تکنیک‌ها و روش‌های مختلف پیاده‌سازی DirectAccess در ویندوز سرور 2019

مرسوم است که تیم شبکه بخواهد کارت شبکه خارجی سرور DirectAccess را پشت یک دیوارآتش و درون یک DMZ قرار دهد. این راهکار به معنای ایجاد یک NAT است که ترافیک را به سمت سرور هدایت می‌کند. درست است که راهکار فوق قابل اجرا است و به سرور DirectAccess اجازه می‌دهد از خود به شکل بهتری در زمان اتصال به اینترنت محافظت می‌کند، اما در عمل سرعت افت بسیار محسوسی خواهد داشت. هنگامی که کارت شبکه خارجی سرور DirectAccess خود را مستقیما به اینترنت وصل می‌کنید به خودتان این توانایی را می‌دهید که آدرس‌های آی‌پی عمومی را روی کارت شبکه قرار دهید. با انجام این کار ، شما می‌توانید هر سه پروتکل قبلی تونل‌سازی انتقال را فعال کنید، به گونه‌ای که کامپیوترهای کلاینت DirectAccess بتوانند از بین آن‌ها بهترین نوع اتصال را انتخاب کنند، اما هر یک از روش‌های فوق چه مزایا یا معایبی دارند؟

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

نصب در لبه واقعی - روی اینترنت

هنگامی که کارت شبکه خارجی سرور DirectAccess خود را مستقیما به اینترنت وصل می‌کنید به خودتان این توانایی را می‌دهید که آدرس‌های آی‌پی عمومی را روی کارت شبکه قرار دهید. با انجام این کار ، شما می‌توانید هر سه پروتکل قبلی تونل‌سازی انتقال را فعال کنید، به گونه‌ای که کامپیوترهای کلاینت DirectAccess بتوانند از بین آن‌ها بهترین نوع اتصال را انتخاب کنند. هنگام نصب از طریق روش لبه واقعی، نه تنها یک آدرس اینترنتی بلکه دو آدرس آی‌پی عمومی روی کارت شبکه خارجی خواهید داشت. اطمینان حاصل کنید که آدرس‌های آی‌پی عمومی به صورت متقارن باشند، زیرا یکی از پیش‌نیازهای اصلی Teredo هستند. هنگامی که سرور DirectAccess دارای دو آدرس آی‌پی عمومی متقارن است که به کارت شبکه خارجی اختصاص داده شده، سرور پروتکل Teredo را برای اتصال‌ها فعال می‌کند.

کارت شبکه لزوماً لازم نیست مستقیماً به اینترنت وصل شود تا کار کند. بسته به قابلیت‌های دیوارآتش، ممکن است یک ارتباط DMZ Bridged را زمانی‌که از هیچ ارتباط NAT استفاده نمی‌کنید منتشر کنید. در این زمینه باید از تولیدکننده دیوارآتش سوال کنید که آیا گزینه‌ای در این ارتباط برای سازمان شما دارند یا خیر. در این سناریو، شما هنوز هم می‌توانید آدرس‌های آی‌پی واقعی را در کارت شبکه خارجی پیکربندی کنید، اما برای محافظت و مدیریت ترافیک، استریم‌های داده‌ای ابتدا باید از دیوارآتش عبور کنند.

نصب پشت یک NAT

مرسوم است که تیم شبکه بخواهد کارت شبکه خارجی سرور DirectAccess را پشت یک دیوارآتش و درون یک

DMZ قرار دهد. این راهکار به معنای ایجاد یک NAT است که ترافیک را به سمت سرور هدایت می‌کند. درست است که راهکار فوق قابل اجرا است و به سرور DirectAccess اجازه می‌دهد از خود به شکل بهتری در زمان اتصال به اینترنت محافظت می‌کند، اما در عمل سرعت افت بسیار محسوسی خواهد داشت. وقتی سرور DA را پشت یک NAT نصب می‌کنید پروتکل Teredo دیگر کار نمی‌کند. در حقیقت، ویزاد پیکربندی DirectAccess هنگامی که یک آدرس آی‌پی خصوصی در کارت شبکه خارجی مشخص کرده باشید آن‌را تشخیص می‌دهد و حتا پروتکل Teredo را فعال نمی‌کند. هنگامی که Teredo در دسترس نباشد، تمامی کلاینت‌های DirectAccess شما با استفاده از پروتکل IP-HTTPS متصل می‌شوند. چرا در دسترس نبودن پروتکل Teredo مشکل خاصی ایجاد می‌کند؟ به دلیل این‌که این پروتکل کارآمدتر از IP-HTTPS است. هنگامی که Teredo برای بسته‌ها یک تونل‌زنی انجام می‌دهد به سادگی IPv6 را درون IPv4 کپسوله می‌کند. جریان ترافیک DirectAccess همواره با الگوی IPsec رمزگذاری می‌شوند، بنابراین نیازی به تونل Teredo برای رمزگذاری بیشتر نیست. از طرف دیگر، هنگامی که IP-HTTPS برای بسته‌ها تونل‌زنی می‌کند، جریان ترافیک IPsec که از قبل رمزگذاری شده را دریافت می‌کند و بازهم با استفاده از SSL آن‌ها را رمزگذاری می‌کند. این بدان معنا است که تمام بسته‌هایی که می‌آیند و می‌روند در معرض یک رمزگذاری مضاعف قرار می‌گیرند که باعث افزایش چرخه پردازشی و فعالیت بیش از اندازه پردازنده می‌شوند که اتصال کندتری را به وجود می‌آورند. همچنین بار سخت‌افزاری اضافی روی خود سرور DirectAccess ایجاد می‌شود، زیرا یک پردازش رمزگذاری دوبرابری را انجام می‌دهد.

این مشکل بویژه هنگام اجرای ویندوز 7 روی کامپیوترهای کلاینت باعث بروز مشکل می‌شود، زیرا یک پردازش مضاعف رمزگذاری باعث ایجاد اتصالی به مراتب کندتر برای کاربران می‌شود. DirectAccess هنوز هم خوب کار می‌کند، اما اگر یک لپ‌تاپ متصل به Teredo در کنار یک لپ‌تاپ متصل به IP-HTTPS قرار دهید، تفاوت سرعت بین این دو را مشاهده خواهید کرد.

خوشبختانه، در ویندوز 8 و ویندوز 10 برخی تمهیدات اضافی در نظر گرفته شده تا این اختلاف سرعت کمتر شود. این سیستم‌عامل‌های جدید کلاینتی به اندازه کافی هوشمند هستند تا بتوانند با بخش SSL تونل IP-HTTPS با استفاده از الگوریتم رمزگذاری NULL مذاکره کنند تا IP-HTTPS رمزگذاری دوم را انجام ندهد، اما در مقابل عملکرد IP-HTTPS هم‌طراز با Teredo شود.

با این حال، این تکنیک تنها در ارتباط با سیستم‌عامل‌های کلاینتی جدید کار می‌کند (در ویندوز 7 همیشه IP-HTTPS یک رمزنگاری تکراری رمزگذاری می‌دهد.) و در برخی نیز ممکن است به درستی کار نکند. به عنوان مثال، هنگامی که شما سرور DirectAccess خود را فعال می‌کنید و اتصال شبکه خصوصی مجازی را فراهم می‌کنید یا اگر تصمیم دارید که یک سیستم گذرواژه یکبارمصرف (OTP) را در کنار DirectAccess قررا دهید، الگوریتم NULL غیرفعال می‌شود، زیرا در این مواقع یک خطر امنیتی شکل می‌گیرد و بنابراین حتی کامپیوترهای ویندوز 8 و ویندوز 10 نیز هنگام اتصال از طریق IP-HTTPS رمزگذاری مضاعف را انجام می‌دهند. همان‌گونه که ممکن است حدس زده باشید فعال بودن پروتکل و در دسترس بودن Teredo روی هر کامپیوتری مفید است و در صورت امکان باید از آن استفاده کرد. به‌طور خلاصه، شما مطمئناً می‌توانید کارت شبکه خارجی سرور DirectAccess خود را در پشت یک NAT نصب کنید، اما توجه داشته باشید که تمام کامپیوترهای کلاینت DA با استفاده از پروتکل IP-HTTPS متصل می‌شوند و درک اثر جانبی احتمالی در زمان پیاده‌سازی مهم است.

Network Location Server

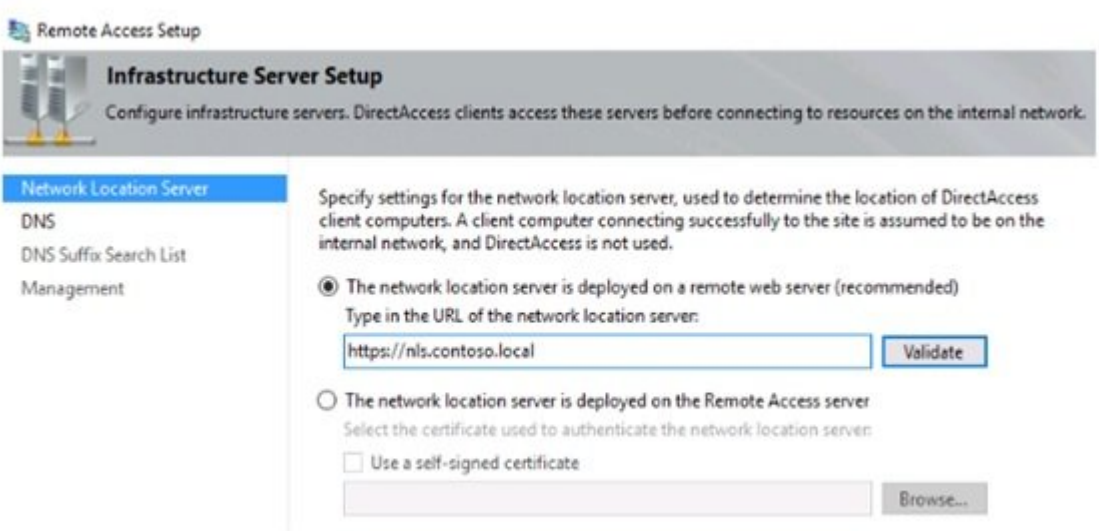
Network Location Server یک مؤلفه اصلی در یک زیرساخت DirectAccess است که حتا در خود سرور DA وجود ندارد یا حداقل اگر شما به درستی تنظیم کنید، نباید این‌گونه باشد. سرور موقعیت‌یابی شبکه (NLS) سرنام Network Location Server به بیان ساده وب‌سایتی است که درون شبکه سازمانی اجرا می‌شود و برای دسترسی به آن نیازی به اینترنت نیست و بهتر است این‌گونه نباشد. NLS به عنوان بخشی از یک مکانیسم تشخیص داخل یا خارج در کامپیوترهای کلاینت DirectAccess بوده و عملکرد آن مشابه با Trusted Detection Network برای Always On VPN است. هر زمان که یک کلاینت DA به یک شبکه وصل می‌شود، به دنبال وب‌سایت NLS است. اگر بتواند سایت را ببیند، می‌داند که شما در داخل شبکه سازمانی هستید و DirectAccess مورد نیاز نیست، بنابراین آن‌را خاموش می‌کند. با این حال، اگر با وب‌سایت NLS ارتباط برقرار نکند، به این معنی است که خارج از شبکه شرکت است، در این حالت مؤلفه‌های DirectAccess خود را روشن می‌کنند.

این پیش شرط به راحتی برآورده می‌شود. تمام کاری که باید انجام دهید این است که یک VM را ایجاد کنید و IIS را

روی آن نصب کنید تا این وب‌سایت جدید را میزبان کند یا حتا می‌توانید یک وب سایت جدید به یک وب سرور موجود در شبکه خود اضافه کنید. در تنظیم وب‌سایت NLS فقط باید به دو مورد دقت کنید. مورد اول این است که باید یک سایت HTTPS داشته باشید، بنابراین به یک گواهینامه SSL نیاز نیاز دارید که در DA از آن استفاده کنید و دوم آن‌که اطمینان حاصل کنید که دسترسی به وب‌سایت از طریق HTTPS انجام می‌شود، همچنین باید اطمینان حاصل کنید که نام DNS که برای تماس با این وب‌سایت استفاده می کنید منحصر به‌فرد باشد. همچنین باید در انتخاب نام برای وب‌سایت NLS دقت کنید، هنگامی که کامپیوترهای کلاینت در خارج از شبکه شرکتی قرار بگیرند، این نام قابل ویرایش نیست. این موضوع به دلیل طراحی است، زیرا شما به شکل صریح و روشن نمی‌خواهید کلاینت‌های DA بتوانند هنگام کار از راه دور با موفقیت به وب‌سایت NLS متصل شوند، به دلیل این‌که در این حالت اتصال DirectAccess غیر فعال می‌شود.

دلیل اینکه نام DNS منحصر به فرد را مطرح می‌کنیم این است که اغلب مدیران DirectAccess را مشاهده می‌کنیم که از یک وب‌سایت داخلی موجود به عنوان وب‌سایت NLS استفاده می‌کنند. به عنوان مثال، اگر https: // intranet به عنوان یک سایت SharePoint در حال اجرا است، به سادگی از این تعریف در تنظیمات DA و به عنوان تعریف سرور NLS استفاده می‌کنند. پس از انجام این‌کار به سرعت متوجه می‌شوند که هیچ کلاینتی که از راه دور کار می‌کند قادر نیست به وب‌سایت https: // intranet دسترسی پیدا کند. این مشکل به دلیل طراحی است، زیرا محیط DA فعلی وب‌سایت intranet شما را سرور NLS می‌داند و زمانی‌که در وضعیت ثابت قرار ندارید، فرآیند resolve را نمی‌توانید انجام دهید. راه حل این مشکل چیست؟ اطمینان حاصل کنید که یک نام جدید DNS را برای استفاده در وب‌سایت NLS انتخاب کرده‌اید. چیزی شبیه به https://nls.contoso.local مناسب است.

مهم‌ترین نکته‌ای که در مورد سرور موقعیت‌یابی شبکه باید به آن دقت کنید این است که باید این وب‌سایت را کاملاً در سرور شبکه و نه در سرور DirectAccess پیاده‌سازی کنید. هنگامی که از ویزاد پیکربندی DA استفاده می‌کنید، روی صفحه مکانی که NLS در آن تعریف می‌شود را مشاهده می‌کنید که توصیه می‌کند NLS را روی یک وب سرور از راه دور مستقر کنید، اما این امکان را نیز به شما می‌دهد که وب سایت NLS را به صورت مستقیم در سمت خود و روی خود سرور DirectAccess قرار دهید. اما بهتر است این کار را نکنید! هنگامی که NLS را در سرور DA میزبانی می‌کنید، پارامترهای مختلفی وجود دارند که ممکن است اشتباه شوند. اجرای NLS روی سرور DA در آینده محدودیت‌هایی برای DirectAccess به وجود می‌آورد، زیرا برخی از تنظیمات پیشرفته DA وجود دارند که به آن‌ها نیاز دارید و ممکن است بخواهید یکسری تنظیمات NLS که درون سرور DA قرار دارند حذف کنید، بنابراین بهتر است اولین باری که آن‌را تنظیم می‌کنید به این موارد دقت کنید. تغییر وب سایت NLS پس از اجرای DA کار چندان راحتی نیست و اغلب با ترفندهای خاصی تغییرات در آن اعمال می‌شوند. من به شرکت‌های مختلفی کمک کردم تا وب‌سایت NLS خود را بعد از این‌که متوجه شدند که نمی‌توانند NLS را در سرور DA میزبانی کنند انتقال دهند، به ویژه زمانی که برای رشد کسب‌وکار یا افزونگی، مجبور بودند یك سرور DirectAccess دوم اضافه کنند. در تصویر زیر بخشی از ویزاد پیکربندی DA جایی که مکان NLS انتخاب شده است 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:

01 آبان 1398

نشانی منبع:
https://www.shabakeh-mag.com/networking-technology/16182/%D8%AA%DA%A9%D9%86%DB%8C%DA%A9%E2%80%8C%D9%87%D8%A7-%D9%88-%D8%B1%D9%88%D8%B4%E2%80%8C%D9%87%D8%A7%DB%8C-%D9%85%D8%AE%D8%AA%D9%84%D9%81-%D9%BE%DB%8C%D8%A7%D8%AF%D9%87%E2%80%8C%D8%B3%D8%A7%D8%B2%DB%8C-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