



فناوری‌های امروزی شرکت‌ها را ترغیب می‌کنند تا به کارمندان خود اجازه دهند از هر مکانی کارهای خود را انجام دهند. امروزه بیشتر سازمان‌ها به دنبال جذب نیروی دورکار هستند و به همین دلیل برای آن‌که به کارمندان خود اجازه دهند از راه دور به برنامه‌ها و داده‌های سازمانی دسترسی از طریق دستگاه‌های همراه دسترسی پیدا کنند به روش‌های کارآمد، پایدار و ایمنی نیاز دارند. نقش Remote Access در ویندوز سرور 2019 به گونه‌ای طراحی شده که همین کار را انجام دهد. به لطف سه روش مختلفی که برای دسترسی از راه دور به منابع سازمانی ارائه کرده، سازمان‌ها می‌توانند با خیال آسوده به دنیای جذب کارمندان دورکار وارد شوند.

برای مطالعه قسمت قبل آموزش رایگان ویندوز سرور 2019 [اینجا](#) کلیک کنید.

Web Application Proxy

DirectAccess و VPN هر دو جزء بهترین فناوری‌های دسترسی از راه دور هستند. ترکیب این دو فناوری با یکدیگر می‌تواند یک راه‌حل جامع دسترسی از راه دور را برای سازمان شما فراهم کند، بدون آن‌که به راه‌حل‌های ثالث یا پرداخت هزینه‌های بیشتر نیازی داشته باشد. در ویندوز سرور 2019 و درون Remote Access هنوز هم یک مولفه جالب و کاربردی دیگر برای استفاده نیاز دارد. این مولفه کاربردی (WAP) سرنام Proxy Application نام دارد. مولفه فوق در حقیقت یک مکانیسم پراکسی معکوس است و به شما امکان می‌دهد برخی از برنامه‌های HTTP و HTTPS که درون شبکه سازمانی میزبان می‌شوند را به شکل ایمن در اینترنت منتشر کنید. مدیران شبکه که سابقه کار با فناوری‌های تحت شبکه مایکروسافت را دارند به خوبی می‌دانند که مایکروسافت محصولی به نام Forefront Unified Access Gateway (UAG) را چند سال پیش ارائه کرد که عملکردی مشابه با WAP دارد. UAG یک راه‌حل جامع مبتنی بر SSLVPN بود که برای انتشار برنامه‌های داخلی روی بستر اینترنت از طریق پروتکل SSL طراحی شده بود. محصول فوق عملکردی به مراتب قدرتمندتر از یک پروکسی معکوس ساده داشت و ویژگی‌هایی همچون تأیید هویت از پیش تعریف شده، SSTP VPN و گیت‌وی RDS را ارائه می‌کرد. جالب آن‌که DirectAccess را می‌توان از طریق UAG اجرا کرد. اگر تمامی کارمندان دورکار سازمان از DirectAccess یا VPN برای دسترسی به شبکه استفاده کنند، به احتمال زیاد شاید هیچ‌گاه به سراغ WAP نروید. با این حال، به دلیل این‌که فناوری‌های ابرمحور به سرعت در حال رشد هستند، انتظار می‌رود در چند سال آینده کاربران یک مرورگر وب را روی هر دستگاه و هر مکانی اجرا کنند و به برخی از برنامه‌های کاربردی دسترسی پیدا کنند. امروزه در بیشتر سازمان‌ها برای دسترسی به اسناد از سرویس‌های تحت وب شبیه به شیرپوینت و برای دسترسی به ایمیل از راه دور، از طریق هر کامپیوتری از Outlook Web Access استفاده می‌شود.

به همین دلیل ظرف چند سال آینده بسیاری از برنامه‌ها و برخی از داده‌ها تنها از طریق مرورگر وب در دسترس خواهند بود و کارمندان بدون نیاز به ایجاد یک تونل شرکتی تمام و کامل تمام عیار همچون شبکه خصوصی مجازی قادر به دسترسی به داده‌ها خواهند بود. بنابراین کاربرد WAP در دنیای واقعی چیست؟ کامپیوترهای خانگی که تمایلی ندارند به شبکه خصوصی مجازی متصل شوند. به این ترتیب، دیگر لازم نیست از بابت وضعیت امنیتی یا کارکرد درست کامپیوتر خانگی خود نگران باشید، زیرا تعامل با شرکت تنها از طریق مرورگر وب انجام می‌شود. این راهکار مانع از آن می‌شود تا کارمندانی که قصد شیطننت در شبکه سازمانی را دارند با موفقیت بتوانند طرح خود را به سرانجام برسانند. همان‌گونه که مشاهده می‌کنید، فناوری‌هایی همچون WAP بدون تردید در آینده جایگاه خود در بازار دسترسی از راه دور را به دست خواهند آورد.

البته با گذشت زمان، قابلیت‌های WAP بهبود پیدا خواهند کرد و جایگزینی واقعی برای UAG خواهند شد. UAG اولین بار همراه با در ویندوز سرور R2 2008 معرفی شد و اکنون به‌طور رسمی مایکروسافت آن‌را کنار گذاشته است. نزدیک‌ترین راه‌حلی که مایکروسافت برای فناوری UAG ارائه کرده، نقش WAP است. البته نقش فوق هنوز کاملاً فراگیر نشده، اما مایکروسافت در تلاش است با بهبود قابلیت‌ها آن‌را به یک فناوری تاثیرگذار تبدیل کند. در حال حاضر، WAP برای دسترسی به برنامه‌های ساده وب مفید است. همچنین می‌توانید نحوه دسترسی به برنامه‌های کلاینت‌های قدرتمندی که از مکانیزم احراز هویت مبتنی بر HTTP استفاده می‌کنند همچون Exchange ActiveSync را با استفاده از این فناوری ساده کنید. به‌کارگیری فناوری فوق مزیت دیگری نیاز دارد که اجازه می‌دهد داده‌های موردنیاز کلاینت‌هایی که از MSOFBA استفاده می‌کنند را به‌اشتراک قرار دهید. به‌طور مثال کاربران می‌توانند از طریق برنامه‌های ورد و اکسل که روی کامپیوتر محلی آن‌ها اجرا می‌شود به واکشی داده‌های سازمانی بپردازند.

WAP می‌تواند توسط پروکسی معکوس برای دسترسی به نرم‌افزارهایی همچون Exchange و SharePoint استفاده شود. این قابلیت موضوع کوچکی نیست، زیرا همه کاربران می‌توانند از این فناوری‌ها استفاده کنند و بدون شک چنین رویکردی برای هر سازمانی سودمند خواهد بود تا WAP را برای ایمن‌سازی دسترسی به داده‌ها و منابع پیاده‌سازی کند.

WAP به عنوان AD FS Proxy

روش جالب دیگر به‌کارگیری سرور WAP در زمان پیکربندی (AD FS) سرنام Active Directory Federation Services در شبکه سازمانی است. AD FS فناوری است که برای فعال‌سازی ورود تک مرحله‌ای به سیستم برای کاربران و شرکت‌های فراملیتی طراحی شده است، در نتیجه قادر است ترافیک اینترنت را به شبکه داخلی یک سازمان وارد کند. در گذشته، مولفه‌ای در AD FS به نام AD FS Proxy قرار داشت. در جدیدترین نسخه منتشر شده از AD FS این نقش جداگانه دیگر وجود ندارد و مولفه Web Application Proxy جایگزین آن شده است. مولفه فوق یک راه‌کار دسترسی از راه دور منسجم‌تر ارائه می‌کند و به جای آن‌که کاربر را مجبور کند تا یک سرور مجزا AD FS Proxy آماده کند، ترافیک ورودی AD FS را از طریق سرور رسمی Remote Access Server وارد می‌کند. هر سرپرست شبکه‌ای که AD FS را در محیط خود اجرا می‌کند متوجه خواهد شد که استقرار WAP تقریباً اجتناب‌ناپذیر است.

الزامات WAP

متأسفانه Proxy Application Web به یکسری ملزومات اولیه نیاز دارد. شما مجبور هستید AD FS را در محیط شبکه نصب کنید، زیرا پیکربندی WAP در AD FS ذخیره می‌شود. هیچ یک از اطلاعات پیکربندی WAP در خود Remote Access Server ذخیره نمی‌شود که اجازه می‌دهد سرور به راحتی اجرا شود و در صورت لزوم کارهای مدیریتی همچون انتقال یا اعمال تغییرات را بدون مشکل روی آن انجام داد. همان‌گونه که اشاره شد باید AD FS را در محیط خود اجرا کنید تا WAP بتواند مکانی برای ذخیره‌سازی اطلاعات پیکربندی داشته باشد.

درست است که یکپارچگی دقیق با AD FS به این معنا است که ما گزینه‌های تأیید هویت بهتری داریم و کاربران می‌توانند از مزایای ورود تک مرحله‌ای به AD FS در ارتباط با برنامه‌هایی که از طریق WAP منتشر کرده‌اند، استفاده کنند، اما در برخی موارد مشکلاتی برای کسب‌وکارهای کوچک به وجود می‌آورد. بسیاری از شرکت‌ها هنوز AD FS را اجرا نکرده‌اند و اگر تنها دلیل پیاده‌سازی AD FS این باشد که بتوانید از WAP برای انتشار چند برنامه وب در اینترنت استفاده کنند، شاید سازمان‌ها هیچ‌گاه چنین کاری را انجام نخواهند داد.

همان‌گونه که اشاره شد برای به‌کارگیری WAP به AD FS نیاز دارید که خوشبختانه AD FS کارکردهای دیگری نیز دارد. در زمان نگارش این مقاله، یکی از رایج‌ترین کاربردهای آن ادغام با Office 365 است. اگر می‌خواهید Office 365 را در محیط سازمان وارد کنید و از آن استفاده کنید، AD FS ابزاری عالی است، زیرا قابلیت قدرتمندی برای تأیید هویت مربوط به ترافیک آفیس 365 ارائه می‌کند، هرچند آفیس 365 همانند سایر کشورها در ایران قابل استفاده نیست.

آخرین پیشرفت‌های WAP

Web Application Proxy اولین بار همراه با سرویس پک ویندوز سرور 2012 معرفی شد و زمانی‌که ویندوز سرور 2016 معرفی شد، بسیاری از قابلیت‌های آن بهبود پیدا کردند. از آن زمان تا به امروز تغییرات اساسی خاصی در آن انجام شده و موارد جزئی از آن ویرایش شده‌اند، اما بدیهی است که برخی از ویژگی‌ها هنوز هم باید تکمیل شوند. از جدیدترین پیشرفت‌های انجام گرفته در WAP به موارد زیر می‌توان اشاره کرد:

پیش تعیین هویت برای HTTP Basic

دو روش مختلفی که کاربران می‌توانند برای تعیین هویت خود به برنامه‌هایی که توسط Web Application Proxy منتشر شده‌اند از آن‌ها استفاده کنند preauthentication و pass-thru authentication است. زمانی‌که برنامه‌ای توسط preauthentication منتشر می‌شود، به معنای آن است که کاربران توسط رابط AD FS متوقف می‌شوند تا اعتبار خودشان را پیش از آن‌که بتوانند به برنامه وب دسترسی پیدا کنند به اثبات برسانند. گزینه دوم احراز هویت pass-thru است و عملکرد مشابهی دارد. زمانی‌که دسترسی به یک برنامه داده می‌شود و گزینه احراز هویت pass-thru را انتخاب می‌کنید، WAP بسته‌هایی که از اینترنت به برنامه سرور وارد شده یا بالعکس از آن خارج می‌شود را انتقال می‌دهد. کاربران می‌توانند بدون احراز هویت به برنامه وب دسترسی پیدا کنند، بنابراین به لحاظ تئوری، هر کسی می‌تواند به وبسایت برنامه شما دسترسی پیدا کند. از آنجایی که خود برنامه به احتمال زیاد نیاز به تأیید اعتبار کاربر نیاز دارد، اما هیچ‌گونه مکانیسم محافظت در برابر حمله مرد میانی وجود ندارد، برنامه وب به شکل عمومی برای همه مردم قابل مشاهده است. بنابراین پیشنهاد نمی‌کنم از مکانیسم دوم استفاده کنید.

ارسال آدرس‌های آی‌پی کلاینت‌ها برای برنامه‌ها

در دنیای پروکسی معکوس و SSLVPN، گاهی اوقات برنامه‌هایی اجرا می‌کنیم که به آدرس آی‌پی محلی کلاینت نیاز دارند. درست است که این حالت میراثی از گذشته است و شاید چنین اتفاقی رخ ندهد، اما احتمال آن صفر نیست. زمانی‌که برنامه اصلی آدرس آی‌پی کلاینت را بداند، چالش بزرگی در ارتباط با راه‌حل‌های پروکسی معکوس به وجود می‌آورد. هنگامی که ترافیک کاربر از طریق WAP یا هر پروکسی معکوس دیگری شبیه به یک NAT در جریان باشد، اطلاعات آدرس آی‌پی منبع در بسته‌ها تغییر می‌کند. در این حالت برنامه اصلی سرور نمی‌تواند آدرس آی‌پی کلاینت را تشخیص دهد و مشکلی رخ می‌دهد. Proxy Application Web اکنون امکان انتشار آدرس آی‌پی سمت مشتری از طریق برنامه سرور اصلی را دارد و بروز این مشکل را کاهش می‌دهد.

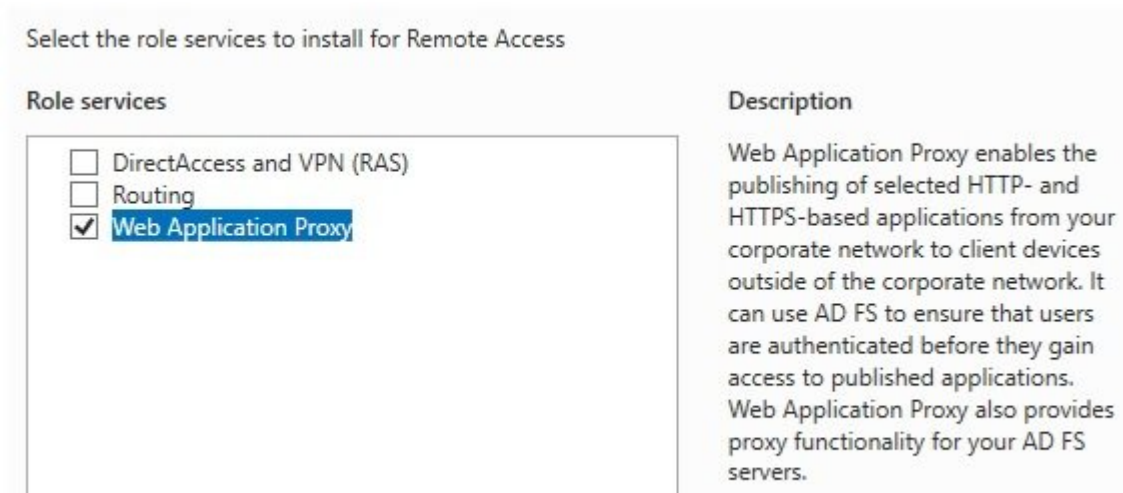
انتشار Remote Desktop Gateway

یکی از مواردی که UAG معمولاً از آن استفاده می‌کرد، انتشار دسترسی به Remote Desktop Services بود. UAG در باطن Remote Desktop Gateway مخصوص به خود را داشت و به شما امکان انتشار دسترسی به سرورهای RDSH، اتصالات انفرادی RDP به کامپیوتری دستکاپ از قبیل پیاده‌سازی VDI و حتی دسترسی به برنامه‌های RemoteApp را می‌داد. متأسفانه، WAP حتی در نسخه جدید نمی‌تواند هیچ یک از کارهای فوق را انجام دهد، البته مواردی که به آن‌ها اشاره شد عملکرد خیلی تاثیرگذار نداشتند و شاید بهتر است که چنین قابلیت‌هایی در WAP قرار ندارد، در مقابل WAP دسترسی به خود سرور Remote Desktop Gateway را منتشر می‌کند. به‌طور سنتی RDG در لبه شبکه نشسته و کاربران خارجی را از طریق سرورهای Remote Desktop به یکدیگر متصل می‌کند. قرار دادن WAP در جلوی RD Gateway یک مکانیزم احراز هویت از پیش تعریف شده قدرتمندی برای سرویس‌های Remote Desktop به وجود می‌آورد.

بهبود کنسول مدیریتی

کاربران با استفاده از پاورشل WAP را در ویندوز سرور 2012 سرویس پک دو پیاده‌سازی و مدیریت می‌کردند. شما

هنوز هم می‌توانید از پاورشل برای ساخت قواعد نشر استفاده کنید، اما Remote Access Management Console عملکردی به مراتب بهتری دارد و به شکل بهتری با Web Application Proxy ارتباط برقرار می‌کند. برای مشاهده کنسول فوق باید مطمئن شوید در زمان نصب نقش Remote Access تیک مربوط به این گزینه را فعال کرده باشید. اگر در زمان نصب نقش فوق تیک Web Application Proxy را فعال نکرده‌اید، برای افزودن WAP به سرور خود به بخش add/remove Roles در ابزار Server Manager مراجعه کنید و WAP را به سرور خود اضافه کنید.



پس از اضافه شدن نقش یاد شده، دومرتبه کنسول مدیریت از راه دور را اجرا کنید تا گزینه اضافه شده به بخش Configuration Wizard را مشاهده کنید. از طریق بخش فوق قادر هستید Web Application Proxy Configuration Wizard را اجرا کنید و سایر کارهای مدیریتی را انجام دهید.



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:

نشانی منبع:

<https://www.shabakeh-mag.com/networking-technology/16230/%D9%82%D8%A7%D8%A8%D9%84%DB%8C%D8%AA-web-application-proxy-%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-%DA%86%DB%8C%D8%B3%D8%AA-%D9%88-%DA%86%D9%87-%DA%A9%D8%A7%D8%B1%DB%8C-%D8%A7%D9%86%D8%AC%D8%A7%D9%85-%D9%85%DB%8C>