# حفاظت شبکه با پیکربندی دقیق دیوارهٔ آتش

# Firewall


وب، ملغمه‌ای از عناصر خوب و بد است. به ازای هر قدیس بر روی وب، یک نفر هم وجود دارد که سعی می‌کند به کامپیوتر شما نفوذ کند و از هویت شما سوءاستفاده کند، کامپیوتر شما را به منظور ارسال **هرزنامه** به گروگان بگیرد، یا از آن برای حمله به شبکه‌های دیگر استفاده کند، و همهٔ گناهان را به گردن شما بیندازد. برای اکثر کامپیوترها، بهترین راه‌حل، یک **دیوارهٔ آتش** است که به خوبی تنظیم‌شده است.

دیواره‌های آتش در گذشته به دلیل پیچیدگی، تحت نظر و استفادهٔ کاربران پیشرفته و باتجربه بودند، اما خوشبختانه، در حال حاضر دیگر لازم نیست که برای برپاسازی دیوارهٔ آتش، یک مهندس کامپیوتر باشید. دیواره‌های آتش امروزی حاوی برنامه‌های مدیریت خوش‌طرح و تنظیمهای **پیش‌گزیدهٔ** (default) خوبی هستند که تأمین امنیت را خیلی سریع فراهم می‌سازند. با وجود این، نصب یک دیوارهٔ آتش بدون برنامه‌ریزی دقیق، شبکهٔ شما را امن نخواهد کرد.

## ترافیک و نشانیهای اینترنت

زبان میانجی اینترنت، **TCP/IP**[1] است. وقتی چیزی را در گوگل جستجو می‌کنید، کامپیوتر شما تعدادی **بسته–بیت** (**packet**) داده‌ای را به **خدمات‌دهندهٔ** (server) گوگل ارسال می‌کند؛ این بسته–بیتها با TCP/IP بسته‌بندی می‌شوند. ساختار TCP/IP پیچیده است، اما فقط دو خصوصیت مهم وجود دارد که ما برای نیازهای خود باید آنها را بشناسیم. TCP/IP شامل دو بخش اصلی **داده‌ها** (data) و **عنوان** (header) است. در مثال ما، **داده‌ها** همان چیزهایی هستند که می‌خواهیم خدمات‌دهنده‌های گوگل دریافت کنند. **عنوانها** حاوی اطلاعات نشانی هستند، هم نشانی جایی که داده‌ها باید تحویل شوند و هم نشانی مبدأ.

برای پیکربندی یک دیوارهٔ آتش، می‌توانیم بسیاری از داده‌هایی را که در بسته–بیت‌های TCP/IP حمل می‌شود نادیده بگیریم. دیواره‌های آتشی که می‌توانند به **داده‌های** یک بسته–بیت نگاه کنند و آنها را مورد بررسی قرار دهند، پیچیده‌تر از نیاز بسیاری از شبکه‌های خانگی هستند. با وجود این، ما در مورد نوع داده‌های ارسالی نیز حساس هستیم.

[1] Transmission Control Protocol/Internet Protocol

**عنوان** (header) در یک بسته–بیت TCP/IP، حاوی نشانیهای مقصد و منبع بسته–بیت در یک فرمت **۳۲**بیتی شبیه به فرمت زیر است: 192.168.1.1.

اگر پیشتر یک شبکهٔ خانگی برپا کرده باشید، یا به اینترنت وصل شده باشید، احتمالاً با این نوع نشانی‌دهی آشنا هستید. هر کامپیوتر روی شبکه به یک **نشانی IP**[2] منحصر به فرد شبیه به فرمت مذکور نیاز دارد. این نشانی را می‌توانید به صورت نشانی یک آپارتمان یا خانه تصور کنید. هر خدمات‌دهندهٔ گوگل یک **نشانی IP** دارد، و کامپیوتر شما هم یک **نشانی آی‌پی** (IP) برای خودش دارد. وقتی با گوگل جستجو می‌کنید، یک جریان از بسته–بیتها را به نشانی یکی از خدمات‌دهنده‌های گوگل ارسال می‌کنید، و گوگل در پاسخ، جریانی از بسته–بیتها را به نشانی کامپیوتر شما ارسال می‌کند.

## پورتها داده‌ها را به برنامهٔ کاربردی متناسب، هدایت می‌کنند

یک **نشانی آی‌پی** به تنهایی برای ارسال و دریافت داده‌ها در اینترنت کافی نیست. به عنوان مثال، ممکن است موقع دریافت یک فایل از یک **خدمات‌دهندهٔ FTP**[3]، همزمان در حال مرور اینترنت باشید، یا ایمیلی را از یک **خدمات‌دهندهٔ پستی**[4] متعلق به ISP[5]

[2] IP (Internet Protocol) address
[3] FTP (File Transfer Protocol) server
[4] mail server
[5] Internet service provider

(فراهم‌کنندهٔ خدمات اینترنت) خود دریافت می‌کنید. اگر همهٔ این داده‌ها فقط به نشانی آی‌پی کامپیوتر شما نشانی‌دهی می‌شدند، کامپیوتر روشی برای فهمیدن این مسئله نداشت که آیا باید داده‌ها را به برنامهٔ ایمیل بفرستد، یا به برنامهٔ FTP، یا به برنامهٔ مرورگر وب.

راه‌حل این مسئله، استفاده از **پورتها** (port) یا درگاههاست. **پورتها** اعدادی هستند که بخشی از **عنوان** بسته–بیت TCP/IP را تشکیل می‌دهند. بیش از ۶۵۰۰۰ پورت قابل دستیابی است، و هر شمارهٔ پورت معمولاً مرتبط با یک سرویس اینترنت ویژه، یا یک برنامهٔ ویژه است. به عنوان مثال، **خدمات‌دهنده‌های وب**[6] معمولاً به ترافیک روی پورت 80 «گوش می‌دهند». وقتی برنامهٔ مرورگر شما یک درخواست را برای دریافت یک صفحهٔ وب ارسال می‌کند، سیستم‌عامل خدمات‌دهندهٔ وب، بسته–بیتهایی را که در **عنوان** آنها پورت 80 مشخص شده است می‌یابد، و سپس آنها را به برنامهٔ کاربردی http خود ارسال می‌کند.

## فیلترگذاری دیوارهٔ آتش

چرا باید در کامپیوتر یک دیوارهٔ آتش نصب کرد؟ **دیوارهٔ آتش**، در ساده‌ترین شکل خود، صرفاً یک کامپیوتر است که بسته–بیتهای TCP/IP را بر بنیاد نشانیهای آی‌پی و شمارهٔ پورت از صافی (فیلتر) می‌گذراند. اگر کسی بسته–بیتی را برای کامپیوتر شما بفرستد، یک دیوارهٔ آتش خوب، آن بسته– بیت را بررسی خواهد کرد، از مجموعه قواعد خود، برای بررسی این که آیا باید به این بسته–بیت اجازهٔ ورود بدهد یا نه، بهره می‌گیرد، و در صورت تأیید، آن را به طرف کامپیوتر شما هدایت می‌کند.

[6] Web server

## ناپیدایی

یک دیوارهٔ آتش شخصی معمولاً جلوی ورود داده‌های ناخواسته به کامپیوتر را می‌گیرد. دیوارهٔ آتش چگونه ناخواسته‌بودن داده‌ها را تعیین می‌کند؟ دیواره‌های آتش جدید از روش **فیلترگذاری بسته–بیت جامع**[7] برای تعیین داده‌های ناخواسته بهره می‌گیرند.

دیوارهٔ آتشی که «فیلترگذاری بسته–بیت جامع» را اجرا می‌کند، به بسته–بیتهای TCP/IP ارسالی از جانب کامپیوتر شما نگاه می‌کند و نشانی منبع آنها را به خاطر می‌سپارد. این بسته–بیتها را ردیابی می‌کند، و وقتی یک خدمات‌دهندهٔ وب، یک صفحه را برای شما می‌فرستد (که باز هم از طریق بسته–بیتهای TCP/IP حمل می‌شود)، دیوارهٔ آتش، درخواست اولیهٔ شما _ و آن نشانی منبع _ را به یاد می‌آورد و اجازهٔ ورود بسته–بیتها را می‌دهد. بدون روش فیلترگذاری جامع، دیوارهٔ آتش به طور پیش‌گزیده این بسته–بیتهای ورودی را رد می‌کند.

«فیلترگذاری بسته–بیت جامع»، رمز پنهان نگاه‌داشته‌شدن کامپیوتر شما در اینترنت است. در خارج از محیط شما، هیچ‌کس متوجه نخواهد شد که کامپیوتر شما به اینترنت وصل است، اما هر وقت اراده کنید، کامپیوترتان می‌تواند به طور مطمئن، اینترنت را دستیابی کند.

## درون‌مرز و برون‌مرز

بسیاری از دیواره‌های آتش، ترافیک داده‌ها را فقط در یک جهت فیلتر می‌کنند: ورود به مرز کامپیوتر شما. هرچند، گونهٔ جدیدی از دیواره‌های آتش سعی می‌کنند حضور **پایش‌افزار** (spyware) و ویروسهایی را که کامپیوتر شما را آلوده ساخته‌اند تشخیص بدهند و از حملهٔ آنها به سایر کامپیوترهای اینترنت جلوگیری کنند. این دیواره‌های آتش، همچنین ترافیک خروجی شما را زیر نظر می‌گیرند و فقط به برنامه‌هایی اجازهٔ دستیابی اینترنت را می‌دهند که شما برای آنها مجوز صادر کرده‌اید.

[7] stateful packet filtering

دیواره‌های آتش دوجهتی از لحاظ تئوری عالی هستند، اما در عمل آنها از دو عیب رنج می‌برند. اول این که شما مجبورید برای هر برنامهٔ کاربردی‌ای که بخواهد اینترنت را دستیابی کند، موافقت خود را اعلان کنید. این حالت می‌تواند خسته‌کننده شود و مستعد پذیرش خطا است.

دومین _ و شاید مهمترین عیب_ آن است که دیواره‌های آتش در عمل هیچ روشی برای تعیین مجازبودن یک برنامهٔ کاربردی در اختیار ندارند. اگر یک ویروس یا پایش‌افزار، کامپیوتر شما را آلوده کند، چنین خرابکاری می‌تواند نقاب یک برنامهٔ کاربردی مجاز را بر چهره بزند، و دیوارهٔ آتش را برای موافقت‌کردن با دستیابی اینترنت توسط آن برنامه فریب بدهد.

## پس دیواره‌های آتش چگونه برنامه‌های غیرمجاز را تشخیص می‌دهند؟

دیواره‌های آتش، ایمنی کامل کامپیوتر شما را در برابر انواع مسائل امنیتی فراهم نمی‌سازند. همچنان که پیشتر ذکر کردیم، دیوارهٔ آتش فقط داده‌هایی را کنترل می‌کند که از کامپیوتر خارج یا به آن داخل می‌شود. یک دیوارهٔ آتش به تنهایی نمی‌تواند با ویروسها، پایش‌افزار، و سایر خرابکارهای داده‌ای مقابله کند. (از همین‌روست که ما برنامه‌های کاربردی ضدویروس و ضدپایش‌افزار را نیز در کامپیوتر خود نصب

می‌کنیم). با وجود این، دیواره‌های آتش، کامپیوتر شما را در برابر نفوذیهایی در اینترنت محافظت می‌کنند که به آسانی می‌توانند یک کامپیوتر ویندوز بی‌پناه را به گروگان بگیرند، زیرا اکثر کامپیوترهای ویندوز دارای چندین پورت باز هستند که یک نفوذی خرابکار می‌تواند از آنها برای حمله به سیستم شما و ربودن کنترل سیستم شما بهره بگیرد.

## مکان یک دیوارهٔ آتش

تکلیف اول در برپاسازی یک دیوارهٔ آتش، مشخص‌کردن جای استقرار آن است. اگر فقط یک کامپیوتر داشته باشید، حفاظت از خود با یک دیوارهٔ آتش، بسیار آسانتر از زمانی است که یک شبکه از کامپیوترها را دارید. در حالت یک‌کامپیوتری، هم می‌توانید از یک **دیوارهٔ آتش نرم‌افزاری** بهره بگیرید که بر روی کامپیوتر شما اجرا می‌شود، هم می‌توانید از یک **دستگاه دیوارهٔ آتش** استفاده کنید که بین کامپیوتر شما و اینترنت قرار می‌گیرد.

دیواره‌های آتش نرم‌افزاری، مانند برنامهٔ ZoneAlarm[8] و برنامهٔ Windows Firewall متعلق به ویندوز اکس‌پی برای اکثر کاربران کامپیوتر در حفاظت از تنها کامپیوترشان کافی هستند.

اگر یک شبکهٔ خانگی دارید و می‌خواهید از همهٔ کامپیوترهای خود محافظت کنید، به دیوارهٔ آتشی نیاز خواهید داشت که برای همهٔ کامپیوترهای شما به عنوان یک **دروازه** (gateway) عمل می‌کند. این دیوارهٔ آتش می‌تواند یک **روتر**[9] DSL[10] مجهز به بخش دیوارهٔ آتش باشد، یا می‌تواند یک دستگاه اختصاصی دیوارهٔ آتش باشد.

یک گزینهٔ دیگر برای کاربران ویندوز اکس‌پی وجود دارد. این سیستم‌عامل، برنامه‌ای به نام ICS[11] دارد که به یک کامپیوتر امکان می‌دهد که برای گروهی از کامپیوترهای یک شبکه، به عنوان یک دیوارهٔ آتش عمل کند. کامپیوترهای دیگر شبکه، تمام ترافیک اینترنت خود را از مسیر این کامپیوتر انجام می‌دهند، و این کامپیوتر نیز به نوبهٔ خود جلوی نفوذیها را می‌گیرد.

ما این مدل را به چند دلیل توصیه نمی‌کنیم. اول این که ICS نمی‌تواند آن مقدار حفاظتی را که یک دستگاه دیوارهٔ آتش مجزا می‌تواند تأمین کند فراهم سازد. همچنین، استفاده از ICS، کارایی کامپیوتری را که به عنوان دیوارهٔ آتش عمل می‌کند، بسته به مقدار ترافیکی که بخواهید در آن فیلتر کنید، کاهش می‌دهد.

سناریوی بهینه برای اکثر شبکه‌ها، استفاده از یک دستگاه دیوارهٔ آتش است که بین محل اتصال اینترنت شما و کامپیوترهای شما می‌نشیند. هر کامپیوتر از طریق یک **هاب** (hub) یا **سوئیچ** به شبکه، ودر نتیجه به دروازه وصل می‌شود. این کامپیوترها برای استفاده از دستگاه دیوارهٔ آتش به عنوان **دروازهٔ پیش‌گزیده** باید پیکربندی شوند. همچنین می‌توانید از یک دیوارهٔ آتش نرم‌افزاری به عنوان یک لایهٔ محافظتی اضافی در کنار دستگاه دیوارهٔ آتش بهره بگیرید.

## پیکربندی دیوارهٔ آتش ویندوز اکس‌پی

اگر از ویندوز اکس‌پی استفاده می‌کنید و سیستم خود را با Service Pack 2 ارتقا داده‌اید، یک دیوارهٔ آتش از پیش پیکربندی‌شده بر روی کامپیوتر خود در اختیار دارید. مایکروسافت حتی در این نگارش ویندوز، برنامهٔ Windows Firewall را به طور پیش‌گزیده فعال کرده است.

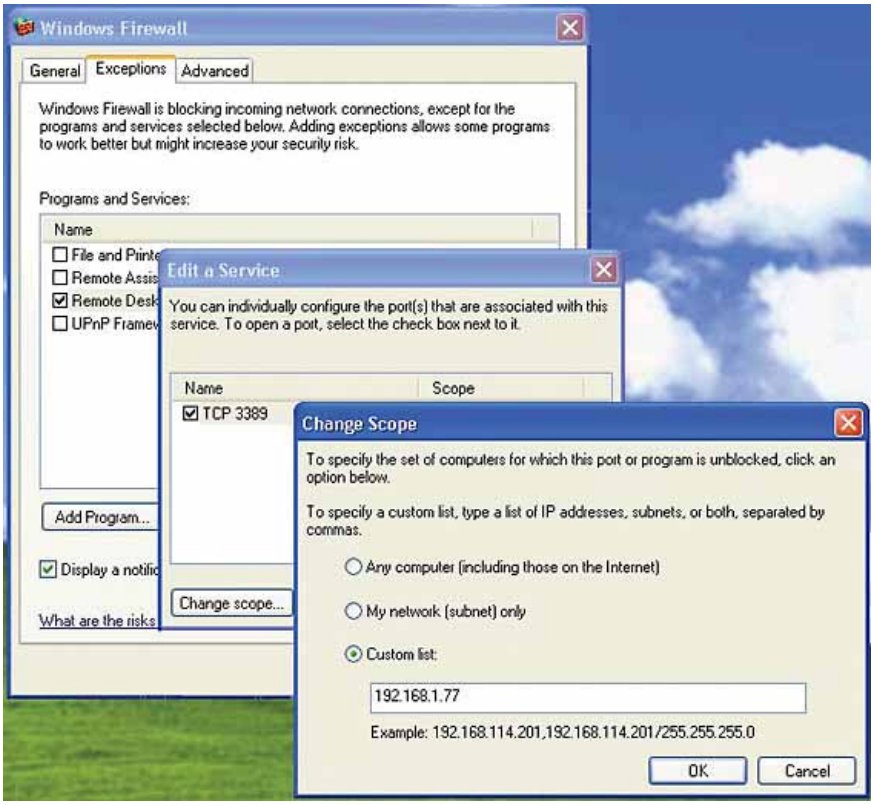
برنامهٔ Windows Firewall، یک دیوارهٔ آتش خوب برای اکثر کاربران است و جلوی تلاشهای نفوذیها را به آسانی می‌گیرد. اما همچون بسیاری از برنامه‌ها، چند ترفند ساده می‌تواند کارایی آن را بهتر کند.

ابتدا، برنامهٔ Windows Security Center را به اجرا درآورید. این برنامه، یک برنامهٔ مرکزی امنیت کامپیوتر است. روی Start، Control Panel، و Security Center کلیک کنید. اگر پیشتر، Windows Firewall را غیرفعال نکرده باشید، باید یک دکمهٔ سبز On در کنار نماد دیوارهٔ آتش ببینید.

سپس، روی Windows Firewall، تحت Manage Security Settings For کلیک کنید. این کار، صفحهٔ General از برنامهٔ Windows Firewall را باز خواهد کرد. تنظیم پیش‌گزیده برای Windows Firewall، تنظیم On (Recommended) و همچنین بدون‌تیک‌بودن گزینهٔ Don't Allow Exceptions است. (یک روش آسان برای فهمیدن **استثناها** [exception]، تصور آنها به عنوان پورتهای باز است. هر استثنایی که شما به وجود آورید یک پورت یا در را برای کامپیوتر شما باز می‌کند. به طور پیش‌گزیده، برنامهٔ Windows Firewall، چهار استثنای از پیش پیکربندی‌شده دارد، و یکی از این چهار استثنا فعال شده است: Remote Assistance. تا جایی که ممکن است، استثنا به وجود نیاورید.)

اگر به ساختن یک استثنا نیاز دارید، می‌توانید خطرات را کمتر کنید. به عنوان مثال، برنامهٔ Remote Desktop یک برنامهٔ

[8] http://www.zonelabs.com/
[9] router
[10] Digital Subscriber Line
[11] Internet Connection Sharing




**استثناسازی در برنامهٔ *Windows Firewall*، به شما امکان می‌دهد که کسانی را که می‌توانند یکی از سرویس‌های روی کامپیوتر شما را دستیابی کنند، کنترل کنید.**

مفید برای مدیریت یک کامپیوتر از راه دور است، اما حتماً نمی‌خواهید که کل اینترنت دست «یاری» به شما بدهند. برای محدودکردن کسانی که می‌توانند کامپیوتر شما را از طریق Remote Desktop دستیابی کنند، به صفحهٔ Exceptions بروید. Remote Desktop را انتخاب (های‌لایت) کنید، و روی دکمهٔ Edit کلیک کنید. این کار، پنجرهٔ Edit A Service را باز خواهد کرد.

سپس، روی Change Scope کلیک کنید. به طور پیش‌گزیده، هر کامپیوتری می‌تواند به کامپیوتر شما وصل شود. روی گزینهٔ Custom List کلیک کنید و **نشانی IP** کامپیوتری را وارد کنید که می‌خواهید اجازه بدهید به کامپیوتر شما وصل شود. روی OK کلیک کنید.

## آزمایش دیوارهٔ آتش

برپاسازی یک دیوارهٔ آتش، اولین گام است. حتماً برای اطمینان‌یافتن از این که دیوارهٔ آتش، کار خود را به طور احسن انجام می‌دهد، آن را تحت آزمایش قرار دهید. یکی از آسانترین روشها برای بررسی این که دیوارهٔ آتش کار می‌کند، سر زدن به پایگاه وب Shields Up! است:

**http://www.grc.com/**

Shields Up!، دیوارهٔ آتش شما را بررسی و منفذهای ورود نفوذیها را به شما گزارش می‌کند.

## آیا واقعاً به یک دیوارهٔ آتش نیاز دارم؟

بسیاری از مردم فکر می‌کنند که دیوارهٔ آتش یک مزاحم است. اگر اینترنت را مرور کنید، داستانهایی را از کسانی خواهید شنید که مدعی هستند که هرگز از دیوارهٔ آتش (و یا ضدویروس) بهره نگرفته‌اند و تا به حال اتفاقی برای آنها نیفتاده است.

از آن دست آدمها نباشید. به طور پیش‌گزیده، ویندوز برای اهداف شبکه‌سازی، بعضی از پورتها را باز نگه می‌دارد. وقتی کامپیوتر شما به اینترنت وصل است، به گونه‌ای خطرناک آسیب‌پذیر می‌شود، مگر این که معلومات فنی کافی برای بستن آن پورتها داشته باشید. آزمایشها نشان داده است که یک کامپیوتر محافظت‌نشده که ویندوز را اجرا می‌کند، وقتی به اینترنت وصل می‌شود، می‌تواند حدود ۱۰ دقیقه دوام بیاورد. پس از آن، این احتمال وجود دارد که مورد حمله قرار گرفته باشد، به گروگان درآمده باشد، و برای حمله به کامپیوترهای بدون محافظ دیگر به کار رفته باشد.

اجرای یک برنامهٔ دیوارهٔ آتش و استفاده از یک دستگاه دیوارهٔ آتش، ضرورت مطلق ندارد، اما حفاظت اضافی آنها به کسی صدمه نمی‌زند. و بی‌گمان، تصمیم به عدم استفاده از دیوارهٔ آتش یک تصمیم احمقانه است.

کاربران هوشمند می‌دانند که اینترنت می‌تواند یک مکان خصمانه باشد و این که زحمت پیاده‌سازی یک دیوارهٔ آتش _ اگرچه ممکن است دشوار باشد _ از زحمت پاک‌کردن کدهای زیان‌آوری که یک نفوذی بر جای گذاشته است، بسیار آسانتر است.

## نصب یک برنامهٔ دیوارهٔ آتش بازار

با آن که دیوارهٔ آتش گنجانده‌شده در

ویندوز اکس‌پی یک لایهٔ حفاظتی توانمند را به کامپیوتر شما اضافه می‌کند، همه از طرز کار آن رضایت ندارند. یک گزینهٔ عالی، برنامهٔ ZoneAlarm است که به رایگان از پایگاه وب Zone Labs می‌توانید دریافت کنید:

**http://www.zonelabs.com/**

برای نصب ZoneAlarm، برنامه را از اینترنت دریافت کنید و سپس روی فایل نصب آن کلیک–دوضرب کنید. روی Next کلیک کنید، دو مربعی را که به خبرنامهٔ Zone Labs مربوط هستند بدون تیک کنید، و دوباره روی Next کلیک کنید. با License Agreement موافقت کنید، و روی Install کلیک کنید. پس از چند لحظه، برنامهٔ نصب‌کننده کار خود را به پایان می‌رساند، و درخواست نمایش نتایج یک پژوهش را می‌دهد که می‌توانید از آن عبور کنید. روی Finish کلیک کنید، و وقتی پیام درخواست اجرای ZoneAlarm به نمایش درآمد، روی Yes برای اجرای ZoneAlarm کلیک کنید. روی Free ZoneAlarm در License Wizard کلیک کنید، سپس روی Next و Finish کلیک کنید.

مرحلهٔ بعدی، پیکربندی ZoneAlarm است. وقتی برنامهٔ Configuration Wizard به اجرا درآمد، روی Next کلیک کنید، و روی Yes تحت گزینهٔ زیر کلیک کنید:

Configure Internet Access To Allow Web Surfing

(فرض می‌کنیم که ترجیح می‌دهید وب را دستیابی کنید، البته!) روی Next کلیک کنید و سپس روی Done کلیک کنید. روی OK برای بازراه‌اندازی کامپیوتر کلیک کنید، و نصب ZoneAlarm کامل خواهد شد. وقتی کامپیوتر شما بازراه‌اندازی شود، ZoneAlarm فعال می‌شود، و پنجره‌ای را با آمارهای امنیتی مختلف به نمایش درمی‌آورد. می‌توانید این پنجره را ببندید، و در صورت لزوم، با کلیک‌کردن روی نماد ZoneAlarm در نوار پایین **میزکار** (Desktop) ویندوز (System Tray)، آن را باز کنید. به خاطر داشته باشید که می‌توانید با میزان‌کردن گزینه‌های دیوارهٔ آتش ZoneAlarm، به کامپیوترهای خاصی از شبکه اجازهٔ دستیابی سیستم خود را بدهید.

هرگاه برنامه‌های گوناگون تلاش کنند اینترنت را دستیابی کنند، ZoneAlarm هشدار خواهد داد. فراوانی این پیامهای هشدار پس از آن که سیستم «آموزش» ببیند که کدام برنامه‌ها اجازهٔ دسترسی دارند، کاهش خواهد یافت. □


**کتابهای انتشارات ریزپردازنده را می‌توانید مستقیماً از کیوسک مطبوعاتی فشمی (شعبه شماره ۲) تهیه فرمایید**

**نشانی: تهران، میدان انقلاب، ابتدای کارگرشمالی، روبروی سازمان انتقال خون**

**تلفن: ۶۶۹۲۳۷۷۷**

***برگزیده مقاله‌های ماهنامه ریزپردازنده در کتاب جدید انتشارات ریزپردازنده:***

**● همه چیز درباره اینترنت**

**□قیمت: ۲۰۰۰ تومان**

**□برای دریافت کتاب فوق مبلغ ذکرشده را به حساب جاری شماره ۲۹۱۷ بانک ملی ایران شعبه کسری (کدشعبه ۱۸۵) تهران به نام علیرضا محمدی‌فر (قابل پرداخت در کلیه شعب بانک ملی ایران) واریز کنید و اصل فیش را به همراه فرم زیر به نشانی مجله (تهران، صندوق‌پستی ۱۵۸۷۵/۶۵۹۱، مجله‌ریزپردازنده) ارسال نمایید.**

**□نام و نام خانوادگی:** **□ تلفن:**

**□نشانی:**