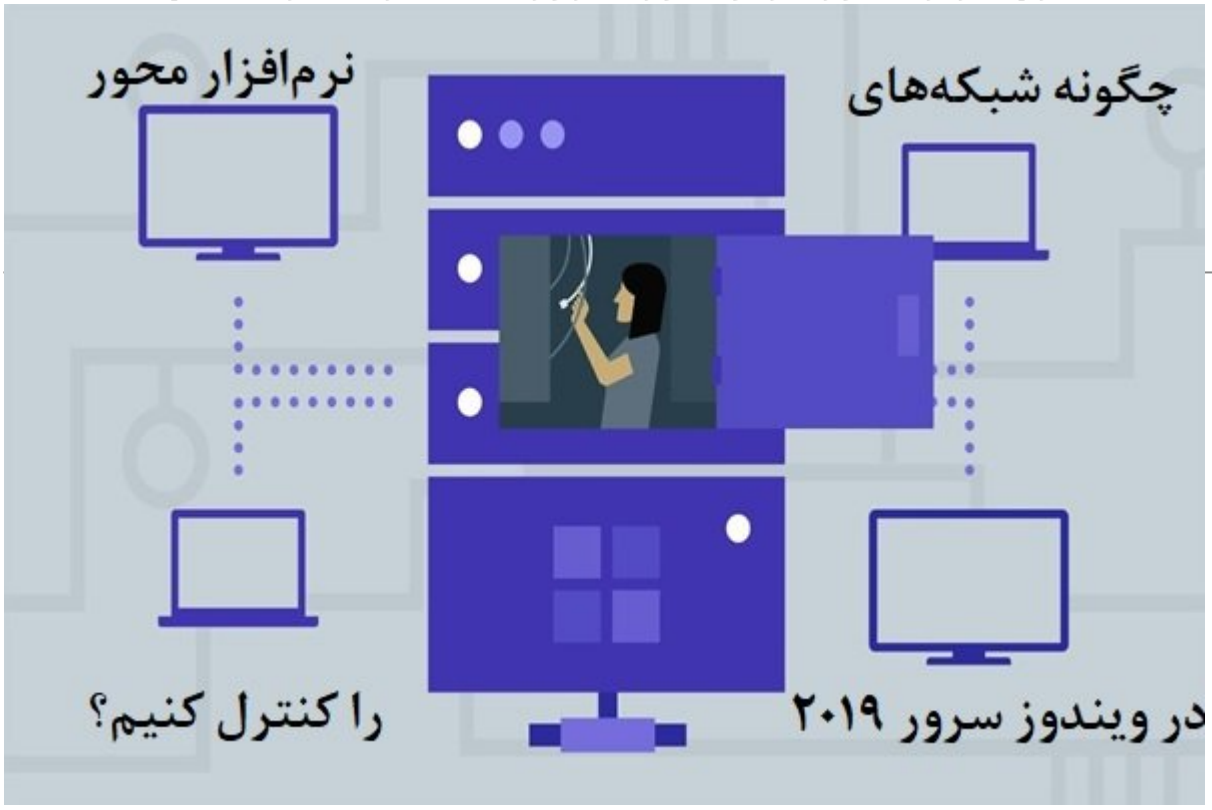
چگونه شبکه‌های نرم‌افزار محور در ویندوز سرور 2019 را کنترل کنیم؟



هنگامی که مجازی‌سازی شبکه را با استفاده از Hyper-V درون شبکه شرکتی خود اعمال می‌کنید و از دغدغه تفکیک شبکه‌های فیزیکی و مجازی آسوده خاطر می‌شوید، به احتمال زیاد دوست دارید درباره قابلیت‌هایی که اجازه می‌دهند با سرویس‌های ابری شرکت ارائه دهنده خدمات تعامل بهتری داشته باشید اطلاعاتی به دست آورید. همچنین باید از فناوری محصورسازی/کپسوله مسیریابی عمومی (GRE) سرنام Encapsulation Generic Routing که یک پروتکل تونل‌زنی است، برای پیاده‌سازی موفقیت‌آمیز مجازی‌سازی شبکه استفاده کنید.

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

System Center Virtual Machine Manager

Microsoft System Center یک مولفه اصلی برای ایجاد مدلی از شبکه نرم‌افزارمحوری است که قصد ساخت آن‌را دارید، به ویژه آن‌که مولفه Virtual Machine Manager سرنام (VMM) نیز در آن قرار دارد. توانایی اخذ آدرس‌های آی‌پی و انتقال آن‌ها به هر نقطه از جهان که نیاز دارد هماهنگ با دستگاه تحت شبکه‌ای که در اختیار دارید از قابلیت‌های VMM است. VMM مولفه‌ای است که اجازه می‌دهد خط اتصالی با مرکز مدیریت خود تعریف کنید و به پیکربندی ماشین‌های مجازی بپردازید. System Center مبحث گسترده‌ای است و از بخش‌های مختلفی تشکیل شده است که امکان پرداختن به تمامی موارد در این سریس آموزشی وجود دارد، بنابراین پیشنهاد می‌کنیم برای آشنایی بیشتر با VMM به آدرس **system-center** مراجعه کنید.

کنترل‌کننده شبکه

کنترلر شبکه مایکروسافت نقشی است که اولین بار همراه با ویندوز سرور 2016 معرفی شد و همان‌گونه که از نامش پیدا است برای کنترل منابع شبکه در داخل سازمان استفاده می‌شود. در بیشتر موارد، این مولفه در تعامل با VMM کار می‌کند تا پیکربندی شبکه تا حد امکان متمرکز و یکپارچه شود. کنترل‌کننده شبکه (Network Controller) یک نقش مستقل است و می‌تواند روی سرور 2016 یا 2019 نصب شود و سپس به‌طور مستقیم و بدون VMM استفاده شود. ارتباط مستقیم با کنترل‌کننده شبکه از طریق یک واسط برنامه‌نویسی که درون محیط پاورشل در دسترس است امکان‌پذیر است.، اما از طریق به‌کارگیری یک رابط گرافیکی که اجازه می‌دهد شبکه‌های جدید را پیکربندی کنید، شبکه‌ها و دستگاه‌های موجود را رصد می‌کنید یا در مدل‌سازی مجازی مشکلات را برطرف می‌کنید، کار ساده‌تر می‌شود. رابط گرافیکی که می‌توان از آن استفاده کرد System Center VMM نام دارد. کنترلر شبکه می‌تواند برای پیکربندی جنبه‌های مختلف شبکه‌های مجازی و فیزیکی استفاده شود. شما می‌توانید زیرشبکه‌های آی‌پی و آدرس‌ها، پیکربندی VLANها در سوئیچ‌های Hyper-V را با استفاده از این ابزار پیکربندی کنید و حتا می‌توانید از

ابزار فوق برای پیکربندی کارت‌های شبکه درون ماشین‌های مجازی نیز استفاده کنید. کنترلر شبکه همچنین به شما اجازه می‌دهد قواعدی از نوع فهرست کنترل دسترسی (ACL) سرنام Access Control List را در سوئیچ Hyper-V ایجاد و مدیریت کنید تا امکان پیاده‌سازی راه‌حل دیوارآتش در این سطح میسر شود بدون این‌که نیازی به پیکربندی دیوارهای آتش محلی در خود ماشین‌های مجازی یا داشتن دیوارهای آتش اختصاصی ضرورتی داشته باشد. کنترل‌کننده شبکه حتا برای پیکربندی تعادل بار و فراهم آوردن دسترسی VPN از طریق سرورهای RRAS نیز قابل استفاده است.

محصورسازی مسیریابی عمومی

محصورسازی/کپسوله مسیریابی عمومی (GRE) سرنام Encapsulation Generic Routing تنها یک پروتکل تونل‌زنی است، اما برای آن‌که مجازی‌سازی شبکه با موفقیت به سرانجام برسد ضروری است. پیش از این، در مورد جابه‌جایی زیرشبکه‌های آی‌پی و در مورد چگونگی نشستن شبکه‌های مجازی در بالای شبکه‌های فیزیکی بدون در نظر گرفتن اطمینان از سازگاری پیکربندی آی‌پی آن‌ها با شما صحبت کردیم، اکنون این نکته را بدانید که تمامی این قابلیت‌ها در کرنل GRE قرار دارند. وقتی شبکه فیزیکی شما در حال اجرا است x.192.168.0، اما در نظر دارید میزبان برخی از ماشین‌های مجازی روی زیرشبکه در یک مرکزداده باشید، این شانس را دارید تا بدون مشکل یک شبکه مجازی با x.10.10.10 ایجاد کنید، اما این ترافیک باید قادر باشد از شبکه فیزیکی 192.168 عبور کند تا بتواند کار کند. اینجا است که مبحث محصورسازی مسیریابی به میدان وارد می‌شود. تمام بسته‌های شبکه x.10.10.10 قبل از انتقال به شبکه فیزیکی x.192.168.0 کپسوله می‌شوند.

در این‌جا دو پروتکل خاص محصورسازی مسیریابی وجود دارد که توسط محیط مجازی‌سازی شبکه Hyper-V مایکروسافت پشتیبانی می‌شوند. در نسخه‌های قبلی سیستم‌عامل ویندوز سرور فقط می‌توانستیم روی محصورسازی مسیریابی عموم شبکه مجازی‌سازی (NVGRE) سرنام Network Virtualization using Generic Routing Encapsulation تمرکز کنیم، زیرا تنها پروتکلی بود که توسط ویندوز در مجازی‌سازی شبکه پشتیبانی می‌شد. با این حال، پروتکل دیگری وجود دارد به‌نام شبکه محلی توسعه یافته مجازی (VXLAN) سرنام Virtual Extensible Local Area Network ، که مدت مدیدی است وجود دارد در اختیار ما قرار دارد که بسیاری از سوییچ‌های شبکه – به ویژه سیسکو - که ممکن است در محیط کار خود داشته باشید از آن پشتیبانی می‌کنند. برای زیرساخت‌های مجازی‌سازی شبکه مدرن امروزی که توسط ویندوز سرور 2016 و ویندوز سرور 2019 ایجاد می‌شوند، مدیران شبکه می‌توانند از NVGRE یا VXLAN استفاده کنند که انتخاب گزینه مناسب به نوع فعالیت‌های کسب‌وکار بستگی دارد.

شما نیازی ندارید درباره عملکرد پروتکل‌های GRE و این‌که چگونه برای شما کار می‌کنند اطلاعات دقیقی کسب کنید، زیرا آن‌ها توسط ابزارهای مدیریتی که در پشته مجازی‌سازی Hyper-V Network قرار دارند پیکربندی می‌شوند. اما درک کلی محیطی که شبکه‌های مجازی از طریق GRE پیاده‌سازی و مدیریت می‌شوند، حائز اهمیت است.

Microsoft Azure Virtual Network

هنگامی که مجازی‌سازی شبکه را با استفاده از Hyper-V درون شبکه شرکتی خود اعمال می‌کنید و از دغدغه تفکیک شبکه‌های فیزیکی و مجازی آسوده خاطر می‌شوید، به احتمال زیاد دوست دارید درباره قابلیت‌هایی که اجازه می‌دهند با سرویس‌های ابری شرکت ارائه دهند خدمات تعامل بهتری داشته باشید اطلاعاتی به دست آورید. هنگامی‌که از مایکروسافت آژور (Microsoft Azure) به عنوان ارائه‌دهنده خدمات ابری خود استفاده می‌کنید، قادر هستید یک محیط ابری ترکیبی ایجاد کنید که شبیه به پلی شبکه‌های فیزیکی درون سازمانی را با شبکه‌ای مجازی راه دور میزبانی شده توسط آژور به یکدیگر متصل می‌کند. شبکه مجازی آژور مؤلفه‌ای در آژور است که به شما اجازه می‌دهد آدرس آی‌پی و زیرشبکه‌های شخصی خود را وارد ابر کنید. برای کسب اطلاعات بیشتر به‌کارگیری آزمایشی آژور به لینک **Virtual Network** مراجعه کنید.

Windows Server Gateway / SDN Gateway

زمانی‌که در حال کار با شبکه‌های فیزیکی و شبکه‌های مجازی هستید که در محیط‌های ابری ذخیره شده‌اند به برخی از مؤلفه‌ها برای بستن شکاف‌های موجود نیاز دارید تا این شبکه‌ها بتوانند با یکدیگر ارتباط برقرار کرده و تبادل اطلاعات بپردازند. درست در این نقطه است که ویژگی Windows Server Gateway (که به آن SDN Gateway نیز گفته می‌شود) به میدان وارد می‌شود. Windows Server Gateway اصطلاح جدید است. این موقله قبلا به نام

Hyper-V Network Virtualization Gateway وجود داشت و ممکن است مستندات منتشر شده در ارتباط با این مولفه را مشاهده کنید. Windows Server Gateway بسیار ساده است. مولفه فوق ارتباط بین شبکه‌های مجازی و فیزیکی را برقرار می‌کند. این شبکه‌های مجازی را می‌توان در محیط محلی یا در فضای ابری میزبانی کرد. در هر صورت، وقتی می‌خواهید شبکه‌ها را وصل کنید باید از Windows Server Gateway استفاده کنید. هنگامی که در حال ساخت پلی میزان محیط سازمان و ابر هستید، ارائه‌دهنده خدمات ابری شما از دروازه سمت خود استفاده می‌کند که می‌توانید از طریق یک تونل VPN از شبکه فیزیکی به آن وارد شوید.

Windows Server Gateway به‌طور کلی یک ماشین مجازی است که مولفه مجازی‌سازی شبکه Hyper-V یکپارچه شده است. WSG یک دروازه منفرد برای مسیریابی ترافیک است که کلاینت‌ها، مشتریان یا واحدهای مختلف از آن استفاده می‌کنند. حتی اگر این مشتریان شبکه‌هایی از هم جدا داشته باشند که باید ترافیک مشتریان از یکدیگر جدا شود، ارائه‌دهنده ابر - عمومی یا خصوصی - هنوز هم می‌تواند از یک دروازه واحد برای مدیریت این ترافیک استفاده کند، زیرا دروازه‌ها این پتانسیل را دارند تا استریم ترافیک را به شکل دقیقی از یکدیگر متمایز کنند. ویژگی Windows Server Gateway در ویندوز سرور 2016 نیز وجود داشت، اما زمانی‌که به شکل رسمی از سوی مایکروسافت عرضه شد، برخی از محدودیت‌های عملکردی آن که باعث افزایش توان ترافیک شبکه شده و عملکردهای شبکه را کاهش می‌داد به سرعت خود را نشان دادند. این مشکلات در ویندوز سرور 2019 برطرف شدند و در نتیجه می‌توانید ترافیک تعداد بیشتری از کلاینت‌ها را از طریق یک دروازه واحد مدیریت کنید.

رمزگذاری شبکه مجازی

تیم‌های امنیتی به‌طور مداوم از بابت به خطر افتادن رمزگذاری داده‌ها نگران هستند. آن‌ها نگران این مسئله هستند که آیا داده‌های ذخیره شده یا در حال انتقال در امنیت کامل قرار دارند و مصون از دستکار هستند یا باید تهمیدات سخت‌گیرانه‌ای روی آن‌ها اعمال کرد. قبل از **ویندوز سرور 2019**، ترافیک درون شبکه داخلی عموما توسط برنامه‌های کاربردی و نه شبکه انجام می‌شد. اگر نرم‌افزار شما توانایی رمزگذاری ترافیک را در حالی که بین کلاینت و سرور اطلاعاتی در حال مبادله بود انجام می‌داد یا بین سرور برنامه و سرور پایگاه داده مکانیزم رمزنگاری وجود داشت همه چیز در حالت عالی بود. اگر برنامه شما قابلیت رمزگذاری بومی را نداشت، به احتمال زیاد ارتباطات از طریق آن برنامه کاربردی به شکل یک متن ساده میان کلاینت و سرور انجام می‌شد. حتی برای برنامه‌هایی که رمزگذاری را انجام می‌داند، الگوریتم‌ها و سایفرهای رمزنگاری گاهی اوقات کرک می‌شدند و امنیت به خطر می‌افتاد که خود زمینه‌ساز بروز آسیب‌پذیری‌های جدیدی می‌شد. بهتر است روشی که برنامه شما برای رمزنگاری ترافیک استفاده می‌کند را بررسی کنید و مطمئن شوید از روش‌های رمزنگاری جدید استفاده می‌کند.

خوشبختانه **ویندوز سرور 2019** قابلیت جدیدی برای شبکه‌های نرم‌افزار محور ارائه کرد. این قابلیت جدید رمزگذاری شبکه مجازی نام دارد و دقیقا همان کاری را انجام می‌دهد که از نامش می‌توان حدس زد. هنگامی که ترافیک بین ماشین‌های مجازی و بین سرورهای Hyper-V (در همان شبکه) در حال مبادله است، این امکان وجود دارد تا کل زیرشبکه‌ها را برای رمزگذاری پرچم‌گذاری کرد، به این معنی که تمام ترافیک‌های موجود در آن زیر شبکه‌ها به‌طور خودکار در سطح شبکه‌های مجازی رمزگذاری می‌شوند. سرورهای ماشین مجازی و برنامه‌های کاربردی شما که در آن سرورها اجرا می‌شوند برای استفاده از این رمزگذاری نباید پیکربندی شده یا تغییر کنند، زیرا این راهکار درون شبکه اعمال می‌شود و به‌طور خودکار تمام ترافیکی که در آن شبکه جریان دارد را رمزگذاری می‌کند.

همراه با ارائه Server 2019 SDN، هر زیرشبکه در یک شبکه مجازی می‌تواند با مشخص کردن یک گواهی برای استفاده در رمزگذاری پرچم‌گذاری شود. اگر در آینده مشکلی رخ دهد شبیه به این‌که سناریوی فعلی رمزگذاری از بین رفته است یا ایمن نیست، این امکان وجود دارد تا SDN fabric را با استانداردهای جدید رمزگذاری به‌روز کرد و آن زیرشبکه‌ها را با استفاده از روش‌های جدید رمزگذاری ایمن کرد، بدون آن‌که نیازی باشد در برنامه کاربری یا ماشین‌های مجازی خود تغییراتی اعمال کنید. اگر از شبکه‌های SDN و شبکه‌های مجازی در محیط سازمانی استفاده می‌کنید، فعال کردن رمزگذاری در زیرشبکه‌ها اجتناب‌ناپذیر است.

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:

15 مهر 1398

نشانی منبع:
https://www.shabakeh-mag.com/networking-technology/16115/%DA%86%DA%AF%D9%88%D9%86%D9%87-%D8%B4%D8%A8%DA%A9%D9%87%E2%80%8C%D9%87%D8%A7%DB%8C-%D9%86%D8%B1%D9%85%E2%80%8C%D8%A7%D9%81%D8%B2%D8%A7%D8%B1-%D9%85%D8%AD%D9%88%D8%B1-%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%B1%D8%A7-%DA%A9%D9%86%D8%AA%D8%B1%D9%84-%DA%A9%D9%86%DB%8C%D9%85%D8%9F