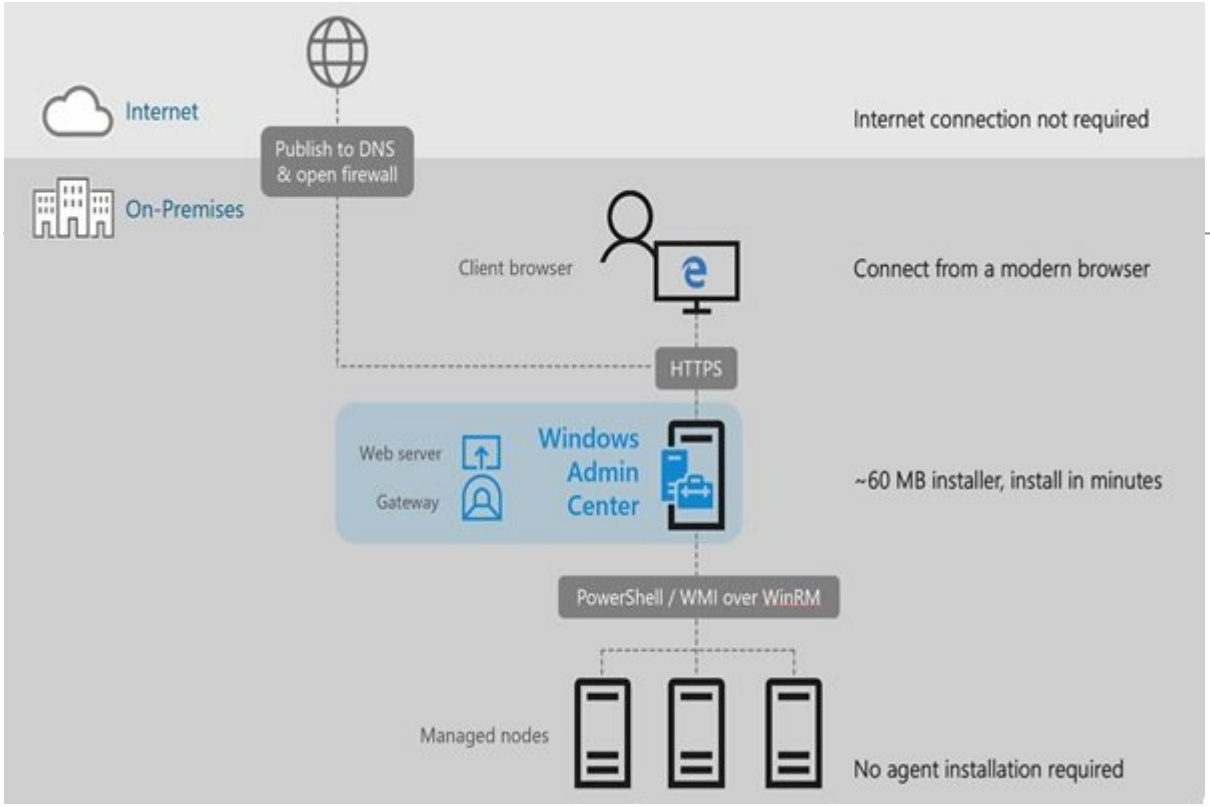
ویندزو سرور 2019 چه راهکارهایی برای برقراری اتصال به یک شبکه خصوصی مجازی ارائه می‌کند؟



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. پروتکل‌های فوق هر یک مزایای خاص خود را دارند که IKEv2 جزء متداول‌ترین آن‌ها است. از طرفی زمانی که درباره ویژگی Always On VPN صحبت کردیم، چند مرتبه به فناوری DirectAccess مایکروسافت اشاره کردیم. DirectAccess شکل دیگری از اتصال خودکار شبیه به شبکه خصوصی مجازی است، اما نسبت به روش Always On VPN رویکرد متفاوتی دارد.

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

IKEv2

IKEv2 جدیدترین و قوی‌ترین پروتکل در دسترس است که بهترین راهکار برای اتصال کامپیوترهای کلاینت از طریق شبکه خصوصی مجازی، AOVPN را ارائه می‌کند. IKEv2 تنها راه اتصال به شبکه خصوصی مبتنی بر Tunnel Device است. IKEv2 برای آن‌که بتواند از طریق مکانیسم احراز هویت اتصالی را انتشار دهد به گواهی‌نامه ماشین نیاز دارد. این حرف به معنای آن است که اگر می‌خواهید کلاینت‌های شما از طریق IKEv2 متصل شوند، کلاینت‌ها باید عضوی از دامنه باشند. دقت کنید که IKEv2 از درگاه‌های UDP 500 و 4500 برای برقراری ارتباط خود استفاده می‌کند.

SSTP

SSTP یک روش بازگشتی برای برقراری اتصال به AOVPN است. SSTP از یک جریان SSL برای برقراری ارتباط استفاده می‌کند. به همین دلیل باید گواهینامه SSL روی Remote Access Server نصب شده باشد، اما به گواهی‌نامه ماشین روی کامپیوترهای کلاینت نیازی ندارد. SSTP از پورت TCP 443 استفاده می‌کند، بنابراین می‌تواند حتا از داخل شبکه‌های بسیار محدود که IKEv2 قادر به ارائه سرویس به آن‌ها نیست (به دلیل وابستگی IKEv2 به پروتکل UDP) یک اتصال را برقرار کند.

L2TP

این پروتکل زیاد برای استقرار AOVPN استفاده نمی‌شود، L2TP قادر است با استفاده از گواهینامه‌ها یا یک کلید از پیش به‌اشتراک قرار گرفته یک اتصال مبتنی بر شبکه خصوصی مجازی را ایجاد کند. اگر دو پروتکل یاد شده را در اختیار دارید بهتر است از پروتکل فوق استفاده نکنید.

PPTP

در حالی که هنوز یک گزینه پیکربندی معتبر در RRAS به شمار می‌رود، اما به تدریج در حال محو شدن است. مکانیزم امنیتی PPTP شکسته شده است، در نتیجه اگر هنوز اتصالات شبکه خصوصی مجازی را بر اساس PPTP اجرا می‌کنید، باید بدانید که جریان ترافیک شما بدون رمزگذاری و در قالب یک متن ساده روی اینترنت مبادله می‌شود.

مرجع صدور گواهینامه (CA)

گواهینامه‌های ماشین، گواهینامه‌های کاربر، گواهینامه‌های SSL ...! بدیهی است برای استفاده از Always On VPN باید با سازوکار و نحوه استقرار گواهینامه‌ها آشنا باشید. این تعامل با ارائه فناوری‌های جدید متداول‌تر می‌شود، زیرا یک مکانیسم امنیتی خوب را ارائه می‌کند. شرط اصلی این است که برای صدور گواهینامه‌ها زیرساخت کلید عمومی (PKI) موردنیاز را در محیط خود و حداقل یک سرور ویندوز مرجع صدور گواهی‌نامه داشته باشید. مکان‌هایی که گواهی‌نامه‌ها می‌توانند با استفاده از زیرساخت AOVPN از آن استفاده کنند به شرح زیر است:

User certificates: این‌ها گواهینامه‌هایی هستند که برای کاربران شبکه خصوصی مجازی از طریق یک سرور مرجع صدور گواهی داخلی انتشار پیدا می‌کنند. این گواهی‌نامه‌ها توسط User Tunnel برای احراز هویت استفاده می‌شوند.

Machine certificates: این‌ها گواهینامه‌هایی هستند که از یک مرجع صدور گواهی‌نامه داخلی برای ایستگاه‌های کاری (عمدتا لپ‌تاپ‌ها) صادر می‌شوند و برای احراز هویت Device Tunnel به کار گرفته می‌شوند.

SSL certificates: این گواهی‌نامه‌ها برای اعتبارسنجی ترافیک ورودی برای اتصالات SSTP VPN روی سرور دسترسی از راه دور نصب می‌شوند.

VPN and NPS machine certificates: سرور دسترسی از راه دور شما و همچنین سرورهای NPS که در ادامه با آن‌ها آشنا خواهیم شد نیاز به گواهی‌های ماشینی دارند که توسط مرجع صدور گواهی‌نامه داخلی صادر شده است.

سرور خط‌مشی شبکه (NPS)

سرور تعیین خط‌مشی شبکه (NPS) سرنام Network Policy Server اساساً روش احراز هویت اتصالات شبکه خصوصی مجازی هستند. هنگامی‌که یک درخواست برای اتصال به شبکه خصوصی مجازی وارد می‌شود، Remote Access Server مکانیسم تایید اعتبار کلاینت را توسط نقش NPS انجام می‌دهد و همچنین تأیید می‌کند که کاربر مجوز ورود به سیستم از طریق شبکه خصوصی مجازی را دارد.

در اغلب موارد زمانی‌که درباره اتصال به شبکه خصوصی مجازی مبتنی بر محصولات مایکروسافت صحبت می‌کنیم، ما نقش NPS را پیکربندی می‌کنیم تا فقط به کاربرانی که بخشی از یک گروه امنیتی خاص در اکتیو دایرکتوری هستند اجازه دهیم به شبکه خصوصی مجازی متصل شوند. به‌عنوان مثال، اگر گروهی به نام VPN Users ایجاد کنید و سپس در نقش NPS به آن گروه اشاره کنید، فقط به کاربران آن گروه اجازه خواهید داد به شکل موفقیت‌آمیز یک اتصال به شبکه خصوصی مجازی را برقرار کنند. NPS یکی دیگر از نقش‌های ویندوز سرور است که می‌تواند روی خود سیستم میزبان شود یا به دلیل افزونگی در سرورهای مختلف پخش شود. در محیط‌های کوچک که فقط یک سرور دسترسی از راه دور دارند، به‌طور مشترک می‌توان نقش NPS را در همان سروری که اتصال VPN را فراهم می‌کند، میزبانی کرد.

DirectAccess

در مدت زمانی که درباره ویژگی Always On VPN صحبت می‌کردیم، چند مرتبه به ویژگی DirectAccessمایکروسافت اشاره کردیم. DirectAccess شکل دیگری از اتصال خودکار شبیه به شبکه خصوصی مجازی است، اما نسبت به روش Always On VPN رویکرد متفاوتی دارد. در جایی که AOVPN به سادگی از پروتکل‌های VPN شناخته شده و مشهور استفاده می‌کند و برخی کارهای حیرت‌انگیز انجام می‌دهد تا به‌طور خودکار تونل‌های VPN سنتی را اجرا کند، تونل‌های DirectAccess کاملا اختصاصی هستند. تونل‌ها توسط IPsec محافظت می‌شوند و در واقع غیر قابل نفوذ هستند. تیم‌های امنیتی عاشق مکانیسم‌های امنیتی و پیچیده‌ای هستند که پیرامون

تونل‌های DA قرار دارند، زیرا یک بستر ارتباطی ایجاد می‌شود که مهاجمان هیچ راهکاری برای دستکاری یا تکثیر آن ندارند.

Microsoft DirectAccess اصلی‌ترین دلیلی این است که مدیران نقش Remote Access را روی ویندوز سرور نصب می‌کنند. همان‌گونه که اشاره شد، عملکرد DirectAccess را می‌توانید شبیه به یک شبکه خصوصی مجازی خودکار تصور کنید. مشابه شبکه خصوصی مجازی، هدف این است که کامپیوتر کاربران از راه دور به شبکه سازمانی متصل شود. با این حال، روشی که برای اتصال استفاده می‌شود متفاوت از روشی است که کارمندان برای اتصال به شبکه خصوصی مجازی از آن استفاده می‌کنند. DirectAccess یک مولفه نرم‌افزاری نیست، بلکه مجموعه‌ای از مؤلفه‌هایی است که قبلا در سیستم‌عامل ویندوز به تکامل رسیده‌اند و در کنار هم کار می‌کنند تا دسترسی کاملا یکپارچه‌ای را ارائه کنند. منظورم از یکپارچه بودن چیست؟ یعنی به همان روشی که AOVPN بدون تعامل با کاربر امکان برقراری ارتباط را می‌دهد، در این‌جا هیچ کاری لازم نیست کاربر برای اتصال به DirectAccess انجام دهد. DirectAccess همه این‌کارها را خودش انجام می‌دهد. به محض اینکه لپ‌تاپ کاربر یک اتصال اینترنتی را از وای‌فای خانگی، اینترنت عمومی در کافی‌شاپ یا هات‌اسپات سلولی دریافت می‌کند، تونل‌های DirectAccess به‌طور خودکار و زمانی که اتصال اینترنتی برقرار می‌شود ایجاد می‌کنند، بدون آن‌که کاربر نقشی در این زمینه داشته باشد.

خواه از Always On VPN یا DirectAccess استفاده کنید، زمانی‌که کامپیوتر شما به‌طور خودکار به شبکه متصل می‌شود، به میزان قابل توجهی در وقت و هزینه شما صرفه‌جویی می‌کند. در زمان صرفه‌جویی می شود زیرا کاربر دیگر مجبور نیست اتصال VPN را راه‌اندازی کند. در هزینه صرفه‌جویی می‌شود، زیرا زمان برابر است با پول است و شما با داشتن یک اتصال همیشگی ضمن آن‌که خط‌مشی‌های امنیتی را رعایت کرده‌اید به کلاینت‌ها و کامپیوترهای راه‌دور اجازه داده‌اید به شبکه متصل شوند. دیگر لازم نیست صبر کنید تا کاربران دوباره به دفتر خود برگردند یا این‌که تصمیم بگیرند که اتصال شبکه خصوصی مجازی را به شکل دستی راه‌اندازی کنند تا بتوانند تنظیمات و خط‌مشی های جدید را به سمت کامپیوترهای خود هدایت کنند. همه کارها مادامی که دسترسی به اینترنت امکان‌پذیر باشد انجام می‌شود. واضح است که با پیشرفت دو فناوری دسترسی از راه دور که هر دو روی اتصال خودکار کاربران از راه دور متمرکز شده‌اند ، مایکروسافت در حال بهبود بهره‌وری کارمندان یک سازمان است. شبکه‌های خصوصی مجازی هیچ‌گاه به این شکل ساده در دسترس ما قرار نداشتند و به نظر می‌رسد در حال ورود به عصر جدیدی هستیم که همه چیز به سمت خودکار شدن پیش می‌رود.

DirectAccess از زمان انتشار ویندوز سرور 2008 R2 وجود داشت، اما با این حال چندان از سوی مدیران شبکه استفاده نمی‌شد. در روزهای آغازین ارائه، استقرار آن دشوار بود و دردسرهای زیادی را متوجه مدیران شبکه می‌کرد، اما طی چند سال گذشته تغییرات زیادی رخ داده و DirectAccess اکنون استقرار این فناوری ساده‌تر از هر زمان دیگری شده و مزایای متعددی برای محیط شما به همراه می‌آورد.

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:

24 مهر 1398

نشانی منبع:
https://www.shabakeh-mag.com/networking-technology/16160/%D9%88%DB%8C%D9%86%D8%AF%D8%B2%D9%88-%D8%B3%D8%B1%D9%88%D8%B1-2019-%DA%86%D9%87-%D8%B1%D8%A7%D9%87%DA%A9%D8%A7%D8%B1%D9%87%D8%A7%DB%8C%DB%8C-%D8%A8%D8%B1%D8%A7%DB%8C-%D8%A8%D8%B1%D9%82%D8%B1%D8%A7%D8%B1%DB%8C-%D8%A7%D8%AA%D8%B5%D8%A7%D9%84-%D8%A8%D9%87-%DB%8C%DA%A9-%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