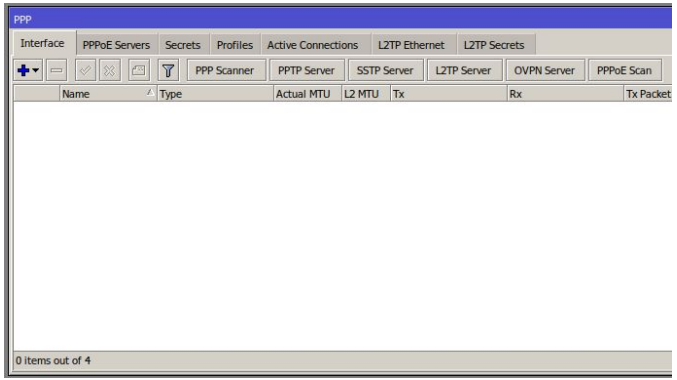
Mikrotik Certified User Manager Engineer

گردآورنده : شاهین واثقی
ویراستار: علیرضا کهن ترابی

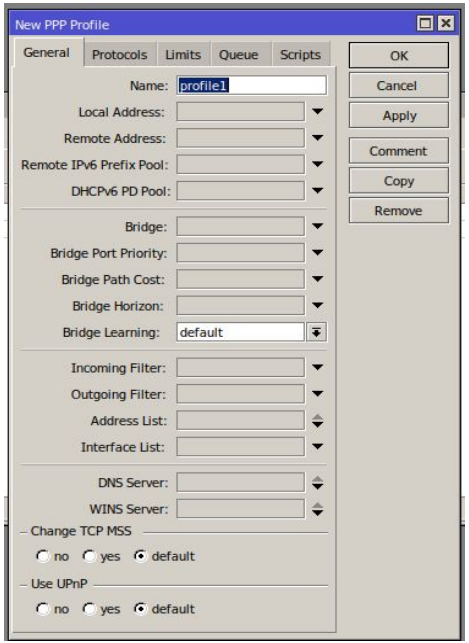
Instagram.com/vaseghi.it
youtube.com/shahin vaseghi
github.com/shahinvaseghi

Point To Point

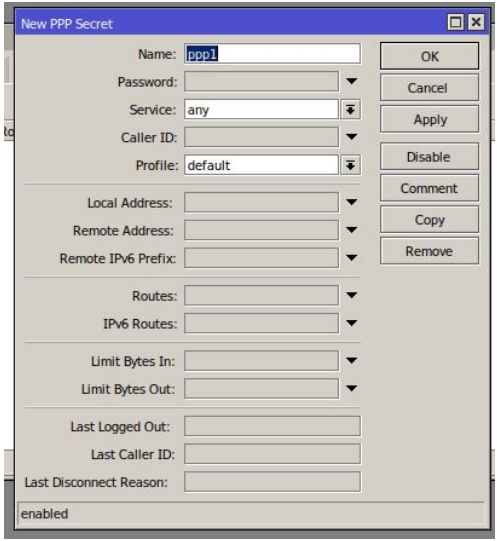
Site To Site (Router to Router)	Client to Site (Endpoint to Router)
1- Tunneling IPIP GRE 4/6 EoIP VxLAN IPsec	VPN PPTP L2TP SSTP OpenVPN WireGuard
2- VPN PPTP L2TP SSTP OpenVPN WireGuard	



برای ارتباط از راه دور در روتر ها ۲ روش Tunneling و VPN وجود دارد . که از تانل ها برای ارتباط بین روتر ها استفاده می کنیم و از VPN ها برای ارتباط کاربران با شبکه .
هنگام استفاده از تانل باید در هر دو سمت آدرس ثابت داشته باشند و بتوانند Ping یکدیگر را بگیرند.
هنگام استفاده از VPN ها تنها کافی است یکی از طرفین که نقش Server را ایفا می کند آدرس ثابت داشته باشد.
تنظیمات مربوط به VPN ها در منو PPP قرار دارد و تنظیمات مربوط به تانل ها در منو Interface
۱.VPN : برای راه اندازی وی پی ان باید یکی از پروتکل های موجود را انتخاب و آن را تنظیم کنید اما ابتدا چند اقدام است که بین تمامی آنها مشترک است.
۱.۱ IP > Pool : با استفاده از این منو باید یک ظرف آدرس برای کاربرانی که متصل میشوند ایجاد کنید.
۱.۲ PPP > Profile : ایجاد یک پروفایل:



Name : اسم این پروفایل
Local Address : آدرسی که روتر بر روی اینترفیس VPN خود قرار می دهد که میتواند تک آدرس باشد یا یک Pool IP
Remote Address : آدرسی است که به کاربر می دهیم؛ این آدرس می تواند یک آدرس باشد یا یک Pool IP
DNS Server : آدرس DNS Server برای کاربرها
در قسمت limit میتوانید بر روی ارتباطاتی که از طریق این پروفایل متصل شده اند محدودیت قرار دهید.



برای ایجاد یوزرنیم و پسورد برای کاربر های VPN به منو PPP > Secret بروید و یک سکرت جدید ایجاد کنید.

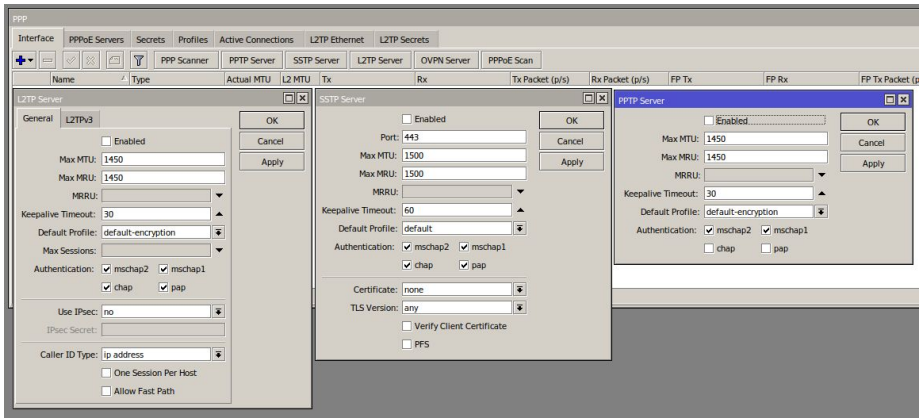
Name : همان Username کاربر می باشد Password : رمز کاربر

Service : پروتکل هایی که با رمز کاربر میتوان به آنها متصل شد

Caller ID : آدرس دستگاه هایی که کاربر فقط می تواند با آن به سرور متصل شود

Profile : پروفایلی که رمز کاربر به آن متصل می شود و کاربرانی که با این رمز به سرور متصل شوند از آن پروفایل آدرس دریافت می کنند.

Limit Byte In / Out : محدودیت حجم برای آپلود و دانلود



برای راه اندازی VPN Server در میکروتیک در PPP > Interface پروتکل مورد نظر را فعال می کنیم.

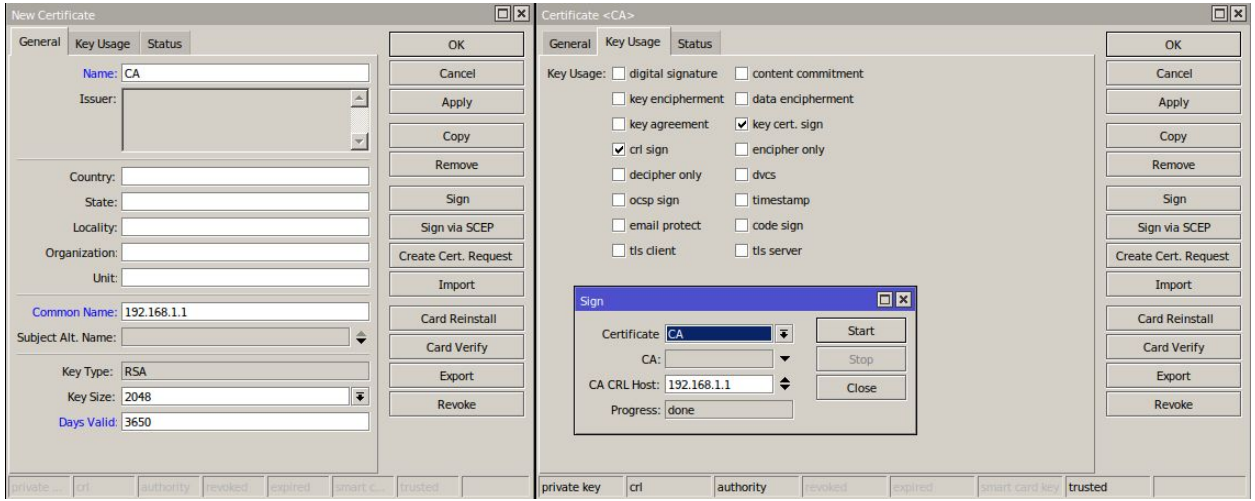
بهتر است برای امنیت الگوریتم های mschap1 و mschap2 را غیر فعال کنیم.

در L2tp میتوانید IPSec را نیز فعال کنید.

SSTP بین دو دستگاه میکروتیک نیازی به سرتیفیکیت ندارد اما اگر کاربر غیر میکروتیکی باشد به سرتیفیکیت نیاز دارد.

کاربرانی که به VPN Server متصل شده اند را میتوانید از طریق تب Active Connection مشاهده کنید.

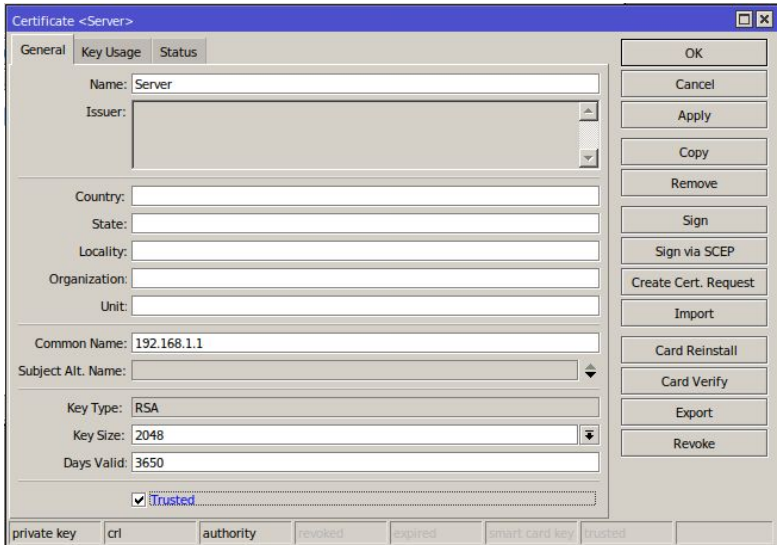
برای راه اندازی SSTP بین دو روتر میکروتیک به Certificate احتیاجی نیست اما اگر یک طرف میکروتیک نباشد باید به روش زیر Certificate بسازید.
برای ایجاد کردن Certificate به منو System > Certificate رجوع کنید و یک Certificate جدید اضافه کنید.
برای انجام این کار به سه Certificate از نوع CA و Server و Client احتیاج داریم.

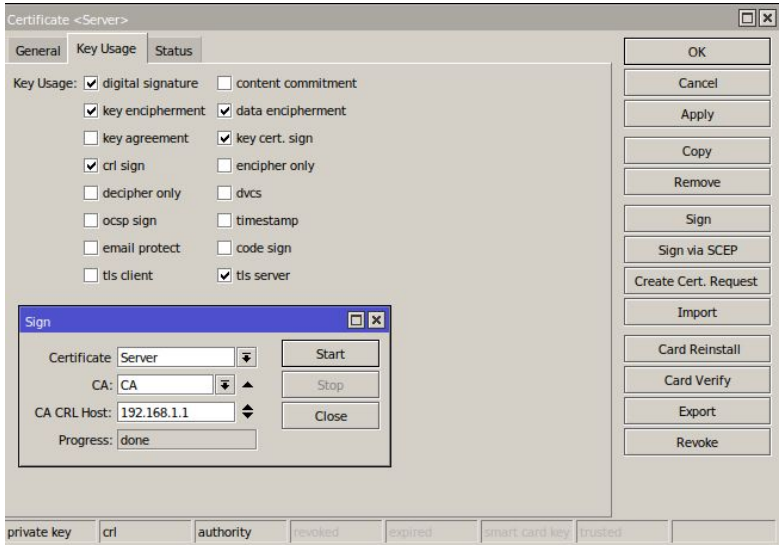


برای ساخت CA
در تب General برای این Certificate یک اسم انتخاب کنید. دیگر گزینه ها انتخابی هستند اما باید گزینه Common Name را با آدرس روتر تنظیم کنید و Days Valid را مشخص کنید که در این مثال ما ۱۰ سال قرار دادیم.
سپس در تب Key Usage باید گزینه های crl sign و key cert. Sign را فعال کنید.

پس از Apply کردن باید این Certificate را Sign کنید. در سمت راست دکمه را فشار دهید در منو Sign باید Certificate خود را مشخص کنید؛ به دلیل آنکه از نوع CA هست گزینه CA را خالی میگذاریم و در CA URL Host باید آی پی آدرس روتر را وارد کنید و کلید Sign را فشار دهید.

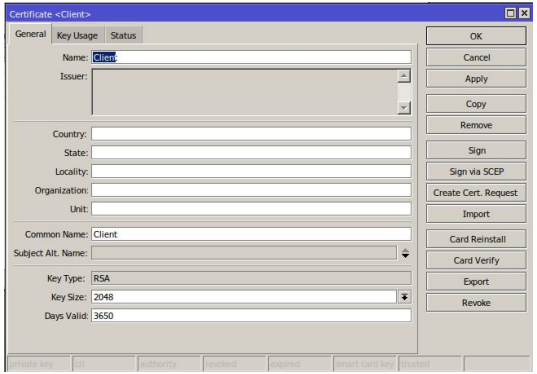
برای ساخت Certificate از نوع Server باید یک Certificate اضافه کنید .
در تب General برای این Certificate یک اسم انتخاب کنید. دیگر گزینه ها انتخابی هستند اما باید گزینه ی Common Name را با آدرس روتر تنظیم کنید و Days Valid را مشخص کنید که در این مثال ما ۱۰ سال قرار دادیم.
سپس در تب Key Usage گزینه های
digital signature , key encipherment , data encipherment , key cert. sign , crl sign , tls server را فعال کنید.

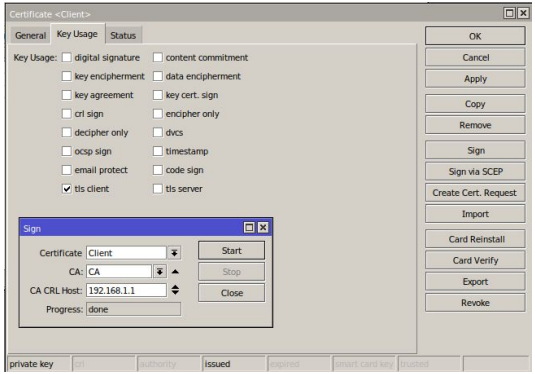




برای Sign کردن سرور باید CA را انتخاب کنید و آدرس را مجددا وارد کنید. در آخر در تب General گزینه Trusted را فعال کنید.

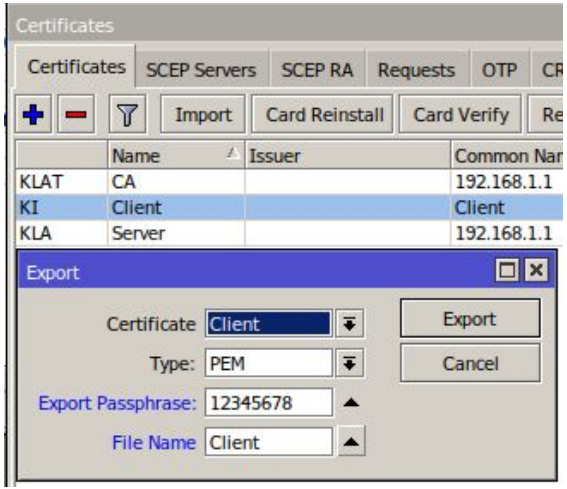
برای ساخت Certificate از نوع Client در تب General برای این Certificate یک اسم انتخاب کنید. دیگر گزینه ها انتخابی هستند اما باید گزینه ی Common Name را Client و Days Valid را مشخص کنید که در این مثال ما ۱۰ سال قرار دادیم.
سپس در تب Key Usage گزینه ی tls client را فعال کنید.

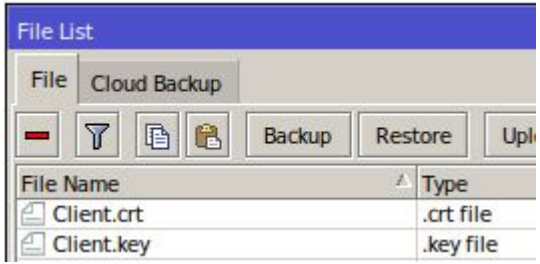




برای Sign کردن سرور باید CA را انتخاب کنید و آدرس را مجددا وارد کنید. در آخر در تب General گزینه Trusted را فعال کنید.

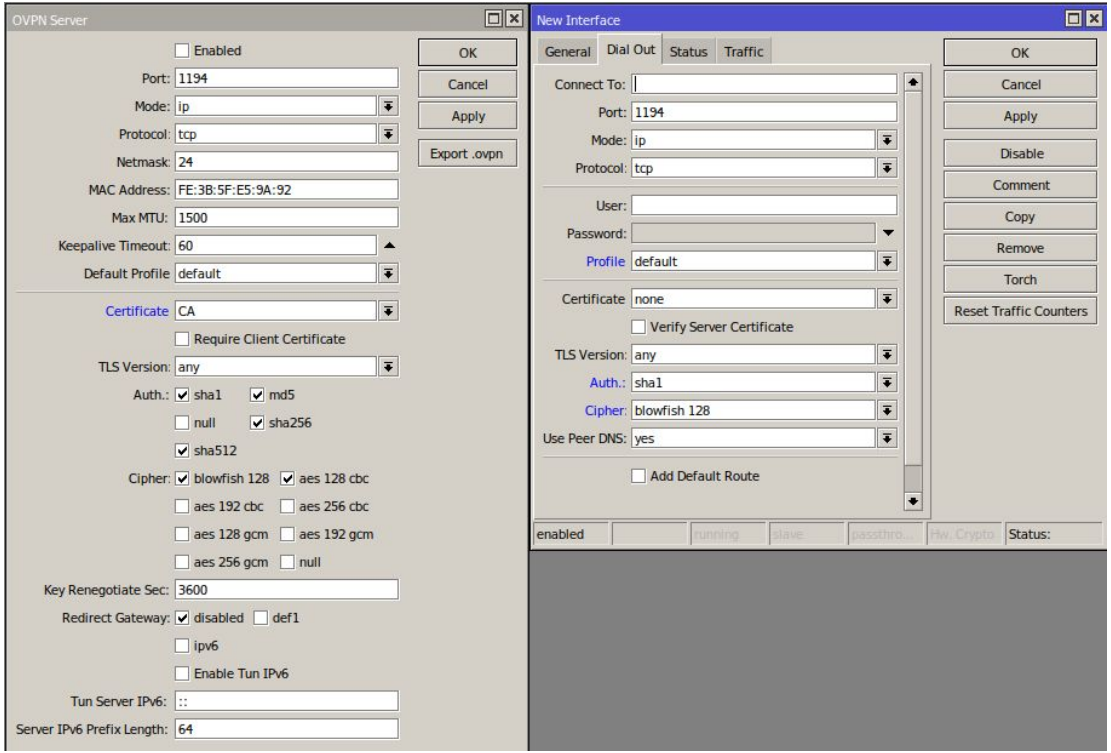
حالا باید از Client یک Export بگیرید و حتما برای فایل رمز بگذارید.
۲ فایل برای شما ایجاد می شود:
۱.Cilent.crt که فایل Certificate است .
۲.Client.key که فایل رمز است .





کاربرهایی که قصد دارند به این Server SSTP متصل شوند باید این ۲ فایل را وارد دستگاه کنند.

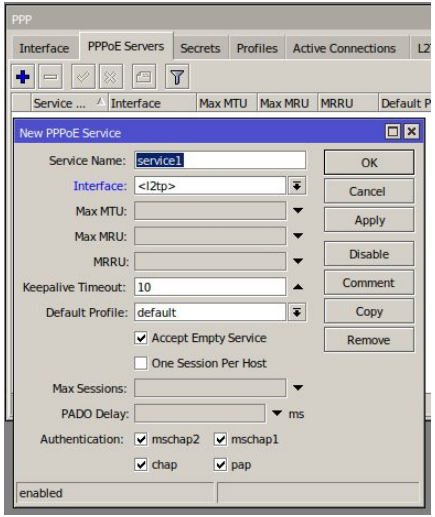
در صورتی که کاربر شما ویندوز است باید فایل CA را به او بدهید



برای راه اندازی OpenVPN نیاز به Certificate هایی مانند بالا دارید با این تفاوت که برای ارتباط راحت تر کاربرها میتوانید با این Certificate ها یک فایل بسازید که وارد کردن آن برای کاربر ساده تر باشد.

برای اینکار باید یک نسخه نمونه فایل OpenVpn.ovpn Client را دانلود کنید و اطلاعات فایل را با اطلاعات شخصی سازی شده خودتان جایگزین کنید.

برای اینکه در میکروتیک Ovpn Client بسازید کافی است Certificate نوع Client را داشته باشید.



VPN هایی که در بالا مشاهده کردیم از نوع لایه ۳ هستند میکروتیک از VPN لایه ۲ نیز تحت پروتکل PPPoE پشتیبانی می کند.

برای راه اندازی PPPoE سرور به منو PPP > PPPoE Server رجوع کنید و یک گزینه اد کنید :

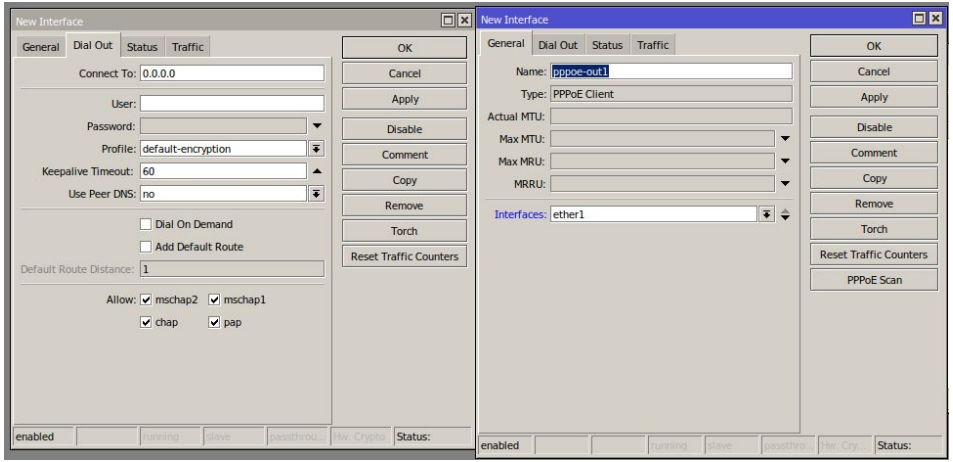
Service Name : اسم سرور Interface : پورت مورد نظری که سرویس را روی آن ارائه کنیم

برای ایجاد VPN Client در میکروتیک به Interface بروید و بر روی Add کلیک و پروتکل دلخواه را انتخاب کنید .

در PPPoE Client ابتدا در General پورتی که سرویس را از آن دریافت می کنید انتخاب کنید سپس در Dial Out یوزرنیم و پسورد را انتخاب کنید

در بقیه پروتکل ها کافی است که در Dial Out آدرس سرور و یوزرنیم و پسورد را وارد کنید.

توجه داشته باشید که در پروتکل L2tp ممکن است لازم باشد IPSec را نیز وارد کنید.



برای راه اندازی PPPoE Client ابتدا باید در تب General پورت یا Interface ی که از طریق آن به سرور متصل هستید را انتخاب کنید.

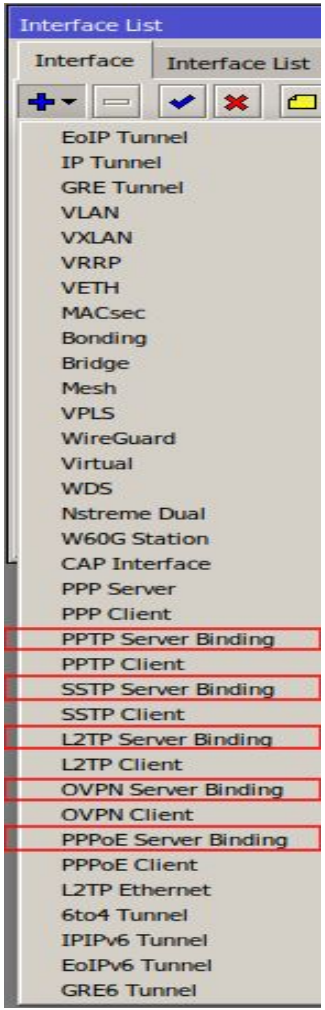
سپس در تب Dial Out در قسمت Connect To آدرس VPN Server را وارد کنید.

User : در این قسمت Username را وارد میکنید

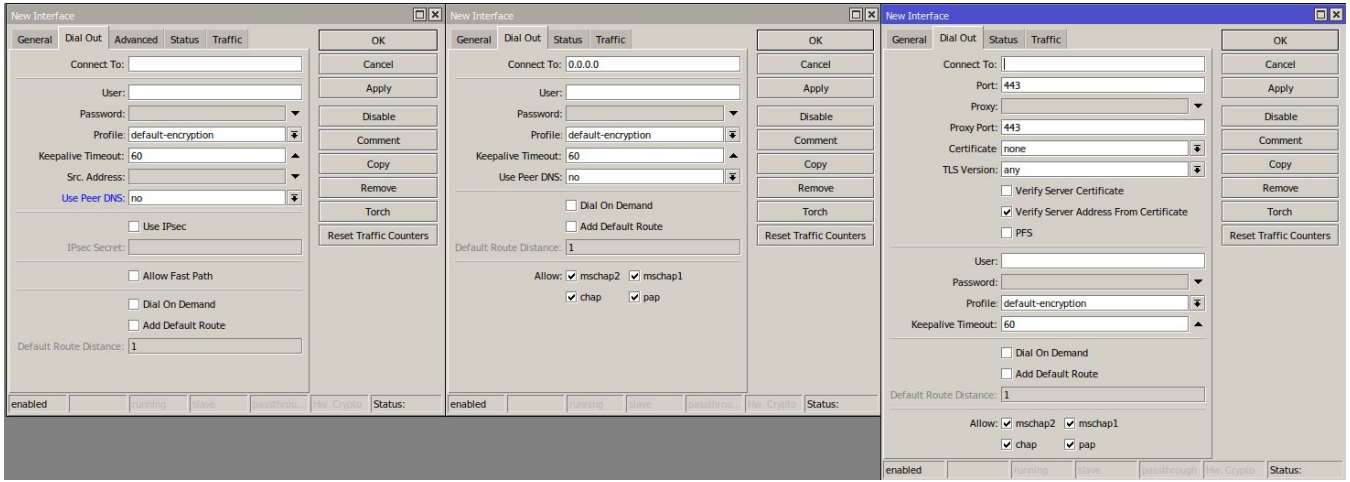
Password : رمز را وارد کنید.

Add Default Route : با انتخاب این گزینه بعد از اتصال به سرور یک Default Route به سمت سرور در جدول ایجاد می شود

قسمت Allow رمزنگاری بسته های ارسال شده توسط VPN انتخاب می شود که باید گزینه های mschap1 و mschap2 را انتخاب کنید زیرا الگوریتم های Chap و Pap شکسته شده اند



برای اینکه اینترفیس سرور های VPN با هر بار قطع و وصل شدن کاربر از بین نرود و همیشه وجود داشته باشد باید از گزینه های Server Binding در Interface یا PPP استفاده کنید.



برای راه اندازی VPN Client باید در تب Dial Out در قسمت Connect To آدرس VPN Server را وارد کنید.

User : در این قسمت Username را وارد میکنید

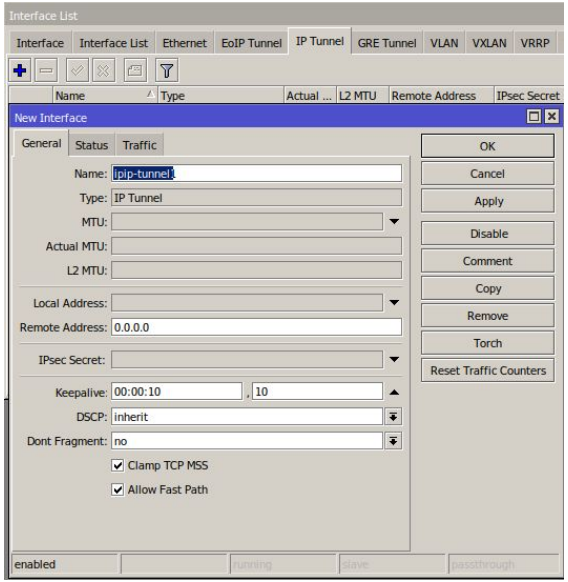
Password : رمز را وارد کنید.

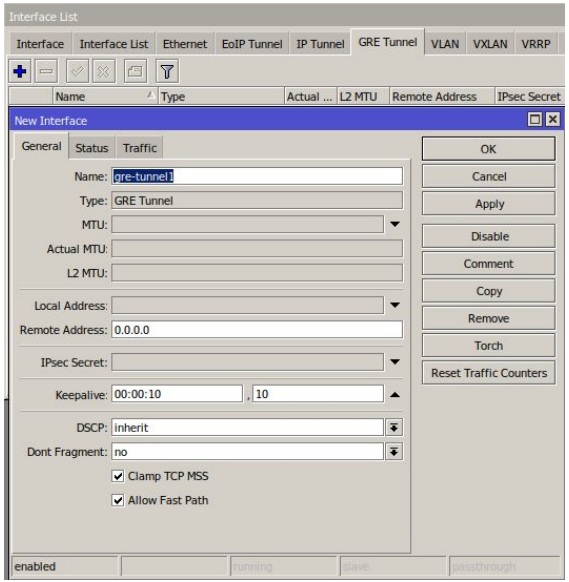
Dial On Demand : در صورتی که بار روی لینک نباشد کانکشن قطع می شود و در زمان استفاده دوباره متصل می شود.

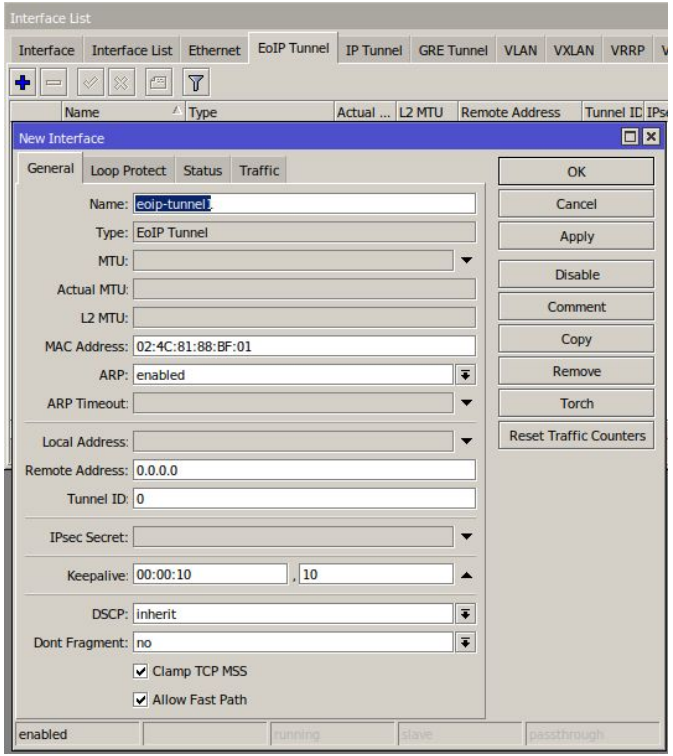
Add Default Route : با انتخاب این گزینه بعد از اتصال به سرور یک Default Route به سمت سرور در جدول ایجاد می شود

در PPTP و SSTP قسمت Allow رمزنگاری بسته های ارسال شده توسط VPN انتخاب می شود که باید گزینه های mschap1 و mschap2 را انتخاب کنید زیرا الگوریتم های Chap و Pap شکسته شده اند

در L2tp Client در صورتی که سرور از IPSec استفاده کند با فعال کردن گزینه Use IPSec رمز را وارد کنید.



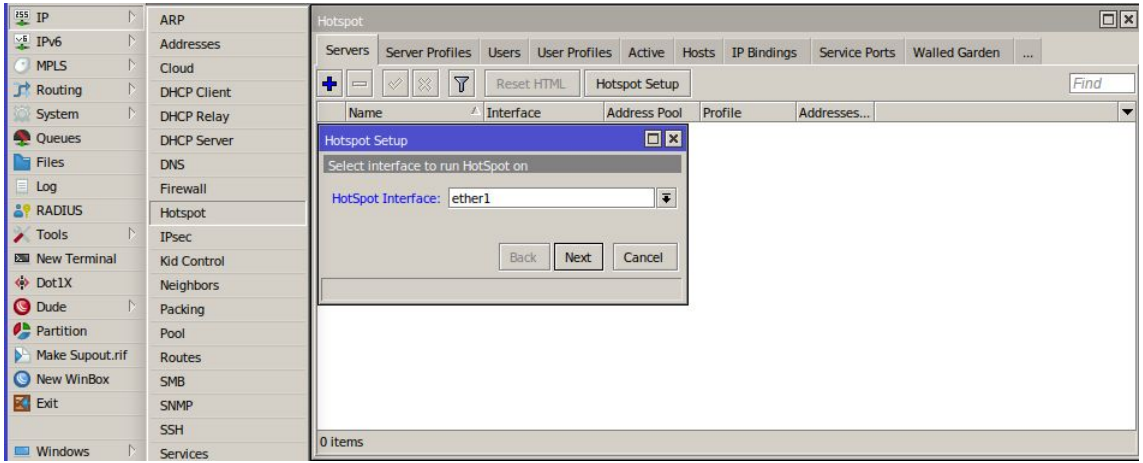


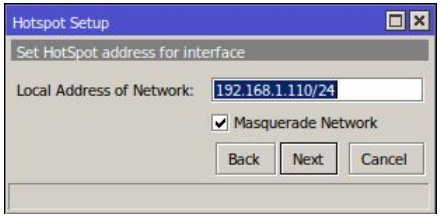


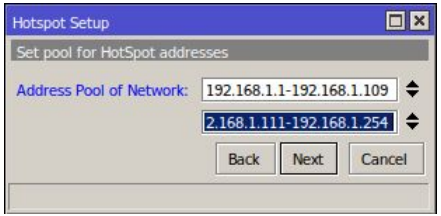
برای راه اندازی تانل ها در میکروتیک ابتدا باید یک پروتکل انتخاب کنید؛ در Interface منو های مختلفی برای پروتکل های مختلف وجود دارد.
پروتکل های موجود در میکروتیک ipip - GRE - EoIP و ... هستند.

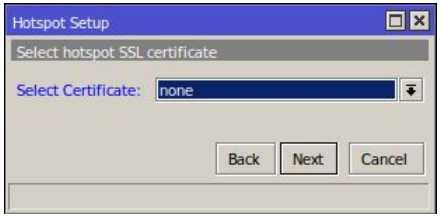
برای راه اندازی تانل های مختلف ۲ مورد در تمامی آنها مشترک است؛ Local Address آدرس روتری است که در حال راه اندازی تانل در آن هستید و Remote Address که آدرس روتر روبرو است. توجه داشته باشید که تانل ها مانند VPN خودشان فرایند آدرس دهی را انجام نمی دهند بلکه باید خودتان بر روی Interface ها آدرس دهی انجام دهید.
توجه داشته باشید که تانل های IPIP و GRE از نوع لایه ۳ هستند اما پروتکل EoIP که انحصاری میکروتیک است به صورت لایه ۲ای کار می کند.
مهمترین تفاوت ipip و GRE در MTU آنها است. GRE MTU = 1476 IPIP MTU = 1480
توجه داشته باشید که پروتکل IPSEC به دلیل رمزنگاری، ۵۰ واحد از MTU هر پروتکلی که به آن اضافه شود کم میکند.
برای راه اندازی IPSec باید حتما گزینه Allow Fast PAth را غیرفعال کنید.
برای راه اندازی EoIP باید در هر دو سمت Tunnel ID یکسان تنظیم کنید.

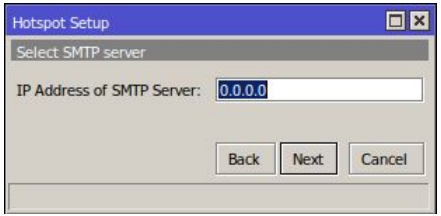
HotSpot یکی از روش های کنترل کاربر است که بسیار رایج است.
برای راه اندازی Hotspot باید به منو IP>Hotspot بروید و گزینه Hotspot Setup را فشار دهید.
اولین سوال این است که Hotspot روی کدام پورت حقیقی یا مجازی تنظیم شود.
سوال بعدی آدرس روتر در آن پورت است و گزینه فعال سازی Nat Masquerade
گزینه بعدی ساختن یک Pool IP است.





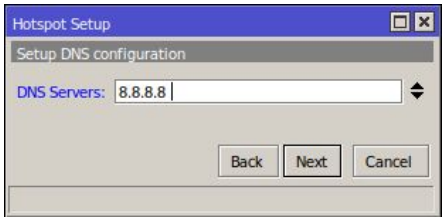


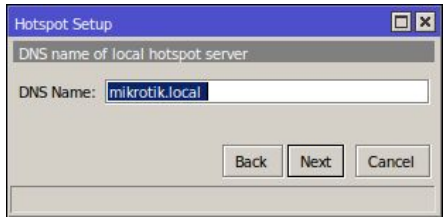


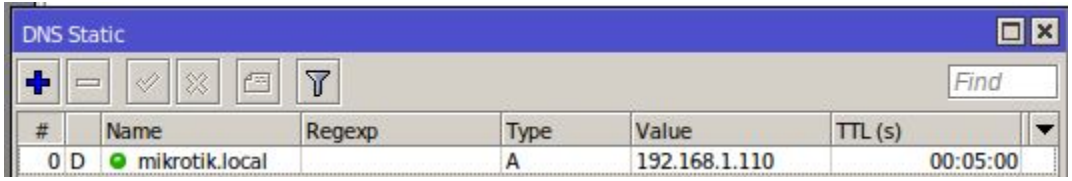


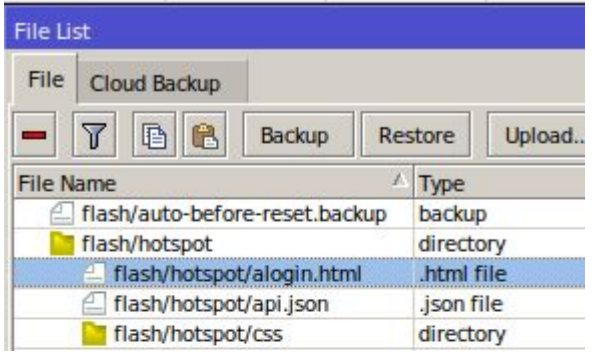
همانطور که میندازید در هات اسپات بعد از اتصال یک صفحه وب باز می شود و از شما می خواهد که یوزر و پسورد را برای اتصال وارد کنید.
سوال بعدی این است که آیا میخواهید یک Certificate برای صفحه وب اضافه کنید تا صفحه HTTPS باز شود.
سوال بعدی این است که اگر ایمیل سرور در شبکه وجود دارد آدرسش را وارد کنید تا اطلاعات کاربران را برایشان ایمیل کند.

سوال بعدی انتخاب یک DNS Server برای کاربران است
سوال اخر انتخاب یک Domain Name برای صفحه لاگین Hotspot است.
این کار باعث می شود که یک Static DNS ایجاد شود.

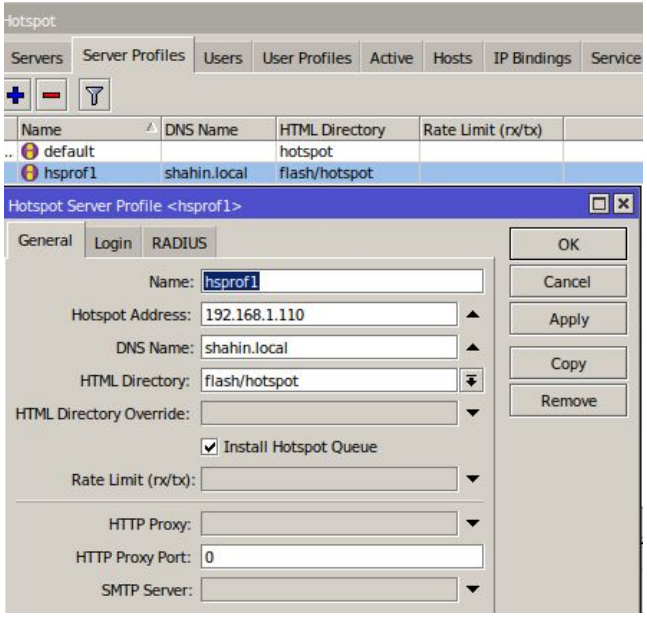




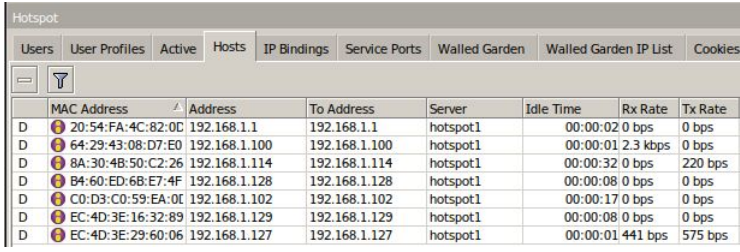




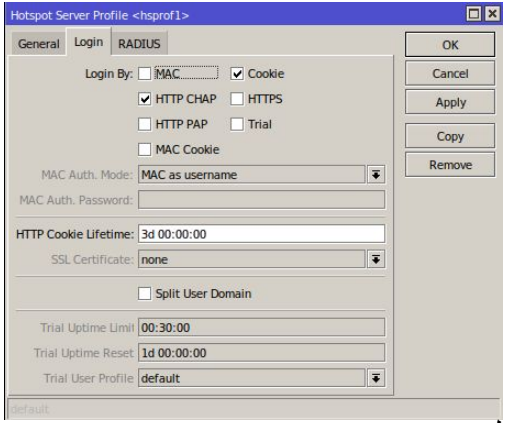
تمامی فایل های hotspot در files دستگاه و قابل ویرایش است.



در تب Server Profiles میتوانید اطلاعات بیشتری از سرور ها به دست بیاورید. با باز کردن یک گزینه با موارد زیر روبرو می شوید:
Name : اسم سرور
Hotspot Address : آدرس سرور
DNS Name : آدرس Url صفحه ورود
HTML Directory : آدرسی که فایل های صفحه را از آنجا فراخانی می کند
Rate Limit : با این گزینه می توانید برای تمام اعضا این سرور محدودیت سرعت تعیین کنید.
HTTP Proxy : با این گزینه می توانید تمام اطلاعات عبوری Hotspot را Cache کنید



در تب Hosts تمام Device هایی که به صورت لایه ۲ ای به این سرور هستند چه متصل شده باشند چه نه نمایش داده می شود.



به چند روش امکان Login به Hotspot وجود دارد:

۱. Mac : در صورت وجود Radius سرور و ایجاد لیست Mac Add های مورد نظر با فعال کردن این گزینه افراد لیست بدون Login کردن متصل می شوند.

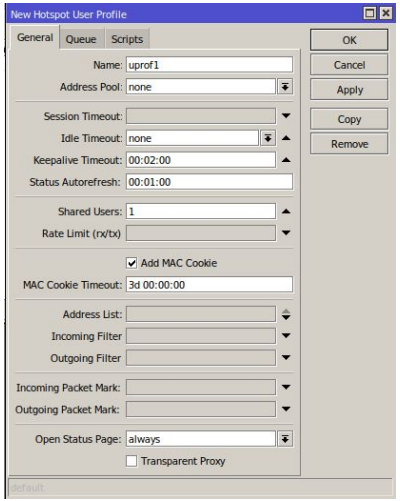
۲. HTTP CHAP : احراز هویت رمزنگاری شده از طریق وب

۳. HTTP PAP : احراز هویت بدون رمزنگاری از طریق وب

۴. Cookie : افراد Login کرده را به یک مدت زمان مشخص متصل می ماند و نیاز به ورود مجدد ندارد.

۵. HTTPS : احراز هویت رمزنگاری شده از طریق وب

Trial : در صورت انتخاب این گزینه افراد بدون وارد کردن یوزر و رمز در یک تایم مشخصی میتوانند متصل شوند.



User Profile یک پروفایل کلی برای کاربرها است که می توانید کاربر ها را به آنها متصل کنید و کاربر ها از شرایط عام پروفایل پیروی کنند. گزینه های User Profile به شرح زیر است:

Name : اسم پروفایل.

Address Pool : استفاده از یک Add Pool متفاوت.

Session Timeout : مدت زمان اتصال در هر ارتباط.

Idle Timeout : قطع ارتباط بعد از این زمان بدون ارسال و دریافت.

Keepalive Timeout : هر چند وقت یکبار ارتباط با کاربر چک شود.

Status Autorefresh : هر چند مدت یکبار صفحه کاربر Refresh شود.

Shared User : تعداد کاربر مجاز برای اتصال توسط یوزر های این پروفایل.

Rate Limit : محدودیت پهنای باند یوزرهای این پروفایل.

Add MAC Cookie : ایجاد Cookie برای مک آدرس های متصل شده توسط این پروفایل

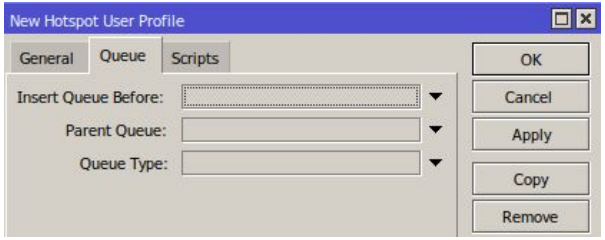
Address List : کاربرهای متصل شده توسط این پروفایل به یک آدرس لیست اضافه شوند.

Incoming Filter : بسته های ورودی کاربر های متصل شده توسط این پروفایل به فایروال ارسال شود.

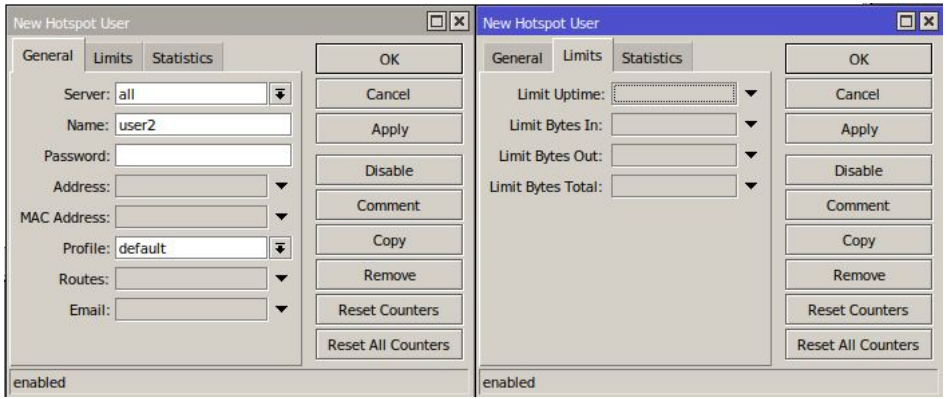
Outgoing Filter : بسته های خروجی کاربر های متصل شده توسط این پروفایل به فایروال ارسال شود.

Incoming Packet Mark : بسته های ورودی افراد متصل شده توسط این یوزر برچسب زده شوند.

Outgoing Packet Mark : بسته های ورودی افراد متصل شده توسط این یوزر برچسب زده شوند.

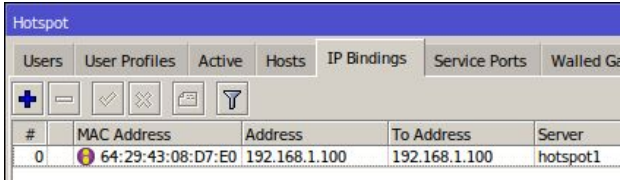


در تب Queue میتوانید تنظیمات زیر را انجام دهید.
Insert Queue Before : وضعیت قرارگیری این Queue در لیست
Parent : Parent Queue، این Queue که توسط پروفایل ساخته می شود.
Queue Type : نوع Queue



برای ایجاد یوزر در هات اسپات از تب Users انجام می شود. برای ایجاد یوزر جدید گزینه های زیر موجود است :
۱. Server : این یوزر در چه سروری معتبر باشد.
۲. Name : همان Username
۳. Password
۴. Address : آدرسی که پس از احراز هویت به کاربر می دهیم
۵. MAC Address : مک آدرس مجاز برای این یوزر

۶. Profile : یوزر پروفایل مربوط به یوزر
۷. Route : یک Route دستی که پس از اتصال به جدول مسیریابی کاربر اضافه می شود.
Email : آدرس ایمیل این کاربر در SMTP Server تنظیم شده در این Hotspot



در تب Limit مدت زمان اتصال و محدودیت حجمی برای کاربر قابل تنظیم است.

میتوانید کاربران موجود در Hosts را توسط کلید Make Binding به IP Binding اضافه کنید یا به طور دستی ایجاد کنید. کاربران این لیست نیاز به احراز هویت ندارند.