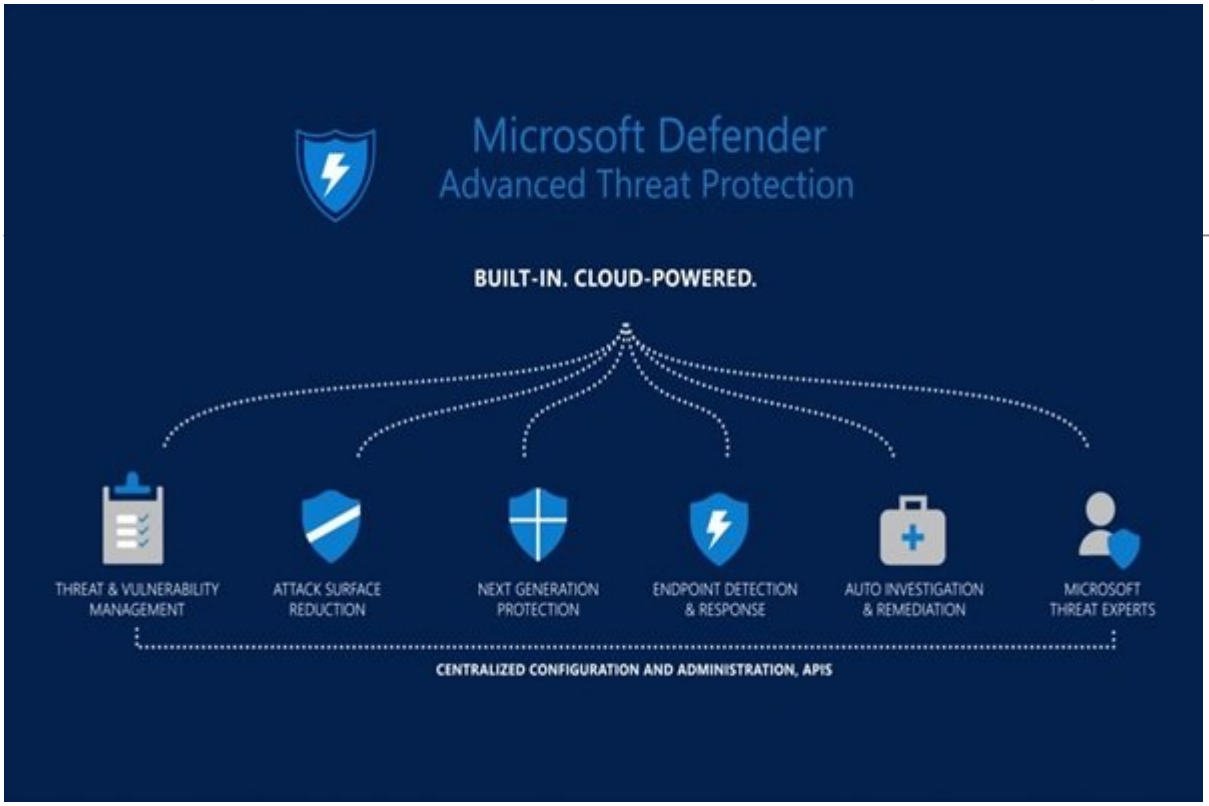
Windows Defender ATP Exploit Guard و دیوارآتش چه نقشی در ویندوز سرور 2019 دارند؟



همان‌گونه که پیش‌تر به آن اشاره کردیم، ضدویروس، قابلیت دیوارآتش، محافظت از سخت‌افزار و حتا محافظت در برابر باج‌افزارها در ترکیب با یکدیگر و در تعامل با بخش Windows Security ویندوز سرور 2019 همگی تحت عنوان ATP شناخته می‌شوند. ATP از بخش‌های مختلفی ساخته شده که هر یک از آن‌ها برای محافظت از بخش خاصی از ویندوز سرور استفاده می‌شوند. از طرفی دیوارآتش از پیش نصب شده در ویندوز سرور 2019 نیز عملکردی به مراتب بیشتر از یک مسدودکننده ترافیک دارد. شاید بد نباشد، دیوارآتش ویندوز را به عنوان بستری برقراری ارتباط توصیف کنیم.

برای مطالعه قسمت قبل آموزش رایگان **ویندوز سرور 2019** **اینجا** کلیک کنید.

Windows Defender ATP Exploit Guard

قابلیت جدید Exploit Guard در اصل یک قابلیت جدید نیست، بلکه مجموعه‌ای کامل از قابلیت‌هایی است که در ویندوز دیفندر به بلوغ رسیده‌اند. به‌طور خاص، این قابلیت جدید برای کمک به شناسایی حملات و پیشگیری از بروز حملات رایج بدافزاری بر مبنای الگوهای رفتاری است. قابلیت Defender ATP Exploit Guard از چهار مولفه زیر ساخته شده است:

ASR : Attack Surface Reduction مجموعه‌ای از کنترل‌ها است که در زمان فعال بودن مانع اجرای انواع خاصی از فایل‌ها می‌شود. این قابلیت می‌تواند به کاهش بدافزارهایی که توسط کاربران با کلیک روی پیوست‌های ایمیل یا باز کردن انواع خاصی از فایل‌های آفیس نصب می‌شوند کمک کند. امروزه بیشتر کارمندان یک سازمان می‌دانند که هیچ‌گاه نباید روی فایل‌های اجرایی ضمیمه شده یک ایمیلی کلیک کنند، اما هنوز هم هستند کاربرانی که میان یک فایل اجرایی و یک فایل اجرایی قانونی تفاوتی قائل نمی‌شوند. ASR می‌تواند به مسدود کردن اجرای هرگونه فایل اجرایی یا اسکریپت‌های درون ایمیل‌ها کمک کند.

Network protection: محافظت از شبکه به ویژگی Windows Defender SmartScreen اجازه می‌دهد مانع برقراری ارتباط بدافزارها با سرورهای کنترل و فرمان دهی شوند. بدافزارهایی که با هدف خارج کردن اطلاعات یک شرکت طراحی می‌شوند. وب‌سایت‌های اینترنتی دارای یک رتبه‌بندی هستند و بسته به نوع ترافیکی که در گذشته به آدرس آی‌پی آن‌ها رسیده، به عنوان یک قابل اعتماد یا غیرقابل اعتماد شناخته می‌شوند. SmartScreen برای آن‌که مانع از آن شود تا ترافیک مشکوک یک سازمان به خارج از سازمان و سرورهای مشکوک ارسال شود از بانک‌های اطلاعاتی معروفی استفاده می‌کند.

Controlled folder access: محافظت در برابر باج‌افزارها واقعا کاربردی است، زیرا باج‌افزارها اصلی‌ترین نگرانی امنیتی در دنیای فناوری‌اطلاعات هستند. اگر با این مفهوم آشنا نیستید، باید بگوییم باج‌افزار نوعی بدافزار است که در قالب یک برنامه روی کامپیوترها نصب می‌شود و سپس فایل‌های روی یک کامپیوتر را رمزگذاری می‌کند. پس از رمزگذاری، شما هیچ توانایی برای باز کردن یا تعمیر فایل‌ها ندارید و دسترسی به فایل‌ها تنها از طریق کلید رمزنگاری انجام می‌شود که هکر برای ارائه این کلید از شما درخواست مبلغ زیادی پول می‌کند. همه ساله بسیاری از شرکت‌ها قربانی حملات باج‌افزاری می‌شوند و برای دسترسی مجدد به فایل‌های خود مجبور می‌شوند باج تعیین شده از سوی هکرها را پرداخت کنند، زیرا به اصول پشتیبان‌گیری از اطلاعات و بازیابی اطلاعات در مواقع حساس توجه نکرده‌اند. ویژگی دسترسی به پوشه کنترل شده با مسدود کردن دسترسی‌های غیرمجاز و تعریف نشده به بخش‌های خاصی از هارددیسک از فایل‌ها در برابر حملات باج‌افزارها محافظت می‌کند و اجازه نمی‌دهد فایل‌های درون منطقه قرنطیه شده توسط باج‌افزارها نابود شوند.

Exploit protection: ویژگی فوق یک لایه حفاظتی عمومی برای مقابله با سوءاستفاده‌های احتمالی از یک کامپیوتر ارائه می‌کند. عملکرد ویژگی حفاظت در برابر سوء استفاده Defender ATP در اصل مجموعه‌ای از قابلیت‌هایی است که پیش از این به‌نام (EMET) سرنام Enhanced Mititation Toolkit Toolkit در دسترس بود، اما در اواسط سال 2018 مایکروسافت به کار ویژگی فوق پایان داد. ویژگی محافظت در برابر بهره‌برداری غیر مجاز به‌طور مستمر فرآیندهای سیستمی و فایل‌های اجرایی را بررسی کرده و از آن‌ها محافظت می‌کند.

دیوارآتش ویندوز دیفندر

زمانی‌که درباره امنیت دستگاه‌های تحت شبکه صحبت می‌کنیم، لازم است به محیط پیرامون نیز توجه داشته باشیم. محیط‌هایی که توسط دیوارهای آتش که عمدتاً سخت‌افزاری هستند تعریف و محافظت می‌شوند. دیوارهای آتش با دستگاه‌های تحت شبکه ارتباط مستقیم و غیر مستقیمی دارند و ترافیک شبکه از میان آن‌ها خارج شده یا وارد می‌شود. در کنار دیوارهای آتش سخت‌افزاری، دیوارهای آتش دیگری نیز وجود دارند که موضوع بحث ما هستند و در حالت نرم‌افزاری استفاده می‌شوند. دیوارآتش ویندوز یکی از این موارد است.

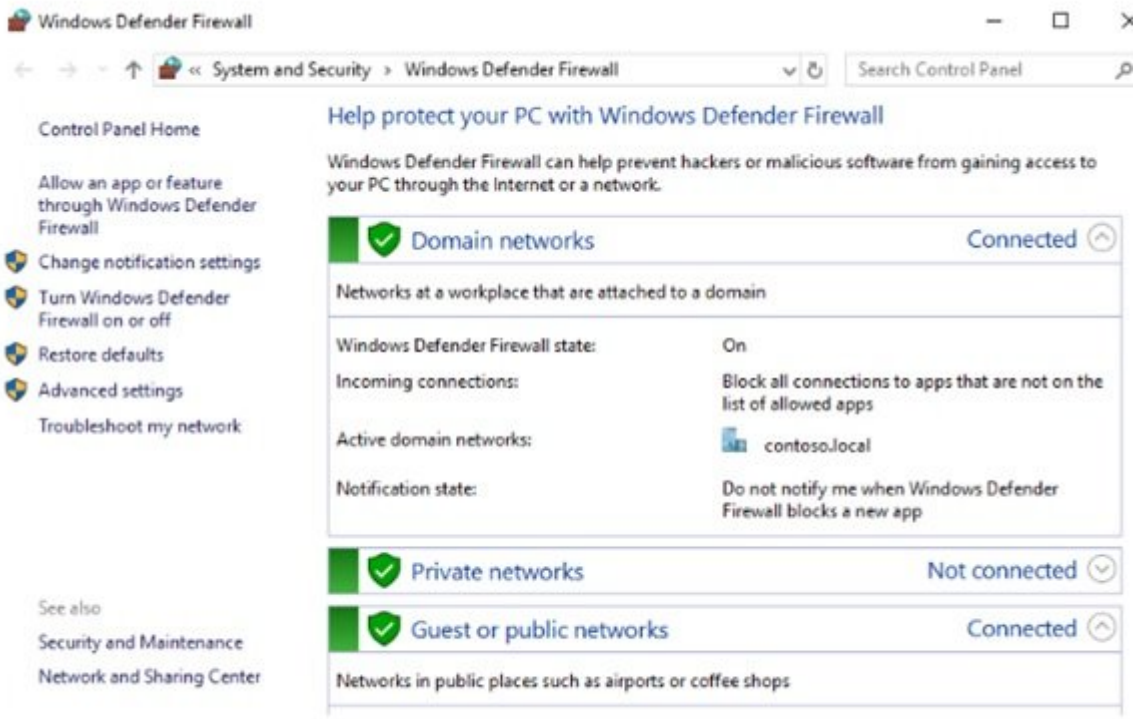
در روزهای پیدایش ویندوز ایکس‌پی و سرور 2003 دیوارآتش ویندوز عملکرد رضایت‌بخشی نداشت و بیشتر دردسرآفرین بود. دردسرهای دیوارآتش ویندوز به اندازه‌ای زیاد بود که برخی از شرکت‌ها به‌طور کامل دیوارآتش ویندوز را در تمام سیستم‌های متصل به دامنه غیر فعال می‌کردند. آن‌ها در توصیف اقدام خود اعلام می‌داشتند که خط‌مشی‌های امنیتی سازمان هیچ‌گونه سنخیتی با عملکرد دیوارآتش ویندوز ندارد و به همین دلیل آن‌را غیر فعال کرده‌اند. اما این مشکل بزرگ به سرعت برطرف شد و دیوارآتش (WFAS) سرنام Windows Defender با Advanced Security که امروزه در سیستم‌عامل‌های ویندوز وجود دارد مقاوم‌تر و پیشرفته‌تر از گذشته است و کاملاً می‌تواند برای تقویت معماری امنیتی یک سازمان استفاده شود. این ابزار به اندازه‌ای پیشرفته کرده است که باید بگوییم غیر فعال کردن WFAS در سیستم‌عاملی که از آن استفاده می‌کنید یک کار غیرعقلانی است، مگر اینکه دلیل بسیار خوبی برای انجام این کار داشته باشید.

سه کنسول مدیریتی دیوارآتش ویندوز

اولین نکته‌ای که باید از آن مطلع باشید در ارتباط با سه کنسول مختلفی است که برای تنظیم و پیکربندی دیوارآتش ویندوز در اختیارتان قرار دارد. دو مورد از این کنسول‌ها چندان کاربردی نیستند، اما گزینه سوم قابلیت‌های قدرتمندی در اختیارتان قرار می‌دهد. اجازه دهید به شکل گذرا به هر یک از آن‌ها نگاهی داشته باشیم.

دیوارآتش ویندوز دیفندر (کنترل پنل)

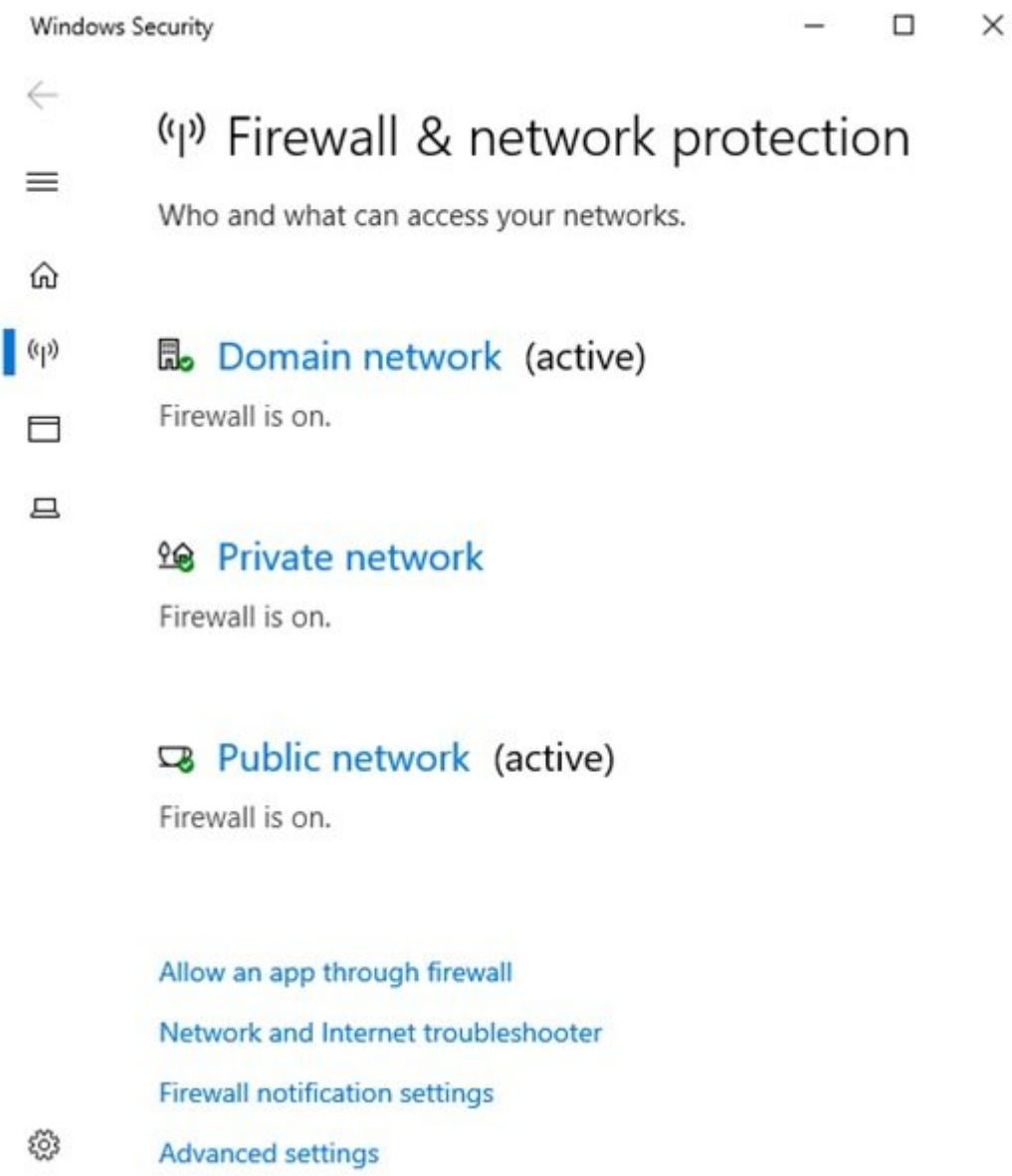
هنگامی که تصمیم می‌گیرد هر برنامه یا تنظیمی در ویندوز سرور 2019 را اجرا کنید به سادگی روی دکمه Start کلیک کنید و سپس یک کلمه مربوط به کاری که قصد انجام آن‌را دارید تایپ می‌کنید. به‌طور مثال اگر روی دکمه شروع کلیک کنید و واژه firewall را تایپ کنید در این حالت گزینه‌های مختلفی ارائه می‌شوند که یکی از آن‌ها Windows Defender Firewall است.



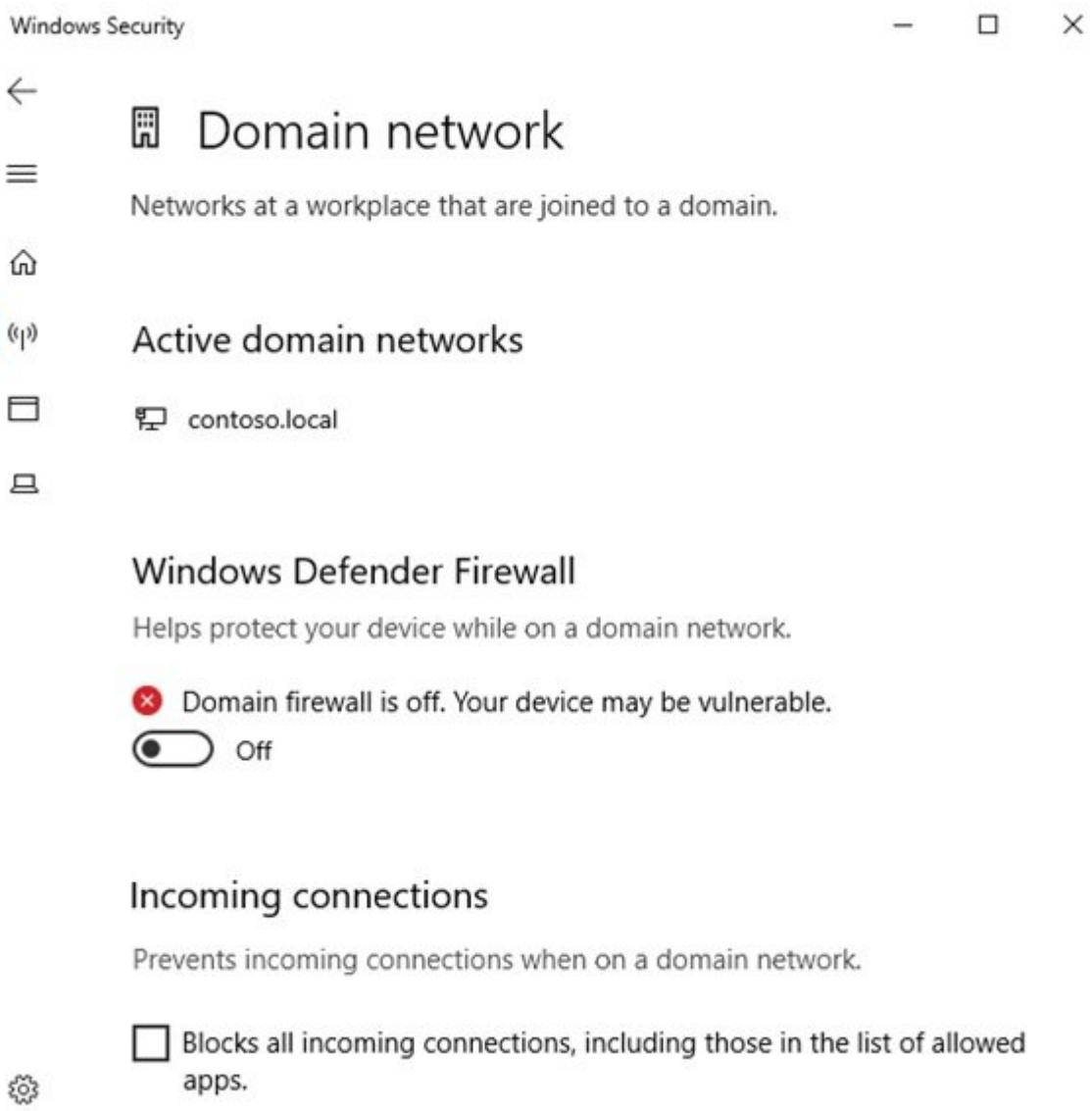
اگر روی گزینه فوق کلیک کنید کنسول پیکربندی دیوارآتش ویندوز از داخل کنترل پنل باز می‌شود که روشی قدیمی دسترسی به تنظیمات سیستم است. این کنسول هنوز هم قابل استفاده است و برای پیکربندی و تنظیم عملکردهای اصلی دیوارآتش همچون فعال یا غیرفعال کردن دیوارآتش ویندوز استفاده می‌شود، اما از آن‌جایی که این ابزار در داخل کنترل پنل قرار دارد باید فرض کنیم که این ابزاری نیست که مایکروسافت دوست داشته باشد ما از آن استفاده کنیم. به یاد داشته باشید تمامی قابلیت‌های پیکربندی به جای آن‌که در صفحه کنترل پنل قدیمی قرار داشته باشند به صفحه تنظیمات ویندوز منتقل شده‌اند.

دیوارآتش و محافظت از شبکه (Windows Security Settings)

در حالی که ابزارهای مبتنی بر کنترل پنل همیشه مکان مناسبی برای ایجاد تغییرات این چنینی در نسخه‌های قبلی سیستم‌عامل‌های مایکروسافت بودند، اما بیشتر گزینه‌های ویندوز دیفندر درون بخش Settings ویندوز ذخیره شده‌اند. دقت کنید برخی از تنظیمات پیکربندی دیوارآتش ویندوز دیفندر در بخش Windows Security برنامه Settings قرار دارند. تنظیمات ویندوز را باز کنید، روی Update & Security و سپس روی Windows Security کلیک کنید. قبلا با این صفحه آشنا شده‌اید، صفحه‌ای که اطلاعات خلاصه شده‌ای در ارتباط با مولفه‌های ویندوز دیفندر ارائه می‌کند. در این صفحه گزینه‌ای به‌نام Firewall & protection قرار دارد. اگر روی این گزینه کلیک کنید به صفحه پیکربندی دیوارآتش ویندوز وارد می‌شود که در نسخه‌های قبل‌تر ویندوز سرور وجود نداشتند.



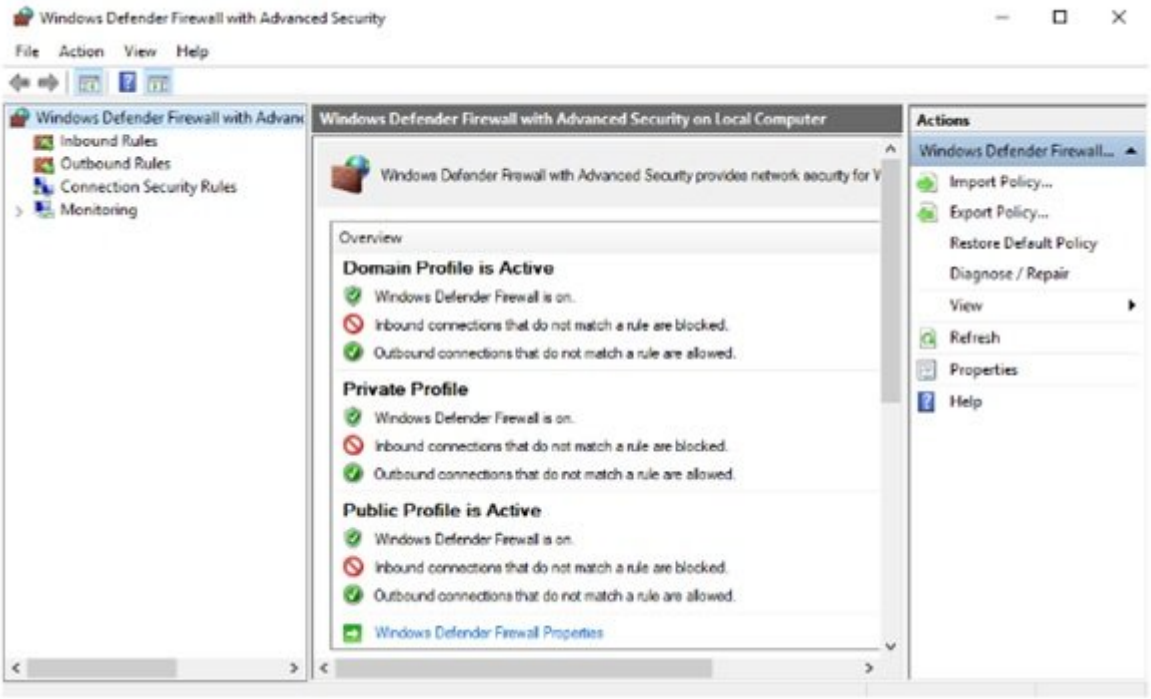
با کلیک روی هر یک از لینک‌های این صفحه دسترسی به گزینه‌های اضافه‌تر پیکربندی امکان‌پذیر می‌شود. به عنوان مثال، اگر تصمیم دارید به شکل سریع پروفایل دیوارآتش خاصی را فعال یا غیرفعال کنید، کافی است روی پروفایلی که قصد پیکربندی آن‌را دارید (به‌طور مثال Domain network profile) کلیک کنید و به سادگی دیوارآترش را برای این پروفایل غیرفعال کنید. بسیاری از شرکت‌ها پروفایل Domain network را روی ماشین‌های خود غیرفعال می‌کنند که باعث می‌شود ترافیک درون شبکه محلی سازمانی توسط دیوارآتش محافظت نشود. اگرچه غیرفعال کردن دیوارآتش در حالت کلی ایده بدی است، اما گاهی اوقات لازم است آن‌را متناسب با مدل تجاری خود تنظیم کنید.



صفحه پیکربندی دیوارآتش درون برنامه Settings ویندوز به شما اجازه می‌دهد به ساده‌ترین شکل درباره نحوه عملکرد دیوارآتش ویندوز دیفندر تصمیم‌گیری کنید، با این حال این رابط کاربری دارای قابلیت‌های محدودی در این مورد است و برای انجام یکسری کارهای پیشرفته‌تر باید به سراغ کنسول مدیریتی قدرتمندتری بروید.

دیوارآتش ویندوز دیفندر همراه با تنظیمات پیشرفته‌تر (WFAS)

تنظیمات ارائه شده در صفحه بالا جوابگوی نیاز کارشناسان حرفه‌ای نیستند و تنها اطلاعات مختصری در ارتباط با عملکردی اصلی دیوارآتش ویندوز ارائه می‌کنند. برای آن‌که بتوانید به تنظیمات پیشرفته‌تر دسترسی پیدا کنید مطابق با آن‌چه در تصویر زیر مشاهده می‌کنید به یک کنسول مدیریتی کارآمدتر نیاز دارید. برای دسترسی به این کنسول در خط فرمان یا کارد جست‌وجوی ویندوز دستور wf.msc را تایپ کنید و کلید اینتر را فشار دهید. با این‌کار کنسول مدیریت WFAS اجرا می‌شود.



در این صفحه به اطلاعات عمیق‌تری در مورد فعالیت و خط‌مشی‌هایی که دیوارآتش ویندوز بر مبنای آن‌ها کار می‌کند دسترسی خواهید داشت و قادر هستید ضمن مشاهده آن‌ها تغییری در آن‌ها اعمال کرده یا خط‌مشی‌های خاص خود را اعمال کنید. در این کنسول همچنین بخشی به‌نام Monitoring وجود دارد که اجازه می‌دهد خط‌مشی‌های که برای برقراری اتصال استفاده می‌شوند همچون Connection Security Rules را مشاهده کنید. این یک بخش مهم است، زیرا نشان می‌دهد که WFAS کاری به‌مراتب بیشتری از مسدود کردن ترافیک شبکه انجام می‌دهد و نه فقط یک دیوارآتش، بلکه زیرساختی برای برقراری ارتباطات است. اگر قصد دارید از IPsec برای رمزگذاری ترافیک شبکه، خواه IPsec به شکل بومی درون شبکه استفاه شود خواه از طریق فناوری دسترسی از راه دور DirectAccess استفاده شود در این بخش خط‌مشی‌هایی را مشاهده خواهید کرد که تونل‌های IPsec را تعریف می‌کنند. دیوارآتش ویندوز در واقع وظیفه رمزگذاری اطلاعات و تونل‌هایی را دارد که ایجاد می‌شوند. این قابلیت به مراتب پیشرفته‌تر از کاری است دیوارآتش ویندوز در سال‌های دور انجام می‌داد.

در شماره آینده آموزش رایگان ویندوز سرور 2019 مبحث فوق را ادامه خواهیم رفت.

برای مطالعه تمام بخش‌های آموزش **ویندوز سرور 2019** روی لینک زیر کلیک کنید:

آموزش رایگان ویندوز سرور 2019

تاریخ انتشار:
15 آبان 1398

نشانی منبع:
https://www.shabakeh-mag.com/networking-technology/16256/windows-defender-atp-exploit-guard-%D9%88-%D8%AF%DB%8C%D9%88%D8%A7%D8%B1%D8%A2%D8%AA%D8%B4-%DA%86%D9%87-%D9%86%D9%82%D8%B4%DB%8C-%D8%AF%D8%B1-%D9%88%DB%8C%D9%86%D8%AF%D9%88%D8%B2-%D8%B3%D8%B1%D9%88%D8%B1