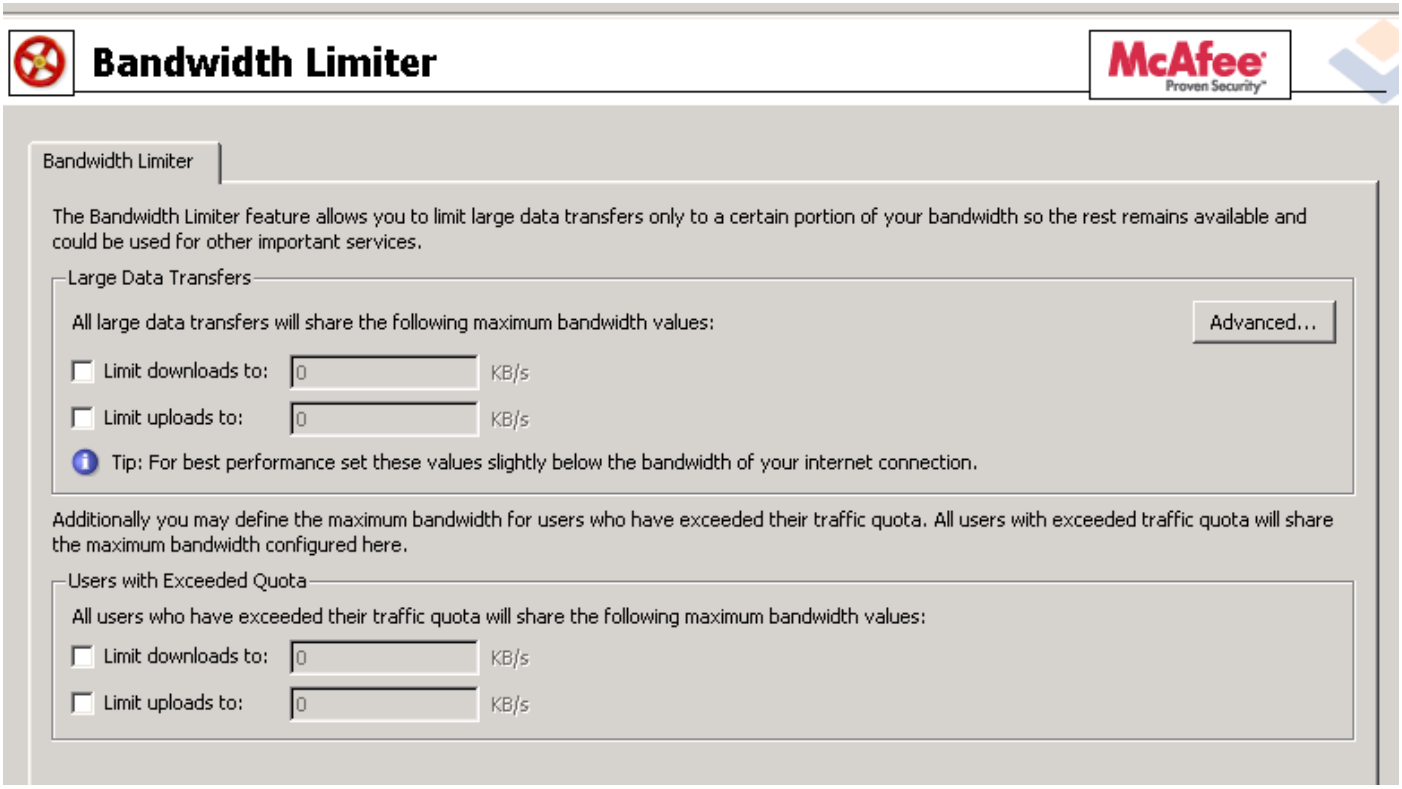
عنوان	**برنامه فایروال وینروت کریو – بخش چهارم، مدیریت مصرف کاربران LAN Accounting**
عنوان اصلی	**Kerio WinRoute Firewall 6, LAN accounting**
کلمات کلیدی	Network, Firewall, Server, Windows, Proxy, Filter, Cache, Internet, NAT, Port, TCP , UDP, Proxy, DNS Forward, Filter, Bandwidth Limit, LAN Accounting شبکه، دیوار آتش، فایروال، ویندوز، سرور، اینترنت، کنترل، فیلتر، پروکسی، پورت، محدودیت پهنای باند
مؤلف	مهدی عبداللهی
مرجع	
سطح	متوسط
مترجم	
تاریخ انتشار	۲۰ اردیبهشت ۱۳۹۰
تعداد صفحه	۲۶
فایل های ضمیمه	

در بخش چهارم و پایانی این سری مقاله به محدودیت مصرف اینترنت و به بیان دیگر سهمیه بندی مصرف اینترنت در شبکه ی محلی می پردازیم. در این مقاله نخست فرض بر این داریم که شما در شبکه تان اکتیو دایرکتوری دارید و روش کار را نیز در همین نوع شبکه بیان می کنیم. در پایان مقاله برای شبکه های عادی نیز روشی را یاد می دهیم که شما بتوانید بدون اکتیو دایرکتوری هم از این امکان فایروال کریو استفاده نمایید.

محدود کننده ی پهنای باند Bandwidth Limiter

این پنجره را از شاخه ی Configuration باز کنید. دو بخش برای تنظیم این بخش هست که می توانید از هر کدام به دلخواه استفاده نمایید. نخست تبادل بسته های داده ی حجیم (Large Data Transfers) که از این طریق می توانید برای داده های حجیم محدودیت ایجاد کنید به طوری که فشاری به پهنای باند وارد نکنند و باعث نگردند که تمام سرعت اینترنت توسط یک یا چند کاربر به طور کامل اشغال شود. در واقع می توانید برای داده هایی که از شبکه ی بیرون به داخل منتقل می شوند (یا همان دانلود ها) و همچنین داده های داخل به بیرون (یا همان آپلود ها) برای کاربرانی که سهمیه ی دانلود یا آپلودشان تمام شده است، محدودیت در سرعت ایجاد کنید. البته این دو هیچ وابسته گی به هم ندارند و می توانید به صورت مستقل نیز از این محدودیت ها استفاده نمایید. چرا که



توجه داشته باشید که در این بخش از نرم افزار کریو فایروال، محدودیت ها بر حسب کیلوبایت بر ثانیه (KB/s) است در حالی که سرویس دهنده ها پهنای باند را بر حسب کیلوبیت بر ثانیه (Kb/s) یا مگابیت بر ثانیه (Mb/s) محاسبه می کنند. هر ۸ بیت یک بایت را تشکیل می دهند بنا بر این برای مثال ۲۵۶ کیلوبیت بر ثانیه یعنی ۳۲ کیلوبایت بر ثانیه. یا ۱ مگابیت بر ثانیه یعنی ۱۲۸ کیلوبایت بر ثانیه.

تعیین مقدار محدودیت ها

در بخش بالای این پنجره مقدار محدودیت سرعت برای دانلود و آپلود را برای تبادل داده های حجیم می توانید تعیین کنید. با این کار پهنای باند مورد نظر شما برای داده های حجیم و باقی مانده ی پهنای باند برای ترافیک های دیگر اختصاص داده می شود.

تجربه نشان داده که اگر این میزان را حدود ۹۰ درصد کل پهنای باند تعیین کنید کارآیی مطلوب را خواهد داشت. اگر خیلی بیشتر از این مقدار باشد در آن صورت سرعت لازم برای سایر ترافیک های اینترنت باقی نمی ماند و اگر خیلی کمتر از این مقدار باشد در آن صورت بخش بزرگی از پهنای باند بدون استفاده می ماند.

نکته: برای این که تنظیمات این بخش بهینه باشد لازم است که با مقادیر واقعی پهنای باند کار کنید که این مقدار با آنچه سرویس دهنده ی اینترنت (ISP) به شما اعلام کرده در عمل متفاوت است. یکی از راه های تشخیص پهنای باند واقعی استفاده از نمودار های آماری ترافیکی است. این کار را باید در فاصله ی زمانی که می دانید حداکثر پهنای باند در حال استفاده است انجام دهید. (بخش Statistics نرم افزار کریو)

در بخش پایین این پنجره محدودیت سرعت دانلود و آپلود برای کاربرانی که سهمیه ی دانلود و آپلود آن ها به پایان رسیده است، تعریف می شود. این پهنای باند بین کاربرانی که سهمیه ی شان تمام شده است به اشتراک گذاشته می شود. یعنی مجموع ترافیک این کاربران با همدیگر برابر با مقداری خواهد بود که در این جا تعیین نموده اید.

هیچ مقدار بهنیه ای برای این بخش توصیه نشده است و مدیر سیستم باید خود تصمیم بگیرد. باید این مقادیر رو به گونه ای تنظیم کنید که فعالیت این کاربران اثر نامطلوب روی کاربران دیگر نداشته باشد.

نکته: در نظر داشته باشید که می توان کاربری را که سهمیه اش به پایان رسیده به طور کامل مسدود کرد که دسترسی به اینترنت نداشته باشد. محدودیتی که در اینجا تعریف شده است برای مواردی به کار می رود که نخواهیم کاربر را به طور کامل مسدود کنیم و صرفا سرعت دسترسی اینترنت را برای شان کم کنیم.

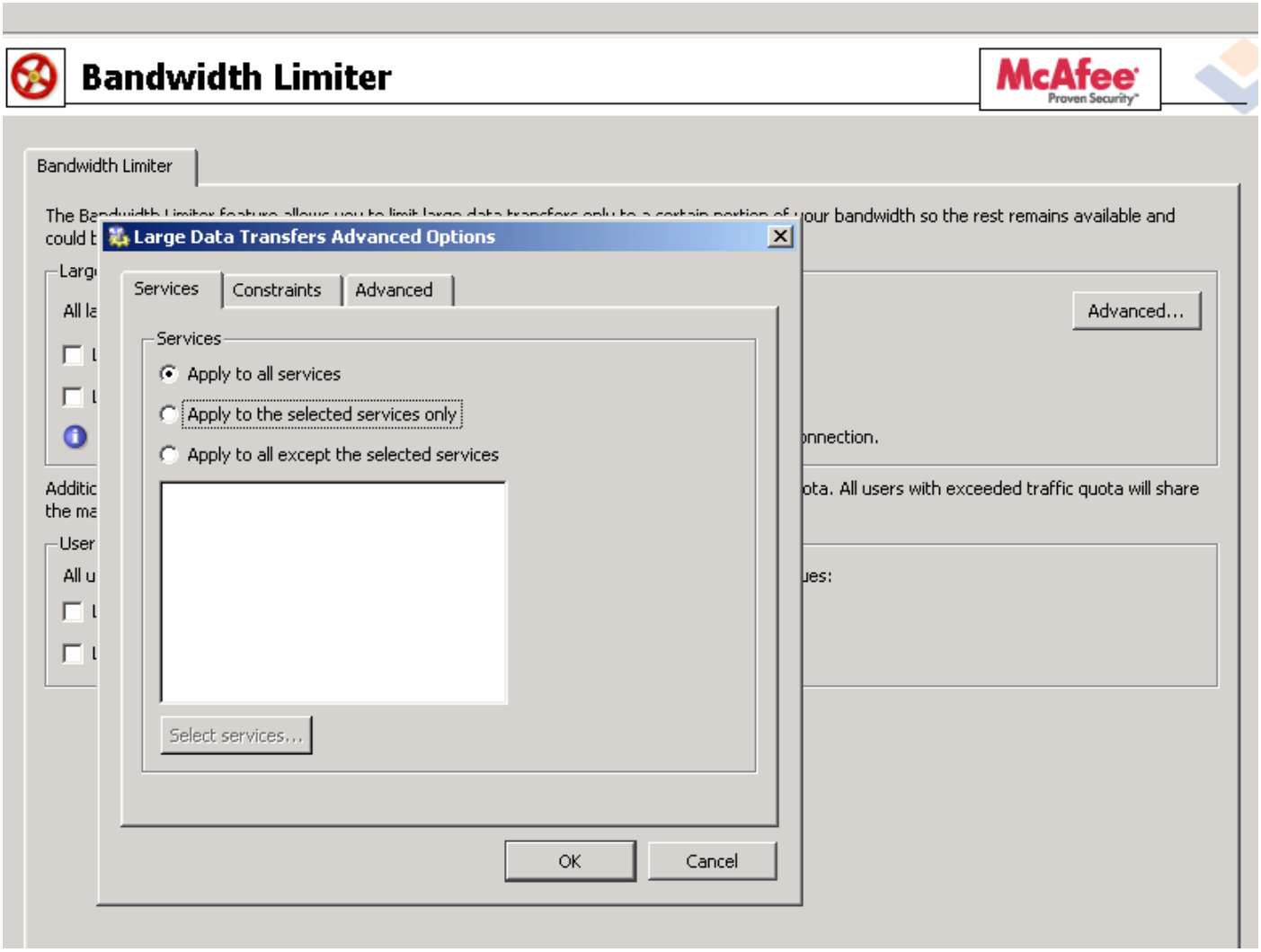
تنظیمات پیشرفته

دکمه ی Advanced را برای تنظیمات پیشرفته ی محدود کننده ی پهنای باند کلیک کنید. این پارامتر ها فقط برای داده های حجیم اعمل می شود. این تنظیمات برای کاربرانی که سهمیه ی اینترنت شان به پایان رسیده باشد، اعمال نخواهد شد.

Services

برخی سرویس ها به نظر می آید که پر مصرف باشند، در حالی که در عمل این طور نیستند. مثلا سرویس تلفن اینترنتی (Voice Over IP – VOIP) یکی از این ها است. در فایروال کریو این امکان هست که در بخش محدود کننده ی پهنای باند تعدادی از سرویس ها را از این امر مستثنی کنیم که این محدودیت روی آن ها اعمال نشود.

در عین حال می توانیم محدودیت پهنای باند را فقط برای سرویس های خاصی تعریف کنیم. مثلا زمانی که بخواهیم دانلود از طریق HTTP و FTP را محدود کنیم.



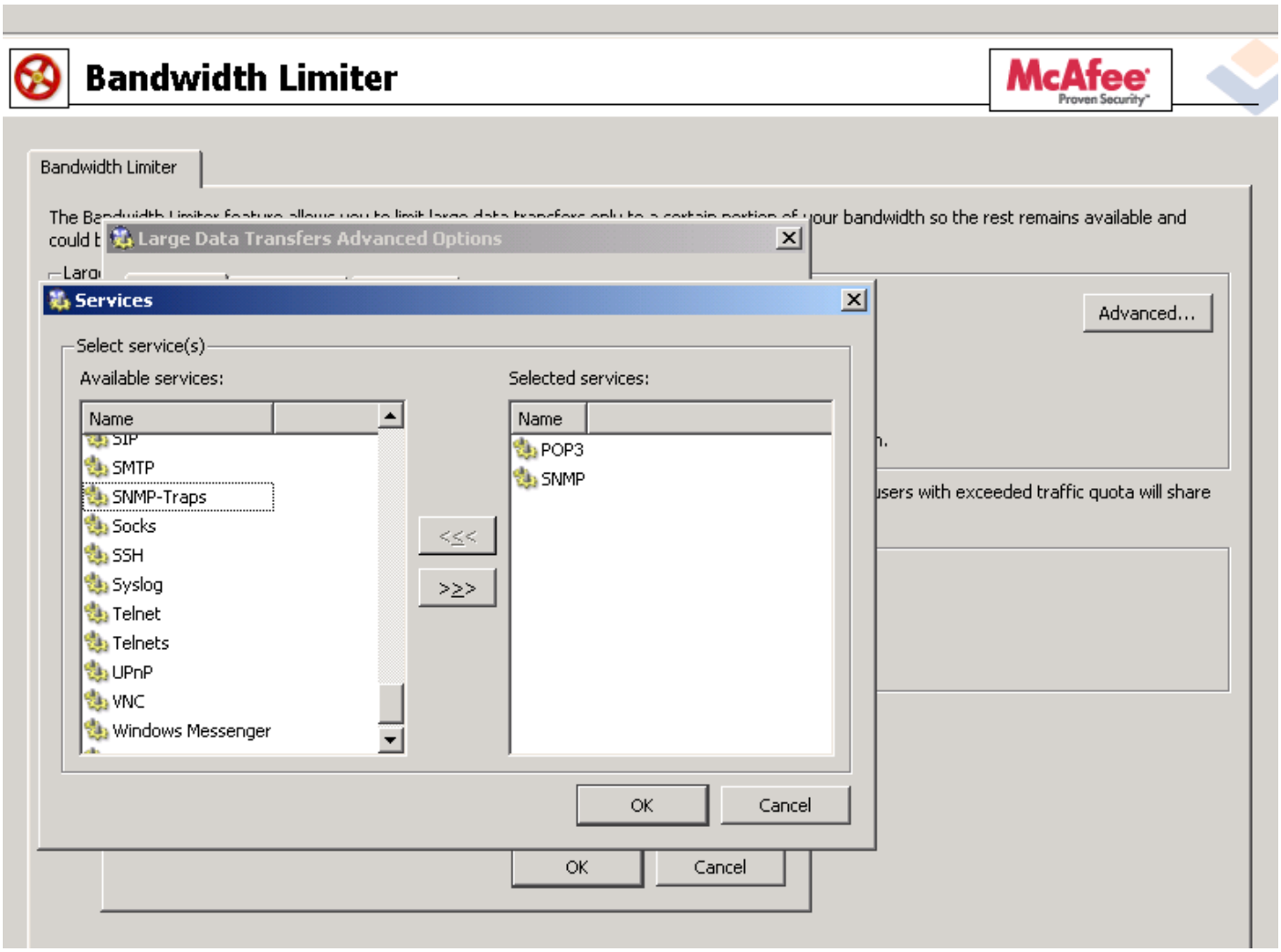
پنجره ی Services این امکان را می دهد سرویس هایی را که قرار است محدودیت پهنای باند بر آن ها اعمال شود، تعریف نماییم:

Apply to all services: محدودیت ترافیک به تمامی سرویس هایی که بین شبکه ی محلی و اینترنت جریان دارند، اعمال می شود.

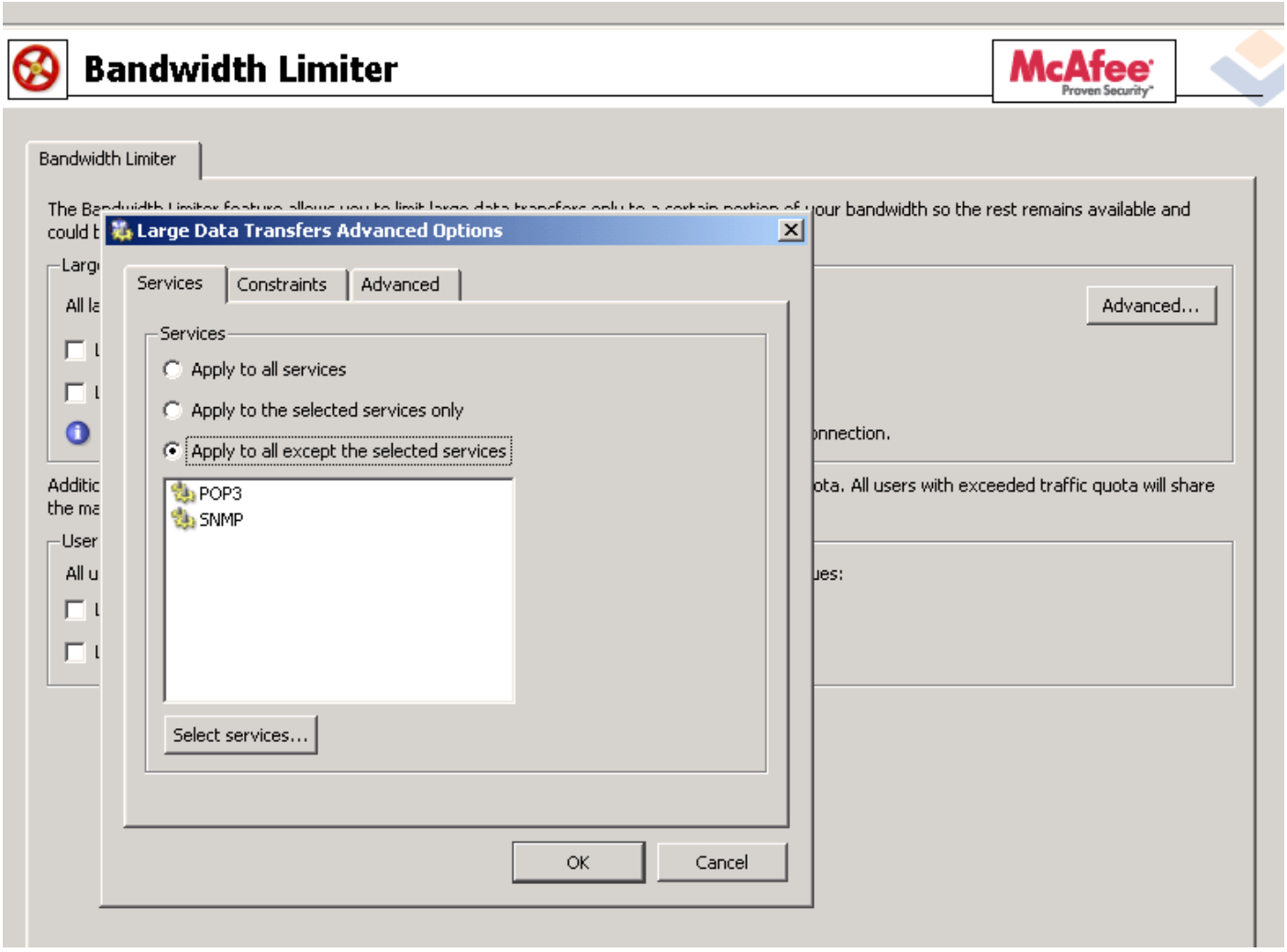
Apply to the selected services only: محدودیت ترافیک فقط برای سرویس های تعیین شده اعمال می شود و دیگر سرویس ها بدون محدودیت خواهند بود.

Apply to all except the selected services: سرویس های تعیین شده بدون محدودیت خواهند بود و به جز این ها، تمامی سرویس ها شامل محدودیت ترافیک خواهند شد.

روی دکمه ی Select Services کلیک کنید تا پنجره ی انتخاب سرویس ها باز شود. با نگه داشتن کلید Ctrl یا Shift صفحه کلید می توانید هم زمان چند سرویس را انتخاب نمایید. تمامی سرویس ها در بخش Configuration->Definition->Services تعریف شده اند.



بسته به اولویت سازمان می توانید سرویس ها را محدود کنید. مثلا در سازمانی که ارسال و دریافت اطلاعات از طریق ایمیل، اولویت بالاتری نسبت به دانلود از طریق وب و ... دارد، می توانید سرویس های مربوط به ایمیل یعنی POP3، SMTP و IMAP را بدون محدودیت تعریف نمایید و بقیه ی سرویس ها به طور خودکار محدود خواهند شد.



محدودیت بر مبنای آدرس آی پی و محدوده ی زمانی

گاهی ممکن است بخواهیم که محدودیت پهنای باند را فقط روی آدرس خاصی اعمال نماییم. مثلا سرور ایمیل که در شبکه ی داخلی قرار دارد و ممکن است ترافیک سنگین از شبکه ی بیرونی (اینترنت) روی این سرور قرار گیرد. در چنین حالتی مثلا اگر ایمیل های ورودی به سرور ایمیل زیاد باشد ممکن است تمامی ترافیک را در لحظاتی به خود اختصاص دهد و باعث شود که مثلا دانلود از صفحات وب و سایر سرویس ها به طور کامل متوقف شود. در این حالت وقتی که محدودیت پهنای باند را روی آدرس آی پی سرور ایمیل اعمال می کنیم، در نتیجه ایمیل ها با تأخیر وارد سرور می شوند ولی در عوض بقیه ی سرویس ها از کار نمی افتند.

یا این که ممکن است ترافیک به سمت یک آدرس آی پی خاصی در اینترنت (مثلا سرور وب شرکت) محدود کنیم.

این گروه آدرس آی پی می توانند شامل هر آدرسی خواه در شبکه ی داخلی یا در شبکه ی اینترنت باشند. زمانی که کامپیوتر های کلاینت در شبکه ی داخلی دارای آی پی ثابت باشند (یعنی از DHCP استفاده نکنند) از این طریق می توانیم کاربران خاصی را از روی آدرس شان محدود کنیم.

همچنین محدودیت پهنای باند را در محدوده ی زمانی خاص هم می توان اعمال کرد. مثلا در ساعت کاری.

این دو پارامتر در بخش Constraints (قید ها) تنظیم می شوند.

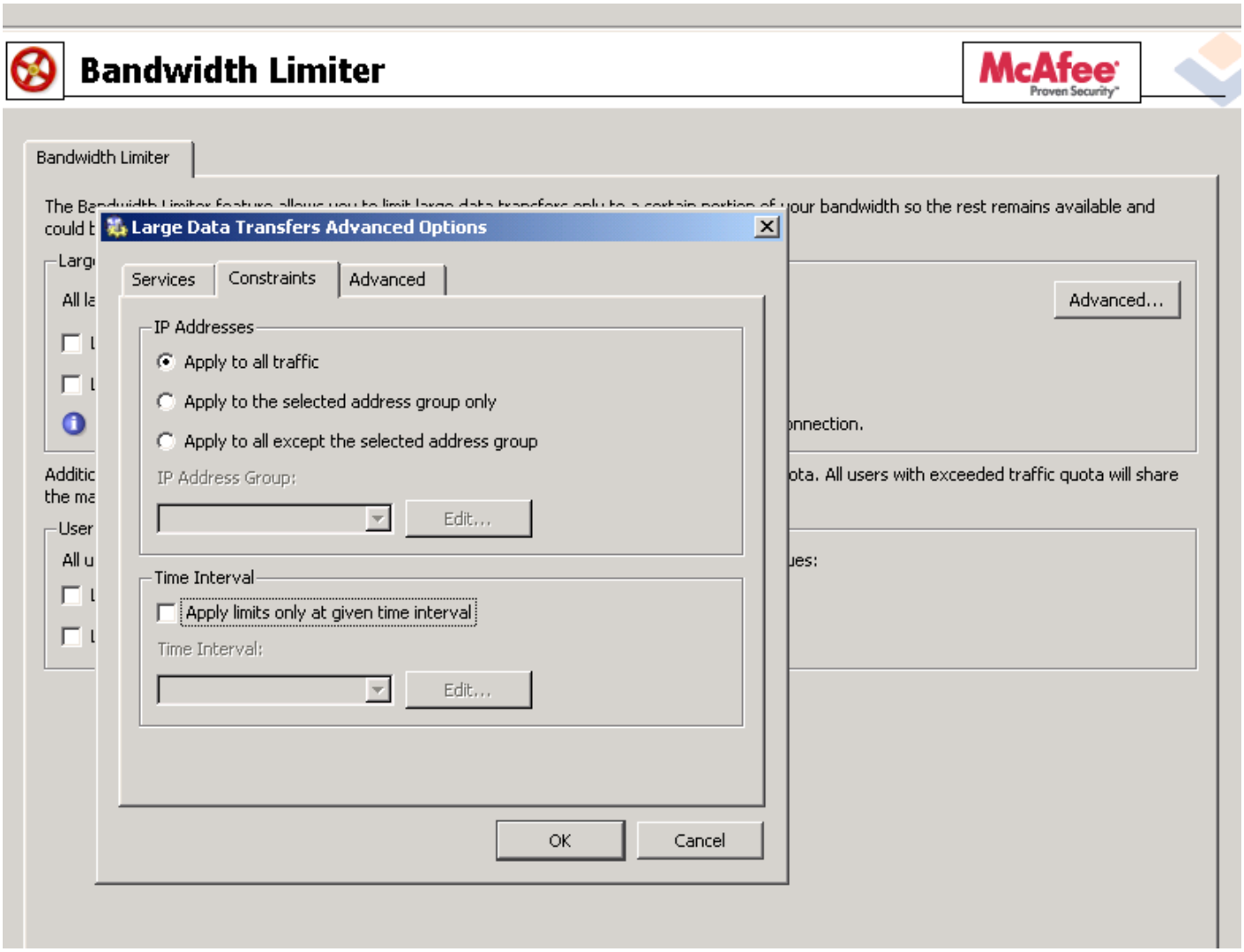
در بخش بالای برگه ی Constraints روش اعمال محدودیت پهنای باند بر مبنای آدرس آی پی را انتخاب نمایید و همچنین می توانید از همین جا به طور مستقیم گروه های آدرس آی پی را نیز تعریف نمایید.

Apply to all traffic: محدودیت برای تمامی آدرس های آی پی اعمال می شود. در این حالت بخش IP Address Group غیر فعال است.

Apply to the selected address group only: اگر یکی از آدرس ای پی های مربوط به یک اتصال به این گروه آدرس متعلق باشد، محدودیت اعمال می شود و در غیر این صورت اعمال نخواهد شد.

Apply to all except the selected address group: محدودیت پهنای باند اعمال نخواهد شد اگر حداقل یکی از آی پی های مربوط به اتصال شبکه به گروه آدرس انتخاب شده متعلق باشد. در بقیه ی موارد محدودیت اعمال می شود.

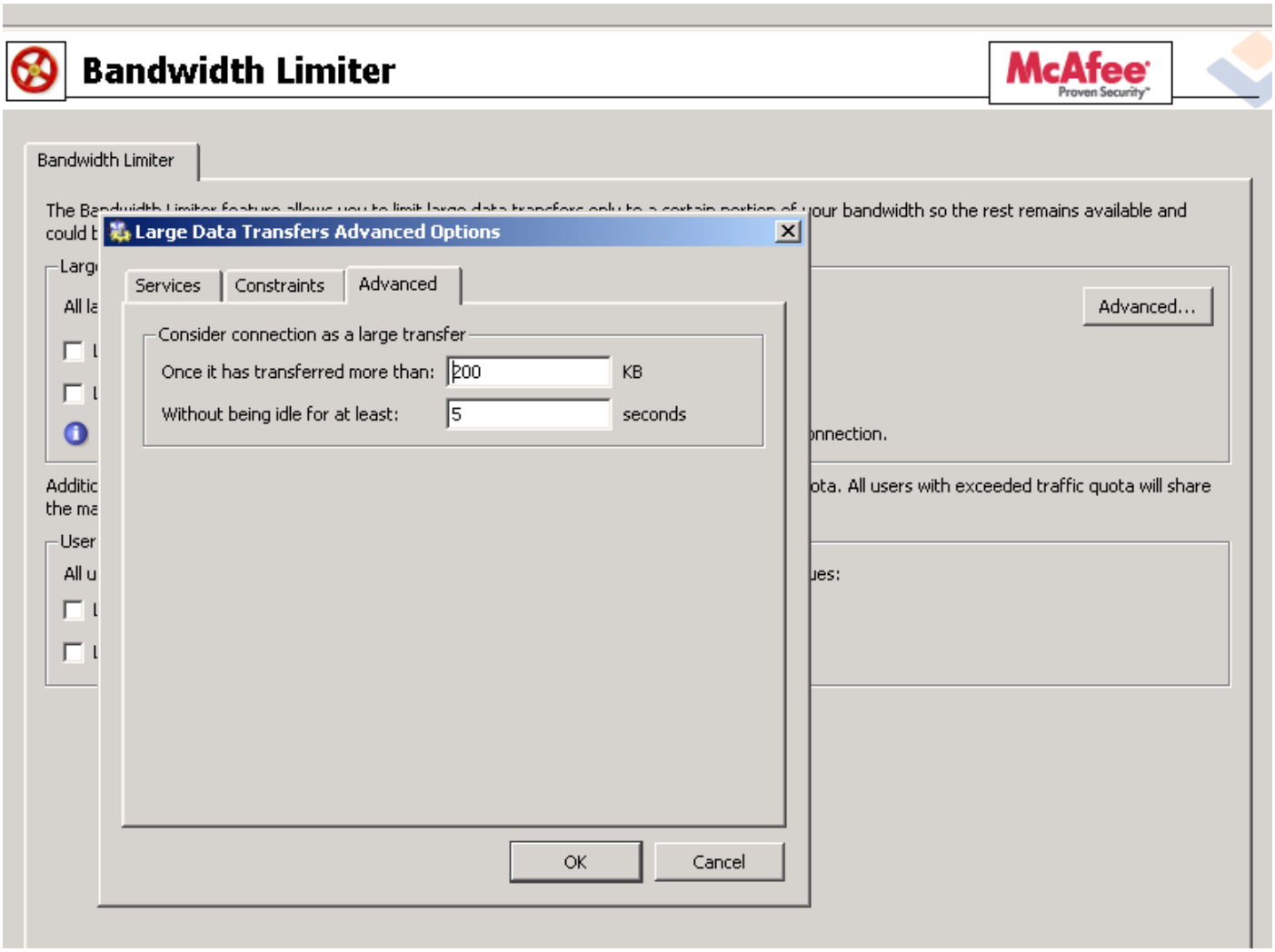
در بخش پایین این پنجره فاصله ی زمانی برای اعمال محدودیت پهنای باند را می توانید تعیین کنید یا این که از طریق دکمه ی Edit یک فاصله ی زمانی جدید تعریف و استفاده کنید.



تنظیم پارامتر ها برای تشخیص داده های حجیم

در برگه ی Advanced باید دو مقدار را تعیین کنیم، حداقل اندازه ی داده های انتقالی بر حسب کیلوبایت و فاصله ی زمانی توقف انتقال داده. مقدار های پیش فرض (۲۰۰کیلوبایت و ۵ ثانیه) پس از آزمایش های متعدد در شرایط واقعی تعیین شده اند.

توجه داشته باشید که تغییر این مقادیر ممکن است باعث افت کارآیی محدود کننده ی پهنای باند شود. مگر در موارد استثنایی (برای آزمایش) که بخواهید مقادیر مورد نظر خودتان را در این بخش قرار دهید.



تشخیص اتصالات با انتقال داده ی حجیم

در این بخش اطلاعاتی را در مورد روش تشخیص داده های حجیم بیان می کنیم که البته برای استفاده از محدود کننده ی پهنای باند به دانستن این ها نیاز ندارید.

ترافیک شبکه برای سرویس های مختلف فرق می کند. برای مثال مرورگر های وب معمولا یک یا چند اتصال را برای باز کردن سایت ها استفاده می کنند تا مقدار مشخصی از داده ها (شامل اشیای داخل صفحه) را دریافت و سپس اتصال را ببندند. سرویس های ترمینال (مانند telnet و SSH) معمولا یک اتصال باز را برای انتقال داده های کم حجم ولی طولانی مدت استفاده می کنند. داده های حجیم معمولا بدین روش عمل می کنند که جریان داده را به صورت پیوسته و با مکث های زمانی کوتاه بین بسته های اطلاعاتی انتقال می دهند.

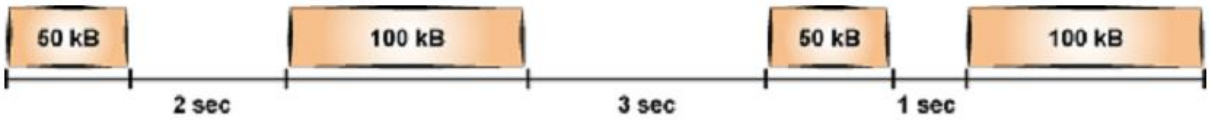
دو پارامتر اصلی در هر اتصال بررسی می شوند: حجم داده ی انتقالی و بیشترین زمان توقف یا بی کار بودن انتقال داده. اگر حجم داده ها بدون سپری شدن فاصله ی زمانی توقف انتقال داده، از میزان مشخصی بیشتر بشود، اتصال مذکور به صورت انتقال داده ی حجیم در نظر گرفته می شود و محدودیت های تعیین شده روی آن اعمال می گردد.

اگر زمان توقف، از میزان تعریف شده بیشتر شود، شمارنده ی انتقال داده دوباره مقدار صفر می گیرد و محاسبه از اول آغاز می شود. این یعنی اگر یک اتصال در طول زمان کارکرد خود یک بار از این پارامتر ها عبور نماید به عنوان اتصال با داده ی حجیم در نظر گرفته خواهد شد.

چند مثال

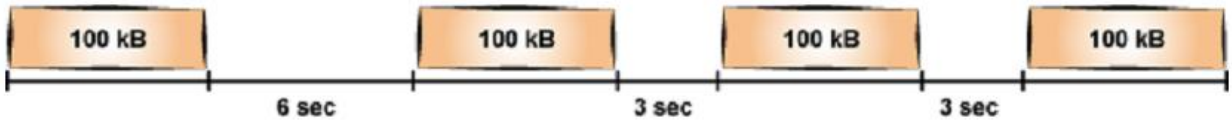
تنظیم پیش فرض به این صورت است: حداقل باید ۲۰۰ کیلوبایت متقل شود و در مدت انتقال آن توقف به مدت ۵ ثانیه یا بیشتر صورت نگیرد.

۱- در شکل زیر یک اتصال می بینید که پس از انتقال قطعه ی سوم داده ها، به صورت انتقال داده ی حجیم در نظر گرفته خواهد شد.در این مرحله، انتقال داده به حجم ۲۰۰ کیلوبایت صورت می گیرد در حالی که زمان توقف ۳ ثانیه است.



۲- در شکل زیر اتصال به صورت داده ی حجیم در نظر گرفته نمی شود چون پس از ۱۵۰ کیلوبایت، ۵ ثانیه توقف هست و پس از آن ۱۵۰ کیلوبایت دیگر منتقل می شود.

۳- در شکل زیر نخست ۱۰۰ کیلوبایت داده منتقل می شود و پس از آن ۶ ثانیه مکث هست. به همین دلیل شمارنده ی داده ها دوباره صفر می شود. سپس سپس سه بلوک ۱۰۰ کیلوبایتی داده منتقل می شوند. وقتی بلوک سوم داده ها منتقل می شود فقط ۲۰۰ کیلوبایت در شمارنده ثبت شده است. (تا زمانی که ۵ ثانیه سپری نشده باشد). چون فاصله زمانی توقف بین بلوک دوم و سوم داده ها ۳ ثانیه (کمتر از ۵ ثانیه ی تعیین شده) است، این اتصال از نوع انتقال داده ی حجیم در نظر گرفته می شود.



شناسایی کاربران

فایروال کریو این امکان را به مدیر شبکه می دهد که وضعیت ترافیک شبکه (بسته های اطلاعاتی، اتصال، صفحه وب یا اشیای FTP) مربوط به هر کاربر را نظارت نماید. نام کاربر در هر گزینه ی فیلترینگ (filtering rule)، آدرس آی پی کامپیوتری را که کاربر از آن وصل شده است، نشان می دهد. (مثلا تمام کامپیوتر هایی که کاربر هم اکنون از طریق آن ها وصل شده است) به عبارت دیگر یک گروه کاربری تمامی ادرس آی پی هایی را که اعضایش در حال حاضر از آن ها متصل شده اند، نشان می دهد.

در کنار محدودیت های دسترسی، شناسایی کاربران نیز می تواند برای نظارت بر کارکرد آنان با واسط کاربری کریو استار (Kerio StaR)، در بخش گزارش ها (Logs) ، فهرست اتصالات فعال و مرور کلی کاربران و کامپیوترها به کار برود. اگر کاربر شناسایی شده ای از یک کامپیوتر وصل نشده باشد، فقط آدرس آی پی آن در بخش گزارش ها و آمار نشان داده می شود. در بخش آمار (Statistics) ترافیک این کامپیوتر ها در یک گروه به نام کاربران ناشناس (not logged in) نمایش داده می شود.

روش های شناسایی کاربران توسط فایروال

هر کاربری که در کریو تعریف شده باشد می تواند توسط فایروال شناسایی شود و این شناسایی به سطح دسترسی و مجوز های کاربر، بستگی نخواهد داشت.

روش دستی: از طریق واسط کاربری وب کریو در مرورگر اینترنت

https://server:4081
http://server:4080

(نام سرور و شماره ی پورت فرضی هستند و می توانید آن ها را تغییر دهید. به جای نام سرور آدرس آی پی هم می توانید به کار ببرید)

در ضمن برای دیدن آمار استفاده ی کاربر در صفحه ی وب می توانید از آدرس های زیر استفاده نمایید:

https://server:4081/star
http://server:4080/star

و البته کاربر پس از ورود به این صفحه در فایروال هم به همین نام و آدرس شناسایی خواهد شد.

هدایت توسط مرورگر (redirection): هنگام ورود به یک سایت اینترنتی، بدون توجه به این که آیا ورود به این صفحه برای کاربران شناسایی شده مجاز باشد یا خیر.

استفاده از NTLM: اگر مرورگر اکسپلورر میکروسافت یا فایرفاکس موزیلا به کار ببرید و کاربر در شبکه ی دامین ویندوز ان تی یا اکتیو دایرکتوری شناسایی شده باشد، در این حالت بدون نمایش صفحه ی ورود به فایروال، کاربر شناسایی خواهد شد. برای این کار تنظیماتی لازم است که اشاره خواهم کرد.

خودکار: آدرس آی پی کامپیوتر هایی را که قرار است کاربران شان به طور خودکار شناسایی شوند، می توانید به نام کاربر ها منتسب کنید. در این حالت هر ترافیک شبکه ای که از آدرس آی پی مورد نظر تشخیص داده شود، فرض بر این خواهد بود که کاربر مشخصی (که شما تعیین کرده اید) در حال استفاده از شبکه است. در عین حال کاربر می تواند از کامپیوتر های دیگر هم با روش های قبلی که بیان کردیم شناسایی شود. آدرس آی پی برای شناسایی خودکار یک کاربر می تواند در بخش user account تعیین گردد.

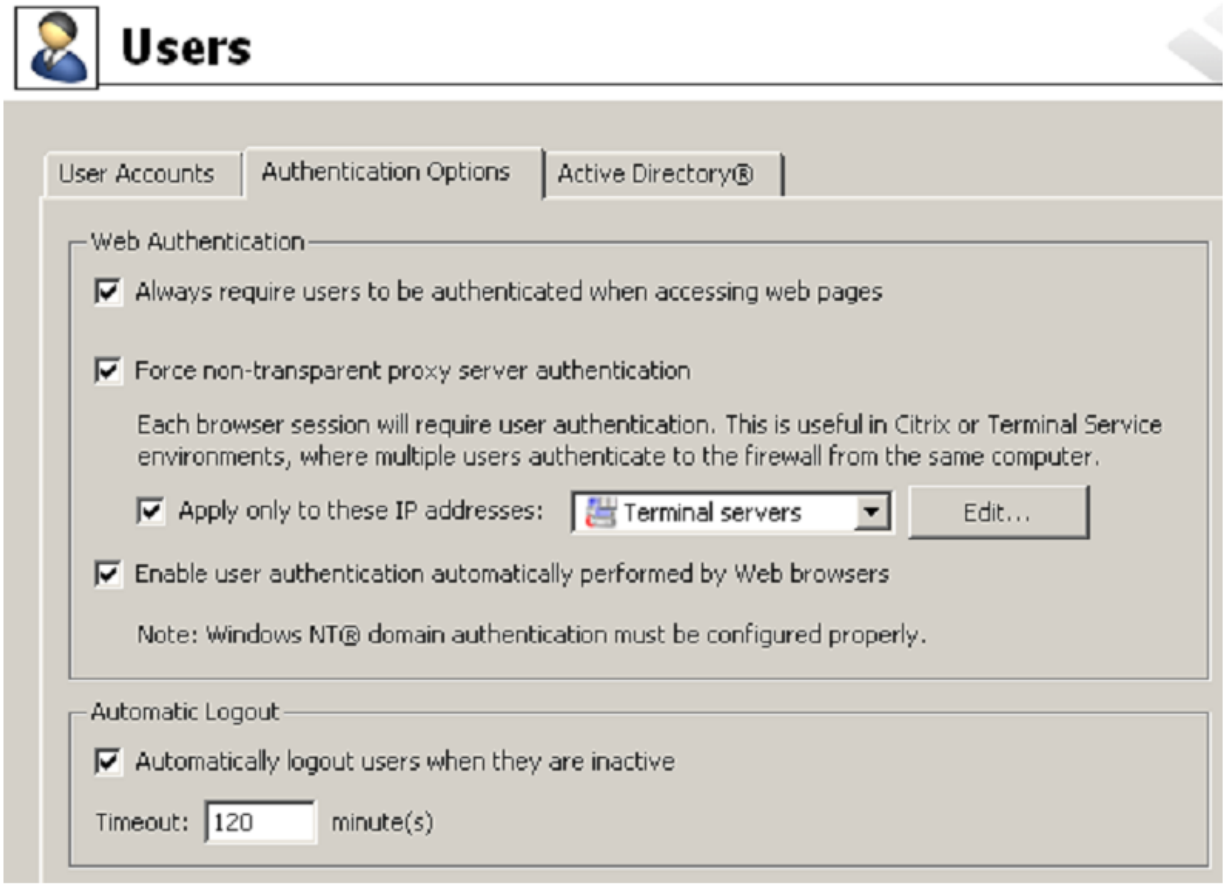
توجه داشته باشید اگر بیش از یک کاربر از یک کامپیوتر استفاده می کنند، روی آن کامپیوتر شناسایی خودکار کاربر را تعریف نکنید. نکته ی بعدی این که اگر آدرس آی پی کامپیوتر به گونه ای هست که در فاصله های زمانی ممکن است تغییر کند (مثلا تنظیم عمومی با DHCP) در این حالت هم شناسایی خودکار کاربر ممکن نیست. مگر این که آدرس آی پی را به صورت دستی تنظیم کنید یا در تنظیماتDHCP به گونه ای باشد که روی آدرس مک (Mac Address) کارت شبکه شماره ی آی پی ثابتی تعیین شده باشد.

روش هدایت توسط مرورگر بدین روش است: کاربر آدرس صفحه ی وب دلخواه خود را در مرورگر وارد می کند. اگر کاربر شناسایی نشده باشد، توسط کریو به صفحه ی ورود کاربر هدایت می شود. پس از ورود نام کاربری و گذرواژه، به طور خودکار به صفحه وب مورد نظر هدایت خواهد شد و اگر ورود به صفحه وب مذکور ممنوع شده باشد در این مرحله یک صفحه نمایش داده می شود که در آن پیغام ممنوعیت ورود به صفحه ی وب مورد نظر نمایش داده خواهد شد.

کاربران بسته به تنظیمات کریو برای ورود به فایروال به صفحه ی امن (https) یا صفحه ی وب معمولی (http) هدایت می شوند. اگر هر دو حالت در تنظیمات فعال شده باشند، به طور پیش فرض صفحه ی امن نمایش داده خواهد شد.

گزینه های پیشرفته ی شناسایی کاربران

پارامتر های ورود و خروج را می توانید در برگه ی Authentication Options پنجره ی Users تنظیم کنید.



هدایت به صفحه ی شناسایی کاربر

اگر گزینه ی Always require users to be authenticated when accessing web pages را فعال نمایید، برای دسترسی به هر سایت باید کاربر شناسایی شود. روش شناسایی بستگی به مرورگر دارد:

Direct access: مرورگر به طور خودکار به صفحه ی شناسایی کاربر هدایت می شود و پس از ورود نام کاربر و گذرواژه از طریق واسط وب کریو، اگر اطلاعات شناسایی روشن باشد، صفحه ی وب نمایش داده خواهد شد.

Winroute proxy server: مرورگر یک پنجره برای ورود نام کاربری و گذرواژه نشان می دهد و پس از شناسایی موفق کاربر، صفحه ی وب نمایش داده می شود.

اگر گزینه ی Always require users to be authenticated when accessing web pages غیر فعال شود، صفحه ی شناسایی کاربر فقط هنگام دیدن صفحه هایی که در بخش URL rules برای کاربران شناسایی نشده در دسترس نیستند، نمایش داده خواهد شد.

نکته: شناسایی کاربر در هر دو مورد دسترسی به یک صفحه ی وب (یا سرویس های دیگر) و برای نظارت بر کارکرد یک کاربر مشخص لازم است.

Force non-transparent proxy server authentication

در شرایط عادی یک کاربر که از یک کامپیوتر مشخص به فایروال وصل شده است، با آدرس آی پی آن کامپیوتر شناسایی می شود تا زمانی که به صورت دستی از سیستم خارج شود یا به خاطر فعال نبودنش به طور خودکار خارج گردد. اما اگر کامپیوتر کلاینت امکان اتصال چند کاربر به صورت هم زمان را داشته باشد، (مانند ترمینال سرویس میکروسافت، سیتریکس یا سوئیچ کاربر در ویندوز ایکس پی، سرور ۲۰۰۳ ، ویستا، سون و سرور ۲۰۰۸) فایروال فقط برای نخستین کاربری که از اینترنت استفاده کند، شناسایی را انجام می دهد و بقیه ی کاربران با همان نام کاربر نخست شناسایی می شوند.

در مورد HTTP و HTTPS این مانع نادیده گرفته می شود. در کامپیوتر هایی که چند کاربر از آن ها استفاده می کنند، تنظیم بخش اتصال اینترنت مرورگر را به طور خودکار از طریق سرور پروکسی کریو انجام دهید. (توضیح کامل این کار در راهنمای نرم افزار هست) و گزینه ی Enable non-transparent proxy server را فعال نمایید. در این حالت برای هر صفحه ی جدید در هر مرورگر، نیاز به شناسایی کاربر خواهد بود.

الزام کاربران برای وارد کردن اطلاعات شناسایی برای هر صفحه ی جدید مرورگر، برای کاربرانی که روی کامپیوتر شان به صورت انفرادی کار می کنند دردسر ساز می شود. بدین منظور می توانید این قاعده را بر روی کامپیوتر های با ادرس آی پی خاص به کار ببندید. گزینه ی Apply only for these IP addresses البته به شرطی که آدرس آی پی کامپیوترهای چند کاربره متغیر نباشد.

Automatic authentication (NTLM)

با فعال سازی شناسایی خودکار کاربر اگر از مرورگر اینترنت اکسپلورر (۵.۰۱ یا بالاتر) یا فایرفاکس (نگارش ۱.۳ یا بالاتر) استفاده نمایید، شناسایی خودکار کاربر از طریق NTLM ممکن خواهد شد.

در این حالت به نام کاربر و گذرواژه نیازی نخواهد بود و شناسایی از طریق کاربری که به ویندوز وارد شده است انجام می گیرد. این روش شناسایی فقط در سیستم عامل ویندوز قابل استفاده است.

خروج خودکار کاربران به هنگام فعال نبودن شان

پارامتر Timeout یک فاصله ی زمانی بر حسب دقیقه است که در این مدت کاربر می تواند با اینترنت کار نکند. پس از گذشتن این زمان، کاربر به طور خودکار از فایروال خارج می شود. مقدار پیش فرض آن ۱۲۰ دقیقه است.

این گزینه برای زمانی که کاربر فراموش می کند از فایروال خارج شود، کارایی دارد. پس بهتر است این گزینه را غیر فعال نکنید چون در این صورت داده های مربوط به ورود یک کاربر ممکن است توسط کاربر دیگر استفاده شود.

با این مقدمات وارد مرحله ی LAN Accounting می شویم.

نرم افزار های متعددی برای بحث کنترل مصرف اینترنت یا همان LAN Accounting هم اکنون در بازار هستند که امکانات آن ها بیشتر به درد سرویس دهنده های حرفه ای اینترنت می خورد تا یک سازمان. برای ISP هم تعداد ساعت های مصرف می تواند مهم باشد و هم حجم داده های ارسالی (upload) و دریافتی (download). در حال حاضر که اینترنت پر سرعت با تکنولوژی DSL بیشتر استفاده می شود عملا مقوله ای به نام تعداد ساعت مصرف ماهیانه مطرح نیست و صرفا حجم مصرف محاسبه می گردد.

در این بخش راه اندازی سرویس LAN Accounting را به صورت گام به گام در نرم افزار فایروال کریو توضیح خواهم داد. برای این که راه اندازی این سرویس برای خواننده ی مطلب آسان باشد، جزئیاتی را که در این روش به کار نمی روند، توضیح نمی دهم و در مطالب تکمیلی به صورت مفصل از راهنمای نرم فزار ترجمه و منتشر خواهم کرد.

برای شبکه ای که می خواهیم اکانتینگ اینترنت راه اندازی کنیم، شرایط زیر در نظر گرفته شده اند:

- شبکه ی سیستم عامل ویندوز با سرور ۲۰۰۳ یا بالاتر و کلاینت های ویندوز ایکس پی یا بالاتر
- سرویس اکتیو دایرکتوری برای یک دامین (اتصال به چند دامین در نظر گرفته نشده است)
- تمامی کامپیوتر ها و کاربرانی که از اینترنت استفاده می کنند به اکتیو دایرکتوری متصل هستند
- کامپیوتر ها به طور مستقیم به مودم یا روتر وصل نیستند و سروری که نرم افزار کریو بر روی آن نصب شده است، از حداقل دو کارت شبکه استفاده می نماید که یکی از آن ها به اینترنت و دیگری به شبکه ی داخلی (مثلا با محدوده ی آی پی 192.168.0.x) وصل است.

گام نخست: معرفی کاربران - اتصال به اکتیو دایرکتوری

کریو به دو طریق می تواند کاربران را مدیریت کند:

- سیستم داخلی (Local User Database)
- اکتیو دایرکتوری

در سیستم داخلی معمولا نام کاربران و گذرواژه ی آن ها در فایلی داخل پوشه ی نصب برنامه ی کریو ذخیره می شود که به لحاظ ایمنی در سطح پایین تری است. اگر شبکه ی تان اکتیو دایرکتوی باشد، استفاده از سیستم داخلی برای کاربران باعث دوباره کاری برای آن ها در ورود نام و گذرواژه خواهد شد.

یک روش آن است که نام کاربران به صورت داخلی تعریف می شود ولی شناسایی آن ها از طریق گذرواژه در اکتیو دایرکتوری انجام می شود. در این حالت لازم است که نام کاربر در کریو منطبق با نام آن در سرور ویندوز باشد.

روش دیگر ورود (import) اطلاعات کاربران از اکتیو دایرکتوری است که نام کاربران فایروال منطبق بر نام کاربری آن ها در سرور ویندوز خواهد بود و این روش، مدیریت آن ها را آسان تر می سازد. ولی هر گونه تغییر در کاربران یا غیر فعال شدن آن ها نیاز مند به این است که ورود کاربران از سرور ویندوز دوباره صورت بگیرد و در شبکه هایی که تغییر و تحولات زیاد صورت می گیرد یا تعداد کاربران زیاد است این روش می تواند مشکلات عدم انطباق را به دنبال داشته باشد.

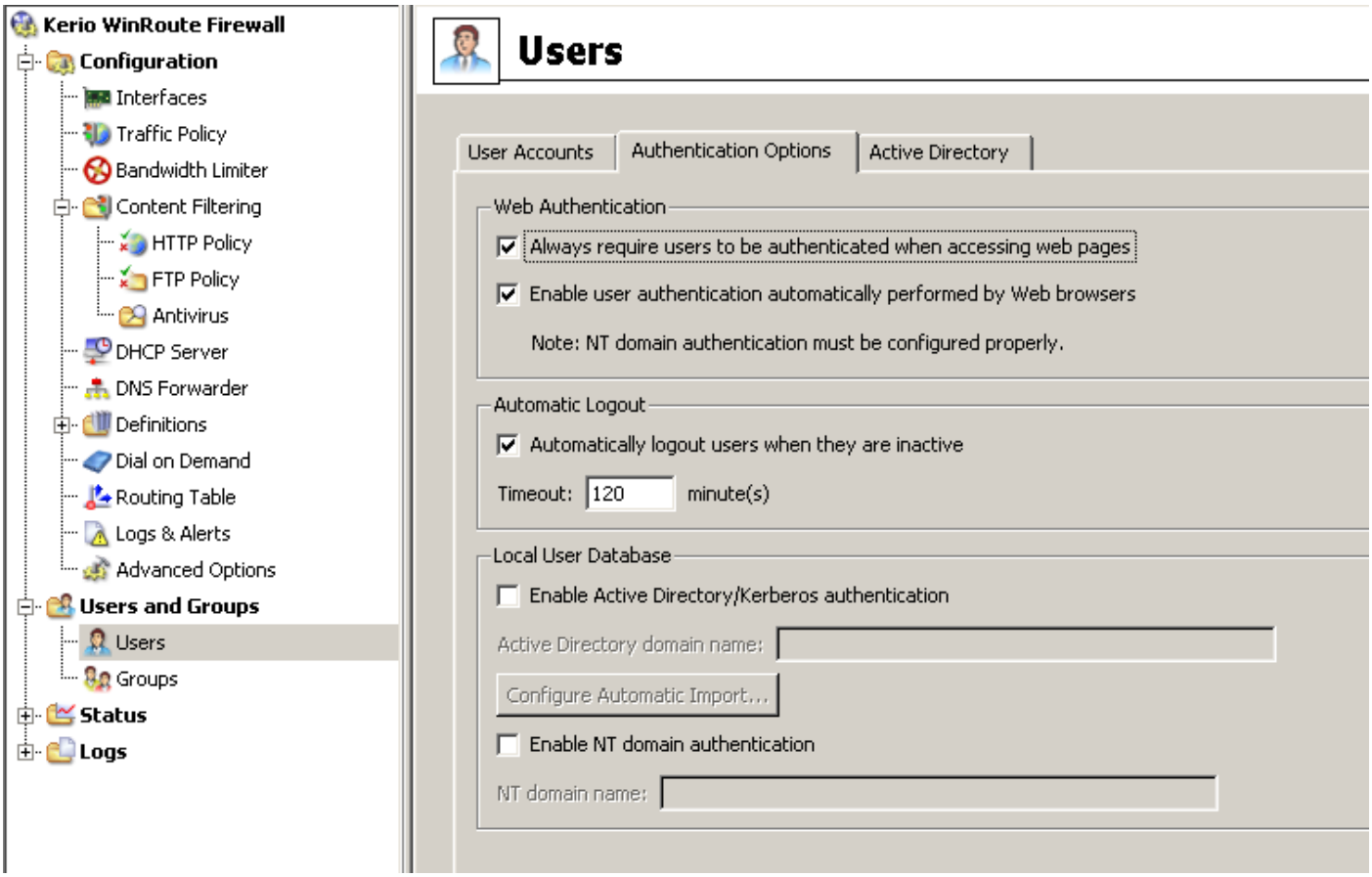
استفاده از سیستم داخلی کریو برای کاربران یک مزیت دارد و آن هم برای زمانی است که سرور اکتیو دایرکتوری به هر دلیل (مثلا خرابی) در دسترس نباشد. در شبکه هایی که اینترنت پرکاربرد و حیاتی است و فقط یک سرور اکتیو دایرکتوری (Domain Controller) مجزا از سرور فایروال وجود دارد، می توانیم برای احتیاط از این روش استفاده نماییم که در صورت از کار افتادن سرور اکتیو دایرکتوری، کاربران به مشکل برخورد نکنند.

لیکن ممکن است سیاست امنیتی که توسط شما به عنوان مدیر شبکه پیاده می شود بر این قاعده استوار شود که کار در شبکه باید همراه با اکتیو دایرکتوری باشد. البته برای پیاده سازی درست و پایدار چنین روشی لازم است که مقدمات آن را پیش بینی کرده باشید که از حوصله ی این بحث خارج است و به مبحث دیگری در باره ی نصب سرور های ویندوز مربوط می شود.

روش دیگر استفاده ی مستقیم از اکتیو دایرکتوری (mapping) است که نام کاربران و گذرواژه ی آنان در کریو ذخیره نمی شود. در این روش لازم است که:

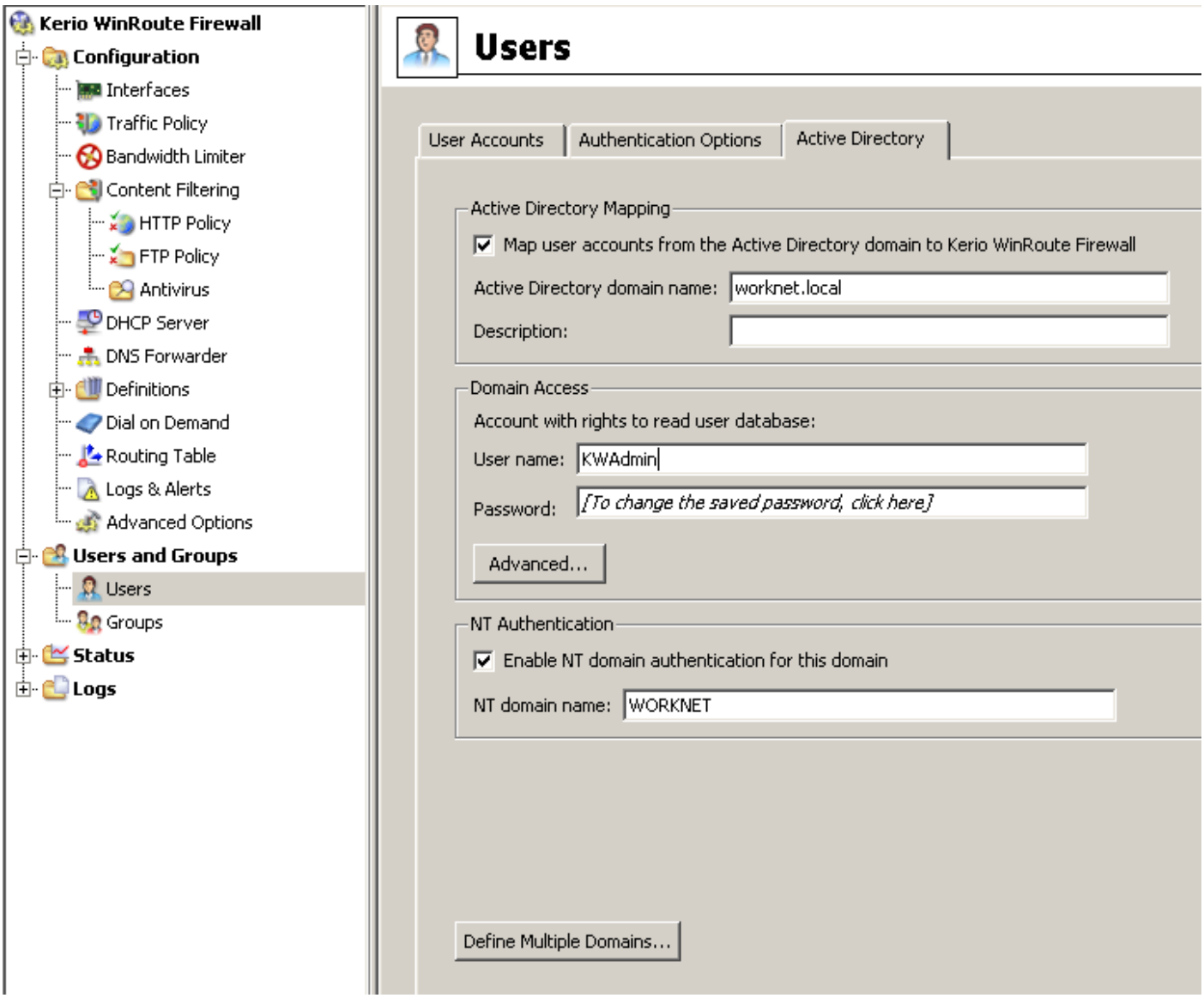
- کامپیوتری که فایروال روی آن نصب شده است باید متعلق به دامین مورد نظر باشد.
- سرور دامین کنترلر اکتیو دایرکتوری باید به عنوان سرویس دهنده ی نام اولیه (Primary DNS Server) تعریف شده باشد.

در بخش Authentication Options گزینه های مروبط به شناسایی کاربران را فعال نمایید. با توجه به این که از روش شناسایی مستقیم اکتیو دایرکتوری استفاده می کنید، این که کاربر ناشناس از طریق کامپیوتر لپ تاپ یا هر وسیله ی دیگری به شبکه متصل شود و از اینترنت بدون گذاشتن رد پا استفاده نماید، امکان پذیر نخواهد بود.
دو گزینه ی مربوط به Web Authentication را پیش تر توضیح داده ایم. البته تصویر پیشین مربوط به نگارش ۶.۵ و این تصویر مربوط به نگارش ۶.۲ است که گزینه های کمتری دارد.

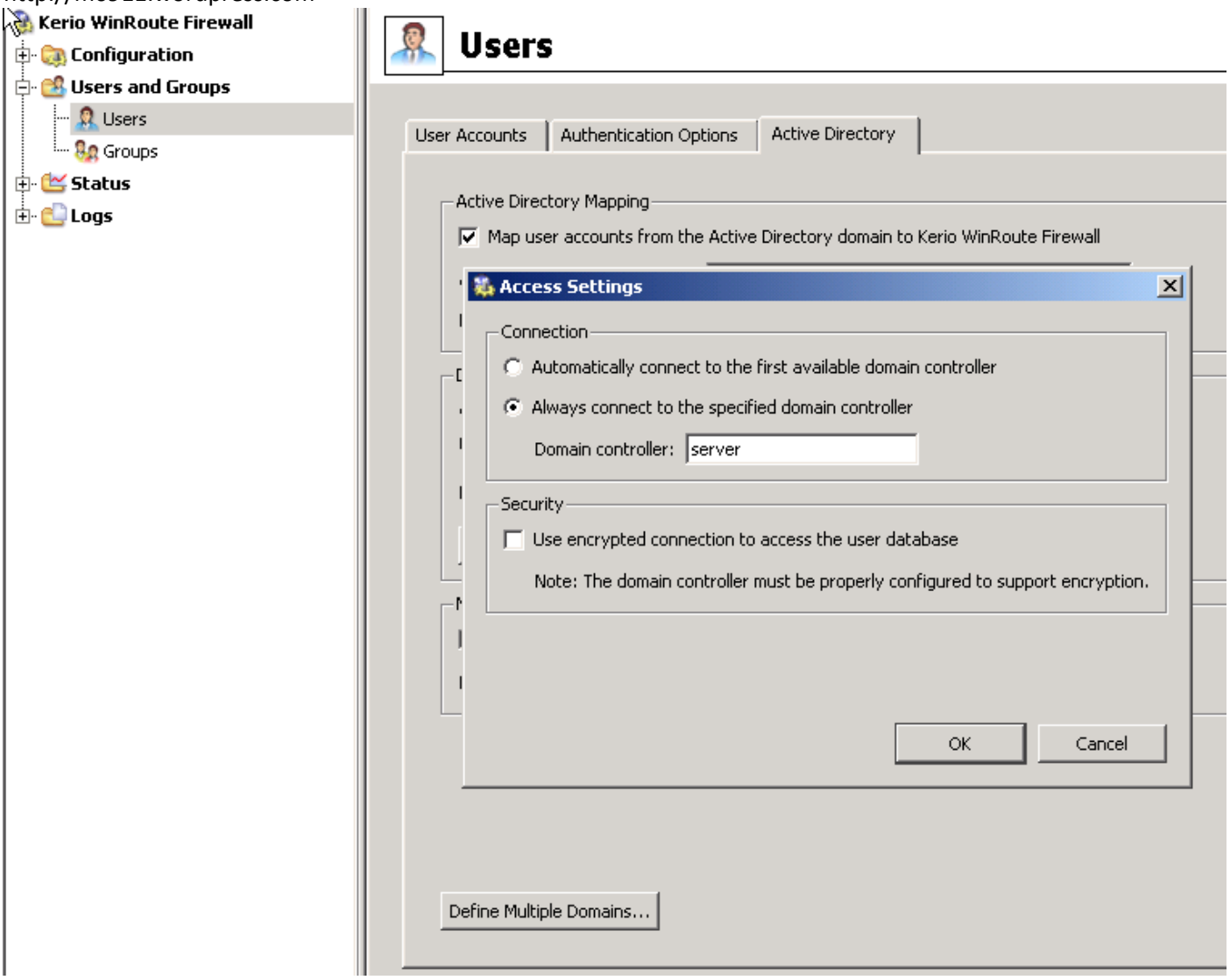


در صفحه ی مربوط به تنظیمات اکتیو دایرکتوری، گزینه ی Map user accounts... را فعال نمایید و نام دامین مورد نظر را به طور کامل وارد کنید. در این مثال نام دامین worknet.local است. بخش Description اختیاری است.
برای دسترسی به اطلاعات کاربران لازم است که نام و گذرواژه ی یک کاربر با اختیار دسترسی به اکتیو دایرکتوری را در بخش Domain Access وارد نمایید. به طور معمول ممکن است بخواهید همان کاربر پیش فرض Administrator را استفاده نمایید.
من ترجیح می دهم کاربری را استفاده کنم که ویژه ی همین برنامه باشد و جای دیگر به کار نرود. در نظر داشته باشید مثلا اگر کاربر Administrator یا هر کاربر مدیر شبکه را که در جای دیگر هم استفاده می کنید ممکن است مجبور شوید گذرواژه ی آن را هر چند وقت یک بار تغییر دهید. به محض تغییر گذرواژه، دسترسی به اکتیو دایرکتوری توسط فایروال کریو از بین می رود و هیچ کاربری شناسایی نخواهد شد و در نهایت تمام کاربران به هنگام ورود به صفحه ی وب با درخواست نام کاربر و گذرواژه رو در رو می شوند.
همان طور که در تصویر بعدی می بینید کاربری به نام KWAdmin را در این بخش به کار برده ام. در واقع این کاربر را در بخش Active Directory Users and Computers ایجاد می نماییم. البته این کاربر باید عضو گروه Domain Admins باشد یا ممکن است از روی همان کاربر Administrator اصلی کپی کرده باشیم.

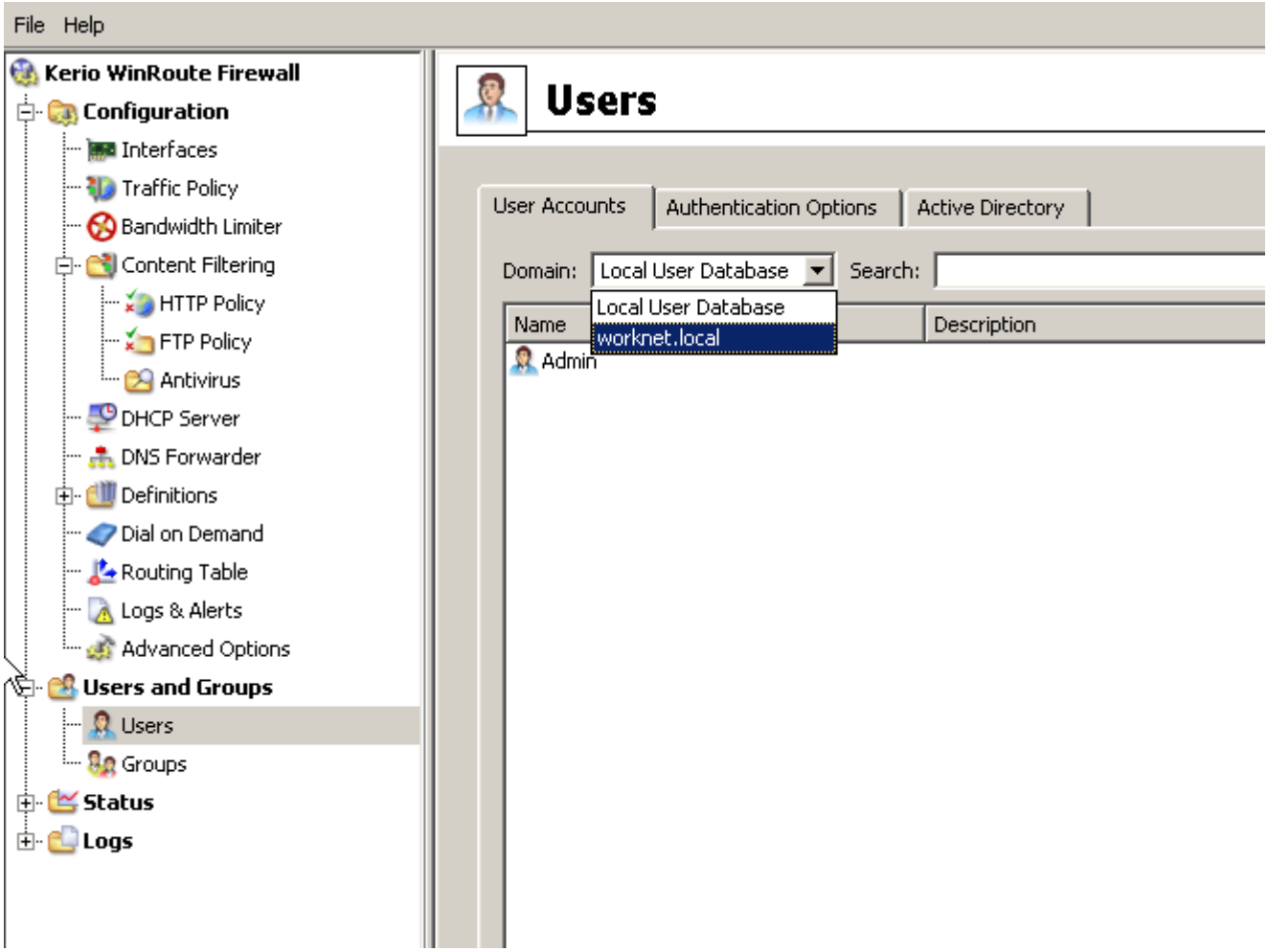
برای ایمنی بیشتر می توانید در بخش Logon to مشخصات کاربر در اکتیو دایرکتوری، ورود آن را فقط روی کامپیوتر سرور فایروال مجاز اعلام کنید. چرا که این کاربر ویژه ی دسترسی به اطلاعات کاربران در اکتیو دایرکتوری توسط فایروال کریو است و جای دیگر کاربرد ندارد. بدین ترتیب امکان سؤ استفاده ی احتمالی از این کاربر را از میان می برید.
به علاوه لازم است بخش NT Authentication را نیز فعال نمایید. در بخش NT domain name همان طور که می بینید نام دامین اکتیو دایرکتوری **بدون پسوند و با حروف بزرگ** نوشته شده است.



به طور پیش فرض برنامه ی کریو به نخستین سرور دامین کنترلر برای دریافت اطلاعات کاربران مراجعه می نماید. اگر بیش از یک سرور دامین کنترلر در شبکه تان دارید یعنی علاوه بر سرور اصلی (Primary Domain Controller) سرور (های) پشتیبان (Backup Domain Controller) دارید می توانید نام آن ها را وارد نمایید. بدین منظور در بخش Domain Access دکمه ی Advanced را بزنید تا صفحه مربوط به تنظیمات پیشرفته ی سرور باز شود. در بخش Connection گزینه ی Automatically connect... به طور پیش فرض انتخاب شده است که باعث می شود نرم افزار کریو به نخستین سرور در دسترس برای دریافت اطلاعات کاربران اکتیو دایرکتوری متصل شود. اگر گزینه ی بعدی Always connect to ... را انتخاب نمایید می توانید نام سرور را خود تان تعیین کنید.
همچنین در بخش Security می توانید تعیین نمایید که از اتصال امن رمز گذاری شده برای دسترسی به بانک اطلاعاتی کاربران استفاده نمایید، به شرطی که سرور شما برای این نوع اتصال از پیش تنظیم شده باشد.


Kerio WinRoute Firewall
Configuration
Users and Groups
Users
Groups
Status
Logs
Users
User Accounts
Authentication Options
Active Directory
Active Directory Mapping
Map user accounts from the Active Directory domain to Kerio WinRoute Firewall
Access Settings
Connection
Automatically connect to the first available domain controller
Always connect to the specified domain controller
Domain controller:
server
Security
Use encrypted connection to access the user database
Note: The domain controller must be properly configured to support encryption.
OK
Cancel
Define Multiple Domains...

برای اعمال تنظیم های گفته شده، دکمه ی Apply در پایین پنجره را بزنید. حال در برگه ی User Accounts فهرست Domain را باز کنید.

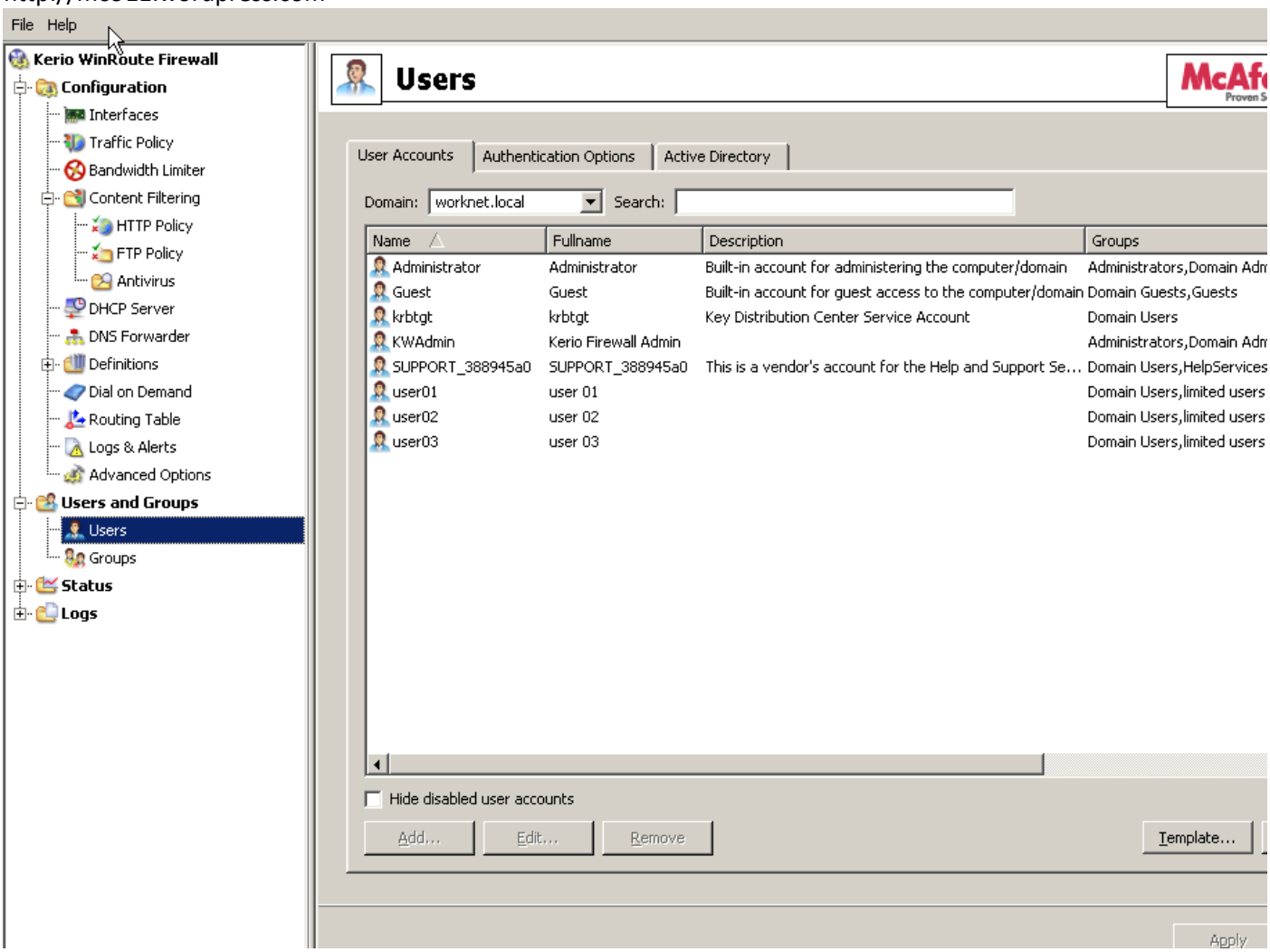


پس از انتخاب دامین، فهرست کاربران ظاهر می شود. اگر اطلاعات را درست وارد نموده باشید باید پس از انتخاب نام دامین (در این جا worknet.local) بتوانید نام کاربران را ببینید.

در این پنجره با استفاده از بخش Search می توانید نام کاربران را جستجو نمایید.

در عین حال گزینه ی hide disabled user accounts در پایین همین پنجره به شما امکان می دهد که فهرست را خلوت تر کنید و فقط کاربران فعال را در این فهرست ببینید.

توجه داشته باشید که فعال یا غیر فعال بودن در نرم افزار فایروال کریو مطرح است نه در اکتیو دایرکتوری. یعنی اگر یک کاربر را در اکتیو دایرکتوری غیر فعال (disabled) کنید در کریو همچنان در دسترس خواهد بود.



تعیین الگوی کلی برای کاربران (Domain template)

دکمه ی Template را در بخش سمت راست پایین پنجره ی User Accounts می بینید. تنظیمات این بخش به صورت الگو برای تمامی کاربران اینترنت به صورت پیش فرض اعمال می گردد مگر این که برای کاربر (های) دلخواهی تنظیمات اختصاصی (individual) به کار ببریم.

پنجره ی Template سه برگه برای تنظیمات عمومی کاربران دارد.

Rights: برای تنظیم مجوز ها که از دو بخش مجوز های مدیریتی (Administrative rights) و مجوز های اضافی (Additional rights) تشکیل شده است.

مجوز های مدیریتی به صورت دکمه ی رادیویی سه گزینه ای است که فقط یکی از آن ها را می توانید انتخاب نمایید:

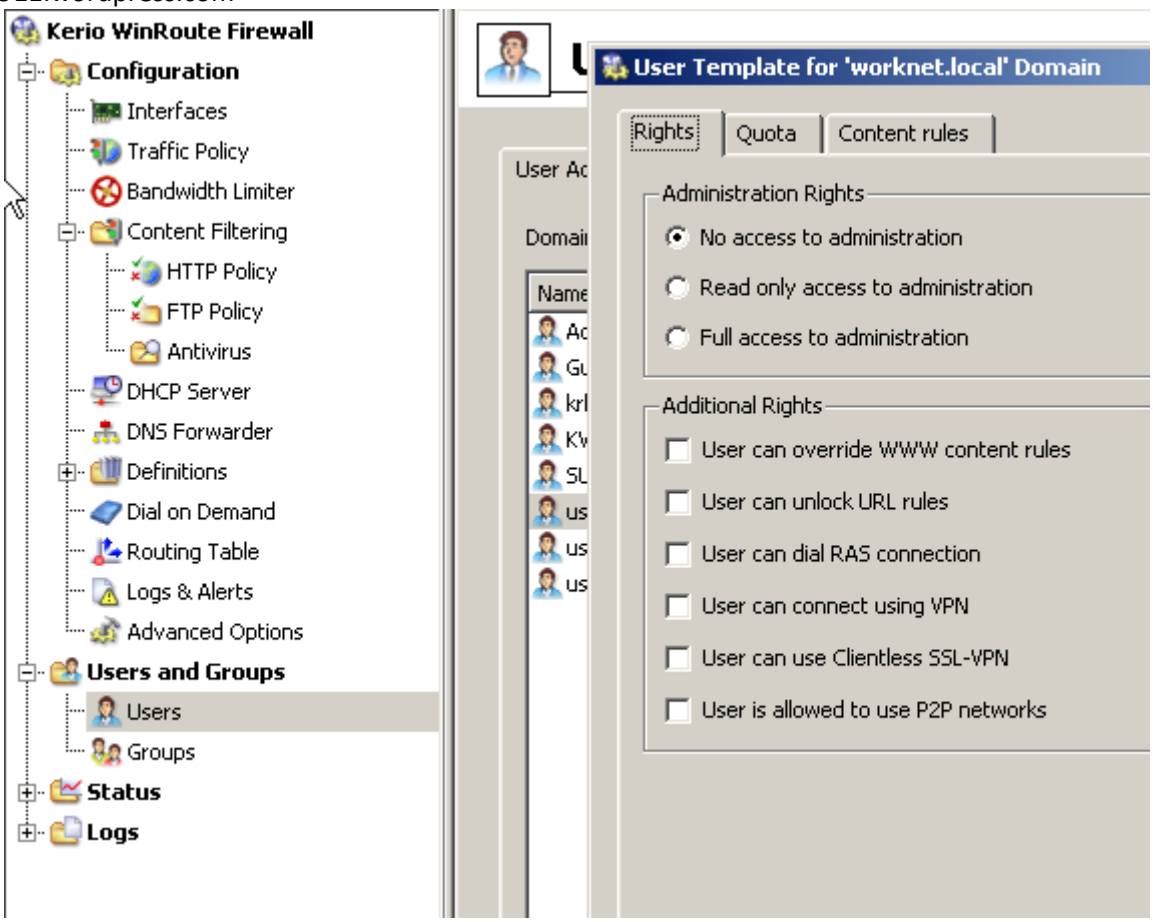
No access to administration: به طور پیش فرض این گزینه فعال است و باعث می شود که هیچ کدام از کابران به جز کاربر Admin داخلی فایروال به گزینه های مدیریتی تنظیمات دسترسی نداشته باشند.

Read only access to administration: دسترسی فقط خواندنی بخش های مدیریتی که در این حالت می توانند تنظیمات بخش مدیریتی را فقط ببینند.

Full access to administration: دسترسی کامل به مدیریت. در حالت عادی فقط کاربر Admin داخلی کریو این اختیار را دارد.

توجه داشته باشید در یک شبکه به صورت پیش فرض باید تمامی کاربران بدون اختیار مدیریت باشند و هر گونه سطح دسترسی دیگری باید به صورت اختصاصی به آن ها داده شود.

بخش مجوز های اضافی نیز شامل گزینه های دیگری از جمله مجوز اتصال به طریق وی پی ان، امکان استفاده از شبکه های نقطه به نقطه و ... است که به طور پیش فرض برای تمام کاربران شبکه غیر فعال هستند.



بخش Quota شاید مهم تر از بقیه باشد. در این برگه بخش محدودیت انتقال داده (Transfer quota) وجود دارد که ترافیک روزانه و ماهیانه را می توانید محدود نمایید.

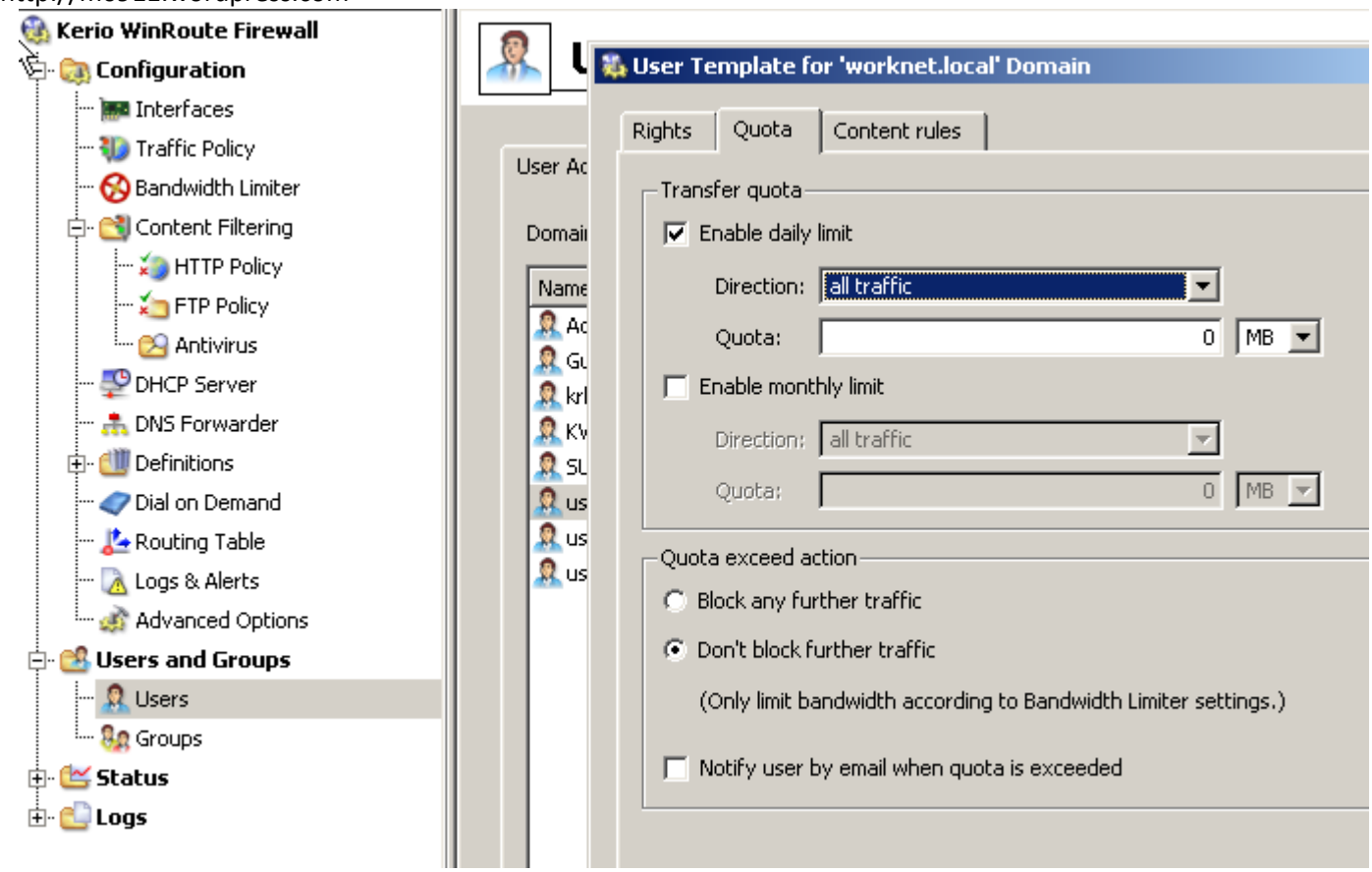
گزینه ی Enable daily limit برای محدویت روزانه است. هنگامی که آن را فعال می نمایید در بخش Direction می توانید جهت ترافیک را مشخص کنید. Download برای دریافتی ها، Upload برای ارسالی ها و All traffic برای مجموع هر دو. در جعبه متن Quota هم می توانید مقدار را بر حسب مگابایت (MB) و گیگابایت (GB) تعیین نمایید.

گزینه ی Enable monthly limit نیز به روشی مشابه محدودیت ماهیانه را تعیین می نماید.

توجه داشته باشید که اگر میزان ترافیک روزانه و ماهیانه را هم زمان محدود می کنید، مقدار های آن ها باید با هم متناسب باشند. مثلا اگر مجموع ترافیک ارسال و دریافت روزانه را ۵۰ مگابایت تعیین کنید، میزان ماهیانه باید کمتر از ۱۵۰۰ مگابایت (هر ماه ۳۰ روز کاری در نظر می گیریم) باشد تا محدودیت ماهیانه معنا دار باشد. اگر تقویم کاری عادی یعنی همراه با تعطیلی باشد مثلا ۲۵ روز، در این صورت مقدار ترافیک ماهیانه باید کمتر از ۱۲۵۰ مگابایت باشد. یا اگر مجموع ترافیک ارسال و دریافت روزانه را ۵۰ مگابایت محدود می کنید و مثلا در ترافیک ماهیانه فقط دانلود یا فقط آپلود را محاسبه کنید باید میزان ترافیک را (با فرض ۳۰ روز کاری) کمتر از حالت پیشین در نظر بگیرید.

نکته ی بعدی این که برای این تعیین حدود بهتر است ابتدا به مدت چند روز شبکه اینترنت را بدون محدودیت انتقال داده استفاده نمایید تا آمار کاربران و نوع پروتوکل ها و میزان ارسال و دریافت آنان را بتوانید برآورد کنید.

و همان طور که در شکل نیز می بینید می توان فقط ترافیک روزانه یا فقط ترافیک ماهیانه را محدود کرد و الزامی به استفاده از هر دو محدودیت نیست.



بخش Quota exceed action مربوط به حالتی است که میزان مصرف یک کاربر از مقدار تعیین شده اش (روزانه یا ماهیانه) بیشتر شود. در این حالت دو گزینه در دسترس است:

Block any further traffic: مسدود کردن کاربر تا آغاز دور بعدی. مثلا اگر سهمیه ی روزانه به پایان رسیده باشد تا آغاز روز بعدی کاربر را مسدود می کند. همچنین اگر جمع سهمیه های روزانه ی استفاده شده از سهمیه ی ماهیانه بیشتر شود تا آغاز ماه بعدی (تقویم میلادی) کاربر مسدود خواهد بود.

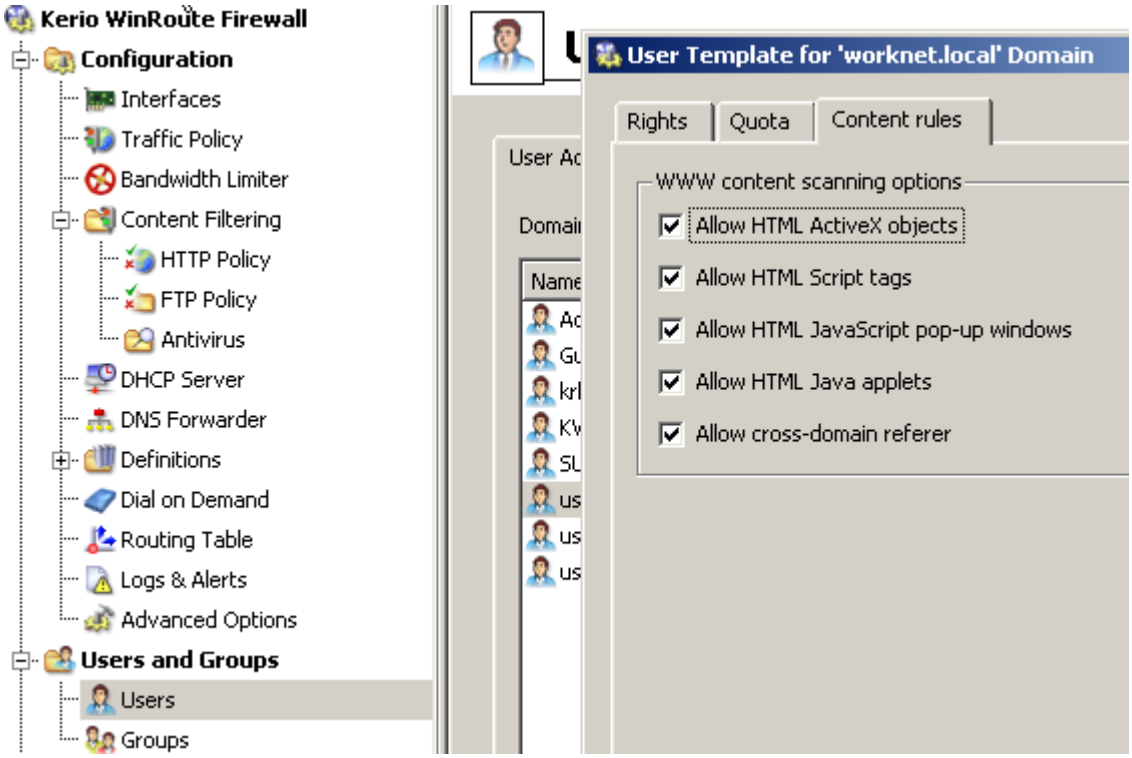
Don't block further traffic: در این حالت کاربر مسدود نمی شود و از پهنای باندی که به این منظور در بخش bandwidth limiter تعیین شده به صورت اشتراکی با سایر کاربرانی که آن ها هم سهمیه شان را تمام کرده اند استفاده می کند.

گزینه ی آخر Notify user... در صورتی که سهمیه ی کاربر تمام شود از طریق ایمیل به او خبر می دهد. البته برای استفاده از این امکان باید آدرس ایمیل سرور و ... در بخش مربوط به آن فعال شده باشد که در این مبحث به آن نپرداخته ایم.

برگه ی آخر content rules است که مربوط به بخش اسکن و فیلتر محتوایی صفحات وب می باشد و محتوا های خاصی را به کاربر اجازه می دهد که استفاده نمایند.

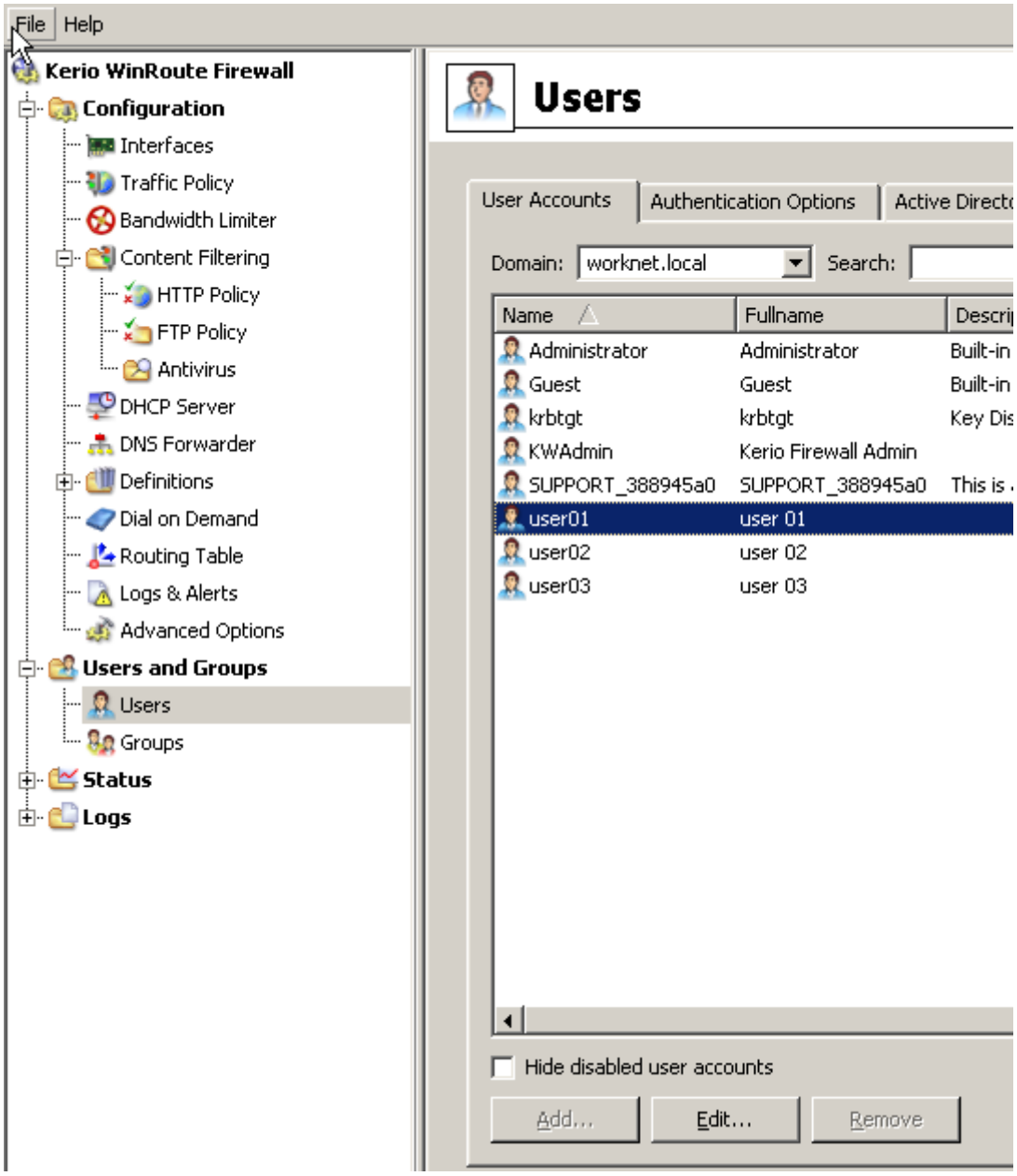
تمامی این تنظیمات که گفتیم برای همه ی کاربر ها از طریق الگوی کلی (Domain template) اعمال می شوند.

برای دیدن ویدئوی کوتاه مربوط به این بخش اینجا را کلیک کنید.


Kerio WinRoute Firewall
Configuration
Interfaces
Traffic Policy
Bandwidth Limiter
Content Filtering
HTTP Policy
FTP Policy
Antivirus
DHCP Server
DNS Forwarder
Definitions
Dial on Demand
Routing Table
Logs & Alerts
Advanced Options
Users and Groups
Users
Groups
User Template for 'worknet.local' Domain
Rights
Quota
Content rules
WWW content scanning options
Allow HTML ActiveX objects
Allow HTML Script tags
Allow HTML JavaScript pop-up windows
Allow HTML Java applets
Allow cross-domain referer

ویرایش کاربر

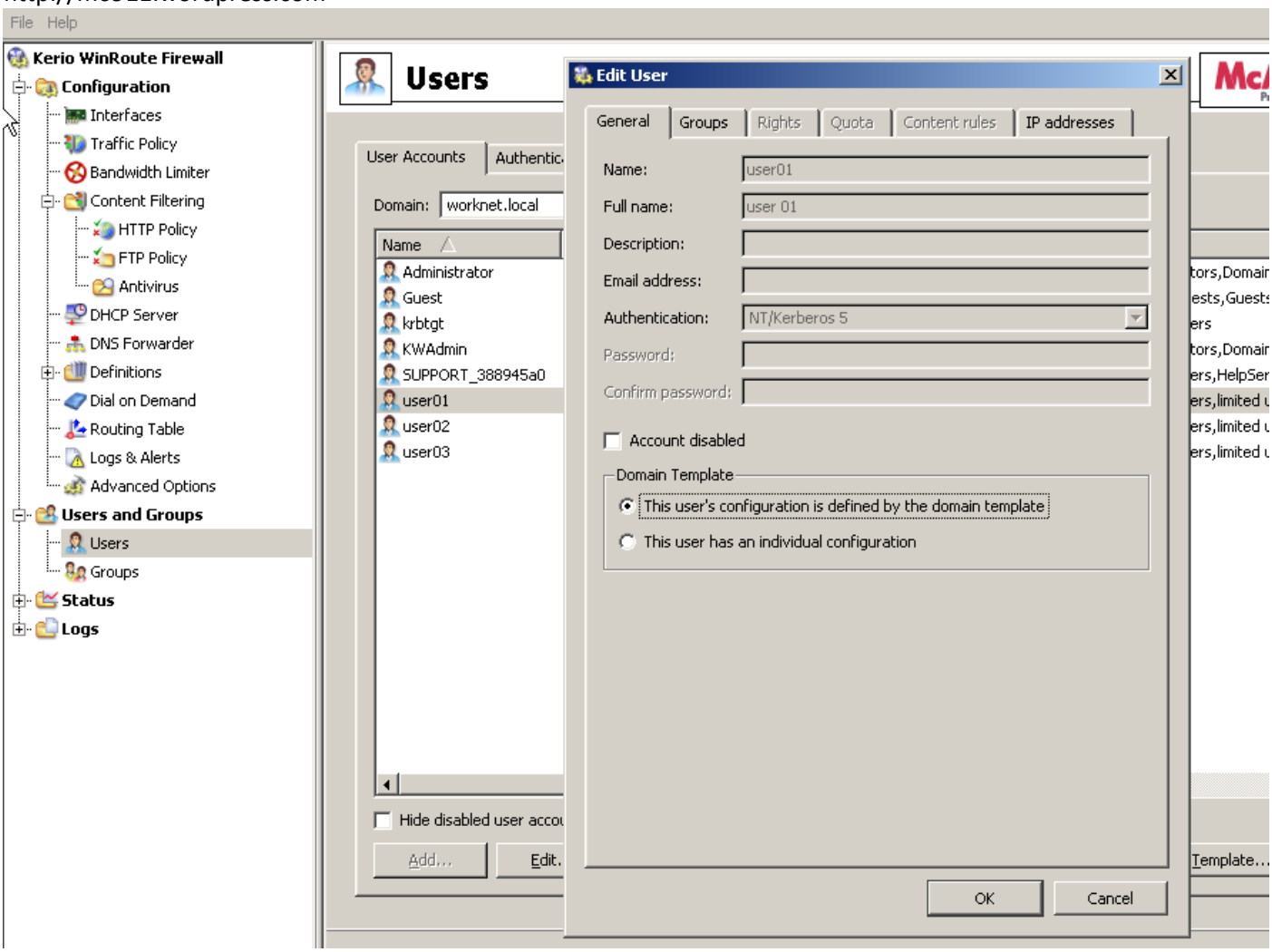
برای تغییر یک کاربر نخست آن را انتخاب نمایید. همان طور که در تصویر بعدی می بینید گزینه های Add و Remove در این حالت که کاربران مستقیما در اکتیو دایرکتوری تعریف می شوند، غیر فعال است. این دکمه ها فقط برای زمانی فعال می شوند که اطلاعات کاربران در داخل نرم افزار کریو (به ترتیبی که پیش از این اشاره کردیم) ذخیره شوند.



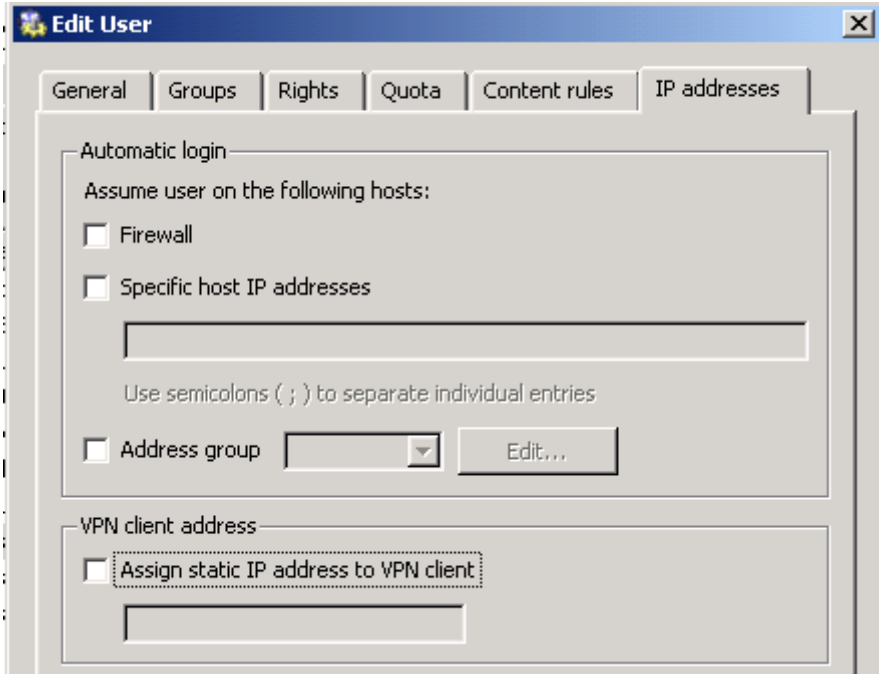
با زدن دکمه ی Edit پنجره ی ویرایش مشخصات کاربر در کریو باز می شود.

برای قطع دسترسی یک کاربر اکتیو دایرکتوری به اینترنت کافی است در این جا گزینه ی Account disabled را انتخاب و تنظیمات را ذخیره نماییم.

برگه ی Groups گروه کاربری مربوط به اکتیو دایرکتوری را نشان می دهد و در این حالت که ما تنظیم کرده ایم (یعنی Active Directory mapping) قابل تغییر نیست.



برگه ی IP addresses مربوط به شناسایی خودکار کاربر است. یعنی آدرس آی پی یا گروه آدرس خاصی را به یک کاربر اختصاص می دهد و اگر درخواست از روی کامپیوتر با آدرس آی پی مزبور باشد برای این کاربر خاص در نظر می گیرد. در حالتی که آی پی کلاینت ها ثابت باشد و هر کامپیوتر کاربر مشخص داشته باشد می توانید از این روش برای تسریع شناسایی کاربر استفاده نمایید.



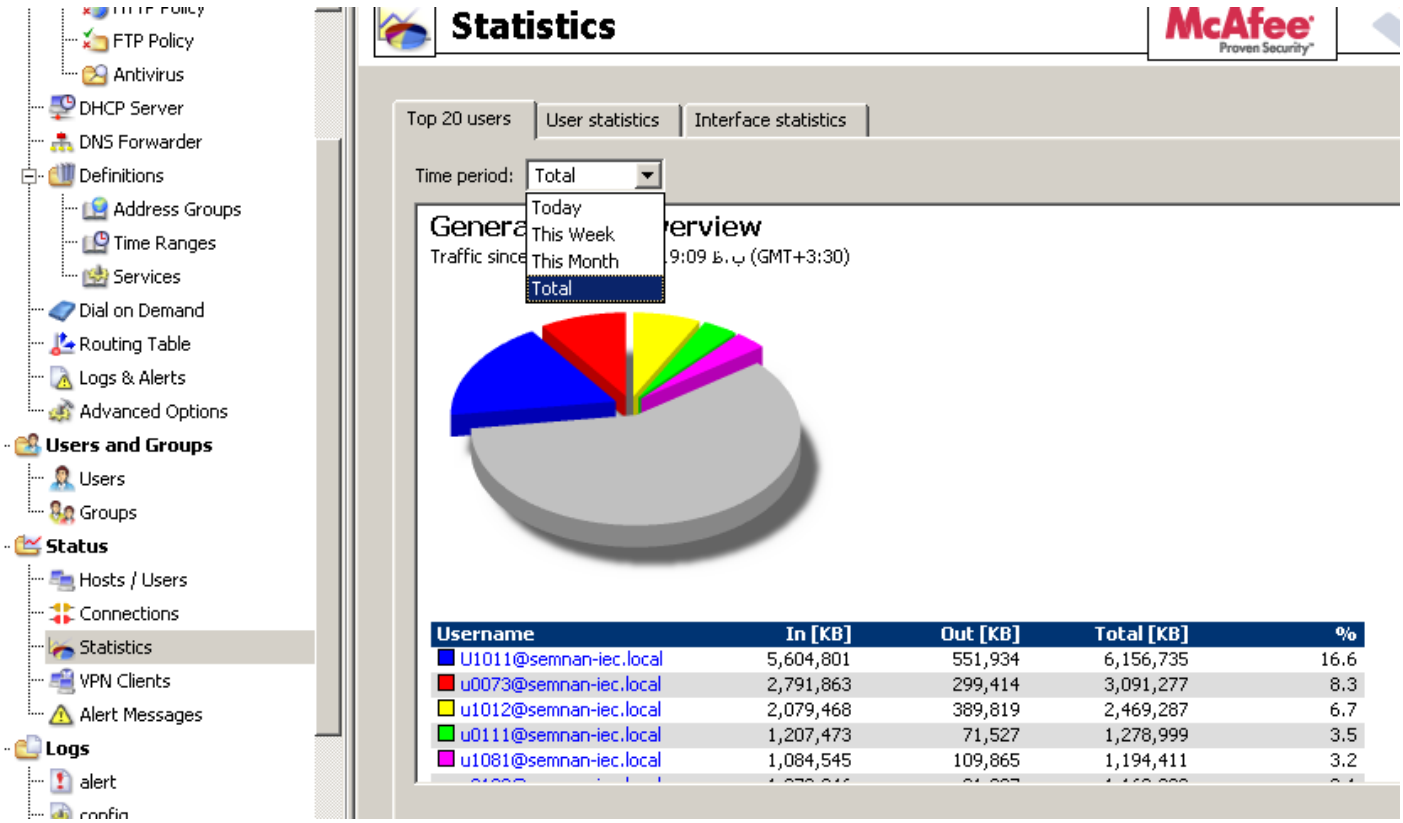
در بخش VPN client address در صورتی که کاربر برای اتصال به فایروال از وی پی ان استفاده می کند می توانید آدرس خاصی را به طور ثابت به او نسبت دهید.

ابتدای کار که پنجره ی ویرایش کاربر را باز می کنید به طور پیش فرض گزینه ی This user's configuration is defined by domain template فعال است و برگه های Rights، Quota و Content rules غیر فعال هستند. چون این تنظیمات را از الگوی کلی کاربران استفاده می کند. اگر بخواهیم تمامی شرایط یک کاربر، جداگانه تنظیم شوند باید گزینه ی تنظیم اختصاصی یا همان this user has an individual configuration را فعال نمایید. در این حالت سه برگه ی مذکور نیز فعال می شوند.
مثلا ممکن است بخواهید یک یا چند کاربر محدودیت ترافیک نداشته باشند در حالی که الگوی کلی برای همه شان محدودیت ترافیک قرار داده است. در این حالت می توانید کاربران را به صورت اختصاصی تنظیم کنید و محدودیت ترافیک آن ها را تغییر داده یا غیر فعال نمایید.
یا مثلا می خواهید یکی از کاربران (مثلا مدیر سازمان که مهارت فنی در زمینه ی فایروال ندارد) بتواند میزان مصرف کاربران را ببیند در این صورت پس از تنظیم اختصاصی در بخش Rights می توانید گزینه ی Read only access to administration را فعال نمایید تا بدون امکان دستکاری در تنظیمات بتواند آمار استفاده ی کاربران را ببیند.
برای دیدن ویدئوی کوتاه مربوط به این بخش اینجا را کلیک کنید.

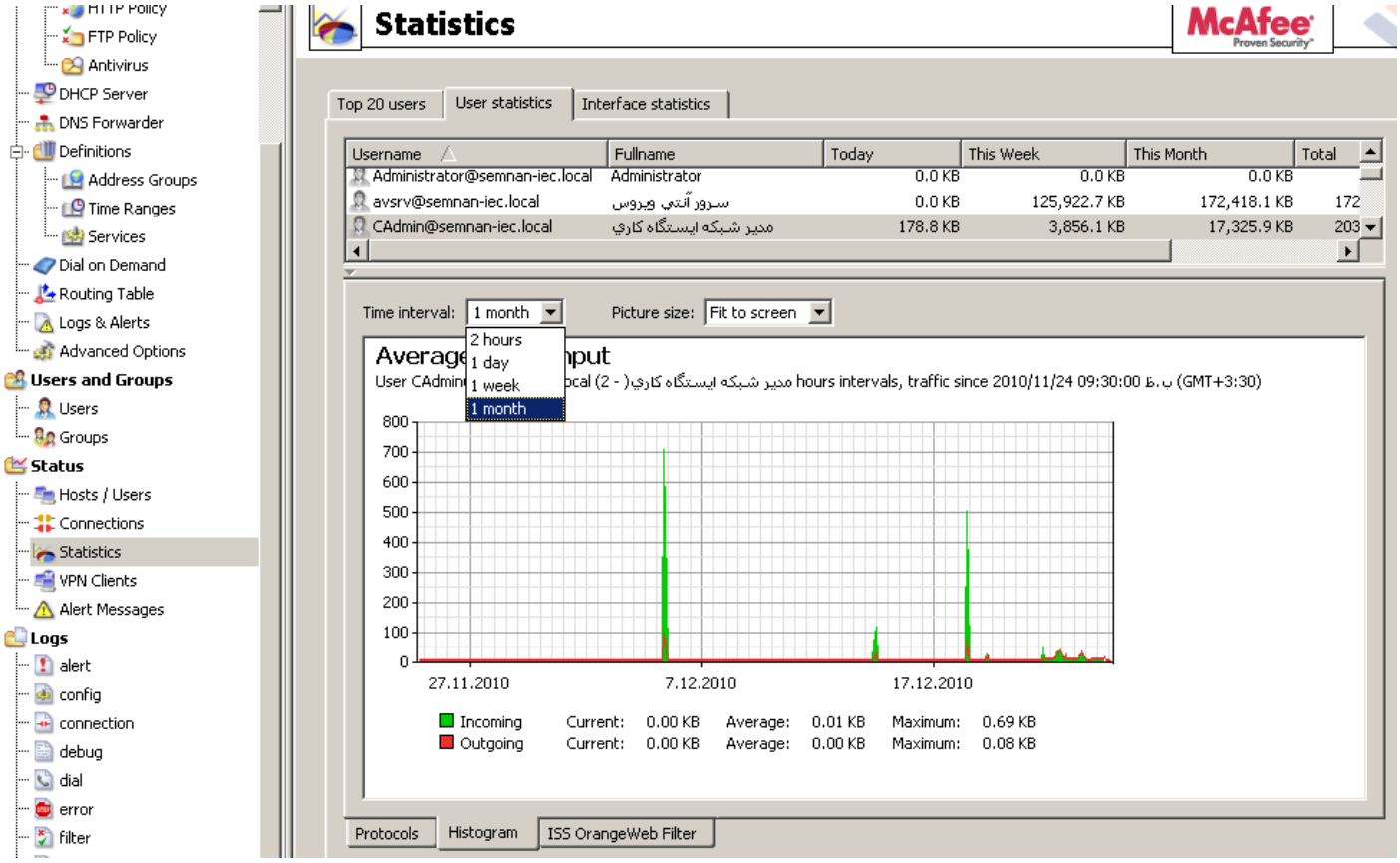
مشاهده ی آمار کاربران

داخل برنامه ی مدیریت فایروال کریو می توانید آمار کاربران را مشاهده نمایید. برای این کار کافی است در پانل سمت چپ روی گزینه ی Statistics در بخش Status کلیک کنید. در بخش آمار سه برگه می بینید.

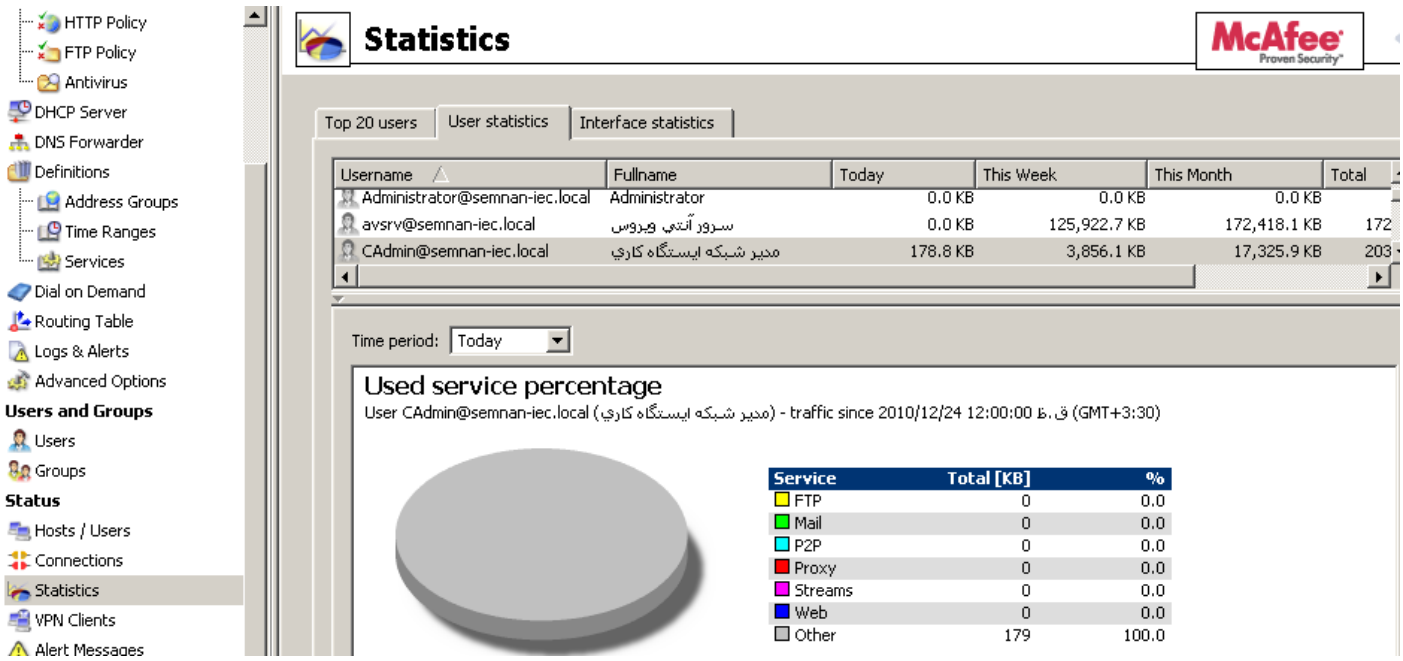
Top 20 users: همان طور که از نامش پیدا است آمار ۲۰ کاربری که بیشتر از بقیه مصرف داشته اند نشان می دهد. با انتخاب دوره ی زمانی می توانید آمار را به صورت روزانه، هفتگی، ماهیانه و کلی ببینید. مثالی که در این عکس می بینید آمار استفاده را به صورت توزیع فراوانی نشان داده است. کاربران هر کدام با یک رنگ مشخص شده اند و رنگ خاکستری مربوط به کاربران شناسایی نشده است. دلیل بودن کاربران شناسایی نشده در آمار این است که در این مورد خاص فایروال به گونه ای تنظیم شده است که شناسایی کاربران الزامی نباشد.



User statistics: آمار کاربران. در این بخش می توانید تک تک کاربران را انتخاب و آمار استفاده ی آن ها را به صورت روزانه، هفتگی، ماهیانه و کلی ببینید. این صفحه از دو بخش تشکیل شده است. بالای صفحه که فهرست کاربران و میزان استفاده ی آن ها به تفکیک بازه ی زمانی در ستون های کنار هم نشان داده می شود و پایین صفحه که در آن نمودار با جزئیات بیشتر بر حسب ترافیک (محور عمودی) و زمان (محور افقی) نمایش داده می شود. رنگ سبز برای دانلود و رنگ قرمز برای آپلود مشخص شده است.



در تصویر زیر ترافیک روزانه ی یک کاربر را به تفکیک نوع سرویس استفاده شده می بینید.



برگه ی آخر Interface statistics است که ترافیک را به تفکیک کارت شبکه نشان می دهد.

در نگارش ۷ فایروال کریو امکانات آماری وسیع تری وجود دارد که مستندات آن را از روی کارهای انجام شده ی واقعی به زودی منتشر خواهم کرد.

آن چه در این سری ۴ بخشی آموزش فایروال کریو منتشر کردم امکانات پر کاربرد این نرم افزار را در بر می گرفت و سعی کردم توضیحات به گونه ای باشد که برای افراد مبتدی نیز قابل فهم گردد. در صورتی که سؤالی در این زمینه دارید می توانید با نشانی ایمیل m0911w@gmail.com که نشانی اختصاصی من برای این وبلاگ است تماس بگیرید تا پاسخ آن را به صورت تکمیلی در بخش های آینده منتشر نمایم.

همکاری و حمایت مالی

برای پیاده سازی های واقعی شبکه (که این فایروال می تواند بخشی از آن باشد در حد امکان می توانم با شما همکاری تجاری داشته باشم.

در ضمن با توجه به این که پیاده سازی LAN Accounting یک کار تجاری است، در صورتی که از محتوای این سری مقاله رضایت دارید و می توانید از این مهارت برای کسب در آمد استفاده نمایید از شما می خواهم که در صورت تمایل تان، من را به عنوان یک همکار و هم صنف حمایت مالی نمایید تا بتوانم با کیفیت و سرعت بهتری مطالب آموزشی را منتشر نمایم.

در صورتی تمایل به حمایت مالی با آدرس ایمیل m0911w@gmail.com تماس بگیرید.