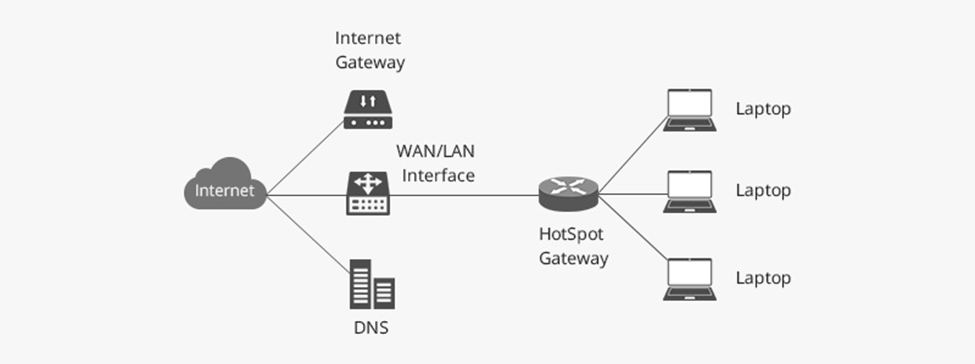
**درگاه یا فایروال**

از مهم‌ترین جنبه‌های امنیت شبکه که باید در هنگام کار با اینترنت به آن توجه داشت شبکه‌های LAN یا سایر روش‌هاست که با صرف‌نظر از بزرگ یا کوچک بودن شبکه باید به آن‌ها توجه شود. هر دو مورد درگاه یا فایروال از تجهیزات محافظتی شبکه‌ای مهمی هستند که خطرات بالقوه امنیتی را در عملکرد شبکه‌های رایانه‌ای به‌موقع شناسایی و برطرف می کند و تجربه بهتری را در اختیار کاربران قرارمی دهد.

**مقایسه درگاه با فایروال**

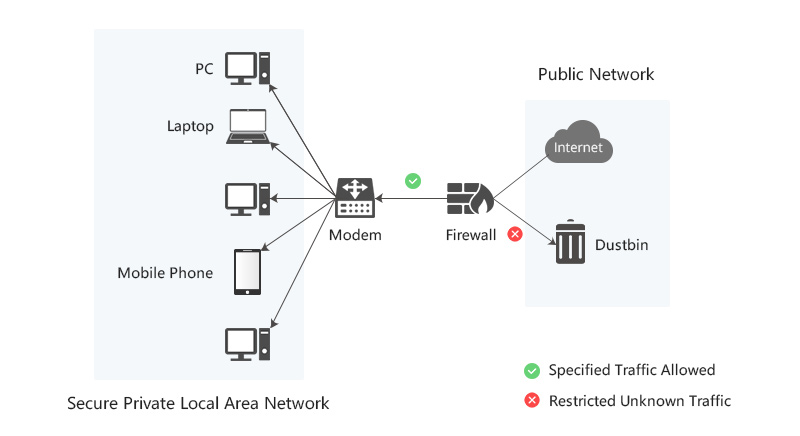
درگاه یا GateWay برای اتصال دو شبکه مختلف به یکدیگر از درگاه استفاده می‌شود. که درگاه دستگاه سخت‌افزاری شبکه یا گره شبکه است و به کاربران این امکان را می‌دهد تا از طریق چندین شبکه با یکدیگر در ارتباط باشند.

رایج ترین درگاه‌ها رایانه‌ها و روترها هستند که یک شرکت را به شبکه‌ها متصل می‌کنند این درگاه‌ها برای برقراری ارتباط بین پایانه‌های متصل به شبکه‌های ناهمگن با ویژگی‌های مختلف شبکه و استفاده از پورت‌های مختلف ضروری می‌باشد.



**فایروال در شبکه چیست؟**

برای نظارت بر ترافیک ورودی و خروجی شبکه و تصمیم در مورد مسدود کردن ترافیک خاص براساس مجموعه‌ای از قوانین امنیتی طراحی می‌شود. برای جلوگیری از ترافیک مخرب مثل ویروس ها و هکر ها مانعی بین شبکه داخلی شما و ترافیک ورودی از منابع خارجی ایجاد می‌شود که فایروال می‌تواند نرم‌افزاری یا سخت افزاری بهتر از هر دو را در شبکه اعمال کند، فایروال نرم‌افزاری برنامه‌ای است که روی هر رایانه نصب می‌شود و از طریق شماره پورت و برنامه‌ها ترافیک را تنظیم می‌کند درحالی‌که فایروال فیزیکی قطعه‌ای از تجهیزات شبکه است که بین شبکه و درگاه شما نصب می‌شود و عمل نظارت بر ترافیک شبکه را انجام می‌دهد.



**تفاوت GateWay با فایروال**

از نظر هدف و GateWay ارتباط بین دو شبکه مختلف را با معماری‌ها و پروتکل‌های مختلف امکان‌پذیر می‌کند. درگاه‌ها می‌توانند به‌صورت سخت‌افزاری، نرم‌افزاری یا ترکیبی از هر دو اجرا شود. اگرچه می‌توان از درگاه امنیتی برای محافظت از شبکه استفاده کرد اما میزان ایمنی آن به اندازه‌ی فایروال نیست.

فایروال می‌تواند با جلوگیری از دسترسی کاربران غیرمجاز یا هکر ها به شبکه‌های خصوصی اتصال پیدا کند و از رایانه شما محافظت نماید. فایروال ها اساساً ترافیک‌های مشکوک مثل ویروس و هکر ها را مسدود کرده و هدف اصلی آن‌ها جلوگیری از خطر در شبکه‌ی شماست. از نظر عملکرد به سه دسته طبقه‌بندی می‌شوند:

1. **درگاه پروتکل**
2. **درگاه برنامه**
3. **درگاه امنیتی**

Porotocol Gatewayبرای تبدیل پروتکل بین شبکه‌ای مرتبط به‌هم و دارای پروتکل‌های متفاوت استفاده می‌شود. این مورد متداول‌ترین عملکرد درگاه‌ها می باشد.

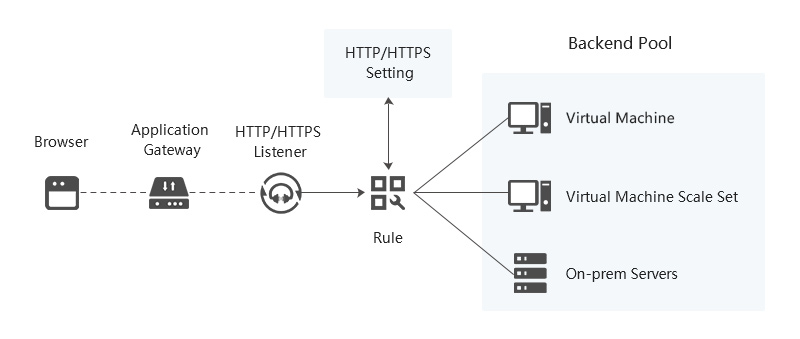
درگاه برنامه دو برنامه مختلف را در لایه برنامه به یکدیگر متصل می‌سازد و برای ترجمه پروتکل باید یک برنامه خاص مناسب استفاده کرد. درمورد درگاه‌های امنیتی، با اعمال سیاست‌های امنیتی و فیلتر کردن ترافیک مخرب اینترنت در زمان واقعی، شبکه را در برابر تهدیدات امنیتی آنلاین، محافظت می‌کند.

در مقایسه‌ی درگاه و فایروال، فایروال ها سه عملکرد اساسی امنیتی را برای شبکه دارد:

1. **فیلتر کردن:** در فیلتر کردن بسته ها در سطح بسته عمل می‌کند و ورود یا خروج از طریق شبکه رایانه بسته داده‌ها را بررسی می‌کند. فایروال از قوانین تعریف‌شده توسط کاربر برای تصمیم‌گیری درمورد پذیرش یا رد بسته استفاده می‌کند اگر داده مناسب باشد قابل دریافت است و بالعکس اگر با قوانین مطابقت نداشته باشد داده رد می‌شود. فیلتر کردن بسته معمولاً برای مقاومت در برابر حملات از طریق LAN بسیار مؤثر است.
2. **بازرسی ایستا:** برخلاف فیلتر کردن بسته‌ها، فیلترینگ استاتیک یا ایستا عناصر مختلف هر داده را بررسی می‌کند و آن‌ها را با اطلاعات معتبر پایگاه داده مقایسه می‌کند در حین بررسی بسته با ضبط آدرس IP و شماره پورت در لایه‌های خود تجزیه‌وتحلیل می‌شود. بنابراین این سطح از فیلترینگ از فیلترینگ بسته جدی تر است.
3. **عمل کردن به‌عنوان پراکسی برنامه**: وقتی فایروال به‌عنوان پراکسی برنامه تنظیم شود در لایه برنامه کار می‌کند تا اطلاعات بین شبکه داخلی و خارجی متوقف شود.

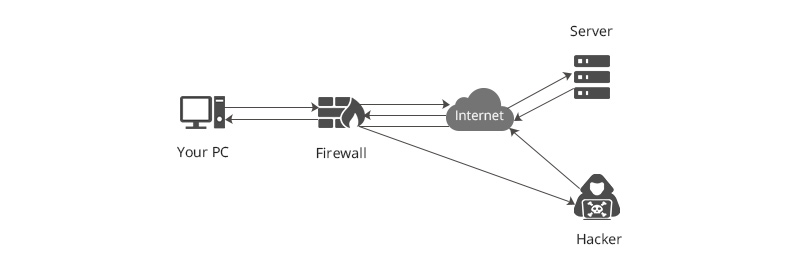
**از نظر اصل کار**

درگاه معمولاً در لایه OSI4 یا بالاتر کار می‌کند و پروتکل‌ها را ترجمه می‌کند تا به پایانه‌های دو شبکه مختلف اجازه ارتباط با یکدیگر را بدهد همچنین درگاه می‌توانند سخت‌افزاری و نرم‌افزاری باشد یا ترکیبی از هر دو برابر اصول کار با عملکردهایی که انجام می‌دهند تعیین می‌شود. تصویر زیر روش کار درگاه برنامه را نشان می‌دهد.



ترافیک ورودی براساس قوانین ازپیش‌تعیین‌شده به‌دقت تجزیه‌وتحلیل می‌کنند و توسط فایروال ها تجزیه‌وتحلیل می‌گردد و برای جلوگیری از حملات ترافیکی که از منابع ناامن یا مشکوک داریم فیلتر می‌کند. همچنین ترافیک‌ها را در محل ورودی رایانه یا همان پارت‌ها که تبادل اطلاعات در این نقاط صورت می‌گیرد محافظت می‌کند.

اساساً فایروال مانند نگهبانان امنیتی در مقابل ورودی خانه عمل می‌کند که بازدیدکنندگانی را که می‌آیند شناسایی و از ورود افراد غیرمجاز جلوگیری کند. همچنین فایروال از ورود اطلاعات مزاحم ناامن به رایانه شخصی جلوگیری کرده و ترافیک و کامپیوتر را با استفاده از آدرس IP، شماره پورت و پروتکل ها فیلتر می‌کند.



**جمع‌بندی نهایی**

در مقایسه درگاه با فایروال موارد مهم بررسی شد. که فایروال و درگاه‌ها می‌توانند بین اینترنت و اینترانت/ LAN استفاده گردد. هنگامی‌که از دستگاه شبکه مثل روترها یا سوئیچ‌ها به‌عنوان درگاه شبکه استفاده می‌شود می‌توان از آن به‌عنوان فایروال در همان شبکه استفاده کرد. اگر می‌خواهید دو شبکه مختلف با پروتکل مختلف را داشته باشیم درگاه می‌تواند مطابق با خواسته شما عمل کند یا اگر می‌خواهید از حمله هکر ها جلوگیری کنید فایروال ها بهترین راه‌حل برای شما هستند.

[**منبع**](https://community.fs.com/blog/gateway-vs-firewall-what-are-the-differences.html)