انواع فایروال

موضوع : امنیت شبکه > فایروال > بخش دو

نویسنده : سینا احمدی نشاط

تاریخ انتشار : 22 مرداد 92

ایمیل : Encoder@programmer.net

وب سایت شخصی : http://hazyoon.ir

فروم امنیتی آشیانه : http://ashiyane.org

بیشتر فایروال های تجاری (هم سخت افزاری و هم نرم افزاری) دارای امکانات زیادی به منظور پیکربندی بهینه می باشند. با توجه به تنوع بسیار زیاد فایروال ها، می بایست به منظور پیکربندی بهینه آنان به مستندات ارائه شده، مراجعه نماییم تا مشخص گردد که آیا تنظیمات پیش فرض فایروال شما نیاز شما را تامین می کند یا خیر ؟

پس از پیکربندی، فایروال در یک سطح امنیتی و حفاظتی مناسب در خصوص ایمن سازی اطلاعات ایجاد خواهد شد. لازم است به این موضوع مهم اشاره گردد که پس از پیکربندی 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 به .دنبال داشته باشد

انواع فایروال

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

فایروال های سطح مدار (Circuit-Level):

این فایروال ها به عنوان یک رله برای ارتباطات TCP عمل می کند. آنها ارتباط TCP با رایانه پشتشان را قطه می کنند و خود به جای آن رایانه به پاسخگویی اولیه می پردازند. تنها پس از برقراری ارتباط است که اجازه می ده رد تا داده به سمت رایانه مقصد جریان پیدا کند و تنها به بسته های داده ای مرتبط اجازه عبور می

دهند. این نوع از فایروال ها 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.

فایروال های پروکسی سرور (Proxy Server Firewall) :

فایروال های پروکسی سرور به بررسی بسته های اطلاعات در لایه کاربرد می پردازد. یک پروکسی سرور، درخواست ارائه شده توسط برنامه های کاربردی پشتش را قطه 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 آنجچایی که این فایروال ها پروتکلهای سطح کاربرد را می شناسد ، لذا می توانند بر مبنای این پروتکلها محدودیت هایی را ایجاد کنند. همچنین آنها می توانند با بررسی محتوی بسته های داده ای به ایجاد محدودیت .های لازم بپردازند. البته این سطح بررسی می تواند به کندی این فایروال ها بیانجامد

فیلترهای Nosstateful Packet:

این فیلتر ها روش کار ساده ای دارند. آنها بر مسیر یک شبکه می نشیند و با استفاده از مجموعه ای از قواعد، به بعضی بسته ها اجازه عبور می دهند و بعضی دیگر را بلوکه می کنند. این تضمین ها با توجه به اطلاعات

آدرس دهی موجود در پروتکلهای لایه شبکه مانند IP و در بعضی با توجه به اطلاعات موجود در پروتکلهای لایه انتقال مانند سرآیند های TCP و UDP اتخاذ می شوند.

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.

فیلترهای Stateful Packet :

این فیلترها بسیار باهوشتر از فیلترهای ساده هستند. آنها تقریبا تمامی ترافیک ورودی را بلوکه می کنند. اما می توانند به ماشین های پشتشان اجازه بدهند تا به پاسخگویی بپردازند. آنها این کار را با نگهداری رکود اتصالاتی که ماشینهای پشتشان در لایه انتقال ایجاد می کنند، انجام می دهند. این فیلتر ها، مکانیزم اصلی .مورد استفاده ، جهت پیاده سازی فایروال در شبکه های مدرن هستند

این فیلتر ها 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 لایه کاربرد، مانند FTP و HTTP را تشخیص دهند و لذا می توانند اعمال کنترل دسترسی را با توجه به نیاز ها و سرعت این پروتکلها انجام دهند.

فایروال های شخصی

فایروال های شخصی ، فایروال هایی هستند که بر روی رایانه های شخصی نصب می شوند. آنها برای مقابله با جملات شبکه ای طراحی شده اند. معمولا از برنامه های در حال اجرا در ماشین آگاهی دارند و تنها به ارتباط ایجاد شده توسط این برنامه ها اجازه می دهند که به کار بپردازند. نصب یک فایروال شخصی بر روی یک کامپیوتر شخصی 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.
شایان ذکر است که معمولا نیازی به تغییر برنامه جهت عبور از فایروال شخصی نصب شده (همانند پروکسی) نیست.

ادامه آموزش در مقالات بعدی منتشر خواهد شد.

برای دانلود مقالات بعدی به لینک زیر مراجعه فرمایید :

http://hazyoon.ir/category/%D8%B4%D9%80%D9%80%D9%80%D8%A8%D9%80%D9%80%D9%80%D9%80%DA%A9%D9%80%D9%80%D9%80%D9%80%D9%80%D9%87/%D8%A7%D9%85%D9%86%DB%8C%D8%AA%20%D8%B4%D8%A8%DA%A9%D9%87/

موفق و پیروز باشید.