یکی از سوال های رایج در شبکه این است که فایروال چیست ؟

و چه کاربرد های دارد

در این ساعات که در کنار شما هستیم

شما رو با فایروال آشنا خواهیم کرد

وقتی که ما در مورد اینترنت گفتوگو میکنیم اولین سوالی که پیش می اید بحث امنیت است

اینترنت و امنیت دو مقوله جدا نشدنی از هم هستند که هرکس در اینترنت در حال انجام

کاری است به مانند کسب کار اینترنتی یا بالعکس خرید از کسب کار های اینترنتی

و یا هر کار دیگیری باید به امنیت کار خود در بستر اینترنت اهمیت بسیار زیادی داد

فایروال یا ترجمه فارسی ان دیوار اتش به نرم افزاری یا سخت افزاری گفته میشود

که از دسترسی باز کامپیوتر ها جلوگیری کرده تا برنامه یا هرچیز دیگری که

حامل الودگی هستند نتوانند به کامپیوتر شما نفوذ پیدا کنند تا بتوانند

به سیستم و اطلاعات مهم شما صدمه یا انهارا کنترل کنند

همچنین فایروال ترافیک رد بدل شده در شبکه نیز کنترل میکند و از دسترسی های

غیر مجاز به شبکه ی خصوصی جلوگیر میکند و یک ستون امنیتی در شبکه است

و کار های دیگری که فایروال برای ما انجام میدهد

بحث داده ها است : فایروال هر داده ای که میخاهند به کامپیوتر ما وار شود

یا از ان خارج شود کنترل میکند که ایا اجازه ای عبور دارد یا باید مسدود شود

و حال اگر فایروال غیر فعال کنیم چه اتفاقی برای ما ممکن است رخ دهد :

استفاده نکردن از فایروال موجب میشود که هکر ها یا مهاجمین به راحتی

وارد شبکه یا کامپیوتر شما شوند و بدن هیچ محدودیتی

خراب کاری های خود را اعمال کنند

و اگر بخواهیم فایروال را به زبان خیلی ساده توضیح دهیم این است که

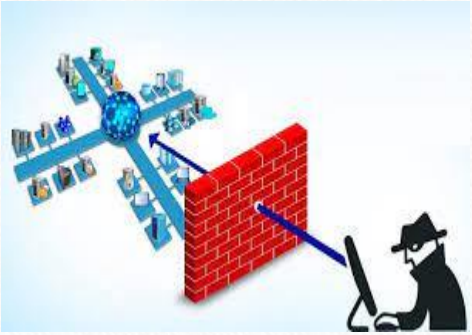
شما یک خانه را تصور کنید که افرادی که میخواهند وارد خانه یه خارج از خانه شوند باید از

درب خانه عبور کنند و یک نگهبان همیشه دم در تمام افرادی که وارد و خارج میشوند رو چک میکنه

که ببینه اجازه وارد شدن یا خارج شدن دارن یا نه

حالا ان خانه میتواند شبکه یا کامپیوتر شما باشد و ان افردای که وارد و خارج میشوند داده ها باشند

و اون در خانه ما (دروازه یا Gateway) ما است و ان نگهبان فایروال ما است



اگیر ما بخواهیم تمام وضایف فایروال لیست کنیم عبارتند از :

1. از منابع محافظت میکند
2. اجازه دسترسی هارا صادر میکند
3. ترافیک شبکه را مدیریت و کنترل میکند
4. اتفاقات را ذخیره و گزارش میدهند

تا اینجای کار با قالب اصلی کار که فایروال بود اشنا شدیم

و حال میخواهیم با جزئیات کار اشنا بشیم

تا به درک وجود حیاتی فایروال برسیم

فایروال شخصی :

در عصر اینترنت پرسرعت کامپیوتر ها به شبکه های کوچک و بزرگ و گسترده مختلفی متصل میشود

و ما برای تامین امنیت خود باید فایروال شخصی داشته باشیم تا به مهاجمین که در کمین ما هستند

اجازه ندهیم به کامپیوتر ما نفوذ پیدا کنند

و فقط متصل بودن به شبکه های مختلف برای ما دردسر ایجاد نمیکنه بلکه اتصال به اینترنت پرسرعت

هم برای ما دردسر ایجاد میکند : چرا که همین سرعت بالا باعث اسیب پذیر شدن ما نیز میشود

مثل این است که ما با سرعت از درب خانه خود خارج شویم و درب را پشت سر خود باز بگذارید

دلایل اهمیت استفاده از فایروال شخصی :

شما همیشه در بستر اینترنت قرار دارید بنابراین باید از فایروال استفاده کنید تا فرصت حمله به مهاجیمن ندهید و همین طور شما در هر مکانی مانند پارک ـ کافه ـ فرودگاه و غیره ممکن است به شبکه های وای فای عمومی متصل شوید که همین باعث یک فرصت عالی به مهاجم برای نفوذ به دستگاه شما را محیا میکند

دسته بندی فایروال ها :

فایروال ها عمدتا در دو دسته قرار دارند یکی از دسته ها (فایروال مبتنی بر میزبان)

و دسته ای دیگر (فایروال مبتنی بر شبکه)

فایروال مبتنی بر میزبان : این فایروال ها بر روی سرور های شخصی نصب شده و سیگنال های

ورودی و خروجی را نظارت میکنند

فایروال مبتنی بر شبکه : این فایروال ها میتوانند در زیر ساخت های ابری ساخته شوند یا میتوانند

سرویس فایروال مجازی باشند

انواع مختلفی از فایروال ها 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 بسته ها به صورت 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

و چناچه این بسته نتواند قوانین فایروال را رعایت کند قطع میشود و به مقصد نمیرسد

این نوع فایروال عمدتا بر روی لایه های شبکه مدل OSI کار میکنند

فایروال های فیلتر بسته ها (Packet-filtering)

این نوع فایروال عمدتا بر روی لایه های شبکه مدل OSI کار میکنند

این فایروال‌ها هر بسته را به صورت 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 دلیل اینکه هر بسته را به تنهایی پردازش می‌کنند

ممکن است در برابر حملات IP آسیب پذیر باشند

فایروال‌های بازرسی قانونی (stateful inspection)

فایروال‌های بازرسی قانونی به فایروال‌های فیلتر دینامیک بسته‌ها نیز معروف هستند

این فایروال دارای جدولی است که مسیر تمام ارتباطات را باز نگه می‌دارد هنگامی که یک بسته‌ی جدید

می‌آید فایروال اطلاعات موجود در سربرگ 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

فایروال های لایه کاربرد و پروکسی (Application Layer and Proxy)

حملات به وب سرورها روزبه‌روز در حال افزایش است به همین دلیل ما برای امنیت خود به یک

فایروال قدرتمند برای محافظت از شبکه خود نیازمندیم

فایروال‌هایی که در اسلاید های قبل با انها اشنا شدیم نمی توانند در میان

درخواست های پروتکل لایه کاربردی معتبر، داده‌ها و ترافیک‌های مضر تمایز قائل شوند

فایروال های لایه کاربرد و پروکسی (Application Layer and Proxy)

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 دقیق تری 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 سخت تر خواهد کرد و آن‌ها نمی‌توانند

به راحتی بفهمند که شبکه در چه مکانی قرار دارد

فایروال‌های نرم افزاری :

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 پورت‌ها وظیفه خود را اعمال میکند

فایروال های نرم افزاری :

یکی از مشکلات فایروال‌های نرم‌افزاری این است که روی سیستم‌عامل کامپیوتر شخصی کار می‌کنند چنان چه 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 به شدت به تصمیمات کاربر وابسته است

اگر کاربر به اشتباه از یک 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 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 نرم افزار دیگری بر روی آن نصب نمی‌شود

به همین دلیل حمله کردن به آن بسیار مشکل است

نتیجه گیری کلی از فایروال :

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 به هیچ عنوان لزوم استفاده از فایروال را نادیده نگیرید.