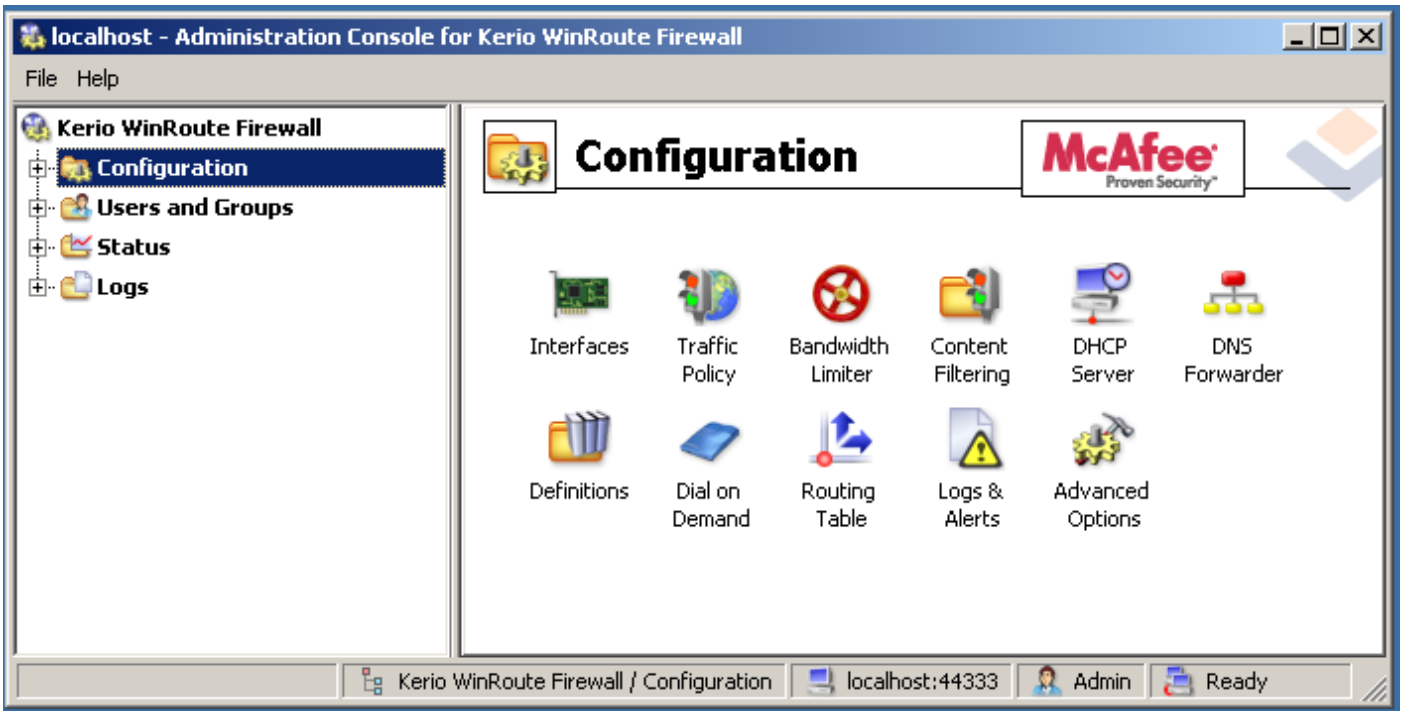
عنوان	برنامه فایروال وینروت کریو – بخش سوم، مروری بر جزئیات نرم افزار
عنوان اصلی	**Kerio WinRoute Firewall 6, Overview of Software Details**
کلمات کلیدی	Network, Firewall, Server, Windows, Proxy, Filter, Cache, Internet, NAT, Port, TCP , UDP, Proxy, DNS Forward, Filter, Bandwidth Limit شبکه، دیوار آتش، فایروال، ویندوز، سرور، اینترنت، کنترل، فیلتر، پروکسی، پورت، محدودیت پهنای باند
مؤلف	مهدی عبداللهی
مرجع	
سطح	متوسط
مترجم	مهدی عبداللهی (http://m0911.wordpress.com)
تاریخ انتشار	۱۰ آذر ماه ۱۳۸۹
تعداد صفحه	۱۳
فایل های ضمیمه	

در این قسمت مروری به امکانات و بخش های مختلف فایروال کریو وبنروت خواهم داشت. تصاویری از محیط نرم افزار می بینید که جزئیات بیشتری را در اختیار شما می گذارند. اتظیمات صورت گرفته به گونه ای است که در برخی بخش ها پیغام خطا یا اخطار فایروال کریو نمایش داده شود. لازم است یادآوری کنم که پرداختن به تمامی امکانات این نرم افزار در حوصله ی این مطلب نمی گنجد. کتاب راهنمای کاربران فایروال کریو وینروت ۴۰۰ صفحه است که فشرده سازی ۴۰۰ صفحه در ۱۰ صفحه نیز امکان ندارد. در این سلسله مطالب، مدیریت شبکه ی کوچک و کنترل پهنای باند و مصرف اینترنت و ... را بحث خواهم کرد.

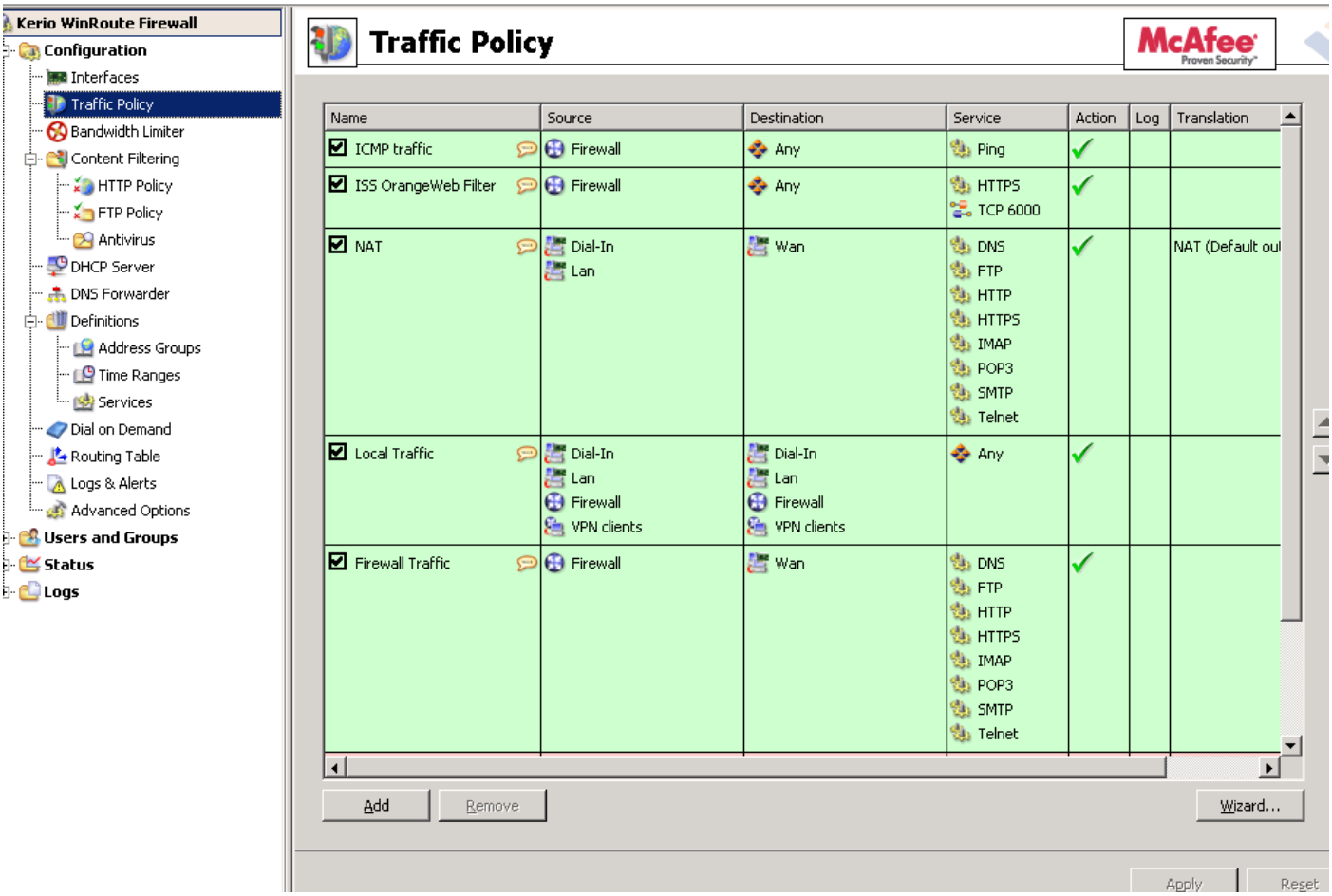
شکل زیر صفحه ی اصلی کنسول مدیریت کریو را نشان می دهد.



Configuration: تنظیمات فایروال کریو که شامل بخش های زیر است:

- Interfaces: فهرست کارت های شبکه و اتصالات اینترنت و وی پی ان در این بخش قرار دارد. برای اتصالات دیال آپ یا دی اس ال تنظیمات خاصی از جمله نحوه ی اتصال و زمان های مجاز برای استفاده از آن ها را می توانید اعمال نمایید. همچنین امکان استفاده از اتصال پشتیبان برای اینترنت وجود دارد؛ روش کار بدین صورت است که دو اتصال (کارت شبکه) مختلف برای اینترنت تعریف و برای بررسی متصل بودن هر کدام شان یک آدرس آی پی را مشخص می نمایید. فایروال کریو از طریق دستور Ping متصل بودن هر کدام از آن ها را لحظه به لحظه بررسی می کند و در صورت قطع اتصال اصلی اینترنت، بلافاصله اتصال پشتیبان را استفاده می نماید. (به جزئیات و تشریفات لازم برای استفاده از این امکان اشاره نکرده ام)

- Traffic Policy: نحوه ی دسترسی از شبکه ی داخلی به شبکه ی بیرون، پورت های مجاز، اشتراک اتصال به اینترنت (NAT) ، یا هدایت درخواست پورت های خاص از بیرون به یک آدرس آی پی داخلی (Port Forwarding) و ... در این بخش تنظیم می شود. در بخش قبلی این مقاله ویزارد مربوط به این بخش را به طور خلاصه مرور کردیم.



تنظیمات ترافیک شبکه -که توسط ویزارد ابتدای نصب اعمال شده است- در این شکل می بینید. هر کدام از قوانین، دارای یک نام دلخواه هستند که این نام ها برای قابل درک بودن آن برای کاربر است.

به عنوان مثال اولین قانونی که می بینید با نام ICMP traffic می باشد.

- پارامتر Source (مبداء) Firewall یا همان سروری است که کریو روی آن نصب می باشد.
- پارامتر Destination (مقصد) برابر با Any (هر مقصدی) تنظیم شده است.
- پارامتر Service برابر با Ping تنظیم شده است و در ستون Action علامت تیک سبز رنگ می بینید که به معنی مجاز بودن این سرویس است.

این قانون بدان مفهوم است که از روی سرور فایروال می توانیم به هر مقصدی دستور Ping را برای بررسی اتصال اجرا نماییم. در این مورد خاص دستور Ping به مقصد فایروال تعریف نشده است و این یعنی به طور پیش فرض از هیچ آدرسی (کامپیوتری) چه در شبکه ی داخلی و چه از شبکه ی بیرون (Wan یا همان اینترنت) امکان اجرای دستور Ping به مقصد فایروال نیست. مثلا اگر آدرس آی پی کارت شبکه ی اینترنت سرور فایروال برابر 78.38.155.3 باشد و از یک کامپیوتر در خارج از شبکه ی محلی دستور ping 78.38.155.3 را اجرا نماییم پیغام خطای تایم اوت را دریافت خواهیم کرد. همچنین اگر آدرس آی پی کارت شبکه ی داخلی سرور فایروال (مثلا) 192.168.0.9 باشد و از کامپیوتر داخل شبکه ی محلی دستور ping 192.168.0.5 را اجرا کنیم باز هم پیغام خطای تایم اوت را دریافت خواهیم کرد. اگر این کار یعنی مسدود کردن

ping به مقصد فایروال را انجام ندهیم در این حال یک یا چند مهاجم می توانند با اجرای دستور های ping متعدد با سایز داده ی بزرگ (large packet size) ترافیک سرور فایروال را به طور نامطلوب بالا ببرند و در نتیجه سرعت واکنش آن و سرعت اینترنت در کل شبکه افت خواهد کرد.

در ردیف سوم قانونی به نام NAT می بینید.

از مبداء شبکه ی محلی (Lan) و همچنین کلاینت هایی که با شماره گیری به سرور فایروال وصل شده اند، می توانند به مقصد اینترنت (Wan) و فقط با سرویس های تعیین شده (ستون Service) دسترسی مجاز (نماد تیک سبز رنگ) داشته باشند. اگر سرویس دیگری مانند کنفرانس اینترنتی تصویری با نرم افزار یاهو مسنجر لازم داشته باشید باید پورت های مربوط به آن را در ستون Service اضافه نمایید.

نکته: برای دسترسی به فهرست پورت های پروتوکل TCP و UDP می توانید به آدرس زیر مراجعه نمایید:

http://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers

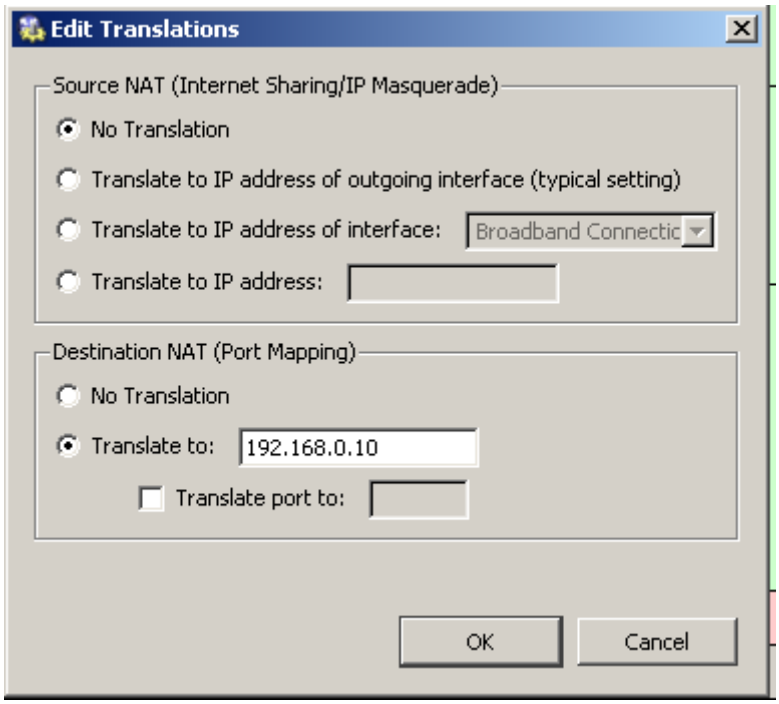
در ستون Translation تنظیمات مربوط به NAT (یا همان Network Address Translation) را انجام می دهید. به طور پیش فرض Source NAT مربوط به اشتراک استفاده از اینترنت در شبکه ی محلی یا همان (Internet Sharing) است.

ردیف چهارم Local Traffic:

همان طور که می بینید ویزارد تنشیمات شبکه به طور پیش فرض تمامی ترافیک های مربوط به شبکه ی محلی (مبداء و مقصد Lan و Firewall و VPN و Dial in) را برای تمامی سرویس ها (Service: Any) مجاز در نظر گرفته است. لیکن شما می توانید ترافیک شبکه ی داخلی را نیز بنا به سیاست هایی که دارید محدود نمایید. مثلا سرور مربوط به بخش حسابداری ممکن است لازم باشد که از دسترس یک سری آدرس خاص دور باشد. در این صورت ترافیک از مبداء (Source) آی پی های مذکور به مقصد (Destination) سرور برنامه ی حسابداری باید ممنوع (Action: Deny) شود.

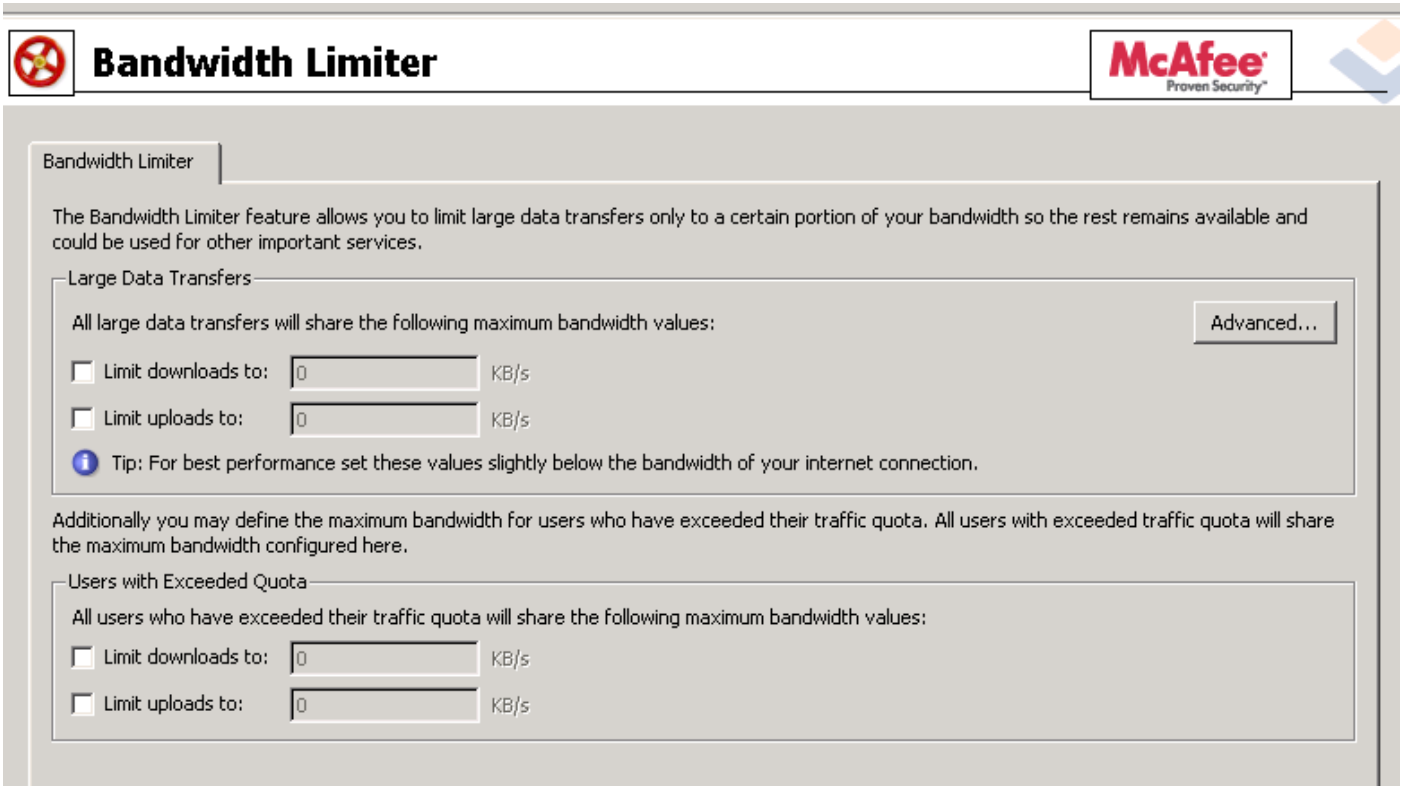
			Telnet			
Local Traffic	Dial-In Lan Firewall VPN clients	Dial-In Lan Firewall VPN clients	Any	✓		
Firewall Traffic	Firewall	Wan	DNS FTP HTTP HTTPS IMAP POP3 SMTP Telnet	✓		
Service MS-SQL	Wan	Firewall	MS-SQL	✓		MAP 192.168.0.
Service HTTP	Wan	Firewall	HTTP	✓		MAP 192.168.0.
Ident	Wan	Firewall	Ident	✗		
Default rule	Any	Any	Any	✗		

در شکل بالا دو قانون دیگر (به رنگ صورتی) می بینید. به خاطر دارید، در ویزارد تنظیمات شبکه، بخش Inbound Policy آدرس آی پی 192.168.0.10 را برای سرور دیتابیس و 192.168.0.3 را برای سرور وب (HTTP) تعیین کردیم. همان طور که می بینید هر گونه درخواست دسترسی به این سرویس ها از بیرون (Source: Wan) به مقصد فایروال به آدرس آی پی داخلی ترجمه خواهد شد.

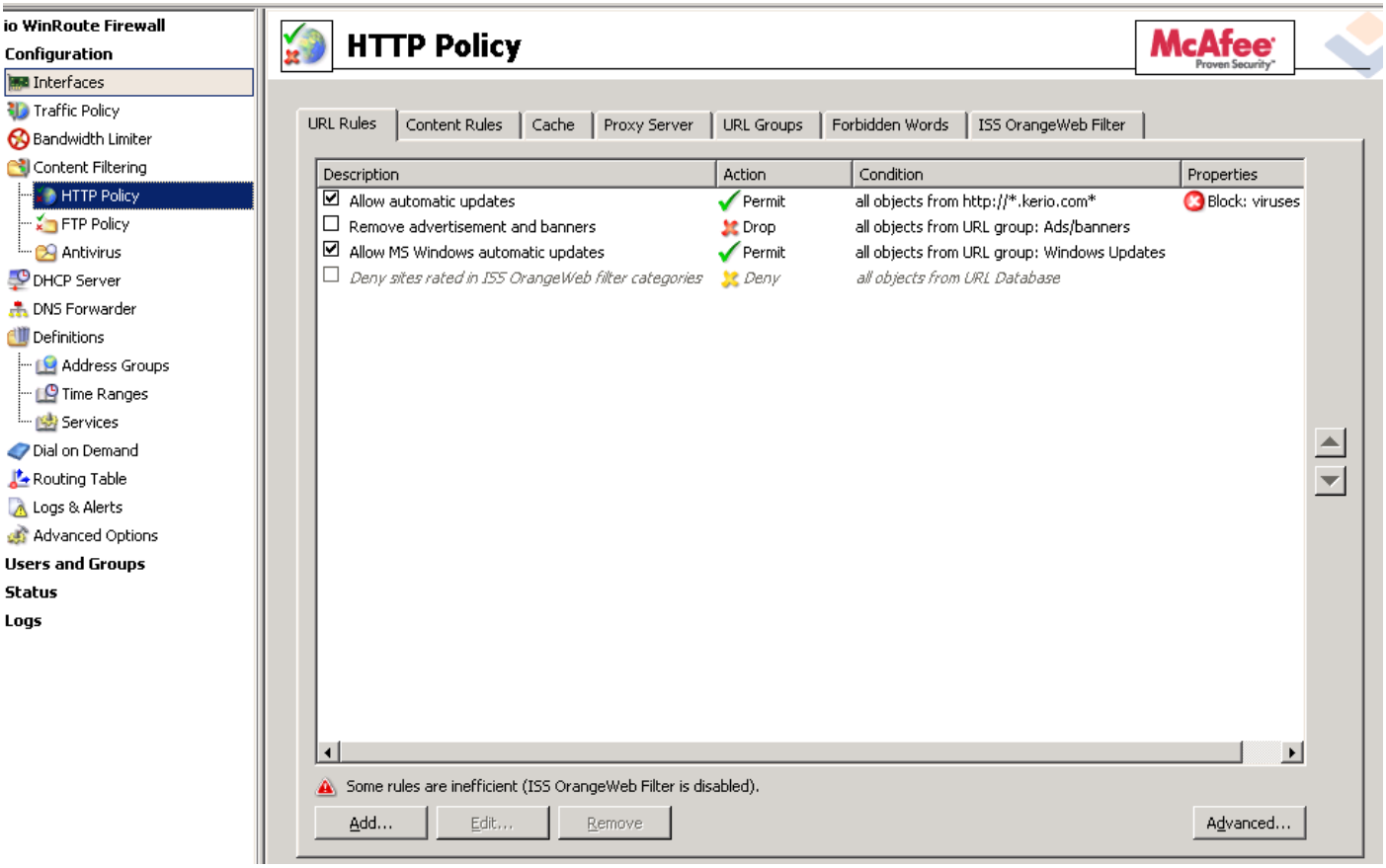


در بخش Translation باید Destination NAT را به مقصد آی پی داخلی مورد نظر تنظیم نماییم.

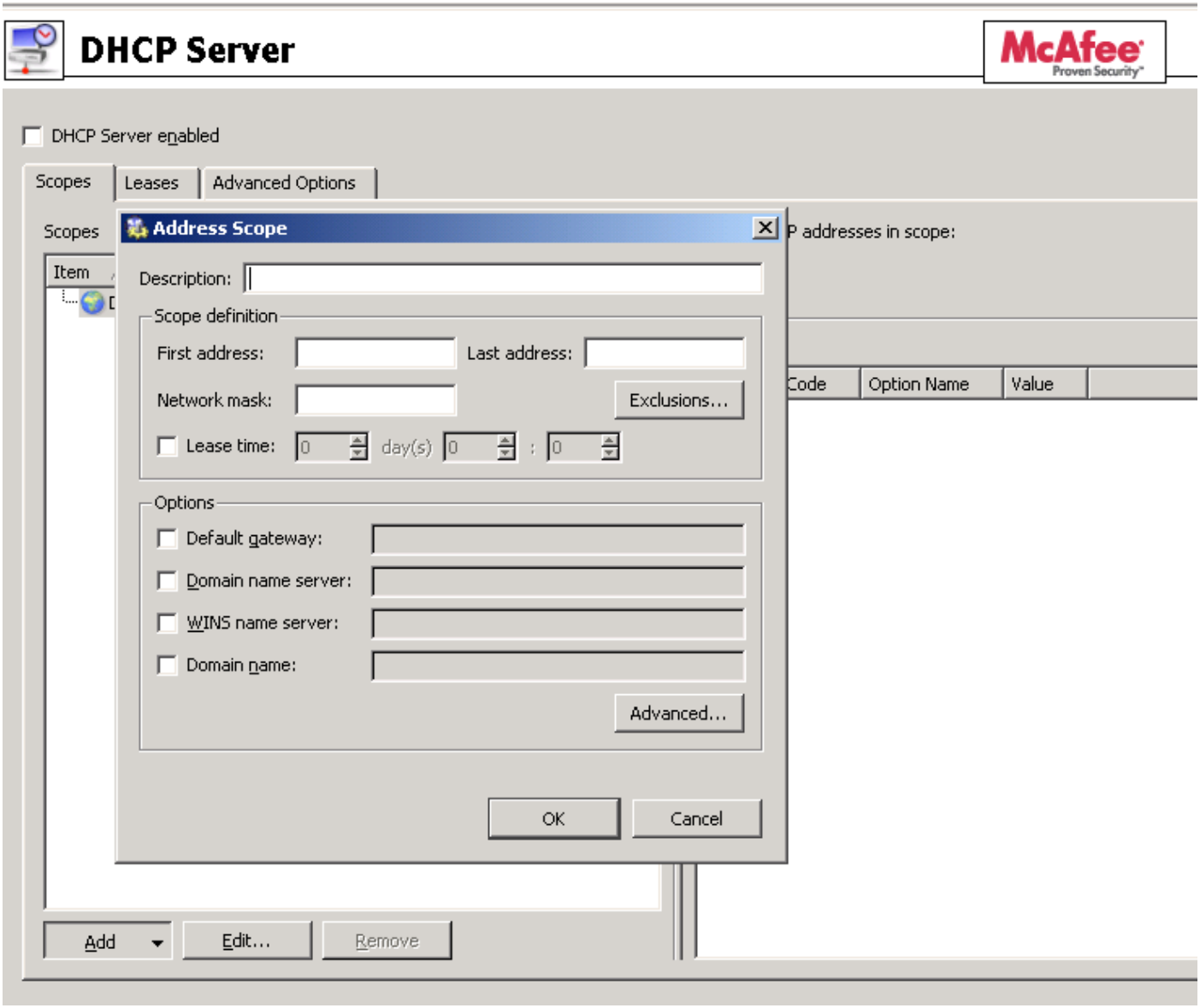
- Bandwidth Limiter: محدود کننده ی پهنای باند. که هم سرعت اینترنت و هم میزان ترافیک را می تواند برای آی پی های خاص یا در محدوده ی زمانی معینی محدود کند. برای بخش Lan Accounting از این بخش استفاده خواهیم کرد.



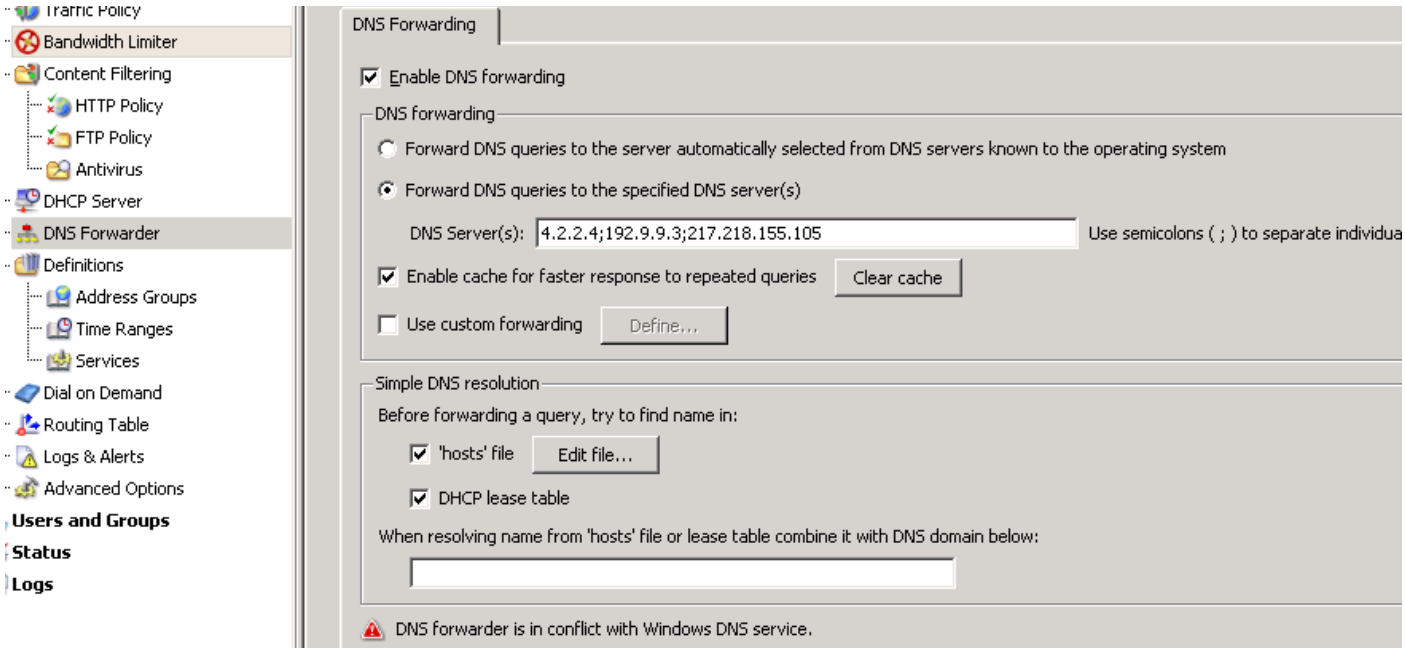
- Content Filtering: فیلتر محتوایی. این بخش دارای سه نوع فیلترینگ می باشد:
  - HTTP: شامل فیلتر آدرس های وب، افزایش سرعت با استفاده از Cache، واژه های ممنوع و ... می باشد. مثلا می توان با گروه بندی آدرس ها، دسترسی به گروهی از آن ها را مسدود نمود. یا استفاده از اکتیو ایکس ها، پنجره های بازشو (Popup) و ... را فعال یا غیر فعال کرد. به دلیل مخالف بودنم با فیلترینگ به این بخش نخواهم پرداخت. نحوه ی کار آن به گونه ای است که بدون نیاز به راهنما می توانید از آن استفاده نمایید.
  - FTP: در این بخش می توانید پروتوکل انتقال فایل را کنترل کنید. از آن جا که این پروتوکل می تواند ترافیک قابل توجهی را به شبکه تحمیل کند می توانید محدودیت های مورد نظر تان را اعمال نمایید. مثلا می توانید دریافت فایل های فیلم و موزیک را از طریق ftp مسدود نمایید. یا برای پیشگیری از خروج اطلاعات سازمان تان فرمان STOR را مسدود کنید.
  - Antivirus: این نگارش از فایروال کریو وینروت به طور پیش فرض از ضد ویروس مک آفی استفاده می نماید. در عین حال می توانید ضد ویروس هایی را که خودتان نصب کرده اید به آن معرفی کنید. این ضد ویروس روی محتوای مربوط به پروتوکل های HTTP و FTP و همچنین ایمیل ها نظارت می نماید و در صورت کشف آلوده گی به ویروس از انتقال محتوای آلوده پیشگیری می نماید.



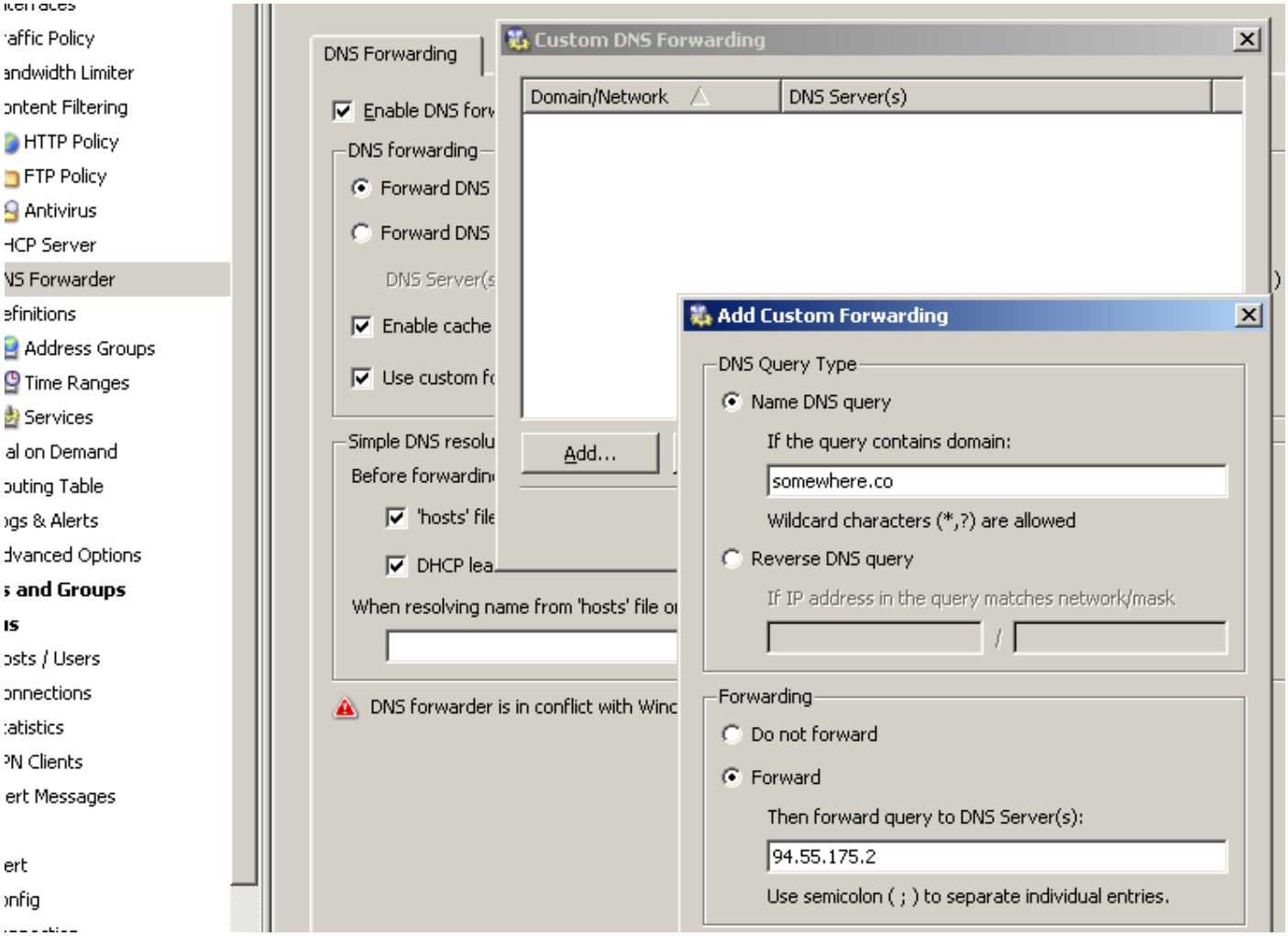
- DHCP Server: یک سرور دی اچ سی پی تمام و عیار برای آدرس دهی کلاینت های شبکه در اختیار شما قرار می دهد. اگر مایل باشید می توانید به عنوان سرور پشتیبان DHCP تنظیم کنید و به صورت غیر فعال نگه دارید و در صورت از کار افتادن سرور اصلی شبکه تان، از سرویس DHCP کریو استفاده نمایید.



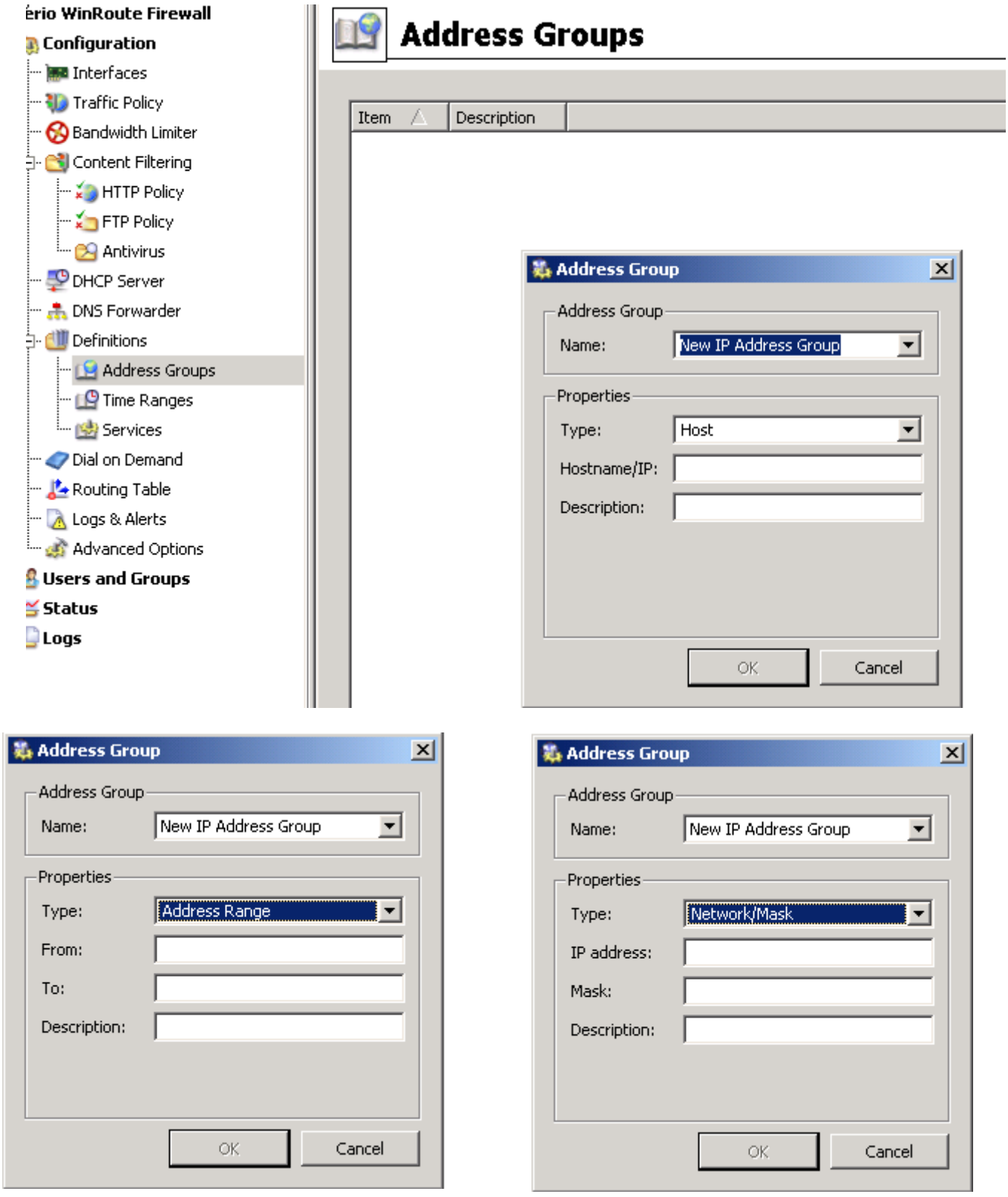
- DNS Forwarder: درخواست نام دامنه را به آدرس سرور DNS ی که شما تعیین می کنید می فرستد. برای کار با این سرویس لازم است که در خصوص DNS اطلاعات کافی داشته باشید. در ضمن می توانید تعیین کنید که تمامی درخواست های نام به آدرس ثابتی ارسال شوند



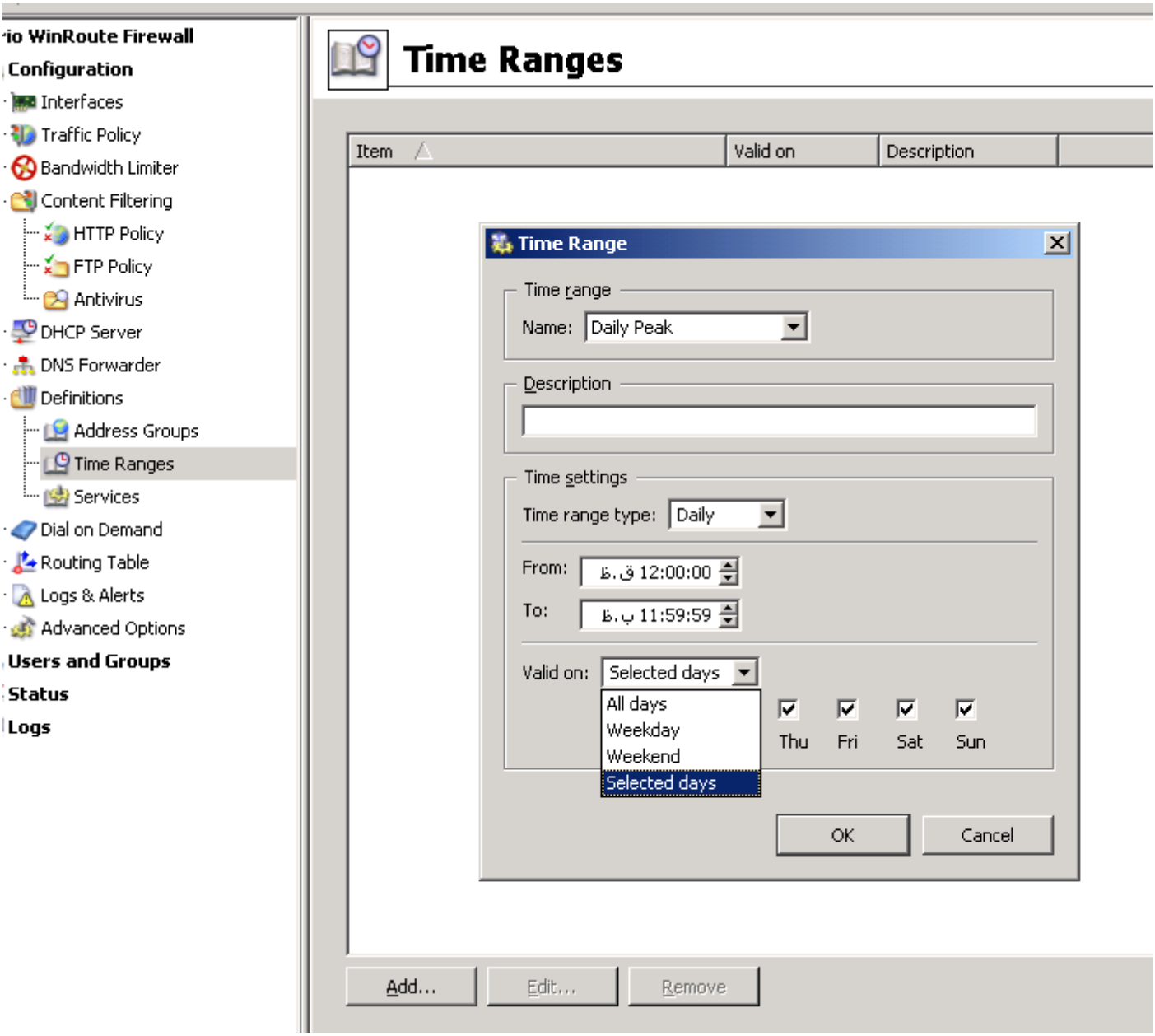
یا این که نام یا آدرس آی پی های خاصی به سرور DNS مجزا فرستاده شوند.

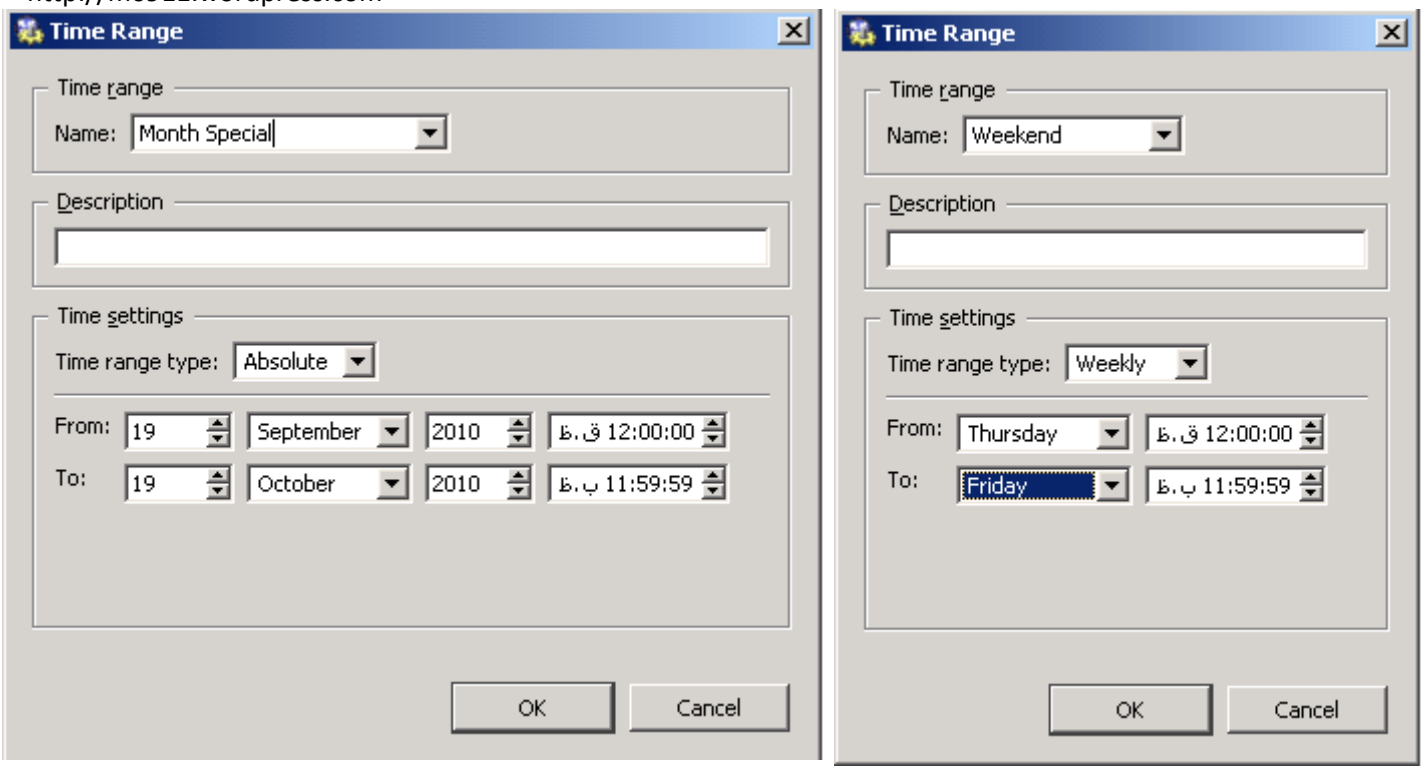


- Definition: تعاریف. در این بخش مقادیر اولیه ای را می توانید تعریف کنید که در بخش های مختلف کریو به عنوان پارامتر استفاده خواهند شد. این مقادیر اولیه شامل گزینه های زیر هستند:
  - Address Group: گروه آدرس ها. می توانید آدرس آی پی خاص یا محدوده ای از آدرس ها را تعریف و نام گذاری نمایید و مثلا محدودیت پهنای باند را فقط برای این گروه از آدرس ها اعمال نمایید.



- Time Range: محدوده ی زمانی. محدوده ی زمانی را به چند روش متنوع می توانید تعریف نمایید و همانند گروه آدرس ها در بخش های مختلف فایروال کریو به عنوان پارامتر استفاده نمایید. مثلا دسترسی به وب سایت هایی را در محدوده ی زمانی خاص ممنوع کنید.



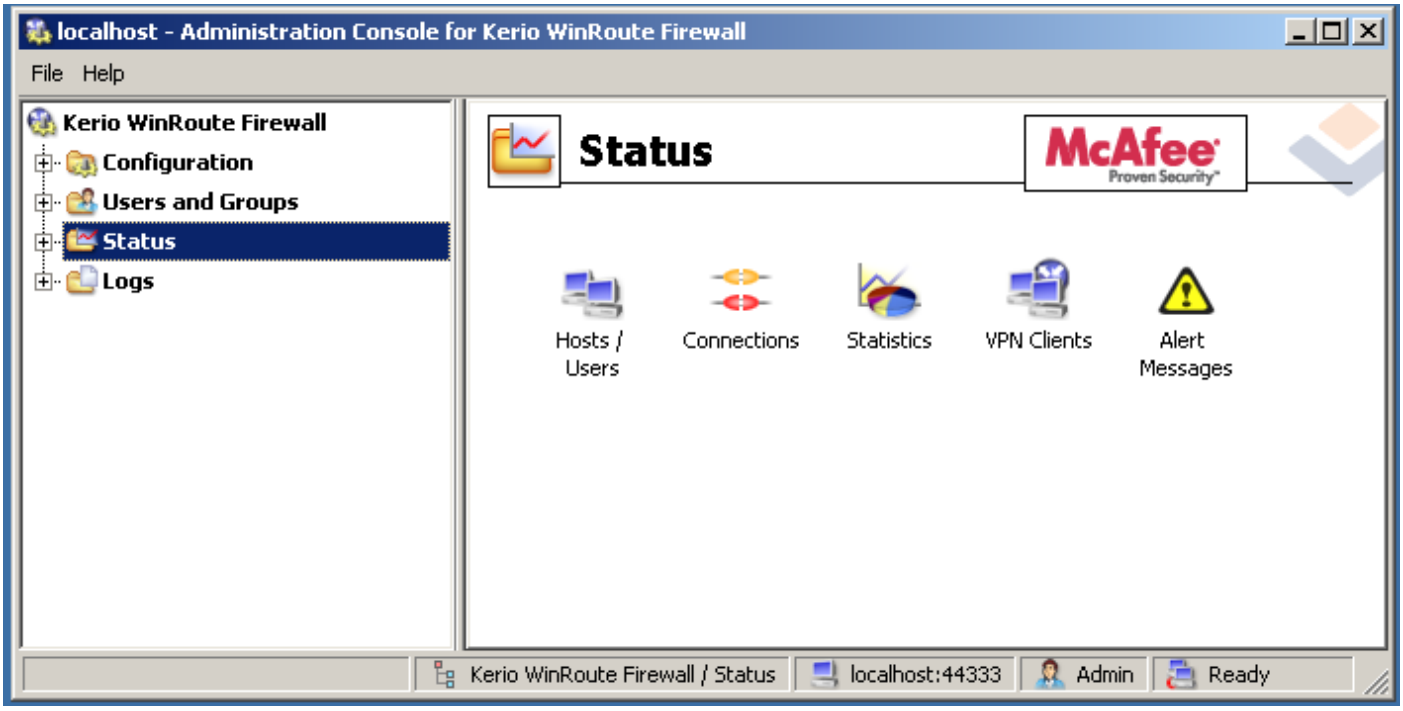


- Services: در این بخش تعدادی از سرویس های مشهور را همراه با پارامترهای تنظیم شده از جمله نوع و شماره ی پورت و ... را می بینید. در عین حال خود تان هم می توانید سرویس هایی را که در این فهرست نیست یا حتی برای عملکرد های خاصی روی پورت های معین، یک نام تعیین کنید و همانند آدرس و محدوده ی زمانی در بخش های مختلف کریو به عنوان پارامتر استفاده نمایید.

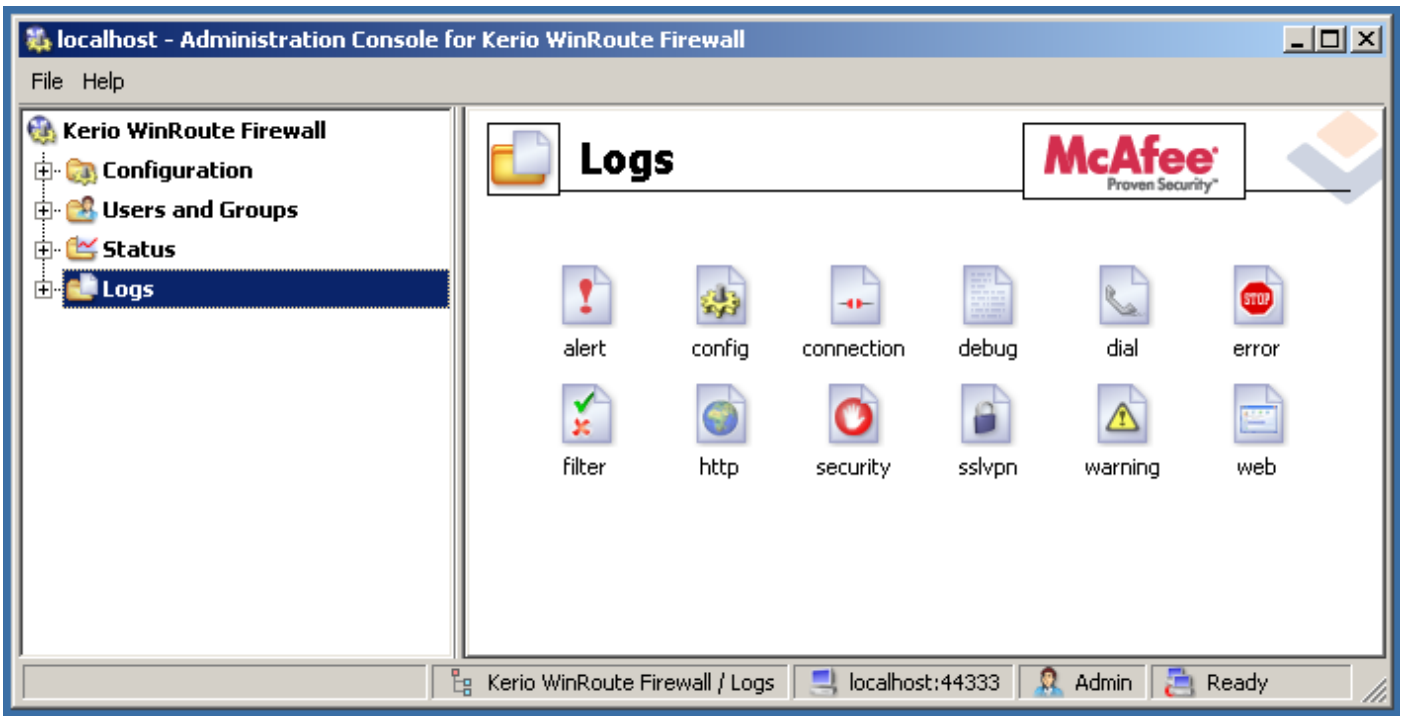
- Demand Dial: در صورتی که یک نام مربوط به شبکه ی داخلی در دسترس نباشد (مثلا شبکه هایی که در دو محل جدا از هم هستند) در این بخش می توانیم تعیین کنیم که از طریق اتصال شبکه ای راه دور به آن دسترسی پیدا کند. عملکرد این بخش به تنظیمات خاصی در Routing Table نیز وابسته است که در این مقاله اشاره ای به این دو بخش نخواهیم کرد.
- Routing Table: جدول مسیر دهی که به صورت استاتیک و دینامیک امکان تعریف پارامتر های مسیر دهی را فراهم می نماید.
- Logs and Alerts: تنظیمات مربوط به گزارش های عملکرد شبکه و کاربران و آدرس ها و ترافیک مصرفی و ... در این بخش قابل دسترس است. همچنین می توانید تنظیم کنید که گزارش ها و اخطار ها چه مدت نگهداری شوند یا این که چند وقت یک بار پاک شوند. تنظیم نحوه ی اطلاع رسانی از طریق ایمیل یا پیامک نیز در این بخش صورت می گیرد. مثلا می توان فایروال را به گونه ای تنظیم کرد که اگر یک کاربر مهاجم پورت های مربوط به فایروال را (برای نفوذ غیر مجاز) اسکن نماید، یک ایمیل یا پیامک به مقصد دلخواه شما ارسال شود.
- Advanced: تنظیمات پیشرفته شامل تنظیمات امنیتی IPSec ، امکان دسترسی به کنسول وب فایروال از آدرس آی پی خاص، تنظیمات SMTP، ذخیره ی آمار کاربران و همچنین مسدود سازی برنامه های اشتراک و انتقال فایل P2P در این بخش صورت می گیرد.

Users and Groups: تنظیمات کاربران و گروه های کاربری. اتصال به اکتیو دایرکتوری و تعیین حدود اختیارات کاربران در این بخش انجام می شود. در بحث Lan Accounting به این بخش به صورت جامع تری خواهیم پرداخت.

Status: وضعیت فعلی شامل کاربران متصل به فایروال، اتصالات، آمار استفاده، کلاینت های وی پی ان و پیغام های خطا از طریق این بخش قابل مشاهده و مدیریت می باشد.



Logs: گزارش های جزء به جزء از فعالیت های مختلف مانند سایت ها و صفحاتی که کاربران باز می کنند، گزارش های امنیتی، گزارش های مربوط به فیلتر های اعمال شده به صورت لحظه به لحظه و ... در این بخش می توانید ببینید.



به عنوان مثال یک کاربرد این بخش می تواند بررسی کیفیت اتصال اینترنت باشد. اگر از کانکشن دی اس ال استفاده می کنید و در بخش Dial به صورت Persistent (دائم متصل) تنظیم کرده اید اگر قطعی اتصال پیش بیاید و اتصال های پشت سر هم ناموفق باشد در این صورت هر بار خطای اتصال به اینترنت در گزارش ثبت می گردد. این کار برای ISP هایی که مرتب بهانه های جور وا جور به مشتری تحویل می دهند مناسب

است. این تنظیم خاص (Persistent) و گزارش مربوط به آن می تواند مدت زمانی قطع بودن اینترنت را به طور مستند نشان دهد. اگر کانکشن به صورت Manual تنظیم شود در این صورت پس از قطع شدن تا زمانی که توسط مدیر سیستم دوباره متصل نشده است هیچ گزارش خطای احتمالی ثبت نمی شود و نمی توانید به طور مستند زمان خرابی سرور های ISP را اعلام کنید.

Load Balancing: یکی از امکانات دیگر فایروال کریو امکان Network Load balancing است که به شما امکان می دهد دو اتصال اینترنت را با یکدیگر ترکیب کرده، سرعت کلی اینترنت را در شبکه ی داخلی تان افزایش دهید. برای این کار شرایط خاصی لازم است از جمله این که کارت شبکه ی متصل به شبکه ی محلی باید بیش از یکی باشد. تنظیمات این بخش در این سری مقالات آموزش داده نشده اند.

در قسمت بعدی که قسمت پایانی این مقاله است نحوه ی اجرای Lan Accounting را به صورت گام به گام همراه با توضیح مفاهیم فنی خواهید دید.