نظارتی همه‌جانبه بر ترافیک وارد و خارج‌شونده

دیوار آتش‌ها چگونه می‌توانند از شبکه‌ها و سامانه‌های کامپیوتری محافظت کنند؟

اینترنت فضای جالب و شگفت‌انگیزی برای اکتشاف است و بدون شک یکی از دستاوردهای بزرگ بشریت به شمار می‌رود. در واقعیت وب تشکیل شده از سرورها و روترهای فراوانی است که بزرگ‌ترین شبکه را ساخته‌اند. سؤال اینجا است که چطور امنیت این دنیا و اطلاعات موجود در آن تأمین می‌شود؟ چه کسانی باید امنیت اینترنت را تأمین کنند؟ و به چه ابزارهایی برای این کار نیاز دارند؟ سازمان خاصی وجود ندارد که مسئولیت امنیت اینترنت را بر عهده داشته باشد. حفاظت از دروازه‌های اینترنت جزء یکی از مشاغلی است که متخصصان این حوزه با استفاده از سخت‌افزارها و نرم‌افزارهایی مانند روتر، سوئیچ، سیستم عامل، اپلیکیشن و دیوارآتش آن را اجرا می‌کنند. در این مقاله صحبتمان را به طور خاص روی دیوارآتش متمرکز می‌کنیم.

دیوارآتش چیست و چه کسانی به آن نیاز دارند؟

واژه «دیوارآتش» یا «فایروال» اولین بار در سال 1764 استفاده شد، زمانی که از دیوار برای جلوگیری از انتشار آتش به همه قسمت‌های ساختمان استفاده می‌شد. این واژه در امنیت شبکه‌های کامپیوتری در دهه 1980 مورد استفاده قرار گرفت که روترها برای جداسازی شبکه‌ها از فایروال استفاده کردند. فایروال یک سیستم یا مجموعه‌ای از سیستم‌ها است که در لبه ارتباطات اینترنتی قرار گرفته و سیاست کنترل دسترسی بین دو یا چند شبکه را اجرا می‌کند. قوانین و وظایفی که برای یک فایروال تعریف می‌شود، تحت عنوان Rule شناخته می‌شود.

وظایف یک فایروال گسترده است، اما به طور کلی دو وظیفه پایه‌ای وجود دارد: یکی بلوکه کردن ترافیک و دیگری دادن اجازه عبور ترافیک. احتمالاً مهم‌ترین چیزی که برای استفاده درست از فایروال نیاز دارید، سیاست‌های دقیق کنترل دسترسی (تعریف rule مناسب) است و اگر ایده خوبی برای نوع دسترسی‌های مجاز و غیرمجاز نداشته باشید، فایروال کمکی به شما نخواهد کرد. مورد دیگری که اهمیت بالایی دارد، نحوه پیکربندی فایروال است، زیرا سیاست‌های لازم روی هر چیزی که در پس آن قرار دارد اعمال می‌شود و گاهاً پیکربندی نادرست باعث زیان بیشتری نسبت به نداشتن فایروال می‌شود. به‌علاوه در بیشتر موارد، فایروال در شبکه‌ای قرار دارد که میزبان‌های زیادی وجود دارند و کسانی که مدیریت دیوارآتش را انجام می‌دهند، مسئولیت زیادی را به دوش می‌کشند.

ساده‌ترین سؤالی که پرسیده می‌شود این است که چه کسانی در چه زمانی به فایروال نیاز دارند؟ اگر قصد اتصال به اینترنت یا شبکه‌ای دیگر را دارید به یک فایروال نیاز دارید و اهمیتی ندارد که در خانه، شرکت یا مکانی دیگر هستید. گاهی برای مقابله با عوامل غیرمعتبری که قصد ارسال داده به داخل را دارند (مثلاً مقابله با نفوذ هکرها و حملات DoS)، گاهی برای جلوگیری از ارسال ترافیک به خارج سازمان، گاهی برای کنترل ایمیل‌ها وغیره. علاوه بر این موارد، فایروال اطلاعات زیادی درباره حجم ترافیک ارسالی و دریافتی، تعداد دفعات برقراری ارتباط و نوع ترافیک تهیه می‌کند و می‌تواند در صورت نیاز هشدارهای لازم را اعلام کند. با این حال یک فایروال به‌تنهایی نمی‌تواند امنیت کامل سیستم‌ها را فراهم کند، بخش زیادی از نفوذها از طریق فلش‌های USB صورت می‌پذیرد، اطلاعات گاهی به سرقت می‌روند و رمزنگاری بر روی آن‌ها اعمال نشده است. وجود در پشتی نیز گاهی دردسرساز می‌شود.

نحوه عملکرد فایروال

نحوه کار یک نوع فایروال را می‌توان به کمک شکل 1 فراگرفت. فایروال‌ها از ACL (Access Control List) برای فیلتر کردن ترافیک بر اساس IP مقصد و مبدأ، پروتکل و وضعیت ارتباطات استفاده می‌کنند. برای مثال ممکن است پروتکل FTP پورت 21 برای همه مسدود باشد. اما طبق یکی از قوانین تعریف شده برای یک IP مجاز است؛ بنابراین، جز IP مشخص شده هیچ‌کس اجازه استفاده از FTP را ندارد.

Rule	Direction	Source Address	Dest. Address	Protocol	Source Port	Dest. Port	Action
A	In	External	Internal	TCP	> 1023	25	Permit
B	Out	Internal	External	TCP	25	> 1023	Permit
C	Out	Internal	External	TCP	> 1023	25	Permit
D	In	External	Internal	TCP	25	> 1023	Permit
E	Either	Any	Any	Any	Any	Any	Deny

شکل 1- نمونه‌ای از rule تعریف شده برای یک فایروال (packet filtering)

مطلب پیشنهادی

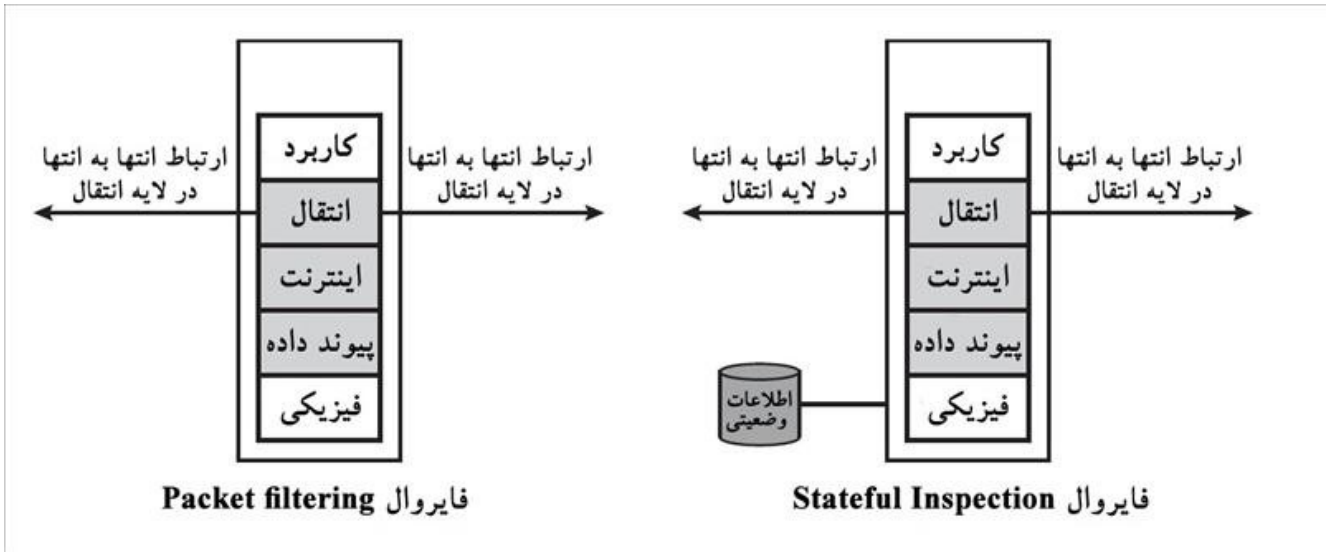
یک ویژگی امنیتی در اختیار توسعه‌دهندگان
تا چه اندازه با دیوارآتش سرویس App Engine گوگل آشنا هستید؟

فایروال‌های سخت‌افزاری و نرم‌افزاری

از نظر ماهیت وجودی دو نوع فایروال سخت‌افزاری و نرم‌افزاری وجود دارد. نوع سخت‌افزاری یک محصول جداگانه است و سیستم عامل مختص به خود را دارد. برای پیکربندی این فایروال‌ها کار چندان دشواری نیاز نیست و تخصص چندانی لازم ندارند. این دستگاه اغلب بین روترها و ارتباطات اینترنتی قرار می‌گیرند و بیشتر استفاده آن‌ها در شرکت‌ها و سازمان‌های بزرگ است.
فایروال نرم‌افزاری انتخاب اکثر کاربران خانگی است. این نوع دیوارآتش مشابه سایر نرم‌افزارها بر روی کامپیوتر نصب می‌شوند و توانایی ایجاد تغییرات و شخصی‌سازی را به کاربر می‌دهند. برای جلوگیری از ورود تروجان‌ها، کرم‌های موجود در ایمیل، بلوکه کردن اپلیکیشن‌های ناامن و مواردی مشابه، نصب یک فایروال نرم‌افزاری به همه کاربرانی که در محیط شبکه‌ای فعالیت دارند توصیه می‌شود. البته ایراداتی هم به این نوع فایروال وارد است: استفاده از حجم زیادی از منابع، ناسازگاری با بعضی برنامه‌های دیگر و عدم کارکرد صحیح در برخی موارد.

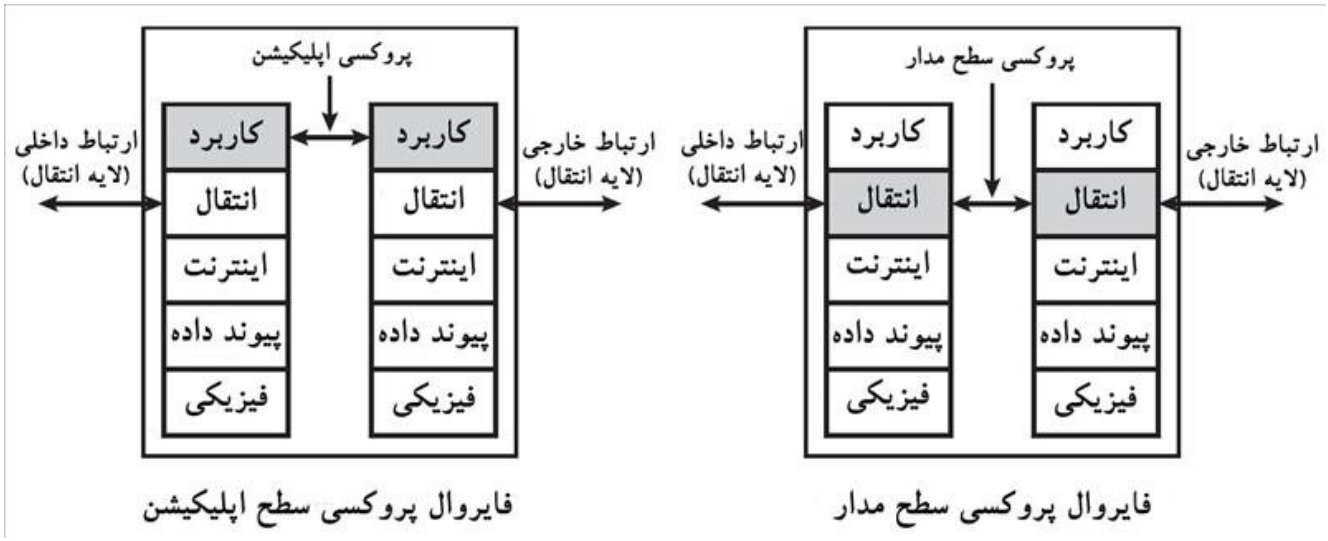
انواع فایروال

دسته‌بندی مختلفی برای فایروال‌ها وجود دارد که در یک نمونه پایه‌ای از آن‌ها (بر حسب فناوری) این چهار نوع وجود دارند: فیلترینگ بسته (Packet Filtering)، بررسی حالتمند (Stateful Inspection)، دروازه سطح اپلیکیشن (Application-Level Gateway) و دروازه سطح مدار (Circuit-Level Gateway).
یک فایروال packet filtering مجموعه‌ای از قواعد را روی بسته‌های IP اعمال می‌کند و بدین ترتیب باعث انتقال یا حذف این بسته‌ها در مسیر ارسال یا دریافت می‌شود. قواعد بر پایه اطلاعات موجود در بسته‌های IP مانند نشانی IP مبدأ و مقصد و شماره پورت هستند. در ضمن یک قاعده پیش‌فرض نیز وجود دارد که در صورت عدم تطابق با همه قواعد این مورد اعمال می‌شود (و معمولاً ترافیک را بلوکه می‌کند). قبلاً فایروال‌های stateless وجود داشت که تنها تا لایه سوم و سرآیند بسته را مورد بررسی قرار می‌دادند و بنابراین بسته‌های یک ارتباط را تشخیص نمی‌دادند. اما با تغییرات این دسته فایروال‌های Stateful Packet Filtering یا SPI (Stateful Packet Inspection) به وجود آمد.
این نوع از دیوارآتش اطلاعات مربوط به ارتباطات را در جدولی نگهداری می‌کند و بدین ترتیب مشخص می‌شود کدام بسته جزء کدام ترافیک است. این دو نسل از شبکه‌ها که جزء Network-Level محسوب می‌شوند، در شکل 2 نشان داده شده‌اند.



شکل 2- فایروال‌های فیلترینگ بسته و بازرسی حالتمند

فایروال Application-Level Gateway یا Application Proxy که به‌عنوان نسل سوم شناخته می‌شود، قادر هستند تا لایه 7 را کنترل کنند. پروکسی‌ها بین مشتری و سرور قرار می‌گیرد و توانایی شناخت و کنترل پروتکل‌ها را دارند. این نوع فایروال قادر است ترافیک HTTP که برای دستیابی به صفحات وب و ترافیک HTTP که برای به اشتراک‌گذاری فایل استفاده می‌شود را از یکدیگر تشخیص دهد. (شکل 3)



شکل 3- فایروال‌های سطح مدار و سطح اپلیکیشن

نوع چهارم دروازه (پروکسی) سطح مدار است که می‌تواند یک سیستم جداگانه یا به‌عنوان یک عملکرد روی یک اپلیکیشن خاص نصب شود. این فایروال اجازه یک اتصال TCP انتها به انتها را نمی‌دهد، در عوض دو اتصال TCP برقرار می‌کنند که یکی بین پروکسی و میزبان داخلی و دیگری بین پروکسی و میزبان خارجی است. یکی از موارد استفاده این فایروال زمانی است که مدیر سازمان به کاربران داخلی اعتماد دارد، در این حالت دروازه سطح اپلیکیشن برای ارتباطات داخلی و دروازه سطح مدار برای ارتباطات خارجی مورد استفاده قرار می‌گیرد. مزیت آن هم بررسی نشدن ترافیک اضافی خارج از شبکه است. (شکل 3)

نسل بعدی فایروال‌ها NGFW(Next Generation Firewalls)

این‌که اصلاً چرا به فایروال‌های پیشرفته‌تر نیاز داریم به این دلیل است که حملات و مخرب‌ها نیز همواره بیشتر و پیچیده‌تر می‌شوند. ارتباطات سازمان‌ها تنها به یک ایمیل محدود نمی‌شود، بلکه تبادل اطلاعات به‌صورت بی‌درنگ، VoIP، اپلیکیشن‌های نظیر به نظیر، استریم ویدئو و بسیاری دیگر را نیز شامل می‌شود.

NGFW جزئی از فناوری نسل سوم فایروال‌ها است که فایروال‌های سنتی را با دیگر فناوری‌های فیلترینگ شبکه ترکیب می‌کند مانند یک فایروال اپلیکیشن یا سیستم مقابله با نفوذ (IDS). فناوری دیگری نیز می‌تواند به کار گرفته شود از جمله: بازرسی ترافیک رمزگذاری شده TLS/SSL، فیلترینگ وب‌سایت، مدیریت پهنای باند و مدیریت سرویس، بازرسی آنتی‌ویروس و امثال آن. هدف NGFW در واقع پوشش بیشتر لایه‌های مدل OSI و بهبود فیلترینگ ترافیک شبکه است که به محتوای بسته‌ها مربوط می‌شود. این نوع فایروال‌ها بازرسی عمیق‌تری نسبت به نسل اول و دوم فایروال‌ها دارند، محتوای بسته‌ها را بررسی می‌کنند و امضا را برای حمله‌ها و malware مطابقت می‌دهند. اینکه چرا امنیت به‌سمت محتوا ـ محور بودن در حرکت است به این دلیل است سیستم‌های امنیتی بر پایه اطلاعات موقعیتی مانند زمان، مکان، دستگاه و عملکرد تجاری ساخته شده‌اند. این سیستم‌های امنیتی مناسب محیط‌های موبایلی و ابری هستند و در صورت قرارگیری در شرایط ناخواسته می‌توانند عملکرد مناسب را اعمال کنند.

مطلب پیشنهادی

چند ترفند ساده برای پیش‌گیری از هک
چگونه از روترها در برابر حملات هکری محافظت به عمل آوریم؟

فایروال بر پایه یادگیری ماشینی

همواره از ایده‌های مطرح شده در این خصوص بوده است که همیشه نباید به یک فایروال دستور داد. اختیار عمل فایروال و ایجاد تغییرات در rule باعث مقابله با تهدیدهای جدید و ناشناخته می‌شود. همچنین اشتباهاتی که در اعمال محدودیت‌ها رخ می‌دهد، می‌تواند اصلاح شود. این دسته از فایروال‌ها بر اساس مدل‌های یادگیری ماشینی به‌دنبال جست‌وجوی ارتباط میان داده‌ها هستند. با استفاده از تحلیل ترافیک، موقعیت و بسیاری از عوامل دیگر ارائه عملکرد مناسب‌تری از یک فایروال را خواهیم دید. این نوع فایروال‌ها گزینه مناسبی برای مقابله با هکرهایی هستند که آن‌ها نیز از یادگیری ماشینی برای سبک کردن کار خود استفاده می‌کنند.

سخن آخر

بدون شک مقابله با تمام تهدیدها در محیط شبکه‌ای به‌خصوص اینترنت امکان‌پذیر نیست و بسیاری از راهکارهای ارائه شده بعد از ایجاد حمله به وجود می‌آیند. با این حال نصب یک فایروال در کنار دیگر مجموعه‌های امنیتی امری ضروری برای سازمان‌ها و کاربران عادی است و مسئله‌ای نیست که نادیده گرفته شود

تاریخ انتشار:

30 بهمن 1396

نشانی منبع:
https://www.shabakeh-mag.com/tricks/network-tricks/11378/%D8%AF%DB%8C%D9%88%D8%A7%D8%B1-%D8%A2%D8%AA%D8%B4%E2%80%8C%D9%87%D8%A7-%DA%86%DA%AF%D9%88%D9%86%D9%87-%D9%85%D9%89%E2%80%8C%D8%AA%D9%88%D8%A7%D9%86%D9%86%D8%AF-%D8%A7%D8%B2-%D8%B4%D8%A8%DA%A9%D9%87%E2%80%8C%D9%87%D8%A7-%D9%88-%D8%B3%D8%A7%D9%85%D8%A7%D9%86%D9%87%E2%80%8C%D9%87%D8%A7%D9%89-%DA%A9%D8%A7%D9%85%D9%BE%DB%8C%D9%88%D8%AA%D8%B1%D9%89-%D9%85%D8%AD%D8%A7%D9%81%D8%B8%D8%AA