انواع فایروال:

فایروال‌ها به سه نوع "لایه شبکه"، "لایه اپلیکیشن یا کاربردی" و "فایروال پراکسی" از لحاظ نحوه عملکرد تقسیم می‌شوند که کاربر می‌تواند در یک زمان از همه یا هیچ کدام از آن‌ها استفاده کند:

* دیوار آتش لایه شبکه یا فیلتر بسته‌ها (Network layer or packet filters):

فایروال‌های شبکه (Network Firewall) یا فیلتر بسته‌ها نوعی دیوار آتش هستند که تنها وظیفه دارند تا با توجه به سربرگ (Header) پکت‌های TCP/IP و مقایسه معیارهای خود با اطلاعاتی نظیر آدرس IP فرستنده ویا گیرنده، پورت انتقالی فرستنده ویا گیرنده، زمان دریافت، نوع سرویس (ToS) و پارامترهای مشابه تصمیم به عبور دادن و مسیر دهی بسته‌ها بگیرد یا آن‌ها را بلاک کند. فایروال لایه شبکه می‌تواند تا حداکثر چهار لایه (از ۱ تا ۴) از مدل OSI را فیلتر کند. از مرحله یک تا سوم که لایه فیزیکی تا شبکه است و لایه چهارم (انتقال) که برای فهمیدن پورت مقصد استفاده می‌کند.

در این نوع، فایروال هیچ کاری به محتوای بسته‌های ارسالی یا دریافتی نداشته و فقط طبق سربرگ‌ها و هدرهای بسته‌ها تصمیم گیری می‌کند. مثلاً بسته‌هایی که فقط در هدر آن‌ها ذکر شده باشد که به پورت ۸۰ (پورت وب یا HTTP) فرستاده شوند را اجازه عبور دهد. این نوع فایروال‌ها معمولاً به دلیل این که مقایسات کلی را انجام نمی‌دهند، سرعت بسیار بالاتری نسبت به سایر دیوارهای آتش دارند. اینگونه فایروال را تقریباً می‌توان در هر دستگاه شبکه‌ای مثل مسیریاب‌ها (روترها - Routers)، سوئیچ‌ها (Switches) و ... یافت.

* فایروال لایه کاربرد (Application firewall):

فایروال‌های لایه کاربردی (Application Firewalls) می‌توانند کل یک بسته را آنالیز کنند که شامل سربرگ‌ها و محتوای آن است. برعکس فایروال لایه شبکه که به محتوا کاری نداشت، در این نوع فایروال فیلتر اصلی بر روی محتوای پکت‌ها داده اعمال می‌شود بنابراین می‌توان گفت که این فایروال می‌تواند در تمامی لایه‌های مدلینگ OSI کار کند یعنی ۷ لایه. از لایه ۱ تا ۴ که عمل مسیریابی و انتقال انجام می‌شود و از لایه ۵ تا ۷ نیز که لایه محتوای داده‌هاست. به همین دلیل این نوع فایروال می‌تواند بسیار امن تر و قابل اعتماد تر باشد.

فهمیدیم که هدرهای بسته‌ها چگونه بررسی می‌شوند حال به بررسی و فیلترینگ محتوای بسته‌ها می‌پردازیم. می‌دانیم که بخش اصلی پکت‌ها همان محتوای آن است پس این همان قسمت است که باید آنالیز شود. منظور از محتوای پکت‌ها همان داده‌هایی هستند که درحال انتقال اند مثلاً ممکن است داده‌های مربوط به یک فایل، صفحه اینترنتی، ایمیل و ... باشد. این نوع فایروال‌ها قابلیت ایجاد معیارهای فیلترینگ دارند که محتوا و هدرهای بسته‌ها را طبق آن معیارها فیلتر کند. مثلاً فرض کنید که این داده‌ها خود آلوده باشند (یعنی فایلی که منتقل می‌شود ویروسی باشد) در اینجاست که برخی از فایروال‌های لایه کاربرد به بررسی و فیلتر کردن این داده‌ها می‌پردازد. از جمله این فایروال‌های اسکنر می‌توان به بخشی از اینترنت سکیوریتی‌ها اشاره کرد.

طبیعی است که چک کردن کل محتوای منتقل شده زمان بر است بنابراین سرعت کار این نوع فایروال‌ها نیز کند است. از جمله فایروال‌های لایه اپلیکیشن می‌توان ویندوز فایروال (Windows Firewall)، کومودو (Comodo) و ... را نام برد.

* فایروال‌های پراکسی (Proxies):

سرورهای پراکسی (یا پروکسی - Proxy) نوعی رابط بین یک شبکه و یک شبکه دیگر یا یک کاربر و اینترنت است که برای مواردی نظیر حفظ امنیت، پنهان کردن هویت و ... استفاده می‌شود در واقع کاربر بجای این که درخواست خود را مستقیماً به یک شبکه یا یک سرور دیگر در اینترنت بفرستد و پاسخ آن را نیز مستقیماً دریافت کند، آن را به یک سرور به نام پراکسی فرستاده و سرور پراکسی آن بسته را به مقصد اصلی می‌رساند. در هنگام دریافت پاسخ نیز ابتدا به سرور پراکسی فرستاده شده و پراکسی در صورت نیاز پردازش‌هایی را بر روی آن انجام داده و به کاربر اصلی بر می‌گرداند.

فایروال‌ پراکسی یا پروکسی (Proxy Firewalls) نوعی از فایروال‌هاست که بر روی سرور پراکسی اجرا می‌شود و کاربر با وصل شدن به آن، در واقع به یک فایروال وصل شده است چون همه داده‌های رد و بدل شده از سرور پراکسی می‌گذرد و ما یک فایروال پراکسی بر روی آن نصب کرده‌ایم، داده‌ها در طول مسیر انتقال فیلتر خواهند شد. این نوع فایروال معایب خود را نیز دارد از جمله آن که می‌توان داده‌ها را در طول مسیر بین پراکسی و کاربر یا پراکسی و اینترنت دزدید یا سایر حملات را بر روی آن عملی کرد. درصورتی که ارتباط بین کاربر و فایروال پراکسی رمزگذاری شده باشد، این احتمال به حداقل خود خواهد رسید.

منابع این بخش: ویکی‌پدیا، وبسایت سیسکو و [NetworkWorld](http://www.networkworld.com/article/2255950/lan-wan/chapter-1--types-of-firewalls.html)