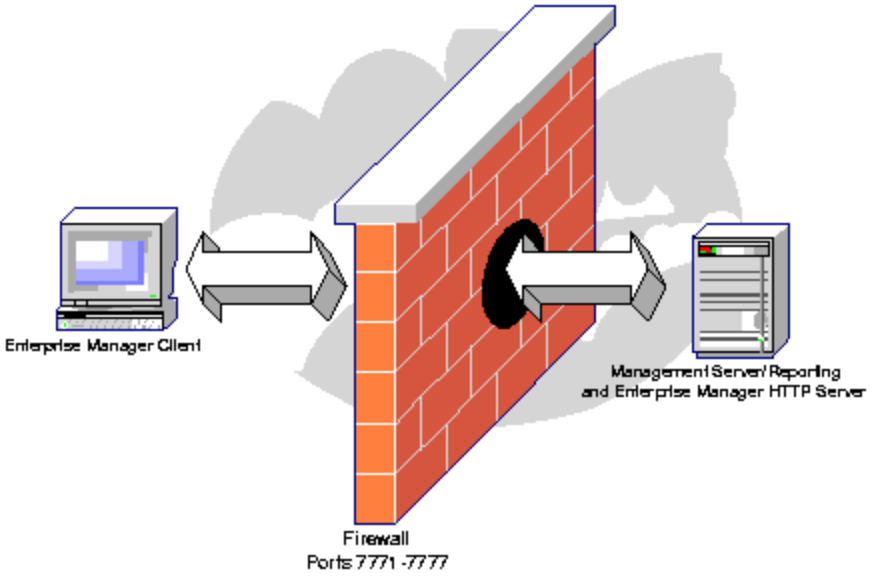

فایروال چیست ؟

موضوع : امنیت شبکه > فایروال > بخش یک

نویسنده : سینا احمدی نشاط

تاریخ انتشار : 2 مرداد 92

ایمیل : Encoder@programmer.net

وب سایت شخصی : http://hazyoon.ir

فروم امنیتی آشیانه : http://ashiyane.org

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 فایروال بر سر راه ورودی یک شبکه قرار میگیرد ، برای ترجمه آدرس شبکه نیز بکار گرفته می شود

فایروال چیست ؟

فایروال دستگاهی است که در صورت دستیابی سایرین به سیستم شما ، کامپیوتر شما دارای استعداد بمراتب بیشتری در قمابل انواع تهاجمات می باشد. شما می توانید با استفاده و نصب یک فایروال، محدودیت لازم در خصوص دستیابی به کامپیوتر و اطلاعات را فراهم نمایید.

فایروال چه کار می کند؟

فایروال 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 نماید. 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 یا مودم های کابلی استفاده می نمایند ، بسیار حیاتی و مهم می باشد

چه نوع فایروال هایی 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 (یا شبکه) و کابل و خط DSL قرار خواهند گرفت . تعداد زیادی از تولیدکنندگان و برخی از مراکز آی اس پی دستگاه هایی 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 از یک دستگاه کامپیوتر نیز وجود دارد) در صورتی که شما صرفاً دارای یک کامپیوتر پشت فایروال می باشید و یا این اطمینان را دارید که سایر Patch کامپیوترهای موجود بر روی شبکه نسبت به نصب تمامی ، ها ، دقیق بوده و عاری از ویروس ها می باشند ضرورتی به استفاده از یک سطح اضافه حفاظتی (یک نرم افزار فایروال) نخواهید داشت . فایروال های سخت افزاری ، دستگاه های سخت افزاری مجزائی می باشند که دارای سیستم عامل اختصاصی خود می باشند . بنابراین بکارگیری آنان .باعث ایجاد یک لایه دفاعی اضافه در مقابل تهاجمات می گردد

فایروال های نرم افزاری :

برخی از سیستم عامل ها 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 نمایید). 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 سی دی یا دی وی دی مربوطه استفاده گردد.

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

توانایی ثبت و اخطار :

ثبت وقایع یکی از مشخصه های بسیار مهم یک فایروال به شمار می رود 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 به راحتی به بخش های 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

بازدید حجم بالایی از بسته های اطلاعات

یکی از تستهای یک فایروال، توانایی آن در بازدید حجم بالایی از بسته های اطلاعاتی بدون کاهی 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

دانرد. بیشترین محدودیتها از طرف سرعت پردازنده و بهینه سازی کد نرم افزار بر کارایی فایروال تحمیل می شوند. عامل محدود کننده دیگر می تواند کارتهای واسطی باشد که بر روی فایروال تثب می شوند . فایروالی که بعضی کارها مانند صدور اخطار ، کنترل دسترسی مبنی یو آر ال و بررسی وقایع ثبت شده را به نرم افزار های دیگر می سپارد از سرعت و کارایی بیشتر و بهتری برخوردار است.

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 ها می شود به پیکربندی غلط فایروال برمی گردد. لذا پیکربندی سریع و ساده یک فایروال ، امکان بروز خطا را کم می کند. برای مثال امکان نمایش گرافیکی معماری شبکه و یا بزاری که بتواند سیاستهای امنیتی را به پیکربندی تبدیل کند ، برای یک فایروال ، بسیار مهم است.

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.

امنیت سیستم عامل فایروال:اگر نرم افزار فایروال بر روی سیستم عامل جداگانه ای کار میکند ، 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

دسترسی امن به فایروال جهت مقاصد مدیریتی : یک فایروال باید مکانیزهای 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.

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%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.