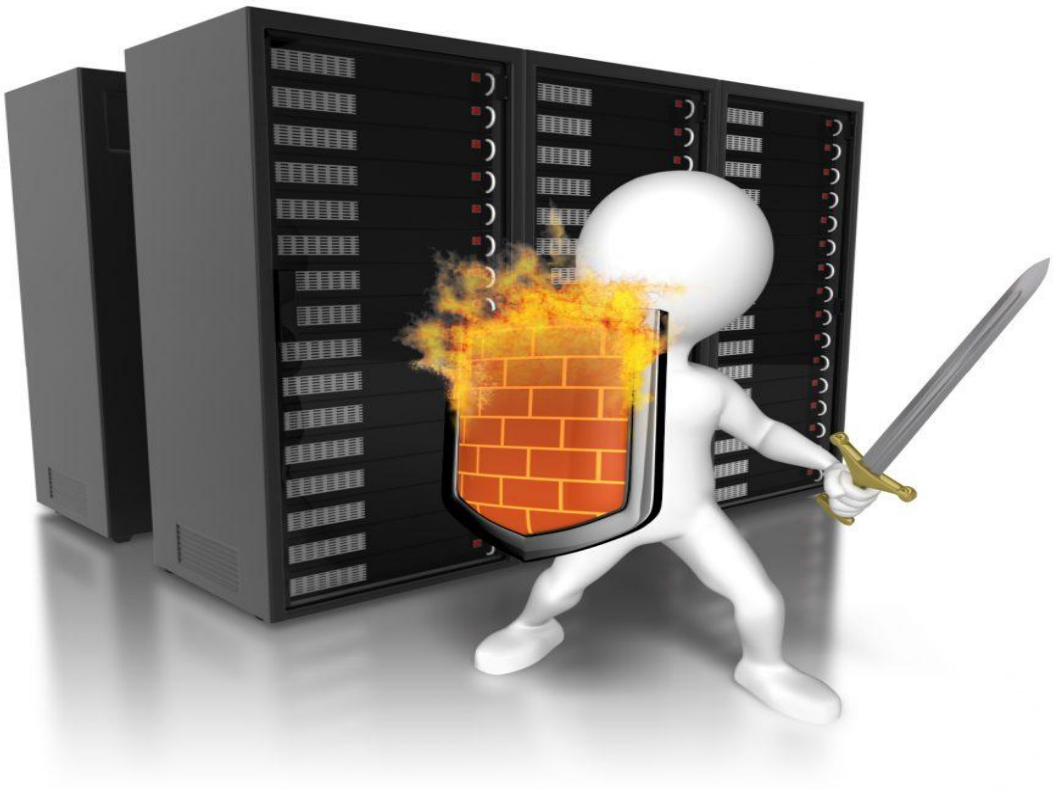
فایروال چیست و چه کاربردهایی دارد؟

یکی از سؤال‌های رایج در حوزه‌ی شبکه این است که فایروال چیست و چه کاربردهایی دارد؟ اصلاً چه لزومی در استفاده از فایروال است؟ انواع فایروال چیست؟

در این مقاله به این سؤالات پاسخ خواهیم داد و شما را با انواع فایروال و کاربردهای آن‌ها آشنا خواهیم کرد. هنگامی که حرف از اینترنت پیش می‌آید، اولین موضوعی که مطرح می‌شود امنیت است. امنیت و اینترنت دو مقوله‌ی جدانشدنی از همدیگر هستند. بنابراین چه کسب‌وکارهای اینترنتی و چه کاربران اینترنتی باید اهمیت بسیار زیادی به موضوع امنیت بدهند.

فایروال چیست؟

فایروال یا دیواره آتش (Firewall) به نرم‌افزار یا سخت‌افزارهایی گفته می‌شود که از دسترسی به کامپیوترها جلوگیری کرده و ترافیک رد و بدل شده در شبکه را کنترل می‌کند. فایروال در حقیقت یک ابزار امنیتی است که می‌تواند یک برنامه‌ی نرم‌افزاری یا یک دستگاه اختصاصی شبکه باشد.



هدف استفاده از فایروال چیست؟

هدف اصلی فایرول جداسازی یک داده‌ی امن از ناحیه‌ی ناامن و کنترل ارتباطات بین این دو است. فایروال می‌تواند کارهای دیگری نیز انجام دهد اما عمدتاً مسئول کنترل ارتباطات ورودی و خروجی از یک دستگاه به شبکه است.

فایروال‌ها از دسترسی غیر مجاز به شبکه‌ی خصوصی جلوگیری کرده و یک چارچوب امنیتی جامع برای شبکه‌ی شما هستند.

نحوه‌ی عملکرد فایروال

فایروال با استفاده از یک **دیوار کد،** کامپیوتر شما را از اینترنت جدا می‌کند. فایروال هر داده‌ای که می‌خواهد به کامپیوتر شما وارد شود یا از آن خارج شود را کنترل می‌کند و بررسی می‌کند که آیا اجازه‌ی عبور دارد یا باید مسدود شود؟

فایروال یکی از مهم‌ترین لایه‌های امنیتی شبکه‌های کامپیوتری بوده و عدم استفاده از آن موجب می‌شود تا هکرها به‌راحتی وارد شبکه یا کامپیوتر شخصی شما شده و بدون هیچ محدودیتی خراب‌کاری‌های خود را انجام دهند.

فایروال در حقیقت فیلتری است که داده‌ها باید از آن عبور کنند. یک خانه را تصور کنید که افرادی که می‌خواهند به آن وارد شوند یا از آن خروج کنند باید از درب خانه عبور کنند. محل قرارگیری فایروال در درب ورود و خروج داده‌ها از کامپیوتر یعنی (Gateway) است .

اگرچه فایروال‌ها دارای سیستم بسیار پیچیده‌ای هستند، اما نصب و راه‌اندازی آن‌ها بسیار آسان است.

فایروال چه‌کاری انجام می‌دهد؟

عموماً فایروال‌ها این کارها را انجام می‌دهند:

- از منابع محافظت می‌کنند.
- اجازه‌ی دسترسی مجاز می‌دهند.
- ترافیک شبکه را مدیریت و کنترل می‌کنند.
- اتفاقات را ذخیره و گزارش می‌دهند.
- نقش یک میانجی را ایفا می‌کنند.

فایروال شخصی چیست؟

بسیار مهم است که بدانیم چرا به فایروال نیز داریم و فایروال چه کمکی به افزایش امنیت ما می‌کند؟ برای پاسخ به این سؤال نیاز داریم تا با اهداف حفاظت از اطلاعات آشنا شویم؛ چون این امر به ما کمک خواهد کرد بفهمیم چگونه فایروال احتیاجات ما را برآورده می‌کند.

چرا به فایروال شخصی نیاز داریم؟

در عصر اینترنت پرسرعت، کامپیوتر شما به‌صورت الکترونیکی به شبکه‌ای گسترده متصل می‌شود. مگر این‌که یک فایروال شخصی داشته باشید و بتوانید از اطلاعات خود محافظت کنید.

اتصال با سرعت بالا هم دارای مشکلات خاص خودش است. ازقضا، همین سرعت بالا باعث آسیب‌پذیر شدن اتصال می‌شود. اتصال به اینترنت پرسرعت مثل این است که به‌سرعت از درب خانه‌ی خود خارج شوید و درب را پشت سرخود باز بگذارید.

ارتباطات اینترنتی با سرعت بالا دارای مشکلات زیر هستند:

- **وجود یک آی‌پی ثابت :**این باعث می‌شود تا مزاحمی که شما را کشف کرده است، همیشه بتواند شما را پیدا کند.
- **دسترسی با سرعت بالا :**بدین معنی که مزاحم بسیار سریع‌تر می‌تواند وارد کامپیوتر شما شود.
- **اتصال دائم :**بدین معنی که هر دفعه سیستم شما به اینترنت متصل شود، آسیب‌پذیر است.

اکنون می‌دانیم که چرا نیاز داریم هنگام استفاده از اینترنت پرسرعت از خود محافظت کنیم. فقط باید بدانیم که چگونه باید از کامپیوتر خود محافظت کنیم؟ پاسخ این سؤال استفاده از فایروال‌های شخصی است.

دلایل اهمیت فایروال شخصی

- شما همیشه در اینترنت هستید، بنابراین نیاز به فایروال دارید.
- در هر مکانی مانند پارک، کافه، فرودگاه و غیره ممکن است به شبکه وای‌فای عمومی متصل شوید.
- شبکه خانگی شما باید توسط فایروال ایمن شود.

بیشتر فایروال‌های شخصی دارای تنظیماتی هستند تا بتوانید به‌راحتی سیاست‌های امنیتی را متناسب با نیاز خودتان اجرا کنید.

دسته‌بندی فایروال‌ها

فایروال‌ها انواع مختلفی دارند که در ادامه به آن‌ها اشاره خواهیم کرد. اما فایروال‌ها عمدتاً دریکی از دودسته‌ی **فایروال‌های مبتنی بر میزبان** و **فایروال‌های مبتنی بر شبکه** قرار می‌گیرند.

فایروال‌های مبتنی بر میزبان

این فایروال‌ها بر روی سرور های شخصی نصب شده و سیگنال‌های ورودی و خروجی را نظارت می‌کنند.

فایروال‌های مبتنی بر شبکه

فایروال‌های مبتنی بر شبکه می‌توانند در زیرساخت‌های ابری ساخته شوند، یا می‌توانند سرویس فایروال مجازی باشند.

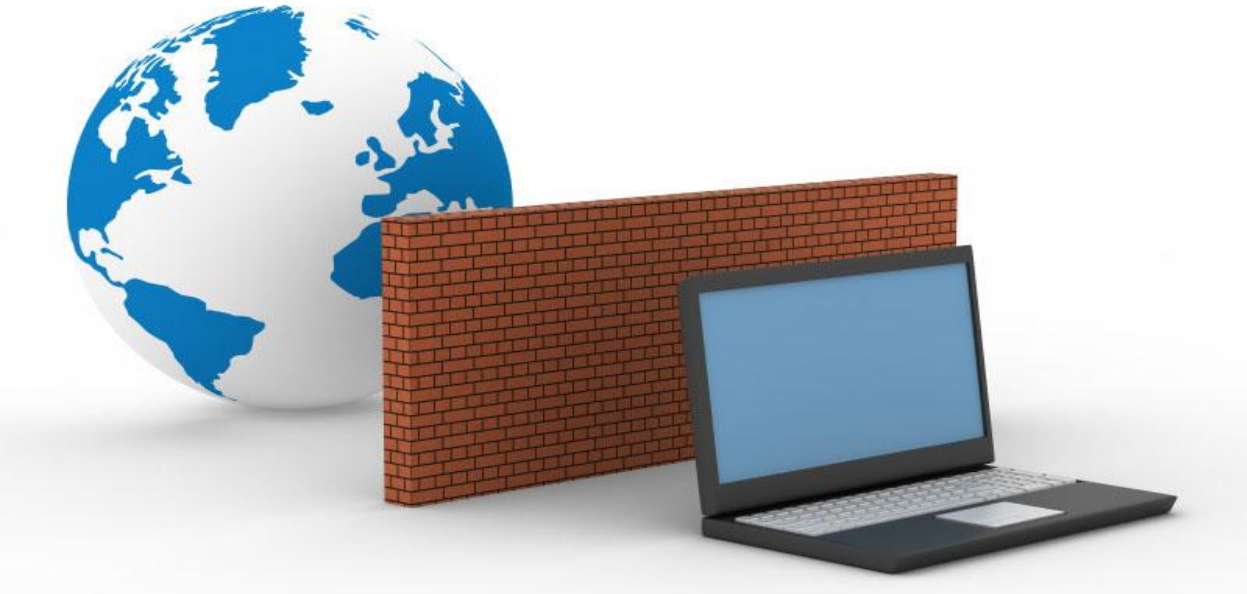
انواع فایروال

انواع مختلفی از فایروال در دنیای شبکه وجود دارند که در این قسمت به آن‌ها اشاره خواهیم کرد:

- **فایروال‌های فیلتر بسته‌ها(Packet-filtering)**

اساس کار این فایروال در بررسی بسته‌ها به‌صورت جداگانه است. هنگامی که یک بسته از این فایروال عبور می‌کند، آدرس منبع و مقصد آن و همچنین پروتکل و شماره پورت مقصد آن بررسی می‌شوند. چنانچه این بسته نتواند قوانین فایروال را رعایت کند، قطع می‌شود و به مقصد نمی‌رسد. برای مثال اگر فایروال به‌گونه‌ای تنظیم شده باشد که به دسترسی Telnet اجازه عبور ندهد، به بسته‌هایی که برای TCP پورت شماره ۲۳ طراحی‌شده باشند، اجازه‌ی عبور را نمی‌دهد.

فایروال‌های فیلتر بسته‌ها، عمدتاً بر روی لایه‌ی شبکه مدل مرجع OSI کار می‌کنند. اگرچه لایه انتقال برای به دست آوردن منبع و شماره درگاه مقصد مورد استفاده قرار می‌گیرد. این فایروال‌ها هر بسته را به‌صورت مستقل بررسی می‌کنند و نمی‌دانند که آیا هر بسته‌ی معین بخشی از جریان ترافیک موجود است یا خیر؟ این نوع فایروال‌ها تأثیرگذار هستند اما به این دلیل که هر بسته را به‌تنهایی پردازش می‌کنند، ممکن است در برابر حملات IP آسیب‌پذیر باشند. به همین دلیل عمدتاً توسط فایروال‌های stateful inspectionجایگزین می‌شوند.



- **فایروال‌های بازرسی قانونی(stateful inspection)**

فایروال‌های بازرسی قانونی به فایروال‌های فیلتر دینامیک بسته‌ها (dynamic packet-filtering) نیز معروف هستند. این فایروال دارای جدولی است که مسیر تمام ارتباطات را باز نگه می‌دارد. هنگامی‌که یک بسته‌ی جدید می‌آید، فایروال اطلاعات موجود در سربرگ (header) بسته را با جدول خود مقایسه می‌کند و تشخیص می‌دهد که آیا این ارتباط قابل انجام است یا خیر؟ چنانچه اطلاعات بسته با ارتباط فعلی مطابقت داشته باشد، بسته اجازه‌ی عبور را خواهد داشت. در غیر این صورت بسته مطابق با قوانین تنظیم شده با ارتباط جدید ارزیابی خواهد شد.

فایروال‌های stateful inspection ارتباطات را در دوره‌های زمانی رصد کرده و بسته‌های ورودی و خروجی را مورد بررسی قرار می‌دهند. تمامی بسته‌های ورودی و خروجی ردیابی شده و تنها بسته‌هایی که واکنش مناسبی نسبت به قوانین فایروال دارند مجاز به عبور خواهند بود.

اگرچه فایروال‌های stateful inspection بسیار مؤثر هستند، اما گاهی اوقات در برابر حملات (DoS) آسیب‌پذیر هستند.

- **فایروال‌های لایه کاربرد و پروکسی(Application Layer and Proxy)**

حملات به وب سرورها روزبه‌روز در حال افزایش هستند. به همین دلیل نیاز به یک فایروال قدرتمند برای محافظت از شبکه در برابر حملات به‌شدت احساس می‌شود. فایروال‌هایی که در بالا به بررسی آن‌ها پرداختیم، نمی‌توانند در میان درخواست‌های پروتکل لایه کاربردی معتبر، داده‌ها و ترافیک‌های مضر تمایز قائل شوند.

فایروال‌های لایه کاربرد می‌توانند ظرفیت انتقال بسته را بررسی کرده و در میان درخواست‌های معتبر، داده و کدهای مضر تمایز قائل شوند. ازآنجایی‌که این نوع فایروال‌ها بر اساس محتوای انتقالی کار می‌کنند، به مهندسین امنیتی کنترل دقیق‌تری نسبت به ترافیک شبکه می‌دهند و قوانین را برای اجازه یا رد درخواست اعمال می‌کنند.

قرار دادن فایروال در پروکسی سرور، کار را برای مهاجمین سخت‌تر خواهد کرد و آن‌ها نمی‌توانند به‌راحتی بفهمند که شبکه در چه مکانی قرار دارد.

رمز موفقیت فایروال‌های لایه کاربرد، توانایی آن‌ها در بلاک کردن محتوای خاص مانندmalware ها و وب‌سایت‌های خاص و همچنین تشخیص مضر بودن پروتکل‌هایی مانندHTTP ، FTPو DNS است.

فایروال‌های لایه کاربرد می‌توانند جهت کنترل اجرای فایل‌ها یا جابه‌جایی داده‌ها توسط برنامه‌های خاص نیز مورد استفاده قرار گیرند.

فایروال‌های نرم افزاری

فایروال‌های نرم‌افزاری (Software Firewall) را فایروال‌های شخصی نیز می‌نامند.

این فایروال‌ها برای راه‌اندازی در یک کامپیوتر طراحی شده‌اند. این نوع از فایروال‌ها معمولاً در خانه یا کامپیوترهای اداری کوچک مورد استفاده قرار می‌گیرند که مدت زمان زیادی به اینترنت متصل هستند. فایروال نرم‌افزاری از دسترسی ناخواسته به کامپیوتر در شبکه از طریق شناسایی و جلوگیری از ارتباط بر روی پورت‌های پر ریسک جلوگیری می‌کند.

کامپیوترها با بسیاری از پورت‌های شناخته شده ارتباط دارند. فایروال نرم‌افزاری تمایل دارد که این ارتباط بدون این‌که به کاربر هشدار یا اخطار دهد، انجام گیرد. برای مثال، کامپیوترها به صفحات وب از طریق پورت ۸۰ دسترسی دارند و از پورت ۴۴۳ برای ایجاد امنیت ارتباط استفاده می‌کنند. یک کامپیوتر خانگی انتظار دارد که دیتا را از طریق این پورت‌ها دریافت کند. یک فایروال نرم‌افزاری به‌احتمال زیاد هرگونه دسترسی را از طریق پورت ۴۲۱

مسدود می‌کند؛ چون کامپیوتر خانگی انتظاری جهت دریافت دیتا از پورت ۴۲۱ را ندارد. علاوه بر این، پورت ۴۲۱ در گذشته توسط **تروجان‌ها** مورد استفاده قرار می‌گرفت.

فایروال‌های نرم‌افزاری توانایی شناخت فعالیت‌های مشکوک از خارج را نیز دارند. آن‌ها می‌توانند دسترسی به کامپیوتر خانگی را از آدرس‌های خارجی مسدود کنند .فایروال‌های نرم‌افزاری همچنین به برنامه‌های خاص کامپیوتری اجازه‌ی اتصال به اینترنت را می‌دهند. البته پیش از اتصال از کاربر مجوز این کار را می‌گیرند. آپدیت ویندوز، آنتی ویروس و مایکروسافت ورد (word)برنامه‌هایی هستند که کاربران انتظار دارند دائماً به اینترنت متصل باشند.

یکی از مشکلات فایروال‌های نرم‌افزاری این است که روی سیستم‌عامل کامپیوتر شخصی کار می‌کنند. چنان‌چه سیستم‌عامل در خطر باشد، فایروال هم به خطر می‌افتد .از آنجا که بسیاری از برنامه‌های دیگر نیز بر روی یک کامپیوتر خانگی اجرا می‌شوند، نرم‌افزارهای مخرب می‌توانند از طریق برنامه‌ی دیگری وارد کامپیوتر شوند و فایروال را به خطر بیندازند. فایروال نرم‌افزاری به‌شدت به تصمیمات کاربر وابسته است. اگر کاربر به اشتباه از یک Keylogger یا تروجان برای ورود به اینترنت استفاده کند، با وجود فایروال باز هم ممکن است امنیت آن دستگاه به‌خطر بیفتد.

فایروال های سخت افزاری

فایروال‌های سخت‌افزاری (Hardware Firewall) از پیچیدگی بیشتری نسبت به فایروال‌های نرم‌افزاری برخوردار هستند. آن‌ها دارای اجزای نرم‌افزاری هم هستند اما یا روی یک دستگاه از شبکه‌ای خاص طراحی شده‌اند، یا روی یک سرور وجود دارند که به اجرای فایروال اختصاص داده شده است.

سیستم‌عاملی که مجهز به فایروال سخت‌افزاری است، تا حد ممکن ساده بوده و هیچ نرم‌افزار دیگری بر روی آن نصب نمی‌شود. به همین دلیل حمله کردن به آن بسیار مشکل است. فایروال سخت‌افزاری بین یک شبکه (مانند شرکت) و یک ناحیه‌ی دارای امنیت کمتر دیگر)مانند اینترنت) قرار می‌گیرد. این فایروال‌ها می‌توانند شبکه‌های امن‌تر را از شبکه‌های نا امن‌تر جدا کنند.

البته فایروال‌های سخت‌افزاری فقط مخصوص شبکه‌های شرکتی نیستند و افرادی که می‌خواهند از کامپیوترهای شخصی و خانگی خود حفاظت بیشتری کنند، می‌توانند از فایروال‌های سخت‌افزاری استفاده کنند. در صورت استفاده از فایروال‌های سخت‌افزاری برای کامپیوترهای خانگی باید پیکربندی پیش‌فرض آن‌ها را تنظیم کرد. چون پیکربندی برخی از آن‌ها ممکن است به‌گونه‌ای باشد که اجازه نداشته باشند با خارج ارتباط داشته باشند. تنظیمات ممکن است به‌گونه‌ای باشند که به‌سادگی اجازه‌ی عبور از پورت ۸۰ را در هر دو جهت بدهند، یا برعکس اجازه‌ی عبور هیچ اطلاعاتی را ندهند. از نمونه‌های فایروال‌های سخت‌افزاری خانگی می‌توان Linksys را نام برد.

فایروال‌ها در پروتکل (NAT) هم استفاده می‌شوند .این امر به شبکه اجازه می‌دهد از آی‌پی آدرس‌های خصوصی استفاده کند که در اینترنت مسیریابی نشده‌اند. آی‌پی آدرس‌های خصوصی به سازمان‌ها (یا حتی شبکه‌های خانگی) اجازه می‌دهند تا تعداد آی‌پی آدرس‌های که مورد استفاده قرار می‌گیرند را محدود کنند. آن‌ها همچنین آدرس‌های عمومی برای سرورهای وب و دیگر تجهیزات شبکه را محافظت می‌کنند.

پروتکل (NAT) به مدیران اجازه می‌دهد که از یک آی‌پی آدرس عمومی برای تمام کاربرانشان استفاده کنند و به اینترنت متصل شوند. فایروال‌ها آن‌قدر هوشمند هستند که درخواست‌ها را به آی‌پی داخلی درخواست کننده ارسال کنند. پروتکل (NAT) همچنین به کاربران درون یک شبکه اجازه می‌دهد که به یک سرور با استفاده از یک آی‌پی خصوصی متصل شوند. درحالی‌که کاربران خارج از شبکه اگر بخواهند به همان سرور متصل شوند باید از آی‌پی خارجی استفاده کنند.

علاوه بر پورت و آی‌پی آدرس، فایروال‌ها کارهای دیگری نیز انجام می‌دهند. آن‌ها می‌توانند نقش caching server، VPN، روتر و غیره را بازی کنند. نمونه‌هایی از فایروال‌های سخت‌افزاری CheckPoint ، Cisco PIX، SonicWall و Contivity from Nortel هستند.

نمونه‌ای از فایروال سخت‌افزاری شرکت CISCO

نتیجه گیری

استفاده از فایروال برای مدیریت شبکه یک امر حیاتی است. بدون فایروال شبکه‌ها نمی‌توانند داده‌ها و اطلاعات حساس خود را برای بازیابی انتخابی ذخیره کنند. فایروال از کامپیوتر و شبکه‌ی شما در برابر حملات مختلف محافظت می‌کند. شرکت‌ها و سازمان‌ها، شبکه‌ها و کامپیوترهای خانگی باید به فایروال مجهز شوند تا ریسک از دست رفتن اطلاعات کاهش بیابد. بنابراین به‌هیچ عنوان لزوم استفاده از فایروال را نادیده نگیرید.