چگونه فرآیند نوسازی گواهی‌های منقضی شده در ویندوز سرور 2019 را خودکارسازی کنیم؟

فرآیند تخصیص گواهی به ایستگاه‌های کاری و سرورها ممکن است در ظاهر کار چندان خاصی نداشته باشد و شما در مدت زمان کوتاهی گواهی‌ها را تخصیص دهید، اما زمانی‌که صحبت از صدها یا هزاران کامپیوتر به میان می‌آید که نیازمند گواهی هستند و این گواهی‌ها در یک بازه زمانی مشخص منقضی می‌شوند و باید فرآیند تخصیص گواهی‌ها از نو انجام شود تبدیل به یک کابوس می‌شوند. اما ویندوز سرور 2019 به شما اجازه می‌دهد با خودکارسازی این فرآیند کابوس روزانه را به یک کار راحت و ساده تبدیل کنید.

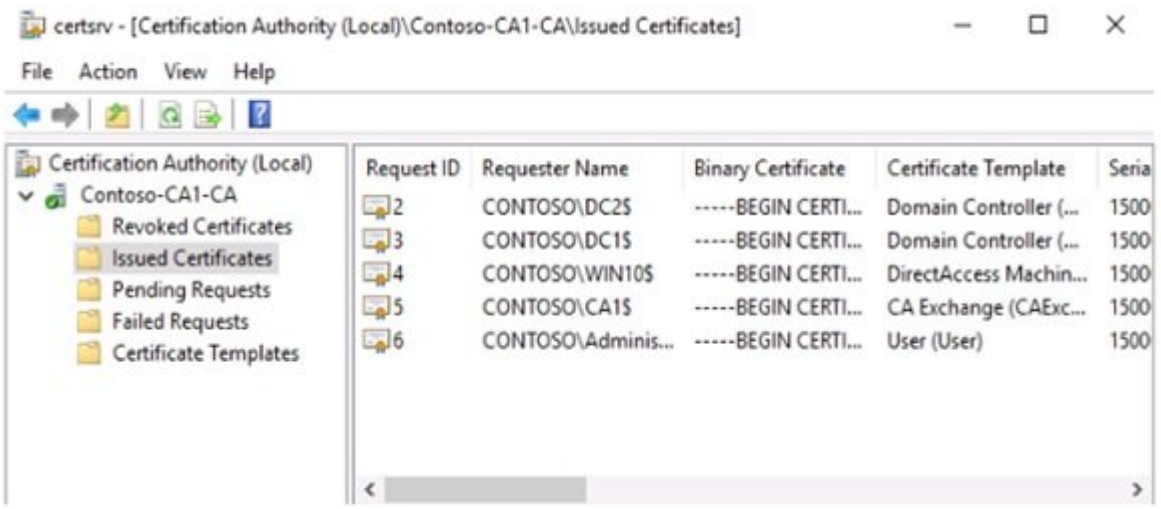
برای مطالعه قسمت قبل **آموزش رایگان ویندوز سرور 2019** اینجا کلیک کنید.

ایجاد یک خط‌مشی ثبت و نوسازی خودکار گواهی‌ها

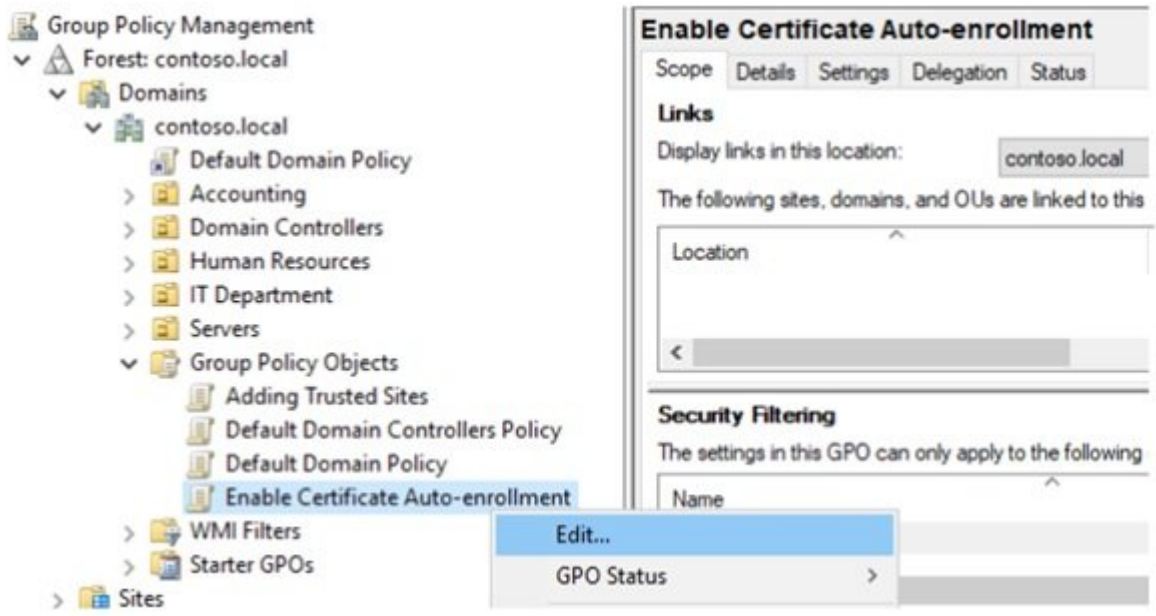
سرور مرجع صدور گواهی ما پیکربندی و اجرا شده و می‌توانیم با موفقیت گواهی‌ها را برای دستگاه‌های کلاینت صادر کنیم. این عالی است! حال بیایید فرض کنیم پروژه جدیدی داریم و یکی از الزامات پروژه این است که تمام کلاینت‌های موجود در شبکه به یک نسخه از این گواهی ماشین جدید نیاز دارند. به نظر کار سخت و زیادی پیش‌رو داریم، حتا اگر روند درخواست یک گواهی به سرعت انجام شود و شما برای هر ایستگاه کاری تنها چند ثانیه زمان صرف کنید، زمانی‌که مجبور شوید به‌طور جداگانه به وضعیت دو هزار ایستگاه کاری پاسخ دهید، زمان قابل توجهی را از دست خواهید داد. علاوه بر این، در بسیاری موارد گواهی‌هایی که صادر می‌کنید فقط برای یک سال اعتبار دارند. آیا این بدان معناست که ما هر ساله با کارهای مدیریتی شدید روبرو می‌شویم و مجبور هستیم هر ساله این گواهی‌ها را دوباره صادر کنیم؟ قطعا این‌گونه نیست!

اجازه دهید به واکاوی این مسئله بپردازیم که چگونه از Group Policy برای ایجاد یک GPO استفاده کرده و کاری کنیم تا گواهی‌های جدید برای کلیه دستگاه‌های موجود در شبکه ثبت خودکار شوند و ما آن‌ها به گونه‌ای پیکربندی کنیم تا وقتی تاریخ انقضاء یک گواهی فرا رسید، گواهینامه در فواصل زمانی مناسب تمدید خودکار می‌شود.

بیایید به سراغ کنسول مدیریتی Certification Authority در سرور CA خود وارد شده و به پوشه Issued Certificates نگاهی بیندازیم. در نظر داریم یک جست‌وجوی ساده انجام دهیم تا ببینیم چه تعداد گواهی‌هایی تاکنون در شبکه خود صادر کرده‌ایم. به نظر می‌رسد فقط تعداد معدودی وجود دارد، امیدواریم هستیم پس از پیکربندی خط‌مشی‌های خود، این‌کار را به درستی انجام دهیم تا خط‌مشی جدید به‌طور خودکار روی گواهی‌ها اعمال شود. در تصویر زیر فهرستی از گواهی‌ها را مشاهده می‌کنید.

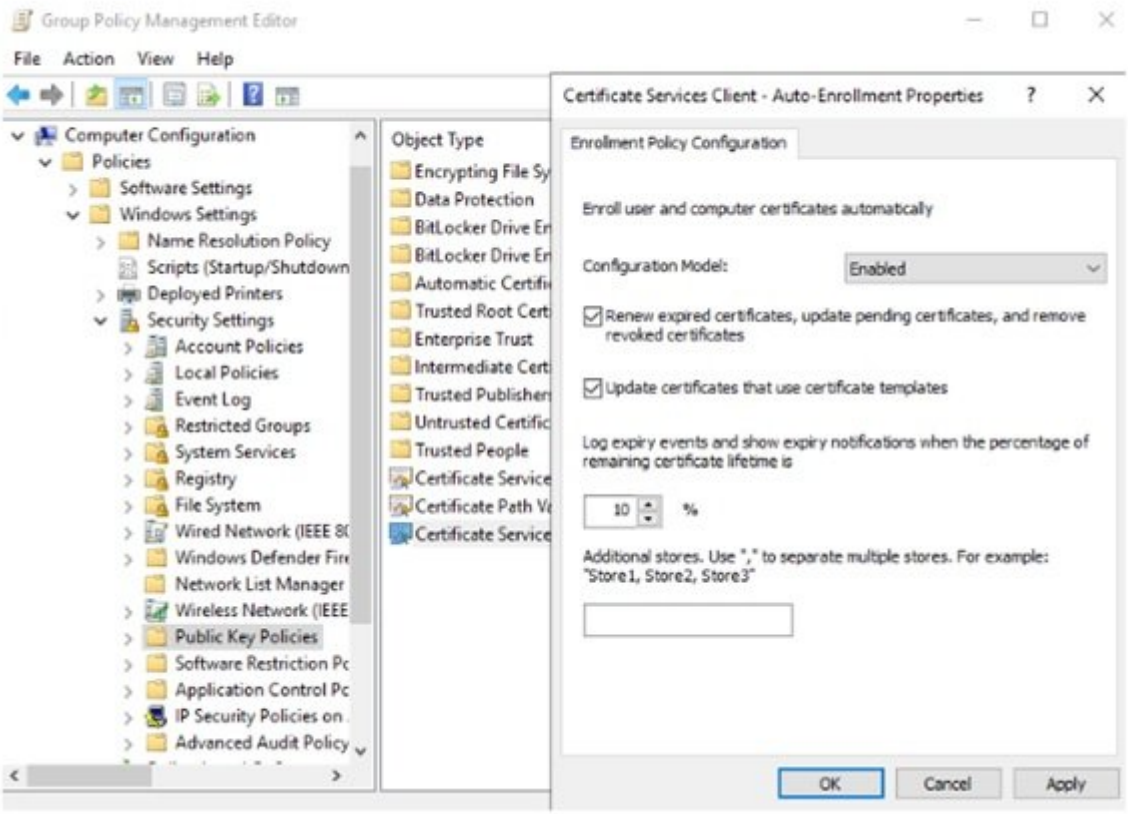


وارد سرور کنترل‌کننده دامنه شوید و سپس کنسول Group Policy Management را باز کنید. ما یک GPO جدید به‌نام Enable Certificate Auto-enrollment را از قبل ایجاد کرده‌ایم و اکنون قصد داریم GPO را برای هماهنگ بودن با تنظیماتی که قرار است اعمال شوند پیکربندی کنیم.



تنظیمات این GPO که قرار است آن‌را پیکربندی کنیم در مسیر Computer Configuration | Policies | Windows Settings | Security Settings | Public Key Policies | Certificate Services Client – Auto-Enrollment قرار دارد.

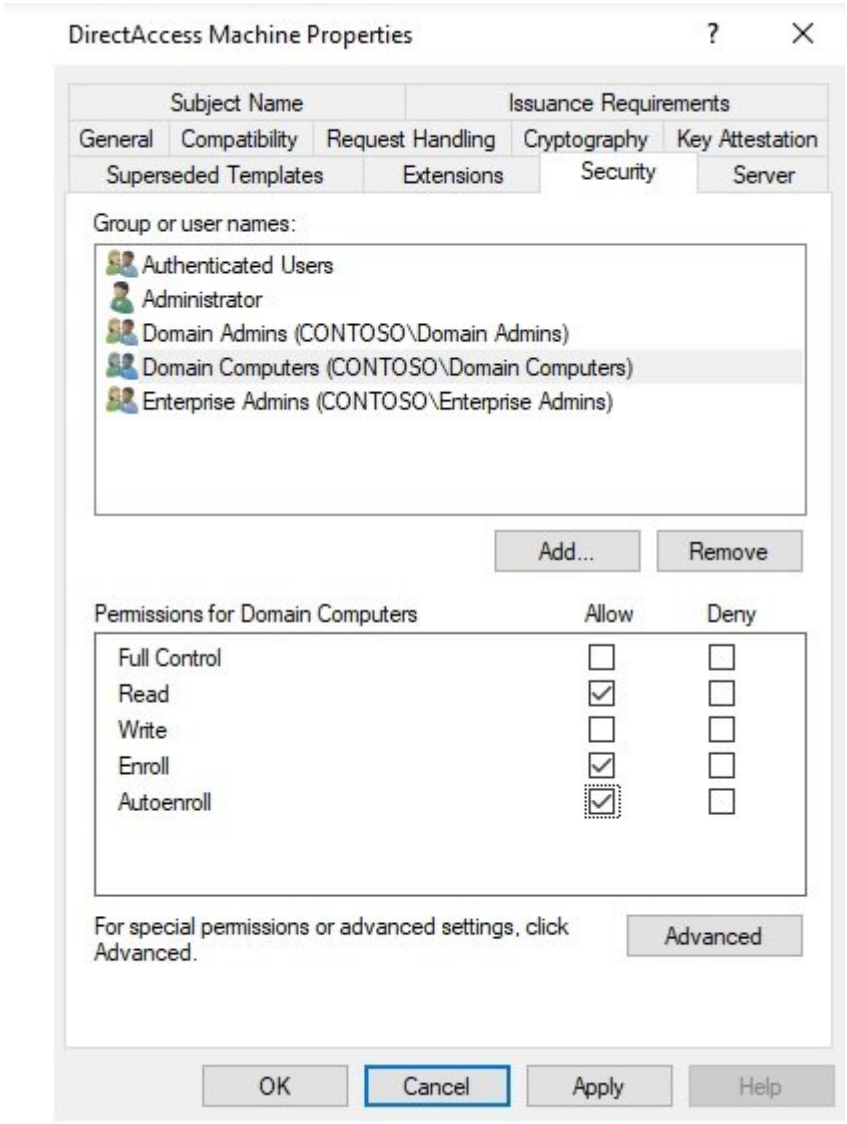
برای مشاهده خاصیت‌های تنظیمات دوبار روی آن کلیک کنید. تنها کاری که باید انجام دهیم تغییر Configuration Model به حالت Enabled و فعال کردن تیک گزینه Renew expired certificates, update pending certificates, and remove revoked certificates است. همچنین تیک کادر Update certificates that use certificate templates را نیز فعال کنید. این تنظیمات به شما اطمینان می‌دهند که هر ساله فرآیند تمدید خودکار گواهی‌ها پس از انقضای آن‌ها انجام خواهد شد.



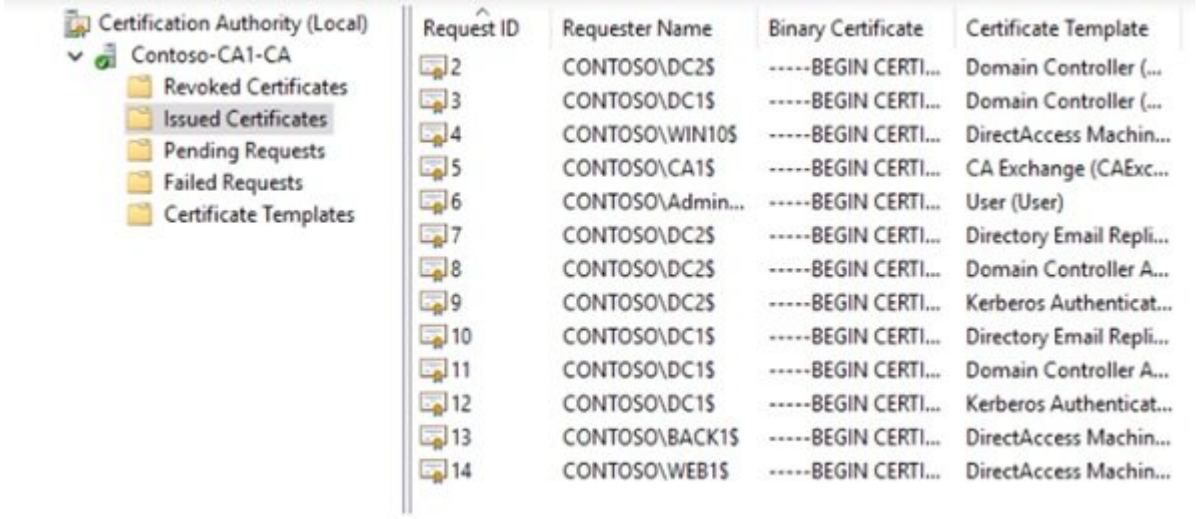
آخرین کاری که برای ایجاد GPO خود باید انجام دهید، ساخت یک لینک است تا کار آغاز شود. برای محیط کاری خود همان‌گونه که پیش‌تر اشاره کردیم باید لینکی که ایجاد می‌کنید به واحد سازمانی خاصی (OU) نسبت داده شود، اما در آموزش فوق در نظر داریم این گواهی‌ها به هر کامپیوتر منفردی که عضو دامنه است اعمال شود. بنابراین GPO جدید خود را با ریشه دامنه مرتبط می‌کنیم تا روی همه کلاینت‌ها و سرورها اعمال شود.

اکنون که GPO ایجاد و پیکربندی شده و آن‌را به دامنه مرتبط کردیم، فکر می‌کنم برخی از گواهینامه‌های جدید صادر شوند و نام‌های بیشتری درون پوشه Issued Certificates در داخل کنسول مرجع صدور گواهی نشان داده شوند. اما چنین چیزی را مشاهده نمی‌کنیم. یک دقیقه صبر کنید، در GPO که ایجاد کردیم، ما واقعا گزینه‌ای را برای الگوی گواهی DirectAccess Machine ماشین خود مشخص نکردیم، آیا این موضوع می‌تواند عامل بروز این مشکل باشد؟ پاسخ منفی است. در واقع گزینه‌ای برای مشخص کردن الگویی که قصد داریم روند ثبت خودکار برای آن انجام شود وجود ندارد.

هنگامی که ثبت خودکار در Group Policy را فعال می‌کنید، به سادگی با چرخش سوئیچ روشن / خاموش، خط‌مشی روی هر الگوی گواهی اعمال می‌شود. بنابراین اکنون که خط‌مشی پیکربندی شده‌ای برای ثبت خودکار در اختیار داریم و آن‌را با دامنه مرتبط کردیم، خط‌مشی فعال است و ثبت خودکار روی هر کامپیوتر متصل به دامنه و هر الگوی گواهی منتشر شده روی سرور مرجع صدور گواهی اعمال می‌شود. با این حال، شاهد حضور هیچ یک از الگوها روی کامپیوترهای‌مان نیستیم، زیرا باید تنظیمات امنیتی را در الگوی جدید DirectAccess Machine تنظیم کنیم. در حال حاضر ما آن‌را به‌گونه‌ای پیکربندی کرده‌ایم تا تمامی کامپیوترهای دامنه مجوز Enroll را داشته باشند، اما اگر به یاد داشته باشید در زبانه امنیتی درون خصوصیات الگوی گواهی یک شناسه امنیتی اضافی به نام Autoenroll وجود دارد. هر الگوی گواهی دارای شناسه مجوزدهی خودکار خاص خود است و به‌طور پیش‌فرض روی حالت allowed قرار ندارد. اکنون که گواهی‌ها و ملزومات ما در وضعیت ثبت‌خودکار در دامنه قرار دارند، ما باید مجوز ثبت‌خودکار برای هر الگو را فعال کنیم تا الگوها بتوانند خود را توزیع کنند. به محض این‌که مجوز فوق را فعال کردیم، این گواهی‌ها در شبکه فعال شده و قابل استفاده می‌شوند. برای این منظور به بخش مدیریت گواهی در سرور مرجع صدور گواهی رفته و Properties را برای الگوی جدید خود باز کرده، سپس به زبانه Security رفته و اجازه AutoEnroll را برای گروه Domain Computer را فعال کنید. این‌کار به سرور CA می‌گوید که توزیع این گواهینامه‌ها را آغاز کند:



اکنون مطمئن هستیم به Active Directory و Group Policy فرصتی داده‌ایم تا فرآیند به‌روزرسانی تمامی دستگاه‌ها را انجام دهند و اکنون می‌توانیم گواهینامه‌های بیشتری که سرور CA صادر کرده است را مشاهده کنیم.



به منظور صدور گواهینامه به‌طور خودکار از هر الگویی که ایجاد می‌کنید، به سادگی این الگو را منتشر کنید و مطمئن شوید که مجوزهای ثبت خودکار برای آن الگو را به درستی پیکربندی کرده‌اید. هنگامی که GPO ثبت خودکار

برای کلاینت‌ها را مستقر کردید، آن‌ها می‌توانند به سرور CA دسترسی پیدا کرده و از هر الگویی برای دریافت گواهی که مجوز به دریافت آن هستند از سرور سوال کنند. در آینده، هنگامی که گواهینامه به زمان انقضا رسید و دستگاه به نسخه جدیدی نیاز داشت، خط‌مشی ثبت خودکار قبل از تاریخ انقضا بر اساس زمان‌های تعیین شده در GPO نسخه جدیدی را صادر می‌کند. ثبت خودکار گواهی می‌تواند فرآیندی که معمولا یک بار عظیم کاری محسوب می‌شود را به یک فرآیند کاملا خودکار تبدیل کند!

فرآیند اخذ گواهی SSL از مرجع عمومی

ما می‌توانیم گواهی‌ها را از سرور CA خودمان در شبکه به راحتی دریافت کنیم، اما اگر قصد داشته باشیم گواهی‌های SSL را برای وب‌سرورهای‌مان از مراجع صدور گواهی عمومی دریافت کنیم چه اتفاقی می‌افتد؟ برای بسیاری از ما، رایج‌ترین نوع تعامل با گواهینامه‌ها دریافت گواهی‌های SSL عمومی است. هنگامی که نیاز به اخذ گواهی SSL از مراجع عمومی دارید، یک فرآیند سه مرحله‌ای، ایجاد یک درخواست گواهی، ثبت و ارسال درخواست گواهی و نصب گواهی به دست آماده را باید پشت سر بگذارید. ما قصد داریم از سرور WEB1 که وب‌سایت روی آن فعال است استفاده کنیم. در حال حاضر این سایت فقط قادر به کنترل ترافیک HTTP است، اما زمانی که ارتباط با اینترنت قطع می‌شود باید HTTPS را فعال کنیم تا اطلاعاتی را که در سایت رمزگذاری و ثبت شده نگه‌داری شود. برای استفاده از HTTPS ما ابتدا باید یک گواهی SSL را روی سرور WEB1 نصب کنیم. این وب‌سرور پلت‌فرم خدمات وب مایکروسافت یا به عبارت دقیق‌تر (IIS) را اجرا می‌کند. فرآیند سه مرحله‌ای که ما پشت سر خواهیم گذاشت یکسان با حالتی است که شما یک وب‌سرور مختلف شبیه به آپاچی را اجرا می‌کنید، اما یکسری جزییات ممکن است در این سه مرحله متفاوت باشند، زیرا آپاچی یا هر وب‌سرور دیگری از رابط‌های کاربری متفاوتی نسبت به IIS استفاده می‌کنند. از آن‌جایی که ما روی وب‌سرور ویندوز سرور 2019 کار می‌کنیم از IIS 10 استفاده می‌کنیم.

جفت کلید عمومی یا خصوصی

قبل از این‌که به فرآیند سه مرحله‌ای خود وارد شویم، اجازه دهید به مبحث مهم جفت کلیدهای عمومی و خصوصی اشاره‌ای داشته باشیم. احتمالاً شما با اصطلاح کلید خصوصی آشنا هستید، اما ممکن است به درستی متوجه نشده باشید که این اصطلاح چه معنایی دارد. زمانی‌که ترافیک کامپیوترهای کلاینت ما از طریق اینترنت به یک وب‌سایت مبتنی بر HTTPS ارسال می‌شود، متوجه می‌شویم که ترافیک رمزگذاری شده است. این حرف بدان معنا است که بسته‌ها قبل از ترک کامپیوتر ما در بسته‌های کوچک مهر و موم شده قرار می‌گیرند تا در فرآیند انتقال هر کسی نتواند محتوای آن‌ها را مشاهده کند و بسته‌ها به درستی به وب‌سرور برسند. لپ‌تاپ من از یک کلید برای رمزگذاری ترافیک استفاده می‌کند و سرور از یک کلید برای رمزگشایی آن ترافیک استفاده می‌کند، اما کلاینت و سرور چگونه می‌دانند باید از چه کلیدهایی استفاده می‌کنند؟ دو روش مختلف رمزنگاری وجود دارد که می‌توان از آن‌ها استفاده کرد:

رمزگذاری متقارن: روش ساده‌تر رمزگذاری متقارن به معنای وجود یک کلید واحد است که هر دو طرف از آن استفاده می‌کنند. ترافیک با استفاده از یک کلید بسته‌بندی می‌شود و از همان کلید برای باز کردن ترافیک در هنگام رسیدن به مقصد استفاده می‌شود. از آن‌جایی که این کلید واحد همه آن چیزی است که در اختیار دارید، تمایلی ندارید به اشتباه آن‌را در اختیار فرد دیگری قرار دهید، این حرف بدان معنا است که شما آن‌را در اینترنت ارائه نداده و استفاده نمی‌کنید. بنابراین، رمزگذاری متقارن به‌طور کلی برای محافظت از ترافیک وب سایت اینترنتی استفاده نمی‌شود.

رمزگذاری نامتقارن: این تکنیک رمزنگاری تمرکزش روی ترافیک HTTPS است. رمزگذاری نامتقارن از دو کلید استفاده می‌کند: یک کلید عمومی و یک کلید خصوصی. کلید عمومی درون گواهینامه SSL قرار داده شده، بنابراین هر کسی در اینترنت می‌تواند با وب‌سایت شما ارتباط برقرار کرده و کلید عمومی را به‌دست آورد. سپس لپ‌تاپ شما از آن کلید عمومی برای رمزگذاری ترافیک استفاده می‌کند و آن‌را برای وب‌سرور ارسال می‌کند. چرا کلید عمومی در کل اینترنت در دسترس است؟ زیرا ترافیک فقط با استفاده از یک کلید خصوصی مربوطه که به‌طور ایمن در وب‌سرور شما ذخیره می‌شود قابل رمزگشایی است، بنابراین حفظ امنیت کلید خصوصی و وب‌سرور حائز اهمیت است و در نتیجه باید اطمینان حاصل کنید که این کلید در اختیار شخص دیگری قرار نمی‌گیرد.

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:

16 شهریور 1398

نشانی منبع:
https://www.shabakeh-mag.com/networking-technology/16005/%DA%86%DA%AF%D9%88%D9%86%D9%87-%D9%81%D8%B1%D8%A2%DB%8C%D9%86%D8%AF-%D9%86%D9%88%D8%B3%D8%A7%D8%B2%DB%8C-%DA%AF%D9%88%D8%A7%D9%87%DB%8C%E2%80%8C%D9%87%D8%A7%DB%8C-%D9%85%D9%86%D9%82%D8%B6%DB%8C-%D8%B4%D8%AF%D9%87-%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