فایروال چیست؟

فایروال یک برنامه و یا دستگاه سخت افزاری است که با تمرکز بر روی شبکه و اتصال اینترنت ، تسهیلات لازم در جهت عدم دستیابی کاربران غیرمجاز به شبکه و یا کامپیوتر شما را ارائه می نماید. فایروال ها این اطمینان را ایجاد می نمایند که صرفا" پورت های ضروری برای کاربران و یا سایر برنامه های موجود در خارج از شبکه در دسترس و قابل استفاده می باشد. به منظور افزایش ایمنی ، سایر پورت ها غیرفعال می گردد تا امکان سوء استفاده از آنان توسط مهاجمان وجود نداشته باشد . در برخی موارد و با توجه به نیاز یک برنامه می توان موقتا" تعدادی از پورت ها را فعال و پس از اتمام کار مجددا" آنان را غیرفعال نمود . بخاطر داشته باشید که به موازات افزایش تعداد پورت های فعال ، امنیت کاهش پیدا می نماید .

فایروال های نرم افزاری ، برنامه هائی هستند که پس از اجراء ، تمامی ترافیک به درون کامپیوتر را کنترل می نمایند(برخی از فایروال ها علاوه بر کنترل ترافیک ورودی ، ترافیک خروجی را نیز کنترل می نمایند) . فایروال ارائه شده به همراه ویندوز XP ، نمونه ای در این زمینه است . فایروال های نرم افزاری توسط شرکت های متعددی تاکنون طراحی و پیاده سازی شده است . تعداد زیادی از اینگونه فایروال ها، صرفا" نظاره گر ترافیک بین شبکه داخلی و اینترنت بوده و ترافیک بین کامپیوترهای موجود در یک شبکه داخلی را کنترل نمی نمایند .

نحوه استفاده از فایروال ویندوز

امروزه از اینترنت در ابعاد گسترده و با اهدافی مختلف استفاده بعمل می آید . یکی از نکات قابل توجه اینترنت ، تنوع استفاده کنندگان آن در رده های سنی مختلف و مشاغل گوناگون است. در سالیان اخیر و به موازات رشد چشمگیر استفاده از اینترنت خصوصا" توسط کاربران خانگی ، مشاهده شده است به محض شیوع یک ویروس و یا کرم جدید ، اغلب قربانیان را کاربرانی تشکیل می دهند که فاقد مهارت های لازم در جهت استفاده ایمن از اینترنت بوده و دارای یک سطح حفاظتی مناسب نمی باشند . کاربران اینترنت همواره در تیررس مهاجمان بوده و همیشه امکان بروز حملات وجود خواهد داشت .

برای استفاده ایمن از اینترنت ، می بایست اقدامات متعددی را انجام داد . قطعا" استفاده از فایروال یکی از اقدامات اولیه و در عین حال بسیار مهم در این زمینه است . استفاده از اینترنت بدون بکارگیری یک فایروال ، نظیر بازنگهداشتن درب ورودی یک ساختمان است که هر لحظه ممکن است افراد غیرمجاز از فرصت ایجاد شده برای ورود به ساختمان استفاده نمایند . با نصب و استفاده از یک فایروال ، ضریب مقاومت و ایمنی کاربران در مقابل انواع حملات افزایش خواهد یافت .

شرکت مایکروسافت اخیرا" Service Pack 2 ویندوز XP را عرضه نموده است (نسخه های Professional و Home) . یکی از ویژگی های مهم SP2 ، نصب پیش فرض یک فایروال است.

فایروال ویندوز XP که از آن با نام (Internet Connection Firewall) ICF نیز یاد می گردد به صورت پیش فرض ، فعال می گردد. پس از فعال شدن فایروال ، شاهد بروز تغییراتی گسترده در رابطه با عملکرد ویندوز بوده و ممکن است برخی برنامه ها ، ابزارها و یا سرویس ها در زمان اجراء با مشکلاتی مواجه گردند (بلاک شدن برخی از پورت های استفاده شده توسط برنامه ها و یا سایر ابزارهای کاربردی) .

در این مطلب قصد داریم به بررسی نحوه استفاده از فایروال ویندوز XP پرداخته و به برخی از سوالات متداول در این زمینه پاسخ دهیم . احازه دهید قبل از هر چیز با فایروال ها و جایگاه آنان در استفاده ایمن از شبکه های کامپیوتری (اینترانت ، اینترنت) بیشتر آشنا شویم .

فایروال

فایروال وسیله ای است که کنترل دسترسی به یک شبکه را بنابر سیاست امنیتی شبکه تعریف می کند.علاوه بر آن از آنجایی که معمولا یک فایروال بر سر راه ورودی یک شبکه می نشیند لذا برای ترجمه آدرس شبکه نیز بکار گرفته می شود.

مشخصه های مهم یک فایروال

مشخصه های مهم یک فایروال قوی و مناسب جهت ایجاد یک شبکه امن عبارتند از:

1. توانایی ثبت و اخطار

ثبت وقایع یکی از مشخصه های بسیار مهم یک فایروال به شمار می شود و به مدیران شبکه این امکان را می دهد که انجام حملات را کنترل کنند. همچنین مدیر شبکه می تواند با کمک اطلاعات ثبت شده به کنترل ترافیک ایجاد شده توسط کاربران مجاز بپردازد. در یک روال ثبت مناسب ، مدیر می تواند براحتی به بخشهای مهم از اطلاعات ثبت شده دسترسی پیدا کند. همچنین یک فایروال خوب باید بتواند علاوه بر ثبت وقایع، در شرایط بحرانی، مدیر شبکه را از وقایع مطلع کند و برای وی اخطار بفرستد.

2. بازدید حجم بالایی از بسته های اطلاعات

یکی از تستهای یک فایروال ، توانایی آن در بازدید حجم بالایی از بسته های اطلاعاتی بدون کاهش چشمگیر کارایی شبکه است. حجم داده ای که یک فایروال می تواند کنترل کند برای شبکه های مختلف متفاوت است اما یک فایروال قطعا نباید به گلوگاه شبکه تحت حفاظتش تبدیل شود.عوامل مختلفی در سرعت پردازش اطلاعات توسط فایروال نقش دارند. بیشترین محدودیتها از طرف سرعت پردازنده و بهینه سازی کد نرم افزار بر کارایی فایروال تحمیل می شوند. عامل محدودکننده دیگر می تواند کارتهای واسطی باشد که بر روی فایروال نصب می شوند. فایروالی که بعضی کارها مانند صدور اخطار ، کنترل دسترسی مبنی بر URL و بررسی وقایع ثبت شده را به نرم افزارهای دیگر می سپارد از سرعت و کارایی بیشتر و بهتری برخوردار است.

3. سادگی پیکربندی

سادگی پیکربندی شامل امکان راه اندازی سریع فایروال و مشاهده سریع خطاها و مشکلات است.در واقع بسیاری از مشکلات امنیتی که دامنگیر شبکه های می شود به پیکربندی غلط فایروال بر می گردد. لذا پیکربندی سریع و ساده یک فایروال ، امکان بروز خطا را کم می کند. برای مثال امکان نمایش گرافیکی معماری شبکه و یا ابزرای که بتواند سیاستهای امنیتی را به پیکربندی ترجمه کند ، برای یک فایروال بسیار مهم است.

4. امنیت و افزونگی فایروال

امنیت فایروال خود یکی از نکات مهم در یک شبکه امن است.فایروالی که نتواند امنیت خود را تامین کند ، قطعا اجازه ورود هکرها و مهاجمان را به سایر بخشهای شبکه نیز خواهد داد. امنیت در دو بخش از فایروال ، تامین کننده امنیت فایروال و شبکه است:

الف- امنیت سیستم عامل فایروال : اگر نرم افزار فایروال بر روی سیستم عامل جداگانه ای کار می کند، نقاط ضعف امنیتی سیستم عامل ، می تواند نقاط ضعف فایروال نیز به حساب بیاید. بنابراین امنیت و استحکام سیستم عامل فایروال و بروزرسانی آن از نکات مهم در امنیت فایروال است.

ب- دسترسی امن به فایروال جهت مقاصد مدیریتی : یک فایروال باید مکانیزمهای امنیتی خاصی را برای دسترسی مدیران شبکه در نظر بگیرد. این روشها می تواند رمزنگاری را همراه با روشهای مناسب تعیین هویت بکار گیرد تا بتواند در مقابل نفوذگران تاب بیاورد.

انواع فایروال

انواع مختلف فایروال کم و بیش کارهایی را که اشاره کردیم ، انجام می دهند، اما روش انجام کار توسط انواع مختلف ، متفاوت است که این امر منجر به تفاوت در کارایی و سطح امنیت پیشنهادی فایروال می شود.بر این اساس فایروالها را به 5 گروه تقسیم می کنند.

1. فایروالهای سطح مدار (Circuit-Level)

این فایروالها به عنوان یک رله برای ارتباطات TCP عمل می کنند. آنها ارتباط TCP را با رایانه پشتشان قطع می کنند و خود به جای آن رایانه به پاسخگویی اولیه می پردازند.تنها پس از برقراری ارتباط است که اجازه می دهند تا داده به سمت رایانه مقصد جریان پیدا کند و تنها به بسته های داده ای مرتبط اجازه عبور می دهند. این نوع از فایروالها هیچ داده درون بسته های اطلاعات را مورد بررسی قرار نمی دهند و لذا سرعت خوبی دارند. ضمنا امکان ایجاد محدودیت بر روی سایر پروتکلها (غیر از TCP) را نیز نمی دهند.

2. فایروالهای پروکسی سرور

فایروالهای پروکسی سرور به بررسی بسته های اطلاعات در لایه کاربرد می پردازد. یک پروکسی سرور درخواست ارائه شده توسط برنامه های کاربردی پشتش را قطع می کند و خود به جای آنها درخواست را ارسال می کند.نتیجه درخواست را نیز ابتدا خود دریافت و سپس برای برنامه های کاربردی ارسال می کند. این روش با جلوگیری از ارتباط مستقیم برنامه با سرورها و برنامه های کاربردی خارجی امنیت بالایی را تامین می کند. از آنجایی که این فایروالها پروتکلهای سطح کاربرد را می شناسند ، لذا می توانند بر مبنای این پروتکلها محدودیتهایی را ایجاد کنند. همچنین آنها می توانند با بررسی محتوای بسته های داده ای به ایجاد محدودیتهای لازم بپردازند. البته این سطح بررسی می تواند به کندی این فایروالها بیانجامد. همچنین از آنجایی که این فایروالها باید ترافیک ورودی و اطلاعات برنامه های کاربردی کاربر انتهایی را پردازش کند، کارایی آنها بیشتر کاهش می یابد. اغلب اوقات پروکسی سرورها از دید کاربر انتهایی شفاف نیستند و کاربر مجبور است تغییراتی را در برنامه خود ایجاد کند تا بتوان داین فایروالها را به کار بگیرد.هر برنامه جدیدی که بخواهد از این نوع فایروال عبور کند ، باید تغییراتی را در پشته پروتکل فایروال ایجاد کرد.

3. فیلترهای Nosstateful packet

این فیلترها روش کار ساده ای دارند. آنها بر مسیر یک شبکه می نشینند و با استفاده از مجموعه ای از قواعد ، به بعضی بسته ها اجازه عبور می دهند و بعضی دیگر را بلوکه می کنند. این تصمیمها با توجه به اطلاعات آدرس دهی موجود در پروتکلهای لایه شبکه مانند IP و در بعضی موارد با توجه به اطلاعات موجود در پروتکلهای لایه انتقال مانند سرآیندهای TCP و UDP اتخاذ می شود. این فیلترها زمانی می توانند به خوبی عمل کنند که فهم خوبی از کاربرد سرویسهای مورد نیاز شبکه جهت محافظت داشته باشند. همچنین این فیلترها می توانند سریع باشند چون همانند پروکسی ها عمل نمی کنند و اطلاعاتی درباره پروتکلهای لایه کاربرد ندارند.

4. فیلترهای Stateful Packet

این فیلترها بسیار باهوشتر از فیلترهای ساده هستند. آنها تقریبا تمامی ترافیک ورودی را بلوکه می کنند اما می توانند به ماشینهای پشتشان اجازه بدهند تا به پاسخگویی بپردازند. آنها این کار را با نگهداری رکورد اتصالاتی که ماشینهای پشتشان در لایه انتقال ایجاد می کنند، انجام می دهند.این فیلترها ، مکانیزم اصلی مورد استفاده جهت پیاده سازی فایروال در شبکه های مدرن هستند.این فیلترها می توانند رد پای اطلاعات مختلف را از طریق بسته هایی که در حال عبورند ثبت کنند. برای مثال شماره پورت های TCP و UDP مبدا و مقصد، شماره ترتیب TCP و پرچمهای TCP. بسیاری از فیلترهای جدید Stateful می توانند پروتکلهای لایه کاربرد مانند FTP و HTTP را تشخیص دهند و لذا می توانندعمال کنترل دسترسی را با توجه به نیازها و سرعت این پروتکلها انجام دهند.

5. فایروالهای شخصی

فایروالهای شخصی ، فایروالهایی هستند که بر روی رایانه های شخصی نصب می شوند.آنها برای مقابله با حملات شبکه ای طراحی شده اند. معمولا از برنامه های در حال اجرا در ماشین آگاهی دارند و تنها به ارتباطات ایجاد شده توسط این برنامه ها اجازه می دهند که به کار بپردازند نصب یک فایروال شخصی بر روی یک PC بسیار مفید است زیرا سطح امنیت پیشنهادی توسط فایروال شبکه را افزایش می دهد. از طرف دیگر از آنجایی که امروزه بسیاری از حملات از درون شبکه حفاظت شده انجام می شوند ، فایروال شبکه نمی تواند کاری برای آنها انجام دهد و لذا یک فایروال شخصی بسیار مفید خواهد بود. معمولا نیازی به تغییر برنامه جهت عبور از فایروال شخصی نصب شده (همانند پروکسی) نیست.

موقعیت یابی برای فایروال

محل و موقعیت نصب فایروال همانند انتخاب نوع صحیح فایروال و پیکربندی کامل آن ، از اهمیت ویژه ای برخوردار است. نکاتی که باید برای یافتن جای مناسب نصب فایروال در نظر گرفت عبارتند از :

موقعیت و محل نصب از لحاظ توپولوژیکی

معمولا مناسب به نظر می رسد که فایروال را در درگاه ورودی/خروجی شبکه خصوصی نصب کنیم. این امر به ایجاد بهترین پوشش امنیتی برای شبکه خصوصی با کمک فایروال از یک طرف و جداسازی شبکه خصوصی از شبکه عمومی از طرف دیگر کمک می کند.

قابلیت دسترسی و نواحی امنیتی

اگر سرورهایی وجود دارند که باید برای شبکه عمومی در دسترس باشند ، بهتر است آنها را بعد از فایروال و در ناحیه DMZ قرار دهید. قرار دادن این سرورها در شبکه خصوصی وتنظیم فایروال جهت صدور اجازه به کاربران خارجی برای دسترسی به این سرورها برابر خواهد بود با هک شدن شبکه داخلی. چون شما خود مسیر هکرها را در فایروال باز کرده اید. در حالی که با استفاده از ناحیه DMZ ، سرورهای قابل دسترسی برای شبکه عمومی از شبکه خصوصی شما بطور فیزیکی جدا هستند، لذا اگر هکرها بتوانند به نحوی به این سرورها نفوذ کنند بازهم فایروال را پیش روی خود دارند.

مسیریابی نامتقارن

بیشتر فایروالهای مدرن سعی می کنند اطلاعات مربوط به اتصالات مختلفی را که از طریق آنها شبکه داخلی را به شبکه عمومی وصل کرده است، نگهداری کنند. این اطلاعات کمک می کنند تا تنها بسته های اطلاعاتی مجاز به شبکه خصوصی وارد شوند. در نتیجه حائز اهمیت است که نقطه ورود و خروج تمامی اطلاعات به/از شبکه خصوصی از طریق یک فایروال باشد.

فایروال‌های لایه‌ای

در شبکه های با درجه امنیتی بالا بهتر است از دو یا چند فایروال در مسیر قرار گیرند. اگر اولی با مشکلی روبرو شود، دومی به کار ادامه می دهد.معمولا بهتر است دو یا چند فایروال مورد استفاده از شرکتهای مختلفی باشند تا در صورت وجود یک اشکال نرم افزاری یا حفره امنیتی در یکی از آنها ، سایرین بتوانند امنیت شبکه را تامین کنند.

فایروال چه کار می کند ؟

فایروال ها حفاظت لازم در مقابل مهاجمان خارجی را ایجاد و یک لایه و یا پوسته حفاظتی پیرامون کامپیوتر و یا شبکه را در مقابل کدهای مخرب و یا ترافیک غیرضروری اینترنت ، ارائه می نمایند . با بکارگیری فایروال ها ، امکان بلاک نمودن داده از مکانی خاص فراهم می گردد . امکانات ارائه شده توسط یک فایروال برای کاربرانی که همواره به اینترنت متصل و از امکاناتی نظیر DSL و یا مودم های کابلی استفاده می نمایند ، بسیار حیاتی و مهم می باشد.

چه نوع فایروال هائی وجود دارد ؟

فایروال ها به دو شکل سخت افزاری (خارجی) و نرم افزاری (داخلی) ، ارائه می شوند . با اینکه هر یک از مدل های فوق دارای مزایا و معایب خاص خود می باشند ، تصمیم در خصوص استفاده از یک فایروال بمراتب مهمتر از تصمیم در خصوص نوع فایروال است .

- فایروال های سخت افزاری:

این نوع از فایروال ها که به آنان فایروال های شبکه نیز گفته می شود ، بین کامپیوتر شما (و یا شبکه) و کابل و یا خط DSL قرار خواهند گرفت . تعداد زیادی از تولید کنندگان و برخی از مراکز ISP دستگاههائی با نام "روتر" را ارائه می دهند که دارای یک

فایروال نیز می باشند . فایروال های سخت افزاری در مواردی نظیر حفاظت چندین کامپیوتر مفید بوده و یک سطح مناسب حفاظتی را ارائه می نمایند(امکان استفاده از آنان به منظور حفاظت یک دستگاه کامپیوتر نیز وجود خواهد داشت) . در صورتی که شما صرفا" دارای یک کامپیوتر پشت فایروال می باشید و یا این اطمینان را دارید که سایر کامپیوتر های موجود بر روی شبکه نسبت به نصب تمامی patch ها ، بهنگام بوده و عاری از ویروس ها و یا کرم ها می باشند ، ضرورتی به استفاده از یک سطح اضافه حفاظتی (یک نرم افزار فایروال) نخواهید داشت . فایروال های سخت افزاری ، دستگاههای سخت افزاری مجزائی می باشند که دارای سیستم عامل اختصاصی خود می باشد . بنابراین بکارگیری آنان باعث ایجاد یک لایه دفاعی اضافه در مقابل تهاجمات می گردد .

- فایروال های نرم افزاری :

برخی از سیستم های عامل دارای یک فایروال تعبیه شده درون خود می باشند . در صورتی که سیستم عامل نصب شده بر روی کامپیوتر شما دارای ویژگی فوق می باشد ، پیشنهاد می گردد که آن را فعال نموده تا یک سطح حفاظتی اضافی در خصوص ایمن سازی کامپیوتر و اطلاعات ، ایجاد گردد .(حتی اگر از یک فایروال خارجی یا سخت افزاری استفاده می نمائید). در صورتی که سیستم عامل نصب شده بر روی کامپیوتر شما دارای یک فایروال تعبیه شده نمی باشد ، می توان اقدام به تهیه یک فایروال نرم افزاری کرد . با توجه به عدم اطمینان لازم در خصوص دریافت نرم افزار از اینترنت با استفاده از یک کامپیوتر محافظت نشده ، پیشنهاد می گردد برای نصب فایروال از CD و یا DVD مربوطه استفاده گردد .

نحوه پیکربندی بهینه یک فایروال به چه صورت است ؟

اکثر محصولات فایروال تجاری (هم سخت افزاری و هم نرم افزاری) دارای امکانات متعددی بمنظور پیکربندی بهینه می باشند . با توجه به تنوع بسیار زیاد فایروال ها ، می بایست به منظور پیکربندی بهینه آنان به مستندات ارائه شده ، مراجعه تا مشخص گردد که آیا تنظیمات پیش فرض فایروال نیاز شما را تامین می نماید یا خیر ؟ . پس از پیکربندی یک فایروال یک سطح امنیتی و حفاظتی مناسب در خصوص ایمن سازی اطلاعات انجام شده است . لازم است به این موضوع مهم اشاره گردد که پس از پیکربندی یک فایروال نمی بایست بر این باور باشیم که سیستم ما همواره ایمن خواهد بود . فایروال ها یک سطح مطلوب حفاظتی را ارائه می نمایند ولی هرگز عدم تهاجم به سیستم شما را تضمین نخواهند کرد . استفاده از فایروال به همراه سایر امکانات حفاظتی نظیر نرم افزارهای آنتی ویروس و رعایت توصیه های ایمنی می تواند یک سطح مطلوب حفاظتی را برای شما و شبکه شما بدنبال داشته باشد .

ضرورت استفاده از فایروال

یک سیستم بدون وجود یک فایروال ، در مقابل مجموعه ای گسترده از برنامه های مخرب آسیب پذیر است و در برخی موارد صرفا" پس از گذشت چندین دقیقه از اتصال به اینترنت ، آلوده خواهد شد . در صورتی که تدابیر و مراقبت لازم در خصوص حفاظت از سیستم انجام نگردد ، ممکن است کامپیوتر شما توسط برنامه هائی که به صورت تصادفی آدرس های اینترنت را پویش می نمایند ، شناسائی شده و با استفاده از پورت های فعال اقدام به تخریب و یا سوء استفاده از اطلاعات گردد .

بخاطر داشته باشید با این که استفاده از فایروال ها به عنوان یک عنصر حیاتی در ایمن سازی محیط های عملیاتی مطرح می باشند ولی تمامی داستان ایمن سازی به این عنصر ختم نمی شود و می بایست از سایر امکانات و یا سیاست های امنیتی خاصی نیز تبعیت گردد . باز نکردن فایل های ضمیمه همراه یک Email قبل از حصول اطمینان از سالم بودن آنان ، پیشگیری از برنامه های جاسوسی معروف به Spyware و یا نصب برنامه های Plug-ins که با طرح یک پرسش از شما مجوز نصب را دریافت خواهند داشت ، نمونه هائی از سایر اقدامات لازم در این زمینه است .

فایروال ها قادر به غیرفعال نمودن ویروس ها و کرم های موجود بر روی سیستم نبوده و همچنین نمی توانند نامه های الکترونیکی مخرب به همراه ضمائم آلوده را شناسائی و بلاک نمایند . به منظور افزایش ضریب ایمنی و مقاومت در مقابل انواع حملات ، می بایست اقدامات متعدد دیگری صورت پذیرد :

نصب و بهنگام نگهداشتن یک برنامه آنتی ویروس

استفاده از ویندوز Upadate (برطرف نمودن نقاط آسیب پذیر ویندوز و سرویس های مربوطه)

استفاده از برنامه های تشخیص Spyware

نصب Plug-ins از سایت های تائید شده

نحوه فعال نمودن فایروال در ویندوز XP

در صورت نصب SP2 ویندوز XP ، فایروال به صورت پیش فرض فعال می گردد . برخی از مدیران شبکه و یا افرادی که اقدام به نصب نرم افزار می نمایند ، ممکن است آن را غیرفعال کرده باشند .

برای آگاهی از وضعیت فایروال از پنجره Security Center استفاده می شود . بدین منظور مراحل زیر را دنبال می نمائیم :

Start | Control Panel | Security Center

انتخاب گزینه Recommendations در صورت غیرفعال بودن فایروال

انتخاب گزینه Enable Now به منظور فعال نمودن فایروال

در صورتی که ویندوز XP بر روی سیستم نصب شده است ولی SP2 هنوز نصب نشده باشد ، پیشنهاد می گردد که در اولین فرصت نسبت به نصب SP2 ویندوز XP ، اقدام شود (استفاده از امکانات گسترده امنیتی و فایروال ارائه شده) .

نسخه های قبلی ویندوز نظیر ویندوز 2000 و یا 98 به همراه یک فایروال از قبل تعبیه شده ارائه نشده اند . در صورت استفاده از

سیستم های عامل فوق، می بایست یک فایروال نرم افزاری دیگر را انتخاب و آن را بر روی سیستم نصب نمود .
ضرورت توجه به امکانات سایر فایروال های نرم افزاری
فایروال ویندوز ، امکانات حفاظتی لازم به منظور بلاک نمودن دستیابی غیرمجاز به سیستم شما را ارائه می نماید . در این رابطه دستیابی به سیستم از طریق کاربران و یا برنامه های موجود در خارج از شبکه محلی ، کنترل خواهد شد . برخی از فایروال های نرم افزاری یک لایه حفاظتی اضافه را نیز ارائه داده و امکان ارسال اطلاعات و یا داده توسط کامپیوتر شما به سایر کامپیوترهای موجود در شبکه توسط برنامه های غیر مجاز را نیز بلاک می نمایند (سازماندهی و مدیریت یک فایروال دوطرفه) . با استفاده از این نوع فایروال ها ، برنامه ها قادر به ارسال داده از کامپیوتر شما برای سایر کامپیوترها بدون اخذ مجوز نخواهند بود . در صورت نصب یک برنامه مخرب بر روی کامپیوتر شما (سهوا" و یا تعمدا") برنامه فوق می تواند در ادامه اطلاعات شخصی شما را برای سایر کامپیوترها ارسال و یا آنان را سرقت نماید . پس از نصب فایروال های دوطرفه ، علاوه بر تمرکز بر روی پورت های ورودی (Incoming) ، پورت های خروجی (Outgoing) نیز کنترل خواهند شد.
آیا می توان بیش از یک فایروال نرم افزاری را بر روی یک سیستم نصب نمود ؟
پاسخ به سوال فوق مثبت است ولی ضرورتی به انجام این کار نخواهد بود. فایروال ویندوز بگونه ای طراحی شده است که می تواند با سایر فایروال های نرم افزارهای همزیستی مسالمت آمیزی را داشته باشد ولی مزیت خاصی در خصوص اجرای چندین فایروال نرم افزاری بر روی یک کامپیوتر وجود ندارد . در صورت استفاده از یک فایروال نرم افزاری دیگر ، می توان فایروال ویندوز XP را غیر فعال نمود .
در صورتی که بر روی شبکه از یک فایروال استفاده می گردد ، آیا ضرورتی به استفاده از فایروال ویندوز وجود دارد ؟
در صورت وجود بیش از یک کامپیوتر در شبکه ، پیشنهاد می گردد که حتی در صورتی که از یک فایروال سخت افزاری استفاده می شود ، از فایروال ویندوز XP نیز استفاده بعمل آید . فایروال های سخت افزاری عموما" ترافیک بین شبکه و اینترنت را کنترل نموده و نظارت خاصی بر روی ترافیک بین کامپیوترهای موجود در شبکه را انجام نخواهند داد . در صورت وجود یک برنامه مخرب بر روی یکی از کامپیوترهای موجود در شبکه ، شرایط و یا پتانسیل لازم برای گسترش و آلودگی سایر کامپیوترها فراهم می گردد. فایروال ویندوز XP علاوه بر حفاظت کامپیوتر شما در خصوص دستیابی غیرمجاز از طریق اینترنت ، نظارت و کنترل لازم در رابطه با دستیابی غیرمجاز توسط کامپیوترهای موجود در یک شبکه داخلی را نیز انجام خواهد داد .

فایروال بر روی چه برنامه هائی تاثیر می گذارد ؟

فایروال ویندوز با هر برنامه ای که تصمیم به ارسال داده برای سایر کامپیوترهای موجود در شبکه داخلی و یا اینترنت را داشته باشد ، تعامل خواهد داشت . پس از نصب فایروال ، صرفا" پورت های مورد نیاز برنامه های متداول مبادله اطلاعات نظیر Email و استفاده از وب، فعال می گردند . در این راستا و به منظور حفاظت کاربران ، امکان استفاده از برخی برنامه ها بلاک می گردد . سرویس FTP (سرویس ارسال و یا دریافت فایل) ، بازی های چند نفره ، تنظیم از راه دور Desktop و ویژگی های پیشرفته ای نظیر کنفرانس های ویدئویی و ارسال فایل از طریق برنامه های (Instant Messaging) IM ، از جمله برنامه هائی می باشند که فعالیت آنان توسط فایروال بلاک می گردد . در صورت ضرورت می توان پیکربندی فایروال را بگونه ای انجام داد که پورت های مورد نیاز یک برنامه فعال تا امکان مبادله اطلاعات برای برنامه متقاضی فراهم گردد .
چگونه می توان فایروال را برای یک برنامه خاص فعال نمود ؟
در صورتی که فایروال ویندوز فعال شده باشد ، اولین مرتبه ای که یک برنامه درخواست اطلاعات از سایر کامپیوترهای موجود در شبکه (داخلی و یا اینترنت) را می نماید ، یک جعبه محاوره ای حاوی یک پیام هشداردهنده امنیتی فعال و از شما سوال خواهد شد که آیا به برنامه متقاضی اجازه مبادله اطلاعات با سایر برنامه ها و یا کامپیوترهای موجود در شبکه داده می شود و یا دستیابی وی بلاک می گردد . در این جعبه محاوره ای پس از نمایش نام برنامه متقاضی با ارائه سه گزینه متفاوت از شما در رابطه با ادامه کار تعیین تکلیف می گردد :
Keep Blocking : با انتخاب این گزینه به برنامه متقاضی اجازه دریافت اطلاعات داده نخواهد شد .
Unblock : پس از انتخاب این گزینه پورت و یا پورت های مورد نیاز برنامه متقاضی فعال و امکان ارتباط با کامپیوتر مورد نظر فراهم می گردد . بدیهی است صدور مجوز برای باز نمودن پورت های مورد نیاز یک برنامه به شناخت مناسب نسبت به برنامه و نوع عملیات آن بستگی خواهد داشت . در صورتی که از طریق نام برنامه نمی توان با نوع فعالیت آن آشنا گردید ، می توان از مراکز جستجو برای آشنائی با عملکرد برنامه متقاضی ، استفاده نمود .
Ask Me Later : با انتخاب گزینه فوق در مقطع فعلی تصمیم به بلاک نمودن درخواست برنامه متقاضی می گردد.در صورت اجرای برنامه ، سوال فوق مجددا" مطرح خواهد شد .
در صورتی که یک برنامه بلاک شده است ولی بدلایلی تصمیم به فعال نمودن و ایجاد شرایط لازم ارتباطی برای آن را داشته باشیم ، می توان به صورت دستی آن را به لیست موسوم به Exception اضافه نمود .

لیست فوق حاوی نام برنامه هائی است که به آنان مجوز لازم به منظور فعال نمودن ارتباطات شبکه ای اعطاء شده است. برای انجام این کار می توان مراحل زیر را دنبال نمود :
Start | Control Panel | Security Center
کلیک بر روی Windows Firewall از طریق Manage security settings for
انتخاب Add Program از طریق Exceptions

انتخاب برنامه مورد نظر (از طریق لیست و یا Browse نمودن)
پس از انجام عملیات فوق ، می بایست نام برنامه مورد نظر در لیست Exception مشاهده گردد. در صورتی که قصد بلاک نمودن موقت فعالیت ارتباطی یک برنامه را داشته باشیم،می توان از Cehckbox موجود در مجاورت نام برنامه استفاده نمود . برای حذف دائم یک برنامه موجود در لیست Exception ، می توان از دکمه Delete استفاده نمود .
کاربرانی که دارای اطلاعات مناسب در رابطه با پورت های مورد نیاز یک برنامه می باشند ، می توانند با استفاده از Add Port ، اقدام به معرفی و فعال نمودن پورت های مورد نیاز یک برنامه نمایند . پس از فعال نمودن پورت ها ، وضعیت آنان صرفنظر از فعال بودن و یا غیرفعال بودن برنامه و یا برنامه های متقاضی ، باز باقی خواهند ماند . بنابراین در زمان استفاده از ویژگی فوق می بایست دقت لازم را انجام داد . اغلب از ویژگی فوق در مواردی که پس از اضافه نمودن یک برنامه به لیست Exception همچنان امکان ارتباط آن با سایر کامپیوتر و یا برنامه های موجود در شبکه وجود نداشته باشد، استفاده می گردد .

آیا فایروال با بازی های اینترنتی کار می کند؟

پاسخ به سوال فوق مثبت است و فایروال ویندوز قادر به باز نمودن پورت های ضروری برای بازی های اینترنت و یا شبکه محلی است . در این رابطه یک حالت خاص وجود دارد که ممکن است برای کاربران ایجاد مشکل نماید. در برخی موارد ممکن است پیام هشداردهنده امنیتی که از شما به منظور ارتباط با سایر برنامه ها تعیین تکلیف می گردد ، بر روی صفحه نمایشگر نشان داده نمی شود . همانگونه که اطلاع دارید اکثر بازی های کامپیوتری به منظور نمایش تصاویر سه بعدی بر روی نمایشگر و استفاده از تمامی ظرفیت های نمایش ، از تکنولوژی DirectX استفاده می نمایند . با توجه به این موضوع که پس از اجرای یک بازی ، کنترل نمایش و خروجی بر روی نمایشگر بر عهده بازی مورد نظر قرار می گیرد ، امکان مشاهده پیام هشداردهنده امنیتی وجود نخواهد داشت . (در واقع پیام پشت صفحه بازی مخفی شده است) . بدیهی است با عدم پاسخ مناسب به پیام هشداردهنده ، فایروال ویندوز امکان دستیابی شما به شبکه بازی را بلاک خواهد کرد . در صورت برخورد با چنین شرایطی در اکثر موارد با نگه داشتن کلید ALT و فشردن دکمه TAB می توان به Desktop ویندوز سوئیچ و پیام ارائه شده را مشاهده و پاسخ و یا واکنش مناسب را انجام داد . پس از پاسخ به سوال مربوطه می توان با فشردن کلیدهای ALT+TAB مجددا" به برنامه مورد نظر سوئیچ نمود .
تمامی بازی های کامپیوتری از کلیدهای ALT+TAB حمایت نمی نمایند . در چنین مواردی و به عنوان یک راهکار منطقی دیگر، می توان اقدام به اضافه نمودن دستی بازی مورد نظر به لیست Exception نمود (قبل از اجرای بازی) .
چرا با این که نام یک برنامه به لیست Exception اضافه شده است ولی همچنان امکان ارتباط صحیح وجود ندارد ؟ علت این امر چیست و چه اقداماتی می بایست انجام داد ؟
در صورت استفاده از یک فایروال سخت افزاری ، می بایست پورت های مورد نیاز یک برنامه بر روی آن نیز فعال گردند . فرآیند نحوه فعال نمودن پورت بر روی فایروال های سخت افزاری متفاوت بوده و به نوع آنان بستگی دارد . مثلا" در اکثر روترهائی که از آنان در شبکه های موجود در منازل استفاده می شود ، می توان با استفاده از یک صفحه وب پارامترهای مورد نظر (نظیر پورت های فعال) را تنظیم نمود . در صورتی که پس از بازنمودن پورت های مورد نیاز یک برنامه مشکل همچنان وجود داشته باشد ، می توان برای کسب آگاهی بیشتر به سایت پشتیبانی مایکروسافت مراجعه نمود .

آیا باز نمودن پورت های فایروال خطرناک است ؟

با باز نمودن هر پورت ، کامپیوتر شما در معرض تهدیدات بیشتری قرار خواهد گرفت . علیرغم باز نمودن برخی پورت ها به منظور بازی و یا اجرای یک کنفرانس ویدئویی ، فایروال ویندوز همچنان از سیستم شما در مقابل اغلب حملات محافظت می نماید. پس از معرفی یک برنامه به فایروال ویندوز ، صرفا" در زمان اجرای این برنامه پورت های مورد نیاز فعال و پس از اتمام کار ، مجددا" پورت های استفاده شده غیرفعال می گردند . در صورتی که به صورت دستی اقدام به باز نمودن پورت هائی خاص شده باشد، پورت های فوق همواره باز شده باقی خواهند ماند . به منظور حفظ بهترین شرایط حفاظتی و امنیتی ، می توان پس از استفاده از پورت و یا پورت هائی که با توجه به ضرورت های موجود فعال شده اند ، آنان را مجددا" غیرفعال نمود (استفاده از checkbox موجود در مجاورت برنامه در لیست Exception) .

چگونه می توان صفحه مربوط به نمایش پیام های هشداردهنده امنتی فایروال ویندز را غیرفعال نمود ؟
در صورتی که فایروال ویندز را اجراء نکرده باشید و مرکز امنیت ویندوز (WSC) قادر به تشخیص فایروال استفاده شده بر روی سیستم شما نباشد ، شما همواره یک پیام هشداردهنده امنیتی فایروال را مشاهده خواهید کرد . برای غیرفعال نمودن این چنین پیام هائی می توان مراحل زیر را انجام داد :
Start | Control Panel | Security Center

در بخش Windows Security Center ، بر روی دکمه ecommendation کلیک نمائید . در صورتی که دکمه فوق مشاهده نشود ، فایروال ویندوز فعال است)
انتخاب گزینه I have a firewall solution that I'll monitor myself

پس از انجام عملیات فوق ، ویندوز وضعیت فایروال را اعلام نخواهد کرد . رویکرد فوق در مواردی که از یک فایروال سخت افزاری و یا

نرم افزاری خاص استفاه می شود ، پیشنهاد می گردد . بدین ترتیب مرکز امنیت ویندوز ، وضعیت فایروال را مانیتور نخواهد کرد .
و اما نکته آخر و شاید هم تکراری !

برای استفاده ایمن از اینترنت ، می بایست اقدامات متعددی را انجام داد . قطعا" استفاده از فایروال یکی از اقدامات اولیه و در عین حال بسیار مهم در این زمینه است . یک سیستم بدون وجود یک فایروال ، در مقابل مجموعه ای گسترده از برنامه های مخرب آسیپ پذیر است و در برخی موارد صرفا" پس از گذشت چندین دقیقه از اتصال به اینترنت ، آلوده خواهد شد . با استفاده از یک فایروال ، ضریب مقاومت و ایمنی کاربران در مقابل انواع حملات افزایش می یابد.

منابع:

http://www.srco.ir/Articles/TipsView.asp?ID=254
http://www.behsazanhost.com/%D8%A7%D8%AE%D8%A8%D8%A7%D8%B1-%D9%88-%D9%85%D9%82%D8%A7%D9%84%D8%A7%D8%AA/%D8%A2%D9%85%D9%88%D8%B2%D8%B4-%D9%85%DB%8C%D8%B2%D8%A8%D8%A7%D9%86%DB%8C-%D9%88%D8%A8/16-%D8%A7%D9%85%D9%86%DB%8C%D8%AA-%D8%B3%D8%B1%D9%88%D8%B1-%D8%A7%D9%86%D8%AA%DB%8C-%D9%88%DB%8C%D8%B1%D9%88%D8%B3-%D9%87%D8%A7/583-%D9%81%D8%A7%DB%8C%D8%B1%D9%88%D8%A7%D9%84-%DA%86%DB%8C%D8%B3%D8%AA%D8%9F.html
http://www.persianelearning.com/fa/rss-articalse/138-computer-science-education/227-what-is-a-firewall
http://www.rasekhoon.net/forum/thread/374384
http://www.parsnice14.com/Text/Archive/General/Healthy/231.html

گردآوری و ارسال: مهندس مجتبی مددی چلیچه

منبع: پایگاه اطلاع رسانی پلیس فتا