فایروال (Firewall)

فایروال مانند در یک ساختمان است و به بسته هایی که مجوز ورود یا خروج از شبکه را دارند اجازه می دهد و در مقابل از ورود یا خروج بسته های غیرمجازجلوگیری می کند.

۱- سرویس IDS با توجه به پایگاه داده ای که از الگوی حملات دارد قادر به شناسایی انواع حملات و سرویس IPS در به جلوگیری و خنثی کردن حملات است.
۲- آنتی ویروس و Spam : یکی دیگر از سرویس های مهم برای جلوگیری از حملات در شبکه ها هستند که ورود ویروس ها و هرزنامه ها به شبکه و سیستم ها جلوگیری می کنند.
۳- سرویس فایروال (Firewall) : این سرویس توانایی های زیادی در جلوگیری از ورود بسته های مشکوک به شبکه دارد . به همین خاطر یکی از فرصت های شغلی برای افراد فعال در حوزه امنیت، نصب و پیکربندی فایروال است.

** برای بازبینی بسته های اطلاعاتی در سیستم های رایانه ای و شبکه ها از فایروال استفاده می شود.

انواع فایروال : ۱- نرم افزاری ۲- سخت افزاری

** فایروال : سیستم های رایانه ای را از دسترسی نفوذگران محافظت کرده، تمام بسته های عبوری را بررسی می کند و در صورت تشخیص غیرمجاز بودن بسته، از ورود آن به شبکه جلوگیری می کند.

** فایروال نرم افزاری مثل بقیه نرم افزار ها روی سیستم عامل نصب می شود.
** به بررسی بسته ها به وسیله فایروال، فیلترکردن بسته ها می گویند.
** فایروال ویندوز، نرم افزارهای ISA Server و Kerio Control و برخی از نرم افزار های آنتی ویروس نمونه ای از فایروال نرم افزاری هستند.

فایروال سخت افزاری :

۱. روی برد های سخت افزاری پیاده سازی شده، در قالب یک سخت افزار مستقل عرضه می شوند
۲. برای شبکه های بزرگ استفاده می شوند .
۳. بار ترافیکی کمتری روی شبکه دارند
٤. هزینه آنها بیشتر است
٥. باید یک متخصص شبکه آن را پیکربندی و آزمایش کند.

** سرویس فایروال مسیریاب میکروتیک از این نمونه است.

انواع فایروال بر اساس فیلترینگ

۱. Packet Filter
۲. Stateful Firewall
۳. Application Proxy Firewall

Packet Filter

این فایروال ها با استفاده از مجموعه ای از قوانین که برای آنها تعریف می شوند، بسته های ورودی و خروجی را بررسی می کنند و تصمیم می گیرند که بسته را عبور دهند یا دور بیندازند. به این قوانین، رول Rule میگویند.

روال های فایروال بر چه اساسی نوشته می شود ؟

۱. نوع پروتکل
۲. آدر ip مبدا
۳. شماره درگاه مبدا
۴. آدرس ip مقصد
۵. شماره درگاه مقصد
۶. رابط کارت شبکه (اینترفیس)

** در این فایروال ها تعدادی رول پشت سر هم نوشته شده است که هر بسته ورودی از ابتدای فهرست با تک تک رول ها مطابقت داده می شود و به محض اینکه با یک رول تطابق داشته باشد، بر اساس آن رول یا عبور داده می شود و یا دور انداخته می شود. بنابراین رول های بعدی بررسی نخواهند شد.

مزایا : این فایروال ها می توان به سادگی کار با آن و سرعت عملکرد آن اشاره کرد؛ زیرا درگیر پردازش محتوای بسته ها نمی شوند.

معایب : در شناسایی بسیاری از حملات اینترنتی ضعیف هستند و توانایی مسدودسازی اکثراپلیکیشن ها را ندارند.

همانند :

۱- فایروال ویندوز و برنامه های
۲- آنتی ویروس نسخه Internet Security

Stateful Firewall

به فایروال حالت مند هم معروف است به شیوه دقیق تری کار می کند

عملکرد این گونه فایروال ها چگونه است ؟

به این صورت است که در حافظه cache خود یک جدول وضعیت بسته دارد. برای هر بسته علاوه بر آدرس ip ، درگاه و نوع پروتکل یک فیلد دیگر به نام state در نظر گرفته می شود.

این نوع فایروال علاوه بر مواردی که در فایروال Packet Filter مطرح شد با بررسی حالت های مختلف بسته ها، به راحتی قادر به اعمال فیلترینگ روی ارتباطات و برنامه ها است. این کار مدت زمان بیشتری برای بررسی تمام بسته ها لازم دارد در عین حال امنیت بیشتری در پی دارد و قیمت آن نیز گران تر است.