مروری بر فایروال‌ها

تا چند سال پيش بسياري از افراد تصور مي‌كردند كه استفاده از فايروال بر روي سيستم به علت ترس بيهوده كاربران است. واقعا چه كسي به اطلاعات كامپيوتر شما نياز دارد؟

اما امروزه با افزايش تعداد كساني كه دائما به اينترنت متصل هستند و ماهرتر شدن ويروس‌ها، wormها، و برنامه‌هاي Trojan وجود فايروال‌ها ضروري به نظر مي‌رسد. اگر كامپيوترتان حتي به مدت زمان بسيار كمي در روز به شبكه متصل مي‌شود، وجود فايروال نه تنها از نظر محافظت سيستم، بلكه براي نشان دادن اينكه شما يك كاربر خوب شبكه هستيد ضروري مي‌باشد.
فايروال‌هاي نرم‌افزاري جديد اين اطمينان را به وجود مي‌آورند كه در صورت آلوده بودن كامپيوتر، آلودگي از طريق شبكه گسترش نخواهد يافت.
راهكار ديگر فايروال سخت‌افزاري است كه مي‌تواند به صورت مستقل يا داخل يك روتر مورد استفاده قرار گيرد. اما اين نوع فايروال گران است و بسياري از مردم معتقدند كه مديريت فايروال‌هاي نرم‌افزاري بر روي كامپيوتر بسيار آسان‌تر است ويندوز ايكس‌پي داراي يك فايروال نرم‌افزاري مي‌باشد.
ما ۹ محصول را (كه فايروال ويندوز هم شامل آن است) مورد آزمايش قرار داده‌ايم تا ميزان سهولت استفاده از آنها، مقدار تداخلي كه با برنامه‌هاي ديگر ايجاد مي‌كنند و نيز ميزان انعطاف‌پذيري آنها را مشخص كنيم. تعدادي از اين محصولات براي كاربران فني در نظر گرفته شده‌اند و تعدادي نيز تسهيلات اضافه‌اي ارائه مي‌كنند و به عنوان مجموعه‌هاي كامل امنيتي مورد استفاده قرار مي‌گيرند. بعضي از محصولات فوق هم به دليل سهولت استفاده مورد توجه قرار گرفته‌اند. با توجه به قيمت مناسب اين مجموعه‌ها دليلي وجود ندارد كه چنين حفاظتي را براي سيستم خود و نيز افرادي كه اينترنت را به طور مشترك با شما مورد استفاده قرار مي‌دهند فراهم نسازيد.

Agnitum outpost 2

فايروال شخصي نه چندان معروف outpost Personal firewall Pro2 داراي اينترفيسي است كه كاربران outlook مايكروسافت با احساس راحتي كامل با آن كار مي‌كنند، اينترفيسي با يك صفحه اصلي خلاصه شده و يك درخت قابل گسترش در سمت چپ صفحه.
در آزمايشات ما نصب برنامه ساده بوده و برنامه توانست شبكه خانگي را كه استفاده مي‌كرديم شناسايي كند، گرچه outpost به طور پيش‌فرض به ماشين‌هاي مرتبط اعتماد ندارد. خوشبختانه ايجاد تغييرات براي امكان به اشتراك گذاري فايل بسيار ساده است. در ضمن كامپيوتر در طي زمان راه‌اندازي (Start up) اسكن مي‌شود تا برنامه‌هاي كاربردي اينترنت مشخص شوند بنابراين برنامه‌ها مي‌توانند مجوز بگيرند بدون اينكه مجبور باشيد هر يك از آنها را به ترتيب كليك كنيد. اما تعدادي از برنامه‌هاي كليدي ما همچون Net Object Fusion يافت نشدند.
همچون اكثر فايروال‌ها در اين محصول نيز تلاش براي اجراي يك برنامه ناآشنا كه به شبكه متصل است به ايجاد يك اخطار pop up منجر مي‌شود.

شما مي‌توانيد قوانيني را بر اساس موارد از پيش تنظيم شده ايجاد كنيد، در ضمن قوانين پيشرفته خودتان نيز مقدور مي‌باشد. انجام دادن چنين كاري آسان بوده و به روش قوانين outlook عمل مي‌نمايد. بدين ترتيب شما با انتخاب گزينه‌ها قانوني ايجاد مي‌كنيد و سپس توصيف نوشتاري كاملي از موارد روي داده در پنجره تهيه مي‌نماييد.
برنامه از معماري plug-in استفاده مي‌كند و plug-inهايي براي مسدود ساختن تبليغات، مديريت و حتي فيلترسازي دستيابي به شبكه بر اساس واژه‌هاي كليدي موجود در صفحات در آن موجود مي‌باشد. البته فيلترسازي محتوا به صورت كامل نيست، اما حفاظت مفيدي را فراهم مي‌سازد. ساير موارد شامل توابع whois و ثبت فعاليتهاي وب است گرچه ما براي آزمايش آنها وقت نداشتيم.
اسكن‌هاي امنيتي نشان مي‌دهد كه سيستم فوق در پنهان‌سازي كامپيوتر از شبكه و نيز سيستم عامل در حال اجرا خوب عمل مي‌كند. در ضمن مي‌توانيد برنامه را طوري تنظيم كنيد كه با آشكار شدن يك عامل مزاحم همچون يك اسكن پورت، آدرس IP يا كل زير شبكه مسدود شود.

CA E-Trash EZ Firewall

EZ Firewall، محصول شركت computer Associates، در حقيقت بر پايه كد Zone Alarm تهيه شده كه البته اندكي تغييرات در آن صورت گرفته است. اول اينكه شما براي نصب آن به مجوز نياز داريد هر چند مي‌توانيد از نسخه آزمايشي ۳۰ روزه آن استفاده كنيد.
در طي نصب به شما يادآوري مي‌شود كه كنترل خصوصي‌سازي را فعال ساخته و با ايجاد يك اسم رمز فايروال را در مقابل تغيير تنظيمات محافظت نماييد. در ضمن از شما پرسيده مي‌شود كه تمايل داريد فايروال باinternet Connection Sharing مايكروسافت كار كند يا خير؟
در آزمايشات ما، شبكه‌اي كه سيستم به آن متصل بود به خوبي نشان داده شد اما بعضي از كاربران احتمالا پرسش فوق را گيج كننده مي‌يابند زيرا تنها دو گزينه دارد و به نظر نمي‌رسد كه هيچ يك از گزينه‌ها كاملا قابل اعمال باشند.
در اين محصول برخلاف Zone Alarm Pro هيچ گزينه‌اي براي افزودن اتوماتيك تعداد زيادي برنامه به ليست برنامه‌هاي مجاز وجود ندارد. شما مي‌توانيد تعدادي برنامه را در يك زمان اضافه كنيد اما براي اين كار بايد هارديسك خود را مرور كنيد تا هر كدام از برنامه‌ها را بيابيد.
كنترل‌هاي خصوصي‌سازي، شامل گزينه‌اي براي تنظيم كنترل‌هاي مختلف براي سايت‌هاي مختلف، ارائه شده كه بسيار مورد استقبال قرار گرفته است. شما حتي مي‌توانيد تبليغاتي را كه در طي محدوده زماني خاص بارگذاري نمي‌شوند مسدود سازيد.
يك دگمه قفل براي مسدود ساختن دستيابي به شبكه وجود دارد اما با تنظيم برنامه‌هاي خاص مي‌توان قفل را باز كرد. بنابراين به عنوان مثال seti screen saver مي‌تواند هنوز كار كند.
فايروال EZ كار خود را انجام مي‌دهد (تعجبي ندارد چون اين برنامه بر اساس Zone Alarm تهيه شده) اما فاقد مجموعه ويژگي‌هاست كه در محصول Pro شركت Zone labs وجود دارد و مسئله حيرت‌آورتر اينكه محصول فوق فاقد يكي از اين ويژگي‌هاست كه حتي در نسخه رايگان Zone Alarm وجود دارد. در حاليكه در نگاه اول هشدارهاي مربوط به نفوذ سيستم يا دستيابي برنامه‌ها به شبكه بسيار شبيه به چنين هشدارهايي در Zone Alarm است اما

جاي يك دگمه خالي مي‌باشد: گزينه اطلاعات بيشتر. اين به آن معناست كه كاربراني كه به دنبال اطلاعات بيشتر درباره يك برنامه در حال اجرا يا يك حمله احتمالي مي‌باشند به نتيجه نخواهند رسيد. دليل حذف اين دگمه هر چه مي‌خواهد باشد، مهم اين است كه فقدان آن سبب شده تا محصول فوق چند امتيازي از دست بدهد.
تصوير بالا: فايروال EZ تقريبا نسخه اصلاح شده Zone Alarm Pro مي‌باشد.
تصوير سمت چپ: متاسفانه فايروال EZ فاقد دگمه More Info مي‌باشد. اين دگمه در نسخه Zone labs به شما كمك مي‌كند تا اطلاعات مورد نظر خود را بيابيد.

ISS Black Ice Pc Protection

Black Ice نام شناخته شده‌اي در زمينه فايروال‌ها مي‌باشد كه مدتهاست براي كاربران آن‌لاين توصيه شده است. نسخه جديد با عنوان 3.66 داراي ويژگي محافظت از برنامه ارائه شده توسط بسياري از برنامه‌هاي كاربردي مي‌باشد. وجود اين ويژگي به معناي توانايي مداخله به هنگام تلاش يك برنامه براي دستيابي به شبكه است. Black Ice از اين هم فراتر رفته و هر گونه تلاش برنامه‌هاي ناشناخته همچون برنامه‌هاي Installer را آشكار مي‌سازد. اما حالت نصب مي‌تواند چنين ويژگي را غير فعال سازد، يك يادآوري كننده را در زمانهاي مشخص ظاهر كند و براي مشخص كردن موقعيت فايل‌هاي جديدي كه كامل كرده‌ايد سيستم را اسكن نمايد. اسكن سيستم مدتي وقت مي‌گيرد. در آزمايشات ما مرحله اسكن در ابتدا ١١ دقيقه بعد از شروع و سپس پايان يافتن عمل نصب، ٤ دقيقه طول مي‌كشد.
Black Ice از نظر وضعيت هشدارها نيز با ساير رقبا تفاوت دارد. در اين سيستم اعلام هشدار به صورت اخطارهاي ظاهر شونده نيست بلكه با چشمك زدن آيكون محافظ در بخش پايين كاربر متوجه خواهد شد كه مسئله‌اي پيش آمده است. با دوبار كليك كردن بر روي آيكون فوق پنجره برنامه اصلي باز مي‌شود و در اينجاست كه مسئله بغرنج‌تر مي‌شود.
Black Ice به به‌روزرساني اينترفيس نياز مبرم دارد و داراي سه بخش Events، Intruders، History مي‌باشد. با كليك بر يكي از آيتم‌هاي بخش Events وارد بخش Intruders خواهيد شد و اطلاعات بيشتري درباره كامپيوترهاي ديگر شبكه به دست خواهيد آورد.
بخش History گراف‌هاي ساده‌اي است كه فعاليت را نشان مي‌دهد. تنظيمات در يك پنجره منفرد چند بخشي قرار دارد و نيازمند بررسي كامل اطلاعات است. براي به اشتراك‌گذاري فايل در شبكه بايد گزينه Allow Internet file sharing، Allow Netbios Neighborhood را كه به معني مرور شبكه است، علامت بزنيد.
Black Ice داراي مجموعه گزينه‌هاي خوبي همچون توانايي مسدود ساختن موقت يك سيستم راه دور براي مدت زمان خاص يا پذيرفتن تمام ارتباطات از كامپيوتر ديگر مي‌باشد. به طور كل Black ice فايروال قابل قبولي است كه از اينترفيس دهه ١٩٩٠ برخوردار بوده و تعدادي از گزينه‌هاي انعطاف‌پذير ساير محصولات را براي كاربر فراهم نمي‌سازد.

Kerio Personal Firewall 4

نصب فايروال kerio آسان است. در آزمايشات ما اين محصول توانست موقعيت شبكه خانگي LAN را به طور صحيح نشان دهد. در هنگام انتقال فايل در شبكه با تنظيمات پيش‌فرض هيچگونه مشكلي پيش نيامد و كامپيوتر از ساير موارد اينترنت محافظت شد.
فيلترسازي اينترنت براي حذف تبليغات و مسدود كردن عناصر فعالي همچون VB Script يا Active X نيز يكي از ويژگي‌هاي kerio است. شما مي‌توانيد با گزينه‌هاي جداگانه براي هر نوع كوكي كوكي‌هاي session، كوكي‌هاي خارجي و كوكي‌هاي پايدار، آنها را مسدود سازيد (كنترل بيشتر نسبت به مجموعه‌هاي ديگر) در ضمن با كمك ويژگي فوق مي‌توانيد اطلاعات شخصي مثل شماره كارتهاي اعتباري ارسال شده از طريق وب را مسدود سازيد.
با تقاضاي دستيابي به شبكه يا مشخص شدن موقعيت يك ارتباط دريافت شده اخطاري ظاهر مي‌شود. شما مي‌توانيد مثل ساير موارد تقاضا را بپذيريد يا آن را رد كنيد و سپس پاسخ خود را براي اخطارهاي مشابه تعيين نماييد. در ضمن مي‌توانيد يك قانون اختصاصي كاملا ساده ايجاد كنيد. (البته نه به سادگي outpost) در صورت تمايل مي‌توانيد ويژگي فيلترسازي پيچيده را نيز تنظيم كنيد.
يكي از نقاط ضعف جزئي kerio اين است كه هيچ گزينه‌اي براي اسكن برنامه‌هاي مجاز به دستيابي وجود ندارد. در اينجا بايد منتظر اعلام هشدارها در هر مورد باشيد و سپس براي ايجاد مجوزها به صورت اتوماتيك آنها را كليك كنيد. از طرف ديگر اين به آن معناست كه شما كاملا به ارتباطات كامپيوتر خود اطمينان داريد.
اينترفيس kerio به خوبي محصولات ديگر نيست و به توان و تخصص كاربر در استفاده از آن بستگي دارد. صفحه اصلي، برنامه‌هاي در حال اجرا و ارتباطات آنها را نشان مي‌دهد.
ثبت وقايع در اين محصول خوب است، در آزمايش ما، kerio تلاش‌هاي fingerprinting و اسكن پورت ما را نشان داد (گرچه در طي فرآيند اخطارهاي فراواني ظاهر شد).
اگر kerio در اسكن پورت هر چند ثانيه يك بار ما را به ستوه نمي‌آورد مي‌توانستيم آن را دوست داشته باشيم. Kerio به طور كل محصول خوبي است و ويژگي‌هاي زيادي را با قيمت مناسب در اختيار كاربران (البته نه افراد مبتدي) قرار مي‌دهد.

McAfee personal firewall plus

McAfee يكي از نام‌هاي مطرح در حوزه محافظت از كامپيوتر مي‌باشد بنابراين جاي تعجب ندارد كه يك فايروال شخصي در ميان محصولات خود ارائه دهد. با كمال تعجب مشاهده مي‌شود كه در روي جعبهMcAfee Personal Firewall plus 2004 v5 توصيه شده كه يك كاربر ابتدايي اينترنت احتمالا نيازي به فايروال نخواهد داشت، چنين توصيه‌اي اين روزها تاييد نمي‌شود.
نصب اين محصول آسان است، اما يك آدرس پست‌الكترونيك براي ثبت‌نام و نيز يك اسم رمز براي زمانيكه برنامه خود را براي اولين اجرا به روزرساني مي‌كند مورد نياز مي‌باشد. مانند ديگر فايروال‌هاي شخصي، مركز امنيت McAfee نيز نصب مي‌شود و مي‌تواند برنامه‌هاي ديگر شركت را اجرا كند. البته ما ترجيح مي‌دهيم اين را تنها زماني ببينيم كه برنامه‌هاي

كاربردي ديگر وجود دارد چون معناي آن اين است كه بايد ابتدا آيكون واقع در System tray را كليك كرده و سپس از انتخاب يك زيرمنو به فايروال برسيد.
نقش McAfee در دنياي فايروال، توصيه‌هاي هوشمند است. برنامه به همراه ديتابيسي از برنامه‌هاي شناخته شده عرضه مي‌شود، بنابراين ديگر مجبور نيستيد تا همه آنها را پيكربندي كنيد، گرچه بار ديگر Netobjects Fusion در آن گنجانده نشده است. شما مي‌توانيد اطلاعاتي را درباره يك برنامه به McAfee بدهيد تا برنامه در آينده وارد مجموعه شود اما اين روند مستلزم چندين Cut، paste است (ما ترجيح مي‌دهيم اين كار به صورت اتوماتيك انجام گيرد).
به اشتراك‌گذاري فايل بر روي شبكه محلي و با استفاده از تنظيمات پيش‌فرض مشكلي ايجاد نمي‌كند اما انتقال فايل‌هاي MSN Messenger با دشواري‌هايي همراه مي‌باشد. كنترل و بررسي حملات و ديگر اخطارهاي دريافتي به سادگي انجام مي‌شود. امكان رديابي، آدرس IP و دامين whois را براي آگاهي از حملات احتمالي مورد بررسي دقيق قرار مي‌دهد و شما مي‌توانيد اطلاعات مشروح در اين باره را به طور اتوماتيك به سايت McAfee Hackerwatch ارائه كنيد. راهنماي آن‌لاين انواع مختلف اخطارها و نگراني‌هاي موجود را شرح مي‌دهد. اخطارهاي نه چندان مهم را مي‌توان طوري تنظيم نمود تا پس از ۱۰ ثانيه قطع شوند و نيازي به كليك كردن اضافه نداشته باشند.
McAfee با قيمت مناسب مجموعه خوبي به نظر مي‌رسد و در صورتيكه ديگر محصولات آن را نيز داشته باشيد مي‌توانيد آنها را در كنار يكديگر كامل كنيد.

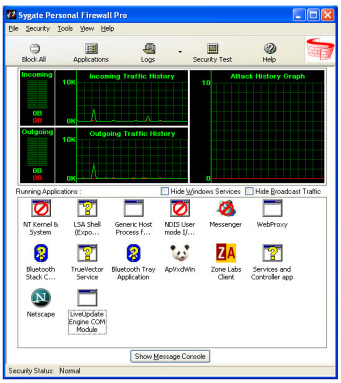
Microsoft Windows XP FireWall

با توجه به انتقادهاي شديد در مورد مسائل امنيتي مايكروسافت و تعداد شكاف‌هايي كه در طي چندين سال در محصولات مختلف مايكروسافت ديده شده اين مسئله كه ويندوز ايكس‌پي داراي فايروال مي‌باشد سبب تعجب بسياري از كاربران شده است. البته فايروال در نگاه اول مشخص نيست. شما مي‌توانيد آن را از طريق بخش Advanced properties شبكه و علامت زدن يك كادر فعال سازيد. طريقه ديگر فعال ساختن آن ويزارد Network setup است، اما گزينه‌هاي پيكربندي زيادي وجود ندارد.
فايروال ويندوز ايكس‌پي اينترفيس مناسبي ندارد. اين موضوع يا به اين دليل است كه مايكروسافت نمي‌خواهد به عنوان شركتي شناخته شود كه به محدوده برنامه‌هاي كمكي ديگر تعدي نموده و يا عدم علاقه در اين زمينه سبب ايجاد چنين اينترفيسي شده است. تنظيمات پيشرفته ۳ بخش ساده Services، Security logging، ICMP را ارائه مي‌كند.
با كليك بر روي بخش Security logging به يك فايل متني مي‌رسيم، در حاليكه دو بخش ديگر كادرهايي را براي آيتم‌هاي خاص همچون سروروب، دسك‌تاپ راه‌دور، سرور FTP يا تقاضاي ICMP echo ارائه مي‌كنند كه مي‌توانيد براي انتخاب هر گزينه آن را علامت بزنيد. گرچه اطلاعات شبكه قابل درك است اما به زبان انگليسي كاملا ساده بيان نشده است. روش مبتني بر برنامه كاربردي كه ساير رقبا در پيش گرفته‌اند براي كاربران مبتدي بيشتر قابل درك است.

در بخش Services شما مي‌توانيد در صورت نياز امكانات اضافه‌اي داشته باشيد، اما بايد بدانيد كه چه شماره پورتي مورد استفاده قرار گرفته است.
بخش logging (ثبت وقايع) براي مبتديان كاربردي ندارد. به راستي اين بخش بسيار بزرگ است و حاوي اطلاعات زيادي مي‌باشد. اين موضوع قابل بحث است كه آيا بخش logging براي همه افراد به جز تحليلگران متعصب شبكه قابل استفاده است. اين بخش يك فايل متني ساده به همراه خط عنوان در بالاي آن و اطلاعات به صورت رديفي مي‌باشد.
فايروال مايكروسافت كار خود را انجام داده و ترافيك را كاملا مسدود مي‌سازد. اگر مي‌خواهيد كارهايي را انجام دهيد كه حفاظت نمي‌شوند بايد به سرعت از آن آگاه شويد. از آنجائيكه شناسايي شبكه به معناي واقعي وجود ندارد به اشتراك گذاري فايل در شبكه محلي مسدود مي‌شود. اگر سيستم شما توسط يك worm، يا Trojan آلوده شود هيچ كنترل ارتباطات ارسالي وجود ندارد.

Sygate Personal Firewall

Sygate نيز مانند محصولات ديگر به صورت نسخه‌هاي رايگان و غير رايگان عرضه مي‌شود.
ما در اينجا نسخه رايگان يعني Sygate Personal Firewall Standard را مورد بررسي قرار داده‌ايم تا دريابيم در صورتيكه شما نخواهيد هزينه‌اي صرف كنيد و يا تمايل داشته باشيد از فايروال دروني ويندوز ايكس‌پي استفاده كنيد انتظار چه نوع امكاناتي را مي‌توانيد داشته باشيد.
اگر داراي شبكه هستيد مي‌توانيد از يك نسخه كوچك شبكه كه براي سه كاربر طراحي شده استفاده كنيد.



نصب اين محصول ساده مي‌باشد. اما در آزمايشات، در مرحله بوت مجدد قبل از رسيدن به صفحه ثبت‌نام اخطارهاي زيادي دريافت نموديم كه كمي گيج‌كننده بود. كادرهاي ظاهر شونده sygate نيز مانند كادرهاي outpost به صورت پنجره‌هاي استاندارد مدل برنامه كاربردي (application-style) مي‌باشند و زياد جلب توجه نمي‌كنند. آنها حاوي اطلاعات بسيار زيادي هستند. كافيست آنها را كليك كنيد تا بتوانيد اطلاعات شبكه و به دنبال آن اخطارهايي را دريافت كنيد.
كنسول اصلي نموداري از فعاليت شبكه را به همراه آيكون برنامه‌هاي در حال اجرا نشان مي‌دهد، شما مي‌توانيد سرويس‌هاي ويندوز را پنهان سازيد. پنهان كردن پيغام‌هاي موجود در انتهاي صفحه نيز اختياري مي‌باشد.
به اشتراك‌گذاري فايل بر روي شبكه ما به صورت پيش فرض توسط يك پيغام خطا مربوط به فايل ntoskrnl.exe مسدود شد، اما فعال ساختن مجدد به اشتراك‌گذاري كار سختي نبود.
هنگاميكه محافظ صفحه نمايش دچار اشكال مي‌شود گزينه‌اي براي مسدود ساختن ترافيك شبكه موجود است.
محدوده گسترده‌اي براي ايجاد قوانين وجود دارد و شما مي‌توانيد آنها را زمانبندي نماييد، به عنوان مثال مي‌توانيد دستيابي با وجود فايروال را در زمانهاي خاص باز بگذاريد.

شما مي‌توانيد علاوه بر زير شبكه‌ها و آدرس‌هاي IP معمولي قوانيني را بر اساس آدرس MAC بسازيد، در صورتيكه از DHCP استفاده مي‌كنيد و مي‌خواهيد كامپيوتر خاصي را بدون توجه به آدرس IP آن مسدود سازيد اين كار بسيار آسان است.
در ضمن تنها محصولي است كه بر اساس ويندوز ۹۵ و البته تنها نسخه OSRZ و نسخه‌هاي بعد از آن كار مي‌كند. تعداد ابزارهاي قدرتمند نسخه رايگان Sygate بسيار زياد است و در نسخه غير رايگان حتي تعداد بيشتري ابزار وجود دارد. تنها نگراني ما اينترفيس Sygate است كه براي مبتديان مناسب نمي‌باشد.

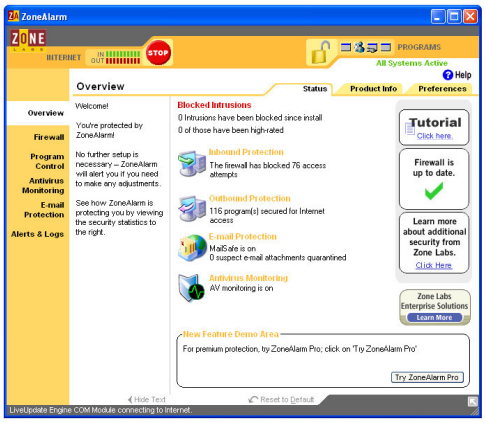
Symantec Internet Security

Norton Internet security 2004 چيزي بيش از يك فايروال است. محصول فوق شامل ابزارهايي براي كنترل اسپم، كنترل از طرف والدين و برنامه‌هاي ضد ويروس مي‌باشد، گرچه نصب هر يك از اين گزينه‌ها به انتخاب كاربر صورت مي‌پذيرد. در اينجا كنترل حريم خصوصي و فايروال مورد بحث مي‌باشد.
در اين محصول نيز مانند McAfee عمل نصب با download كردن برنامه به روز شده نرم‌افزار پايان مي‌يابد، قوانين به طور اتوماتيك براي برنامه‌هاي رايج ايجاد مي‌شود و امكان دستيابي را براي آنها فراهم مي‌سازد. Symantec با كار كردن با Netobjects Fusion و حتي تشخيص putty، كه يك برنامه SSH بر روي كامپيوتر مي‌باشد، نشان داد كه از ساير رقبا بهتر عمل مي‌كند. اين فايروال به ما امكان داد تا فايل‌ها را از طريق MSN Messenger نيز دريافت كنيم.
دستيابي به شبكه در اين محصول با مشكلات بيشتري همراه است. ما توانستيم به ماشين‌هاي ديگر متصل شويم اما امكان به اشتراك‌گذاري فايل بدون تغيير دادن قوانين (اين تغيير قوانين به سادگي محصولات ديگر مثلا outpost نبود) وجود نداشت.
يكي از ويژگي‌هاي Symantec سيستم Location مي‌باشد بدين ترتيب شما مي‌توانيد در زمانيكه كامپيوتر در جاهاي مختلف مثل خانه يا دفتر قرار دارد و يا از طريق يك hotspot بي‌سيم به شبكه متصل است، قوانين مختلفي داشته باشيد.
كنترل‌هاي حريم خصوصي مي‌توانند از ارسال اطلاعات در شبكه جلوگيري كنند اما از قرار معلوم آنها در ارتباطات امن به كار گرفته نمي‌شوند كه اين مسئله مي‌تواند مشكلاتي را ايجاد كند.
اخطارهاي Symantec اطلاعات واضحي از خطر را به شما مي‌دهند اما رديابي بصري نفوذگران، به اپلت جاوا اتكا دارد و مشكلاتي را براي تعدادي از كاربران ايجاد مي‌كند. سيستم فوق تلاشهاي اثر انگشت و اسكن پورت آزمايشي ما را نشان داد و گزينه‌هاي پيش‌فرض ماشين‌هاي مورد حمله قرار گرفته را مسدود ساخت.
فايروال Symantec براي بسياري از كاربران يك راهكار عالي محسوب مي‌شود زيرا بدليل وجود پيش فرض‌هاي معقولانه نيازي به پيكربندي برنامه‌هاي جديد نمي‌باشد. تنها اشكال موجود تغيير قوانين اختصاصي براي شرايط مختلف است. اما وجود ويژگي‌هاي بسيار خوب ديگر مانند برنامه ضد ويروس يا كنترل از طرف والدين قيمت بالاي اين مجموعه را توجيه مي‌كند.

Zone Labs zone Alarm Pro

اگر بخش مربوط به EZ firewall را مطالعه کرده باشید متوجه شباهت آشکار بین آن و zone Alarm خواهید شد: هر دو از روند نصب یکسان (به طور مجازي) برخوردارند، گرچه در این مورد Zone Alarm Pro داراي ليستي از برنامه‌هاي ايمن است كه مي‌توانند به طور اتوماتيك به اينترنت دسترسي داشته باشند و بدين ترتيب كمي در زمان پيكربندي صرفه‌جويي مي‌شود. ليست فوق شامل كلاينت‌هاي پيغام‌گذاري ثالث همچون Trillian مي‌باشد اما Netobjects در آن وجود ندارد (عليرغم اينكه وجود اين قابليت سبب صرفه‌جويي در زمان نصب مي‌شود).

Zone Alarm pro علاوه بر قابليت‌هاي مسدودسازي تبليغات و كنترل‌هاي حفظ حريم خصوصي موجود در EZ firewall، از قابليت محافظت اسم رمز Ebay براي حفاظت از كاربران نيز برخوردار است.



ويژگي اتوماتيك پاكسازي حافظه cache مي‌تواند در زمانهاي تعيين شده هارددیسك شما را پاكسازي نمايد، اين پاكسازي شامل بخش‌هاي Scandisk، فايل‌هاي موقت Media player، حافظه cache نت‌اسكيپ و Internet Explorer مي‌باشد (اين قابليت در مورد opera كارآيي ندارد).

تنظيمات پيش‌فرض شبكه ما را در وضعيت Trusted zone قرار داد اما با اين وجود هنوز امكان به اشتراك‌گذاري فايل وجود نداشت. براي استفاده از اين امكان بايد آن را فعال سازيد كه اين كار به آساني انجام مي‌گيرد. يكي ديگر از كنترل‌هاي مفيد Zone Alarm توانايي آگاه ساختن شما از ارسال يك پيغام، با تعداد ضميمه بيشتر از حد تعيين شده توسط كامپيوترتان مي‌باشد. در ضمن اگر پيغام سريع‌تر از حد معمول نيز ارسال شود پيغام اخطار دريافت خواهيد نمود. اين قابليت به شما كمك مي‌كند تا با بعضي از ويروس‌هاي پست الكترونيك مقابله كنيد.

هر اخطار در Zone Alarm برخلاف EZ FireWall داراي يك دگمه More Info مي‌باشد. شما مي‌توانيد با استفاده از اين دگمه‌ها به سايت Zone Labs رفته و توضيحات مربوط به اخطار را به طور كامل دريافت كنيد.

در اينجا نيز مانند McAfee Hacker watch امكان ارائه اطلاعات به Zone labs به صورت ناشناس وجود دارد در نتيجه شركت مي‌تواند آماري را از طرف كاربران جمع‌آوري نمايد.

نسخه رايگان كه نسخه آزمايشي را نيز در پايان دوره تعيين شده در بر مي‌گيرد تنها قابليت‌هاي ابتدايي فايروال را عرضه مي‌كند اما لازم به ذكر است كه همين قابليت‌هاي ابتدايي نيز مناسب و قابل قبول هستند. وجود دگمه More info نيز سبب شده تا Zone Alarm بسيار مفيدتر از نسخه‌هاي معروف باشد.

نكاتي در رابطه با استفاده از فايروال

همانطور كه مي‌دانيد در استفاده از نرم‌افزارها نكاتي وجود دارد كه بايد آنها را در نظر داشته باشيد. در ضمن بايد قبل و بعد از نصب نرم‌افزار و نيز در طي اين مرحله بسيار محتاطانه عمل نماييد. در اينجا نكاتي را به شما يادآوري مي‌كنيم.
قبل از نصب يك فايروال سيستم خود را اسكن نماييد تا بتوانيد از آن در مقابل ويروس‌ها محافظت كنيد. زيرا بعضي از فايروال‌ها فرض را بر اين مي‌گيرند كه برنامه‌هاي موجود بر روي كامپيوتر شما ايمن هستند در نتيجه به طور اتوماتيك به آنها اجازه مي‌دهند تا به اينترنت دسترسي داشته باشند.
از اعداد خود آگاه باشيد: آدرس‌ها و شماره‌هاي IP سيستم ضروري براي ارتباط اينترنت خود را بررسي نماييد (مثل سرورهاي پستي و سرورهاي DNS) و آنها را به ليست ميزبان‌هاي قابل اعتماد در فايروال خود اضافه كنيد.
با حدس و گمان عمل نكنيد: بعضي از فايروال‌ها شبكه خانگي شما را به طور اتوماتيك شناسايي مي‌كنند و بعضي از آنها فاقد اين ويژگي هستند. تنظيمات سيستم را بطور كامل بررسي كنيد تا اطمينان حاصل نماييد كه تنها به ماشين‌هاي مورد اعتماد شما مجوز داده شده است و نه به طور مثال به تمام مشتريان فراهم‌كننده سرويس اينترنت شما (البته به صورت غير عمدي).
بعد از نصب فايروال آن را به طور كامل آزمايش كنيد تا مطمئن شويد كه تنظيمات در وضعيت مناسب هستند، به عنوان مثال امكان به اشتراك‌گذاري فايل در شبكه يا دريافت فايل از طريق برنامه پيغام فوري مورد استفاده شما وجود دارد. اگر اينطور نيست احتمالا بايد تنظيمات را تغيير دهيد اما بايد مواظب باشيد كه به طور اتفاقي برنامه به اشتراك‌گذاري فايل ويندوز را در معرض اينترنت قرار ندهيد.
وجود يك دوست در ارتباط ديگر شبكه براي انجام آزمايشات بسيار مفيد خواهد بود.
عكس‌العمل افراطي از خود نشان ندهيد زيرا ممكن است بسياري از هشدارهايي را كه از طرف فايروال دريافت مي‌كنيد اخطارهاي نادرست باشند. به عنوان مثال اسكن پورت لزوما به معناي اين نيست كه فردي سيستم شما را تحت نظر دارد. شايد گاهي اوقات فراهم‌كنندگان سرويس اسكن‌هايي را بر روي سيستم شما انجام دهند تا مطمئن شوند كه سرورهاي غير قانوني را اجرا نمي‌كنيد.
لاگ‌هاي خود را بررسي كنيد: غير فعال ساختن اخطارها يا بستن آنها راحت‌ترين كار است اما شما بايد فايل ثبت شده خود را بررسي كنيد تا متوجه شويد كه آيا تلاش‌هاي مجدد از طرف همان آدرس وجود دارد يا خير.

زيرا ممكن است حمله به سيستم شما يا مشتريان سرويس‌دهنده اينترنت شما جدي باشد.
آزمايش كنيد: در عوض اينكه گزينه Always let this program do what it wants را انتخاب كنيد به برنامه‌ها اجازه دهيد تا با يك ارتباط اوليه شروع شوند يا دسترسي آنها را ممنوع سازيد. قوانين فايروال خود را بر پايه ضروريات كار خود تهيه كنيد: آيا واقعا نياز داريد تمام برنامه‌ها در پايين صفحه در بخش system tray قرار گيرند و اجازه ارتباط داشته باشند؟
حدس و گمان نزنيد: بعضي از فايروال‌ها سعي دارند اطلاعات مهم سيستم شما را محافظت نمايند اما آنها خطاناپذير نيستند. به عنوان مثال ممكن است هنگامي كه در يك صفحه امن باشيد آنها سيستم را وارسي نكنند. اينجاست كه نصب يك سروروب ايمن، براي نفوذگر به آساني امكان‌پذير بوده و در نتيجه او مي‌تواند اطلاعاتي در مورد حساب بانكي شما بدست آورد. داشتن فايروال و نرم‌افزارهاي حريم خصوصي به اين معنا نيست كه فعاليت‌هاي آن‌لاين خود را بدون توجه به مسائل امنيتي انجام دهيد.
سيستم خود را به روزرساني كنيد: برنامه‌هاي خود را به طور مرتب به روزرساني كنيد. بسياري از فايروال‌ها نيز بايد برنامه‌هاي ضد ويروس در مدت زمان‌هاي مشخص به روزرساني شوند، در اين زمينه بخصوص اطلاعات مربوط به شناسايي الگوهاي خاص حمله بعضي از wormها بسيار ياري رسانده است. اكثر برنامه‌هايي كه در اين مقاله مورد بررسي قرار گرفته‌اند نسبتا ارزان هستند. به عنوان مثال قيمت استفاده ساليانه آنها از ارزش زماني كه صرف نصب مجدد ويندوز مي‌كند بسيار كمتر است.
وضعيت اقتصادي خود و هزينه‌ها را در نظر بگيريد: مجموعه فايروال‌هايي كه در اينجا بحث شد براي يك كامپيوتر منفرد بسيار ايده‌آل هستند اما در يك شبكه يا ADSL به علت وجود چندين كامپيوتر هزينه افزايش مي‌يابد و شايد در اين مورد استفاده از يك روتر با فايروال داخلي بيشتر مقرون به صرفه باشد (مثل مدل Zyxel prestige 652H) در ضمن با داشتن اين روتر ديگر نيازي نيست كه كامپيوتر خود را براي مرتبط نگهداشتن ساير كامپيوترها با شبكه روشن نگاه داريد.

Special Tanks From Myself Masters To Teach Hacking :

1- Mr c0llect0r , d3vilb0x , shoaliesefid7, s00t_hackers,the_best_hunt

2-And best my friends l0_ll_0l1 , webmaster_zerocalm, satanic_soulful

www.firehackers.net

my email :hack_really@yahoo.com

dangerous_hacker(hack_really)