به دلیل بیماری و همچنین سورپرایز چند روزی نمیتونم ویدیو تولید کنم از همگی عذرخواهی میکنم

ارسال پیام خصوصی ()

() () () مشاهده پروفایل (http://itpro.ir/profiles/unity)

امتیازات این مطلب

۱- UNITY

۷۳۵ امتیاز

مشاهده پروفایل (http://itpro.ir/profiles/unity)

مقاله: تفاوت فایروال نرم افزاری و سخت افزاری ()

زمان ارسال: ۵۴ ماه قبل جزیره امنیت اطلاعات و ارتباطات ()

پسندها (۲۱ نفر) ۳۴۱۳ بازدید

-آ آ +آ () () () ()

در اصطلاح کامپیوتری واژه فایروال به سیستمی اطلاق می شود که شبکه خصوصی یا کامپیوتر شخصی شما را در مقابل نفوذ مهاجمین ، دسترسی های غیرمجاز ، ترافیک های مخرب و حملات هکر (http://itpro.ir/gotorel/technichaltext/۳۱۰۱۰)ی خارج از سیستم شما محافظت می کند . فایروال ها می توانند ترافیک ورودی به شبکه را کنترل و مدیریت کرده و با توجه به قوانینی که در آنها تعریف می شود به شخص یا کاربر خاصی اجازه ورود و دسترسی به یک سیستم خاص را بدهند . مثلا شما می توانید برای فایروال خود که از یک شبکه بانکی محافظت می کند با استفاده از قوانینی که در آن تعریف می کنید بخواهید که به کاربر X در ساعت Y اجازه دسترسی به کامپیوتر Z را که درون شبکه داخلی شما قرار دارد را بدهد .

قوانینی که در یک فایروال وجود دارد بر اساس نیازمندی های امنیتی یک سازمان تعیین می شود . برای مثال اگر فایروال بر اساس قوانینی که در آن تعیین شده تشخیص دهد که ترافیکی که از آن عبور می کند برا شبکه مضر است ، بلافاصله آنرا بلوکه می کند و از ورود آن به شبکه جلوگیری به عمل می آورد . روش هایی که یک فایروال توسط آنها ترافیک را مدیریت می کند به ترتیب روش فیلترینگ بسته یا Packet Filtering ، پروکسی سرور و یا Stateful Inspection هستند . فایروال ها می توانند هم بصورت نرم افزاری و هم بصورت سخت افزاری وجود داشته باشند اما نقطه ایده آل یک فایروال ، یک فایروال ترکیبی سخت افزاری و نرم افزاری است .

فایروال های سخت افزاری معمولا بصورت زیر ساخت هایی هستند که توسط شرکت های تولید کننده بر روی بورد های سخت افزاری نصب و راه اندازی شده اند و معمولا در قالب یک روتر در شبکه فعالیت می کنند ، یک روتر نیز می تواند در یک شبکه به عنوان یک فایروال سخت افزاری فعالیت کند . یک فایروال سخت افزاری می تواند بصورت پیش فرض و بدون انجام هرگونه تنظیمات اولیه در حد مطلوبی از ورود داده ها و ترافیک ناخواسته به شبکه محافظت کرده و اطلاعات ما را ایمن نگه دارد . اینگونه فایروال های معمولا در قالب فیلترینگ بسته یا Packet Filtering فعالیت می کنند و Header های مربوط به مبدا و مقصد (Source & Destination) بسته ها را به دقت بررسی کرده و در صورتیکه که محتویات بسته با قوانینی که در فایروال انجام شده است مقایرت داشته باشد بلافاصله از ورد آن به شبکه جلوگیری کرده و آنرا بلوکه می کند . بسته اطلاعاتی در صورتیکه مقایرتی با قوانین موجود در فایروال نداشته باشد به مقصد مورد نظر هدایت خواهد شد . راحتی کار با فایروال های سخت افزاری این است که هر کاربر ساده ای ممکن است براحتی بتواند آنرا در شبکه قرار داده و از تنظیمات پیشفرض انجام شده در آن استفاده کند ، تنها بعضی از تنظیمات پیشرفته امنیتی در اینگونه فایروال ها هستند که نیاز به داشتن دانش تخصصی فراوان برای انجام دادنشان دارند . اما این را در نظر داشته باشید که فایروال های سخت افزاری می بایشت توسط یک کارشناس متخصص امنیت آزمایش شده تا از کارکرد آنها اطمینان حاصل شود . فایروال های سخت افزاری بار ترافیکی و لود کاری کمتری برای شبکه ایجاد می کنند و طبیعتا سرعت و کارایی بهتری در شبکه دارند اما از نظر هزینه بیشتر از فایروال های نرم افزاری هزینه دارند .

فایروال های نرم افزاری در حقیقت نرم افزار هایی هستند که بر روی سیستم عامل ها نصب شده و ترافیک ورودی و خروجی به شبکه یا سیستم عامل را کنترل می کنند . اینگونه فایروال های بیشتر استفاده های خانگی و سازمان ها و شرکت های کوچک و متوسط را به خود اختصاص داده اند . فایروال های نرم افزاری سیستم ها را از خطرات معمولی که در اینترنت وجود دارند اعم از دسترسی های غیر مجاز ، ترجان ها و کدهای مخرب ، کرم های کامپیوتری و بسیاری دیگر از این موارد حفاظت می کنند . اکثر اینگونه فایروال ها به کاربارن این قابلیت را می دهند که بتوانند برای به اشتراک گذاشتن منابع خود از جمله پرینتر و پوشه ها در قوانین فایروال تغییرات دلخواه خود را اعمال کرده تا بتوانند از امکاناتی که مد نظر دارند استفاده و بهره کافی را ببرند . در برخی اوقات فایروال های نرم افزاری ابزارهای جانبی را در اختیار ما قرار می دهند که توسط آنها میتوانید تنظیمات محرمانگی و فیلترینگ خاصی را برای خود یا کاربران دیگر اعمال کنید . اینگونه فایروال ها در دو نوع شبکه ای و تک محصولی ارائه می شوند ، فایروال های نرم افزاری تحت شبکه می توانند یک شبکه را تحت کنترل خود گرفته و از آن محافظت کنند اما فایروال های تک محصولی صرفا بر روی یک سیستم عامل نصب می شوند و می توانند از آن محافظت کنند ، تصور کنید که شما ۲۰۰ کامپیوتر در شبکه خود داشته باشید و بخواهید از یک محصول فایروال تک محصولی استفاده کنید !!! ۲۰۰ بار نصب بر روی کلی شبکه می تواند بسیار طاقت فرسا و مشکل یاشد . تنوع فایروال های نرم افزاری بسیار زیاد است اما همیشه در نظر داشته باشید که بهترین فایروال نرم افزاری فایروالی است که ضمن اینکه در پس زمینه یا Background سیستم شما فعالیت کند از کمترین منابع سیستمی استفاده کند و بار سیستم را زیاد نکند . فایروال های نرم افزاری ترافیک و لود کاری بیشتری در شبکه ایجاد می کنند اما به نسبت فایروال های سخت افزاری از هزینه قابل قبولتری برخوردارند .

خلاصه :

- فایروال های سخت افزاری بصورت ابزارهایی بر روی برد های سخت افزاری نصب شده اند ، روتر نیز می تواند در نقش یک فایروال عمل کند .
- فایروال های نرم افزاری ، برنامه هایی هستند که بر روی هر سیستم عامل می توانند نصب شده و شروع بکار کنند و هم بصورت شبکه ای و هم بصورت تک محصولی می توانند مورد استفاده قرار بگیرند .
- بصورت پیشفرض شما می تواند از تنظیمات پیشفرض فایروال های سخت افزاری و نر م افزاری برای محافظت از شبکه خود استفاده کنید .
- فایروال سخت افزاری نیز در حقیقت نوعی فایروال نرم افزاری میتواند باشد که بر روی یک برد سخت افزاری نصب شده است.
- فایروال های سخت افزاری سرعتت و کارایی بیشتری نسبت به فایروال های نرم افزاری دارند .
- هزینه پیاده سازی و استفاده از فایروال های نرم افزاری بسیار کمتر از فایروال های سخت افزاری است.
- برای داستن بهترین کارایی در شبکه همیشه می بایست از اینگونه فایروال های بصورت ترکیبی استفاده کرد .

نویسنده : محمد نصیری

منبع : انجمن حرفه ای های فناوری اطلاعات ایران (http://www.itpro.ir)

هرگونه نشر و کپی غیر مجاز از نظر اخلاقی غیر مجاز می باشد