DirectAccess در ویندوز سرور 2019 به چه ملزوماتی نیاز دارد؟

هنگامی که در خانه نشسته‌ایم از لپ‌تاپ شرکت و با استفاده از DirectAccess به شبکه شرکت متصل می‌شویم و کارهای خود را انجام می‌دهیم. اما چگونه می‌توانیم از DirectAccess در ویندوز سرور 2019 استفاده کنیم و چه مولفه‌ها و پیش‌نیازهایی برای انجام این‌کار لازم است.

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

پیش‌نیازهای DirectAccess

DirectAccess مولفه‌های زیادی دارد و به روش‌های مختلفی می‌توانید این مولفه‌ها را تنظیم کنید. با این حال، تمامی راهکارها عملکرد خوبی ندارند. بنابراین، بهتر است با روش‌هایی که اجازه می‌دهند محیط DirectAccess را به درستی پیکربندی کنید آشنا شوید.

اتصال به دامنه

اولین و بزرگ‌تری پیش‌نیازی که برای کار با DirectAccess باید رعایت کنید متصل کردن سامانه‌ها به یک دامنه است. تمامی سرورهای DA یا سایر سرورها باید به دامنه متصل شوند و تمامی کامپیوترهای کلاینتی که می‌خواهید متصل به DA شوند، باید به یک دامنه متصل باشند. عضویت در دامنه برای تأیید اعتبار لازم است به دلیل این‌که تنظیمات کلاینت DirectAccess که باید روی کامپیوترهای همراه اعمال شوند از طریق Group Policy روی کامپیوترها اعمال می‌شود. قبل از به‌کارگیری DirectAccess لازم است به این موضوع اشاره کنیم که در زمان پیاده‌سازی و طراحی برنامه خود به این موضوع توجه داشته باشید که بیشتر کاربران لپ‌تاپ‌های خود از یک فروشگاه اینترنتی یا سنتی خریداری می‌کنند و معمولا نمی‌توانند از DirectAccess استفاده کنند، مگر این‌که شما کامپیوترهای کلاینت‌ها را به دامنه متصل کنید. DA در حقیقت یک فناوری است که برای مدیریت و متصل کردن کامپیوترهای عضو دامنه به منابع سازمانی طراحی شده است. درک این موضوع از دیدگاه امنیتی حائز اهمیت است، زیرا سرور یا سرورهای DirectAccess شما معمولا در لبه شبکه شما قرار دارند. متداول و مرسوم است که کارت‌های شبکه خارجی در یک سرور DA درون یک DMZ قرار بگیرند و همچنین عضوی از دامنه باشند که شاید متفاوت از کاری باشد که به‌طور معمول با سیستم‌هایی که در یک شبکه محیطی قرار دارند انجام می‌دهید.

سیستم‌عامل‌های کلاینت پشتیبانی شده

تمامی سیستم‌عامل‌های کلاینت ویندوز مؤلفه‌هایی که برای ایجاد اتصال با DirectAccess ضروری است را در اختیار ندارند. نسخه سازمانی ویندوز (Enterprise) تمامی مولفه‌هایی که برای اتصال به آن‌ها نیاز است را درون خود جای

داده است، اما همه کاربران چنین سیستم‌عاملی را ندارند. هنوز هم بسیاری از مشاغل کوچک از نسخه‌های حرفه‌ای یا حتا خانگی روی ماشین‌های کلاینت استفاده می‌کنند و این نسخه‌ها فاقد مولفه‌های DirectAccess هستند. در مدت زمان برنامه‌ریزی برای پیاده‌سازی و استفاده از فناوری فوق، لازم است که روی کامپیوترهای همراه یکی از سیستم‌عامل‌های زیر را نصب کنید:

Windows 10 Enterprise

Windows 10 Education

Windows 8.0 or 8.1 Enterprise

Windows 7 Enterprise

Windows 7 Ultimate

سرورهای DirectAccess یک کارت شبکه یا دو کارت شبکه دریافت می‌کنند؟

یک سوال بزرگ که حتی قبل از نصب نقش Remote Access روی سرور جدید باید به آن پاسخ داده شود این است که چه تعداد کارت شبکه در این سرور نیاز است؟ در این‌جا ما دو روش برای پیاده‌سازی DirectAccess در اختیار داریم.

حالت یک کارت شبکه واحد

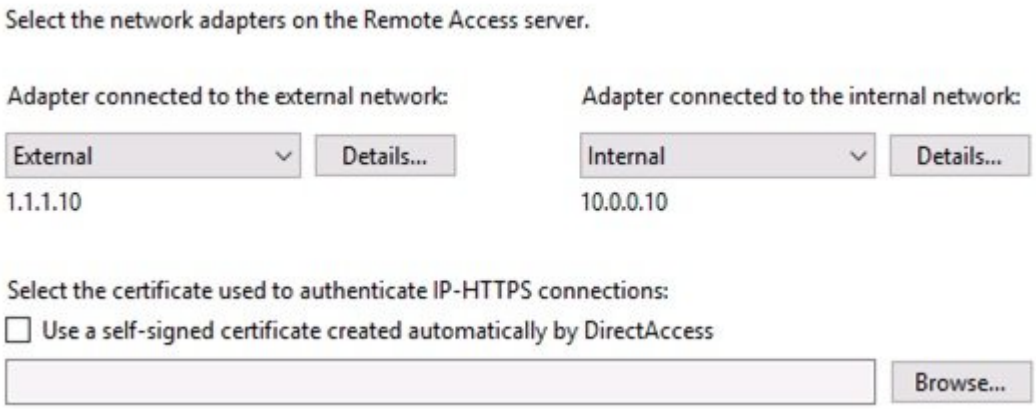
سرور DirectAccess از نصب یک کارت شبکه پشتیبانی می‌کند. در این حالت، معمولا یک اتصال مستقیم به شبکه داخلی خود دارید و به تمام منابع داخلی که کامپیوترهای کلاینت در یک نشست DA به آن نیاز دارند دسترسی خواهید داشت. برای این‌که بتوانید ترافیک اینترنت را به سرور DirectAccess هدایت کنید باید یک آدرس مکانیزم ارتباطی NAT داشته باشید و ترافیک را از یک آدرس آی‌پی عمومی برای هر یک از آدرس‌های آی‌پی داخلی که به سرور DA تخصیص داده‌اید هدایت کنید. بسیاری از مدیران امنیت شبکه این روش را دوست ندارند، زیرا باید یک NAT ایجاد کنند که بدون عبور از هر نوع DMZ مستقیماً به شبکه شرکت وارد می‌شود. بنابر تجربه شخصی باید به شما بگویم که حالت منفرد کارت شبکه همیشه به درستی کار نمی‌کند. امکان استفاده از کارت شبکه واحد قابلیتی است که به تازگی به نسخه‌های اخیر DirectAccess اضافه شده است. بنابراین، توصیه می‌کنم برای آن‌که یک تجربه کاربری خوب با DA داشته باشید از یک روش اصولی‌تر استفاده کنید.

کارت‌های شبکه دوگانه

در این روش، ما دو کارت شبکه در سرور DirectAccess داریم. کارت شبکه داخلی معمولا به‌طور مستقیم به شبکه سازمانی متصل می‌شود و کارت شبکه خارجی بسته به خط‌مشی‌های شبکه ممکن است به شکل‌های مختلفی پیکربندی شود. حالت لبه با دو کارت شبکه راهی است که DirectAccess به بهترین شکل با آن کار می‌کند. همان‌گونه که پیش‌تر اشاره کردیم، پیاده‌سازی ویندوز سرور با چند کارت شبکه به معنای آن است که شما سرورها را به حالت چندکاره (Multihoming) درخواهید آورد و مجبور هستید تنظیمات شبکه را بر این اساس پیکربندی کنید. با داشتن یک Remote Access Server ، کارت شبکه خارجی همواره آن موجودیتی خواهد بود که تنظیمات پیش‌فرض گیت‌وی را دریافت می‌کند، بنابراین باید اطمینان حاصل کنید که از این خط‌مشی پیروی می‌کنید و یک گیت‌وی پیش‌فرض روی کارت شبکه داخلی پیکربندی نمی‌کنید. از طرف دیگر، شما می‌خواهید آدرس‌های سرور سامانه نام دامنه را داخل مشخصات کارت شبکه داخلی پیکربندی کنید، اما نمی‌خواهید سرورهای سامانه نام دامنه را برای کارت شبکه خارجی پیکربندی کنید. از آن‌جایی که این سرور چند کاره است، به منظور اضافه کردن زیرشبکه‌های سازمانی به جدول مسیریابی ویندوز در این سرور پیش از آن‌که ترافیک با موفقیت ارسال و دریافت شود باید برخی دستورات مسیریابی را بسازید. شبکه‌هایی که نیازی نیست مسیرهای ایستا به آن‌ها اضافه کنید، شبکه‌های کوچکی هستند که تمام دستگاه‌های داخلی در یک زیر شبکه قرار دارند. اگر چنین حالتی دارید، دیگر نیازی ندارید تا مسیرهای ایستا را وارد کنید. اما بیشتر شبکه‌های سازمانی دارای زیرشبکه‌های چندگانه هستند. برای اطلاعات بیشتر در این خصوص به بخش multihoming و چگونگی ساخت و پیاده‌سازی دستورات مسیریابی مراجعه کنید.

بیش از دو کارت شبکه

اگر با پیکربندی روترها یا دیوارهای آتش آشنا هستید، از این موضوع اطلاع دارید که می‌توانید کارت‌های شبکه مختلفی روی یک سرور نصب کنید و همه آن‌ها را به زیرشبکه های مختلف وصل کنید. در حالی که دلایل زیادی وجود دارد که باعث می‌شود دسترسی به شبکه را به این شکل شکسته و از مزایاین مختلفی در ارتباط با Remote Access Server استفاده کنیم اما بهتر است زیاد به فکر استفاده از این روش نباشید. پیکربندی خود DirectAccess به گونه‌ای است که تنها قادر به مدیریت دو رابط شبکه مختلف است. همان‌گونه که در تصویر زیر مشاهده می‌کنید در پنجظره تنظیمات شما باید یک کارت شبکه را به عنوان خارجی و دیگری را به عنوان داخلی تعریف کنید. متاسفانه، هیچ کارت شبکه دیگری که در سرور وجود داشته باشد توسط DirectAccess استفاده نخواهد شد. شاید این موضوع در نسخه‌های آینده تغییر کند.



حرکت به سمت NAT یا دوری جستن از NAT؟

حالا که تصمیم گرفتید با دو کارت شبکه در سرور DirectAccess کار خود را انجام دهید، این سوال پیش می‌آید به چه مکانی کارت خارجی را وصل کنیم؟ دو مکان مشترک وجود دارد که این رابط شبکه خارجی می‌تواند به آن متصل شود، اما بسته به نوع انتخاب شما تاثیری که روی محیط DirectAccess می‌گذارد بسیار متفاوت است. قبل از این‌که در مورد قرار دادن مکان واقعی کارت شبکه صحبت کنیم، اجازه دهید درباره چند پروتکل مهم صحبت کنیم، زیرا آن‌ها نقش مهمی در ارتباط با مکانی که کارت شبکه در آن مکان قرار می‌گیرد بازی می‌کنند. هنگامی که لپ‌تاپ DirectAccess شما با سرور DirectAccess ارتباط برقرار می‌کند، این کار را با استفاده از یکی از سه پروتکل تونل‌سازی انتقال IPv6 انجام می‌دهد. این پروتکل‌ها دارای Teredo ، 6to4 و IP-HTTPS هستند. هنگامی که کلاینت DA به تونل‌های DA خود مصتل می‌شود، بسته به نوع اتصال اینترنت فعلی کاربران، به‌طور خودکار انتخاب می‌کند که کدام یک از این پروتکل‌ها بهترین بازدهی را دارند. هر سه پروتکل عملکرد یکسانی را برای یک اتصال DirectAccess ارائه می‌دهند: کار این پروتکل‌ها این است که جریان بسته IPv6 را که از لپ‌تاپ خارج می‌شود را دریافت کرده و آن‌را درون IPv4 محصور می‌کنند تا ترافیک بتواند به شکل موفقیت‌آمیزی مسیر خود در اینترنت مبتنی بر IPv4 را طی کند. هنگامی که بسته‌ها به سرور DirectAccess رسیدند، آن‌ها جدا می‌شوند تا سرور DA بتواند این بسته‌های IPv6 را پردازش کند.

6to4

کلاینت‌های DA تنها زمانی تلاش می‌کنند برای اتصال 6to4 استفاده کنند که لپ‌تاپ راه دور دارای یک آدرس آی‌پی واقعی اینترنتی عمومی باشد. این روزها حالت فوق به سختی به وجود می‌آید، با کمبود آدرس‌های IPv4 اینترنت، به‌طور معمول پروتکل 6to4 توسط هیچ کامپیوتر کلاینت DirectAccess استفاده نمی‌شود. با توجه به این‌که کاربران از اینترنت سلولی استفاده می‌کنند، برای اجتناب از به وجود آمدن مشکلات آداپتور 6to4 روی کامپیوترهای کلاینت غیر فعال می‌شود تا DirectAccess بهترین عملکرد را داشته باشد.

Teredo

هنگامی که کلاینت‌های DA با استفاده از یک آدرس آی‌پی خصوصی از قبیل آدرسی که پشت روتر خانگی یا روتر وایرفای عمومی پنهان شده به اینترنت متصل می‌شوند، آن‌ها با استفاده از پروتکل Teredo سعی در برقراری ارتباط می‌کنند. Teredo از یک جریان UDP برای کپسوله کردن بسته‌های DA استفاده می‌کند و بنابراین تا زمانی‌که اتصال اینترنتی کاربر به UDP 3544 اجازه خروجی ترافیک را می‌دهد، Teredo بطه‌ور کلی متصل است و در نتیجه پروتکل انتقال مورد نظر برای اتصال DirectAccess خواهد بود.

IP-HTTPS

اگر Teredo نتواند اتصال را برقرار کند، مانند مواردی که کاربر از شبکه‌ای استفاده می‌کند که UDP را مسدود می‌کند، اتصال DirectAccess با استفاده از IP-HTTP سرنام (Ip Over HTTPS) برقرار می‌شود. این پروتکل بسته‌های IPv6 را درون سرآیندهای IPv4 کپسوله می‌کند، اما پیش از آن‌که بسته‌ها از طریق اینترنت انتقال پیدا کنند، آن‌ها را درون یک سرآیند HTTP می‌پیچاند و آن‌ها را با پروتکل TLS / SSL رمزگذاری می‌کند. این کار به‌طور موثری باعث می‌شود اتصال DirectAccess از یک جریان SSL استفاده کند، دقیقاً مشابه با زمانی‌که شما از طریق مرورگر خود یک وب‌سایت مبتنی بر HTTPS را مشاهده می‌کنید.

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:

28 مهر 1398

نشانی منبع:
https://www.shabakeh-mag.com/networking-technology/16180/directaccess-%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%D9%87-%DA%86%D9%87-%D9%85%D9%84%D8%B2%D9%88%D9%85%D8%A7%D8%AA%DB%8C-%D9%86%DB%8C%D8%A7%D8%B2-%D8%AF%D8%A7%D8%B1%D8%AF%D8%9F