

در این مقاله آموزشی قصد داریم با نحوه مدیریت ترافیک شبکه با استفاده از میکروتیک در کنار فایروال Kerio Control آشنا شویم.

نظارت و مدیریت اینترنت سازمان ها باعث بالا رفتن بازدهی کاری کاربران و نیز ایجاد امنیت در شبکه مورد استفاده در آن اداره و یا سازمان می باشد. این نوع نظارت و مدیریت هم بصورت نرم افزاری می تواند باشد و هم بصورت سخت افزاری که اصطلاحاً به آنها فایروال Firewall های سخت افزاری و نرم افزاری گفته می شود . نرم افزارها و سخت افزارهای فایروالی متنوعی جهت نظارت و مدیریت اینترنت سازمان وجود دارد که از آن جمله می توان به نرم افزارهای Kerio Control اشاره کرد و از سخت افزارها نیز می توان MikroTik را نام برد. به فایروالهای سخت افزاری UTM گفته میشود.

قابلیتهای کلیدی نرم افزار : Kerio Control

۱. مدیریت کاربر
۲. قابلیت یکپارچه شدن با Active Directory
۳. اعتبار سنجی کاربران برای دسترسی به شبکه
۴. توانایی سریع به اشتراک گذاشتن اینترنت در شبکه از طریق Proxy و NAT
۵. افزایش کارایی اینترنت با استفاده از Web Caching
۶. قابلیت اختصاص IP به طور خودکار (DHCP)
۷. تسریع کننده درخواست ارسالی DNS
۸. پشتیبانی از منطقه DMZ
۹. امکان تعریف قواعد دسترسی به شبکه و اینترنت برای هر کاربر
۱۰. نظارت بر فعالیت کاربران در وب
۱۱. امنیت یکپارچه
۱۲. دارای دیواره آتش جهت کنترل دسترسی، جلوگیری از نفوذ و خرابکاری در شبکه
۱۳. دارای سیستم شناسایی و ممانعت از نفوذ (IPS)
۱۴. قابلیت استفاده از انواع ضد ویروس های قدرتمند برای ترافیک HTTP ,FTP ,SMTP ,POP3
۱۵. ساز و کار سر خود برای پالایش محتوای صفحات وب
۱۶. استفاده اختیاری از پالاینده های پیشرفته
۱۷. توانایی جلوگیری از ورود آگهی های تبلیغاتی اینترنتی
۱۸. بازرسی و کنترل کلیه پرتکل های غیر استاندارد
۱۹. شبکه خصوصی مجازی
۲۰. پشتیبانی از P.N جهت برقراری ارتباط رمزگذاری شده

- ۲۱. قابلیت برقراری ارتباط سایت به سایت، کاربر به سایت
- ۲۲. مدیریت پهنای باند
- ۲۳. قابلیت سهمیه بندی پهنای باند برای برنامه های مختلف
- ۲۴. پشتیبانی از انواع ارتباطات اینترنتی ماهواره ی ، DSL ، ISDN، شماره گیری از طریق مودم و غیره
- ۲۵. پشتیبانی از UPnP ، فناوری ارتباط نرم افزارها بدون پیکره بندی خاص مانند MSN Messenger
- ۲۶. ثبت وقایع مربوط به ترافیک اینترنت
- ۲۷. نمایش فعالیتها بصورت گراف
- ۲۸. مدیریت از راه دور با برخورداری از امنیت کامل
- ۲۹. امنیت در اینترنت
- ۳۰. دیوار آتش برای شبکه

دیوار آتش:

اصلی ترین وظیفه یک دیوار آتش مستقر در محیط، نظارت بر ترافیک ورودی و خروجی شبکه بر مبنای سیاست امنیتی سازمان است کریو قادر است برای نظارت بر ترافیک اینترنت قواعد قابل درک و ساده ای را مبنی بر رویه های امنیتی شبکه پیشنهاد دهد. دستیار نصب خودکار فراهم شده در نرم افزار میتواند خیلی به سرعت این کار را به انجام برساند.

سیستم ضد نفوذ: (IPS)

سیستم ضد نفوذ Kerio Control می تواند بطور غیر محسوس تمامی ترافیک ورودی و خروجی شبکه را تحت نظارت قرار دهد و در کنار دیوار آتش سرویس دهنده های داخل شبکه را از هرگونه نفوذ و ارتباط غیر مجاز در امان دارد.

محافظت در مقابل ویروسها:

داشتن ضدویروس در محیط شبکه، خطر انتشار سریع ویروس را کاهش میدهد Kerio Control به طور اختیاری یک پوششگر قوی، مختص ویروس را برای ترافیک ورودی و خروجی HTTP, FTP, SMTP, POP3 فراهم نموده است.

نظارت بر محتوای Web:

Kerio Control بطور سر خود دارای ویژگی اعمال محدودیت بر روی محتوای صفحات وب است که بر مبنای کلید واژه، دسترسی به یک سایت را میتواند مسدود نماید در این نرم افزار محتوای صفحات وب، به چندین مقوله مختلف نظیر اخبار، بازی، خرید، ورزش، مسافرت و غیره تقسیم شده است و میتواند دسترسی کاربران مختلف، به مقوله های گوناگون را کنترل و یا مسدود نماید.

با توجه به ویژگی ها و قابلیت هایی که این سیستم برای مدیران شبکه فراهم می کند می توانیم از آن برای تکمیل قابلیت های بی شمار میکروتیک به عنوان یک روتر قدرتمند استفاده نماییم.

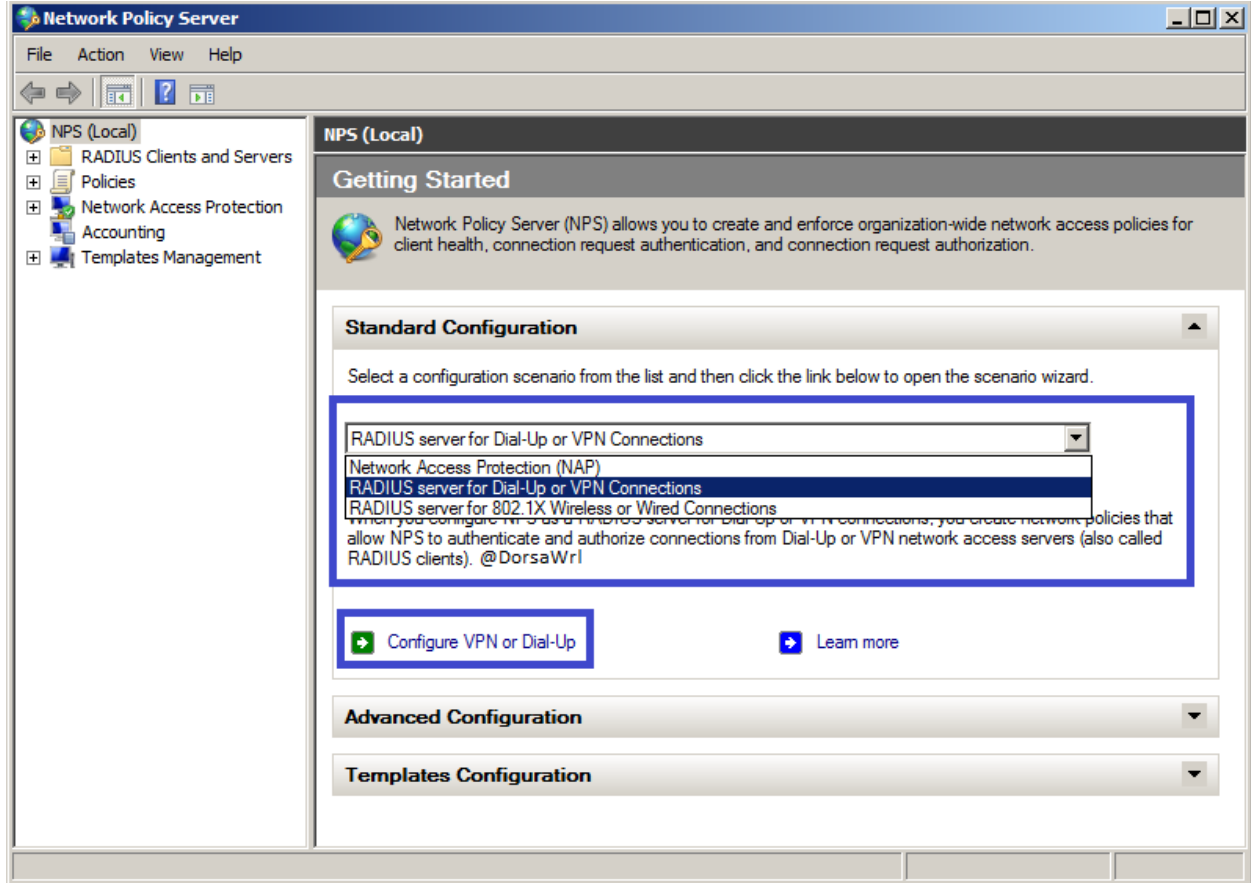
در این سناریو از یک سرور ویندوز به عنوان **Active Directory** برای مدیریت یکپارچه کاربران در شبکه استفاده می کنیم. نحوه راه اندازی سرویس های **Active Directory** بر روی ویندوز سرور در این مقاله قرار داده نمی شود و فرض را بر این میگذاریم که این سرویس از قبل راه اندازی شده است.

در ابتدا باید ویندوز سرور خود را به یک **RADIUS Server** برای احراز هویت کاربران تبدیل کنیم که این کار با استفاده از سرویس **Network Policy Server** ایجاد می شود.


• در این سناریو برای حفظ امنیت کاربران دسترسی کاربران شبکه به اینترنت فقط با اتصال **VPN** برقرار می شود.

ابتدا با استفاده از بخش **Server Manager** نقش **Network Policy Server** را نصب و راه اندازی می نماییم.

بعد از نصب وارد تنظیمات **Network Policy Server** می شویم و طبق عکس زیر مراحل راه اندازی **RADIUS Server** را پیگیری می نماییم.



Configure VPN or Dial-Up [X]

 **Select Dial-up or Virtual Private Network Connections Type**

Type of connections:

Dial-up Connections
When you deploy Dial-up servers on your network, NPS can authenticate and authorize connection requests made by dial-up clients connecting through the servers.

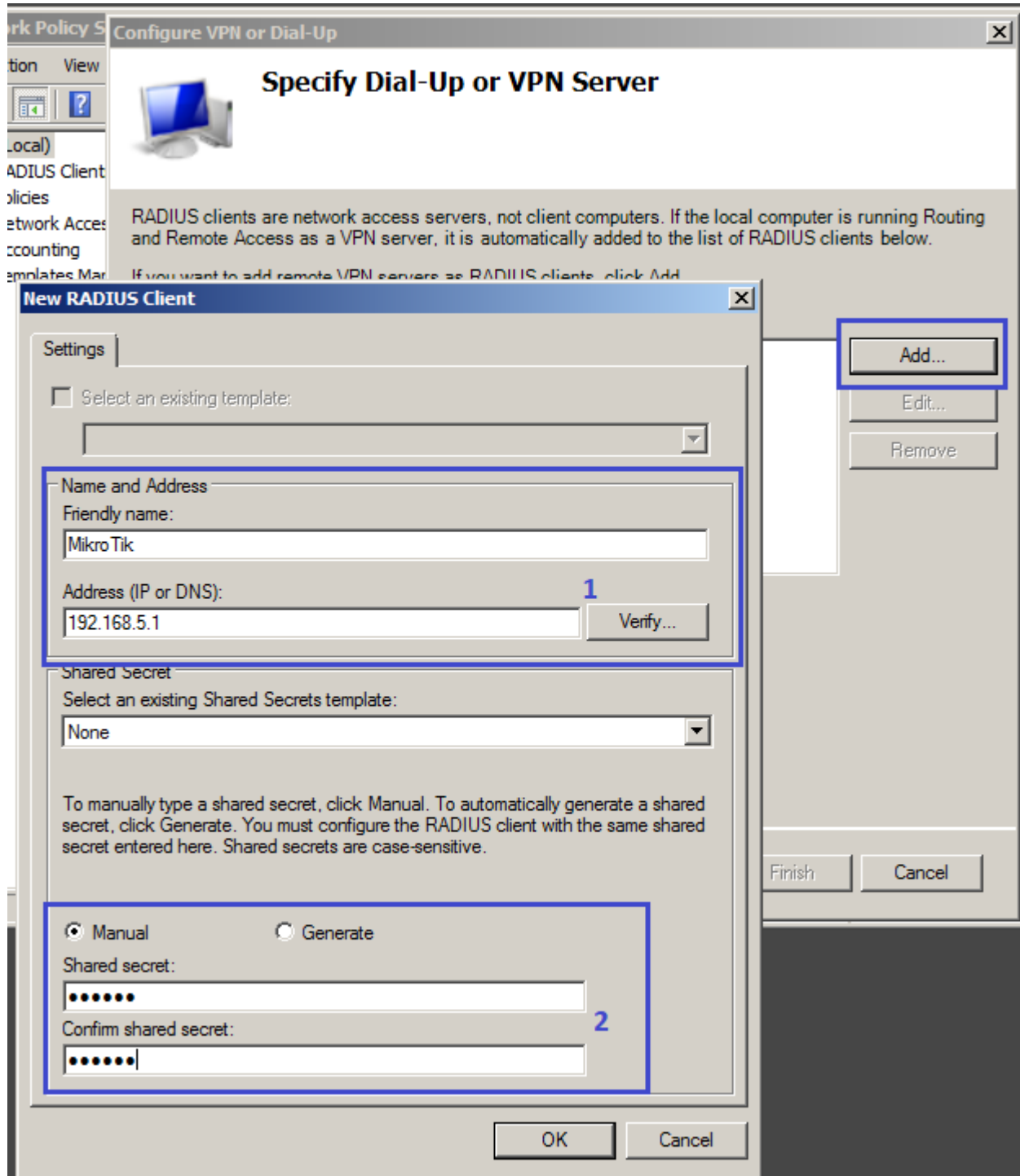
Virtual Private Network (VPN) Connections
When you deploy VPN servers on your network, NPS can authenticate and authorize connection requests made by VPN clients connecting through the servers.

Name:
This default text is used as part of the name for each of the policies created with this wizard. You can use the default text or modify it. @DorsaWr1

Virtual Private Network (VPN) Connections

Previous Next Finish Cancel

در این بخش باید روتر میکروتیک را به عنوان یک RADIUS Client به ویندوز سرور معرفی کنیم:



۱. در این بخش آدرس IP میکروتیک و یک نام دلخواه در نظر می گیریم

۲. در این بخش باید یک رمز به عنوان **Secret** برای برقراری ارتباط بین **RADIUS Server & Client** در نظر بگیریم که در هر دو سمت باید یکسان باشد.

در این بخش متد های احراز هویت را فعال می کنیم

Configure Authentication Methods

The following protocols are supported by servers running Microsoft Routing and Remote Access. If you use a different remote access server, make sure the protocols you select are supported by that software.

Extensible Authentication Protocol

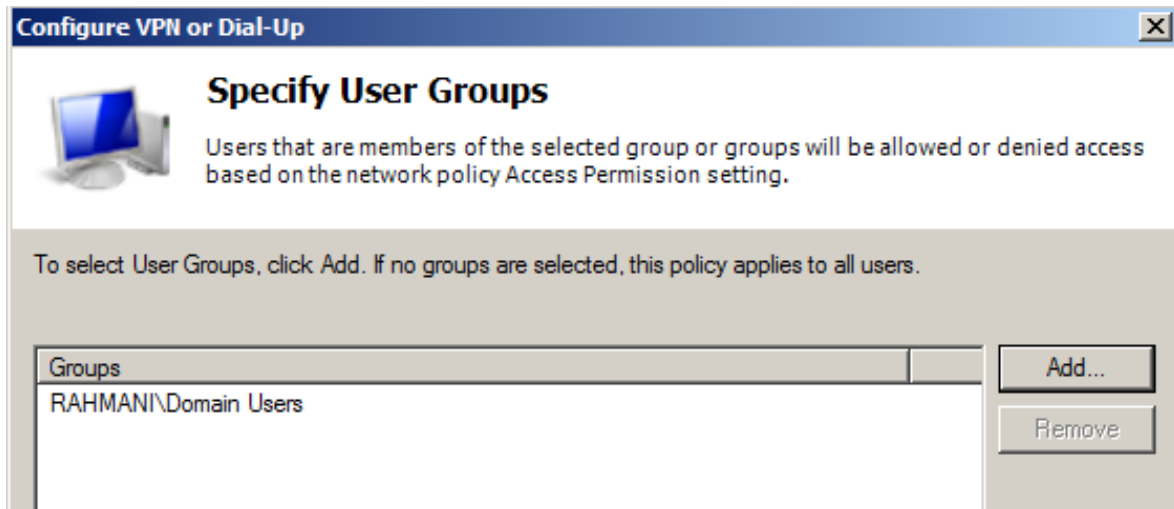
Type (based on method of access and network configuration):
Microsoft: Smart Card or other certificate Configure...

Microsoft Encrypted Authentication version 2 (MS-CHAPv2)
Select this option to allow your users to specify a password for authentication.

Microsoft Encrypted Authentication (MS-CHAP)
Select this option only if your network runs operating systems that do not support MS-CHAPv2.

Previous Next Finish Cancel

در این مرحله باید گروهی از کاربران AD که این Policy روی آن ها اعمال می شود را انتخاب کنیم که در این سناریو ما Domain Users را انتخاب می کنیم.



مابقی موارد را بدون نیاز به تغییر تا انتهای پروسه راه اندازی Next می زنیم و در نهایت Finish می کنیم. در حال حاضر ویندوز سرور Active Directory ما به عنوان یک RADIUS Server فعال می باشد. در ادامه به انجام تنظیمات میکروتیک می پردازیم.

- راه اندازی سرور VPN میکروتیک:

برای اجرای این سناریو به ترتیب موارد زیر را اجرا می کنیم:

ایجاد یک Pool آدرس IP مختص کاربران اینترنت

```
/ip pool
```

```
add name=VPN ranges=192.168.70.0/24
```

سپس برای فعال سازی سرویس VPN Server روی روتر باید یک Profile برای مشخصات و تنظیمات سرور خود در میکروتیک ایجاد کنیم:

```
/ppp profile
```

```
add dns-server=8.8.8.8,4.2.2.4 idle-timeout=59m local-address=10.50.50.1 \
```

```
name="Local VPN" remote-address=VPN
```

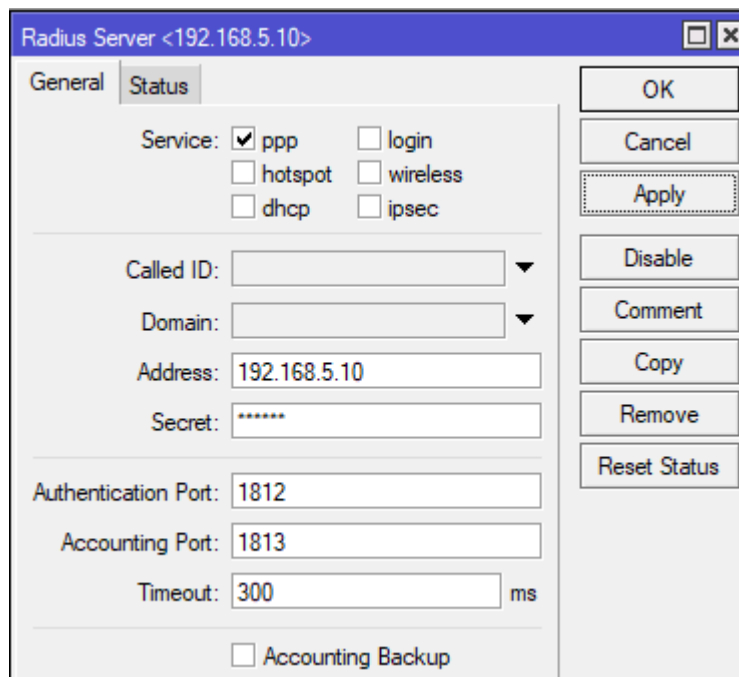

سپس سرویس VPN سرور را فعال می کنیم:

```
/interface ptp-server server
set authentication=pap,chap,mschap1,mschap2 default-profile="Local VPN" \
max-mru=1460 max-mtu=1460
```

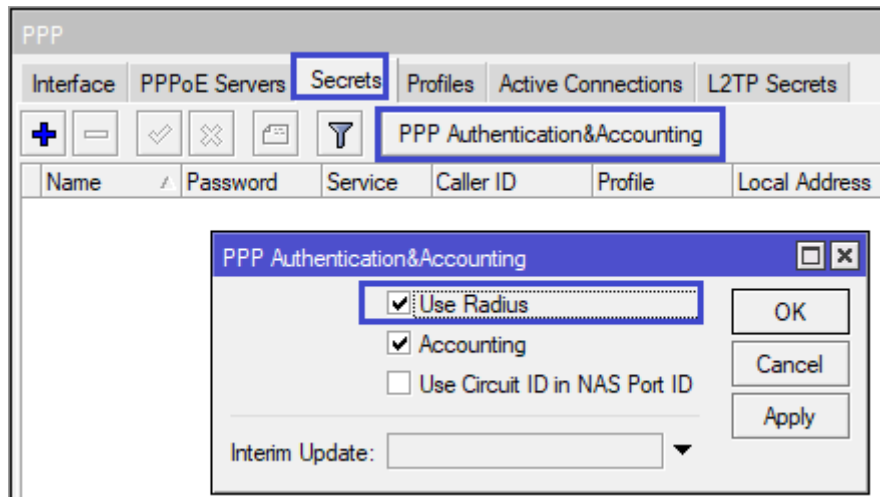
در این سناریو من از سرویس PPTP استفاده می کنم.

در ادامه مشخصات Active Directory را به عنوان Radius به میکروتیک معرفی می کنیم.

برای تعریف Active Directory به عنوان RADIUS Server در میکروتیک به قسمت Radius رفته و به شکل زیر تنظیمات و مشخصات Active Directory را وارد می کنیم:

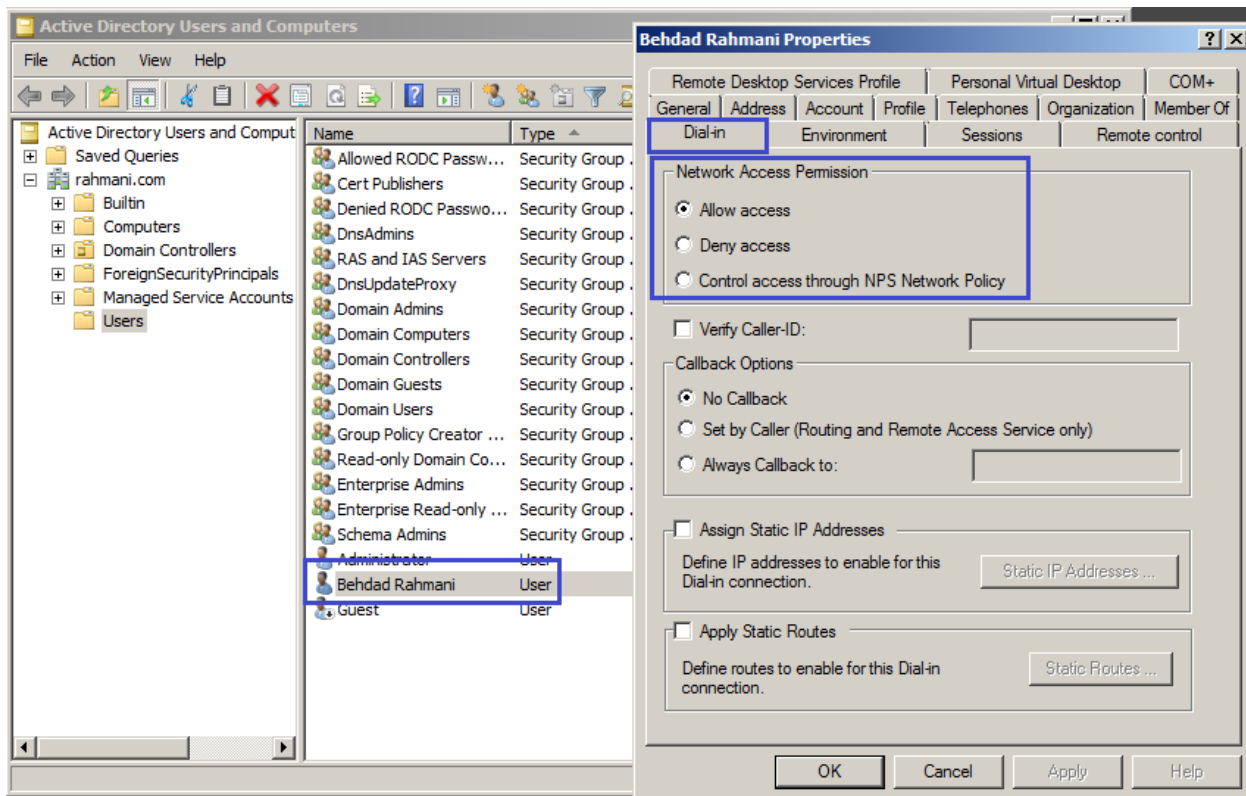


سپس در قسمت PPP بخش Secrets احراز هویت از طریق Radius را فعال می کنیم:



تا این مرحله امکان اتصال کاربران Active Directory به میکروتیک که بصورت VPN Server راه اندازی شده است فراهم شده است.

- نکته قابل توجه این است که در Active Directory کاربری که ایجاد می کنیم دسترسی VPN را داشته باشد:



در ادامه به اتصال Kerio Control به AD می پردازیم.

روش نصب و راه اندازی Kerio Control در این مقاله مورد بررسی قرار نمی گیرد و فرض بر این است که راه اندازی و نصب اولیه از قبل انجام شده است. برای این سرور می توان ۲ کارت شبکه در نظر گرفت که یکی به اینترنت و دیگری به شبکه داخلی متصل گردد.

The screenshot shows the 'Interfaces' configuration page in Kerio Control. The left sidebar lists various system settings. The main area is titled 'Interfaces' and includes a section for 'Internet connectivity' with a dropdown menu set to 'A Single Internet Link'. Below this is a table of network interfaces:

Name	Status	IPv4	IPv6
Internet Interfaces			
WAN	Up	192.168.3.216	IPv6 disabled
Trusted/Local Interfaces			
Ethernet	Up	192.168.5.2	IPv6 disabled
IPsec and Kerio VPN Interfaces			


بصورت پیش فرض Kerio Control بصورت Nat دسترسی کاربران به اینترنت را فراهم می کند و نیاز به اعمال تغییرات خاصی نیست.

در ابتدا باید Kerio Control را هم به Active Directory متصل کنیم که برای احرازهویت کاربران از آن استفاده نماید. برای این کار از بخش Domains and Users تب Directory Services مشخصات اتصال به سرور Active Directory را طبق تصویر زیر وارد می کنیم:





The screenshot shows the 'Domains and User Login' configuration page in Kerio Control. The left sidebar lists various system settings. The main area is titled 'Domains and User Login' and includes tabs for 'Authentication Options', 'Security Options', 'Directory Services', and 'Guest Interfaces'. The 'Directory Services' tab is active, showing configuration options for connecting to an Active Directory server:

- Member of domain rahmani.com.
- Map user accounts and groups from a directory service
- Domain**
 - Directory service type: Microsoft® Active Directory®
 - Domain name: rahmani.com
- Account with read access to the directory service**
 - Username: administrator@rahmani.com
 - Password: [masked]
- Connection**
 - Automatically connect to the first directory server available
 - Connect to the specified directory servers:
 - Primary server: 192.168.5.2
 - Secondary server: [empty]

در صورتی که اتصال با موفقیت برقرار شود در قسمت **Users** می توانید لیست کاربران **Active Directory** را مشاهده نمایید:


 **Users**

Domain: rahmani.com Hide disabled user accounts Filter:

Username	Full Name	Description	Groups
 Administrator	Administrator	Built-in account for administering...	Domain Users, Group Policy Creator Owners, Domain Admin
 behdad	Behdad Rahmani		Domain Users
 Guest	Guest	Built-in account for guest access ...	Domain Guests, Guests
 krbtgt	krbtgt	Key Distribution Center Service A...	Domain Users, Denied RODC Password Replication Group

هم اکنون هم تنظیمات اتصال میکروتیک و هم تنظیمات اتصال **Kerio Control** به سرور **Active Directory** به عنوان مرجع احراز هویت کاربران برقرار شده است.

برای این که **Kerio Control** دسترسی کاربران به اینترنت را با احراز هویت انجام دهد در قسمت **Domains and Users** قسمت **Authentication Options** بخش **Web Authentication** موارد را طبق تصویر زیر فعال می کنیم:

 **Domains and User Login**


Authentication Options | Security Options | Directory Services | Guest Interfaces

Web authentication

- Always require users to be authenticated when accessing web pages
- Force non-transparent proxy server authentication

Each browser session will require user authentication. This is useful in Citrix or Terminal Service environments,

Apply only to these IP addresses:

- Enable automatic authentication using NTLM 

Automatic logout

- Automatically logout users if they are inactive

Timeout: minute(s)

با فعال کردن این گزینه ها در زمان اتصال کاربر به اینترنت صفحه لاگین **Kerio Control** نمایش داده می شود و از کاربر درخواست شناسه کاربری و رمز عبور می کند (همانند هات اسپات میکروتیک) در صورتی که

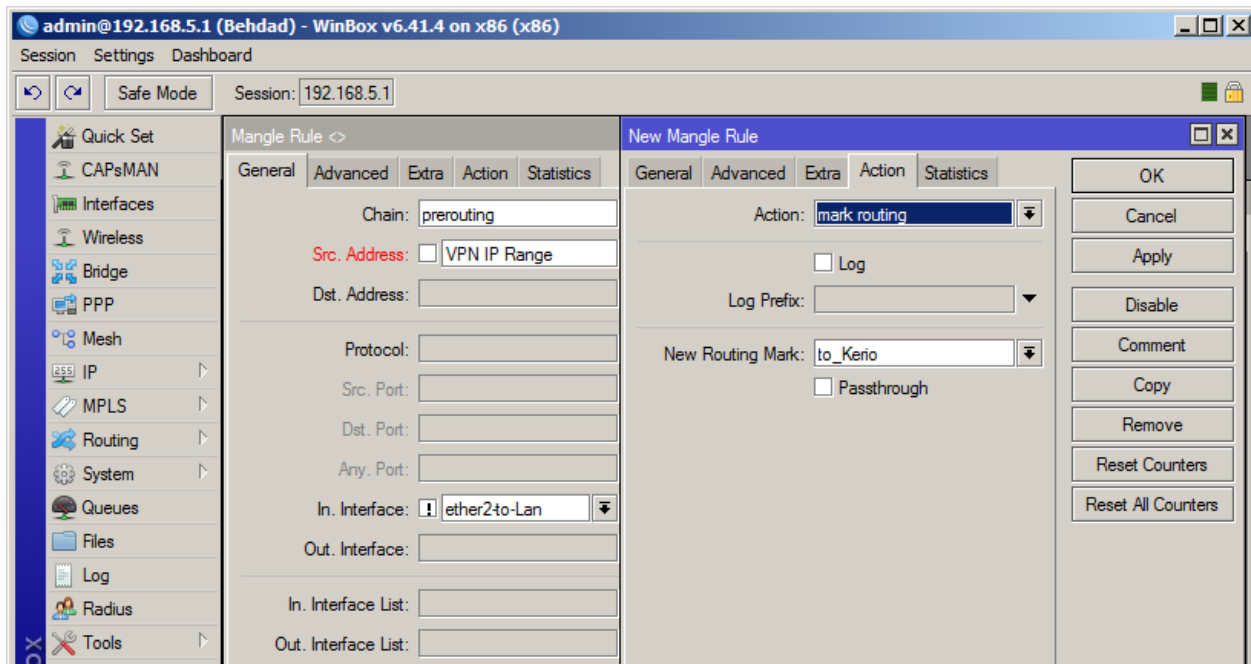
کاربر Join به Domain شده باشد با فعال کردن گزینه Enable automatic authentication using NTLM بصورت خودکار با شناسه و رمز دامنه که با آن به سیستم خود لاگین کرده است احراز هویت انجام می شود و نیازی به وارد کردن دستی اطلاعات کاربری نمی باشد.

ارسال ترافیک کاربران میکروتیک به کریو:

این بخش اصلی مقاله می باشد که با تنظیمات زیر ترافیک کاربران شبکه که با VPN متصل شده اند را به سمت Kerio Control هدایت می کنیم تا بعد از احراز هویت امکان دسترسی به اینترنت را داشته باشند و تمام فعالیت های اینترنتی کاربران تحت نظارت Kerio Control انجام شود.

برای این منظور از ابزار Mangle در میکروتیک استفاده می کنیم تا ترافیک کاربران VPN را با ابزار Mark Routing علامت گذاری کرده و به سمت Kerio Control ارسال نماییم. همانطور که در بالا توضیح داده شد کاربر با شناسه و رمز دامنه خود لاگین می کند و وقتی در کریو گزینه Enable automatic authentication using NTLM فعال باشد بدون نیاز به وارد کردن اطلاعات کاربری دسترسی به اینترنت فراهم می شود ولی اگر این گزینه فعال نباشد یک صفحه لاگین به کاربر نمایش داده می شود. توجه داشته باشید که این صفحه لاگین قابل ویرایش می باشد.

تنظیمات Mangle :



توجه داشته باشید در قسمت **Interface . In** ترافیک ورودی کارت شبکه **Lan** را در میکروتیک از این رول مستثنی می کنیم که ترافیک ورودی به روتر مجدد در این **flow** قرار نگیرد.

سپس از قسمت **Route** یک **static route** برای این **mark routing** به **IP** سرور **Kerio Control** ایجاد می کنیم. در رول بالا ما تمام ترافیک کاربران را به سمت **Kerio Control** منتقل کردیم. در صورت نیاز می توانید ترافیک به مقاصد خاص را **bypass** کنید یا فقط برای پورت های **80,443** پروتکل **TCP** این رول را ایجاد نمایید.

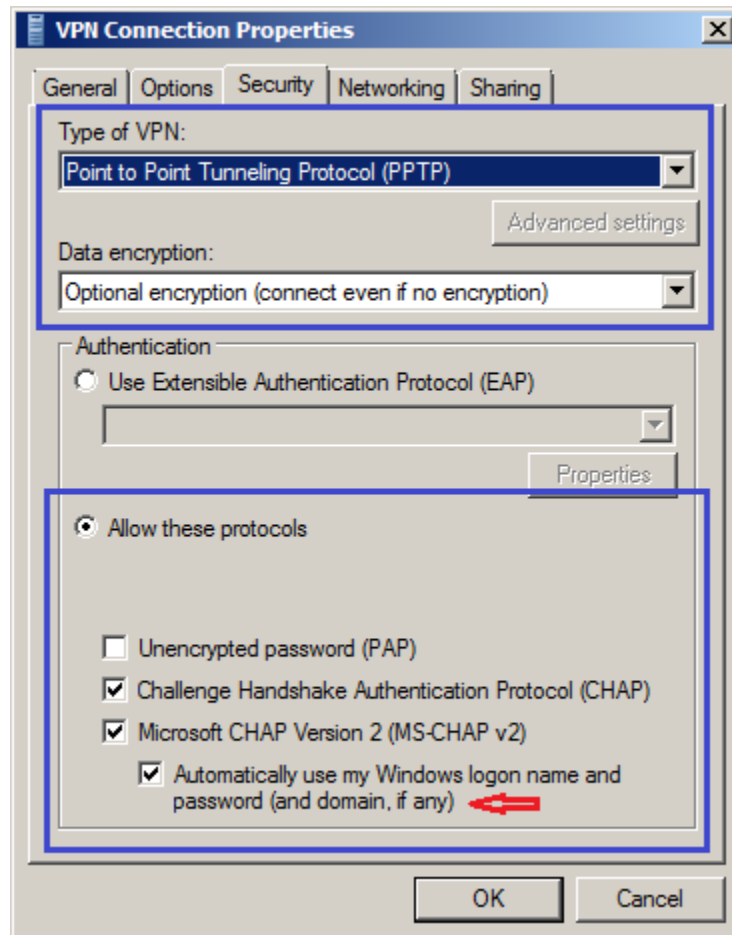
Det. Address	Gateway	Distance	Routing Mark	P
AS 0.0.0.0/0	192.168.5.3 reachable ether2to-Lan	1	to_Kerio	
DAS 0.0.0.0/0	192.168.13.1 reachable ether3to-Wan	1		
DAC 192.168.5.0/24	ether2to-Lan reachable	0		1
DAC 192.168.13.0/...	ether3to-Wan reachable	0		1

بعد از ایجاد رول در قسمت **route** ترافیک کاربران به **Kerio** منتقل می شود و با توجه به اتصال کاربر با **VPN** می توانیم سرعت تبادل اطلاعات کاربر را در میکروتیک محدود کرده و مابقی موارد (حجم مصرفی روزانه و هفتگی و ماهانه و...) را به کریو منتقل کنیم.

بعد از اتصال کاربر با **VPN** به **Mikrotik** در قسمت **Queue** همانطور که مشاهده می کنید یک **Simple Queue** متناسب با تنظیمات قیمت **Limit** در **PPP Profile** ایجاد می شود:

#	Name	Target	Upload Max Limit	Download Max Limit	Packet Marks	Total Ma
0 D	<pptp-behdad>	<pptp-behdad>	1M	1M		

در سمت کاربران فقط نیاز به ساخت یک اتصال VPN می باشد که من در این سناریو با توجه به اینکه روی میکروتیک PPTP Server راه اندازی کردم همین اتصال را برای کاربر ایجاد می کنم.



در صورتی که سیستم کاربر ما join به دامین شده باشد و کاربر با شناسه و رمز دامین خود لاگین کرده باشد با فعال کردن گزینه **Automatically use my Windows logon name and password** در زمان اتصال کاربر نیازی به وارد کردن شناسه و رمز دامنه نمی باشد و کانکشن کاربر بصورت خودکار متصل می شود.

در این زمان تمام فعالیت کاربر توسط Kerio مدیریت می شود و می توانید سایت های خاصی را فیلتر کنید یا دانلود فایل های خاصی را محدود نمایید و ...

نحوه مدیریت ترافیک شبکه با میکروتیک و کریو کنترل

Web	
Alert	
Config	
Connection	
Debug	
Dial	
Error	
Filter	
Host	
Http	
Security	
Warning	
Web	

[16/Apr/2018 16:21:21] 192.168.5.1 behdad@rahmani.com	کجا و به صرفه بخر، استایل باکس، ست برند های معتبر پوشاک"
[16/Apr/2018 16:21:21] 192.168.5.1 behdad@rahmani.com	"فرادرس: بزرگترین مرجع فیلمهای آموزشی" http://beta.kapri.com
[16/Apr/2018 16:21:21] 192.168.5.1 behdad@rahmani.com	"آموزش های ویدئویی منابع کنکور کارشناسی ارشد" http://beta.kapri.com
[16/Apr/2018 16:21:21] 192.168.5.1 behdad@rahmani.com	"آموزش های ویدئویی منابع کنکور کارشناسی ارشد" http://beta.kapri.com
[16/Apr/2018 16:21:21] 192.168.5.1 behdad@rahmani.com	"آموزش های ویدئویی منابع کنکور کارشناسی ارشد" http://beta.kapri.com
[16/Apr/2018 16:21:21] 192.168.5.1 behdad@rahmani.com	"فیلمهای آموزشی طراحی و برنامه نویسی وب" http://beta.kapri.com
[16/Apr/2018 16:21:22] 192.168.5.1 behdad@rahmani.com	"فرادرس: بزرگترین مرجع فیلمهای آموزشی" http://beta.kapri.com
[16/Apr/2018 16:21:22] 192.168.5.1 behdad@rahmani.com	"آموزش های ویدئویی منابع کنکور کارشناسی ارشد" http://beta.kapri.com
[16/Apr/2018 16:21:23] 192.168.5.1 behdad@rahmani.com	"فیلمهای آموزشی طراحی و برنامه نویسی وب" http://beta.kapri.com
[16/Apr/2018 16:21:24] 192.168.5.1 behdad@rahmani.com	بود عملکرد حافظه رم و - Chris-PC RAM Booster v4.60 دانلود"
[16/Apr/2018 16:21:24] 192.168.5.1 behdad@rahmani.com	"صدها ساعت فیلم آموزشی رایگان در فرادرس" http://beta.kapri.com
[16/Apr/2018 16:21:24] 192.168.5.1 behdad@rahmani.com	"فرادرس: بزرگترین مرجع فیلمهای آموزشی" http://beta.kapri.com
[16/Apr/2018 16:21:24] 192.168.5.1 behdad@rahmani.com	"فرادرس: بزرگترین مرجع فیلمهای آموزشی" http://beta.kapri.com
[16/Apr/2018 16:21:24] 192.168.5.1 behdad@rahmani.com	موقع فیلمهای آموزشی درس کنکور مشترک رشته های فنی" http://beta.kapri.com
[16/Apr/2018 16:21:24] 192.168.5.1 behdad@rahmani.com	"در دیجی استایل Gucci جدیدترین عینک های برند گوجهی" http://beta.kapri.com
[16/Apr/2018 16:21:25] 192.168.5.1 behdad@rahmani.com	"صدها ساعت فیلم آموزشی رایگان در فرادرس" http://beta.kapri.com
[16/Apr/2018 16:21:25] 192.168.5.1 behdad@rahmani.com	"آموزش های ویدئویی منابع کنکور کارشناسی ارشد" http://beta.kapri.com
[16/Apr/2018 16:21:25] 192.168.5.1 behdad@rahmani.com	"صدها ساعت فیلم آموزشی رایگان در فرادرس" http://beta.kapri.com
[16/Apr/2018 16:21:25] 192.168.5.1 behdad@rahmani.com	"فرادرس: بزرگترین مرجع فیلمهای آموزشی" http://beta.kapri.com
[16/Apr/2018 16:21:26] 192.168.5.1 behdad@rahmani.com	"مجموعه فیلمهای آموزشی برنامه نویسی اندروید" http://beta.kapri.com
[16/Apr/2018 16:21:26] 192.168.5.1 behdad@rahmani.com	"را در دیجی استایل بینید Skechers جدیدترین مدلهای" http://beta.kapri.com
[16/Apr/2018 16:21:27] 192.168.5.1 behdad@rahmani.com	"صدها ساعت فیلم آموزشی رایگان در فرادرس" http://beta.kapri.com
[16/Apr/2018 16:21:27] 192.168.5.1 behdad@rahmani.com	"آموزش های ویدئویی منابع کنکور کارشناسی ارشد" http://beta.kapri.com
[16/Apr/2018 16:22:36] 192.168.5.1 behdad@rahmani.com	"faradars.org" http://beta.kapri.com/a/go.php?url=https://faradars.org/how-to-
[16/Apr/2018 16:22:38] 192.168.5.1 behdad@rahmani.com	"بخش های رایگان آموزش جاوا" https://faradars.org/how-to-
[17/Apr/2018 09:03:59] 192.168.5.1 behdad@rahmani.com	"تدبیر اندیشان درسا" http://dorsaco.net/

با سپاس
بهداد رحمانی