با نام خدا

Mikrotik Hotspot Gateway

اين نوشتار ترجمه اي ا ست آزاد ازمبحث HotSpot Gateway
از*Document revision 4.2 (Tue Jul 04 2006) و شامل* راهنماي راه اندازي Mikrotik Hotspot Gateway براي ورژن 2.9 نرم افزار است.
اين راهنما بيشتر بر نحوه راه اندازي و مديريت Hotspot تكيه دارد.
www.PersianAdmins.com

Hotspot:

Hotspot يك نقطه دسترسي عمومي است براي كامپيوترهايي كه به صورت كابلي يا بي سيم به شبكه متصل شده اند.در واقع Hotspot امكاني براي اعتبار سنجي(Authenticate) كاربران جهت اتصال به شبكه به وجود مي آورد.
ويژگي خاص Hotspot نياز نداشتن به نرم افزار و يا تنظيمات خاص سمت كاربر است كه باعث سهولت بيشتر براي كاربران معمولي مي شود.فقط كافي است در سمت كاربر يك Internet Browser وجود داشته باشد.با بازكردن مرورگر درخواستي مبتني بر ارسال صفحه وب به Hotspot فرستاده مي شود Hotspot تمام درخواست ها را به صفحه پيش فرض(Redirect(Servlet page or Login Page مي كند.(صفحه پيش فرض قابل تغيير است)،صفحه پيش فرض معمولا شامل فرم درخواست كاربر و پسورد، تبليغات يا چيزهاي اختصاصي شده ديگر است.بعد از اعتبار سنجي كاربر به صفحه دلخواهRedirect مي شود.براي خروج هم كافي است از صفحه status كه به صورت Popup باز مي شود Logout را انتخاب كنند.
امكاناتي كه ميكروتيك Hotspot فراهم مي كند:
اعتبارسنجي كاربران با استفاده از ديتابيس محلي ايجاد شده روي خود ميكروتيك و يا Radius سرور
حسابرسي كاربران با استفاده از ديتابيس محلي ايجاد شده روي خود ميكروتيك و يا Radius سرور
سيستم Walled-garden (دسترسي به بعضي از سايت ها بدون اعتبار سنجي)

راهنماي راه اندازي سريع:

در راهنماي خود ميكروتيك براي راه اندازي يك راهنماي سريع توضيح داده شده و سپس از روش پرسش و پاسخ براي توضيحات بيشتر كمك گرفته شده است.من نيز مشابه همين روش را در پيش خواهم گرفت.پس ابتدا راه اندازي سريع و سپس توضيح قسمت هاي مختلف.
توصيه مي شود براي سادگي كار ازwinbox استفاده كنيد. بعضي توضيحات را با استفاده winbox و بعضي را با command ارائه خواهم داد.
پكيج هايي كه بايد قبل از راه اندازي نصب شده باشند:
Packages required: ***hotspot***, ***dhcp***
سرويس هايي كه بايد قبل از راه اندازي Hotspot فعال كرده باشيد :
1-سرويس DNS با استفاده از كامند /ip dns
2-سرويس DHCP
3-سرويس connection tracking (/ip firewall connection tracking set enabled=yes)

براي راه اندازي Hotspot به حداقل دو كارت شبكه نياز داريد(interface) يكي Public كه به اينترنت متصل است و بايد با RADUS سرور وDNS سرور ارتباط داشته باشد دومي Local كه كاربرهاي Hotspot به آن متصل شوند.روي هر Interface امكان راه اندازي فقط يك Hotspot سرور وجود دارد.پس مي توانيد در آن واحد Hotspot هاي

مختلفي داشته باشيد روي Interface هاي جداگانه.لازم به توضيح است براي راه اندازي Hotspot بي سيم نيازي نيست حتما از كارت شبكه بي سيم استفاده شود مي توانيد يك كارت شبكه به سيستم وصل كنيد و هر AP را مايليد به آن متصل كنيد.نگران سازگاري نباشيد.سازگاري فقط در مورد كارت هاي شبكه بي سيم متصل به MT (Mikrotik Router OS) مهم است.

براي فعال كردن Hotspot روي Local Interface بايد از يك Address Pool مشابه با DHCPسرور راه اندازي شده استفاده كنيد.

/ip hotspot add interface=local address-pool=dhcp-pool-1

در نهايت براي راه اندازي كافي است يك كاربر ايجاد كنيد:

/ip hotspot user add name=admin

اكنون Hotspot راه اندازي شده است.

در سمت كلاينت بايد تنظيمات TCP/IP را انجام دهيد.به صورت پيش فرض تنظيم روي اتوماتيك قرار دارد و همين براي گرفتن يك IP از MT كفايت مي كند ولي توصيه مي شود براي مديريت بهتر در مورد پهناي باند از IP استاتيك استفاده كنيد.يك IPدر رنج Local Interface به كارت شبكه كلاينت اختصاص دهيد،DNS وGateway سرورMT را بدهيد.ميتوانيد با باز كردن مرورگر روي يك كامپيوتر كه به Interface localمتصل شده است از اين موضوع مطمئن شويد.بايد صفحه خوشامدگويي Hotspot به نمايش درآيد.

به صورت پيش فرض در هنگام اتصال كاربران يك رول مبتي بر NAT در قسمت ip firewall/Nat به صورت دايناميك ايجاد مي شود.در صورت ايجاد نشدن بايد Public Interface را Nat كنيد.

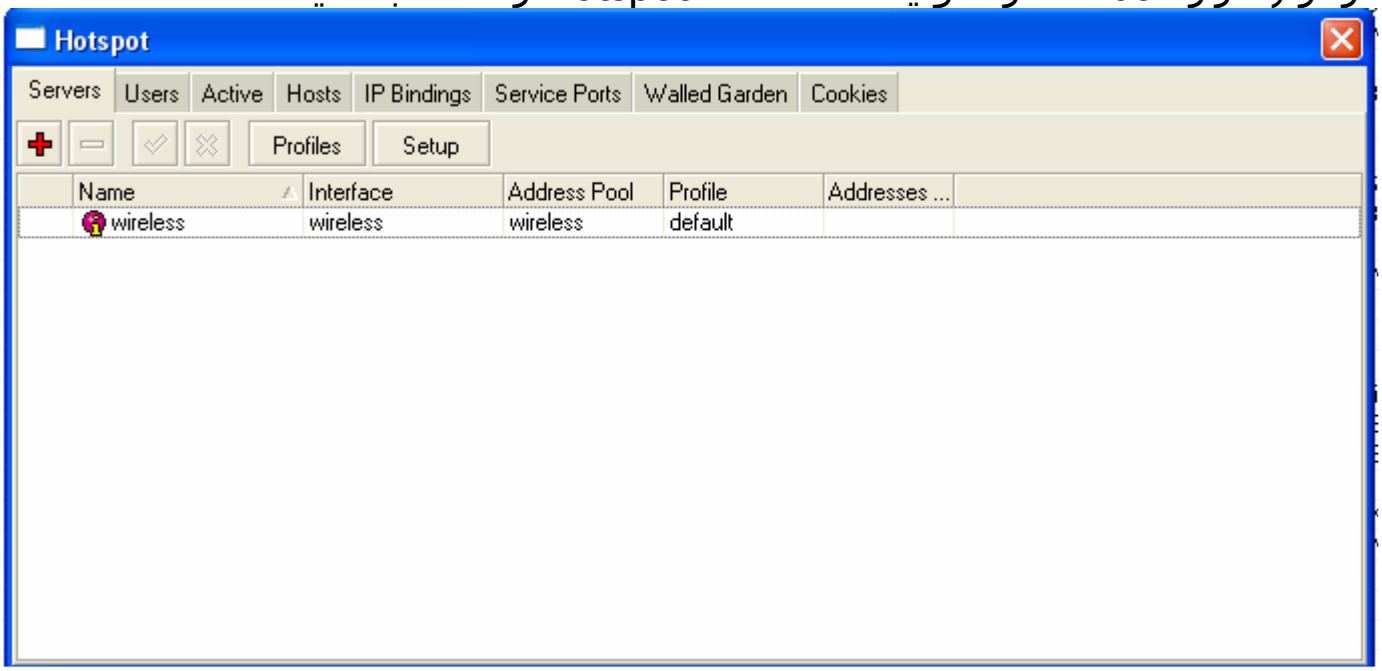
ip firewall nat> add chain=srcnat action=masquerade out-interface=Public

مديريت Hotspot

قسمت مديريت را با استفاده از winbox توضيح خواهم داد.

توضيحات ساده و يا بسيار فني به زبان اصلي درج خواهد شد.

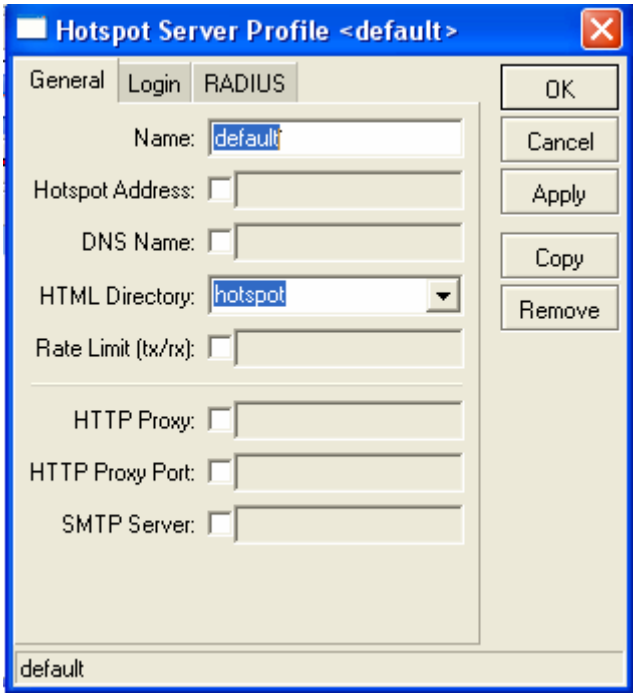
در نرم افزار winbox از منوي IP قسمت Hotspot را انتخاب كنيد.



براي مثال من در اينجا يك سرور Hotspot با نام wireless روي wireless Interface و با address pool با مشخصه wireless ايجاد كرده ام.
گزينه setup يك ويزارد ساده براي راه اندازي سرور Hotspot ايجاد مي كند.در صورتي كه هنوز سرور را راه اندازي نكرده ايد مي توانيد از اين گزينه استفاده كنيد.اين گزينه تمام اطلاعات لازم براي راه اندازي را از شما سوال كرده و در نهايت سرور را راه اندازي خواهد كرد.

address pool of network (*name*) - IP address pool for the HotSpot network
dns name (*text*) - DNS domain name of the HotSpot gateway (will be statically configured on the local DNS proxy
dns servers (*IP address*,[*IP address*]) - DNS servers for HotSpot clients
hotspot interface (*name*) - interface to run HotSpot on
ip address of smtp server (*IP address*; default: **0.0.0.0**) - IP address of the SMTP server to redirect SMTP requests (TCP port 25) to
0.0.0.0 - no redirect
local address of network (*IP address*; default: **10.5.50.1/24**) - HotSpot gateway address for the interface
masquerade network (yes | no; default: **yes**) - whether to masquerade the HotSpot network
name of local hotspot user (*text*; default: **admin**) - username of one automatically created user
passphrase (*text*) - the **passphrase** of the certificate you are importing
password for the user (*text*) - password for the automatically created user
select certificate (*name* | none import-other-certificate) - choose SSL certificate from the list of the imported certificates
none - do not use SSL
import-other-certificate - setup the certificates not imported yet, and ask this question again

گزينه Profiles امكاني براي تنظيمات همزمان سرورهاي مختلف ايجاد مي كند.براي مثال شما چند پروفايل با تنظيمات مختلف ايجاد مي كنيد.سپس سرورهاي مختلف Hotspot را به هر كدام كه مايل باشد ارجاع مي دهيد و نيازي به تنظيم جداگانه هر سرور نخواهيد داشت سواي آن بسياري از تنظيمات كليدي و اساسي Hotspot در همين جا انجام خواهد گرفت.
براي نمونه پروفايل default را بررسي مي كنيم:



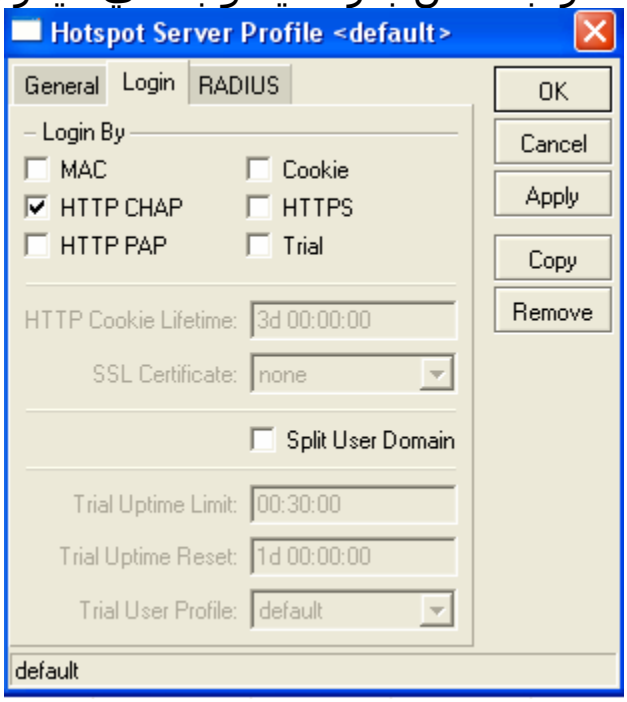
Submenu level: ***/ip hotspot profile***

Property Description

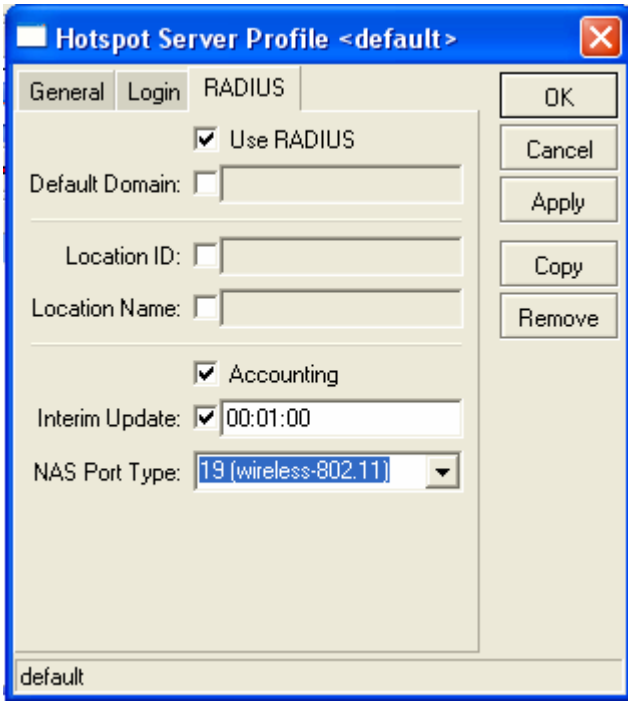
dns-name (*text*) - DNS name of the HotSpot server. This is the DNS name used as the name of the HotSpot server (i.e., it appears as the location of the login page). This name will automatically be added as a static DNS entry in the DNS cache
hotspot-address (*IP address*; default: **0.0.0.0**) - IP address for HotSpot service
html-directory (*text*; default: **""**) - name of the directory (accessible with FTP), which stores the HTML servlet pages (when changed, the default pages are automatically copied into specified directory if it does not exist already)
http-cookie-lifetime (*time*; default: **3d**) - validity time of HTTP cookies
http-proxy (*IP address*; default: **0.0.0.0**) - the address of the proxy server the HotSpot service will use as a proxy server for all those requests intercepted by Universal Proxy system and not defined in the **/ip proxy direct** list. If not specified, the address defined in **parent-proxy** parameter of **/ip proxy**. If that is absent too, the request will be resolved by the local proxy
login-by (*multiple choice:* cookie | http-chap | http-pap | https | mac | trial; default: **cookie,http-chap**) - which authentication methods to use
cookie - use HTTP cookies to authenticate, without asking user credentials. Other method will be used in case the client does not have cookie, or the stored username and password pair are not valid anymore since the last authentication. May only be used together with other HTTP authentication methods (HTTP-PAP, HTTP-CHAP or HTTPS), as in the other case there would be no way for the cookies to be generated in the first place
http-chap - use CHAP challenge-response method with MD5 hashing algorithm for hashing passwords. This way it is possible to avoid sending clear-text passwords over an insecure network. This is the default authentication method
http-pap - use plain-text authentication over the network. Please note that in case

this method will be used, your user passwords will be exposed on the local networks, so it will be possible to intercept them
https - use encrypted SSL tunnel to transfer user communications with the HotSpot server. Note that in order this to work, a valid certificate must be imported into the router (see a separate manual on certificate management)
mac - try to use client's MAC address first as its username. If the matching MAC address exists in the local user database or on the RADIUS server, the client will be authenticated without asking to fill the login form
trial - does not require authentication for a certain amount of time
radius-accounting (yes | no; default: **yes**) - whether to send RADIUS server accounting information on each user once in a while (the "while" is defined in the **radius-interim-update** property)
radius-default-domain (*text*; default: **""**) - default domain to use for RADIUS requests. It allows to select different RADIUS servers depending on HotSpot server profile, but may be handful for single RADIUS server as well.
radius-interim-update (*time* | received; default: **received**) - how often to sent cumulative accounting reports.
0s - same as **received**
received - use whatever value received from the RADIUS server
rate-limit (*text*; default: **""**) - Rate limitation in form of **rx-rate[/tx-rate] [rx-burst-rate[/tx-burst-rate] [rx-burst-threshold[/tx-burst-threshold] [rx-burst-time[/tx-burst-time]]]]** from the point of view of the router (so "rx" is client upload, and "tx" is client download). All rates should be numbers with optional 'k' (1,000s) or 'M' (1,000,000s). If tx-rate is not specified, rx-rate is as tx-rate too. Same goes for tx-burst-rate and tx-burst-threshold and tx-burst-time. If both rx-burst-threshold and tx-burst-threshold are not specified (but burst-rate is specified), rx-rate and tx-rate is used as burst thresholds. If both rx-burst-time and tx-burst-time are not specified, 1s is used as default
smtp-server (*IP address*; default: **0.0.0.0**) - default SMTP server to be used to redirect unconditionally all user SMTP requests to
split-user-domain (yes | no; default: **no**) - whether to split username from domain name when the username is given in "user@domain" or in "domain\user" format
ssl-certificate (*name* | none; default: **none**) - name of the SSL certificate to use for HTTPS authentication. Not used for other authentication methods
trial-uptime (*time*/*time*; default: **30m/1d**) - is used only when authentication method is trial. Specifies the amount of time the user identified by MAC address can use hotspot services without authentication and the time, that has to pass that the user is allowed to use hotspot services again
trial-user-profile (*name*; default: **default**) - is used only only when authentication method is trial. Specifies user profile, that trial users will use
use-radius (yes | no; default: **no**) - whether to use RADIUS to authenticate HotSpot users

نكاتي مهمي كه در اينجا به نظر مي رسد:
در قسمت General گزينه Html Directory مكان قرار گرفتن فايل هاي وب Login Page است.
بنابراين اين امكان وجود دارد كه سرورهاي مجزاي Hotspot login Page هاي متفاوتي داشته باشند.براي استفاده از اين گزينه بايد با نحوه كپي كردن فايل ها در MT با استفاده ازFTP و يا Winbox آشنا باشيد.
در قسمت Rate limit اين امكان وجود دارد كه پهناي باند كل يك سرور Hotspot را محدود كنيد.
در قسمت HTTP Proxy مي توانيد پروكسي سرور مورد استفاده اين Hotspot را مشخص كنيد.
پس مي توانيد از پروكسي هاي مختلف براي سرورهاي مختلف استفاده كنيد.
مثلا بعضي از Hotspot ها را به كش بفرستيد و بعضي ديگر را ...

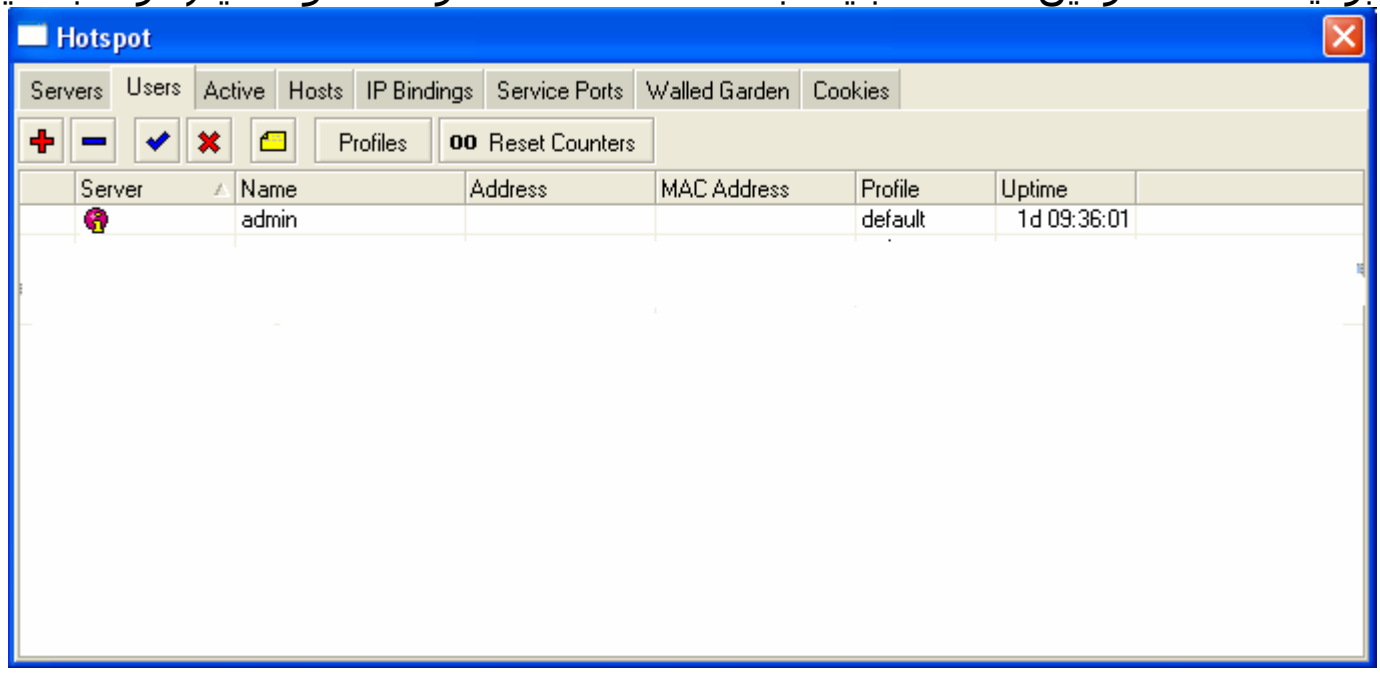


در قسمت Login نوع اعتبار سنجي كاربران را مشخص مي كنيد.محدود به نوع خاصي نيستيد و مي توانيد چند روش را همزمان انتخاب كنيد.
براي مثال براي كاربرهاي LAN كه شناخته شده هستند مي توانيد فقط از MAC استفاده كنيد و براي كاربرهاي Wireless از TTP chap اگر كلاينتي داريد كه Windows 98 و ماقبل روي آن نصب شده مجبوريد از نوع HTTP PAP استفاده كنيد.
توصيه مي كنم اگر از Radius سرور جهت اكانتينگ استفاده مي كنيد روش cookie را از كار بياندازيد.
روش Trial امكاني براي كاربرهايي است كه قصد تست سرويس Hotspot شما را دارند.تنظيم هاي آن در قسمت هاي ديگر قابل انجام است.توجه داشته باشيد كه اين روش حتما بايد با روش هاي ديگر توامان انجام گيرد.



در قسمت Radius مشخص مي كنيد كه اين سرور براي اعتبار سنجي و حسابرسي از Radius استفاده كند يا نه.اگر براي اكانتينگ از Radius سرور استفاده مي كنيد بايد تيك Accounting را بزنيد نكته مهم قسمت Interim Update است.اين قسمت را بايد طبق تنظيمات Radius سرور خود انجام دهيد و الا كاربرهاي شما از ليست Online User ها در نرم افزار Radius حذف مي شوند در حالي كه هنوز متصل هستند.

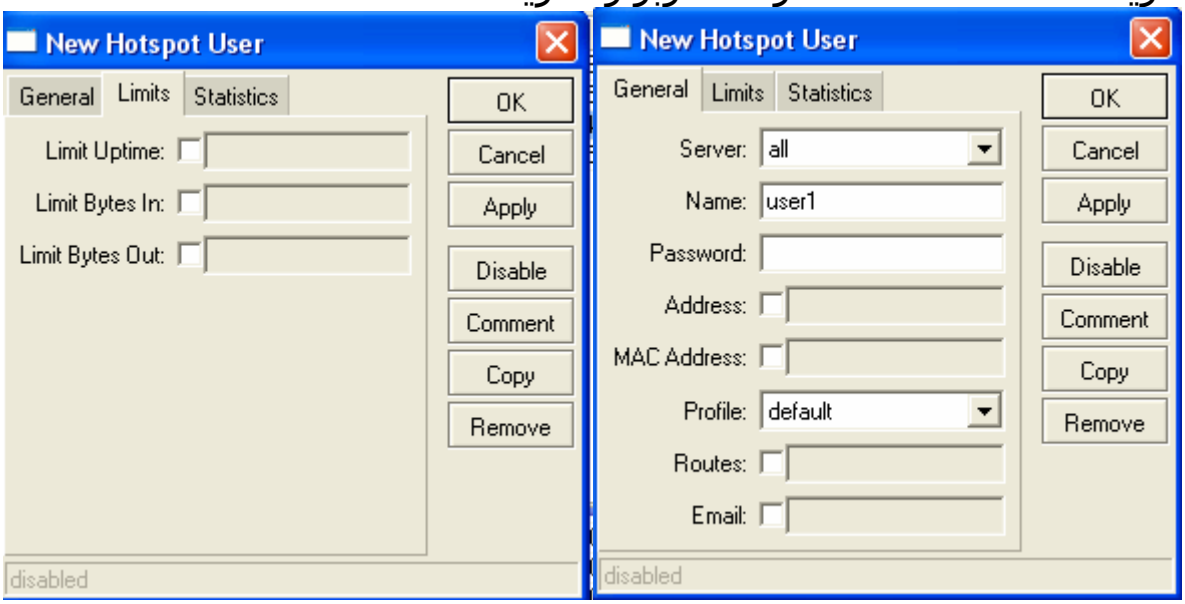
براي استفاده از اين قسمت بايد قبلا قسمت Radius را فعال و تنظيم كرده باشيد.



در قسمت Users مي تونيد كاربرهاي محلي ايجاد كنيد و آنها را به پروفايل هاي كاربر ارجاع دهيد.پروفايل در اين قسمات همان نقش قبلي را به عهده دارند.

نكاتي كه بايد مد نظر قرار دهيد اين است كه هميشه كاربرهاي ديتابيس محلي به كاربرهاي كه از Radius وارد مي شوند اولويت دارند بنابراين اگر يوزي هم در MT و هم در Radius سرور تعريف شده باشد كاربر از ديتابيس محلي وارد مي شود.

ديگر اينكه يوزهايي كه از Radius وارد مي شوند به پروفايل Defaul ارجاع داده مي شوند بنابراين راهي براي ايجاد پروفايل خاص براي كاربران Radius وجود ندارد(احتمالا)
با فشردن گزينه + امكان اضافه كردن كاربر را داريد.



HotSpot Users

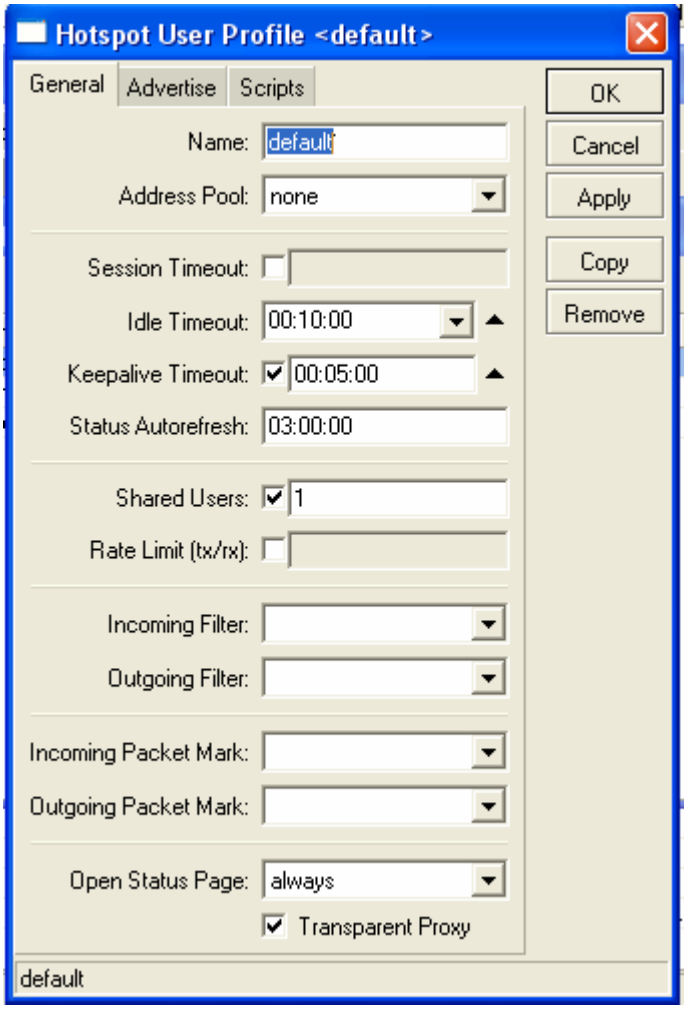
Submenu level: ***/ip hotspot user***

Property Description

address (*IP address*; default: **0.0.0.0**)- static IP address. If not **0.0.0.0**, client will always get the same IP address. It implies, that only one simultaneous login

for that user is allowed. Any existing address will be replaced with this one using the embedded one-to-one NAT
bytes-in (*read-only: integer*) - total amount of bytes received from user
bytes-out (*read-only: integer*)- total amount of bytes sent to user
limit-bytes-in (*integer*; default: **0**)- maximum amount of bytes user can transmit (i.e., bytes received from the user)
0 - no limit
limit-bytes-out (*integer*; default: **0**) - maximum amount of bytes user can receive (i.e., bytes sent to the user)
0 - no limit
limit-uptime (*time*; default: **0s**) - total uptime limit for user (pre-paid time)
0s - no limit
mac address (*MAC address*; default: **00:00:00:00:00:00**) - static MAC address. If not **00:00:00:00:00:00**, client is allowed to login only from that MAC address
name (*name*)- user name. If authentication method is trial, then user name will be set automaticly after following pattern "T-MAC_adress", where MAC_address is trial user Mac address
packets-in (*read-only: integer*)- total amount of packets received from user (i.e., packets received from the user)
packets-out (*read-only: integer*)- total amount of packets sent to user (i.e., packets sent to the user)
password (*text*)- user password
profile (*name*; default: **default**) - user profile
routes (*text*) - routes that are to be registered on the HotSpot gateway when the client is connected. The route format is: "dst-address gateway metric" (for example, "10.1.0.0/24 10.0.0.1 1"). Several routes may be specified separated with commas
server (*name* | all; default:**all**)- which server is this user allowed to log in to
uptime (*read-only: time*)- total time user has been logged in

ايجاد محدوديت حجمي براي كاربر را بايد در اين قسمت انجام دهيد.توانايي محدود كردن زمان آنلاين بودن كاربر را هم دارا هستيد.



پروفايل default را بررسي مي كنيم:

HotSpot User Profiles

Submenu level: ***/ip hotspot user profile***

Description

HotSpot User profiles are used for common user settings. Profiles are like user groups, they are grouping users with the same limits.

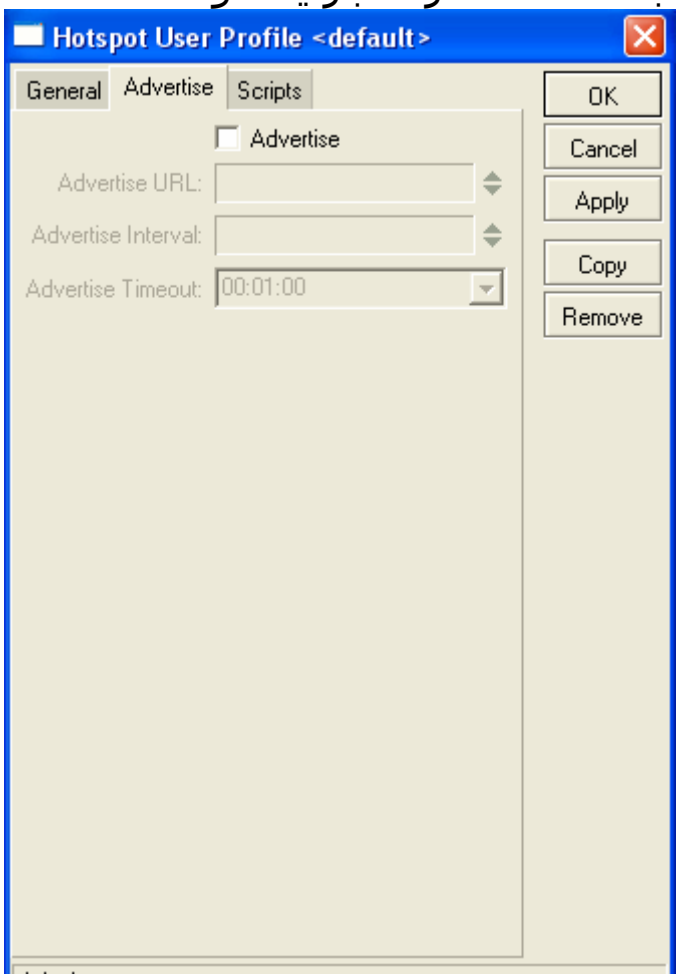
Property Description

address-pool (*name* | none; default: **none**) - the IP poll name which the users will be given IP addresses from. This works like **dhcp-pool** method in earlier versions of MikroTik RouterOS, except that it does not use DHCP, but rather the embedded one-to-one NAT
none - do not reassign IP addresses to the users of this profile
advertise (yes | no; default: **no**) - whether to enable forced advertisement popups for this profile
advertise-interval (*multiple choice: time*; default: **30m,10m**) - set of intervals between showing advertisement popups. After the list is done, the last value is used for all further advertisements

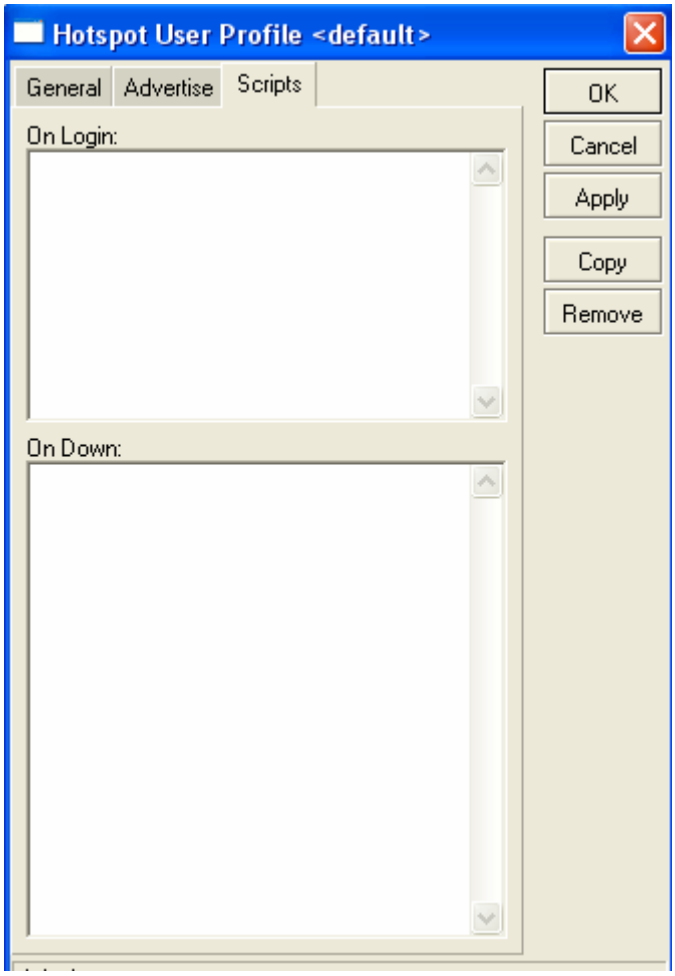
advertise-timeout (*time* | immediately never; default: **1m**) - how long to wait for advertisement to be shown, before blocking network access with walled-garden
advertise-url(*multiple choice: text*; default: **http://www.mikrotik.com/,http://www.routerboard.com/**) - list of URLs to show as advertisement popups. The list is cyclic, so when the last item reached, next time the first is shown
idle-timeout (*time* | none; default: **none**) - idle timeout (maximal period of inactivity) for authorized clients. It is used to detect, that client is not using outer networks (e.g. Internet), i.e., there is NO TRAFFIC coming from that client and going through the router. Reaching the timeout, user will be logged out, dropped of the host list, the address used by the user will be freed, and the session time accounted will be decreased by this value
none - do not timeout idle users
incoming-filter (*name*) - name of the firewall chain applied to incoming packets from the users of this profile
incoming-packet-mark (*name*) - packet mark put on all the packets from every user of this profile automatically
keepalive-timeout (*time* | none; default: **00:02:00**) - keepalive timeout for authorized clients. Used to detect, that the computer of the client is alive and reachable. If check will fail during this period, user will be logged out, dropped of the host list, the address used by the user will be freed, and the session time accounted will be decreased by this value
none - do not timeout unreachable users
name (*name*) - profile reference name
on-login (*text*; default: **""**) - script name to launch after a user has logged in
on-logout (*text*; default: **""**) - script name to launch after a user has logged out
open-status-page (always | http-login; default: **always**) - whether to show status page also for users authenticated using mac login method. Useful if you want to put some information (for example, banners or popup windows) in the alogin.html page so that all users would see it
http-login - open status page only in case of http login (including cookie and https login methods)
always - open http status page in case of mac login as well
outgoing-filter (*name*) - name of the firewall chain applied to outgoing packets to the users of this profile
outgoing-packet-mark (*name*) - packet mark put on all the packets to every user of this profile automatically
rate-limit (*text*; default: **""**) - Rate limitation in form of **rx-rate[/tx-rate] [rx-burst-rate[/tx-burst-rate] [rx-burst-threshold[/tx-burst-threshold] [rx-burst-time[/tx-burst-time] [priority] [rx-rate-min[/tx-rate-min]]]]** from the point of view of the router (so "rx" is client upload, and "tx" is client download). All rates should be numbers with optional 'k' (1,000s) or 'M' (1,000,000s). If tx-rate is not specified, rx-rate is as tx-rate too. Same goes for tx-burst-rate and tx-burst-threshold and tx-burst-time. If both rx-burst-threshold and tx-burst-threshold are not specified (but burst-rate is specified), rx-rate and tx-rate is used as burst thresholds. If both rx-burst-time and tx-burst-time are not specified, 1s is used as default. Priority takes

values 1..8, where 1 implies the highest priority, but 8 - the lowest. If rx-rate-min and tx rate-min are not specified rx-rate and tx-rate values are used. The rx-rate-min and tx rate-min values can not exceed rx-rate and tx-rate values.
session-timeout (*time*; default: **0s**) - session timeout (maximal allowed session time) for client. After this time, the user will be logged out unconditionally
0 - no timeout
shared-users (*integer*; default: **1**) - maximal number of simultaneously logged in users with the same username
status-autorefresh (*time* | none; default: **none**) - HotSpot servlet status page autorefresh interval
transparent-proxy (yes | no; default: **yes**) - whether to use transparent HTTP proxy for the authorized users of this profile

نكاتي كه در اين قسمت نياز به توضيح دارند:
در قسمت GeneralگزينهAutorefresh مشخص مي كند كه چه زماني صفحه popup نمايش داده شده به كاربر كه وضعيت كاربر را مشخص مي كند به روز شود.پيش فرض اين گزينه 1 دقيقه است بهتر است انرا به يك ساعت يا بالاتر افزايش دهيد.به روز شدن اين صفحه كاربرد زيادي ندارد.ولي زمان پايين بروز شدن مي تواند كاربراني كه گيم از طريق اينترنت انجام مي دهند به شدت تحت تاثير قرار دهد و حتي باعث هنگ كردن بازي شود.

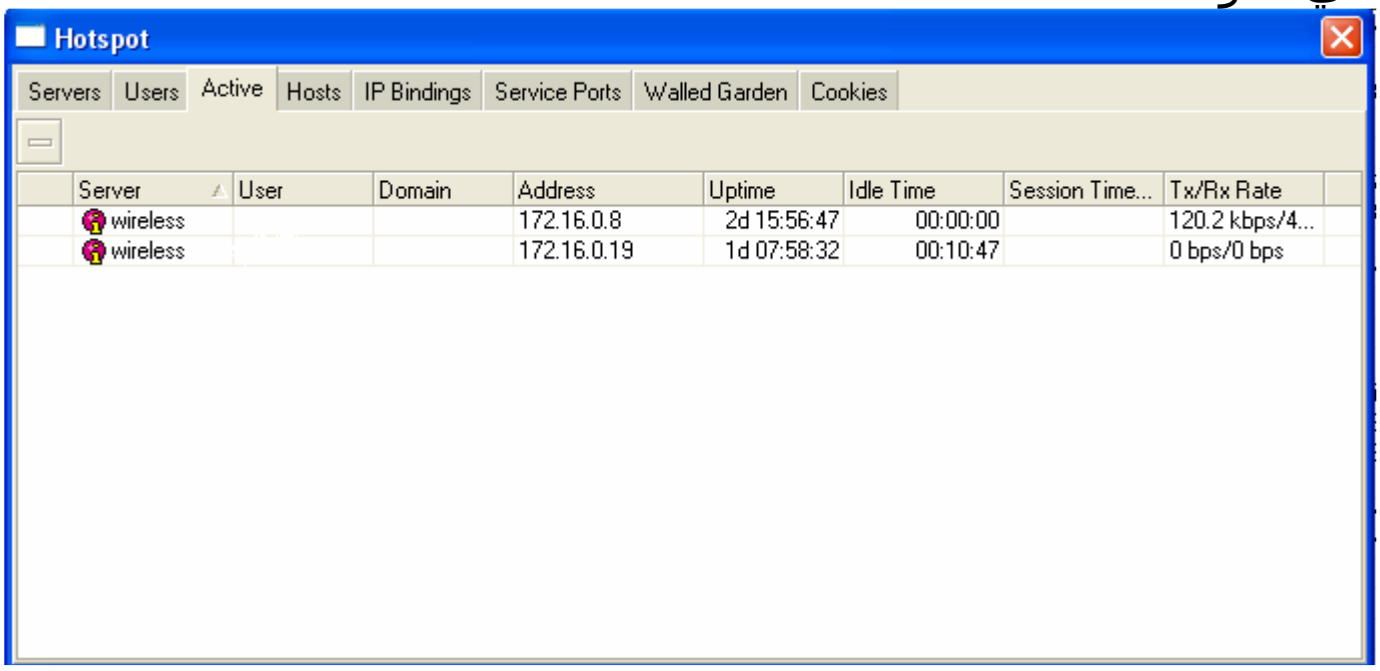


قسمت Advertise براي نشان دادن تبليغات به كاربر در زمانهاي خاص است.

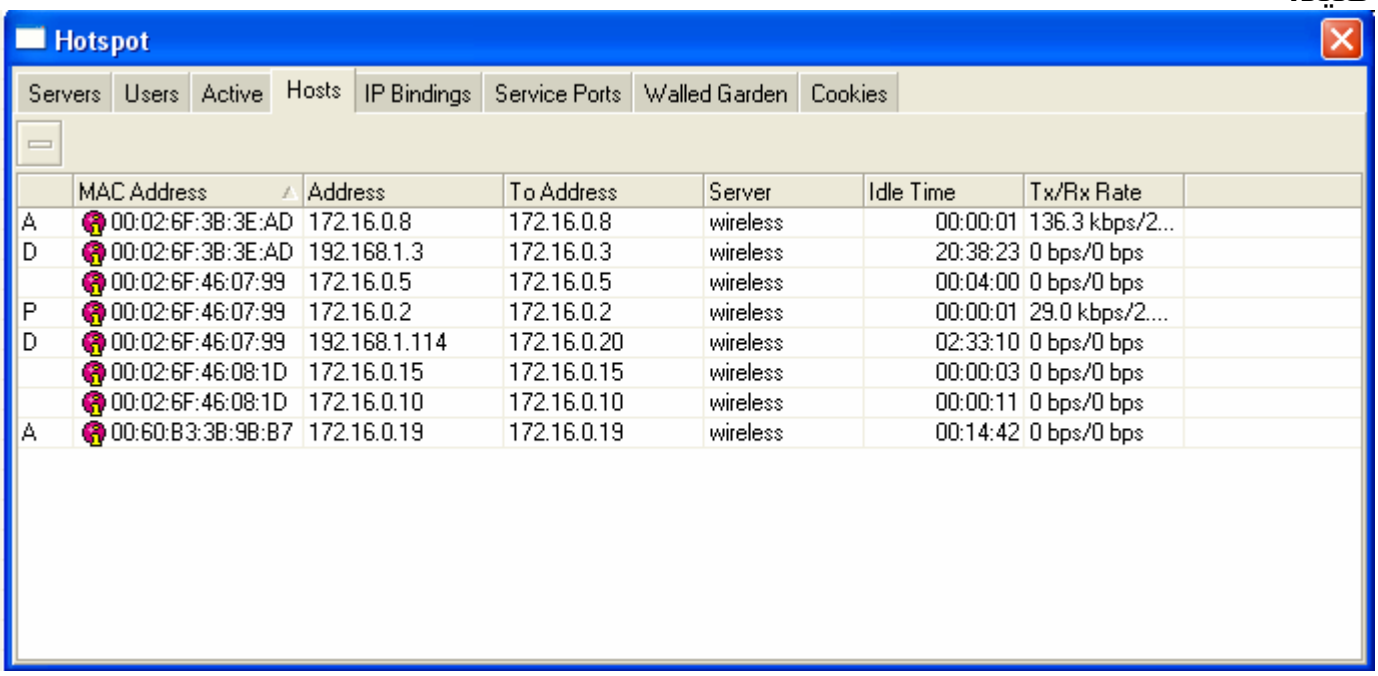


قسمت بسيار كاربردي اين قسمت Script هست كه براي استفاده از اين قسمت بايد به برنامه نويسي مسلط باشيد البته اسكريپت هاي حرفه اي و رايگاني در forum ميكروتيك براي دانلود وجود دارد.

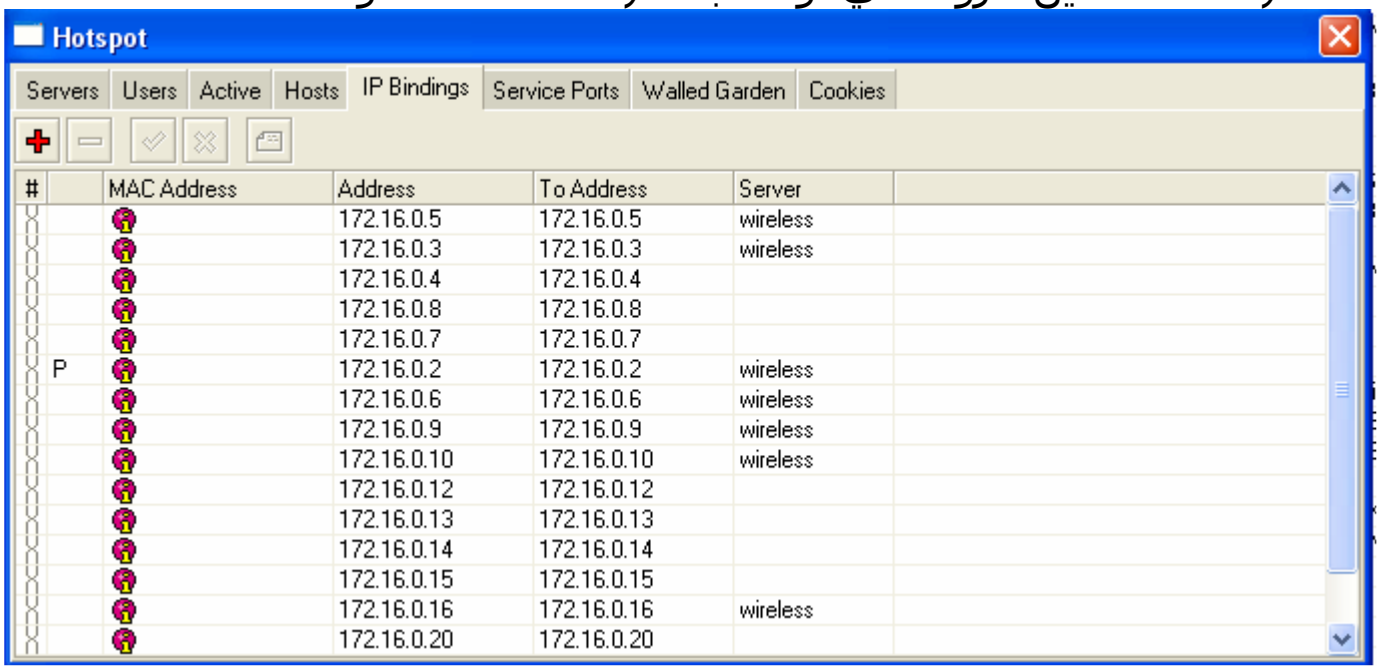
لازم به توضيح است كه اسكريپت ها در زمان ورود و خروج كاربران اعمال مي شوند.



قسمت Active ليست كاربرهاي آنلاين به همراه اطلاعات مفيد ديگر را به شما نشان مي دهد.تنها نكته اينست كه مي توانيد با فشردن گزينه - كاربرها را Kill كنيد.



قسمت Hosts ليستي از IP هاي فعال و اختصاص داده شده را به همراه MAC نشان مي دهد.
حرف A نشان دهنده نشان دهنده اين است كه كاربر يك كاربر ديتابيس داخلي بوده و Authurized شده است.
حرفD نشاندهنده Dynamic بودن IP كاربر است.
مسلم است كه اين حروف مي توانند با هم نشان داده شوند مانند AD



قسمت IP Bindings يكي از مهمترين قسمت هاي Hotspot به شمار ميايد.
براي يادگيري اين قسمت بايد مفهومي به نام One to one nat را درك كنيد.
گفتيم كه كاربر براي ارتباط با Hotspot بايد يك IP در رنج Hotspot ست كند.براي اين مورد الزامي وجود ندارد كاربر مي تواند هرIP دلخواهي ست كند و فقط DNS Gateway را سرور hotspot بدهد(در غير اينصورت صفحه Login نمايش داده

نخواهد شد.)تمامي در خواست ها حالا با هر IP كه باشند به Hotspot مي رسند و Hotspot درخواست ها را به Login Page ارجاع مي دهد اگر كاربر بتواند با موفقيت مرحله ورود را پشت سر بگذارد و به اصطلاح Authenticate شود از آن پس Hotspot يك IP به كاربر اختصاص مي دهد كه اينIP معادل IP كاربر است نه الزاما مشابه آن .اين تكنيك به One to one nat مشهور است.(Universal Client هم ناميده مي شود) پس Hotspot مي تواند هرIP آدرسي را به صورت ترانسپرنت تغيير دهد و اين قابليت بسيار كاربردي است.

اكنون مي توانيد با IP bindings كار كنيد.Mac آدرس كاربر را مشخص كنيد Address را خالي بگذاريد و To Address را با آدرس دلخواه جايگزين كنيد.كاربر هر IP هم كه ست كند باز با IP دلخواه شما به شبكه وصل خواهد شد.پس مشكلي به نام IP conflict نخواهيد داشت.

روشي كه به شخصه استفاده مي كنم و به نظر خودم بهتر جواب مي دهد اينگونه است:

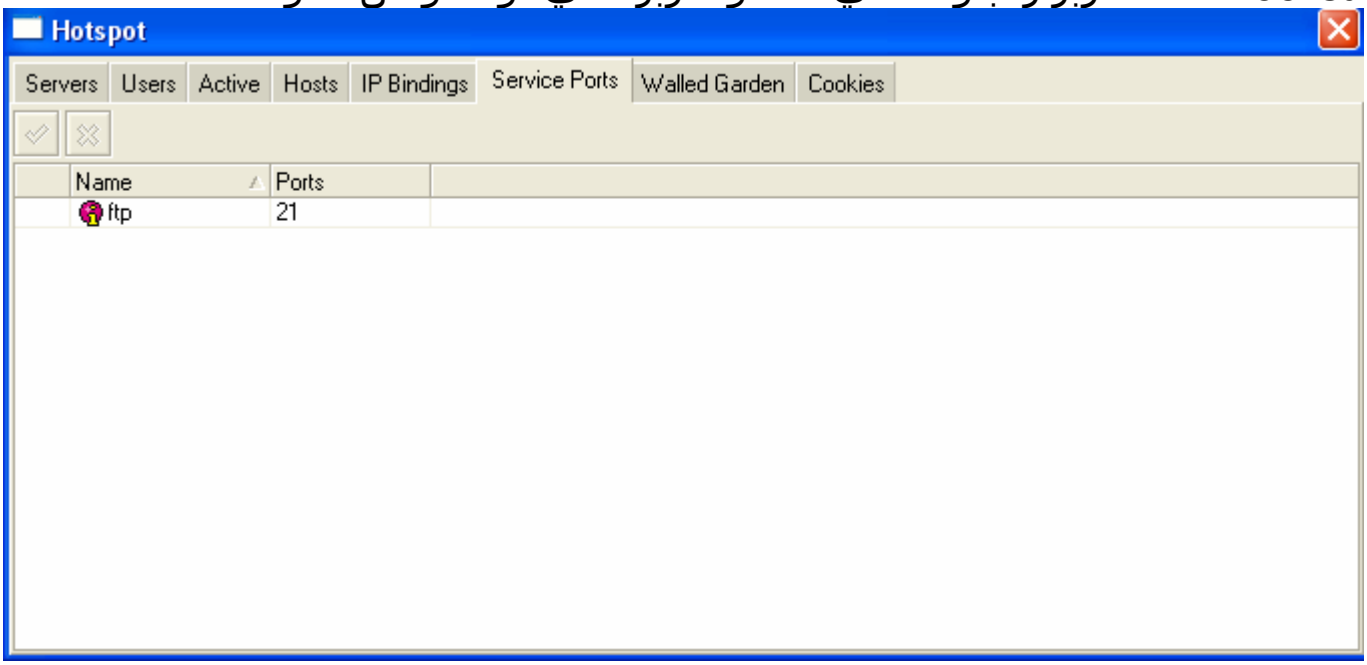
همانطور كه در شكل مي بينيد قسمت Mac Address را خالي گذاشته ام به اين دليل كه ممكن است كاربرها MACدائم نداشته باشند(مشكلاتي مثل سوختن كارت شبكه يا تعويض سرور كه معمول هستند) در عوض به كاربر IP static اختصاص مي دهم و اين IP را به IP مشابه Bind مي كنم. اين كار از به وجود آمدن آشفتگيIP در كنترل پهناي باند جلوگيري مي كند.براي اينكه از تعويض IP توسط كاربر جلوگيري كنم Address اختصاص داده شده به كاربر را در Radius سرور مي بندم بنابراين كاربر فقط از IP تعريف شده امكان اتصال دارد و اگر IP خود را تغيير دهد حتي از Login Page هم نخواهد توانست عبور كند.

نكته مهم ديگر Type اتصال كاربر است كه با كليك كردن روي هر IP كه Bind كرده ايد مي توانيد آنرا تنظيم كنيد.سه نوع type مختلف وجود دارد:

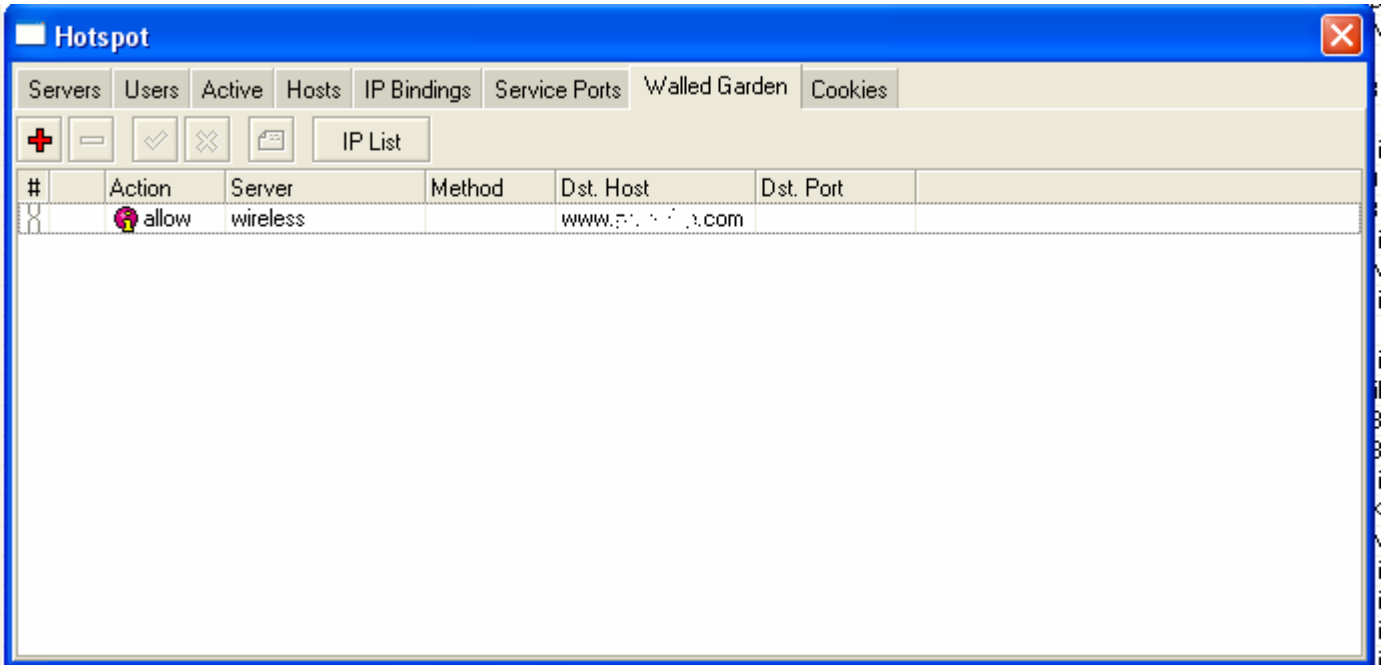
Regular: حالت پيش فرض كه كاربر بايد اعتبار سنجي شود تا وارد شود.

Bypassed: كه كاربر را از قيد اعتبار سنجي خلاص مي كند.يعني اگر كاربري اين آدرس را داشت وارد شود بدون گذر از مرحله اعتبار سنجي

Blocked: كه كاربر را بلوكه مي كند و كاربر نمي تواند وصل شود.



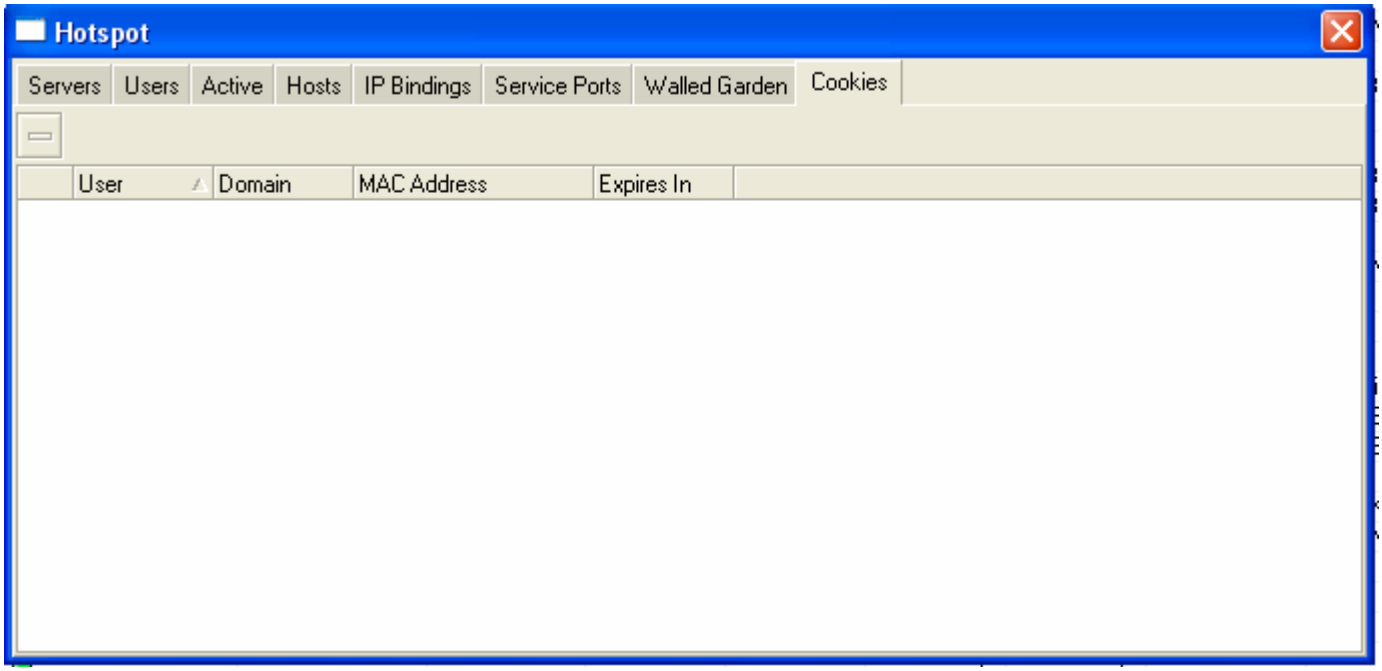
در مورد قسمت Service Port اطلاعات كاملي ندارم بنابراين از اين قسمت صرفنظر مي كنم.



قسمت مهم ديگر Walled-garden است كه اجازه دسترسي كاربران به سايت ها يا IP هاي تعريف شده توسط مدير سيستم را بدون گذر از مرحله اعتبار سنجي مي دهد.مثلا مي توانيد تنظيماتي اعمال كنيد كه كاربران براي اتصال به سايت شما و چك كردن گزارشات نيازي به وارد كردن كاربر و يا پسورد نداشته باشند و يا ...
كار كردن با اين قسمت ساده است و نيازي به توضيح ندارد.

Property Description

action (allow | deny; default: **allow**) - action to undertake if a packet matches the rule:
allow - allow the access to the page without prior authorization
deny - the authorization is required to access this page
dst-address (*IP address*) - IP address of the destination web server
dst-host (*wildcard*; default: **""**) - domain name of the destination web server (this is a wildcard)
dst-port (*integer*; default: **""**) - the TCP port a client has send the request to
method (*text*) - HTTP method of the request
path (*text*; default: **""**) - the path of the request (this is a wildcard)
server (*name*) - name of the HotSpot server this rule applied to
src-address (*IP address*) - IP address of the user sending the reque



و اما قسمت cookiesكه ليستي از كوكي هاي فعال و كوكي هاي اجاره داده شده به همراه زمان انقضاي آنها را نشان مي دهد به شرطي كه روش اعتبار سنجي با كوكي را انتخاب كرده باشيد در غير اينصورت همانند شكل بالا خالي خواهد بود.

اختصاصي كردن صفحات Hotspot

براي اختصاصي كردن صفحات Hotspot بايد از طريق FTP و يا رابط winbox متصل شده صفحات را دانلود كنيد تغييرات را اعمال كرده(مسلما بايد تا حدود زبان HTML بدانيد) و سپس صفحات را به جاي صفحات اصلي قرار دهيد.نگران نباشيد در صورت بروز هر گونه اشتباه به راحتي مي توانيد صفحات پيش فرض را جايگزين كنيد.صفحاتي كه مي توانيد تغيير دهيد عبارتند از:

Available Servlet Pages

Main HTML servlet pages, which are shown to user:

- **redirect.html** - redirects user to another url (for example, to login page)
- **login.html** - login page shown to a user to ask for username and password. This page may take the following parameters:
  - **username** - username
  - **password** - either plain-text password (in case of PAP authentication) or MD5 hash of **chap-id** variable, password and CHAP challenge (in case of CHAP authentication)
  - **dst** - original URL requested before the redirect. This will be opened on successfull login
  - **popup** - whether to pop-up a status window on successfull login
  - **radius<id>** - send the attribute identified with <id> in text string form to the RADIUS server (in case RADIUS authentication is used; lost otherwise)
  - **radius<id>u** - send the attribute identified with <id> in unsigned form to the RADIUS server (in case RADIUS authentication is used; lost otherwise)

    - **radius<id>-<vnd-id>** - send the attribute identified with <id> and vendor ID <vnd-id> in text string form to the RADIUS server (in case RADIUS authentication is used; lost otherwise)
    - **radius<id>-<vnd-id>u** - send the attribute identified with <id> and vendor ID <vnd-id> in unsigned form to the RADIUS server (in case RADIUS authentication is used; lost otherwise)
- **md5.js** - JavaScript for MD5 password hashing. Used together with **http-chap** login method
- alogin.html - page shown after client has logged in. It pops-up status page and redirects browser to originally requested page (before he/she was redirected to the HotSpot login page)
- **status.html** - status page, shows statistics for the client
- **logout.html** - logout page, shown after user is logged out. Shows final statistics about the finished session. This page may take the folllowing additional parameters:
    - **erase-cookie** - whether to erase cookies from the HotSpot server on logout (makes impossible to log in with cookie next time from the same browser, might be useful in multiuser environments)
- **error.html** - error page, shown on fatal errors only

Some other pages are available as well, if more control is needed:

- **rlogin.html** - page, which redirects client from some other URL to the login page, if authorization of the client is required to access that URL
- **rstatus.html** - similarly to rlogin.html, only in case if the client is already logged in and the original URL is not known
- **flogin.html** - shown instead of login.html, if some error has happened (invalid username or password, for example)
- **fstatus.html** - shown instead of redirect, if status page is requested, but client is not logged in
- **flogout.html** - shown instead of redirect, if logout page is requested, but client is not logged in

در پایان آین نکته را متذکر شوم که در اولین راه اندازي Hotspot قوانین فایروال جهت Redirectکردن صفحات Login Page به صورت داینامیك ایجاد مي شوند،شما مي توانید این قوانین را تغییر دهید ولي توصیه میکنم که تا زماني که واقعا مطمئن نشدید این کار را نکنید.در صورت تمایل نحوه انجام این کار در مبحث Customizing HotSpot: Firewall Section توضیح داده شده است.

موفق باشید.التماس دعا

herus_deus **روز اول ماه مبارك رمضان** 13/09/2007