اگر مجاورت با آتش، تهدیدی برای جان شما محسوب می‌شود، لو رفتن آدرس IP و یکی از هزاران پورت TCP/UDP هم تهدیدی برای نفوذ به کامپیوترتان است.

نصب و تنظیم یک دیوارهٔ آتش

ترجمه: بابک احترامی

اشاره

امروزه، اتصال کامپیوتر «غیرمسلح» به اینترنت، مثل قفل نکردن در منزل است؛ هر آن ممکن است دزدی از راه برسد و هر چه دارید و ندارید را به یغما ببرد. چگونه می‌توان در مقابل این سارقین اطلاعات مقاومت کرد؟ با کشیدن دیواری از آتش که هر کسی نتواند از آن عبور کند. البته، معنای لغوی firewall آن‌چنان که در لغتنامه وبستر نوشته شده این است: دیواری که برای جلوگیری از پراکنده شدن آتش ساخته می‌شود، اما در زمینه کامپیوتر، دیواره آتش، سیستمی است که به صورت هم نرم‌افزاری و هم سخت‌افزاری در مدل‌های مختلف عرضه می‌شود تا مانع از نفوذ بیگانگان (از طریق اینترنت) به کامپیوتر شما بشود.

تنظیم و فهم طرز کار دیواره‌های آتش چندان آسان نیست و حتی کاربران مجرب هم در این رابطه گاهی با مشکل مواجه می‌شوند. شما برای شروع می‌توانید از دیواره‌های آتش نرم‌افزاری (که نسخه‌های رایگان آن‌ها نیز وجود دارند) استفاده کنید و بعدها به فکر نمونه سخت‌افزاری آن‌ها باشید. در این مقاله می‌خواهیم ضمن توضیح بعضی مفاهیم دیواره آتش، طریقه نصب و تنظیم آنها را مورد بررسی قرار دهیم.

اگر مجاورت با آتش، تهدیدی برای جان شما محسوب می‌شود، لو رفتن آدرس IP و یکی از هزاران پورت TCP/UDP هم تهدیدی برای نفوذ به کامپیوترتان است. نـــرم‌افزارهایی چون برنامه پست الکترونیک، مرورگر وب یا هر برنامه‌ای که برای گرفتن اطلاعات از اینترنت به کار می‌رود، عملاً داده‌ها را از طریق این پورت‌ها رد و بدل می‌کند. تهدیدی که اطلاعات کامپیوتر شما را به خطر می‌اندازد، چه از طرف نفوذگر بچه‌سالی باشد که قصد ورود به کامپیوترتان را دارد، و چه از طرف

شکل ۱- اگر هیچ چاره دیگری ندارید، حداقل دیواره آتش ویندوز اکس‌پی را فعال کنید.

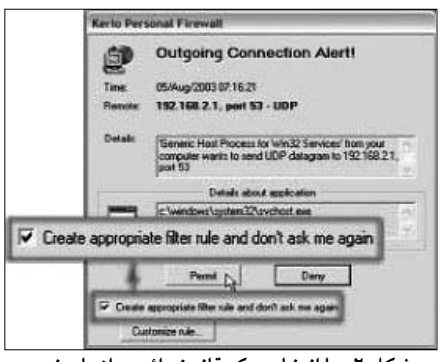
جاسوس‌افزاری باشد که می‌خواهد به یک سرور دور دسترسی پیدا کند، در یک صورت می‌تواند خطرآفرین باشد: یک پورت باز را پیدا کند که راه ورود به کامپیوترتان را نشان می‌دهد.

یکی از وظایف نرم‌افزارهای دیواره آتش این است که مراقب این پورت‌ها باشند و اجازه ندهند از طریق آن‌ها عبور و مرور غیرمجازی صورت گیرد. وظیفه دیگر آن‌ها، جلوگیری از خروج اطلاعات از طریق برنامه‌هایی چون Spywareها، Trojanها و نرم‌افزارهای موسوم به Backdoor است که در کامپیوتر شما در حال اجرا هستند. اگر نحوه اتصال شما به اینترنت صرفاً به صورت dial-up است، فایروال سخت‌افزاری به دردتان نمی‌خورد و در عوض دیوارهٔ آتش نرم‌افزاری برایتان مناسب‌تر خواهد بود. ویندوز اکس‌پی خودش یک دیوارهٔ آتش داخلی دارد که ممکن است تا به حال آن را امتحان کرده باشید. برای فعال کردن این دیوارهٔ آتش، از پنجره Network Connection در کنترل‌پانل، روی آیکون اتصال به اینترنت خود، کلیک راست کنید و از منوی ظاهر شده گزینه Properties را برگزینید. سپس به صفـــحه Advanced بـــروید و گـــزینه Protect my computer را علامت بزنید (شکل ۱).

البته توجه داشته باشید که دیوارهٔ آتش داخلی ویندوز اکس‌پی، اگر چه از نبودن هیچ دیواره آتشی در سیستم‌تان بهتر است، ولی چیز کاملی نیست. این فایروال، فقط ترافیک ورودی را کنترل می‌کند و کاری با این که برنامه‌های داخلی چرا دارند با بیرون ارتباط برقرار می‌کنند ندارد. بنابراین اگر یکی از برنامه‌های Backdoor از قبیل Back Orifice یا NetBus به کامپیوتر شما راه پیدا کرده باشد، اکس‌پی هیچ کاری نمی‌کند که این برنامه به بیرون دسترسی پیدا نکند.

انتخاب کنید

ما چهار نرم‌افزار رایگان فایروال را مورد



شکل ۲- با انتخاب یک قانون دائمی، از پاسخ به پرسش‌های مکرر دیوارهٔ آتش خلاص می‌شوید.

آزمایش قرار دادیم (برای آشنایی با آن‌ها، کادر «برای همه رایگان است» را مطالعه کنید). اگر چه این برنامه‌ها از نظر ظاهر و امکاناتی که به کاربر می‌دهند با هم فرق دارند، ولی همه آن‌ها با قدرت از کامپیوتر شما دفاع می‌کنند. نصب دیوارهٔ آتش نرم‌افزاری کاری ندارد، ولی مدتی را باید صرف آموزش آن بکنید تا با مرورگر، شبکه و برنامه‌هایی که می‌خواهند به بیرون وصل شوند آشنا بشود.

هر چهار نرم‌افزار فوق هنگامی که برای اولین بار متوجه می‌شوند برنامه‌ای می‌خواهد به بیرون دسترسی پیدا کند، پیـــام هشداری را به نمایش درمی‌آورند. در چنین مواقعی، کافی است با یک کلیک تعیین کنید برنامه اجازه این کار را دارد یا خیر. غالباً گزینه‌ای هم در اختیار شما گذاشته می‌شود که بتوانید اعلام کنید این اجازه یا عدم اجازه دائمی است یا موقتی (شکل ۲). بعد از مدتی که به این پرسش‌های دیواره آتش پاسخ دادید و روال فعالیت‌های اینترنتی خود را برای آن روشن کردید، دیواره آتش دیگر با شما کاری ندارد، مگر این که برنامه جدیدی را به سیستم خود اضافه کنید که بخواهد به اینترنت وصل شود.

شناخت برنامه‌ها و دانستن این که ارتباط کدام یک با بیرون بی‌خطر و کدام یک خطرآفرین است، در دادن پاسخ صحیح به سؤالات دیوارهٔ آتش و آموزش آن راه‌گشاست. خیلی از برنامه‌ها از روی اسمشان معلوم است که مطمئن هستند؛ مثلاً Internet Explorer یا Outlook Express. اما بعضی از برنامه‌ها نام آشنا و عادی ندارند؛ مثلاً بسیاری از خدمات شبکه‌ای ویندوز اکس‌پی توسط برنامه‌ای انجام می‌شوند به نام svchost.exe که برای خیلی از کاربران ناآشناست (گرچه حالا آشنا شد). بدتر از آن این که، بسیاری از جاسوس‌افزارها و برنامه‌های مخرب ممکن است از اسامی آشنا یا با مسمایی چون clever screensaver استفاده کنند، که باعث می‌شود به آنها اجازه دسترسی بدهید. به همین دلیل به کاربران مبتدی توصیه می‌شود سختگیر باشند و تا وقتی به طور کامل از یک برنامه، خاطرجمع نیستند، اجازه فعالیت به آن ندهند. بعداً راه‌هایی هست که بتوانید تصمیم‌تان را عوض کنید.

اگر معلومات شما به حدی نیست که بتوانید تصمیم بگیرید کدام بـــــرنامه مطمئن و کـــــدام غیرمطمئن است، از دیواره آتشی استفاده کنید که اطلاعات بیشتری صرفاً از اسم برنامه به شما می‌دهد. مثلاً Kerio و Sygate زیاد راهنمایی نمی‌کنند که برنامه مورد سؤال قـــابل اطمینان هست یا نه و به همین دلیل به درد مبتدی‌ها نمی‌خورند (گر چه حرفه‌ای‌ها اتفاقاً از این «کم حرفی» خیلی هم خوشحال می‌شوند).

ZoneAlarm اطلاعات نسبتاً بیشتری در مورد برنامه می‌دهد و لینکی را در اختیار کاربر می‌گذارد که با کلیک روی آن می‌تواند شرح حالی از برنامه را در سایت وب آزمایشگاه ZoneAlarm مشاهده کند. این فایروال به طور پیش‌فرض، به برنامه‌های Internet Explorer و svchost.exe ویندوز اکس‌پی اجازه کار می‌دهد تا بی‌خودی کاربر را با سؤالات زیادی خسته نکند.

دیوارهٔ آتش Outpost در پیـــام هشداری که به کاربر نشان می‌دهد، تصمیم وی را به طور پیش‌فرض «دائمی» تلقی می‌کند، ولی کاربر اگر بخواهد می‌تواند با کلیک روی دکمه‌های Allow once یا Block once اعلام کند که تصمیمش (اجازه یا ممنوعیت) فقط برای همین دفعه بوده است نه برای همیشه. گذشته از امکانات جانبی خوبی که در Outpost گنجانده شده (از قبیل مسدود کردن پنجره‌های تبلیغاتی یا محافظت در مقابل ضمیمهٔ نامه‌ها)، این برنامه هم مثل Kerio و Sygate، اطلاعات کمی در مورد برنامه به کاربر می‌دهد.

اصلاح تنظیمات

بعد از انجام تنظیـــمات اولیه و اســـاسی دیوارهٔ آتش و پاسخ به سؤالات هشدارآمیز، ممکن است بخواهید بعضی از مقررات و تصمیمات خود را حذف یا اصلاح کنید. تمام این چهار برنامه فهرستی را مورد استفاده قرار می‌دهند که (از طریق پاسخ‌هایی که خود شما داده‌اید) مشخص می‌کند کدام برنامه اجازه فعالیت اینترنتی دارد و کدام ندارد. شیوه اصلاح و تغییر این فهرست در هر برنامه متفاوت است.

● در Kerio، روی آیکون برنامه واقع در ناحیه موسوم به System Tray ویندوز کلیک راست کنید و از منوی ظاهر شده، گزینه‌های Administration، Firewall و Advanced را به ترتیب برگزینید. در فهرست برنامه‌های شناخته شده، برنامه‌ای را انتخاب کنید که قصد تغییر و دستکاری مقررات وضع شده برای آن را دارید. با کلیک روی دکمه Edit، کادر محاوره Filter rule باز می‌شود. برای تغییر قوانین مربوط به این برنامه، گزینه Permit یا Deny را در پایین کادر محاوره انتخاب کنید. سایر گزینه‌ها برای محدود کردن IP آدرس‌های سرور و پورت‌های ورودی و خروجی مورد استفاده قرار می‌گیرند. اگر از این گزینه‌ها سر در می‌آورید، پس اصلاً نیازی به خواندن این مقاله ندارید و خودتان بلدید چه کار باید بکنید، ولی اگر ناوارد هستید، همان حالت‌های پیش‌فرض را بپذیرید و روی OK کلیک کنید.

● در Outpost، با کلیک راست روی آیکون برنامه در ناحیه System Tray، گزینه‌های Options و سپس Application را انتخاب کنید. بعد از انتخاب برنامه مورد نظر از یکی از لیست‌های «مسدود شده»، «کاملاً مجاز» و «نسبتاً مجاز»، دکمه Edit را فشار دهید. حال یکی از گزینه‌های Always block this app یا Always trust this app را انتخاب کنید تا برنامه به گروه مربوطه منتقل شود. البته مطمئن‌ترین کار این است که برنامه‌ای که جزو گروه «کاملاً مجاز» است را انتخاب و به گروه «نسبتاً مجاز» منتقل کنید. با این کار، برنامه اجازه دسترسی به اینترنت را خواهد داشت اما تحت شرایط محدود و کنترل شده. مجموعه قوانین browser، برنامه را به یک سری قوانین ورودی و خروجی TCP یا UDP و پورت‌هایی محدود می‌کند که مورد نیاز یک مرورگر معمولی هستند. Outpost برای email، Instant Messaging و سایر برنامه‌ها هم قوانین محدودکننده مناسبی دارد.

● در Sygate، برای تغییر قوانین محدودکننده بـــرنامه‌ها، روی آیکون دیوارهٔ آتش در نـــاحیه System Tray کلیک راست کرده و گزینه Application را برگزینید. در فهرست برنامه‌های شناخته شده، با کلیک راست روی نام برنامه‌ای که قصد تغییر قوانین آن را دارید، یکی از گزینه‌های Allow یا Block را انتخاب کنید. انتخاب گزینه Ask بدین معنی است که از Sygate می‌خواهید قبل از هر اقدامی، از خود شما کسب تکلیف کند.

● در ZoneAlarm، بعد از کلیک راست روی آیکون برنـامه در نـاحیه System Tray، گزینه Restore ZoneAlram Control Center را انتخاب می‌کنید. سپس از سمت چپ، Program Control و بعد از آن، در سمت راست زبانه Programs را کلیک کنید. برای تغییر حالت برنامه، یکی از دکمه‌های علامت سؤال، علامت ضربدر یا علامت تیک را فشار داده و سپس عمل مورد نظر را انتخاب کنید.

برای همه رایگان است

با هیچ چیز به همه چیز برسید

Kerio Personal Firewall 2 - دیواره آتش کاملی که امکان اعمال قوانینی را برای دسترسی برنامه‌ها به آدرس‌های IP و پـــورت‌ها می‌دهد. حـــجم برنامه ۲ مگابایت است.

Outpost Firewall Free - این محصول رایگان شرکت Agnitum، قابلیت‌های فوق‌برنامه‌ای دارد همچون سد کردن نمایش پنجره‌های تبلیغاتی، فیلتر کردن سایت‌های وب از روی محتوا، فیلتر کردن ضمیمه نامه‌های الکترونیک، و یک DNS cache برای بیشتر کردن سرعت گشت‌زنی شما. حجم برنامه ۲/۵ مگابایت است.

Sygate Personal Firewall 5.1 - این برنامه بدون زرق و برق Sygate، کنترل کامل روی زمان و نحوهٔ ارتباط برنامه‌ها با سرور دور را به شما می‌دهد. اندازه برنامه ۵/۲ مگابایت است.

ZoneAlram 3.7.202 - دیواره آتشی مخصوص تازه‌کاران که با قابلیت اسکن email عرضه شده تا مانع از نفوذ ویروس‌های اسکریپتی از طریق ضمیمه نامه بشود. حجم برنامه ۳/۶ مگابایت است.