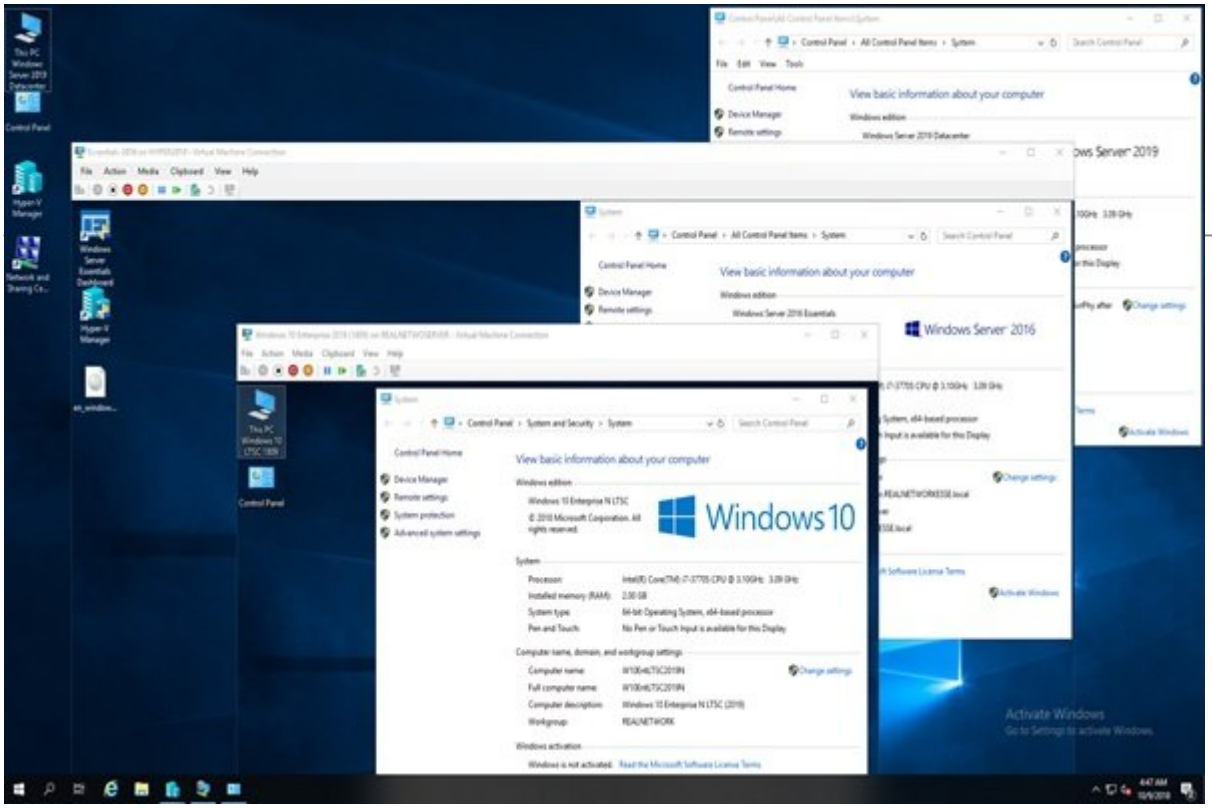
Remote Access Server در ویندوز سرور 2019 از چه بخش‌هایی ساخته شده است؟



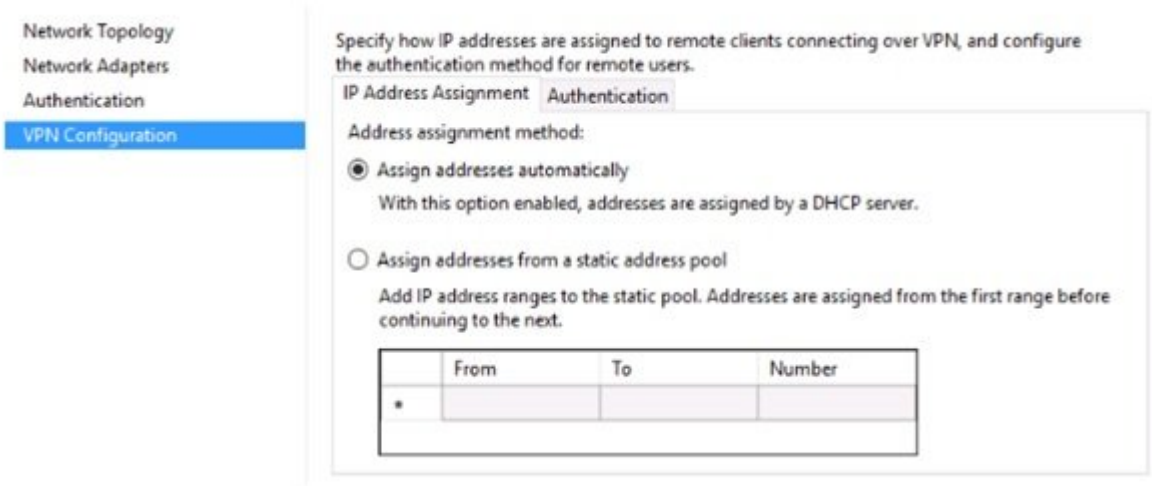
افرادی که سال‌ها است در دنیای فناوری‌اطلاعات کاری می‌کنند به خوبی با شبکه‌های خصوصی مجازی آشنا هستند، با این حال، قابلیتی که Always On VPN به دنیای فناوری‌اطلاعات اضافه کرد این است که تلفیقی از ویژگی‌های جدید را در تعامل با مکانیسم ارتباطی مبتنی بر شبکه خصوصی مجازی سنتی پیشنهاد داد. به همین دلیل نحوه برقراری ارتباط به همان شکلی انجام می‌شود که همه ما با آن آشنایی داریم.

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

Configuration

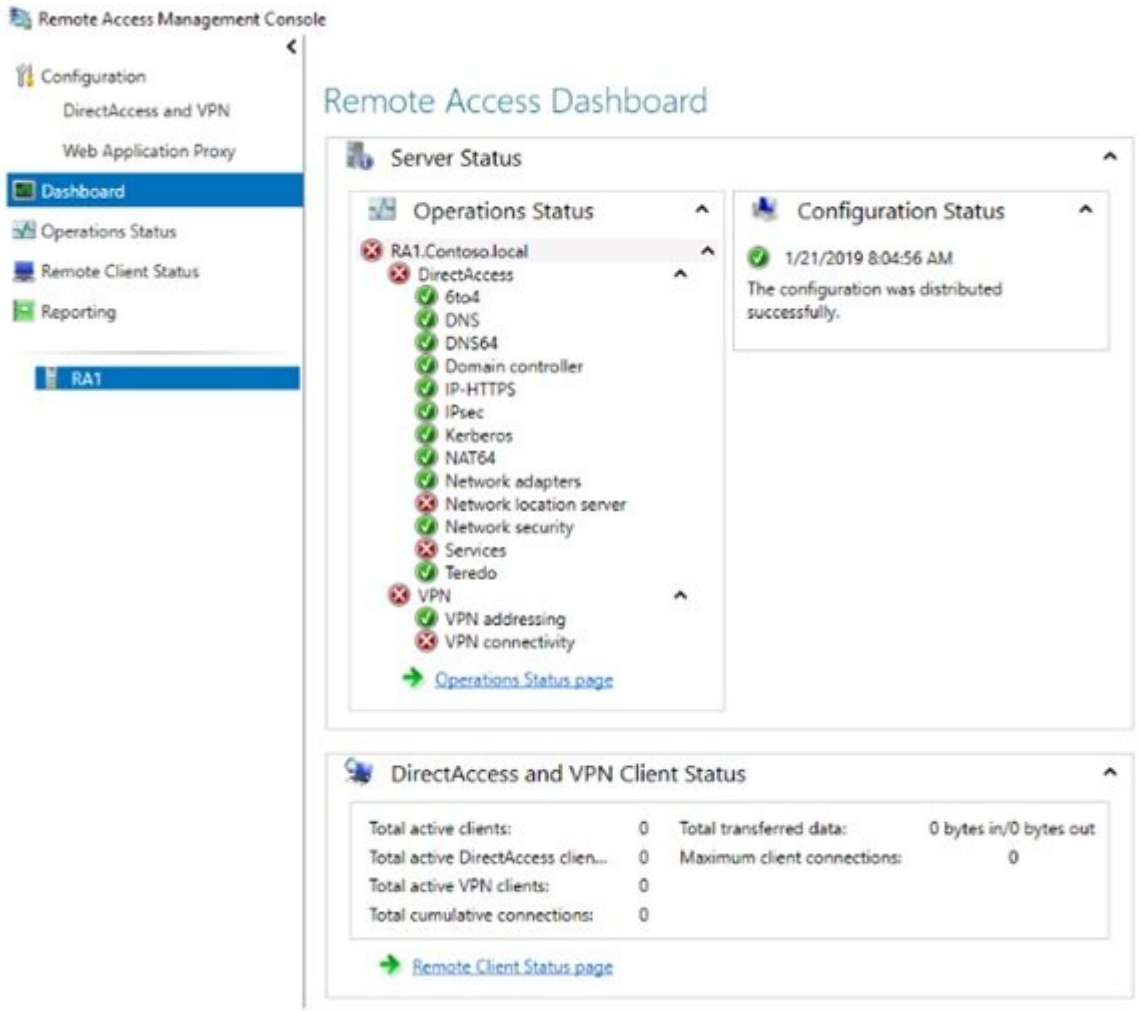
صفحه تنظیمات تا حد زیادی گویا است و بدون مشکل خاصی می‌توان از آن استفاده کرد. این صفحه مکانی است که پیکربندی‌های اولیه مربوط به دسترسی از راه دور را درون آن انجام می‌دهد و همچنین در آینده هرگونه تنظیماتی را از طریق این صفحه به‌روزرسانی می‌کنید همان‌گونه که در شکل زیر مشاهده می‌کنید، دسترسی به تنظیمات DirectAccess، VPN و حتا Proxy Application Web از درون کنسور مدیریت از راه دور امکان‌پذیر است. اگر در تصویر زیر دقت کنید، متوجه می‌شوید که من هر دو نقش DA/VPN و WAP را در کنار یکدیگر روی سرور یکسانی اجرا کرده‌ام، اما توصیه نمی‌کنم این‌کار را انجام دهید. من این کار را به دلیل این‌که توضیح این مطلب در آموزش فوق ساده باشد انجام دادم.

در ارتباط با VPN پیکربندی زیادی وجود ندارد و در بیشتر مواقع تنها یک صفحه از گزینه‌ها در اختیار دارید که باید نوع آدرس‌های آی‌پی که کلاینت‌های شبکه مخصوصی به آن متصل می‌شوند را تعریف می‌کنید و همچنین تعیین می‌کنید که فرآیند احراز هویت شبکه خصوصی مجازی چگونه انجام شود. داخل بخش مربوط به پیکربندی DirectAccess و VPN اگر روی Edit ... کلیک کنید دسترسی به ویزاد دیگری امکان‌پذیر می‌شود. آخرین صفحه این جادوگر ویزاد کوچک VPN Configuration نام دارد. این صفحه مکانی است که اجازه می‌دهد آدرس آی‌پی و تنظیمات احراز هویت برای ارتباطات مبتنی بر شبکه خصوصی مجازی را پیکربندی کنید. سایر تنظیمات مربوط به به پیکربندی شبکه خصوصی مجازی از طریق کنسول پیکربندی سنتی VPN یا همان RRAS انجام می‌شود، اما هر چیزی که در ارتباط با پیکربندی ارتباطات DirectAccess به آن‌ها نیازی دارید از داخل کنسول مدیریت از راه دور دسترسی و آن چهار مینی جادوگر کوچک انجام می‌شود.



Dashboard

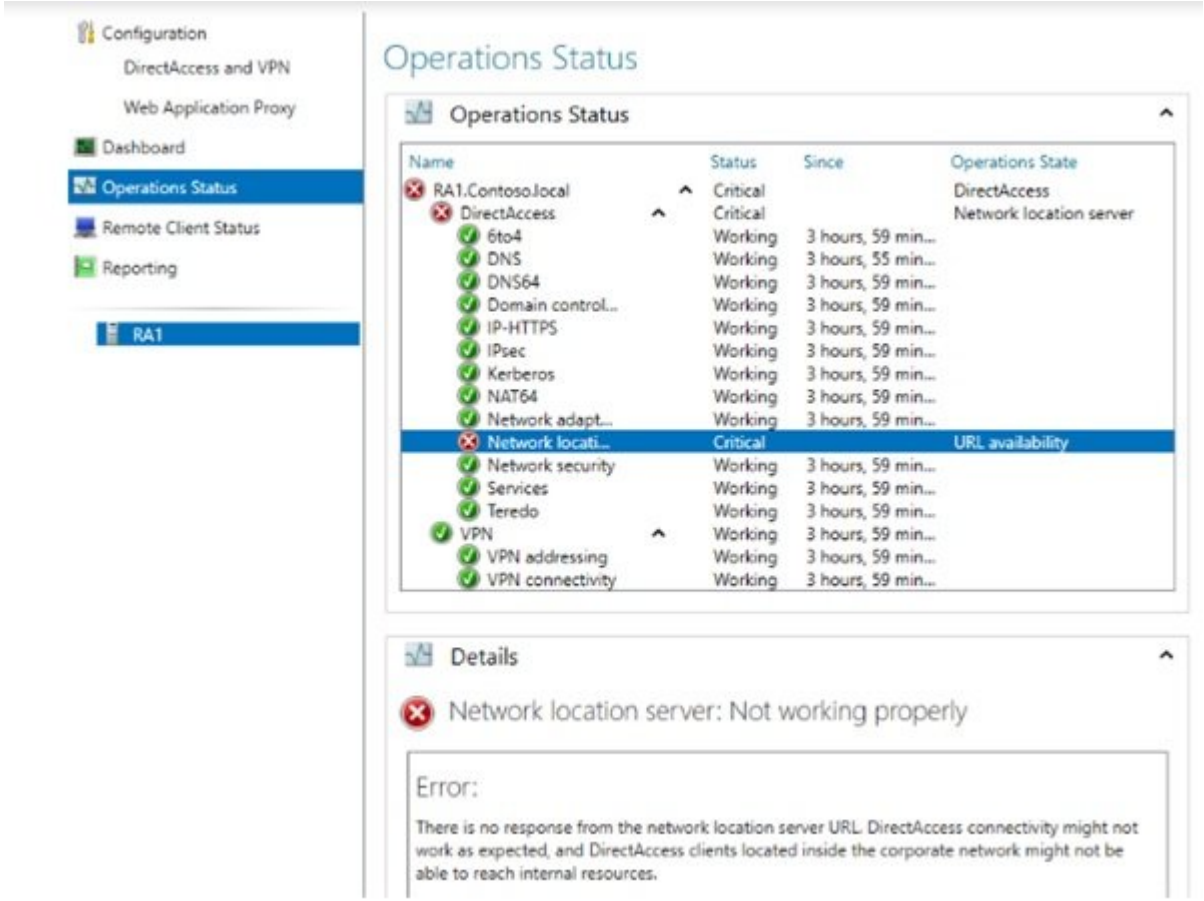
Dashboard Remote Access به شما اجازه می‌دهد وضعیت Remote Access Server را مشاهده کنید، نگاهی سریع به مولفه‌های در حال اجرا سرور داشته باشید، آخرین تغییرات اعمال شده روی پیکربندی‌ها را مشاهده کنید و نگاهی سریع به تعداد ارتباطات مبتنی بر DirectAccess و VPN داشته باشید.



Operations Status

اگر می‌خواهید اطلاعات بیشتری در ارتباط با اتصالات و اتفاقاتی که روی سرور رخ می‌دهد به دست آورید، صفحه

وضعیت عملیات (Operations Status) برای همین منظور طراحی شده است. در این صفحه اطلاعات دقیق‌تر و عمیق‌تری در مورد هر یک از مؤلفه‌هایی که در پشت صحنه اجازه می‌دهند ارتباطات مبتنی بر DA و VPN شکل بگیرند به دست می‌آورید. اگر هر یک از مولفه‌ها مشکلی دارند، کافی است روی مؤلفه خاصی کلیک کنید تا جزییات مرتبط با آن مولفه را مشاهده کنید. به عنوان یک آزمایش ساده وب‌سرور NLS را در شبکه خودم خاموش کردم. با این‌کار در صفحه وضعیت عملیات مشاهده می‌کنم که NLS همراه با یک پیغام خطا نشان داده شده است.



Remote Client Status

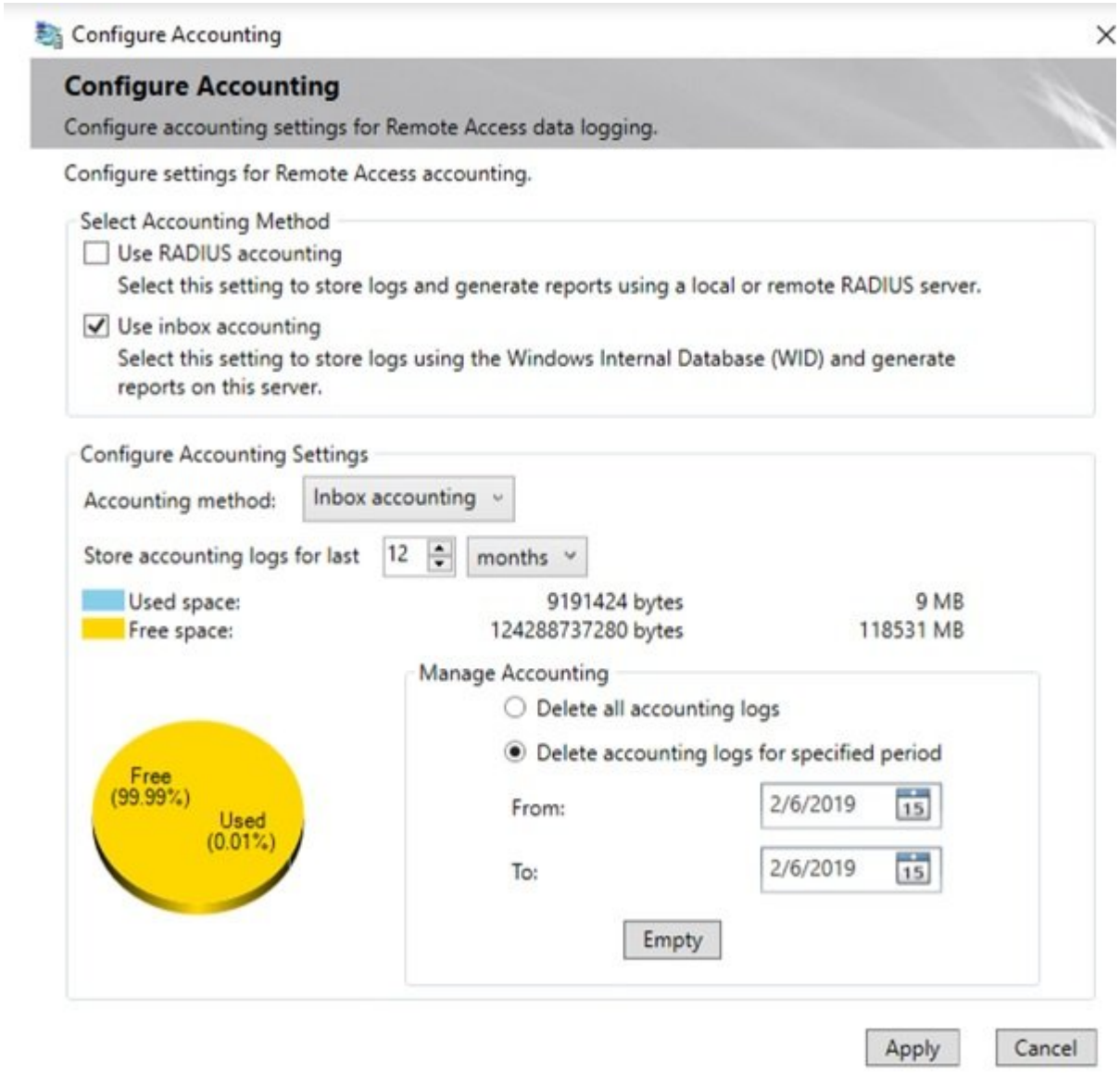
صفحه بعد، صفحه وضعیت کلاینت از راه دور (Remote Client Status) قرار دارد. همان‌گونه که در تصویر زیر مشاهده می‌کنید، در این بخش می‌توانید کامپیوترهای کلاینتی که متصل شده‌اند را مانیتور کنید. این صفحه ارتباطات مبتنی بر DirectAccess و VPN را نشان می‌دهد. در صفحه فوق می‌توانیم نام کامپیوترها، نام‌های کاربری و حتا منابعی که توسط اتصالات استفاده شده است را مشاهده کنیم. اطلاعات موجود در این صفحه را می‌توان با قرار دادن پارامترهایی از طریق نوار جستجوی بالای پنجره فیلتر کرد. توجه به این نکته مهم است که صفحه Remote Client Status فقط اتصالات فعال و زنده را نشان می‌دهد. در این صفحه هیچ اطلاعات مربوط به تاریخچه‌ها ذخیره نمی‌شود.

Reporting

همان‌گونه که حدس زده‌اید، پنجره فوق زمانی که قصد دارید تاریخچه‌ای از اطلاعات دسترسی از راه دور را مشاهده کنید به یاری‌تان می‌آید. این صفحه تقریباً دقیقاً مشابه صفحه Remote Client Status است با این تفاوت که اجازه می‌دهد گزارش‌هایی در ارتباط با تاریخچه داده‌ها را همراه با مشخص کردن زمان‌های خاصی مشاهده کنید. زمانی که داده‌ها نشان داده می‌شود، قابلیت جست‌وجو و فیلتر شبیه به صفحه Remote Client Status در اختیارتان قرار می‌گیرد.

گزارش‌گیری به صورت پیش‌فرض غیرفعال است، اما برای فعال‌سازی آن کافی است به صفحه Reporting بروید و گزینه Configure Accounting را کلیک کنید. پس از فعال‌سازی، گزینه‌هایی در ارتباط با ذخیره‌سازی اطلاعات

تاریخچه اتصالات ظاهر می‌شود. شما می‌توانید داده‌ها را در WID محلی یا روی سرور RADIUS از راه دور ذخیره کنید. در این بخش گزینه‌هایی برای مدت زمانی که داده‌ها باید ذخیره شده و مکانیسمی که داده‌های قدیمی باید پاک شوند وجود دارد.



Tasks

آخرین پنجره در کنسول مدیریت از راه دور دسترسی نوار Tasks نام دارد که سمت راست صفحه قرار دارد. عملکردها و گزینه‌هایی که در نوار وظیفه نمایش داده می‌شود بسته به اینکه در کدام قسمت از کنسول قرار دارید تغییر می‌کند. دقت کنید برای دسترسی به یکسری عملکردهای پیشرفته‌تر باز از نوار وظیفه استفاده کنید. از جمله کارهایی که با نوار وظیفه می‌توانید انجام دهید ساخت گزارش‌های کاربردی، به‌روزرسانی صفحه، فعال یا غیرفعال کردن شبکه‌های خصوصی مجازی و و پیکربندی توازن بار شبکه یا پیکربندی‌های چندگانه در صورتی که از چند سرور از راه دور دسترسی استفاده می‌کنید اشاره کرد.

VPN ، DA یا AOVPN کدامیک بهترین هستند؟

افرادی که سال‌ها است در دنیای فناوری‌اطلاعات کاری می‌کنند به خوبی با شبکه‌های خصوصی مجازی آشنا هستند، با این حال، قابلیتی که Always On VPN به دنیای فناوری‌اطلاعات اضافه کرد این است که تلفیقی از ویژگی‌های جدید را در تعامل با مکانیسم ارتباطی مبتنی بر شبکه خصوصی مجازی سنتی پیشنهاد داد. به همین دلیل نحوه برقراری ارتباط به همان شکلی انجام می‌شود که همه ما با آن آشنایی داریم. در چند شماره گذشته اطلاعات تقریبا کاملی در ارتباط با DirectAccess به دست آوردیم و اکنون می‌توانید به شکل دقیق‌تری به روش‌های پیشنهادی برای برقراری

یک ارتباط خودکار برای کلاینت‌های راه دور و اتصال آن‌ها به مرکز داده شرکت فکر کنید. اکنون که می‌دانید دو زیرساخت منحصر به‌فرد برای برقراری یک اتصال ایده‌آل و از پیش ساخته شده در ویندوز سرور 2019 در اختیار دارید، این توانایی را دارید که بدون مشکل خاصی به کارمندان خود اجازه دهید از دستگاه‌های همراه خود برای انجام کارها استفاده کنند.

جالب آن‌که شما نیازی به انتخاب ندارید، زیرا امکان به‌کارگیری و اجرای هر دو فناوری در سرور راه دور وجود دارد. هر فناوری مزایا و معایب خاص خود را دارد، اما روشی که شما از آن استفاده می‌کنید به عوامل متغیر متعددی بستگی دارد. کاربران ، کامپیوترهای کلاینت و سازمان شما نیازهای منحصر به‌فردی دارند که روی فرآیند تصمیم‌گیری اثرگذار هستند. اجازه دهید برخی از تفاوت‌های موجود میان DirectAccess و VPN را بررسی کنیم تا بتوانید در آینده یک تصمیم هوشمندانه اتخاذ کنید.

متصل به دامنه یا منفصل

یکی از بزرگ‌ترین ملزومات کامپیوترهای کلاینتی که از DirectAccess استفاده می‌کنند این است که باید به دامنه وصل شوند. در حالی که این الزامات به خودی‌خود مهم به نظر نمی‌رسند، اما در پس‌زمینه ممکن است به موضوعات بسیار مهمی اشاره کنند. اعتماد به یک کامپیوتر و متصل کردن آن به یک دامنه به معنای آن است که شما به لپ‌تاپ کارمندی اعتماد کامل دارید و لپ‌تاپ او را همانند کامپیوترهای شرکت در نظر گرفته‌اید. به عبارت دقیق‌تر، لپ‌تاپ توسط تیم فناوری‌اطلاعات تهیه و آماده شده است. شرکت‌هایی که عادت دارند به کارمندان خود اجازه دهند کامپیوترهایی را خریداری کنند و از آن‌ها برای انجام کارهای شرکت استفاده کنند به احتمال زیاد در زمان به‌کارگیری DirectAccess ممکن است با مشکلاتی روبرو شوند. DA همچنین برای شرایطی که کارمندان از کامپیوترهای خانگی برای اتصال به شبکه شرکت و انجام کارها از راه دور استفاده می‌کنند ایده‌آل نیست.

در شرایطی که ممکن است کامپیوترهای خانگی یا شخصی برای انجام کارها استفاده شوند، شبکه خصوصی مجازی گزینه مناسب‌تری است. شما می‌توانید از یک دستگاه مجهز به سیستم‌عامل ویندوز 10 که عضو دامنه نیست ، اما ویژگی Always On VPN روی آن قرار دارد، برای برقراری اتصال به شبکه خصوصی مجازی استفاده کنید و حتا می‌توانید ارتباطات مبتنی بر شبکه خصوصی مجازی (ارتباطات دستی) غیر مایکروسافتی را با شبکه خصوصی مجازی برقرار کنید. سیستم‌عامل‌های اندروید، iOS ، گوشی‌های ویندوزی و مک یک قابلیت از پیش ساخته شده VPN client دارند که می‌توانند برای برقراری اتصال با ویژگی Remote Access Server ویندوز 10 از آن استفاده کرد. اگر تنها راه‌حل شما برای برقراری یک ارتباط از راه دور DirectAccess است، در این حالت نمی‌توانید به دستگاه‌هایی که عضو دامنه نیستند اجازه برقراری ارتباط دهید. به خاطر داشته باشید اگرچه Always On VPN Tunnel User انعطاف‌پذیری بیشتری نسبت به DirectAccess دارد، اما اگر قصد به‌کارگیری AOVPN Device Tunnel را دارید، دستگاه شما باید عضوی از دامنه باشد.

راه‌اندازی خودکار یا دستی

روش‌های مختلفی برای برقراری ارتباط وجود دارد. زمانی‌که درباره به‌کارگیری DirectAccess یا شبکه خصوصی مجازی سنتی صحبت می‌کنیم، مشخص است که DirectAccess برنده است. هیچ سازمانی نمی‌خواهد کاربرانش ارتباطی را باز کنند و به شیوه دستی با شبکه خصوصی مجازی ارتباط برقرار کنند، در حالی که گزینه دیگری که امکان برقراری یک اتصال خودکار به شبکه خصوصی مجازی را فراهم می‌کند در دسترس است.

Always On VPN یک اتصال خودکار و یکپارچه به دنیای شبکه خصوصی مجازی پیشنهاد می‌دهد. AOVPN تقریبا همانند DirectAccess یکپارچه است. در زمان نگارش این مقاله پیاده‌سازی یک مکانیسم Device Tunnel کار چندان راحتی نیست. این بدان معنا است که اکثر شرکت‌هایی که AOVPN را استفاده می‌کنند تنها از حالت User Tunnel استفاده می‌کنند. در سناریوی User Tunnel ، شبکه خصوصی مجازی به‌طور خودکار راه‌اندازی می‌شود، اما تا زمانی‌که کاربر از صفحه ورود به سیستم وارد نشده باشد، این ارتباط ایجاد نمی‌شود، به عبارت دقیق‌تر، در چنین شرایطی DirectAccess باز هم نسبت به AOVPN برتری دارد، زیرا DA به‌طور یکپارچه در صفحه ورود به سیستم اتصال را برقرار می‌کند. در این حالت امکان تنظیم مجدد گذرواژه و کاربران دامنه جدید برای ورود به دستگاه‌های متصل به DA فراهم است. احتمال دارد در آینده شاهد پیشرفت‌هایی در ارتباط با دستگاه‌های AOVPN و User Tunnel باشیم تا یک اتصال واقعی و بدون مشکل برای کلاینت‌های AOVPN فراهم شود.

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:

06 آبان 1398

نشانی منبع:
https://www.shabakeh-mag.com/networking-technology/16215/remote-access-server-%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-%D8%A7%D8%B2-%DA%86%D9%87-%D8%A8%D8%AE%D8%B4%E2%80%8C%D9%87%D8%A7%DB%8C%DB%8C-%D8%B3%D8%A7%D8%AE%D8%AA%D9%87-%D8%B4%D8%AF%D9%87-%D8%A7%D8%B3%D8%AA%D8%9F