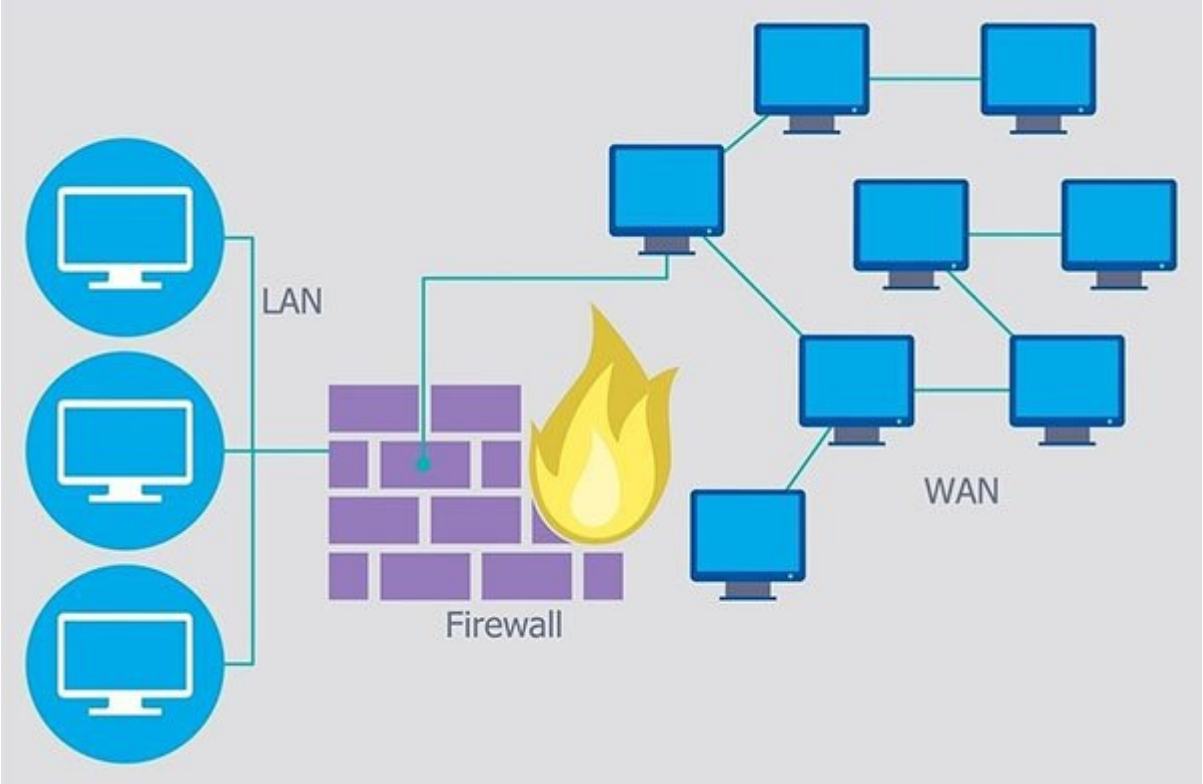
آیا می‌توان هر دو فایروال را در شبکه‌ها به کار گرفت؟

تفاوت دیواره آتش سخت‌افزاری با دیواره آتش نرم‌افزاری

دیواره‌های آتش یا فایروال‌ها را می‌توان به دو گروه تقسیم کرد: دیواره آتش (فایروال) نرم‌افزاری و دیواره آتش (فایروال) سخت‌افزاری. دیواره آتش نرم‌افزاری، نرم‌افزاری امنیتی است که روی رایانه یا سرور نصب می‌شود. دیواره آتش سخت‌افزاری، دستگاهی مستقل با پردازنده، حافظه، سیستم‌عامل و نرم‌افزار اختصاصی است. بعضی از فایروال‌های سخت‌افزاری نیز جزئی از روتر هستند و در آن ادغام شده‌اند. تفاوت فایروال‌های نرم‌افزاری با فایروال‌های سخت‌افزاری در قابلیت‌های‌شان ریشه دارد. باتوجه به تفاوت فایروال سخت‌افزاری با فایروال نرم‌افزاری و مزایا و کاستی‌هایی هر یک، می‌توان هر دو فایروال را در شبکه‌ها به کار گرفت تا هر کدام کاستی‌های دیگری را جبران کند.

دیواره آتش یا فایروال چیست؟

دیواره آتش یا فایروال، نرم‌افزار یا سخت‌افزاری است که مانند حصاری امنیتی، شبکه یا سامانه‌های کامپیوتری را احاطه می‌کند و آن‌ها را از برخی خطرات سایبری ایمن می‌دارد. فایروال را می‌توان نخستین سد امنیتی در ورودی شبکه دانست. لذا هر داده‌ای پیش از آن‌که بتواند از اینترنت یا دیگر شبکه‌ها به شبکه شما راه پیدا کند، ابتدا باید از فایروال بگذرد.



شکل 1. دیواره آتش (فایروال)، سدی امنیتی است که شبکه محلی را در برابر تهدیدهای سایبری اینترنت، شبکه‌های گسترده و... محافظت می‌کند.

اما فایروال چگونه تشخیص می‌دهد که چه چیز باید و چه چیز نباید از مرز شبکه عبور کند؟ فایروال برای این منظور بسته‌های داده (data packet)، از جمله نشانی مبدا و مقصد بسته‌ها را وارسی می‌کند و آن‌ها را با مجموعه قوانینی که برای شبکه تعریف شده است، مطابقت می‌دهد و سپس مشخص می‌کند که آیا بسته اجازه عبور دارد یا نه. با تنظیم فایروال می‌توان سایت‌های مضر را مسدود و از دسترسی غیرمجاز یا ورود ویروس‌ها و دیگر بدافزارها به شبکه جلوگیری کرد.

دیواره‌های آتش (فایروال‌ها) یا نرم‌افزاری و یا سخت‌افزاری هستند.

دیواره آتش (فایروال) نرم‌افزاری چیست؟

دیواره آتش (فایروال) نرم‌افزاری، نرم‌افزاری است که روی رایانه یا سرور نصب می‌شود. یکی از معروف‌ترین دیواره‌های آتش نرم‌افزاری، فایروال اختصاصی سیستم‌عامل ویندوز است که از صفحه تنظیمات امنیتی ویندوز قابل دسترسی است. علاوه بر این، شرکت‌های سازنده نرم‌افزارهای امنیتی (کاسپرسکی، پاندا و...) نیز فایروال‌های خاص خود را تولید می‌کنند که معمولا نسخه‌های مختلفی دارند. برخی از آن‌ها مختص رایانه‌های شخصی و برخی دیگر برای نصب روی سرورهای شبکه و مختص محیط‌های سازمانی طراحی شده‌اند تا تنها با یک بار نصب روی سرور، دیگر رایانه‌های شبکه نیز زیر چتر امنیتی آن بروند، زیرا در غیر این‌صورت باید به‌ازای هر رایانه متصل به شبکه، فایروال جداگانه‌ای خریداری و نصب شود که بدیهی است هزینه آن بسیار گزاف و نصب و راه‌اندازی آن روی ده‌ها یا صدها کامپیوتر بسیار زمان‌بر خواهدبود.

شکل 2. دیواره آتش سیستم‌عامل ویندوز یکی از آشناترین فایروال‌های نرم‌افزاری است.

برخی از فایروال‌های نرم‌افزاری علاوه بر پایش ترافیک ورودی شبکه می‌توانند بر ترافیک خروجی شبکه نیز نظارت کنند. علاوه بر این، فایروال‌های نرم‌افزاری معمولا گزینه‌ها و تنظیمات امنیتی بیشتری دارند و اصطلاحا انعطاف‌پذیرترند.

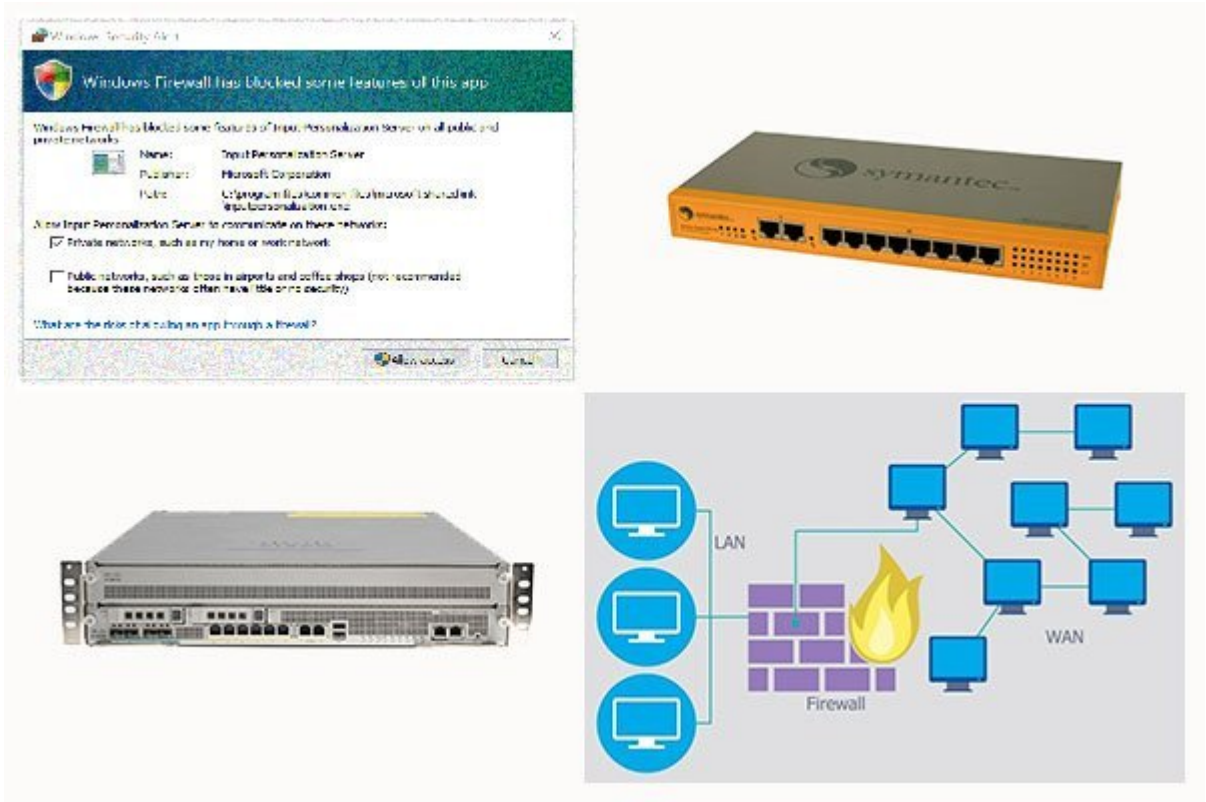
مزایای دیواره آتش (فایروال) نرم‌افزاری

- فایروال‌های نرم‌افزاری خانگی معمولا ارزان و برخی حتی رایگان هستند. نسخه‌های حرفه‌ای و سازمانی آن‌ها نیز مجوز چندکاربری دارند و لذا می‌توانند تمام سامانه‌های یک شبکه را پوشش دهند.
- نصب و پیکربندی نسخه‌های عادی فایروال‌های نرم‌افزاری، ساده است و فقط با چند کلیک می‌توان سطح حافظتی مورد نیاز را تعیین کرد. اما نسخه‌های سازمانی دانش و تخصص بیشتری می‌طلبند.
- بعضی از فایروال‌های نرم‌افزاری می‌توانند علاوه بر ترافیک ورودی، ترافیک خروجی شبکه را نیز پایش و پالایش کنند و از این حیث بر فایروال‌های سخت‌افزاری برتری دارند.
- فایروال‌های نرم‌افزاری انعطاف‌پذیرترند. مثلا با استفاده از آن‌ها می‌توان دسترسی برخی برنامه‌ها به شبکه را محدود و نتیجتا احتمال نفوذ برخی بدافزارها را کاهش داد.
- دیواره‌های آتش نرم‌افزاری، به‌ویژه نسخه‌های تک‌کاربره آن چون روی رایانه نصب می‌شوند، جابه‌جایی‌پذیرترند، یعنی رایانه هر جا که برود، فایروال نیز همراه آن است. این قابلیت برای کسانی که اغلب با لپ‌تاپ سفر می‌کنند اهمیت دارد.

معایب دیواره آتش (فایروال) نرم‌افزاری

- دیواره آتش نرم‌افزاری از منابع (پردازنده، حافظه و...) سامانه میزبان استفاده می‌کند و درنتیجه ممکن است سرعت یا کارایی آن را کاهش دهد.

- هرچه رایانه‌ها و سامانه‌های موجود در شبکه بیشتر باشند، هزینه خرید فایروال نرم‌افزاری نیز افزایش می‌یابد، چون استفاده از فایروال‌های نرم‌افزاری تک‌کاربره در چنین شبکه‌هایی چه از نظر زمانی و چه از نظر مالی مقرون به‌صرفه نیست، پس باید نسخه‌ای خریداری شود که همه سامانه‌ها را پشتیبانی کند؛ ضمن این‌که معمولا فایروال‌های ارزان یا رایگان در محیط‌های حساس و سازمانی کارایی چندانی ندارند.



دیواره آتش (فایروال) سخت‌افزاری چیست؟

دیواره آتش (فایروال) سخت‌افزاری دستگاه مستقلی است که پردازنده، حافظه و سیستم‌عامل اختصاصی دارد. باتوجه به این‌که در بسیاری از شبکه‌های متوسط و بزرگ، سرورها و دیگر تجهیزات شبکه درون رک نصب می‌شوند، بعضی از فایروال‌های سخت‌افزاری مستقل برای نصب در رک‌های سرور طراحی شده‌اند و لذا اندازه استانداردی دارند. بعضی از فایروال‌های سخت‌افزاری نیز به‌جای آن‌که دستگاه مستقلی باشند، جزئی از روتر شبکه هستند. به عبارت دیگر، برخی از مسیریاب‌ها یا روترهای شبکه، فایروال سخت‌افزاری داخلی نیز دارند.

فایروال سخت‌افزاری در مرز شبکه، یعنی بین روتر و دنیای خارج (اینترنت یا دیگر شبکه‌ها) جای می‌گیرد و لذا اولین سد دفاعی در ورودی شبکه است. هر داده‌ای پیش از آن‌که به روتر و سپس رایانه‌های موجود در شبکه برسد، باید از فایروال سخت‌افزاری بگذرد.

مزیت دیگر فایروال سخت‌افزاری این است که کامپیوتر یا شبکه محلی را از چشم دنیای خارج پنهان می‌دارد؛ طوری که ناظر خارجی، به‌جای شبکه، فقط یک دستگاه سخت‌افزاری می‌بیند که سیستم‌عامل ناآشنایی دارد (زیرا گفته شد که سیستم‌عامل فایروال‌های سخت‌افزاری، اختصاصی است). این شیوه پنهان‌کاری را اصطلاحا ترجمه آدرس شبکه یا NAT می‌نامند (مخفف network address translation). البته این تمهید در برابر ورود ویروس‌های ایمیلی کارایی

ندارد.

شکل 3. نمونه‌ای از فایروال‌های سخت‌افزاری سیسکو

مزایای دیواره آتش (فایروال) سخت‌افزاری

- فایروال سخت‌افزاری یک‌قدم جلوتر از فایروال نرم‌افزاری به دفاع از شبکه می‌پردازد، زیرا فایروال نرم‌افزاری روی رایانه یا سرور شبکه نصب می‌شود، اما فایروال سخت‌افزاری حتی پیش از روتر و درست در مرز شبکه جای می‌گیرد.
- یک دستگاه فایروال سخت‌افزاری می‌تواند تمام یک شبکه را پوشش دهد. این قابلیت در مراکزی که رایانه‌های زیادی دارند، بسیار ارزشمند و از نظر مالی مقرون به صرفه است.
- فایروال سخت‌افزاری مستقل چون پردازنده، حافظه و سیستم‌عامل اختصاصی دارد و روی رایانه دیگری نصب نمی‌شود، پربازده‌تر و سریع‌تر از فایروال نرم‌افزاری است.
- فایروال سخت‌افزاری در برابر بدافزارها مقاوم‌تر است، چون سیستم‌عامل آن با سیستم‌عامل‌های رایجی همچون ویندوز که بیشتر مورد توجه هکرها است، تفاوت دارد.

معایب دیواره آتش (فایروال) سخت‌افزاری

- پیکربندی فایروال‌های سخت‌افزاری سازمانی، برای تازه‌کارها سخت است.
- دیواره‌های آتش سخت‌افزاری برای پایش ترافیک خروجی مناسب نیستند.

شکل 4. نمونه‌ای از فایروال‌های سخت‌افزاری سوفوس

تفاوت‌های مهم فایروال سخت‌افزاری با فایروال نرم‌افزاری

فایروال سخت‌افزاری اولین سد دفاعی در ورودی شبکه است و از این حیث بر فایروال نرم‌افزاری برتری دارد، زیرا ترافیک ورودی را پیش از آن‌که حتی به روتر شبکه برسد، پایش می‌کند. اما فایروال نرم‌افزاری روی رایانه یا سرور

شبکه نصب می‌شود و درنتیجه، ترافیک ورودی پیش از آن‌که پایش شود، تا پای رایانه یا سرور شبکه جلو می‌آید.

در مقابل، فایروال‌های سخت‌افزاری برای پایش ترافیک خروجی شبکه مناسب نیستند، حال آن‌که برخی از فایروال‌های نرم‌افزاری ترافیک خروجی را هم پایش می‌کنند.

البته پایش ترافیک خروجی، چندان رایج نیست زیرا گاهی با چالش‌هایی همراه است. مثلا پایش ترافیک خروجی ممکن است نرم‌افزارهای کاربردی مورد استفاده در شبکه را دچار وقفه و روند کار سازمان را مختل کند. پس پیکربندی فایروال باید طوری باشد که کار مجموعه مختل نشود.

فایروال ورودی (inbound firewall) و فایروال خروجی (outbound firewall)

به فایروالی که برای نظارت بر ترافیک ورودی تنظیم شده است، فایروال ورودی (inbound firewall) و به فایروالی که برای نظارت بر ترافیک خروجی تنظیم شده است، فایروال خروجی (outbound firewall) می‌گویند. برخی فایروال‌ها قابلیت پایش هر دو نوع ترافیک را دارند.

معمولا فایروال‌ها در حالت پیش‌فرض فقط ترافیک ورودی شبکه را پایش و پالایش می‌کنند، زیرا اغلب فرض بر این است که شبکه از بیرون تهدید می‌شود و سمت‌سوی تهدیدهای سایبری از خارج به داخل است. اگر واقعا چنین باشد، پایش ترافیک ورودی برای تامین امنیت شبکه کافی است. اما گاهی در برخی شبکه‌ها (مثل شبکه‌های مهم سازمانی) لازم است که ترافیک خروجی شبکه نیز پایش و پالایش شود. تصور کنید، کاربری نادانسته یا دانسته چیزی را از خارج شبکه درخواست کند (ترافیک خروجی) که در پاسخ به آن، بدافزار یا برنامه مخربی به شبکه ارسال شود (ترافیک ورودی)؛ یا بدافزاری را تصور کنید که قبلا به درون شبکه راه یافته است (ترافیک ورودی) و اکنون می‌خواهد ضمن اتصال به اینترنت، داده‌های سازمان را به بیرون بفرستد (ترافیک خروجی). پس گاهی پایش و پالایش ترافیک خروجی نیز به‌اندازه پایش ترافیک ورودی، ضروری است.

همانطور که گفته شد، برای نظارت بر ترافیک خروجی شبکه معمولا از دیواره آتش نرم‌افزاری استفاده می‌شود. دیواره آتش نرم‌افزاری معمولا فهرست آماده‌ای از برنامه‌های امن دارد. اگر برنامه‌ای که در فهرست سفید (مجاز) فایروال ثبت نشده است، درخواستی صادر کند، فایروال از شما می‌پرسد که آیا می‌خواهید به آن برنامه اجازه دهید به اینترنت متصل شود یا نه.

باتوجه به آنچه گفته شد، گاهی توصیه می‌شود که هم از فایروال نرم‌افزاری و هم از فایروال سخت‌افزاری استفاده شود تا هر یک از آن‌ها کاستی‌های دیگری را پوشش دهد.

پیکربندی‌های مختلف فایروال

پس از نصب فایروال معمولا پیکربندی‌های مختلفی می‌توان صورت داد. می‌توان فایروال را طوری تنظیم کرد که ترافیک شبکه را بسته به معیارهای مختلفی پایش و پالایش کند، از جمله:

- پایش براساس آدرس آی‌پی: آدرس آی‌پی شماره‌ای 32 بیتی است که به هر آدرس وب اختصاص می‌یابد. این شماره 32 بیتی به چهار بخش تقسیم و هر بخش با نقطه از دیگر بخش‌ها جدا می‌شود؛ مثلا: 216.28.62.138
- پایش براساس محتوا: فایروال می‌تواند طوری تنظیم شود که تنها وب‌سایت‌های خاصی را روی شبکه باز کند یا وب‌سایت‌های خاصی (مثلا شبکه‌های اجتماعی) را مسدود کند.
- پایش براساس نام دامنه: فایروال می‌تواند طوری تنظیم شود که وب‌سایت‌ها را براساس نام دامنه‌شان مجاز یا غیرمجاز بداند.
- پایش براساس پروتکل: فایروال می‌تواند نحوه دسترسی کاربر به یک سرویس آنلاین را تعیین کند.
- پایش براساس پورت: سرورهای شبکه خدمات‌شان را از طریق پورت‌هایی که هر یک شماره خاصی دارند، در دسترس کاربران می‌نهند. مثلا ممکن است یک وب‌سرور روی پورت 80 تنظیم شده باشد.
- پایش براساس واژه‌ها یا عبارات: می‌توانید فایروال را نسبت به برخی واژه‌ها یا عبارات حساس کنید تا وب‌سایت‌های حاوی آن واژه‌ها و عبارات را مسدود کند.
- پایش براساس رفتارها و تغییرها: فایروال می‌تواند رفتارهای مشکوک را شناسایی و از آن جلوگیری کند. پاک شدن یک‌باره داده‌ها یا حملات هک از جمله رفتارهای مشکوک هستند.

فایروال به طرق مختلفی پیکربندی می‌شود. با مشورت کارشناس فناوری اطلاعات می‌توان تصمیم گرفت که کدام روش موثرتر است. مثلا یکی از روش‌ها این است که دسترسی به همه‌چیز موقتا مسدود و سپس دسترسی‌های مجاز یک‌به‌یک تعیین شوند.

دیواره آتش کافی نیست

دیواره‌های آتش به‌رغم قابلیت‌های‌شان همیشه و در برابر هر تهدیدی موثر نیستند. گاهی برخی نرم‌افزارهای امنیتی و ملاحظات انسانی نیز لازم است تا ایمنی مجموعه هرچه بیشتر ارتقا یابد.

دیواره‌های آتش همیشه نمی‌توانند کاربر را از حملات مهندسی اجتماعی یا حملات جعل (spoofing) مصون بدارند. مثلا ممکن است هکری خود را در نقش یکی از مشتریان جا بزند و با فریفتن کاربران به اطلاعات شرکت دست پیدا کند. معمولا در چنین مواردی کاری از دست دیواره آتش برنمی‌آید و نرم‌افزارهای پایشگر ایمیل کارآمدترند.

ضمنا دیواره‌های آتش همیشه نمی‌توانند از ورود بدافزارها، ویروس‌ها و کرم‌ها جلوگیری کنند. برای این منظور باید از برنامه‌های ضدویروس نیز کمک گرفت تا اگر بدافزاری توانست از دیواره آتش بگذرد، نرم‌افزار ضدویروس با آن مقابله کند.

اما حتی با این تمهیدات نیز نمی‌توان امنیت شبکه را کاملا تضمین کرد. پس کاربران شبکه تا می‌توانند باید دانش خود در حوزه امنیت سایبری را افزایش دهند، چون گاهی افراد آموزش‌دیده بهترین سد امنیتی و افراد کم‌اطلاع بزرگ‌ترین تهدید برای شبکه متبوع‌شان هستند.

تاریخ انتشار:
28 دی 1398

نشانی منبع:
https://www.shabakeh-mag.com/networking-technology/16395/%D8%AA%D9%81%D8%A7%D9%88%D8%AA-%D8%AF%DB%8C%D9%88%D8%A7%D8%B1%D9%87-%D8%A2%D8%AA%D8%B4-%D8%B3%D8%AE%D8%AA%E2%80%8C%D8%A7%D9%81%D8%B2%D8%A7%D8%B1%DB%8C-%D8%A8%D8%A7-%D8%AF%DB%8C%D9%88%D8%A7%D8%B1%D9%87-%D8%A2%D8%AA%D8%B4-%D9%86%D8%B1%D9%85%E2%80%8C%D8%A7%D9%81%D8%B2%D8%A7%D8%B1%DB%8C