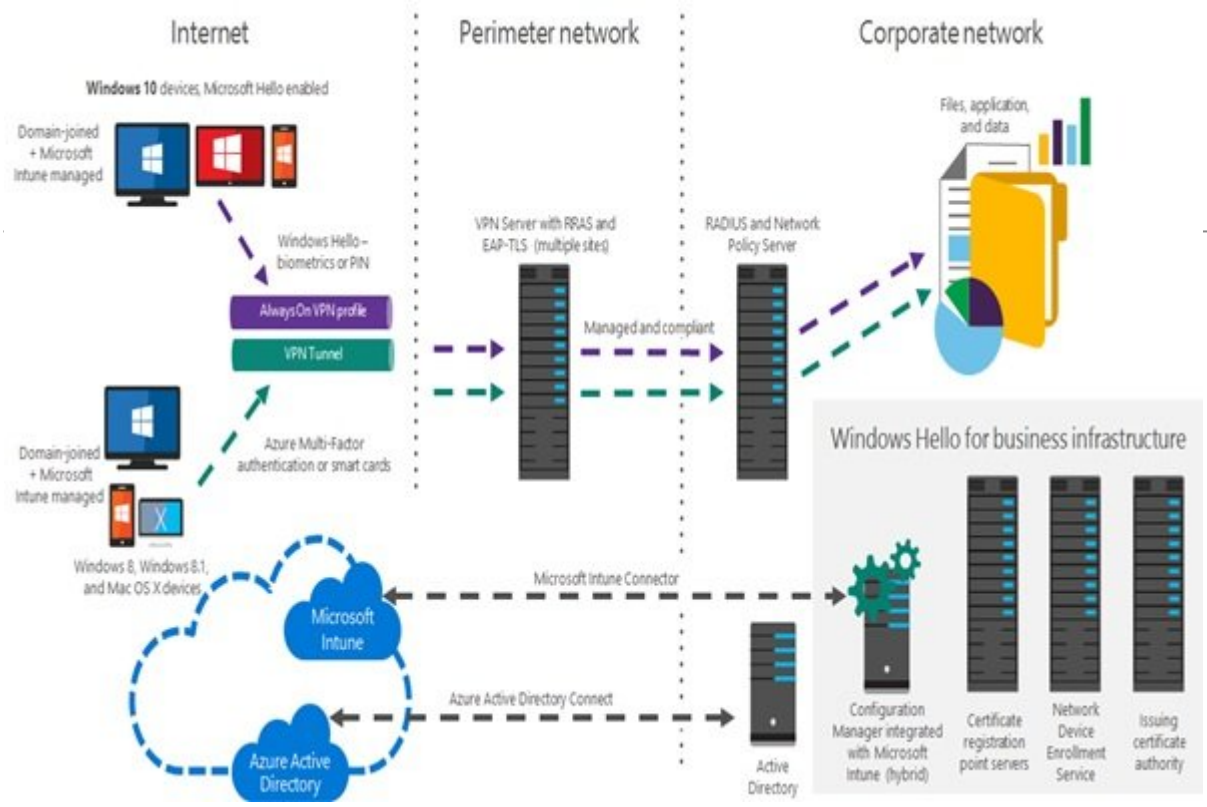
به چه ملزوماتی در ویندوز سرور 2019 برای استفاده از Always On VPN نیاز داریم؟



درک این نکته مهم است که بدانیم مولفه Always On بخشی از ویژگی Always On VPN است که عملکردی در سطح کلاینت دارد. شما می‌توانید از AOVPN در کامپیوترهای کلاینت استفاده کنید تا به انواع مختلف زیرساخت‌های شبکه خصوصی مجازی متصل شوید.

ملزومات کلاینتی موردنیاز برای AOVPN

درک این نکته مهم است که بدانیم مولفه Always On بخشی از ویژگی Always On VPN است که عملکردی در سطح کلاینت دارد. شما می‌توانید از AOVPN در کامپیوترهای کلاینت استفاده کنید تا به انواع مختلف زیرساخت‌های شبکه خصوصی مجازی متصل شوید.

در حالی که نزدیک به 15 تا 20 سال است که ما می‌توانیم به شکل دستی و عادی ارتباط مبتنی بر شبکه‌های خصوصی مجازی را در سیستم‌عامل کلاینت ویندوز ایجاد کرده و از آن استفاده کنیم، اما Always On VPN یک ویژگی کاملا جدید است. برای آن‌که بتوانید از ویژگی فوق استفاده کنید، کامپیوترهای کلاینت و کارمندان شما باید از ویندوز 10 استفاده کنند. به‌طور خاص، آن‌ها باید سیستم‌عامل ویندوز 10 نسخه 1607 یا جدیدتر را روی سامانه‌های خود داشته باشند. در حالت کلی ویژگی فوق با نسخه‌های زیر هماهنگ است:

ویندوز 10 1607+

ویندوز 10 1709+

ویندوز 10 1803+

یک دقیقه صبر کنید، چرا ما به بیلدهای مختلف و جداگانه اشاره کردیم؟ پاسخ روشن است. از نظر فنی Always On VPN به‌طور رسمی در زمان انتشار ویندوز 10 نسخه 1607 معرفی شد، اما به مرور زمان پیشرفت کرد. اجازه دهید به‌طور خلاصه و مختصر آن‌چه در طول سال‌ها تغییر کرده و پیشرفت کرده است را دومرتبه فهرست کنیم.

ویندوز 10 1607: قابلیت اصلی برای راه‌اندازی-خودکار اتصال به یک VPN را ارائه کرد.

ویندوز 10 1709: به‌روزرسانی‌ها و تغییراتی که شامل اضافه کردن حالت Device Tunnel در این نسخه اضافه شد. اگر قصد دارید یک حالت Device Tunnel را برای مدیریت کامپیوترها استفاده کنید کاری که بیشتر شرکت‌ها انجام می‌دهند حداقل به نسخه 1709 روی کامپیوترهای کلاینتی نیاز دارید.

ویندوز 10 1803: یکسری باگ‌های شناسایی شده در بیلد 1709 را برطرف کرد. در واقعیت، امروزه کمتر شرکتی را پیدا می‌کنید که از ویژگی Always On VPN استفاده کند و از نسخه 1803 استفاده نکرده باشد. خوشبختانه، زیرساخت به‌روزرسانی ویندوز 10 بسیار بهتر از قبل شده است، به این معنا که بسیاری از سامانه‌های امروزی به‌طور خودکار در حال ارتقا به نسخه‌های جدیدتر ویندوز 10 است.

لازم به توضیح است که ویژگی Always On VPN با نسخه‌هایWindows 10 Home ، Pro، Enterprise کار می‌کند. در نتیجه User Tunnel با تمامی نسخه‌های ویندوز سازگاری دارد.

یکبار دیگر تکرار می‌کنیم که اگر می‌خواهید از حالت Device Tunnel و ویژگی Always On VPN استفاده کنید باید به دامنه متصل باشید و همچنین از نسخه‌های سازمانی یا آموزشی ویندوز استفاده کنید.

متصل به دامنه

همان‌گونه که اشاره شد، زمانی‌که قصد دارید از حالت AOVPN Device Tunnel استفاده کنید، کامپیوترهای کلاینت باید به دامنه متصل باشند. با این وجود، اگر تنها به دنبال پیاده‌سازی حالت User Tunnel هستید نیازی نیست کامپیوترها عضوی از دامنه باشند. هرچند کلاینت‌ها هنوز باید Windows 10 1607 یا نسخه‌های جدیدتر را استفاده کنند، در این حالت کلاینت‌ها می‌توانند کامپیوترهای خانگی باشند که به یک ایستگاه کاری ساده متصل شده‌اند و عضوی از دامنه نیستند.

این موضوع به ویژه در مستندات مایکروسافت به آن اشاره شده است، زیرا قابلیت فوق به سازمان‌ها و کارمندان آن‌ها اجازه می‌دهد از ویژگی Always On VPN استفاده کنند و در نتیجه با اصل BYOD کاملا سازگار است. در حالی که این موضوع جالب است، اما انتظار نمی‌رود که تمامی سازمان‌ها به کارمندان خود اجازه دهند کامپیوترهای شخصی را به VPN سازمانی متصل کنند. اکثر سازمان‌ها یک دسترسی محدود در ارتباط با BYOD را با به‌کارگیری فناوری‌های ابرمحور شبیه به Office 365 برای بررسی ایمیل‌ها و اسناد ارائه می‌کنند. اما اتصال کامپیوترها و دستگاه‌ها به شبکه سازمانی بر مبنای یک تونل شبکه خصوصی مجازی لایه 3 که امکان اتصال کامل را ارائه می‌کند چندان عملی نخواهد بود، زیرا یک کابوس شبانه برای مدیران امنیتی سازمان‌ها به وجود می‌آورد و تقریبا همه آن‌ها با این مسئله مخالفت می‌کنند.

پیکربندی تنظیمات

اجازه دهید این‌گونه تصور کنیم که تمامی مولفه‌ها و ملزومات موردنیاز سرور برای اتصال به شبکه خصوصی مجازی را آماده کرده‌اید و اکنون قصد پیکربندی یک اتصال به شبکه خصوصی مجازی را دارید و در حقیقت با موفقیت توانسته‌اید یک اتصال به شبکه خصوصی مجازی سنتی را به شکل دستی پیاده‌سازی کنید و زیرساخت شما در این زمینه مشکلی ندارد. اکنون، چه کاری باید انجام دهیم تا کلاینت‌ها بتوانند از اتصال مبتنی بر ویژگی Always On استفاده کنند؟

پیکربندی تنظیمات و خط‌مشی‌های Always On VPN کار سختی نیست. شما باید درباره گزینه‌های در دسترس اطلاع داشته باشید تا بتوانید به درستی این ویژگی را در محیط سازمانی مستقر کرده و فایل‌ها و اسکریپت‌ها را پیکربندی کنید. ما نمی‌توانیم تمامی گزینه‌ها را به‌طور کامل پوشش دهیم، بلکه در این‌جا روش پیکربندی کلی تنظیمات به منظور برقراری یک اتصال دستی به شبکه خصوصی مجازی، پیکربندی تنظیمات امنیتی و تأیید اعتبار و سپس ابزاری که اجازه می‌دهد پیکربندی‌ها را به برخی از فایل‌های پیکربندی ارسال کنید را بررسی خواهیم کرد. تنظیمات شبکه خصوصی مجازی در قالب‌های XML و PS1 (اسکریپت پاورشل) ذخیره می‌شوند. شما ممکن است در برخی موارد مجبور شوید یک یا هر دو این فایل‌ها را برای کارمندان خاصی به شکل مشخصی پیکربندی کنید. برای اطلاعات بیشتر در ارتباط با سایر تنظیمات پیشنهاد می‌کنم به مقاله **vpn-deploy-client-vpn-connections** مراجعه کنید.هنگامی که فایل‌های پیکربندی را ایجاد کردید در مرحله بعد باید پیکربندی‌ها را برای کلاینت‌ها ارسال کنید. در حالت ایده‌آل شما باید به نوعی یک راه‌حل مدیریت دستگاه تلفن همراه (MDM) داشته باشید تا تنظیمات را برای کارمندان ارسال کنید. در حالی که فناوری‌های مختلفی در ارتباط با MDM ارائه شده‌اند، اما پیشنهاد ما در این زمینه دو محصول مایکروسافت به‌نام‌های (SCCM System Center Manager) و Microsoft Intune است.

اگر به‌طور پیش‌فرض SCCM را به شکل سازمانی در اختیار دارید، عالی است. به راحتی می‌توانید تنظیمات مبتنی بر

پاورشل را پیکربندی کنید و تنظیمات را برای کامپیوترهای کلاینت ارسال کنید تا ویژگی Always On VPN فوق برای آن‌ها فعال شود.

اگر SCCM را در اختیار ندارید، اما کسب‌وکار شما مبتنی بر ابر است، بازهم راهکار جالب دیگری در اختیارتان قرار دارد. شما می‌توانید از Intune برای تنظیم کردن تنظیمات AOVPN از طریق پیکربندی XML استفاده کنید. یکی از مزایای استفاده از مسیر Intune این است که Intune می‌تواند کامپیوترهای غیر عضو دامنه را مدیریت کند، بنابراین می‌توانید به لحاظ تئوری کامپیوترهای خانگی و شخصی کاربران را در زیرساخت‌های مدیریت شده با Intune قرار دهید و آن‌ها را برای اتصال تنظیم کنید.

SCCM و Intune دو راهکار عالی هستند، اما شرکت‌ها نمی‌توانند از آن‌ها استفاده کنند. در چنین حالتی گزینه سومی برای ارسال تنظیمات Always On VPN در اختیار مدیران شبکه‌ها قرار دارد. البته در روش فوق باید با نحوه اسکریپت‌نویسی در پاول‌شل آشنا باشید. در حقیقت راهکار سوم طرح دومی است که مایکروسافت ارائه کرده، هرچند پیشنهاد می‌کند که سازمان‌ها از راهکار MDM برای ارسال تنظیمات AOVPN استفاده کنند. البته راهکار پاورشل به سادگی دو روش یاد شده نیست، بزرگ‌ترین مشکلی که وجود دارد این است که پاورشل برای ارسال تنظیمات AOVPN باید در سطح بالا اجرا شود، در نتیجه خودکارسازی کار سختی خواهد بود، زیرا برای ورود به سیستم کاربر (مکانی که باید ارتباط VPN را منتشر کنید) باید یک مدیر محلی باشید که اسکریپت به درستی اجرا شود.

انتظار می‌رود که مایکروسافت در زمان انتشار نسخه بعدی ویندوز سرور یک الگوی خط‌مشی Group Policy را برای ارسال تنظیمات Always On VPN آماده کند، زیرا همه کاربران Group Policy را دارند، اما همه MDM را ندارند. با توجه به این‌که مباحث مربوط به AOVPN به‌طور مداوم بهبود می‌یابد و احتمالا تغییراتی در این حوزه از فناوری رخ میردهد، پیشنهاد می‌کنم هرچند وقت یکبار مستندات مایکروسافت را بررسی کنید.

مولفه‌های سرور AOVPN

اکنون که می‌دانیم در سمت کلاینت به چه ملزوماتی برای ایجاد Always On VPN نیاز داریم، لازم است درباره ملزوماتی اطلاع به دست آوریم که در سمت سرور/ زیرساخت اجازه برقراری یک اتصال را می‌دهند. جالب است که مولفه‌های Always On AOVPN هیچ ارتباطی با زیرساخت‌های سرور ندارند. بخش Always On به‌طور کامل در سمت کلاینت مدیریت می‌شود. بنابراین، تمام کاری که باید از طرف سرور انجام دهیم این است که مطمئن شویم که امکان دریافت اتصالات VPN ورودی وجود دارد. اگر در حال حاضر نیرویی دارید که می‌تواند ارتباط با شبکه خصوصی مجازی VPN را با موفقیت برقرار کند، به احتمال زیاد زیرساخت سرور برای تعامل با AOVPN آماده است.

سرور دسترسی از راه دور

بدیهی است، شما به یک سرور VPN نیاز دارید تا بتوانید اتصالات VPN را میزبانی کنید، درست است؟ خوب ، نه به این شکل. در ویندوز سرور، نقشی که میزبان اتصالات AOVPN ، VPN و DirectAccess است وجود دارد. این نقش Remote Access نامیده می‌شود، اما شما در واقع می‌توانید Always On VPN را استفاده کنید بدون آن‌که ویندوز سرور به عنوان remote Access Server تعریف شده باشد. از آن‌جایی که Always On عملکرد سمت کلاینت دارد، این امکان را فراهم می‌آورد تا زیرساخت‌های سمت سرور VPN توسط فروشندگان شخص ثالث میزبانی شود. حتی اگر این موضوع به لحاظ فنی دقیق و قابل اجرا باشد، بدون شک چیزی نیست که مایکروسافت انتظار آن‌را داشته باشد. ما علاقه داریم از Microsoft Always On VPN برای میزبانی نقش Remote Access در ویندوز سرور استفاده کنیم که نقش سیستم ورودی را برای تمامی ارتباطات راه دور کلاینت‌ها بازی می‌کند.

بسیاری از افراد فرض می‌کنند که AOVPN جزء جدایی‌ناپذیر ویندوز سرور 2019 است، زیرا یک فناوری کاملا جدید است و سرور 2019 به تازگی عرضه شده، اما در واقع اینگونه نیست. شما می‌توانید زیرساخت VPN خود (نقش Remote Access) را روی سرور 2019 ، سرور 2016 یا حتا Server 2012 R2 میزبان کنید. این کار در پس‌زمینه انجام می‌شود و به کلاینت‌ها امکان می‌دهد تا اتصالات VPN خود را انتخاب کنند.

بعد از نصب نقش Remote Access روی ویندوز سرور جدید خود، متوجه می‌شوید که بیشتر تنظیمات VPN از طریق کنسول سرنام Routing and Remote Access (RRAS) مدیریت و پیکربندی می‌شوند. زمانی‌که پیکربندی

VPN را انجام می‌دهید، متوجه خواهید شد که پروتکل‌های مختلفی وجود دارند که می‌توانند به منظور برقراری ارتباط VPN بین کلاینت و سرور استفاده شوند و شما باید حداقل اطلاع اولیه در مورد این پروتکل‌ها داشته باشید. در شماره آینده به‌طور مختصر به این پروتکل‌ها نگاهی خواهیم داشت.

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:

20 مهر 1398

نشانی منبع:
https://www.shabakeh-mag.com/networking-technology/16150/%D8%A8%D9%87-%DA%86%D9%87-%D9%85%D9%84%D8%B2%D9%88%D9%85%D8%A7%D8%AA%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%B1-2019-%D8%A8%D8%B1%D8%A7%DB%8C-%D8%A7%D8%B3%D8%AA%D9%81%D8%A7%D8%AF%D9%87-%D8%A7%D8%B2-always-vpn-%D9%86%DB%8C%D8%A7%D8%B2-%D8%AF%D8%A7%D8%B1%DB%8C%D9%85