نحوه پیکربندی پیاده‌سازی دیوارآتش ویندوز

دیوارآتش از پیش ساخته شده ویندوز یک بسته امنیتی رایگان و قدرتمند

ما برای محافظت از سامانه‌های خود به محصولات امنیتی قدرتمندی نیاز داریم. در این میان نقش دیوار آتش (firewall) از آن جهت حائز اهمیت است که به ما اطلاع می‌دهد چه اطلاعاتی به درون کامپیوتر ما وارد شده یا در حال خارج شدن از آن هستند. اطلاعاتی که ممکن است به شکل پنهانی از سامانه‌های ما خارج شوند. حصاری میان یک سامانه کامپیوتری و جهان خارج از آن ساده‌ترین تعریفی است که برای دیوار آتش (firewall) می‌توان ارائه کرد. اگر سامانه کامپیوتری شما به یک دیوار آتش خوب تجهیز شده باشد در بیشتر موارد از شما در برابر تهدیدات امنیتی محافظت به عمل می‌آورد.

زمانی که برنامه‌ای مخرب روی یک سیستم نصب می‌شود، در نخستین فرصت سعی می‌کند به اینترنت متصل شده، به تبادل اطلاعات پرداخته و دستورات موردنظر را دریافت کند. در چنین شرایطی این وظیفه **دیوارآتش** (**firewall**) است که این موضوع را بررسی کرده و در صورت مشاهده فعالیت مشکوکی که از نظر امنیتی خطرآفرین است کاربر را مطلع کند. در این حالت کاربر می‌تواند این عملیات را لغو کرده یا ادامه دهد. یک دیوارآتش را مجموعه‌ای از مولفه‌های مرتبط با یکدیگر شکل می‌دهند. در ایده‌آل‌ترین حالت نصب دیوارآتش در ورودی یک شبکه از منابع شبکه و کاربرانی که درون یک شبکه قرار دارند محافظت می‌کند. دیوارهای آتش به دو صورت نرم‌افزاری و سخت‌افزاری و در برخی موارد ترکیبی از دو حالت فوق در اختیار کاربران قرار دارند، به‌عنوان مثال، دیوار آتش داخلی ویندوز 10 که همراه با **ابزار امنیتی** دیفندر یکپارچه شده این توانایی را دارد تا درگاه‌های یک سامانه کامپیوتر را تحت نظارت قرار داده و به کاربر اجازه دهد درگاه‌های موردنظر خود را مسدود کرده و به این شکل نظارت دقیقی بر ترافیک سامانه خود اعمال کند. این سامانه همچنین این پتانسیل را دارد تا با سایر دیوارهای آتش موجود ترکیب‌شده و یک‌لایه امنیتی اضافی و مستحکم‌تر را به وجود آورد تا به این شکل سامانه کامپیوتری شما از دید هکرها در 90 درصد موارد پنهان باقی بماند. به‌طورکلی، وظیفه یک **دیوارآتش** (**firewall**) خوب ممانعت از دستیابی غیرمجاز به یک سیستم است. اما در دنیای امنیت شرکت‌های مختلفی وجود دارند که با توجه به نیاز کاربران نرم‌افزارهای سفارشی و عمومی را تولید می‌کنند.

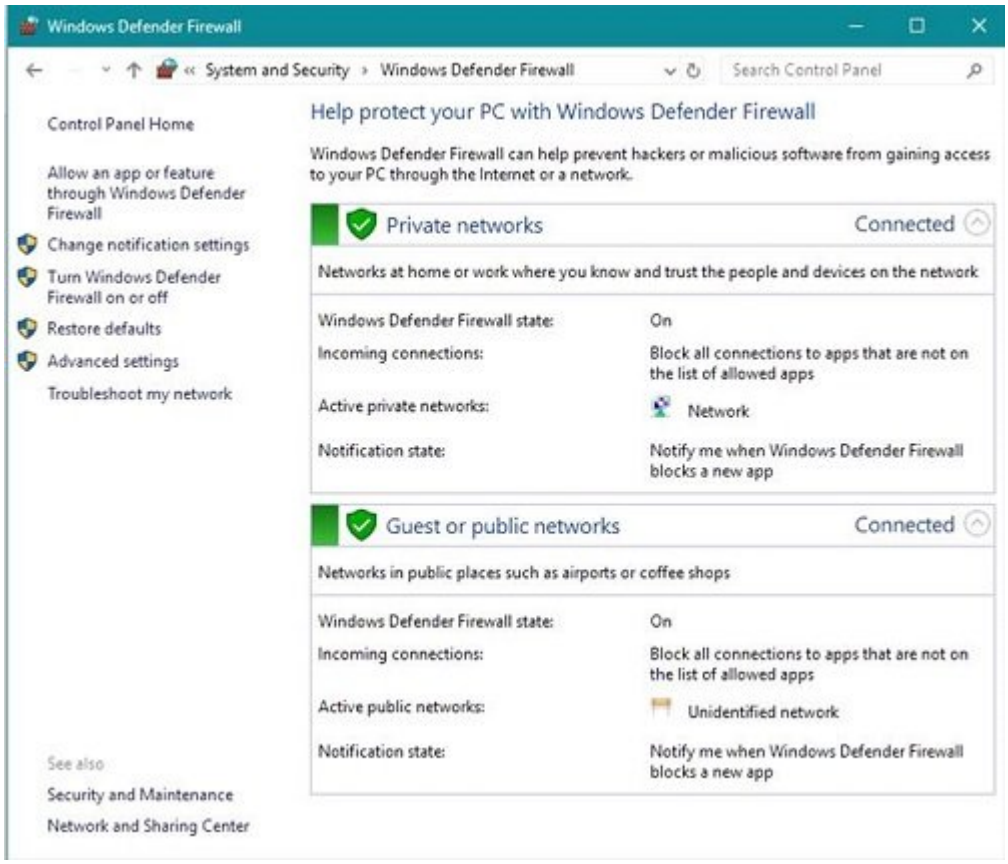
مطلب پیشنهادی

محافظت از داده‌های مالی و نام تجاری
چگونه می‌توانیم از شبکه، سرورها و نقاط پایانی کسب‌وکارمان در برابر هکرها محافظت کنیم؟

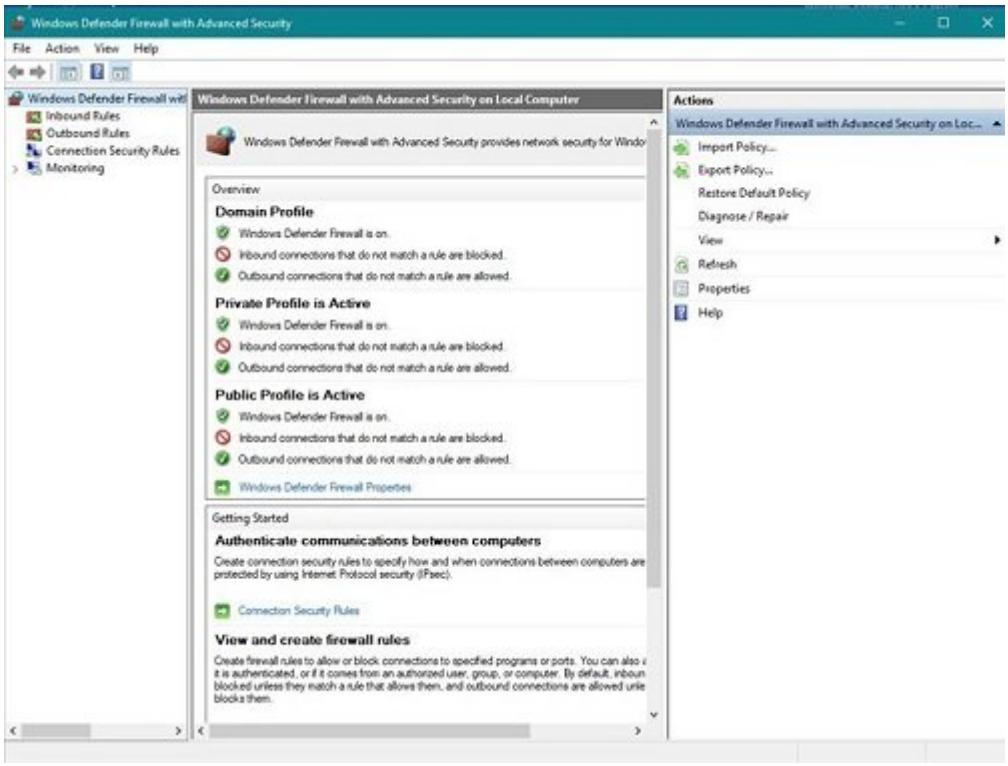
نرم‌افزارهایی که هر کدام مجموعه‌ای از **نرم‌افزارهای امنیتی** همچون ضدویروس‌ها، دیوارهای‌آتش و ضدهرزنامه‌ها را در قالب یک مجموعه واحد در اختیار کاربران قرار می‌دهند. در این میان **دیوارآتش ویندوز** که به‌طور پیش‌فرض همراه با این سیستم‌عامل ارائه می‌شود، به شکل عادی در اختیار کاربران قرار دارد که بدون نیاز به ابزار اضافی روی یک سیستم نصب‌شده است. زمانی‌که دیوارآتش فعال باشد، بسته‌های داده‌ای را که به یک سامانه کامپیوتری یا شبکه ارسال‌شده یا از آن خارج می‌شوند به همراه پورت‌ها تحت کنترل قرار می‌دهد و اگر به فعالیت مشکوکی برخورد کند، واکنش مناسب از خود نشان می‌دهد. دیوارآتش ویندوز، به دلیل این‌که به‌عنوان یکی از مولفه‌های ادغام‌شده با ویندوز ارائه می‌شود، کمترین تداخل را با برنامه‌های جانبی نصب‌شده روی یک سیستم دارد. اما به‌طورکلی برای این‌که دیوارهای آتش بتوانند از عهده این فرآیندها برآیند باید از مکانیزم‌ها و روش‌های مختلفی برای رصد داده‌های مبادله شده استفاده کنند که از میان روش‌های به کارگرفته شده توسط دیوارهای آتش می‌توان به فیلتر کردن بسته‌های داده‌ای اشاره کرد. در این روش هر بسته وارد یا خارج‌شده از شبکه بر مبنای یکسری قواعدی که کاربر آن‌ها را مشخص کرده پذیرفته یا رد می‌شوند. این تکنیک هرچند روش موثری در کنترل داده‌ها است اما پیکربندی آن کار چندان راحتی نیست. در روش دیگری از مکانیزم‌های امنیتی برای مشخص کردن پروتکل‌های خاصی همچون اف‌تی‌پی، اچ‌تی‌تی‌پی و.... استفاده می‌شود. در این راهکار با اعمال محدودیت روی آدرس‌های اینترنتی، نام دامنه‌ها و... نظارت دقیقی بر ورودی‌های وب اعمال می‌شود. اما مهم‌ترین فاکتوری که در استفاده بهینه از یک **دیوارآتش** (**firewall**) نقش دارد به قابلیت سفارشی‌سازی این نرم‌افزار بازمی‌گردد. تنظیماتی که با استفاده از آن‌ها می‌توان گزارش‌های تولیدشده را ثبت کرد، یک پیغام هشدار در زمان یک ورود غیرمجاز نشان داد و کارهایی از این قبیل را که در ظاهر ساده اما مهم هستند، اعمال کرد.

دسترسی به دیوارآتش (firewall) ویندوز

برای دسترسی به **دیوارآتش** (**firewall**) ویندوز 10 و تنظیمات مربوط به این مولفه **امنیتی** عبارت Windows Defender Firewall را در کادر جست‌وجوی کورتانا وارد کرده و روی گزینه نشان داده‌شده کلیک کنید. با این کار پنجره مربوط به دیوار آتش نشان داده می‌شود. (شکل1)



گزینه‌های مختلفی در ارتباط با **دیوارآتش** (**firewall**) **ویندوز** وجود دارد. (شکل2) به‌عنوان مثال برای خاموش یا روشن کردن **دیوارآتش** کافی است روی گزینه Turn Windows Defender Firewall on or off کلیک کرده و در صفحه ظاهرشده **دیوارآتش** را فعال یا غیر فعال کنید.



تنظیمات مربوط به دیوارآتش (firewall) ویندوز

دیوارآتش (**firewall**) **ویندوز** به شکل پیش‌فرض همراه با یکسری تنظیمات اولیه در اختیار کاربران قرار می‌گیرد. اما برای بالابردن ضریب **امنیت** سیستم می‌توان از تنظیمات پیشرفته‌تری استفاده کرد.
برای این منظور در پانل سمت چپ پنجره اگر روی گزینه Advanced Settings کلیک کنید، پنجره مربوط به تنظیمات پیشرفته موسوم به Windows Firewall with Advanced Security همانند شکل2 ظاهر می‌شود.
همان‌گونه که در شکل2 مشاهده می‌کنید، این تنظیمات در سه پانل قرار دارند. در پانل وسط اطلاعاتی در خصوص وضعیت دیوارآتش نشان داده می‌شود که برای هر کدام پیوندی وجود دارد که با کلیک روی آن پیوند به قواعد پیشرفته‌تری که قابل تنظیم هستند، دسترسی خواهید داشت. در پانل سمت راست که به‌نام Action نامیده می‌شود، به سیاست‌هایی که برای دیوارآتش قابل تنظیم هستند دسترسی خواهید داشت.

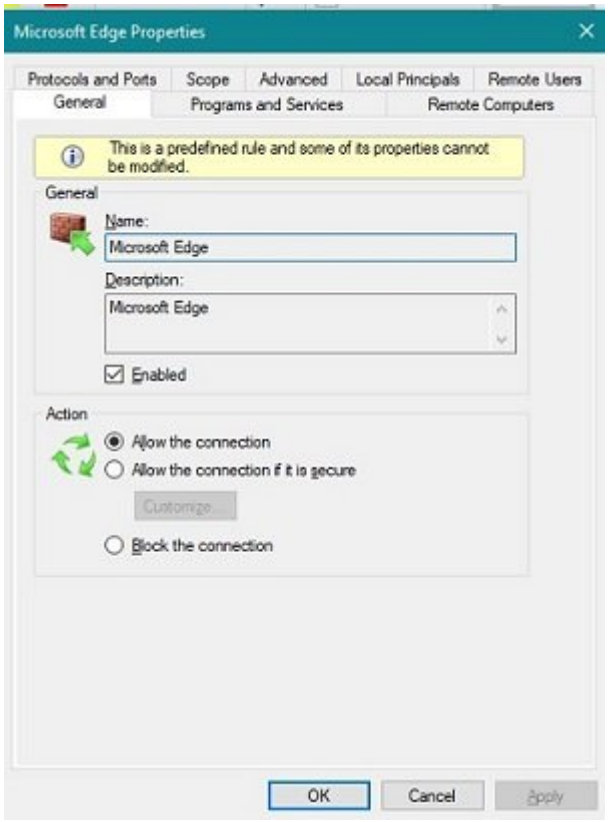
مطلب پیشنهادی

مقابله با تهدیدات از درون هسته سیستم‌عامل
فناوری ممانعت از اجرای داده‌ها در ویندوز چیست و چگونه فعال می‌شود؟

مدیریت تنظیمات در دیوارآتش (firewall)

با استفاده از پانل سمت چپ امکان ساخت قواعدی وجود دارد که بر ارتباطات وارد و خارج‌شونده بر سامانه تاثیرگذار خواهد بود. قواعد وارد شونده (Inbound) تنظیماتی هستند که روی ارتباطاتی که از طریق سیستم‌عامل ساخته می‌شوند و به منظور برقراری ارتباط با شبکه مورداستفاده قرار می‌گیرند، تاثیر می‌گذارند. قواعد خارج شونده (Outbound) تنظیماتی هستند که روی نرم‌افزارهای ویندوز برنامه‌هایی که از سوی کاربر نصب‌شده‌اند و در زمان اتصال به اینترنت تمایل به دریافت و ارسال اطلاعاتی دارند، اثرگذار خواهند بود. با کلیک روی هر کدام از گزینه‌های فوق برنامه‌هایی که این قواعد برای آن‌ها تنظیم شده، نشان داده می‌شوند. برای دسترسی به این قواعد کافی است روی برنامه مورد نظر کلیک راست کرده و گزینه Properties را انتخاب کنید. با این‌کار گزینه‌های قابل تنظیم برای برنامه مورنظر نشان داده می‌شود. به‌عنوان مثال، در شکل3 ما روی گزینه Inbound کلیک کرده و از

میان برنامه‌های موجود برنامه مایکروسافت اج را انتخاب کرده‌ایم.



این‌کار باعث می‌شود تا پنجره مربوط به تنظیمات اعمال شده در ارتباط با این برنامه ظاهر شود. این پنجره اجازه می‌دهد تنظیمات مدنظر خود را به شکل سفارشی در ارتباط با این برنامه اعمال کنید. گزینه‌ها و زبانه‌هایی که در ادامه به معرفی آن‌ها خواهیم پرداخت در ارتباط با سایر برنامه‌ها صدق کرده و در نتیجه این تنظیمات را در ارتباط با سایر برنامه‌ها می‌توانید به کار ببرید. زبانه‌های موجود در این پنجره به شرح زیر هستند.

General

این زبانه اطلاعات کلی مرتبط با قواعد **دیوارآتش** (**firewall**) را به همراه تنظیماتی که برای بلوکه کردن اطلاعات وجود دارند، در اختیارتان قرار می‌دهد. همچنین، امکان درج نام و توضیحی در ارتباط با برنامه موردنظر در این بخش وجود دارد.

Program and Services

اگر قواعد **دیوارآتش** (**firewall**) برای برنامه‌های خاص یا سرویس‌های خاصی از ویندوز به شکل سفارشی تنظیم شوند، امکان مشخص کردن برنامه‌ها، سرویس‌ها و اعمال مدیریت بر آن‌ها در این بخش امکان‌پذیر است.

Remote Computers

این زبانه برای کنترل ارتباطات **دیوارآتش** (**firewall**) و نحوه دسترسی کامپیوترهای از راه دور به یک سامانه مورد استفاده قرار می‌گیرند. با استفاده از این زبانه می‌توانید محدودیت‌هایی را اعمال کرده یا حالت‌های استثنایی را تنظیم کنید. به‌عنوان مثال، در بخش Authorized computers می‌توانید مشخص کنید چه کامپیوترهایی توانایی برقراری ارتباط دارند.

Protocols and Ports

یک سامانه کامپیوتری 65335 پورت دارد که هر کدام مسئولیت داخل و خارج کردن اطلاعات خاصی را بر عهده دارند. برخی از این پورت‌ها برای مقاصد خاصی رزرو شده‌اند. به‌عنوان مثال، پروتکل‌های اینترنتی هر کدام از پورت‌های مخصوص به خود استفاده می‌کنند.

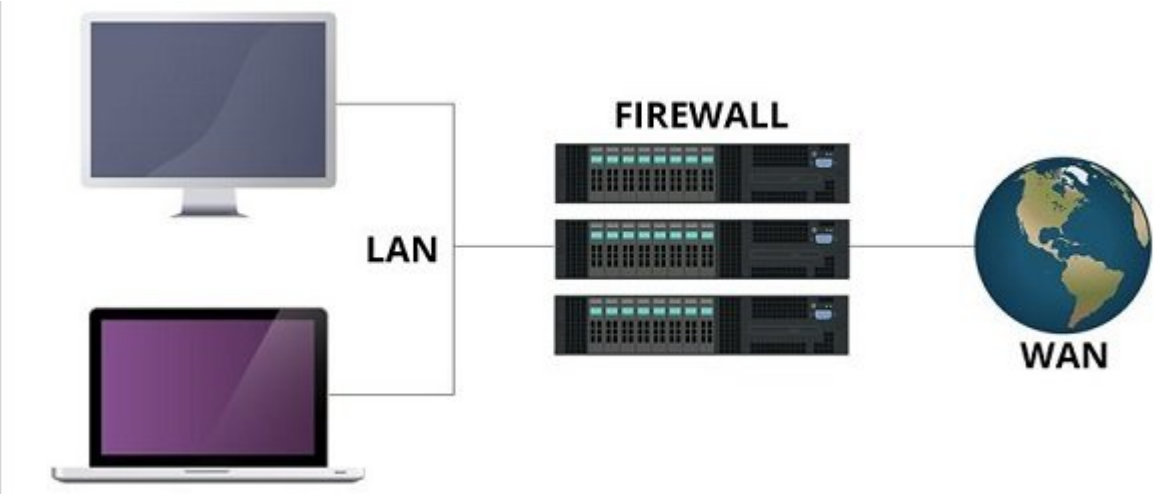
زمانی‌که در نظر دارید به اینترنت متصل شوید، برای دسترسی به اطلاعاتی که روی صفحات وب قرار دارند در حالت عادی از پورت شماره 80 استفاده می‌کنید. پورتی که پروتکل HTTP از آن استفاده می‌کند. در سازمان‌های شخصی یا دولتی با توجه به نیاز کاری سازمان بعضی مواقع لازم است بعضی از این پورت‌ها، پروتکل‌های ارتباطی و پورت‌های راه دور بسته یا باز شوند. با استفاده از این زبانه می‌توانید این فرآیندها را سازمان‌دهی کنید.

Scope

در این زبانه می‌توان دستیابی به/از آدرس‌های آی‌پی مشخصی را محدود کرد و به این شکل یک فهرست سیاه یا سفید ایجاد کرد.

Advanced

در این زبانه پروفایلی را می‌توان تنظیم کرد که بر مبنای یک دستورالعمل مشخصی کار کند. به‌عنوان مثال، می‌توان مشخص کرد یک قاعده زمانی اجرا شود که شما به یک شبکه عمومی با یک ارتباط خاص متصل می‌شوید.

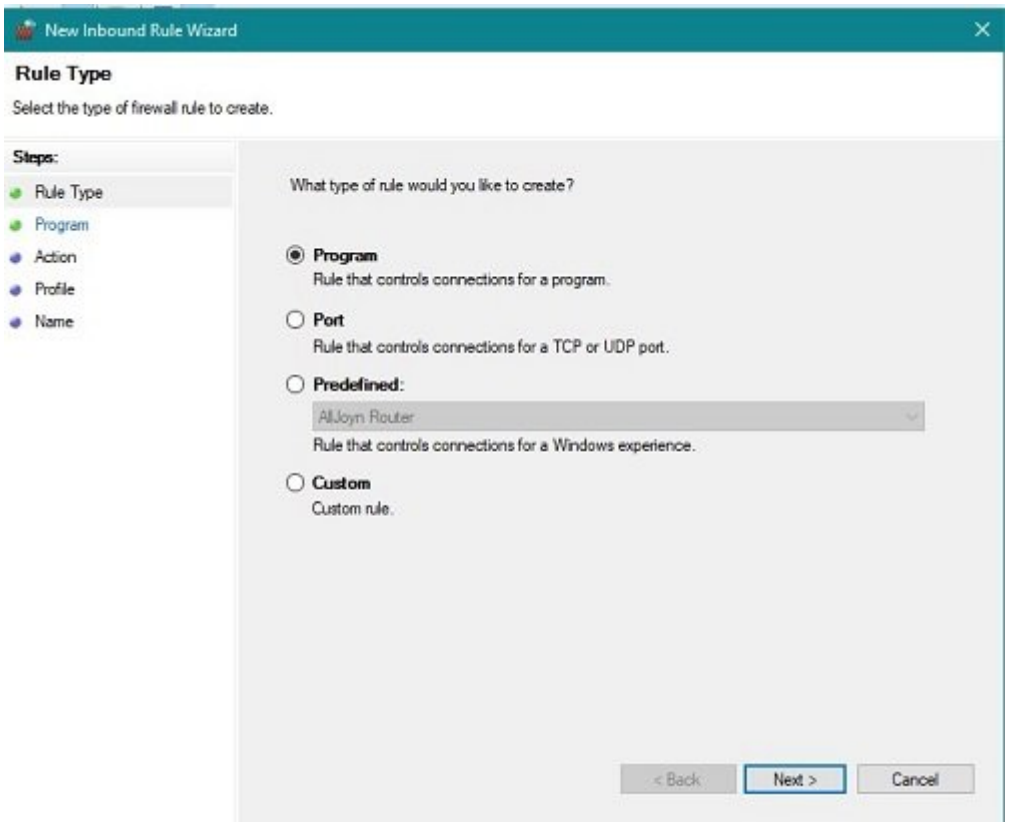


مطلب پیشنهادی

تفاوت‌ها و شباهت‌ها
فرق ضدویروس با ضدبدافزار چیست؟

اضافه کردن یک قاعده وارد و خارج شونده جدید

همان‌گونه که اشاره شد، در یک محیط حرفه‌ای لازم است تا یک قاعده (Rule) وارد یا خارج شونده سفارشی برای یک **دیوارآتش** (**firewall**) ایجاد کرد. برای آن‌که یک قاعده سفارشی را ایجاد کنید باید مراحل زیر را دنبال کنید.
گام اول، امکان ساخت یک قاعده وارد یا خارج شونده بوسیله پانل سمت چپ پنجره Windows Firewall with Advanced Security امکان‌پذیر است. انتخاب گزینه موردنظر به نیاز کاری‌تان بستگی دارد. ما در این مقاله گزینه inbound را انتخاب می‌کنیم.
گام دوم، از پانل سمت راست پنجره (Action) روی گزینه New Rule کلیک کرده تا پنجره New Inbound Rule Wizard ظاهر شود.(شکل 4)



گام سوم، در این مرحله باید مشخص کنید که این قاعده روی چه موضوعاتی اثرگذار خواهد بود. یک برنامه، یک پورت، یک سرویس ویندوز و... از جمله این موارد هستند. ما در این مقاله گزینه Program را انتخاب کرده و روی گزینه Next کلیک می‌کنیم.

گام چهارم، در این بخش باید مشخص کنید که آیا این قاعده روی همه برنامه‌ها باید اعمال شود یا در نظر دارید این قاعده روی برنامه خاصی پیاده‌سازی شود.

گام پنجم، بعد از انتخاب برنامه موردنظر روی دکمه Next کلیک کنید و به بخش Action بروید. در این مرحله باید نوع ارتباط و اتصال به شبکه را مشخص کنید. به‌عنوان مثال می‌توانید تعیین کنید هر زمان ارتباط ایمن برقرار بود، اجازه اتصال داده شود. همچنین با انتخاب گزینه مسدود کردن (Block) ارتباط برنامه یا برنامه‌ها با اینترنت متوقف می‌شود. بعد از انتخاب گزینه موردنظر روی دکمه Next کلیک کنید.

گام ششم، با کلیک روی دکمه Next به تنظیمات Profile می‌روید. با استفاده از تنظیمات این قسمت نوع شبکه ارتباطی را می‌توان مشخص کرد. آیا این قاعده روی همه شبکه‌ها اعمال شود یا شبکه خاصی مدنظرتان است.

گام هفتم، در آخرین مرحله نام قاعده موردنظر را با یک عبارت تشریح اختیاری وارد کرده و کلید Finish را انتخاب کنید تا قاعده تعیین‌شده ساخته شود.

تاریخ انتشار:

19 آبان 1397

نشانی منبع:
https://www.shabakeh-mag.com/security/13977/%D8%AF%DB%8C%D9%88%D8%A7%D8%B1%D8%A2%D8%AA%D8%B4-%D8%A7%D8%B2-%D9%BE%DB%8C%D8%B4-%D8%B3%D8%A7%D8%AE%D8%AA%D9%87-%D8%B4%D8%AF%D9%87-%D9%88%DB%8C%D9%86%D8%AF%D9%88%D8%B2-%DB%8C%DA%A9-%D8%A8%D8%B3%D8%AA%D9%87-%D8%A7%D9%85%D9%86%DB%8C%D8%AA%DB%8C-%D8%B1%D8%A7%DB%8C%DA%AF%D8%A7%D9%86-%D9%88-%D9%82%D8%AF%D8%B1%D8%AA%D9%85%D9%86%D8%AF