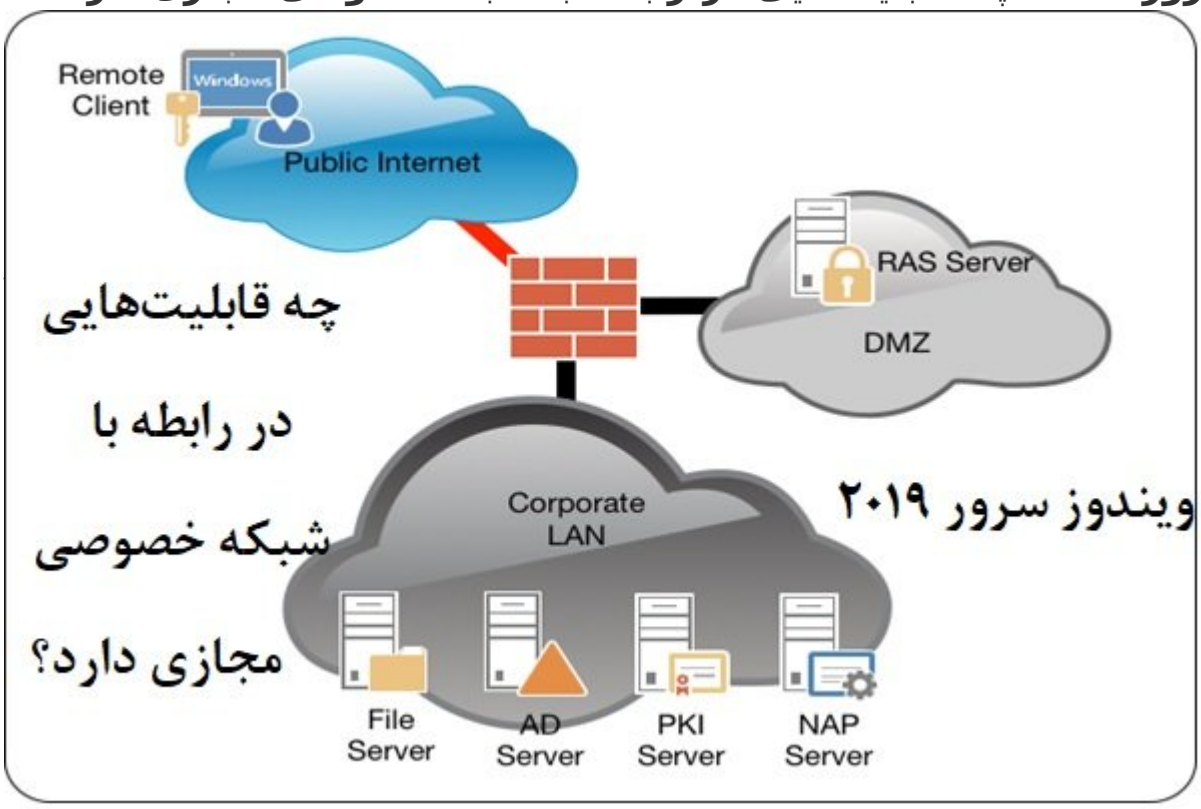
ویندوز سرور 2019 چه قابلیت‌هایی در رابطه با شبکه خصوصی مجازی دارد؟



ویندوز سرور 2019 تنها یک نسخه ارتقا یافته از ویندوز سرور 2016 نیست، بلکه مجموعه‌ای کم نظیر از ویژگی‌های کاربردی است که سبک جدیدی از مدیریت شبکه‌ها، اتصال کلاینت‌ها به شبکه‌ها و مهم‌تر از آن انجام کارها از راه دور را ارائه کرده است. ویژگی انجام کارهای اداری در خارج از محیط سازمانی این روزها حسابی خبرساز است و هر شرکت بزرگ نرم‌افزاری سعی می‌کند ابزارها و فناوری‌های خاصی را برای این منظور ارائه کند. ویندوز سرور 2019 با ارائه راهکارهایی که اجازه می‌دهند شبکه‌های خصوصی مجازی به بهترین شکل در دسترس کاربران و سازمان‌ها باشند، سبک جدیدی از این دورکاری را ارائه کرده است.

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

فعال‌سازی ویژگی Mobile Workforce

اگر به کارکنان خود اجازه دهید از راه دور به منابع شرکت دسترسی داشته باشند، به شکل غیر محسوس به سازمان خود لطف بزرگی کرده‌اید، هرچند اعطای این قابلیت یک ضرورت نیست. در چند سال گذشته رویکرد اتخاذ شده از سوی کارمندان شرکت‌ها تغییر کرده و آن‌ها تمایل دارند از مکان‌های مختلفی بتوانند کارهای خود را انجام دهند. تلفن‌های همراه بخش بزرگی از این داستان هستند، اما با توجه به ابعاد کوچک صفحه‌نمایش و کارکردهای محدود سیستم‌عامل‌های همراه در انجام برخی از کارهای سازمانی قدرت مانور چندانی وجود ندارد. برای این‌که به کارمندان خود اجازه دهید از راه دور و زمانی‌که در خانه، کافی‌شاپ یا هتل مستقر هستند کارهای شرکت ر ا انجام دهند به فناوری به‌نام شبکه‌های خصوصی مجازی (VPN) سرنام Virtual Private Networks نیاز داریم.

بیشتر شبکه‌های خصوصی مجازی در مشاغل امروزی توسط شرکت‌های مختلفی ارائه می‌شوند. به همین دلیل نقش Remote Access در ویندوز سرور 2019 نیز هم‌راستا با این جریان تغییر کرده است. با توجه به پیشرفت‌های قابل ملاحظه انجام شده در ارتباط با مولفه VPN در ویندوز سرور 2019، اکنون یک بستر عملی و ایمن برای دسترسی به منابع سازمانی از طریق کامپیوترهای دسکتاپ راه دور فراهم شده است. علاوه بر شبکه‌های خصوصی مجازی، ویندوز سرور 2019 چند فناوری کارآمدتر و کاربردی‌تر ارائه کرده که مختص دسترسی از راه دور به منابع سازمانی طراحی شده است، فناوری‌هایی که عملکرد متفاوت از شبکه‌های خصوصی مجازی دارند.

Always On VPN

در گذشته برای آن‌که به کاربری اجازه دهیم به یک اتصال شبکه خصوصی مجازی سنتی دسترسی پیدا کند مجبور بودیم یک لینک ارتباطی خاصی را برای او آماده کنیم تا کاربر بتواند اطلاعات هویتی خود را برای نشان دادن اصالتش وارد کند و سپس برای برقراری ارتباط با منابع شرکت به شبکه محیط کاری متصل شود. پس از راه‌اندازی شبکه

خصوصی مجازی کاربران می‌توانند ایمیل خود را باز کنند، اسناد را پیدا کنند، برنامه‌های کاری خود را اجرا کنند و بدون آن‌که در به شکل فیزیکی در محل کار خود قرار داشته باشند فعالیت‌های روزمره را انجام دهند. همچنین، هنگام برقراری اتصال از طریق VPN، مدیریت لپ‌تاپ کاربران امکان‌پذیر است و این امکان را برای شما فراهم می‌کند که یک جریان ارتباطی برای سامانه‌ها را از طریق Group Policy و SCCM به درستی مدیریت و هدایت کنید. اتصالات VPN یک مکانیزم ارتباطی خود برای شبکه شما ارائه می‌دهند، اما (دقت کنید در اینجا درباره اتصالات سنتی و معمولی VPN صحبت می‌کنیم) آن‌ها تنها زمانی کار می‌کنند که کاربر به صورت دستی آن‌ها را راه‌اندازی کرده و به آن‌ها اجازه دهد تا کار کنند. هر زمان کاربر به VPN خود وصل نشده باشد، آن‌ها به شکل عادی به اینترنت متصل می‌شوند بدون آن‌که به مرکز داده شرکت متصل شده باشند. این حرف به این معنا است که یک اتصال سنتی VPN آشکارا هیچ نوع مکانیزم اتصال به صفحه ورود ویندوز ندارد، زیرا کاربران مادامی که به کامپیوتر و دسکتاپ کامپیوتر خود وارد نشده باشند قادر نیستند هیچ تونل شبکه خصوصی مجازی را اجرا کنند. در نتیجه هیچ اتفاقی در صفحه شروع و کارهایی شبیه به احراز هویت آنی یا احراز هویت در مدت زمان ورود یا اجرای اسکریپت‌های ورود از طریق یک شبکه خصوصی مجازی سنتی وجود ندارد.

Always On VPN که به اختصار AOVPN نامیده می‌شود دقیقاً همان‌گونه که از نامش قابل حدس زدن است بر اساس ایده ساخت یک اتصال VPN پایدار و خودکار طراحی شده است. به عبارت دیگر، هر زمان کاربر لپ‌تاپ خود را به بیرون از دفتر خود می‌برد و به اینترنت متصل می‌شود، یک تونل VPN به شبکه شرکت به‌صورت خودکار ایجاد می‌شود و در حالت این فرآیند بدون اجرای هیچ‌گونه پردازش اضافی انجام می‌شود. این فرآیند به اندازه‌ای هوشمندانه و دقیق عمل می‌کند که کاربران فراموش خواهند کرد از طریق یک شبکه خصوصی مجازی به شبکه سازمان متصل شده‌اند، زیرا اتصال همیشه آماده و قابل استفاده است. آن‌ها می‌توانند به دستگاه‌های خود شوند، برنامه‌های خود را اجرا و از آن‌ها استفاده کار کنند. در چنین حالتی یکسری از عملکردهای مدیریتی فناوری اطلاعات شبیه به خط‌مشی‌های امنیتی، به‌روزرسانی‌ها و بسته‌های نصبی می‌توانند با دقت بالایی به سمت دستگاه‌های کلاینت هدایت شوند، در این حالت نگرانی از بابت عدم دریافت بسته‌ها یا انتظار برای دریافت بسته‌ها از سوی کاربران وجود ندارد، همه چیز به شکل خودکار و تقریبا در بیشتر زمان‌ها انجام می‌شود.

در این‌جا سه روش مختلف داریم که اجازه می‌دهند Always On VPN را روی ماشین‌های کلاینت فعال کنیم و در هر سه مورد نیازی نیست کاربر یک اتصال به شبکه خصوصی مجازی را فعال کند.

روش اول این است که AOVPN به گونه‌ای پیکربندی شود که همیشه روشن باشد، به این معنا که به محض دسترسی به اینترنت اتصال بر مبنای شبکه خصوصی مجازی برقرار شود.

یکی دیگر از گزینه‌ها اجرای یک رویداد است، به این معنا که می‌توانید AOVPN را پیکربندی کنید تا در صورت باز شدن برنامه‌های خاص روی ایستگاه کاری AOVPN را راه‌اندازی کند.

گزینه سوم بر مبنای سامانه نام دامنه کار می‌کند. در این حالت زمانی که نام یک DNS خاص فراخوانی شود، یک اتصال VPN فراخوانی و اجرا می‌شود که معمولا در زما اجرای برنامه‌های خاصی توسط کاربران فعال می‌شود.

از آن‌جایی که نیازی به Always On VPN ندارید تا هنگامی که لپ‌تاپ شما در شبکه شرکت قرار دارد به آن متصل شوید و کار کنید باید به این نکته اشاره کنیم که عملکرد AOVPN به اندازه کافی هوشمند است تا وقتی کاربر از آن درهای شیشه‌ای ساختمان عبور کرد و به ساختمان وارد شد به‌طور خودکار خاموش شود. کامپیوترهای مبتنی بر قابلیت AOVPN به‌طور خودکار تصمیم می‌گیرند چه زمانی در شبکه قرار دارند و در این حالت مولفه‌های VPN را غیرفعال می‌کنند و هنگامی که خارج از شبکه هستند و باید یک اتصال تونل‌زنی به VPN را انجام دهند روشن شوند. این فرایند به‌نام تشخیص شبکه مطمئن (Trusted Detection Network) شناخته می‌شود. هنگامی که ویژگی فوق به درستی پیکربندی شده باشد، همیشه مولفه‌های VPN می‌دانند پسوند داخلی DNS شرکت چیست و سپس تنظیمات کارت شبکه و دیوارآتش را کنترل می‌کنند تا تشخیص دهند که آیا این پسوند به همین مؤلفه‌ها اختصاص داده شده است یا خیر. زمانی که فرآیند تطابق انجام شد، VPN می‌داند که شما درون شبکه هستید و AOVPN را غیرفعال می‌کند.

انواع تونل‌های AOVPN

قبل از آن‌که وارد جزییات مربوط به مولفه‌های کلاینت و سروری شویم که روی ساخت AOVPN تاثیرگذار هستند، یک

موضوع اصلی مهم وجود دارد که باید ابتدا به درستی آن‌را درک کنید تا بتوانید در مورد نحوه استفاده از AOVPN در شرکت خود تصمیم درست را اتخاذ کنید. دو نوع تونل VPN کاملا متفاوت از یکدیگر وجود دارد که می‌توان با ویژگی Always On VPN از آن‌ها استفاده کرد. User Tunnel و Device Tunnel دو گزینه‌ای هستند که در اختیارتان قرار دارد. AOVPN به شما اجازه می‌دهد دو تونل مختلف داشته باشید تا بتوانید بدون مشکل آن‌ها را با ویژگی DirectAccess هماهنگ کنید. اجازه دهید این دو تونل را بررسی کنیم.

User Tunnels

متداول‌ترین روش به‌کارگیری ویژگی AOVPN پیاده‌سازی یک User Tunnel به منظور احراز هویت در سطح کاربر است. گواهینامه‌های کاربر از طریق یک زیرساخت کلید عمومی (PKI) داخلی برای کامپیوترها صادر می‌شوند و این گواهینامه‌ها به‌عنوان بخشی از فرآیند احراز هویت هنگام اتصال استفاده می‌شوند. User Tunnels می‌توانند ترافیک تمامی کاربران و ماشین‌ها را انتقال دهند، اما مهم است که توجه داشته باشید که تونل‌های نوع کاربری زمانی که کامپیوتر در صفحه ورود قرار دارد، انتشار پیدا نمی‌کنند، زیرا تأیید هویت کاربر در آن زمان اتفاق نیفتاده است. بنابراین، یک User Tunnel فقط هنگامی که کاربر با موفقیت به کامپیوتر خود وارد می‌شود، اجرا می‌شوند. زمانی‌که از User Tunnel استفاده می‌شود، کامپیوتر نمی‌تواند به شبکه‌های سازمانی متصل شود و تنها زمانی که کاربر فرآیند ورود به سیستم را بر مبنای اطلاعات تایید هویت کش شده انجام دهد قادر است به شبکه سازمانی وارد شود.

Device Tunnel

یک Device Tunnel برای پر کردن شکاف مکانیزم User Tunnel طراحی شده است. یک Device Tunnel از طریق یک گواهی ماشین که از طریق زیرساخت کلید عمومی (PKI) داخلی صادر شده تایید هویت می‌شود. این حرف بدان معنا است که Device Tunnel می‌تواند خودش را منشر کند، حتا قبل از این‌که تأیید اعتبار کاربر تکمیل شود. به عبارت دیگر، حتی زمانی که کامپیوتر در صفحه لاگین ویندوز قرار دارد تونل در سطح دستگاه در وضعیت اجرا قرار داشته و قابل استفاده است. این مکانیزم ابزارهای مدیریتی همچون Group Policy و SCCM را قادر می‌سازد فارغ از ورودی کاربر کار کنند و همچنین تأیید هویت بلادرنگ را روی کنترل‌کننده دامنه انجام دهند و از طرفی کاربران را قادر می‌سازد وارد ایستگاه کاری شوند که تاکنون هیچ‌گاه به آن وارد نشده‌اند. در این حالت تنظیم مجدد منقضی شدن گذرواژه به شکل بلادرنگ نیز امکان‌پذیر است.

ملزومات موردنیاز Device Tunnel

یک User Tunnel می‌تواند تقریبا با هر دستگاه مجهز به سیستم‌عامل ویندوز 10 کار کند، اما برای استفاده از یک Device Tunnel یکسری ملزومات اولیه نیاز است که باید آن‌ها را در اختیار داشته باشید. برای آن‌که بتوانید از یک Device Tunnel استفاده کنید به ملزومات زیر نیاز دارید:

کلاینت باید به دامنه متصل شده باشد.

کلاینت باید یک گواهی ماشین را منتشر کرده باشد

کلاینت باید سیستم‌عامل ویندوز 10 نسخه 1709 یا جدیدتر از آن‌را استفاده کند و فقط نسخه‌های سازمانی یا SKU Education قابل استفاده هستند.

یک Device Tunnel می‌تواند فقط IKEv2 باشد. پیشنهاد می‌کنم برای اطلاعات بیشتر درباره IKEv2 تحقیق کنید، زیرا ممکن است بهترین روش اتصال را در اختیار کلاینت‌ها قرار دهد.

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:

17 مهر 1398

نشانی منبع:
https://www.shabakeh-mag.com/networking-technology/16128/%D9%88%DB%8C%D9%86%D8%AF%D9%88%D8%B2-%D8%B3%D8%B1%D9%88%D8%B1-2019-%DA%86%D9%87-%D9%82%D8%A7%D8%A8%D9%84%DB%8C%D8%AA%E2%80%8C%D9%87%D8%A7%DB%8C%DB%8C-%D8%AF%D8%B1-%D8%B1%D8%A7%D8%A8%D8%B7%D9%87-%D8%A8%D8%A7-%D8%B4%D8%A8%DA%A9%D9%87-%D8%AE%D8%B5%D9%88%D8%B5%DB%8C-%D9%85%D8%AC%D8%A7%D8%B2%DB%8C-%D8%AF%D8%A7%D8%B1%D8%AF%D8%9F