تعریف فایروال (Firewall) و ۲ دسته بندی اصلی آن

فهرست مطالب

این روزها اکثر افراد در خانه حداقل یک سیستم کامپیوتری دارند که اطلاعات مهم شان در آن قرار دارد و هیچکس تمایلی به سرقت این اطلاعات ندارد به همین دلیل است که باید همه ما به خوبی بدانیم فایروال چیست و چطور بر امنیت سیستم تاثیر می گذارد؟ آشنایی با انواع فایروال ها و کاربرد آن ها این اجازه را به ما می دهد که به بهترین انتخاب، متناسب با نیازمان دست پیدا کنیم. در این مقاله همراه ما باشید تا با مفهوم، کاربرد و انواع فایروال ها آشنا شویم.

#۱ فایروال چیست؟ (Firewall)

فایروال یا دیواره آتش در واقع یک سیستم امنیتی شبکه است که ترافیک ورودی و خروجی شبکه را تحت کنترل دارد. به شکل ساده تر در پاسخ به سوال فایروال چیست، باید عنوان کنیم که فایروال از ورود هکرها، ترافیک

های تخریب کننده، دسترسی غیرمجاز به داده ها و... جلوگیری می کند. قوانین فایروال بر اساس نیاز امنیتی یک شرکت یا ارگان هستند؛ بنابراین ترافیکی امکان ورود و خروج را دارد که مطابق سیاست ها و قوانین امنیتی فایروال باشد.

فایروال ها وظایفی بر عهده دارند که عبارت اند از:

- محافظت کامل از منابع
- دسترسی مجاز به منابع
- کنترل و مدیریت ترافیک شبکه
- گزارش گیری و ذخیره سازی تمامی رویدادها
- ظاهر شدن در نقش یک واسطه یا میانجی

#۲ انواع فایروال ها بر اساس شیوه نصب

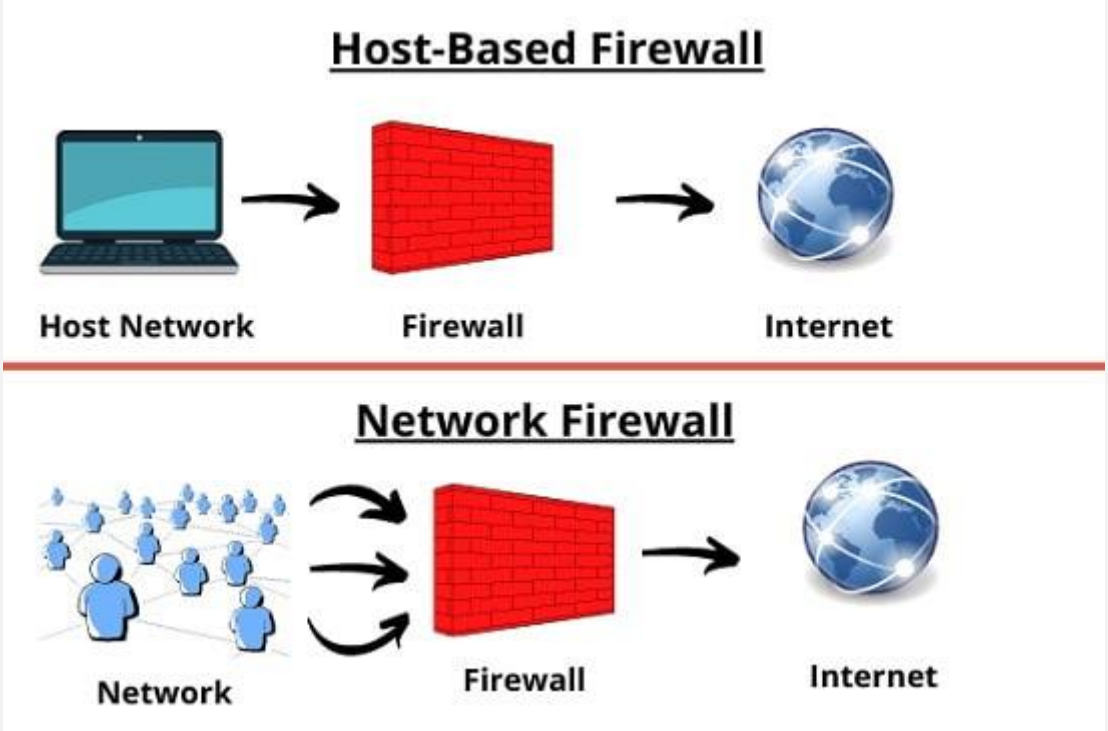
پس از دریافت پاسخ سوال فایروال چیست، اینک باید به انواع فایروال و ویژگی هر یک از آن ها اشاره کنیم.

به طور کلی، فایروال ها براساس شیوه نصب به دو دسته تقسیم می شوند:

۱. فایروال های مبتنی بر شبکه و میزبان
۲. فایروال های نرم افزاری و سخت افزاری

در ادامه به معرفی هر کدام از این دسته بندی ها می پردازیم.

#۲-۱ فایروال مبتنی بر شبکه و میزبان



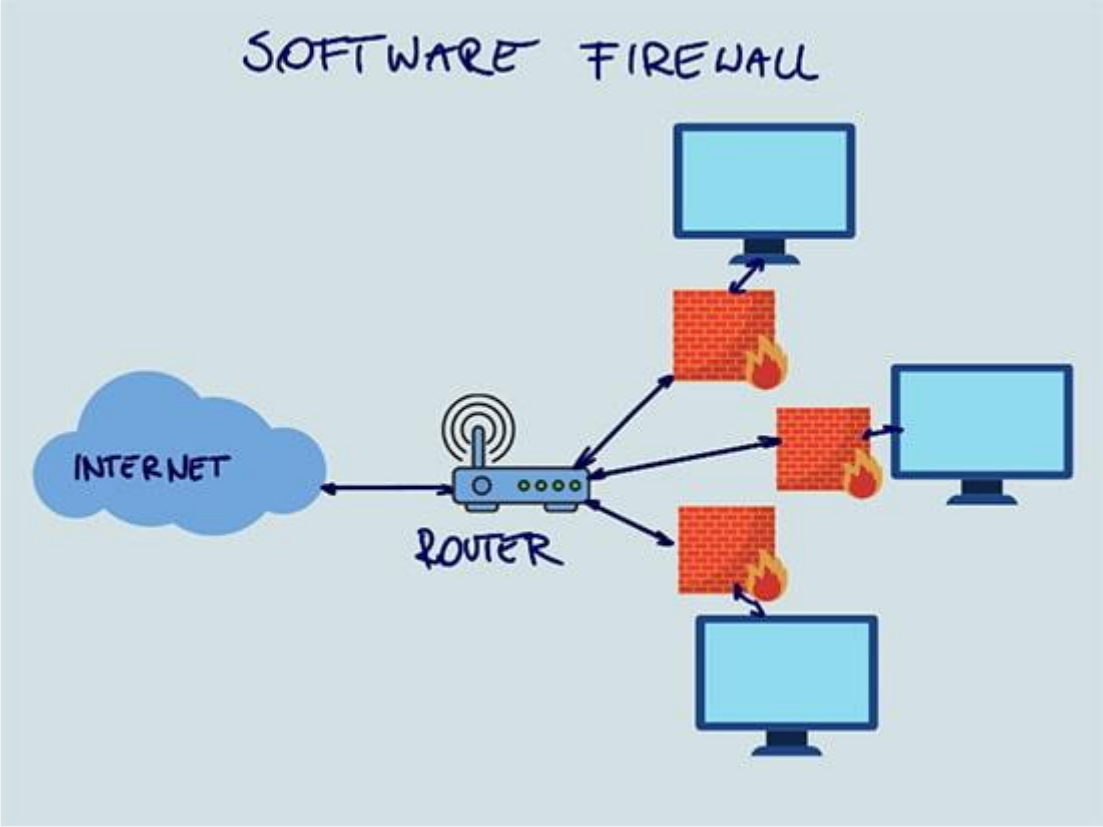
کاربرد فایروال های مبتنی بر شبکه (Network Firewall) در زیرساخت شبکه و فایروال های مبتنی بر میزبان (Host-Based Firewall) در سیستم شخصی کاربران و سرورها است.

#۲-۲ فایروال نرم افزاری و سخت افزاری

برای درک بهتر پاسخ سوال فایروال چیست، اینک لازم است به معرفی دسته بندی دیگری از فایروال ها، یعنی فایروال های نرم افزاری و سخت افزاری بپردازیم.

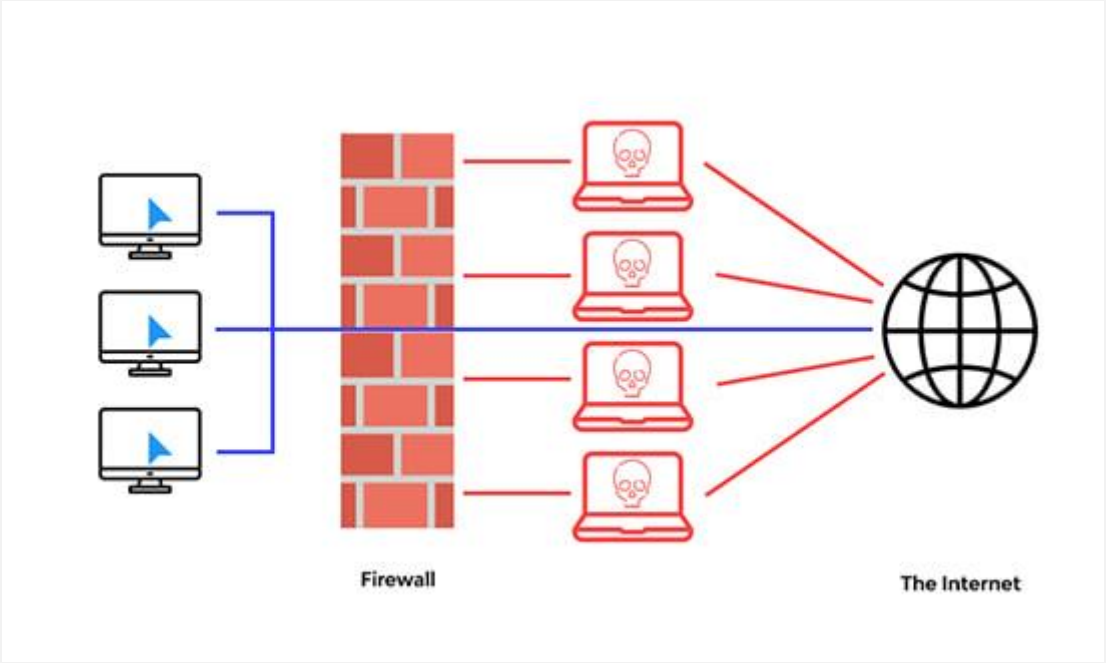
۱. فایروال نرم افزاری (Software Firewall):

به طور کلی این دسته از فایروال ها برای راه اندازی در کامپیوترهای شخصی یا اداری که مدت زمان طولانی به اینترنت متصل هستند، استفاده می شوند و از این سیستم ها در برابر نفوذ هکرها و دسترسی های غیرمجاز محافظت می کنند. همان طور که می دانید سیستم های کامپیوتری با پورت های زیادی ارتباط دارند که به واسطه فایروال های نرم افزاری در برابر ارتباط های پر ریسک محافظت می شوند. بهتر است بدانید که فایروال های نرم افزاری قابلیت تشخیص فعالیت های خارجی تهدیدکننده را دارند؛ بنابراین آدرس های خارجی و غیرمجاز هیچ دسترسی به کامپیوتر شخصی نخواهند داشت.



۲. فایروال سخت افزاری (Hardware Firewall):

یکی دیگر از فایروال های پرکاربرد و مهم است که در مقایسه با فایروال نرم افزاری، پیچیدگی بیشتری دارد. فایروال های سخت افزاری به طور پیش فرض و بدون نیاز به اِعمال تنظیمات اولیه، از ورود داده ها و همچنین ایجاد ترافیک ناخواسته در شبکه، محافظت می کنند. این فایروال ها میان یک شبکه (سازمان) و یک بخش دیگر که حداقل امنیت را دارد (اینترنت) تعبیه می شوند و با کمک آن ها شبکه های امن و ناامن از یکدیگر تفکیک می شوند. البته بهتر است بدانید فایروال های سخت افزاری تنها برای شبکه های سازمانی و شرکتی نیستند و برای شبکه های کامپیوتر خانگی و شخصی نیز مناسب می باشند.

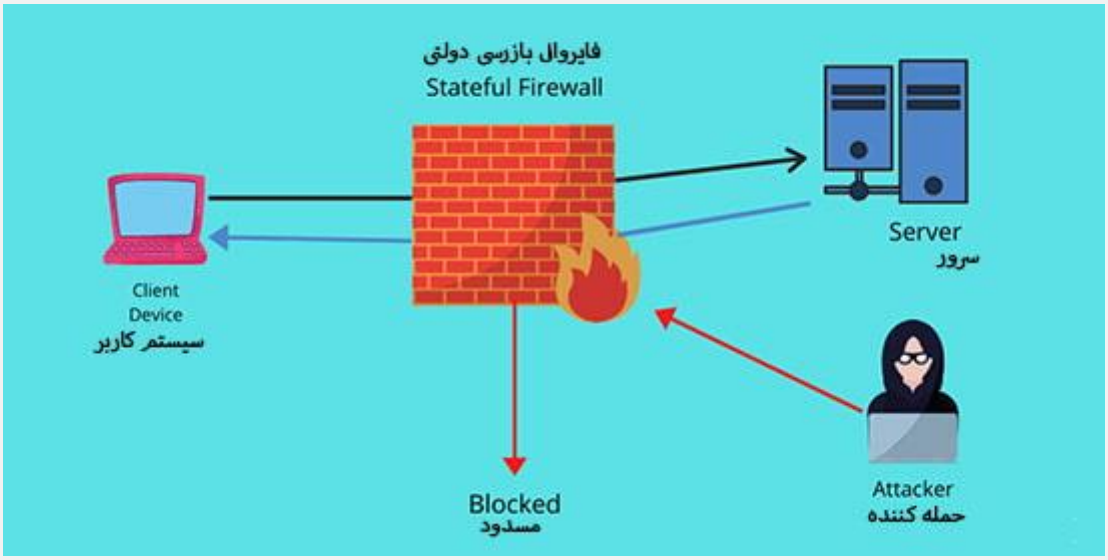


#۳ انواع فایروال ها بر اساس عملکرد و سطح امنیت

انواعی از فایروال ها بر اساس میزان امنیت مورد نیاز می توانند روی سیستم های کامپیوتری اجرا شوند و با عملکردی متفاوت، امنیت سیستم را برقرار کنند.

#۳-۱ فایروال بازرسی دولتی چیست؟ (Stateful Firewall)

فایروال بازرسی دولتی یا بازرسی رسمی یک فایروال سنتی است. این فایروال ترافیک را بر اساس وضعیت پورت یا پروتکل مسدود می کند. ضمن آن که تمام عملکردها را از هنگام باز شدن تا بسته شدن یک اتصال، به طور کامل تحت نظر دارد.



#۲-۳ فایروال مدیریت تهدید یکپارچه چیست؟ (UTM Firewall)

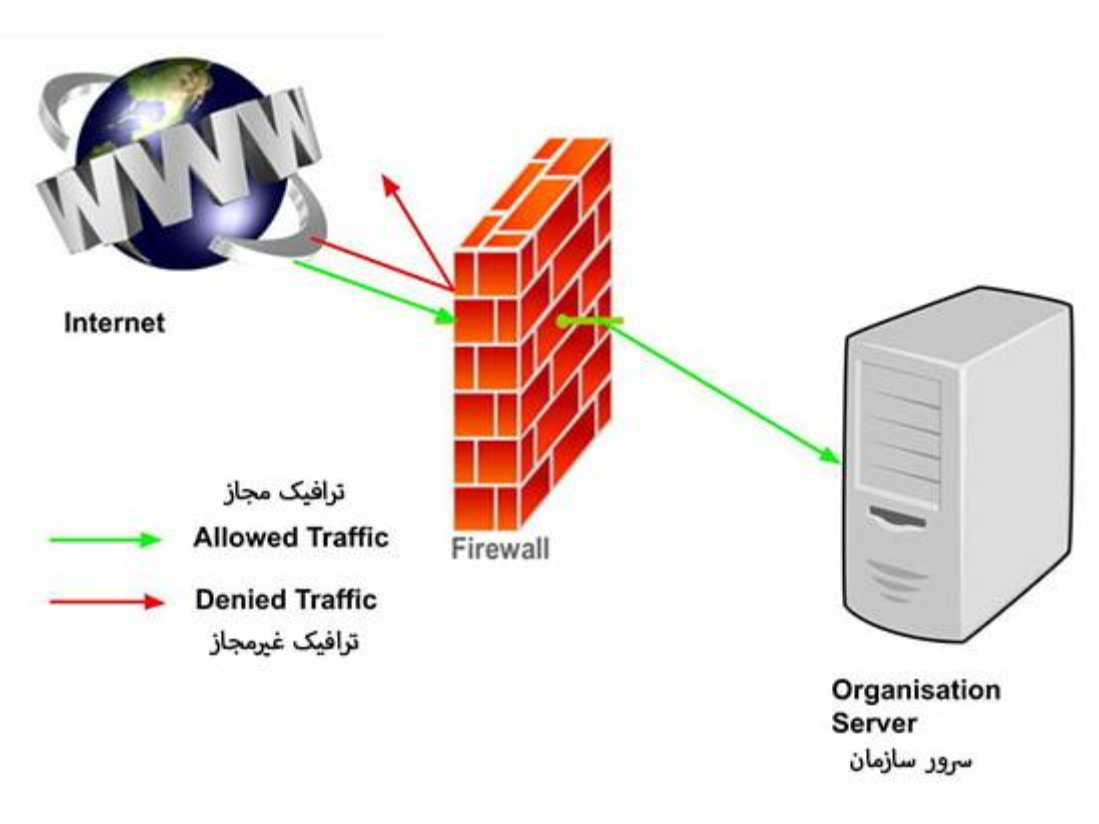
UTM مخفف Unified Threat Management به دستگاه های فایروال سخت افزاری یا نرم افزاری اطلاق می شود که قابلیت جمع آوری تمام توابع و قوانین امنیتی مانند پروکسی ها، دستگاه های جلوگیری از ورود و شناسایی، محافظت در مقابل بدافزارها یا نرم افزار های مخرب و... را دارند. این نوع فایروال ها دربردارنده مدیریت ابری نیز هستند.

اما مزیت اصلی این نوع فایروال چیست؟

لازم به ذکر است که به دلیل عملکرد ساده و سریعی که این نوع فایروال ارائه می دهد، مورد توجه کاربران بیشتری واقع شده است.

#۳-۳ فایروال پروکسی چیست؟ (Proxy Firewall)

نوع اولیه سیستم های فایروال، پروکسی است که مانند درگاه ورودی از یک شبکه به شبکه دیگر عمل می کند. پروکسی فایروال بین اینترنت و سیستم کاربران، به عنوان یک سیستم میانی یا واسطه عمل می کند. این سیستم به جای آن که کاربر به طور مستقیم به اینترنت دسترسی داشته باشد، درخواست های کاربران را دریافت کرده و داده درخواست شده از سوی کاربر را ارسال و جواب آن را از سرور دریافت می کند. در مرحله بعد نیز با بررسی درستی داده ها، آن ها را به سمت کاربر ارسال خواهد کرد.



#۴-۳ فایروال نسل بعدی چیست؟ (NGFW Firewall)

فایروال های NGFW مخفف Next-Generation Firewall از جدیدترین و بهترین نسل فایروال ها هستند. این ها فایروال هایی هستند که عملیات آن ها تنها فیلتر کردن و بازرسی بسته های ساده در حالت ها و وضعیت های مختلف نیست؛ بلکه عملیات بسیار پیشرفته ای را در حفاظت از سیستم بر عهده دارند. بسیاری از شرکت ها و سازمان ها، برای آن که با تهدیدها و برنامه های مخرب و مدرن مقابله کنند، از فایروال های نسل بعدی بهره می برند.

مهم ترین عملکردهای این نوع فایروال چیست؟

- جلوگیری از نفوذ یکپارچه برنامه های مخرب
- برخورداری از امکانات فایروال های استاندارد همانند بازرسی ترافیکی
- کنترل و مدیریت برنامه برای بررسی و مسدود نمودن برنامه های مخرب
- ارتقا و توسعه کلیه مسیرهای ارتباطی بر اساس اطلاعات و داده های تنظیم شده
- در نظر گرفتن تکنیک های جدید برای تهدیدهای امنیتی در حال تغییر و تحول

#۵-۳ فایروال متمرکز بر تهدید چیست؟ (Threat-Focused NG-Firewall)

فایروال های متمرکز بر تهدید، تمام قابلیت ها و امکانات فایروال های NGFW سنتی را دارند و امکان شناسایی و اصلاح آسیب ها و تهدیدها را نیز به صورت کاملاً پیشرفته ارائه می کنند.

مزایای استفاده از این فایروال چیست؟

آگاهی از این که کدام اطلاعات و داده ها، تحت چه مواضع و شرایطی در معرض آسیب هستند. در برابر حملات و تهدیدها با خودکارسازی امنیتیِ سریع و هوشمند، بلافاصله نسبت به حملات واکنش نشان می دهد.
قابلیت شناسایی فعالیت ها و عملیات مشکوک موجود در رویدادها و برنامه های شبکه را دارد. مدت زمان تشخیص یا شناسایی و پاک سازی کامل را کاهش می دهد. قابلیت اجرای سریع و آسان دارد و با در نظر گرفتن سیاست ها و قوانین پیوسته و منسجم از شبکه و سیستم در برابر تمام حملات و تهدیدها محافظت می کند.

#۳-۶ فایروال مجازی چیست؟ (Virtual Firewall)

فایروال های مجازی در یک سیستم ابر خصوصی یا ابر عمومی مستقر می شوند و برای نظارت بر ترافیک ورودی و خروجی شبکه های مجازی و فیزیکی کاربرد دارند. فایروال مجازی به عنوان یک جزء اصلی در شبکه های مختلف نرم افزاری شناخته شده است.


FIREWALL