**فایروال چیست؟**

فایروال چیست؟ فایروال نوعی ابزار [امنیتی سایبری](https://softyab.com/product-category/security/antivirus/) است که شبکه و یا کامپیوتر شخصی شما را در مقابل نفوذ مهاجمین، دسترسی‌های غیرمجاز، ترافیک‌های مخرب و حملات هکرها محافظت کند. نحوه عملکرد فایروال‌ها به اینگونه است که بسته‌ها را بین شبکه‌ها رد و بدل و مسیریابی (Route) می‌کنند. فایروال هم ترافیک ورودی به شبکه و هم ترافیک خروجی از آن را کنترل و مدیریت کرده و با توجه به قوانینی که در آنها تعریف می‌شود به شخص یا کاربر خاصی اجازه ورود و دسترسی به یک سیستم خاص را می‌دهد. مثلا شما می‌توانید برای فایروال خود که از یک شبکه بانکی محافظت می‌کند با استفاده از قوانینی که در آن تعریف می‌کنید 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 قرار دارد بر اساس نیازهای امنیتی یک سازمان و شرکت تعیین می‌شود. ترافیکی می‌تواند اجازه ورود و خروج را داشته باشد که منطبق بر سیاست‌های امنیتی فایروال باشد و بقیه ترافیک غیر مجاز است.

پس کار فایروال چیست؟ اگر فایروال بر اساس قوانینی که در آن تعیین شده تشخیص دهد که ترافیکی که از آن عبور می کند برای شبکه مضر است، بلافاصله آن را بلوکه می‌کند و از ورود آن به شبکه جلوگیری می‌کند.

تفاوت inbound و outbound در فایروال چیست؟ به ترافیک ورودی به فایروال، ترافیک inbound گفته می‌شود و برای آن باید inbound rule تنظیم شود. به ترافیک خروجی از فایروال، ترافیک outbound گفته می‌شود و برای آن باید outbound rule تنظیم شود. این قوانین در access control list – لیست فایروال تعریف می‌شوند.

**نحوه عملکرد فایروال چیست؟**

1. فایروال، ترافیک را از ورودی‌های خود که هر کدام به یک شبکه متصل است، دریافت می‌کند و آن را با معیارهای تعیین شده بر روی خود مقایسه و بر اساس این معیارها تصمیم‌گیری می‌کند .
2. فایروال بسته‌ها را بین شبکه‌ها رد و بدل و مسیریابی و روتینگ می‌کند.
3. فایروال می‌تواند هم ترافیک ورودی (Inbound) و هم ترافیک خروجی (Outbound) را مدیریت و فیلتر کند.
4. این نرم افزار دسترسی عمومی از طریق شبکه‌های بیرونی را به منابع داخلی مانند اتوماسیون اداری یا مثل آن را مدیریت می‌کند.
5. تمامی درخواست‌های دسترسی به شبکه داخلی را لاگ برداری کرده و در صورت مشاهده مورد مشکوک به صورت ارسال هشدار و Alarm، مدیر سیستم را در جریان می‌گذارد.

**انواع فایروال**

انواع فایروال را با توجه به ساختار کلی و روش کار می‌توان به چندین دسته مختلف دسته‌بندی کرد که در اینجا به هشت نمونه از آن‌ها خواهیم پرداخت:

* فایروال‌های فیلترینگ بسته (Packet-Filtering Firewalls)
* فایروال‌های مداری (Circuit-level gateways)
* فایروال‌های بررسی کننده وضعیت (Stateful inspection firewalls)
* فایروال‌های پروکسی (proxy firewalls)
* فایروال‌های نسل بعدی (Next-gen firewalls)
* فایروال‌های نرم افزاری (Software firewalls)
* فایروال‌های سخت افزاری (Hardware firewalls)
* فایروال‌ ابری (Cloud firewall)

1. **فایروال‌های فیلترینگ بسته (Packet-Filtering Firewalls)**

فایروال فیلترینگ بسته از ابتدایی‌ترین و قدیمی‌ترین انواع فایروال است که استفاده از آن مانند یک ایست بازرسی در روتر و سوئیچ ایجاد می‌کند. این فایروال از طریق روتر بررسی ساده‌ای روی داده‌ها انجام می‌دهد که با این بررسی می‌تواند به جزئیات بسیاری مانند مبدا و مقصد داده، آدرس IP، شماره پورت و اطلاعاتی از قبیل بدون باز کردن کردن داده‌ها دست پیدا کند. در صورتی که داده در این قسمت امکان بررسی را برای فایروال به وجود نیاورد، از بین خواهد رفت. نکته مهم درباره فایروال های فیلترینگ بسته آن است که این نوع فایروال به انرژی زیادی برای کار نیاز ندارد و به همین دلیل بهره‌مندی از آن روی عملکرد سیستم تاثیری نخواهد داشت ولی باید گفت که این فایروال عملکرد قوی دارد و کار با آن نیز ساده است.

1. **فایروال‌های مداری (Circuit-level gateways)**

فایروال‌های مداری از دیگر انواع فایروال‌های ساده‌‌ای هستند که به آسانی و بدون استفاده از منابع محاسباتی کار می‌کنند. این به طور کلی TPC نامیده می‌شود که از قانونی بودن داده‌ها اطمینان حاصل می‌کند. هرچند این فایروال بسیار کاربردی است ولی خود بسته داده را بررسی نمی‌کند، بنابراین اگر خو بسته حاوی نرم افزارهای مخرب باشد، وارد شبکه خواهد شد. با توجه به ضعفی که فایروال های مداری دارند، توصیه می‌شود این محصول در کنار یکی دیگر از انواع فایروال‌ها مورد استفاده قرار گیرد.

1. فایروال های بررسی کننده وضعیت (Stateful inspection firewalls)

فایروال‌های بررسی کننده وضعیت از بهترین سطح امنیت برخوردار هستند. عملکرد این فایروال به این ترتیب است که بسته‌ای اطلاعاتی را در لایه سه و لایه IP مانیتور می‌کند و در صورت معتبر بودن بسته اطلاعاتی محتوای این بسته را مورد ارزیابی قرار می‌دهد.

1. **فایروال‌های پروکسی (proxy firewalls)**

فایروال‌های پروکسی، فایروال‌هایی هستند که از آن‌ها به عنوان یک میانجی بین شکبه‌ها استفاده می‌شود. پروکسی فایروال به منظور پردازش درخواست‌های رسیده از خارج شبکه مورد استفاده قرار می‌گیرد. این پروکسی داده را تست می‌کند و با توجه به قوانین تعیین شده تصمیم‌گیری می‌کند که آیا درخواست مورد قبول است یا خیر. همچنین این پروکسی تمامی بسته را پیگیری می‌کند و آن‌ها را داخل شبکه باز فرآوری خواهد کرد.

1. **فایروال‌های نسل بعدی (Next-gen firewalls)**

از جدید‌ترین نوع از انواع فایروال های ارائه شده به بازار فایروال های نسل بعدی (Next-gen firewalls) هستند که بررسی عمیق بسته‌ها و محتواهای آن‌ها و بررسی بسته‌های TCP می‌پردازند. همچنین این فایروال نسل بعدی از فناوری‌های دیگری مانند سیستم‌های پیشگیری از نفوذ حمله علیه شبکه نیز برخوردار است.

1. **فایروال‌های نرم افزاری (Software firewalls)**

فایروال‌های نرم افزاری هر نوع فایروالی هستند که به جای استفاده از یک قطعه سخت افزاری بر روی دستگاه نصب می‌شوند. از مزیت‌های اصلی فایروال‌های نرم افزاری آن است که از آن می‌توان برای جدا کردن نقاط انتهایی شبکه استفاده می‌شود. هرچند این نوع فایروال بسیار کاربرد دارد ولی نصب آن بر روی دستگاه دشوار و زمان‌بر است و در مواردی دستگاه با آن سازگار نیست.

1. **فایروال‌های سخت افزاری (Hardware firewalls)**

فایروال‌های ساخت افزاری دستگاه‌های فیزیکی مانند روتر هستند که از ورود بسته‌ها و محتواهای نامعتبر جلوگیری می‌کنند. از مزیت‌های این فایروال‌ها آن است که از آن‌ها می‌توان برای ایجاد سطح بالایی از امنیت استفاده کرد. قابلیت‌های فایروال‌های سخت افزاری با توجه به شرکت‌های سازنده آن متفاوت است و برخی از آن‌ها بیشتری برای بررسی همزمان چندین اتصال را خواهند داشت.

1. **فایروال ابری (Cloud firewall)**

هرگاه که از یک راه حل ابری برای ارائه فایروال استفاده شود، به آن می‌توان فایروال ابری گفت. در بسیاری از موارد فایروال‌های پروکسی به جای فایروال‌های ابری مورد استفاده قرار می‌گیرند زیرا معمولا از سرور ابری برای نصب فایروال های پروکسی استفاده می‌شود. مزیت اصلی فایروال های ابری آن است که به آسانی در سازمان‌های مختلف قابل استفاده هستند و با افزایش نیاز می‌توان ظرفیت آن را اضافه کرد تا بارهای ترافیکی بیشتری فیلتر شوند. این نوع از فایروال مانند فایروال‌های سخت افزاری از سطح بالایی از امنیت برخوردار هستند.

منبع: [forcepoint](https://www.forcepoint.com/cyber-edu/firewall)

لطفا جهت مشاوره در [انتخاب محصول امنیتی مناسب](https://softyab.com/product-category/security/antivirus/) خود با این شماره **09224971053** تماس بگیرید.

**مارو در شبکه های**[**اجتماعی**](https://www.instagram.com/softyab)**خودتان به اشتراک بگذارید.**