عنوان	**برنامه فایروال وینروت کریو – بخش دوم، نصب و تنظیم مقدماتی**
عنوان انگلیسی	**Kerio WinRoute Firewall 6, Installation and Basic Configuration**
کلمات کلیدی	Network, Firewall, Server, Windows, Proxy, Filter, Cache, Internet, NAT شبکه، دیوار آتش، فایروال، ویندوز، سرور، اینترنت، کنترل، فیلتر، پروکسی
مؤلف	مهدی عبداللهی
مرجع	
سطح	مبتدی
مترجم	مهدی عبداللهی (http://m0911.wordpress.com)
تاریخ انتشار	۴ آذر ماه ۱۳۸۹
تعداد صفحه	۱۵
فایل های ضمیمه	

تعریف – فایروال: فایروال یا دیوار آتش در واقع برنامه ای است که دسترسی به یک یا چند کامپیوتر را در شبکه کنترل می کند. به طور کلی تر کلیه ی بسته ها اطلاعاتی از/به یک یا چند کامپیوتر توسط فایروال کنترل می شود.

این کنترل دسترسی می تواند بر مبنای آدرس یا محدوده ی آدرس باشد. یعنی این که مثلا از آدرس (های) خاصی دسترسی کامل به کامپیوتر حفاظت شده توسط فایروال مسدود شود.

کنترل دسترسی می تواند بر حسب پورت یا سرویس باشد. مثلا سرویس FTP روی یک سرور توسط فایروال مسدود می شود.

ترکیب محدودیت های فوق بنا بر امکانات یک سیستم فایروال می تواند برای کاربران خاص یا در یک محدوده ی زمانی تعریف شود. به عنوان مثال کاربر A می تواند فقط در محدوده ی ساعتی ۱۰-۱۲ از آدرس 80.191.108.5 به کامپیوتر حفاظت شده توسط فایروال، روی پورت ۲۱ پروتوکل TCP – که همان سرویس FTP است – دسترسی داشته باشد.

به علاوه این محدودیت دسترسی می تواند همراه با محدودیت حجم ترافیک شبکه هم تعریف گردد. این همان کاری است که در یک شبکه برای محدودیت دانلود یا آپلود انجام می دهیم.

فایروال ها امکانات بسیار متنوع تری دارند که در چند سطر بالا به موارد مقدماتی اشاره کردم. لازم است که اطلاعات پایه ای راجع به فایروال ها داشته باشید تا بتوانید با هر سیستم فایروال اعم از سخت افزاری یا نرم افزاری کار کنید.

تعریف- سرور فایروال: کامپیوتری که روی آن موتور فایروال کریو نصب می شود. این کامپیوتر الزاما سیستم عامل ویندوز سرور نیست و می تواند از ویندوز کلاینت هم استفاده نماید.

مراحل نصب فایروال کریو ساده است و در ادامه ی این بخش به صورت تصویری آن را خواهید دید.

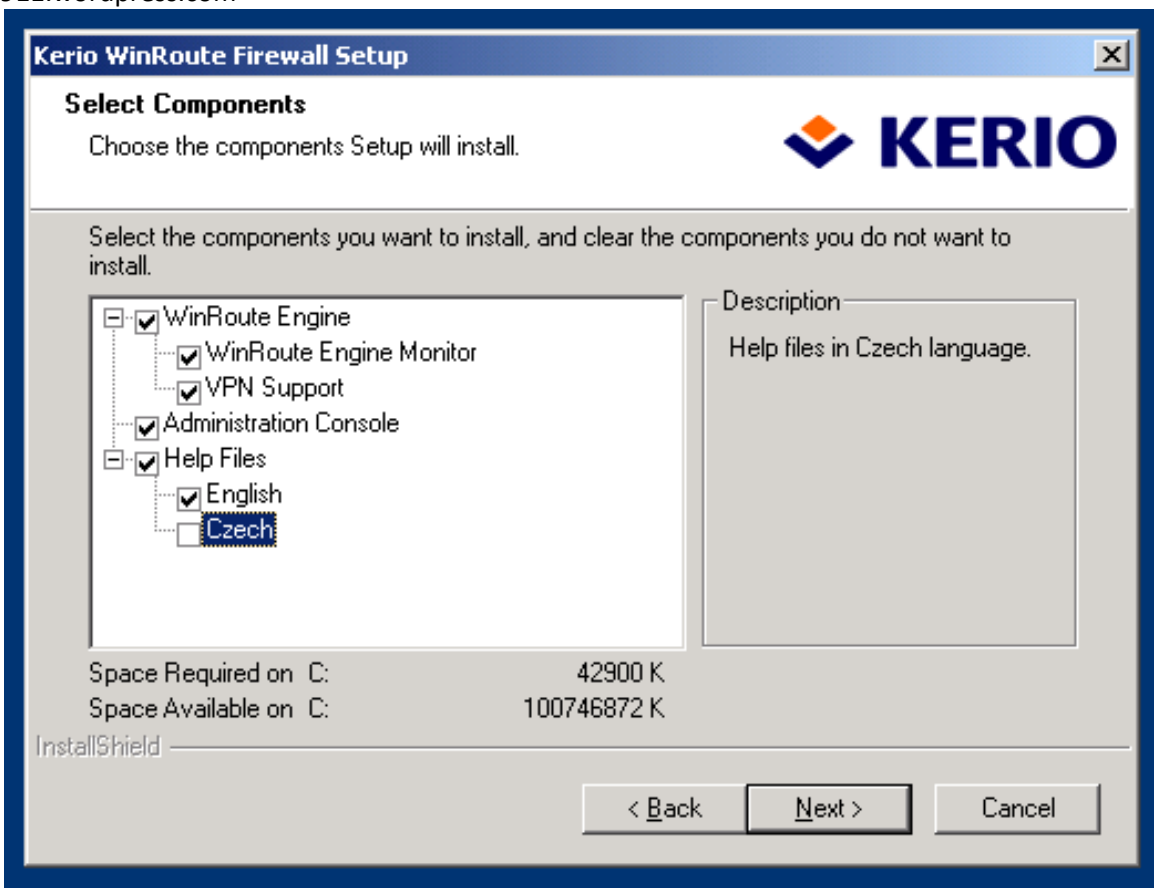
- پس از اجرای برنامه ی نصب، در صفحه ی نخست چاره ای جز زدن دکمه ی Next ندارید!
- در صفحه ی دوم نیز باید I accept را انتخاب کنید تا به صفحه ی بعدی بروید.
- در صفحه ی سوم مسیر نصب برنامه را شامل درایو و پوشه ی مورد نظر تان انتخاب می نمایید.

در صفحه ی چهارم گزینه های نصب را تعیین می نمایید.

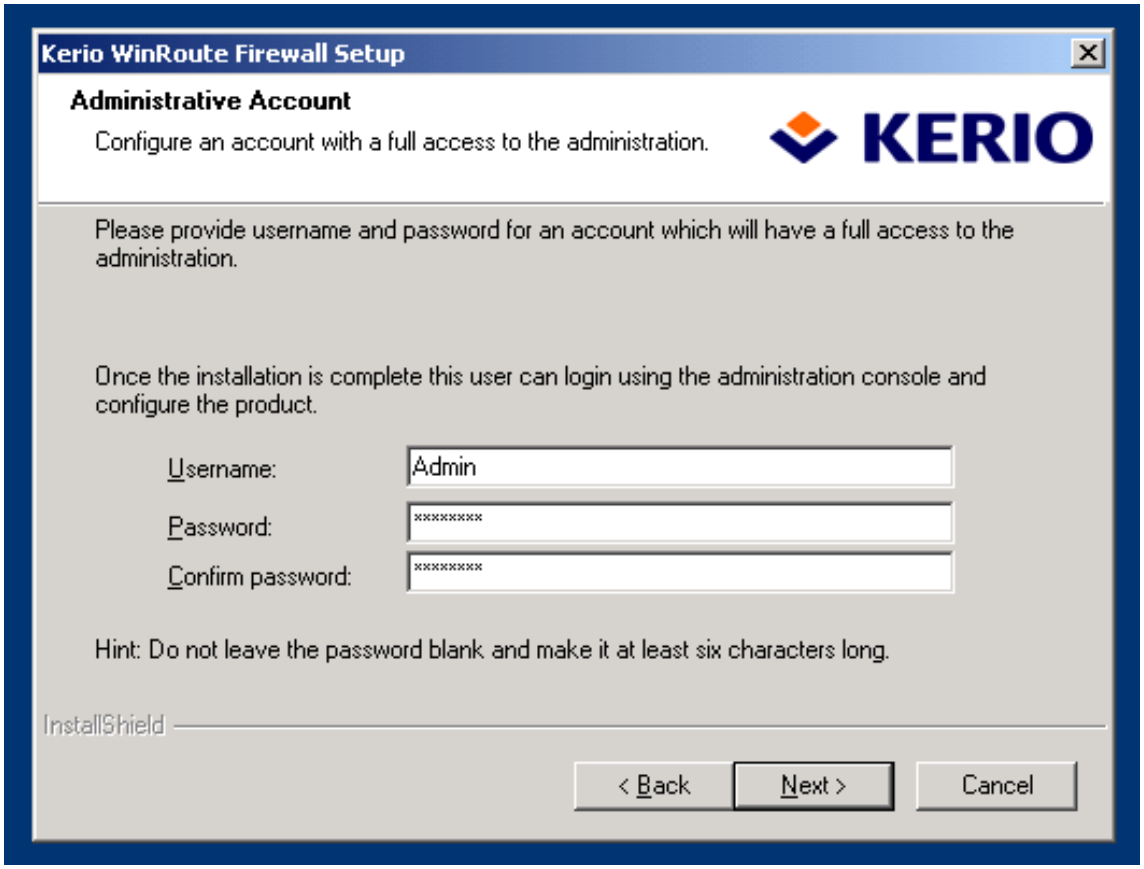
WinRoute Engine Monitor: یک برنامه ی کوچک که وضعیت اجرای فایروال کریو را نشان می دهد و در عین حال می توانید توسط آن فایروال را متوقف نمایید. در بخش Startup Preference می توانید تعیین کنید که فایروال به هنگام بالا آمدن ویندوز اجرا شود یا خیر.

VPN Support: امکان ایجاد اتصال وی پی ان توسط فایروال کریو را نصب می نماید. لیکن فعال سازی آن در مرحله ی تنظیمات پس از نصب صورت می گیرد.

Administration Console: پانل مدیریت فایروال را نصب می کند. اگر این گزینه را فعال کنید روی خود سرور (کامپیوتری که فایروال کریو روی آن نصب می شود) امکان مدیریت فایروال را نخواهید داشت. در نتیجه باید کنسول مدیریت را روی کامپیوتر دیگری نصب کنید و به هنگام اجرای آن آدرس ای پی یا نام سرور فایروال را همراه با کاربر و گذرواژه ی مدیر فایروال وارد نمایید.



در صفحه ی بعدی باید نام کاربر و گذرواژه ی مربوط به مدیر فایروال را تعیین نمایید. توجه داشته باشید که این داده ها به صورت رمزنگاری شده ذخیره می شوند و در صورت فراموشی، نمی توانید آن ها را بازیابی کنید.

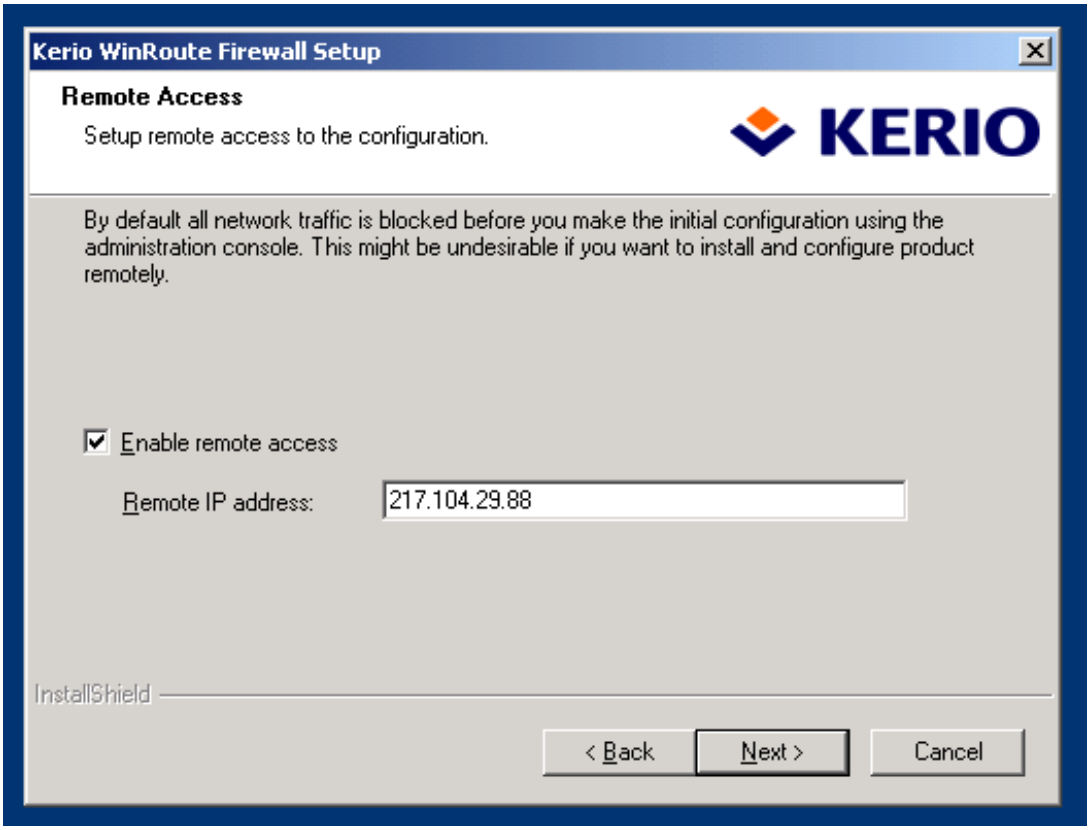


اگر به صورت ریموت دسکتاپ یا ترمینال سرویس به سرور فایروال وصل شده اید و در این حالت فایروال کریو را نصب می کنید باید توجه داشته باشید که بلافاصله پس از نصب، تمامی پورت های دسترسی توسط فایروال به صورت پیش فرض مسدود می شود و شما امکان وارد شدن به سرور را از دست می دهید.

توصیه می کنم اگر سروری که برای فایروال در نظر گرفته اید با تعداد قابل توجهی کلاینت مرتبط است، عملیات نصب و تنظیم فایروال را مستقیم پشت سرور انجام دهید. اگر امکان حضور در محل سرور را ندارید ترجیحا موقعیت به گونه ای باشد که یک نفر دیگر در محل استقرار سرور حضور داشته باشد تا در صورت لزوم بتواند یک سری دستورالعمل های مقدماتی را انجام دهد.

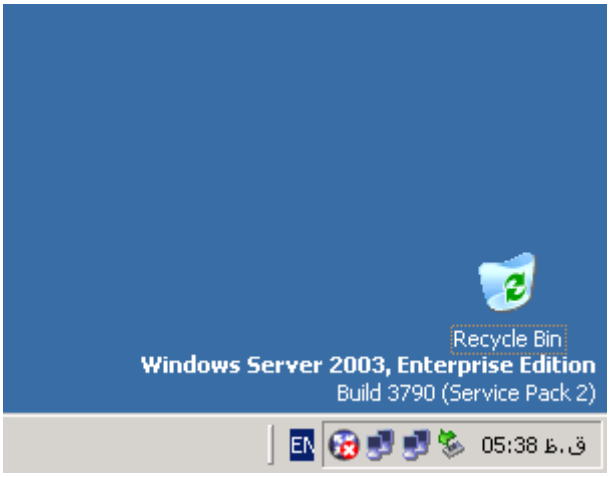
اگر شرایط به گونه ای است که مجبور هستید فایروال را از راه دور نصب کنید باید در نظر داشته باشید که باید آدرس IP تان را در مرحله بعدی نصب اعلام نمایید تا پس از اجرای فایروال، مجوز دسترسی از این آدرس برای شما تنظیم شده باشد. این آدرس آی پی باید ثابت (Static) باشد و اگر به فرض اتصال اینترنت شما به گونه ای است که در هر بار اتصال آدرس متفاوتی دریافت می کنید ممکن است دچار دردسر شوید.

چرا که اگر پس از تعیین آدرس فعلی تان به عنوان نقطه ی دسترسی مجاز، اتصال شما قطع شود و با آدرس دیگری دوباره به اینترنت وصل شوید فایروال به شما اجازه ی دسترسی به سرور را از آدرس IP جدید تان نخواهد داد.

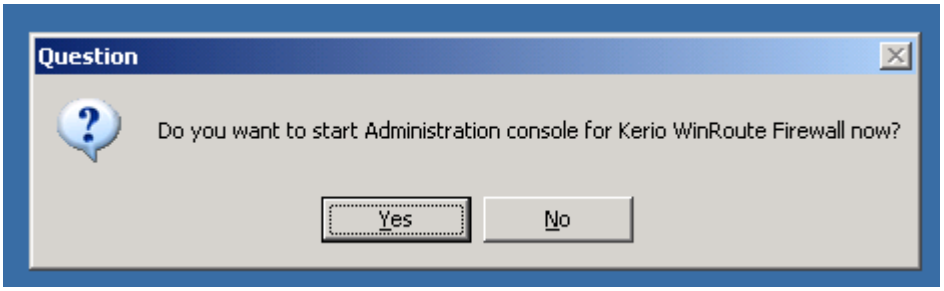


در مرحله ی پایانی از شما خواسته می شود که که کامپیوتر را مجدد راه اندازی نمایید.

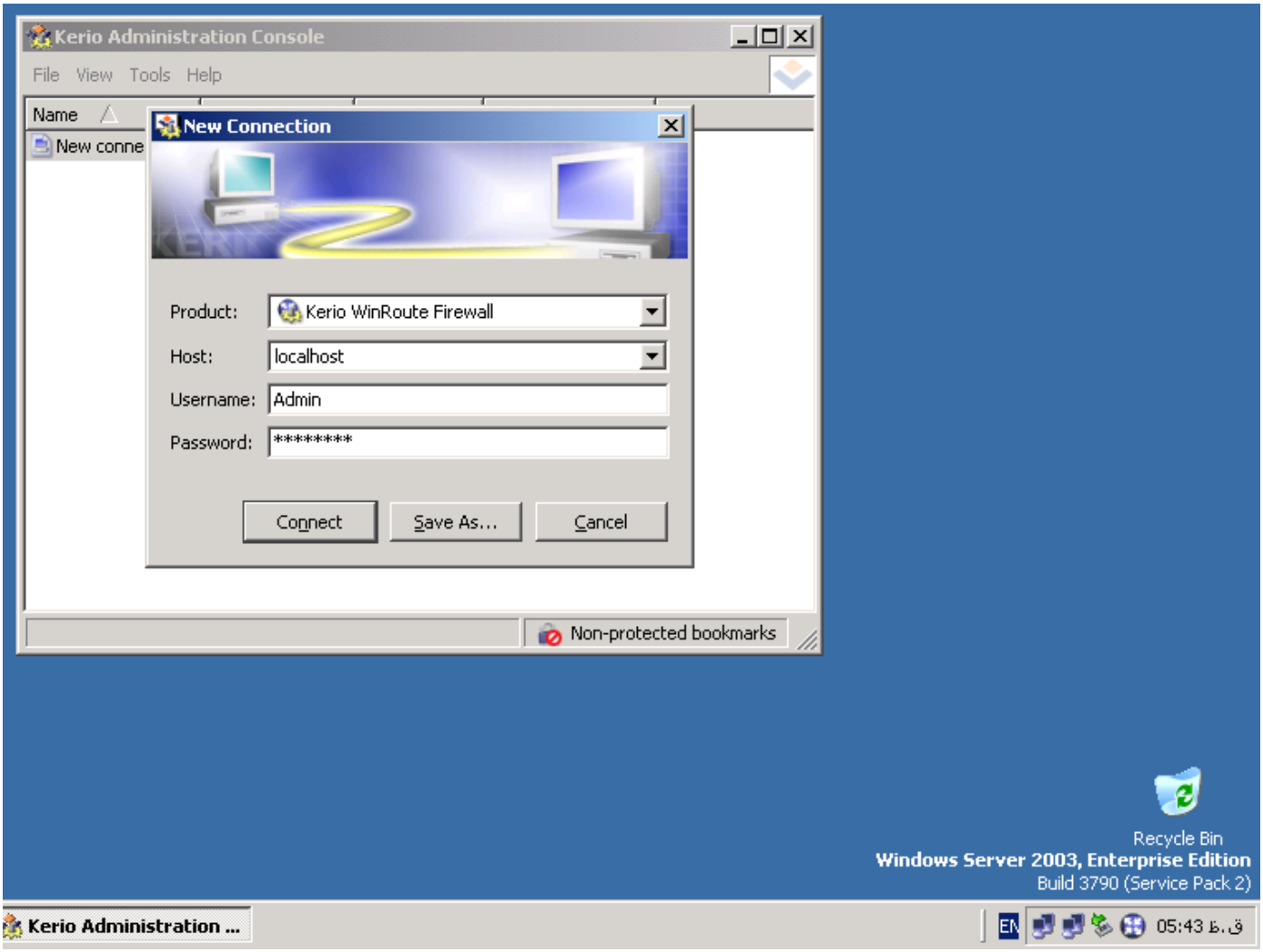
پس از بالا آمدن دوباره ی ویندوز اگر نشان ضربدر قرمز روی آیکن برنامه ی Engine Monitor باشد به معنی آن است که هنوز سرویس فایروال کریو اجرا نشده است. در بخش Manage -> Services and Applications -> Services می توانید وضعیت سرویس Kerio Firewall را بررسی نمایید. با راست کلیک روی آیکن می توانید گزینه ی Start Kerio Engine را انتخاب کنید تا اجرای فایروال آغاز شود.



در نخستین بار پس از نصب فایروال که ویندوز بالا می آید، برنامه ی کریو از شما سؤالی مبنی بر اجرای پانل مدیریت فایروال می پرسد که از این طریق تنظیمات آن را انجام دهید. اگر این کار را انجام ندهید به طور پیش فرض تمامی دسترسی ها از طریق همه ی کارت های شبکه مسدود خواهد گردید. اگر به این سؤال پاسخ مثبت بدهید پانل مدیریت فایروال اجرا خواهد گردید.



نام کاربر مدیر و گذرواژه را –که به هنگام نصب برنامه تعیین کرده اید – وارد نمایید. اگر پانل مدیریت را از کامپیوتر دیگری به جز سرور فایروال اجرا می نمایید می توانید در بخش Host نام یا آدرس آی پی سرور را وارد نمایید. سپس دکمه ی Connect را بزنید. می توانید اطلاعات ورود به پانل مدیریت (نام سرور، کاربر و گذرواژه) را توسط دکمه ی Save As... ذخیره نمایید. مثلا هم زمان از طریق کامپیوتر تان چند فایروال را کنترل می کنید که هر کدام را با آدرس های آی پی و نام کاربری شان به یک نام دلخواه ذخیره می نمایید و برای اتصال به هر کدام کافی است که روی نام آن – که در فهرست صفحه ی Administration Console می بینید - کلیک نمایید.



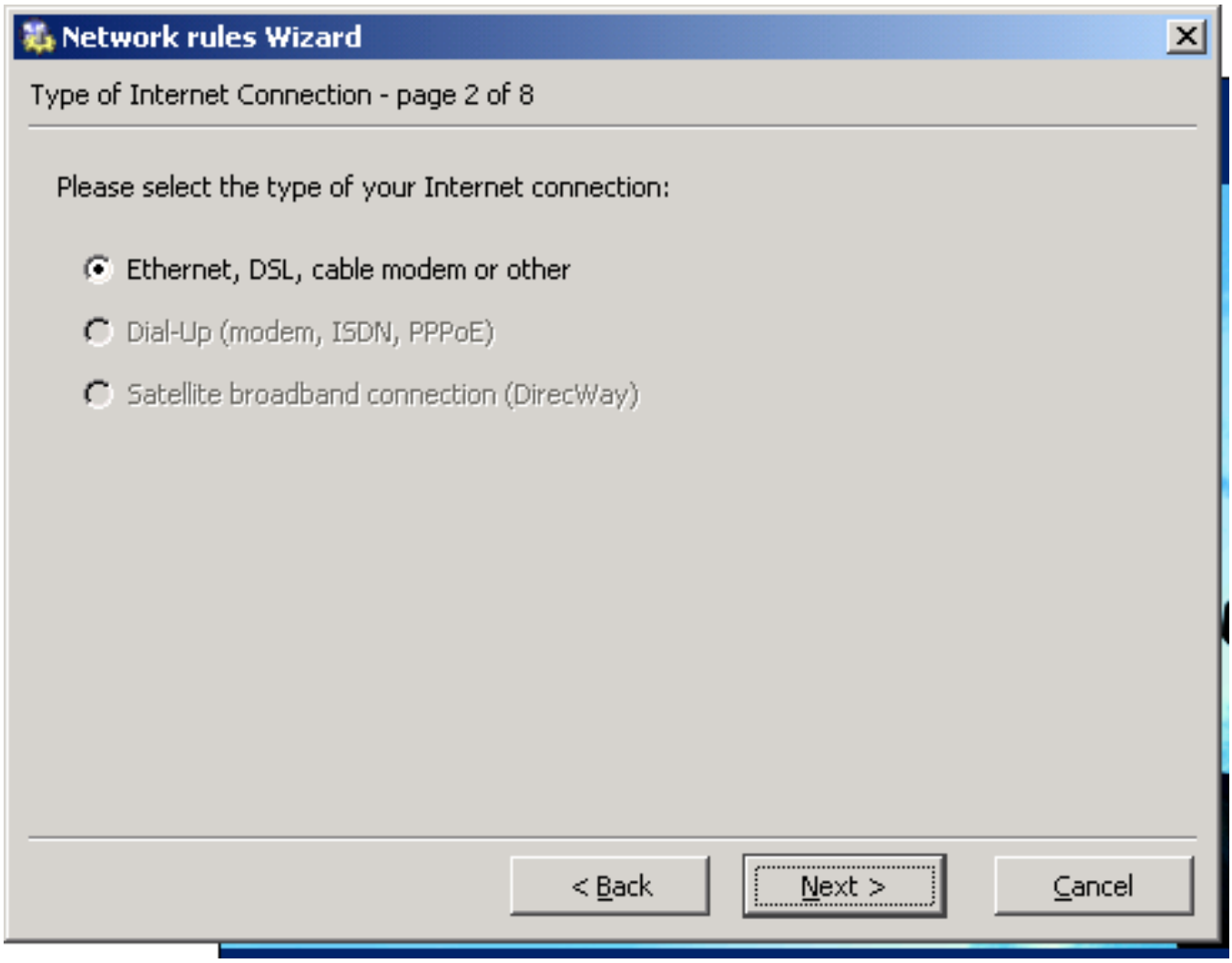
آیکن سفید و آبی در گوشه ی پایین صفحه نشان می دهد که فایروال روی همین کامپیوتر در حال اجرا است. البته اگر از راه دور به کنسول مدیریت فایروال متصل شوید آیکن مذکور چیزی را نشان نمی دهد.

نکته: پیش از اجرای تنظیمات مطمئن شوید که کارت شبکه ی محلی و اتصال اینترنت روی سرور فایروال به درستی تنظیم شده اند و کار می کنند.

در نخستین اجرای کریو پنجره ی Network rules Wizard را خواهید دید که در چند مرحله سؤالاتی را از شما می پرسد و توضیحاتی راجع به هر مرحله به شما نشان می دهد که فهم آن کار آسانی خواهد بود. پس از اتمام این چند مرحله، فایروال به طور مقدماتی شروع به کار می کند و البته شما هم می توانید تنظیمات را بعدا به صورت دستی تغییر دهید.

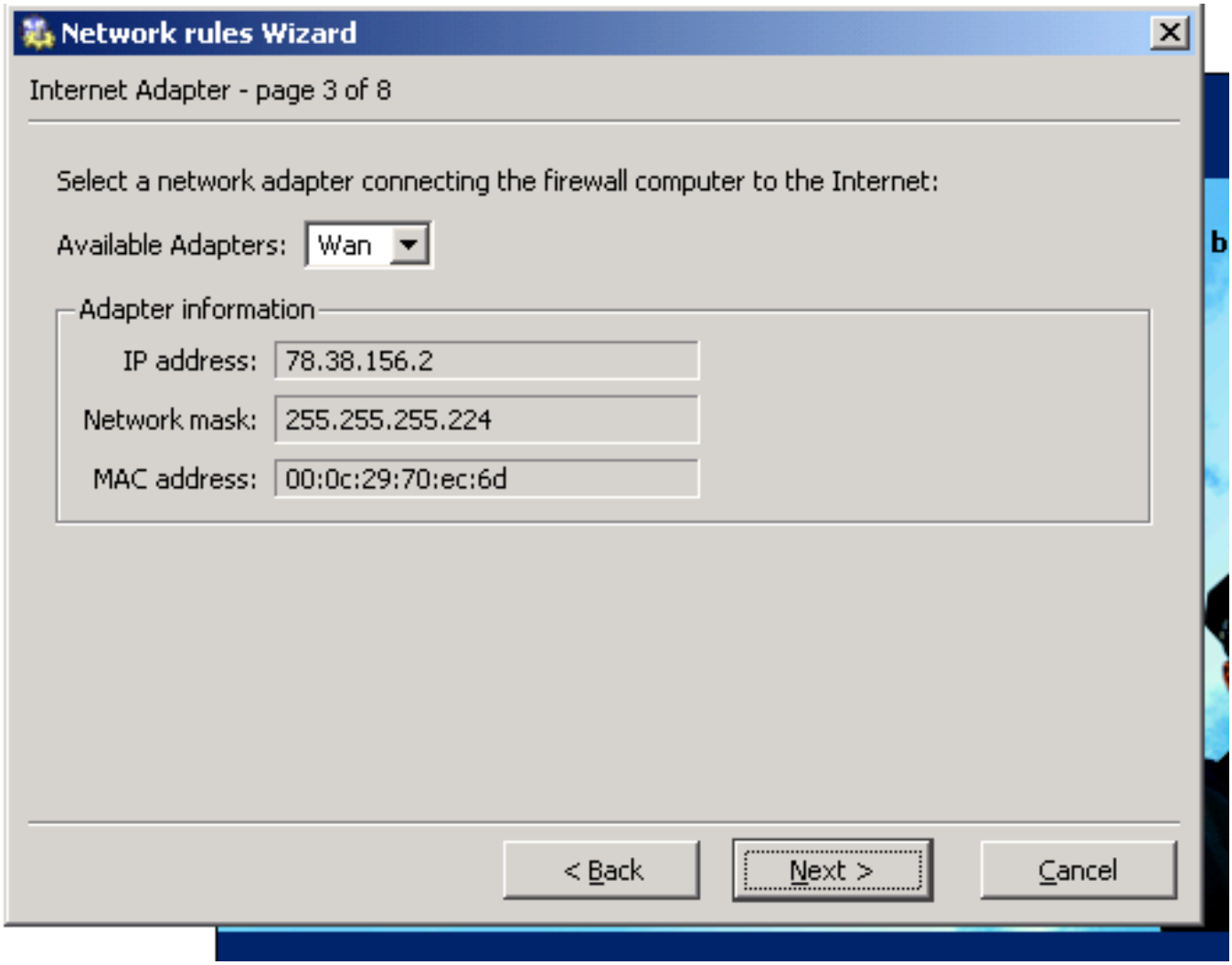
گام دوم – تعیین نوع اتصال اینترنت: در این مرحله بسته به تنظیمات شبکه تان سه گزینه نمایش داده خواهد شد:

- اگر یک کارت شبکه را برای اتصال به مودم لیزلاین یا دی اس ال و ... استفاده می کنید، گزینه ی نخست را باید استفاده نمایید.
- اگر از کانکشن ISDN یا PPPoE استفاده می نمایید باید گزینه ی دوم را انتخاب نمایید. لازم است که پیش از اجرای برنامه، کانکشن ها را ساخته باشید و نام کاربر و گرواژه ی اتصال را نیز ذخیره کرده باشید.
- گزینه ی سوم هم برای اتصال ماهواره به کار می رود.



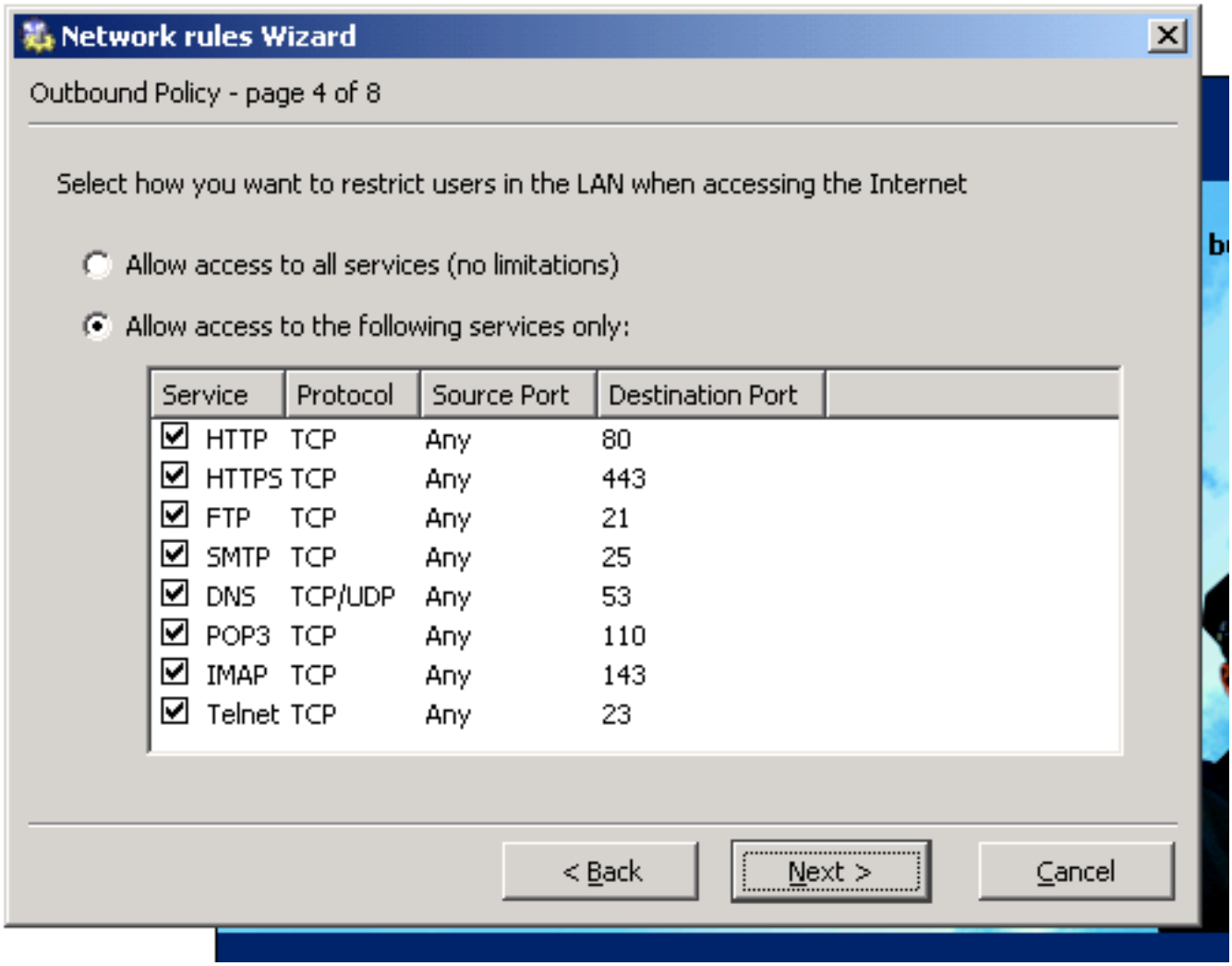
در صورتی که بیش از یک اتصال اینترنت استفاده می نمایید، می توانید در این مرحله گزینه ی اصلی تان را انتخاب نمایید و در مراحل بعدی اتصال پشتیبان تان را هم معرفی نمایید.

گام سوم- اتصال اینترنت: در مرحله ی سوم بسته به این که نوع اتصال اینترنت را چگونه تعیین کرده اید، اتصال مورد نظر تان را انتخاب می نمایید. در این مثال کامپیوتر سرور ما توسط مودم لیزلاین و به طور مستقیم به اینترنت وصل می شود. به همین دلیل با توجه به گزینه ی انتخاب شده ی مرحله ی قبلی، کارت شبکه ای را که به اینترنت متصل است انتخاب می نمایید. در این جا پیش از اجرای تنظیمات کریو، نام Local Area Connection را در بخش Network Connections از کنترل پانل به Wan تغییر داده ایم.

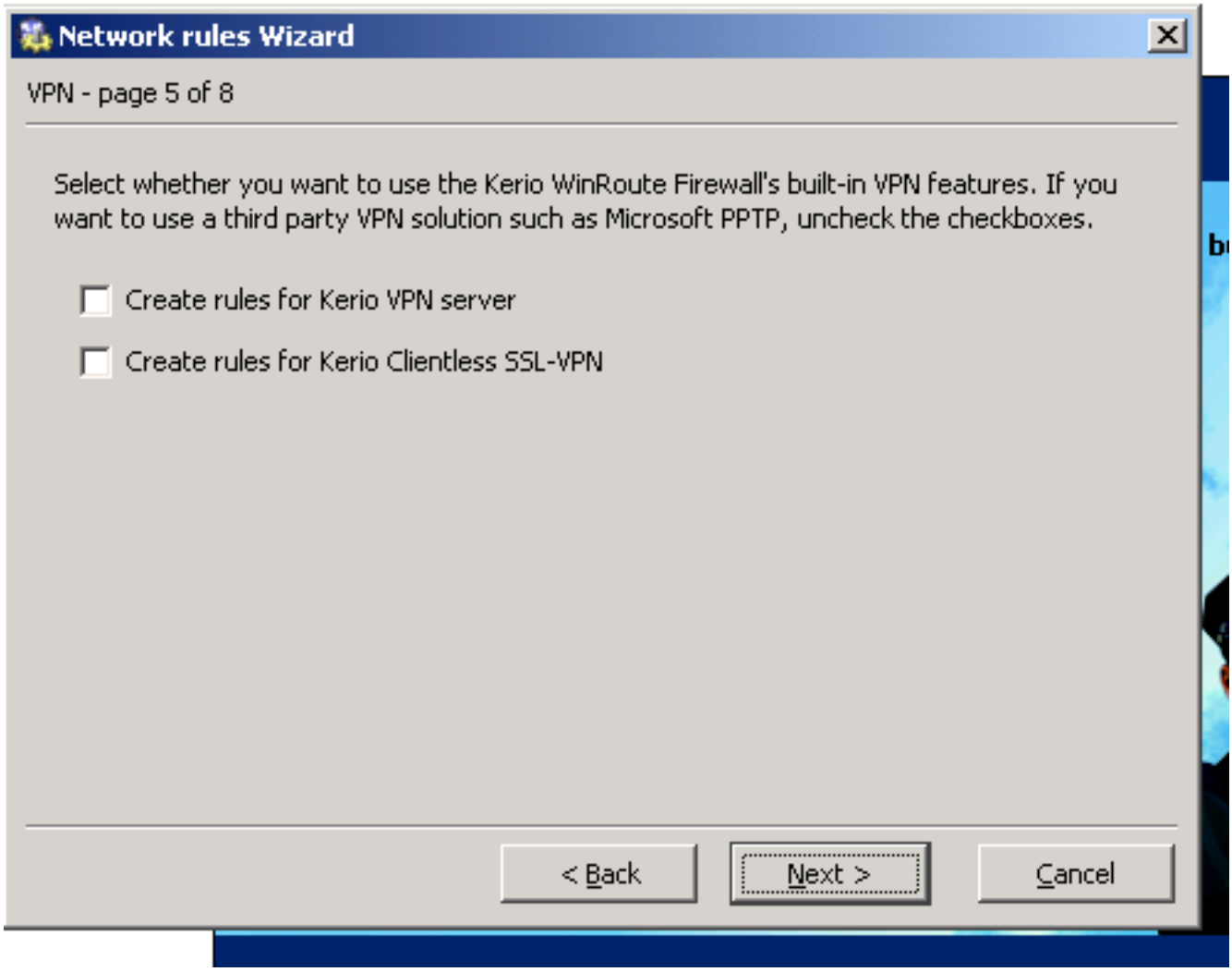


گام چهارم – سیاست های خروجی: در این مرحله پنجره ی Outbound Policy نمایش داده می شود. در واقع شما تعیین می کنید که کاربران شبکه ی محلی تان با چه سرویس هایی به اینترنت دسترسی پیدا کنند.

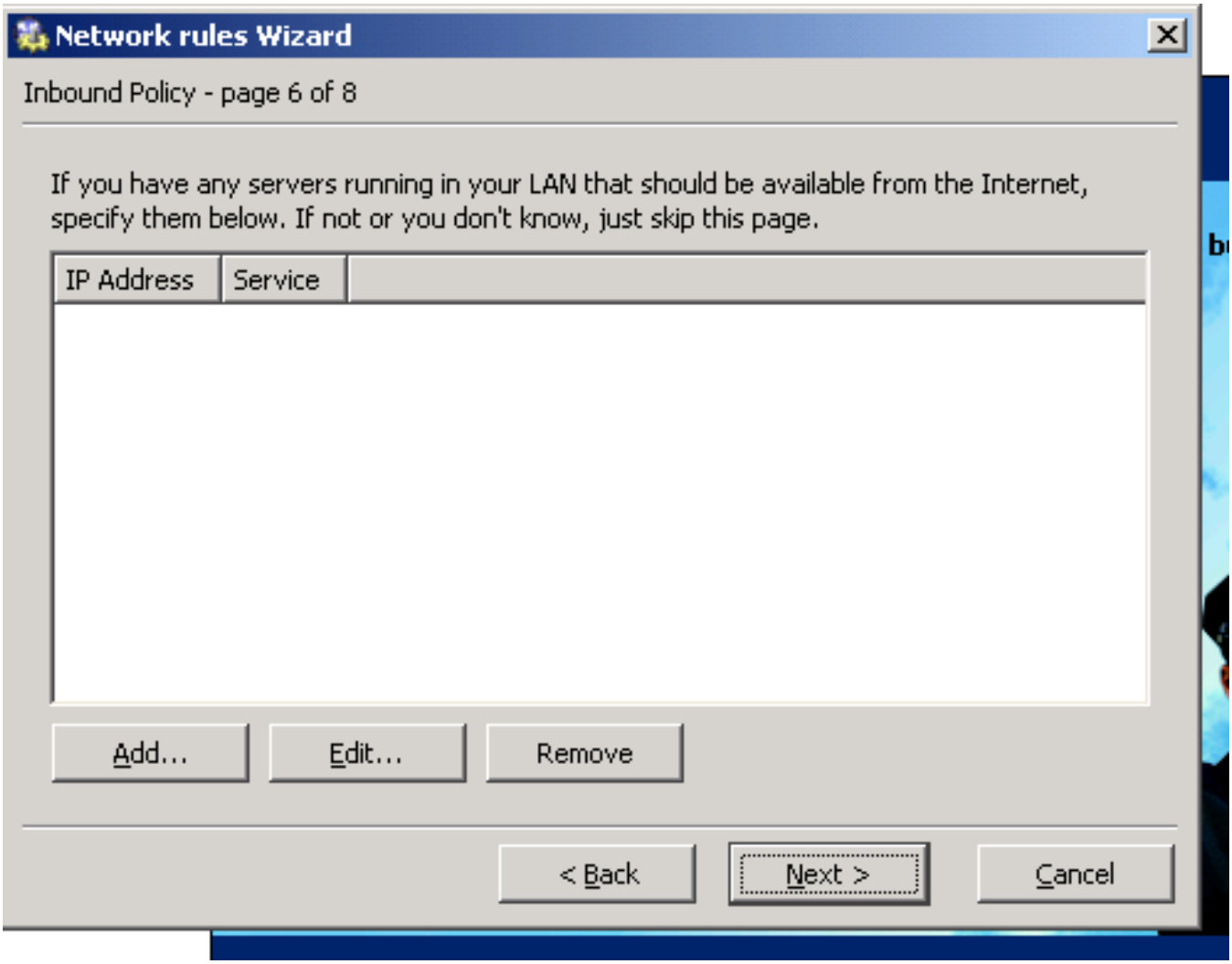
- گزینه ی نخست این امکان را فراهم می آورد که کاربران شبکه ی محلی به تمامی سرویس های اینترنت (یا اینترانت) دسترسی پیدا کنند.
- گزینه ی دوم ۸ سرویس منتخب و مشهور را به شما نشان می دهد که می توانید هر کدام از این ۸ مورد را هم غیر فعال نمایید. سرویس هایی مانند وب، ایمیل، DNS و FTP و ... در این مرحله قابل دسترس هستند. البته بعد از این هم می توانید سرویس های دلخواه تان را به این فهرست بیفزایید.



گام پنجم – وی پی ان: در این مرحله می توانید گزینه های مربوط به سرویس وی پی ان کریو را انتخاب کنید. در این صورت مراحل بعدی به گونه ای خواهد بود که تنظیمات وی پی ان را انجام دهید. با توجه به این که وی پی ان مقوله ای جدا از محتوای این سری مقاله آموزشی می باشد و هدف نهایی این مقاله ی آموزشی راه اندازی سرویس Lan Accounting است، مرحله ی مربوط به تنظیمات وی پی ان را نادیده می گیریم و به عهده ی خودتان می گذاریم. در ضمن اگر از سرویس وی پی ان دیگری مانند PPTP میکروسافت استفاده می نمایید می توانید این گزینه ها را غیر فعال نموده، به گام بعدی بروید.



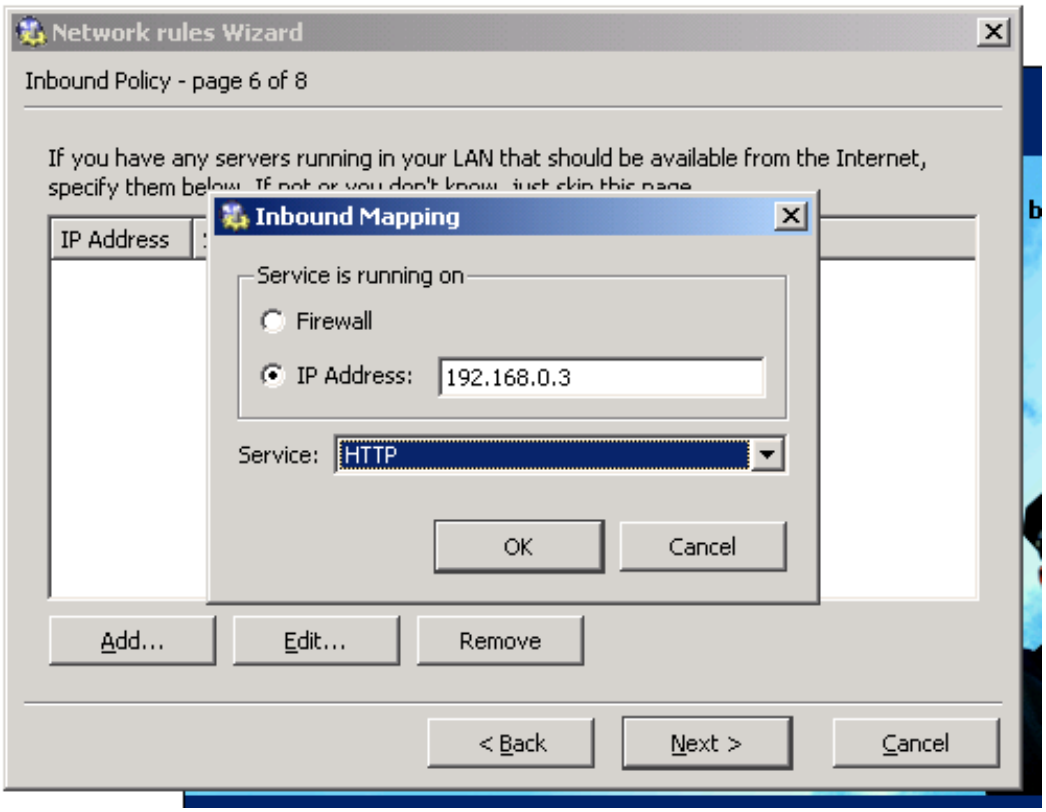
گام ششم – سیاست های ورودی: اگر در شبکه ی داخلی تان سرور هایی دارید که قرار است از طریق اینترنت قابل دسترس باشند، در این مرحله می توانید مشخص نمایید. در صورتی که چنین سرور هایی ندارید می توانید این مرحله را رد کنید.

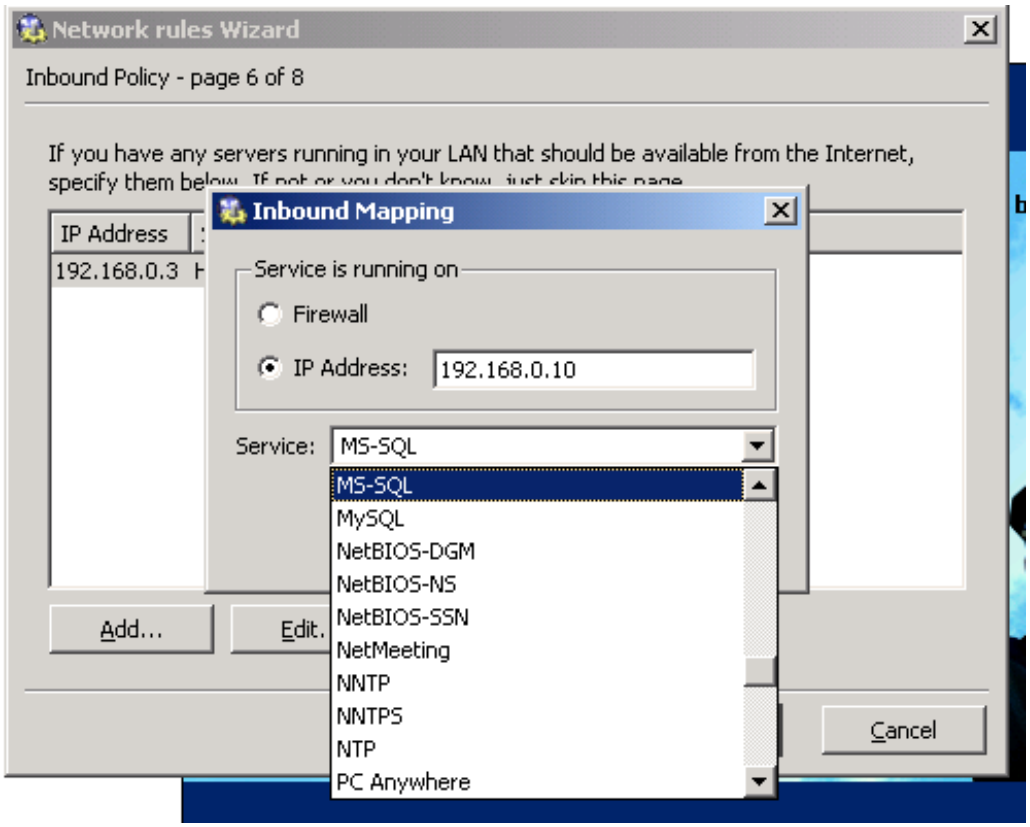


مثلا ممکن است یک سرور وب داشته باشید که به دلیل نبود آی پی اختصاصی، به طور مستقیم به اینترنت وصل نباشد. در این بخش می توانید آدرس آی پی داخلی آن را وارد نمایید. حالا اگر کاربری بخواهد صفحه وب سایتی را که روی سرور وب قرار دارد، ببیند کافی است که آدرس آی پی (و در صورت لزوم شماره ی پورت خاص) سرور فایروال را در نوار آدرس مرورگر اینترنت وارد نماید. فایروال پس از دریافت درخواست دسترسی به سرور وب (مثلا روی پورت ۸۰) درخواست مذکور را به آدرس آی پی داخلی سرور وب هدایت (دایورت یا فوروارد) می کند.

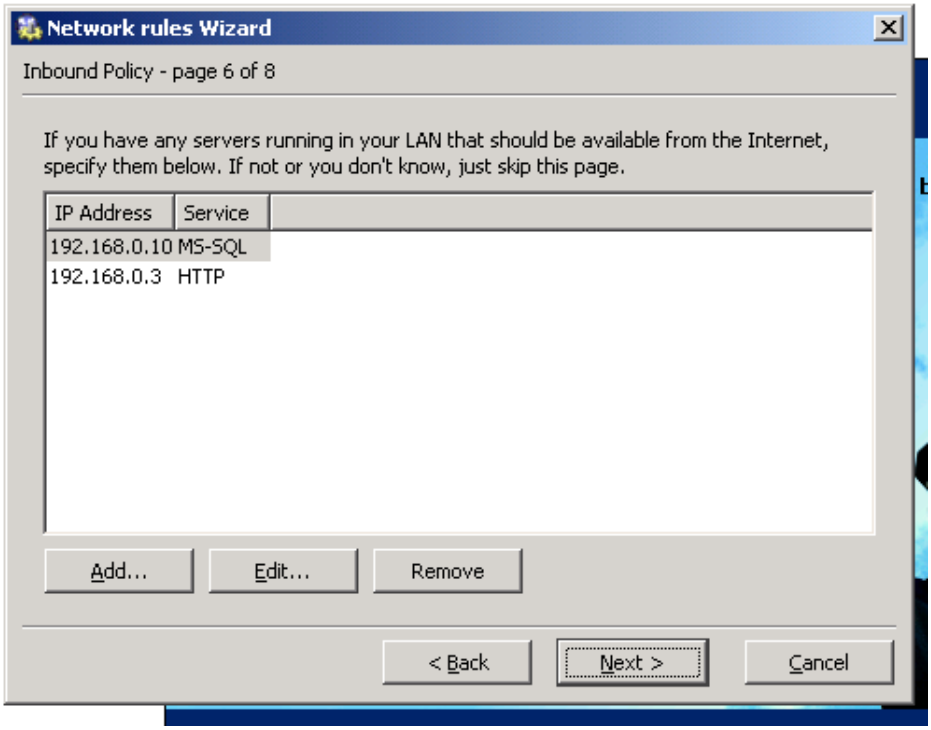
به عنوان مثال در شبکه ی داخلی ما سرور با آدرس 192.168.0.3 سرویس وب و سرور دیگری با آدرس 192.168.0.10 سرویس بانک اطلاعاتی MS SQL Server را اجرا می نماید. البته در فایروال کریو (یا هر فایروال دیگری) سرویس های مشهور با نام شان نمایش داده می شوند و بقیه ی سرویس ها یا نرم افزار های شبکه ای را باید از طریق شماره ی پورت شناساند. البته در برخی فایروال ها فارغ از هر تبعیضی باید تمامی سرویس های شبکه را به صورت شماره ی پورت مشخص نماییم.

دکمه ی Add را بزنید تا پنجره ی Inbound Mapping باز شود. سرویس مورد نظر را از فهرست باز شوی Service انتخاب نمایید. در بخش تعیین محل اجرای سرویس می توانید آدرس ای پی سرور مربوط به آن را وارد نمایید. اگر سرویس مذکور روی سرور فایروال اجرا می شود می توانید گزینه ی Firewall را انتخاب نمایید. در این صورت به ساده گی پورت مربوط به آن سرویس برای دسترسی مستقیم روی سرور فایروال باز می شود.

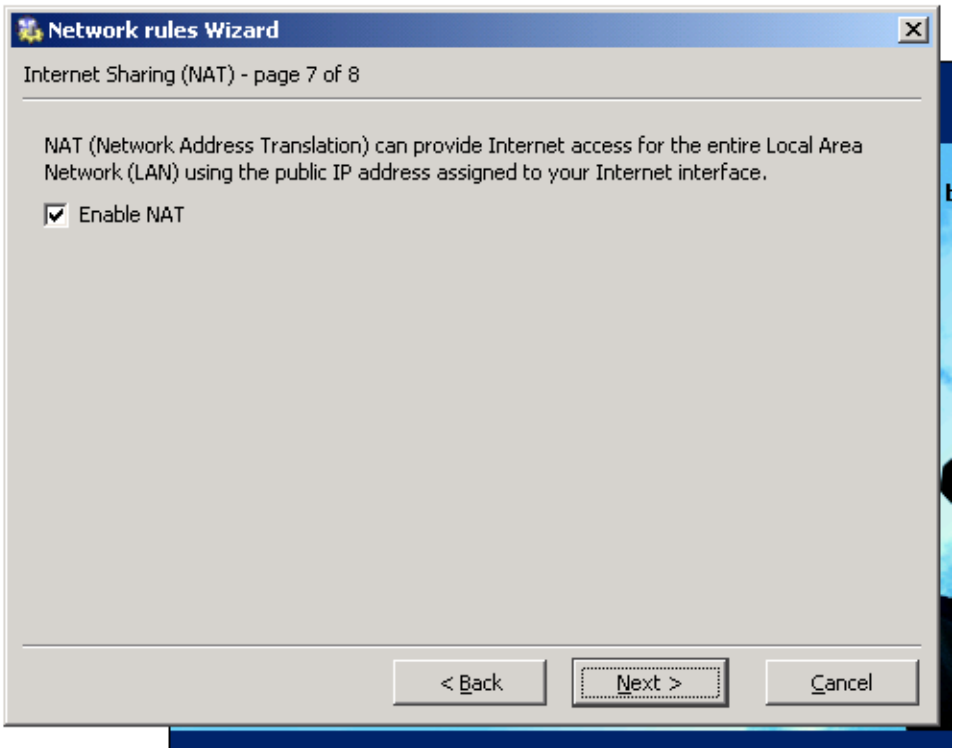




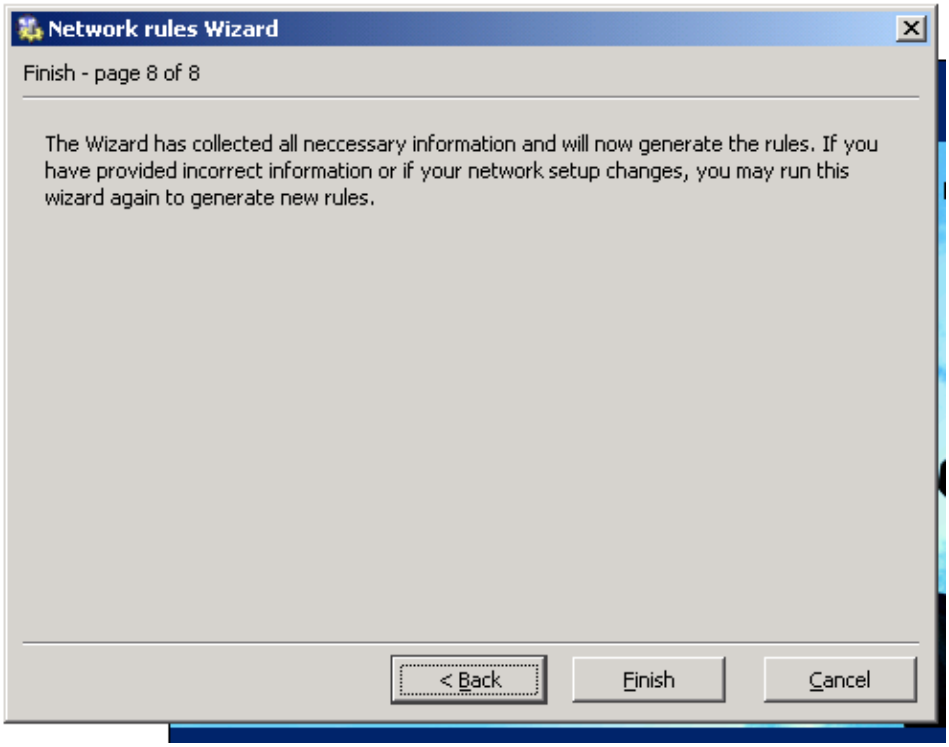
پس از انتخاب سرویس ها فهرستی مانند زیر خواهید داشت. به گام بعدی بروید.



گام هفتم – استفاده ی مشترک از اینترنت: در بخش Internet Sharing یا همان NAT می توانید تعیین کنید که تمامی کامپیوتر های شبکه ی محلی از طریق سرور فایروال به اینترنت دسترسی داشته باشند. در این حالت تنظیمات ای پی باید به گونه ای باشد که در کامپیوتر های کلاینت شبکه، پارامتر Default Gateway برابر با آدرس ای پی سرور فایروال تعریف شود. البته می توانید با استفاده از سرویس پروکسی که در کریو تنظیم می نمایید، بدون نیاز به Gateway امکان دسترسی فیلتر شده به اینترنت را فراهم کنید که در قسمت های بعدی به آن اشاره خواهیم کرد.



گام هشتم – پایان: تمام شد! فایروال کریو را با داشتن کمترین اطلاعات راجع به آن راه اندازی کردید. حال می توانید برای تنظیمات بیشتر به صورت دستی عمل کنید.



در بخش بعدی مروری کلی به امکانات مختلف فایروال کریو خواهیم داشت.