آشنایی با پروفایل‌های مختلف دیوارآتش در ویندوز سرور 2019

هنگامی که کارت شبکه‌ای در یک کامپیوتر یا سرور به شبکه‌ای وصل شود، دیوارآتش ویندوز به آن کارت شبکه و اتصال سه پروفایل مختلف اختصاص می‌دهد. شاید در گذشته با چنین حالتی روبرو شده باشید یا حتا متوجه این موضوع نشده‌اید. وقتی لپ‌تاپ خود را به وای‌فای یک کافی شاپ محلی وصل می‌کنید، آیا ویندوز از شما سؤال می‌کند که قصد اتصال به شبکه عمومی، کاری یا خانگی را دارید؟ این پرسشی است که دیوارآتش ویندوز از شما می‌پرسد و قصد دارد بر اساس پاسخی که می‌دهید پروفایل مناسب را برای اتصال به شبکه جدید اعمال کند.

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

سه پروفایل مختلف دیوارآتش

هنگامی که کارت شبکه‌ای در یک کامپیوتر یا سرور به شبکه‌ای وصل شود، دیوارآتش ویندوز به آن کارت شبکه و اتصال سه پروفایل مختلف اختصاص می‌دهد. شاید در گذشته با چنین حالتی روبرو شده باشید یا حتا متوجه این موضوع نشده‌اید. وقتی لپ‌تاپ خود را به وای‌فای یک کافی شاپ محلی وصل می‌کنید، آیا ویندوز از شما سؤال می‌کند که قصد اتصال به شبکه عمومی، کاری یا خانگی را دارید؟ این پرسشی است که دیوارآتش ویندوز از شما می‌پرسد و قصد دارد بر اساس پاسخی که می‌دهید پروفایل مناسب را برای اتصال به شبکه جدید اعمال کند.
اصلی‌ترین دلیلی که باعث می‌شود به کارت‌های شبکه و اتصالات شبکه پروفایل‌های مختلف دیوارآتش را اختصاص دهید این است که در نظر دارید قواعد و معیارهای مختلف دسترسی و مجوزهایی که برای انجام برخی از کارها روی یک شبکه عمومی امکان‌پذیر است و کارهایی که فقط باید در یک شبکه خصوصی انجام شود را مشخص می‌کنید. به‌طور موثر از شما سؤال می‌شود که چقدر به شبکه‌ای که قصد اتصال به آن‌را دارید اعتماد دارید؟ به عنوان مثال، هنگامی که لپ‌تاپ شما به شبکه شرکت متصل است، احتمالاً کمی راحت‌تر می‌توانید از لپ‌تاپ خود در مقایسه با زمانی که به اینترنت هتل متصل می‌شوید استفاده کنید. با تعیین خط‌مشی‌های سخت‌گیرانه در زمان اتصال به وای‌فای هتل یک مکانیسم امنیتی محکم‌تر پیرامون لپ‌تاپ خود می‌کشید تا هکرها به راحتی موفق نشوند به لپ‌تاپ شما نفوذ کنند. اجازه دهید به شکل اجمالی این سه پروفایل را بررسی کنیم.

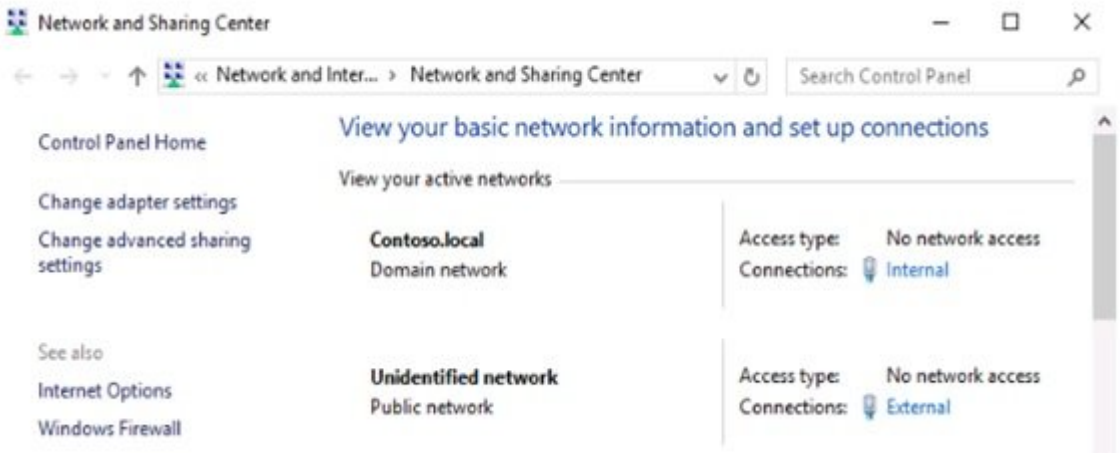
Domain Profile: تنها پروفایلی است که نمی‌توانید برای تخصیص آن‌را انتخاب کنید. این تنها شخصی است که شما نمی توانید انتخاب کنید که اختصاص دهید. Domain Profile تنها زمانی فعال است که یک کامپیوتر متصل به دامنه به تازگی به شبکه‌ای متصل شده است که یک کنترل‌کننده دامنه برای آن دامنه در دسترس باشد. بنابراین، برای هر کامپیوتر یا دستگاه شرکتی که درون شبکه شرکت قرار دارد، پروفایل فوق فعال خواهد بود.

Private Profile: هنگامی که به شبکه جدیدی متصل می‌شوید، پیغامی طاخر می‌شود تا شما مکانی که قصد اتصال

به آن‌را دارید مشخص کنید. اگر گزینه‌هایHome یا Work را انتخاب کنید، به ارتباطی که ساخته خواهد شد پروفایل Private تخصیص پیدا می‌کند.

Public Profile: هنگامی که پیغام اتصال به شبکه ظاهر شود و گزینه Public را انتخاب کنید، یک پروفایل عمومی دیوارآتش برای آن ارتباط انتخاب می‌شود. همچنین اگر به دلایلی چنین پیغامی نشان داده نشود، گزینه‌ای را انتخاب نکنید یا پنجره انتخاب تعیین وضعیت را ببندید، ویندوز برای اتصالی که ایجاد خواهد شد پروفایل Public را اختصاص می‌دهد، زیرا پروفایل فوق حالت پیش‌فرض است و هر اتصالی که برای آن پروفایلی تعیین نشده باشد، پروفایل عمومی اختصاص داده می‌شود. در نسخه‌های جدیدتر ویندوز (به ویژه Win10)، معمولا پیغامی مبنی بر انتخاب پروفایل عمومی را مشاهده نمی‌کنید و از شما در ارتباط با نوع شبکه‌ای که قصد اتصال به آن‌را دارید سوالی نمی‌شود، به جای آنکه از شما این سوال پرسیده می‌شود که آیا به کامپیوتر خود اجازه می‌دهید با سایر دستگاه‌ها در شبکه جدید ارتباط برقرار کند. به لحاظ فنی، هنوز هم نوع پرسش یکسان است و شما تصمیم می‌گیرد که ارتباط بر مبنای یک پروفایل خصوصی ایجاد شود یا یک پروفایل عمومی. هر اتصال شبکه پروفایل خاص خود را دارد، اما نکته‌ای که مهم است این است که شما می‌توانید بیش از یک پروفایل دیوارآتش را در یک لحظه در یک سیستم فعال کنید. به عنوان مثال، سرور شرکت ممکن است به‌طور همزمان به شبکه سازمانی و همچنین اینترنت عمومی متصل باشد. درون WFAS شما هر دو گزینه Domain Profile و Public Profile را مشاهده می‌کنید که فعال هستند.

از طرف دیگر، بخش Network and Sharing Center را در سرور خود باز کنید، پروفایل‌ها فهرست شده را مشاهده می‌کنید که به سادگی می‌توانید اعلام دارید یک کارت شبکه از چه پروفایلی استفاده می‌کند.

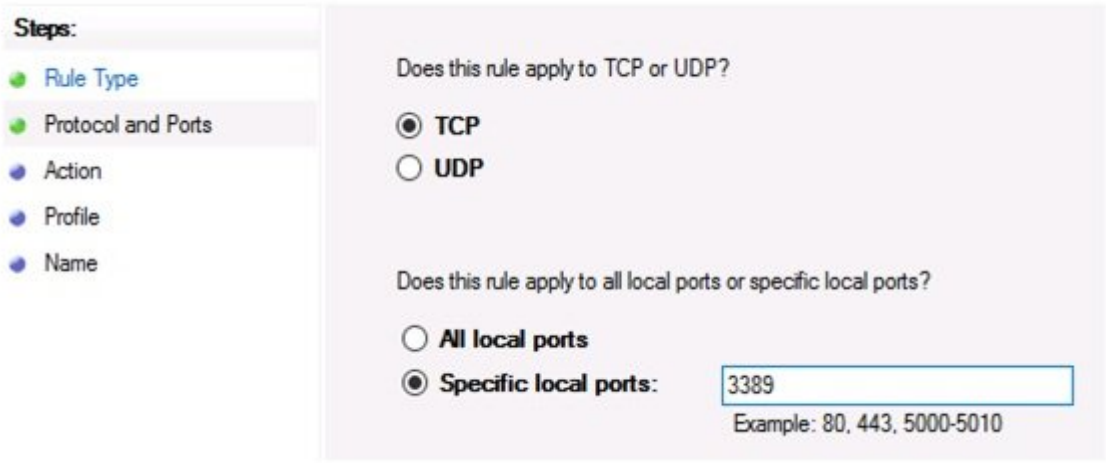


ایجاد یک قاعده جدید ورودی در دیوارآتش

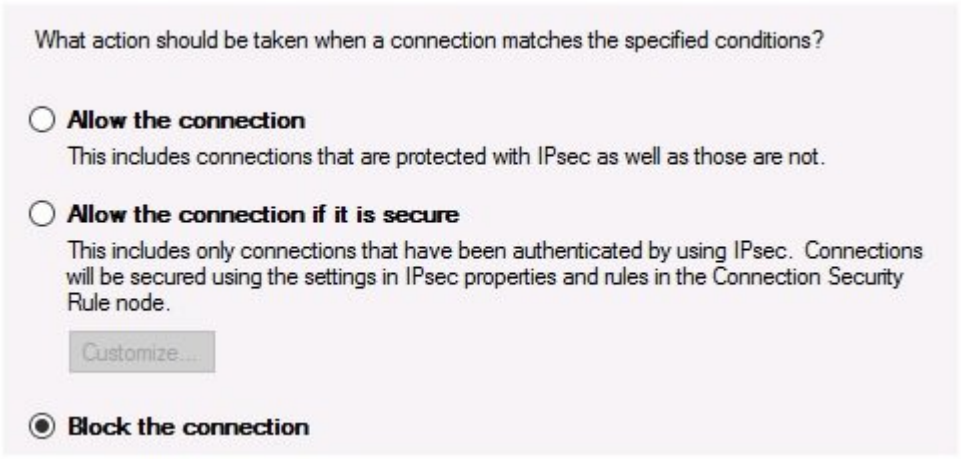
اکنون می‌دانیم درون کنسول WFAS چه قابلیت‌ها و تنظیماتی قرار دارد، پس اجازه دهید از WFAS برای ساخت یک قاعده جدید استفاده کنیم. برای ساخت قاعده جدید در سرور خود باید دسترسی به RDP را فعال کنید تا بتوانید به شکل ساده‌تری سرور را کنترل کنید. با این حال با فعال‌سازی RDP از هر نقطه از شبکه دسترسی به RDP وجود دارد. در نتیجه نه تنها از طریق شبکه خود RDP دسترسی خواهیم داشت، بلکه امکان دسترسی از راه دور از طریق اینترنت امکان‌پذیر است. بدون شکل این اتفاق، مشکل بزرگی است، زیرا هر شخصی قادر است سرور ما را پیدا کند، پیغام ورود RDP را مشاهده کند و از طریق یک حمله جست‌وجوی فراگیر به سرور ما وارد شود.

برای این‌که این مشکل را برطرف کنیم باید به شکلی پیکربندی کنیم که دسترسی از طریق کارت شبکه خارجی امکان‌پذیر نباشد. به عبارت دقیق‌تر قصد داریم دسترسی به شکل داخلی فعال باشد و بتوانیم از درون شبکه به سرور خود دسترسی داشته باشیم، خوشبختانه WFAS یک راهکار ساده برای ساخت یک قاعده دیوارآتش برای محدود کردن دسترسی خارجی به RDP دارد.

برای دسترسی به تنظیمات پیشرفته دیوارآتش فرمان wf.msc را اجرا کنید و به بخش Inbound Rules بروید. در این بخش تمامی قواعد ورودی دیوارآتش که روی سرور تنظیم شده‌اند را مشاهده می‌کنید. روی گزینه Inbound Rules راست کلیک کنید و گزینه New Rule را انتخاب کنید .... با انجام این‌کار پنجره‌ای ظاهر می‌شود که اجازه ساخت قواعد جدید را می‌دهد. صفحه اول مکانی است که برای مشخص کردن نوع قاعده‌ای که قصد ایجاد آن‌را داریم استفاده می‌شود. شما می‌توانید قاعده‌ای را ایجاد کنید که ترافیک را برای یک برنامه خاص تغییر دهد یا می‌توانید گزینه Predefined را انتخاب کنید و فهرستی از پروتکل‌های از پیش تعریف شده را مشاهده کنید. در این‌جا ما قصد داریم به درستی بدانیم قاعده‌ای که قصد ایجاد آن‌را داریم قرار است چه کاری انجام دهد، زیرا به دنبال ساخت یک قاعده سفارشی هستیم و دلیلی برای تعریف یک پروتکل نداریم به دلیل این‌که می‌دانیم که RDP از پروتکل TCP و درگاه 3389 استفاده می‌کند. بنابراین، قصد داریم درگاه فوق را انتخاب کنیم و سپس دکمه Next را کلیک کنیم.



در مرحله سوم باید مشخص کنیم پورتی که آن‌را انتخاب کرده‌ایم اجازه دارد ترافیکی را عبور دهد یا خیر. گزینه دوم در این صفحه اجازه می‌دهد ترافیک تنها در صورتی که توسط پروتکل IPsec تایید شده است، انتقال پیدا کند. یک گزینه کارآمد به شرطی که پروتکل IPsec قبلا نصب شده باشد. به دلیل این وابستگی بیشتر افراد از گزینه یاد شده استفاده نمی‌کنند. به عنوان مثال، اکنون ما در حال کار با RDP هستیم، اما قصد داریم آن‌را روی کارت‌های شبکه مسدود کنیم، بنابراین گزینه مسدود کردن اتصال را انتخاب می‌کنیم.



ما نمی‌خواهیم RDP را برای همه کارت‌های شبکه مسدود کنیم، بنابراین تنظیمات صفحه بعدی حائز اهمیت هستند. در اینجا باید به دانش خود در مورد پروفایل‌های دیوارآتش که پیش‌تر در مورد آن‌ها صحبت کردیم مراجعه کنیم. به این نکته دقت کنید که کارت‌های داخلی متصل به دامنه شبکه پروفایل Domain را خواهند داشت. اما به هر کارت شبکه‌ای که به شبکه داخلی وصل نیست، در حالی که کنترل کننده دامنه در دسترس است، باید پروفایل عمومی یا خصوصی را دریافت کند. اگر می‌خواهیم RDP را فقط در کارت شبکه خارجی غیرفعال کنیم، لازم است که این قاعده فقط برای پروفایل خصوصی و عمومی فعال باشد. در حقیقت، با نگاهی به عکس‌هایی که قبلاً گرفتیم، مشاهده می‌کنیم که کارت شبکه خارجی یک پروفایل عمومی دریافت کرده است، بنابراین در این‌جا فقط باید تیک مربوط به پروفایل عمومی را بررسی کنیم تا مطمئن شویم در ادامه RDP روی کارت شبکه خارجی مسدود خواهد بود. در صورتی که در آینده کارت‌های شبکه بیشتری به سرور خود اضافه خواهید کرد باید مطمئن شوید که دسترسی RDP روی آن‌ها امکان‌پذیر نیست. اطمینان حاصل کنید که پروفایل Domain را غیر فعال کرده‌اید. اگر این موضوع را رعایت نکنید دسترسی RDP را به‌طور کامل مسدود خواهید کرد و در آینده قادر به برقراری اتصال مجدد نخواهد بود.

ما به سادگی موفق شدیم یک قاعده جدید برای خود ایجاد کنیم و خیلی زود موفق شدیم دسترسی مستقیم به سرور با اتکا با RDP و از طریق اینترنت را غیر فعال کنیم.

ایجاد یک قاعده برای انجام پینگ (ICMP)

در اغلب موارد، مجبور هستیم قاعده‌ای برای تعیین وضعیت پروتکل ICMP ایجاد کنیم. به عبارت دیگر، در برخی موارد مجبور هستیم دیوارآتش را به شکلی روی سرور تنظیم کنیم که توانایی پاسخ‌گویی به درخواست‌ها پینگ وجود داشته باشد. احتمالاً متوجه شده‌اید که با سیستم‌عامل‌های جدید سرور کار ساده و عادی است که اجازه دهیم دیوارآتش به‌طور خودکار پینگ‌های (ICMP) را مسدود کند، اما ویژگی فوق برای محیط‌هایی که برای مشخص کردن یک آدرس آی‌پی مصرف شده یا در دسترس از پینگ استفاده کنند مشکل‌ساز است. هنوز هم مدیران شبکه زیادی وجود دارند که آدرس‌های آی‌پی که در شبکه خود استفاده کرده‌اند را یادداشت نمی‌کنند و هنگامی که باید سرور جدیدی را پیکربندی کنند به سراغ پینگ می‌روند و تا زمانی که پیغام time out را مشاهده نکنند این‌کار را انجام می‌دهند. من این را بارها دیده‌ام. بدیهی است این روش خوبی برای مدیریت آدرس‌های آی‌پی نیست، اما این اتفاق رخ می‌دهد. متأسفانه، این روش مشکلات عدیده‌ای را به وجود می‌آورد، زیرا بیشتر نصب‌های جدید ویندوز به‌گونه‌ای انجام می‌شوند که پاسخ‌های ICMP را مسدود می‌کنند. به‌طور مثال، ممکن است به یک آدرس آی‌پی پینگ کنید و پیغام time out را مشاهده کنید در حالی که سرور در واقعیت در حال استفاده از یک آدرس آی‌پی است. برای حل این مشکل باید ICMP را روی سرور فعال کنید، موضوعی که در شماره آینده به بررسی آن خواهیم پرداخت.

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:
18 آبان 1398

نشانی منبع:
https://www.shabakeh-mag.com/networking-technology/16258/%D8%A2%D8%B4%D9%86%D8%A7%DB%8C%DB%8C-%D8%A8%D8%A7-%D9%BE%D8%B1%D9%88%D9%81%D8%A7%DB%8C%D9%84%E2%80%8C%D9%87%D8%A7%DB%8C-%D9%85%D8%AE%D8%AA%D9%84%D9%81-%D8%AF%DB%8C%D9%88%D8%A7%D8%B1%D8%A2%D8%AA%D8%B4-%D8%AF%D8%B1-

%D9%88%DB%8C%D9%86%D8%AF%D9%88%D8%B2-%D8%B3%D8%B1%D9%88%D8%B1-2019