چگونه ارتباطات شبکه درون سازمانی را در ویندوز سرور 2019 رمزگذاری کنیم؟

بیشتر فناوری‌های رمزگذاری که به شکل توکار درون سیستم‌عامل‌ها قرار می‌گیرند با هدف رمزنگاری داده‌ها ساخته می‌شوند، اما در ارتباط با داده‌های در حال انتقال چه باید کرد؟ آیا راهکاری برای ایمن‌سازی ترافیک شبکه درون سازمانی وجود دارد؟ پاسخ مثبت است. IPsec مجموعه‌ای از پروتکل‌ها است که می‌تواند برای تأیید صحت داده‌ها و رمزگذاری بسته‌هایی که قرار است در یک شبکه انتقال پیدا کنند استفاده شود.

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

ماشین‌های مجازی محافظت شده

به‌کارگیری بیت‌لاکر BitLocker و TPMهای مجازی با هدف رمزگذاری و محافظت از فایل‌های مربوط به هارددیسک‌های مجازی مفهومی به‌نام ماشین‌های مجازی محافظت شده (Shielded VMs) را پدید آورده است. ماشین‌های مجازی محافظت شده اولین بار همراه با ویندوز سرور 2016 معرفی شدند و در سرور 2019 بهبود پیدا کردند. در شماره‌های آینده بیشتر در مورد ماشین‌های مجازی صحبت خواهیم کرد، در این‌جا به این دلیل که بحث رمزگذاری را داریم اشاره‌ای به این مفهوم داشتیم.

شبکه‌های مجازی رمزگذاری شده

ایده بدی نیست که بتوانیم شبکه‌ها را توسط یک رابط گرافیکی مدیریتی پیکربندی، کنترل و اداره کنیم. کارشناسان حرفه‌ای از انعطاف‌پذیری شبکه‌ها به منظور انتقال سرورها و بار کاری از یک زیر شبکه به زیرشبکه دیگری، بدون نیاز به تغییر آدرس آی‌پی یا مسیریابی در آن سرورها استفاده می‌کنند. برای آن‌که بتوانیم از چنین پتانسیل بالایی استفاده کنیم در اولین گام باید به جای آن‌که به سراغ پیکربندی و رمزگذاری درون خود سرورها برویم به فکر رمزگذاری خودکار تمام ترافیکی باشیم که میان سرورها در جریان است. بله این قابلیت در اختیار شما قرار دارد. با استفاده از شبکه‌های نرم‌افزار محور (SDN) و قابلیت جدیدی به‌نام شبکه‌های مجازی رمزگذاری شده تمامی نکاتی که به آن‌ها اشاره کردیم در دسترس‌مان قرار دارند. قبلا در مورد SDN و قابلیت جدید آن برای ایجاد و رمزگذاری خودکار شبکه‌های مجازی موجود در ماشین‌های مجازی Hyper-V و سرورهای میزبان Hyper-V اطلاعاتی به شما دادیم. اگر این نکات را فراموش کرده‌اید، بهتر است به فصل‌های قبل‌تر بازگردید و این فناوری را دومرتبه مرور کنید.

سیستم رمزگذاری فایل

سیستم رمزگذاری فایل (EFS) یکی از مولفه‌های ویندوز است که روی هر دو سیستم‌عامل کلاینت و سرور این شرکت وجود دارد. در حالی که بیت‌لاکر وظیفه تأمین امنیت یک دیسک یا ولوم کامل را دارد، EFS کمی خاص‌تر عمل می‌کند. هنگامی که تصمیم می‌گیرد فقط اسناد یا پوشه‌های خاصی را رمزگذاری کنید، مولفه فوق ابزاری است که به آن نیاز دارید. هنگامی که برای رمزگذاری فایل‌ها تصمیم می‌گیرد از EFS استفاده کنید باید به این نکته مهم دقت کنید که ویندوز نیاز به استفاده از یک گواهی کاربر به عنوان بخشی از فرآیند رمزگذاری / رمزگشایی دارد و بنابراین در دسترس بودن یک زیرساخت کلید عمومی (PKI) داخلی برای پیاده‌سازی درست این موضوع مهم است. به این نکته دقت کنید که کلیدهای تأیید اعتبار با گذرواژه کاربر عجین هستند، بنابراین اگر یک حساب کاربری هک شود ممکن است ویژگی EFS کارایی خود را از دست بدهد. بیشتر شرکت‌ها از EFS استفاده نمی‌کنند، زیرا فرآیند رمزنگاری فایل‌ها را به کاربران محول می‌کنند. درست است که بیت‌لاکر قابلیت خوبی دارد، اما فراموش نکنید که EFS هنوز هم مکانیزم قدرتمندی برای جلوگیری از دسترسی غیرمجاز به اسناد است.

IPsec

بیشتر فناوری‌های رمزگذاری که به شکل توکار درون سیستم‌عامل‌ها قرار می‌گیرند با هدف رمزنگاری داده‌ها ساخته می‌شوند، اما در ارتباط با داده‌های در حال انتقال چه باید کرد؟ ما در مورد به‌کارگیری پروتکل SSL در وب‌سایت‌های HTTPS به عنوان راهکاری برای رمزگذاری داده‌های مرورگر وب که میان کلاینت‌ها و سرورها انتقال پیدا می‌کنند، صحبت کردیم، اما در ارتباط با داده‌هایی که از طریق یک مرورگر وب انتقال پیدا نمی‌کنند چه باید کرد؟ تهدیدات همیشه از جانب اینترنت نیستند و در برخی موارد ما باید به فکر محافظت از ترافیکی باشیم که از یک نقطه به نقطه‌ای دیگر در شبکه سازمانی انتقال پیدا می‌کند. آیا راهکاری برای ایمن‌سازی ترافیک شبکه درون سازمانی وجود دارد؟ پاسخ مثبت است. IPsec مجموعه‌ای از پروتکل‌ها است که می‌تواند برای تأیید صحت داده‌ها و رمزگذاری بسته‌هایی که قرار است در یک شبکه انتقال پیدا کنند استفاده شود. IPsec یک فناوری منحصر به مایکروسافت نیست، اما مکانیسم‌های مختلفی در ویندوز سرور 2019 وجود دارد که اجازه می‌دهند از IPsec برای تامین امنیت داده‌هایی که قرار است میان دو ماشین مبادله شوند استفاده کنید. ساده‌ترین مکانی که اجازه می‌دهد در ویندوز سرور 2019 با IPsec ارتباط برقرار کنید، زمانی است که از نقش Remote Access استفاده می‌کنید. زمانی‌که در حال پیکربندی شبکه خصوصی مجازی روی سرور RA هستید، پروتکل‌های ارتباطی مختلفی دارید که کلاینت‌های شبکه خصوصی مجازی می‌توانند از آن‌ها برای اتصال به سرور شبکه خصوصی مجازی استفاده کنند. در میان این پروتکل‌های فهرست شده، تونل IPsec موسوم به IKEv2 نیز وجود دارد. دومین فناوری دسترسی از راه دوری که از IPsec استفاده می‌کند DirectAccess است. زمانی‌که یک ارتباط مبتنی بر DirectAccess را در شبکه خود منتشر می‌کنید، هر زمان یک کامپیوتر کلاینت تونل Direct Access مبتنی بر اینترنت را روی سرور DirectAccess ایجاد کند، تونل ایجاد شده توسط IPsec محافظت می‌شود. شما از Remote Access Management Console برای استقرار شبکه خصوصی مجازی و DirectAccess استفاده می‌کنید و خوشبختانه کنسول فوق به اندازه‌ای هوشمند است که می‌داند هر هر ماهیت مبتنی با احراز هویت IPsec باید در شبکه رمزگذاری شود. این فرآیند در شرایطی انجام می‌شود که کاربر حتا از این موضوع مطلع نمی‌شود که در زمان برقراری یک ارتباط از راه دور پروتکل IPsec ارتباط را رمزگذاری می‌کند. اما در ارتباط با ترافیک درون سازمانی و شبکه چه باید کرد؟ زمانی که درباره شبکه خصوصی مجازی یا DirectAccess صحبت می‌کنیم درباره ترافیکی صحبت می‌کنیم که بر پایه اینترنت مبادله می‌شود. اگر مجبور شویم ترافیک میان دو سرور مختلف در یک شبکه یکسان را رمزگذاری کنیم چه کاری باید انجام دهیم؟ یا زمانی که قرار است ترافیک از سمت کامپیوترهای کلاینت به سمت سرورهای محلی آن‌ها ارسال شود چه کاری باید انجام داد؟ این درست همان نقطه‌ای است که تنظیمات خط‌مشی IPsec به میدان وارد می‌شود و به شما اجازه می‌دهد ترافیکی که قرار است در شبکه سازمانی انتقال پیدا کند را توسط IPsec رمزگذاری کنید.

پیکربندی IPsec

در محیط سیستم‌عامل ویندوز دو مکان مختلف برای پیکربندی IPsec وجود دارد. شما می‌توانید از راهکار سنتی IPsec Security Policy snap-in برای پیکربندی تنظیمات استفاده کنید. اگر تمامی سامانه‌ها از سیستم‌های جدید استفاد می‌کنند، بهتر از است Windows Defender Firewall with Advanced Security برای پیکربندی خط‌مشی‌های IPsec استفاده کنید. WFAS یکی از انعطاف‌پذیرترین راه‌حل‌های موجود است. در اولین گام نگاهی به کنسول خط‌مشی IPsec داشته باشید. کار را از این نقطه شروع می‌کنیم، زیرا گزینه‌های مختلف این بخش به ما اجازه می‌دهند تا خط پایه IPsec در تعامل با دو نقطه پایانی را ترسیم کنیم. در این‌جا سه خط‌مشی مختلف IPsec برای تخصیص به ماشین‌هایی که در این کنسول تعیین خواهیم کرد وجود دارد. اجازه دهید به‌طور اجمالی هر یک از

آن‌ها را بررسی کنیم، زیرا نام خط‌مشی‌ها زیاد روشن نیست و ممکن است شما را به اشتباه اندازند. آشنایی دقیق با این گزینه‌ها به شما کمک می‌کنند با نحوه کار تنظیمات در WFAS به خوبی آشنا شوید.

Server Policy

خط‌مشی سرور بهتر بود به خط‌مشی Requestor تغییر نام پیدا می‌کرد، زیرا عملکرد آن دقیقا درخواستی است. زمانی‌که یک کامپیوتر یا سرور درخواست برقراری ارتباط با یک کامپیوتر یا سروری در شبکه دیگری را ارائه می‌کند، به دنبال برقراری ارتباط با یک شبکه برون سازمانی است. در ارتباط با چنین درخواست‌هایی خط‌مشی IPsec Server به خوبی قابل استفاده است. زمانی که این خط‌مشی اعمال شود، خط‌مشی سرور اعلام می‌دارد که کامپیوتر یا سرور نیازمند رمزگذاری IPsec برای برقراری یک ارتباط رمزگذاری شده با ماشین یا سروری هستند که در راه دور قرار دارد. اگر سیستم راه‌دور از IPsec پشتیبانی کند، تونل IPsec برای محافظت از ترافیکی که میان دو ماشین در جریان است ساخته می‌شود. اگر ماشین مقابل از IPsec پشتیبانی نکند، بازهم ارتباط با موفقیت ساخته می‌شود، اما فاقد رمزگذاری است.

Secure Server Policy

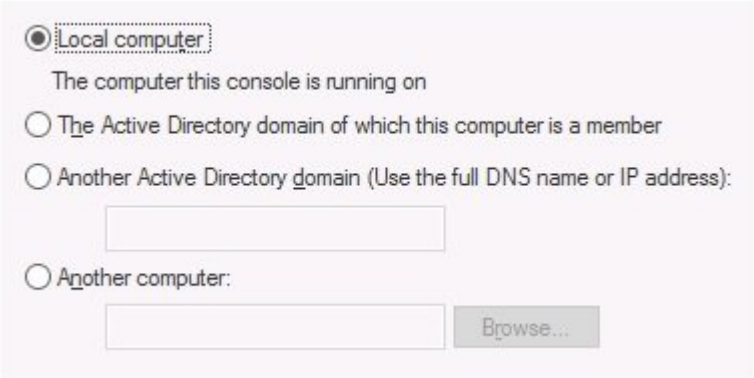
تفاوت خط‌مشی فوق با خط‌مشی Server Policy در این است که خط‌مشی سرور ایمن تنها زمانی اجازه برقراری ارتباط با شبکه را می‌دهد که رمزگذاری IPsec در دسترس باشد. خط‌مشی عادی سرور اگر IPsec در دسترس بود، فرآیند رمزگذاری را انجام می‌دهد، اما در هر صورت ارتباط را برقرار می‌کند، حتا اگر رمزگذاری انجام نشده باشد. در خط‌مشی سرور ایمن اگر IPsec موفق نشود ارتباط میان دو ماشین را رمزگذاری کند، مانع برقراری ارتباط می‌شود.

Client Policy

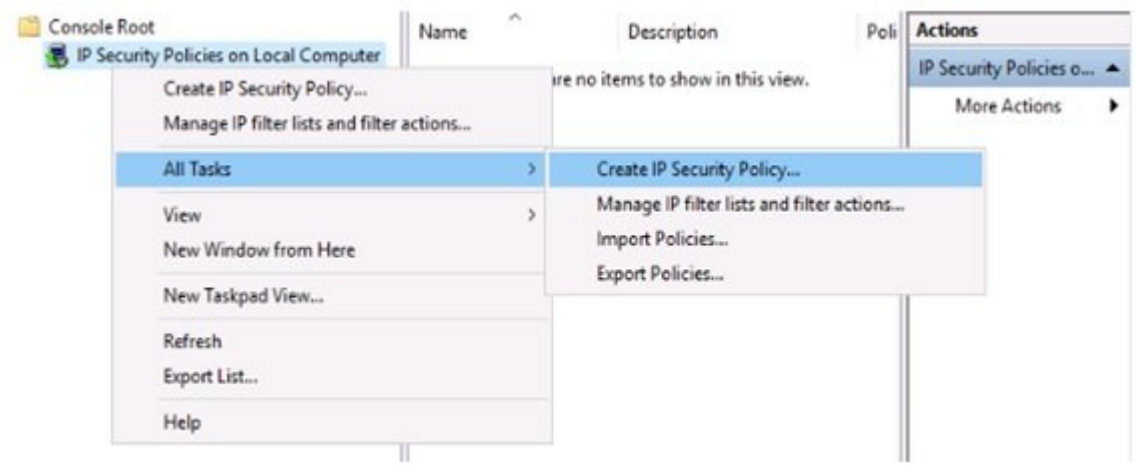
خط‌مشی Client بهتر بود به خط‌مشی Response تغییر نام می‌داد، زیرا در طرف دیگر ارتباط اعمال می‌شود. برای خط‌مشی کلاینت اهمیتی ندارد که درخواست نشست IPsec چگونه ایجاد می‌شود، برای کلاینت تنها دریافت (receiving) مهم است. زمانی‌که یک کامپیوتر تحت شبکه درخواست برقراری ارتباط با یک سرور را ارسال می‌کند و روی سرور خط‌مشی Server یا Secure Server نصب شده باشد، سرور درخواست IPsec می‌کند، در ادامه سرور سعی می‌کند خط‌مشی Client را به درخواست تخصیص دهد تا تونل IPsec ایجاد شود. خط‌مشی کلاینت با اجازه دادن به رمزگذاری نشست به این درخواست پاسخ می‌دهد.

IPsec Security Policy snap-in

کنسول اصلی برای مدیریت تنظیمات IPsec از طریق MMC در دسترس قرار دارد. MMC را باز کنید و سپس ویژگی IP Security Policy Management را به آن اضافه کنید. زمانی که ابزار فوق را اضافه می‌کنید پیغامی ظاهر شده و اعلام می‌دارد که شما می‌توانید هر یک از دو حالت خط‌مشی محلی IPsec ماشین که به آن وارد شده‌اید را مشاهده کنید یا می‌توانید خط‌مشی IPsec مربوط به خود دامنه را مشاهده کنید. در این‌جا گزینه Local computer را انتخاب کنید تا به کنسول مربوطه وارد شوید.

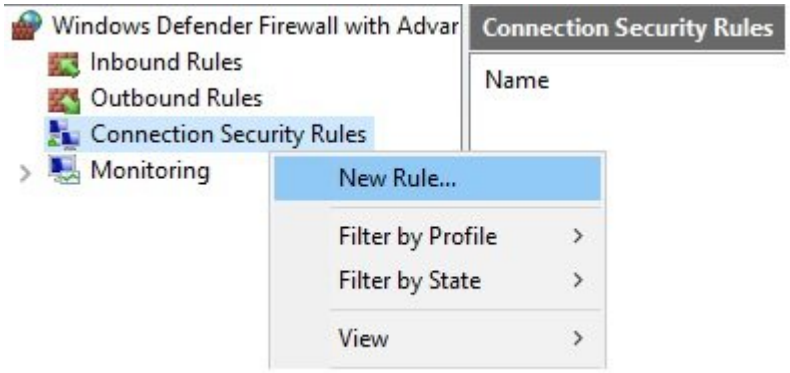


زمانی که به کنسول مربوطه وارد شدید، شما می‌توانید خط‌مشی‌های موجود IPsec که ممکن است نصب شده باشند را مشاهده کنید یا می‌توانید خط‌مشی خودتان را با استفاده از گزینه Create IP Security Policy ایجاد کنید. برای این منظور روی IP Security Policies on Local Computer راست کلیک کنید، گزینه All Tasks را انتخاب کنید و در نهایت روی گزینه Create IP Security Policy کلیک کنید.

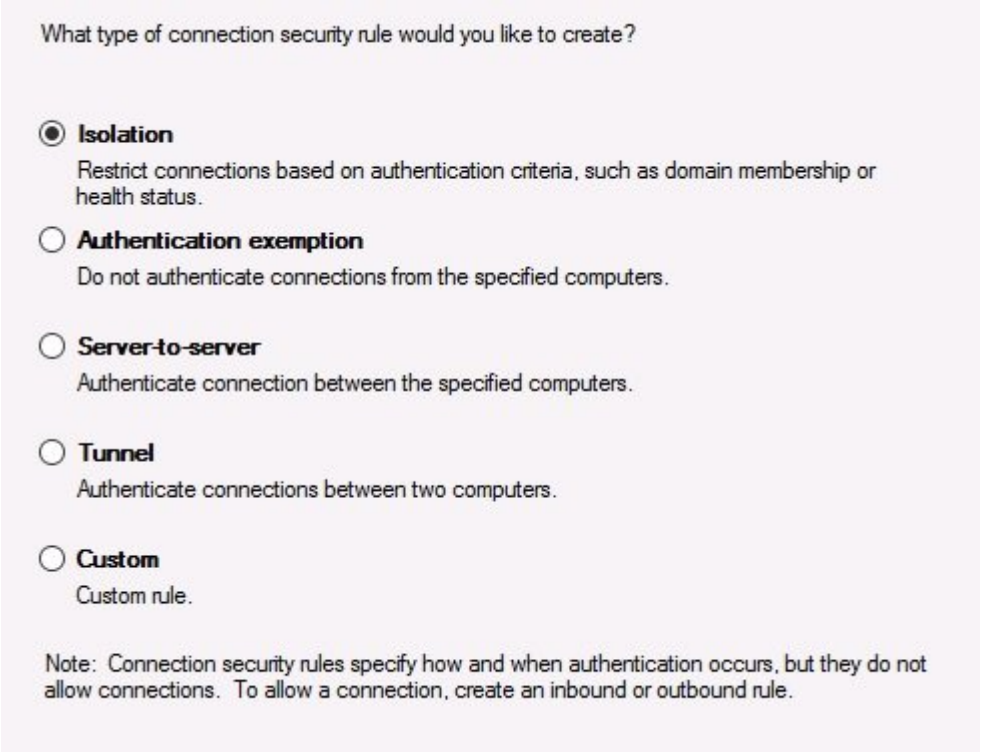


راه‌کار دیگر به‌کارگیری WFAS است

ابزار جدیدتر و قدرتمندتری که برای ایجاد قواعد اتصال IPsec در اختیار قرار دارد Windows Defender Firewall with Advanced Security است. ابزار فوق به همان شکلی که پیش‌تر از آن استفاده کردید، باز کنید و به بخش قواعد امنیتی اتصال (Connection Security Rules) بروید. این بخش در پایین گزینه‌های Inbound Rules and Outbound Rules قرار دارد. Connection Security Rules اجازه می‌دهد قواعد اتصال IPsec را تعریف کنید. اگر روی گزینه Connection Security Rules راست‌کلیک کنید و گزینه New Rule ... را انتخاب کنید، پنجره‌ای ظاهر می‌شود که شبیه به پنجره تعریف قواعد دیوارآتش است.



زمانی که به پنجره تعریف قاعده جدید وارد شدید، گزینه‌هایی متفاوت از گزینه‌های مربوط به تعریف دیوارآتش را مشاهده می‌کنید. ابزار فوق پلتفرمی است که اجازه می‌دهد قواعد امنیتی اتصال IPsec را تعیین کنید و شرح دهید که عملکرد تونل‌های IPsec باید چگونه باشند روی کدام ماشین‌ها یا آدرس‌های آی‌پی فعال باشند.



امکان بررسی تمامی گزینه‌های موجود در این پنجره وجود ندارد، اما پیشنهاد می‌کنم برای اطلاعات بیشتر به **این آدرس** مراجعه کنید.

گذرواژه‌های غیرمجاز

اگر از سرویس‌های ابری همچون Azure Active Directory استفاده می‌کنید، با مفهوم گذرواژه‌های ممنوعه (banned passwords) آشنا هستید. مایکروسافت فهرستی از گذرواژه‌هایی که ضعیف هستند آماده کرده و اگر کاربری سعی کند از گذرواژه‌هایی همچون Password123، P@ssword و مواردی مشابه استفاده کند، مانع انجام این‌کار می‌شود. شما می‌توانید گذرواژه‌های ممنوعه مدنظر خود را به رابط Azure Active Directory اضافه کنید. مایکروسافت به سرپرستان شبکه اجازه می‌دهد فهرستی از گذرواژه‌هایی که نباید از سوی کاربران استفاده شوند را ایجاد کنند. به‌طور مثال، کاربرانی که از Azure Active Directory استفاده می‌کنند، بدون مشکل می‌توانند از ویژگی فوق در Domain Controller استفاده کنند. برای اطلاعات بیشتر در ارتباط با گذرواژه‌های ضعف به **این آدرس** زیر مراجعه کنید.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:

04 آذر 1398

نشانی منبع:
https://www.shabakeh-mag.com/networking-technology/16323/%DA%86%DA%AF%D9%88%D9%86%D9%87-%D8%A7%D8%B1%D8%AA%D8%A8%D8%A7%D8%B7%D8%A7%D8%AA-%D8%B4%D8%A8%DA%A9%D9%87-%D8%AF%D8%B1%D9%88%D9%86-%D8%B3%D8%A7%D8%B2%D9%85%D8%A7%D9%86%DB%8C-%D8%B1%D8%A7-%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%D9%85%D8%B2%DA%AF%D8%B0%D8%A7%D8%B1%DB%8C-%DA%A9%D9%86%DB%8C%D9%85%D8%9F