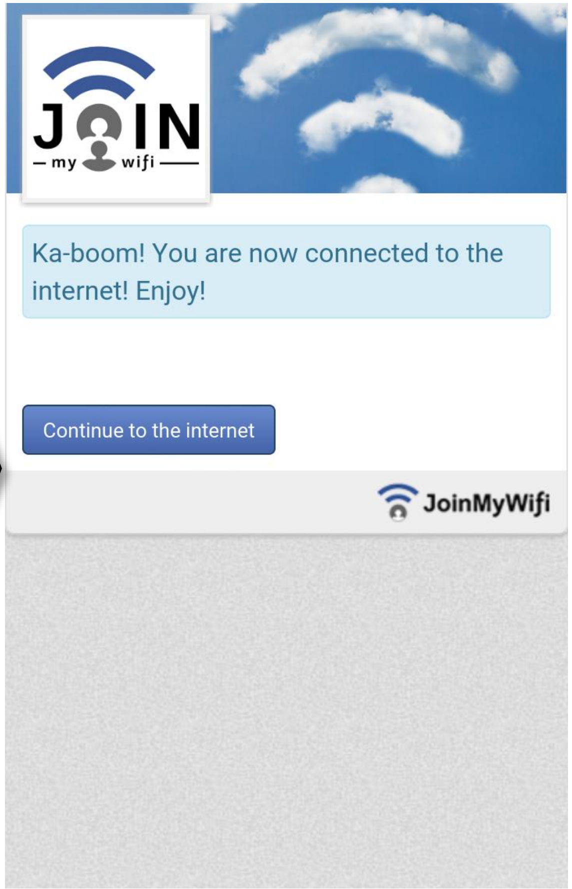
JoinMyWifi would like to post to Facebook for you. Who should be able to see these posts?

Page resides on Facebook 's servers
Shown only the first time of a user's login



Welcome Ionas, please be so kind and share the love… or click "Proceed" and get internet access instantly.

Page resides on JoinMyWifi's servers



Ka-boom! You are now connected to the internet! Enjoy!

Page resides on JoinMyWifi's servers

JoinMyWifi platform - beta version (3/4)

- Examples of use
  - Cafes
  - Bars
  - Clubs
  - Restaurants
  - Hotels
  - Airports
  - Malls
  - Anywhere there is public wifi

JoinMyWifi platform - beta version (4/4)

- Live demo
  - Let’s hope we don’t get a blue screen ☺

```
                              Windows

An exception  06 has occured at 0028:C11B3ADC in VxD DiskTSD(03) +
00001660.  This was called from 0028:C11B40C8 in VxD voltrack(04) +
00000000.  It may be possible to continue normally.

*  Press any key to attempt to continue.
*  Press CTRL+ALT+RESET to restart your computer.  You will
   lose any unsaved information in all applications.

                        Press any key to continue
```

Questions & answers

Thank you!