" Firewall "

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

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

۱. توانایی ثبت و اخطار :ثبت وقایع یکی از مشخصه های بسیار مهم یک Firewall به شمار می شود و به مدیران شبکه این امکان را می‌دهد 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 Firewall خوب باید بتواند علاوه بر ثبت وقایع، در شرایط بحرانی، مدیر شبکه را از وقایع مطلع کند و برای وی اخطار بفرستد.

۲. بازدید حجم بالایی از بسته های اطلاعات: یکی از تستهای یک Firewall ، توانایی آن در بازدید حجم بالایی از بسته های اطلاعاتی بدون کاهش چشمگیر کارایی شبکه است. حجم داده ای که یک Firewall می تواند کنترل کند برای شبکه های مختلف متفاوت است اما یک Firewall قطعا نباید به گلوگاه شبکه تحت حفاظتش تبدیل شود.عوامل مختلفی در سرعت پردازش اطلاعات توسط Firewall نقش دارند. بیشترین محدودیتها از طرف سرعت پردازنده و بهینه سازی کد نرم افزار بر کارایی Firewall تحمیل می شوند. عامل محدودکننده دیگر می‌تواند کارتهای واسطی باشد که بر روی Firewall نصب می‌شوند. Firewall 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.

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

۴. امنیت و افزونگی Firewall: امنیت Firewall خود یکی از نکات مهم در یک شبکه امن است.Firewall ای 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 Firewall ، تامین کننده امنیت Firewall و شبکه است:

- ☑ امنیت سیستم عامل Firewall : اگر نرم افزار Firewall بر روی سیستم عامل جداگانه ای کار می‌کند، نقاط ضعف امنیتی سیستم عامل ، می تواند نقاط ضعف Firewall نیز به حساب بیاید. بنابراین امنیت و استحکام سیستم عامل Firewall و بروزرسانی آن از نکات مهم در امنیت Firewall است.
- ☑ دسترسی امن به Firewall جهت مقاصد مدیریتی : یک Firewall 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 Firewall :

انواع مختلف Firewall کم و بیش کارهایی را که اشاره کردیم ، انجام می‌دهند، اما روش انجام کار توسط انواع مختلف ، متفاوت است که این امر منجر به تفاوت در کارایی و سطح امنیت پیشنهادی Firewall می‌شود.بر این اساس Firewall را به ۵ گروه تقسیم می کنند.

۱. Circuit Level Firewall :

این Firewall 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 می‌دهند تا داده به سمت رایانه مقصد جریان پیدا کند و تنها به بسته های داده ای مرتبط اجازه عبور می دهند. این نوع ازFirewall هیچ داده درون بسته های اطلاعات را مورد بررسی قرار نمی‌دهند و لذا سرعت خوبی دارند. ضمنا امکان ایجاد محدودیت بر روی سایر پروتکلها (غیر از TCP) را نیز نمی دهند.

۲. Proxy Server Firewall :

Proxy Server Firewall به بررسی بسته های اطلاعات در لایه کاربرد می‌پردازد. یک پروکسی سرور درخواست ارائه شده توسط برنامه های کاربردی پشتش را قطع می کند و خود به جای آنها درخواست را ارسال می‌کند.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 Firewall پروتکلهای سطح کاربرد را می‌شناسد ، 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 می‌تواند به کندی این Firewall بیانجامد. همچنین از آنجایی که این Firewall باید ترافیک ورودی و اطلاعات برنامه های کاربردی کاربر انتهایی را پردازش کند، کارایی آنها بیشتر کاهش می یابد. اغلب اوقات Proxy Server ها از دید کاربر انتهایی شفاف نیستند و کاربر مجبور است تغییراتی را

در برنامه خود ایجاد کند تا بتواند این Firewall را به کار بگیرد.هر برنامه جدیدی که بخواهد از این نـوع Firewall عبور کند ، باید تغییراتی را در پشته پروتکل Firewall ایجاد کرد.

۳. No state full packet Filtering :

این Filter ها روش کار ساده ای دارند. آنها بر مسیر یک شبکه می‌نشینند 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 توجـه بـه اطلاعـات آدرس دهی موجود در پروتکلهای لایه شبکه مانند IP و در بعضی موارد با توجه به اطلاعـات موجـود در پروتکلهـای لایـه انتقال مانند سرآیندهای TCP و UDP اتخاذ می شود. این Filter ها زمانی می توانند به خوبی عمل کننـد کـه فهـم خوبی از کاربرد سرویسهای مورد نیاز شبکه جهت محافظت داشته باشند. همچنین این Filter ها می توانند سـریع باشند چون همانند Proxy ها عمل نمی کنند و اطلاعاتی درباره پروتکلهای لایه کاربرد ندارند.

۴. State full Packet Filtering :

این Filterها بسیار باهوشتر از Filterهای ساده هستند. آنها تقریبا تمامی ترافیک ورودی را بلوکه می کننـد امـا 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 Filterها ، مکانیزم اصـلی مـورد اسـتفاده جهت پیاده سازی Firewall در شبکه های مدرن هستند.این Filterها مـی تواننـد رد پـای اطلاعـات مختلـف را از طریق بسته هایی که در حال عبورند ثبت کنند. برای مثال شماره پورت هـای TCP و UDP مبـدا و مقـصد، شـماره ترتیب TCP و پرچمهای TCP. بسیاری از Filterهای جدید Statefull می توانند پروتکلهای لایه کاربرد مانند FTP و HTTP را تشخیص دهند و لذا می توانندداعمال کنترل دسترسی را با توجه به نیازها و سرعت این پروتکلها انجـام دهند.

۵. Personal Firewall :

Firewall های شخصی ، Firewall هایی 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 بـه ارتباطـات ایجاد شده توسط این برنامه ها اجازه می دهند که به کار بپردازند نصب یک Firewall شخصی بـر روی یـک PC بسیار مفید است زیرا سطح امنیت پیشنهادی توسط Firewall شبکه را افزایش می دهد. از طرف دیگـر از آنجـایی که امروزه بسیاری از حملات از درون شبکه حفاظت شده انجام می شوند ، Firewall شبکه نمی تواند کاری برای آنها انجام دهد و لذا یک Firewall شخصی بسیار مفید خواهد بود. معمولا نیازی بـه تغییـر برنامـه جهـت عبـور از Firewall شخصی نصب شده (همانند Proxy) نیست.

موقعیت یابی برای Firewall :

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 می‌کنند 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 لایه ای : 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 می‌دهد.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.