تسلط بر مفاهیم پایه شبکه منطبق با استانداردهای بین‌المللی

آموزش رایگان دوره نتورک‌پلاس، رمزنگاری، پروتکل IPsec، SSL (بخش 45)

در شماره گذشته آموزش نتورک‌پلاس با مدل‌های مختلف رایانش ابری و نحوه استقرار آن‌ها آشنا شدیم. در ادامه برخی از ویژگی‌های مثبت و منفی رایانش ابری را بررسی کردیم. همان‌گونه که وعده دادیم در این شماره به سراغ مبحث پروتکل‌های رمزنگاری و سایر مباحث مرتبط با رایانش ابری خواهیم رفت.

برای مطالعه بخش چهل و چهارم آموزش رایگان و جامع نتورک پلاس (Network+) اینجا کلیک کنید

• بدون استفاده، داده‌ها زمانی که روی دستگاهی ذخیره شوند که توسط یک دیوارآتش، نرم‌افزار ضد بدافزار و بسته‌های امنیتی محافظت شود در امنیت قرار دارند. با این حال، هیچ تضمینی وجود ندارد که داده‌ها در امنیت کامل قرار داشته باشند. حفاظت اضافی شامل ذخیره‌سازی داده‌ها در مکان‌های جداگانه‌ای است که هیچ‌گونه ارتباطی با یکدیگر ندارند.

• در حال استفاده - داده‌ها برای استفاده باید در دسترس باشند که طبیعی است خطراتی آن‌ها را تهدید می‌کند. برای محافظت از داده‌ها تشدید کنترل روی نحوه دسترسی به داده‌ها و احراز هویت کامل پیش از دسترسی به داده‌ها از میزان مخاطرات کم می‌کند.

• در حال انتقال – این وضعیت زمانی است که داده‌ها در معرض آسیب‌پذیری شدید قرار دارند، به ویژه هنگامی که قرار است از شبکه مورد اعتماد به دستگاه‌ها یا شبکه‌های دیگری انتقال پیدا کنند. پیوندهای ضعیف، نفوذ از طریق پیاده‌سازی بردارهای حمله و شکاف‌های بالقوه تنها بخشی از این مخاطرات امنیتی هستند. در زمان انتقال فایل‌ها به ویژه در حالت بی‌سیم داده‌ها به شدت در معرض دستبرد یا تغییر قرار دارند. به همین دلیل بیشتر سازمان‌ها و شرکت‌ها در زمان انتقال داده‌ها از یک لایه امنیتی مضاعف برای مراقبت از داده‌ها استفاده کنند.

رمزنگاری آخرین ابزار دفاعی در برابر سرقت اطلاعات است. به عبارت دیگر، اگر یک هکر از تمامی روش‌های امنیتی، از جمله مکانیزم‌های دفاع فیزیکی (به‌طور مثال ورود مستقیم به مرکز داده) و مکانیزم‌های دفاع نرم‌افزاری شبکه (شکستن الگوی فیلترینگ بسته‌ها از سوی دیوارآتش) عبور کند، ممکن است شانس کمی داشته باشد که بتواند از سد مکانیزم‌های رمزنگاری عبور کند. پروتکل‌های رمزنگاری از یک کد ریاضی به نام سایفر استفاده می‌کنند تا داده‌ها را به فرمتی تبدیل کنند که فقط با معکوس کردن رمز که به آن دیسایفر یا در اصطلاح رایج رمزگشایی می‌گویند قابل خواندن باشند. هدف از رمزنگاری اطلاعات ایمن‌سازی و خصوصی‌سازی آن‌ها است. دقت کنید که همه الگوهای رمزنگاری عملکرد یکسانی ندارند و برخی از آن‌ها قدرتمندتر هستند. از طرفی به دلیل آن‌که در برخی از

الگوریتم‌ها رخنه‌هایی شناسایی شده و تجهیزات سخت‌افزاری نیز پیشرفت‌های قابل ملاحظه‌ای داشته‌اند، پژوهشگران تصمیم گرفتند الگوریتم‌های رمزنگاری توسعه یافته‌ای را طراحی کنند تا ایمنی داده‌ها همچنان حفظ شود. در دنیای امنیت و به ویژه رمزنگاری، الگوریتم‌ها باید سه ویژگی مهم زیر را داشته باشند:

• محرمانگی- داده‌ها باید فقط توسط گیرنده یا در مقصد تعیین شده قابل مشاهده باشند

• یکپارچگی- داده‌ها نباید پس از ارسال از سوی فرستنده و قبل از آن‌که توسط گیرنده دریافت شوند، قابل ویرایش باشند

• دسترس‌پذیری- داده‌ها هر زمان دریافت‌کننده درخواست کرد در دسترس او باشند. این حرف بیان‌گر این موضوع است که فرستنده با موفقیت توانسته است داده‌ها را به مقصد تحویل دهد.

این سه اصل با یکدیگر ترکیب شده و مدل استاندارد امنیتی به نام CIA (محرمانگی، یکپارچگی و دسترس‌پذیری) را تشکیل می‌دهند. رمزنگاری می‌تواند در لایه‌های مختلف مدل OSI اعمال شود. اما برای آشنایی بهتر، اجازه دهید ابتدا مختصری درباره کلید رمزنگاری صحبت کرده و سپس برخی از رایج‌ترین پروتکل‌های رمزنگاری مورد استفاده برای محافظت از داده‌های ذخیره شده در شبکه یا زمانی که داده‌ها در حال انتقال هستند را بررسی کنیم.

کلید رمزنگاری

محبوب‌ترین نوع رمزنگاری، کدگذاری بیت‌های اصلی داده‌ها با استفاده از یک کلید یا یک رشته تصادفی از کارکترها است که گاهی چند مرتبه در توالی‌های مختلف ظاهر می‌شوند تا داده‌ها و شکل داده‌ها به یک الگوی منحصر به فرد کدگذاری تبدیل شود تا داده‌ها غیرقابل خواندن شوند. رشته‌ای که این‌گونه تولید می‌شود ciphertext نام دارد. کلید فوق بر مبنای مجموعه خاصی از قواعد یا الگوریتم‌ها ایجاد می‌شود. کلید رمزنگاری می‌تواند به دو بخش کلید خصوصی و کلید عمومی رمزنگاری تقسیم شود.

رمزنگاری کلید خصوصی

داده‌ها با استفاده از یک کلید واحد رمزنگاری می‌شوند که تنها فرستنده و گیرنده آن‌را می‌دانند. کلید رمزنگاری خصوصی به عنوان رمزنگاری متقارن شناخته می‌شود، زیرا همان کلید در طی رمزنگاری و رمزگشایی داده‌ها استفاده می‌شود. یک مشکل بالقوه با کلید رمزنگاری خصوصی این است که فرستنده باید به نوعی کلید را با گیرنده به اشتراک بگذارد بدون آن که جزییات کلید آشکار شود.

رمزنگاری کلید عمومی

داده‌ها با یک کلید خصوصی که تنها کاربر در مورد آن اطلاع دارد رمزنگاری شده و با یک کلید عمومی که بر مبنای محاسبات ریاضی ایجاد می‌شود و از منابع ثالثی دریافت می‌شوند رمزگشایی می‌شوند. این تکنیک یکپارچگی داده‌ها را تضمین می‌کند، زیرا کلید عمومی که فرستنده آن‌را ارسال می‌کند تنها در صورتی کار می‌کند که داده‌ها در طول مسیر دستکاری نشده باشند. در این رویکرد داده‌ها با کلید عمومی رمزنگاری شده و تنها در صورتی که با کلید خصوصی مطابقت داشته باشند رمزگشایی می‌شوند. در روش رمزنگاری کلید عمومی اصل محرمانگی اطلاعات تضمین می‌شود، زیرا تنها گیرنده مشخص شده قادر است داده‌ها را رمزگشایی کند. ترکیبی از کلید عمومی و یک کلید خصوصی به عنوان یک جفت کلید شناخته می‌شود. از آنجایی که رمزنگاری کلید عمومی نیاز به استفاده از دو کلید مختلف دارد، یکی برای رمزنگاری و دیگری برای رمزگشایی، این روش به نام رمزنگاری نامتقارن شناخته می‌شود. تکنیک فوق به دلیل سهولت و کارایی مورد توجه قرار دارد، البته تنها نکته‌ای که کاربران باید به آن دقت کنند نگه‌داری ایمن کلیدها است. یک راهکار برای حل این مشکل گواهی‌های دیجیتالی هستند. یک فرد یا کسب‌وکار می‌توانند یک گواهی دیجیتال را درخواست کنند که یک فایل کوچک حاوی اطلاعات شناسایی تأیید شده توسط کاربر و کلید عمومی کاربر است. گواهینامه دیجیتال می‌تواند توسط یک مرجع صدور گواهی دیجیتال CA سرنام certificate authority ارائه می‌شود. این مرجع می‌تواند یک شخصی حقیقی یا حقوقی باشد که گواهی‌نامه‌های کلید عمومی را صادر می‌کند. به‌کارگیری مرجع صدور گواهی دیجیتال برای مرتبط کردن کلیدهای عمومی با کاربران خاص زیرساخت کلید عمومی PKI سرنام Public-key Infrastructure نام دارد. زیرساخت کلید عمومی (PKI) مجموعه‌ای متشکل از سخت‌افزار، نرم‌افزار، افراد، خط‌مشی‌ها و چارچوب‌های مورد نیاز برای مدیریت، توزیع، استفاده، ذخیره‌سازی و ابطال گواهی‌های دیجیتال است.

نکته: رمزنگاری داده‌ها در مبحث شبکه و به ویژه امنیت کاربرد دارد و ممکن است در آزمون **نتورک‌پلاس** نیز به آن اشاره شود. پیشنهاد می‌کنم تا حد آشنایی این مبحث را دنبال کنید. برای شروع می‌توانید **به مقاله فناوری رمزگذاری چگونه از اطلاعات ما محافظت می‌کند و آیا نفوذپذیر است؟** مراجعه کنید.

حال که اطلاعات مختصری درباره رمزنگاری به دست آوردید، زمان آن فرارسیده است به سراغ پروتکل‌های ویژه رمزنگاری همچون SSL برویم که نقش مهمی در دنیای شبکه و به ویژه در زمان انتقال داده‌ها بازی می‌کند در ابتدا به سراغ پروتکل رمزنگاری IPsec می‌رویم که روی لایه شبکه کار می‌کند.

IPsec سرنام Internet Protocol Security

امنیت پروتکل اینترنت IPsec سرنام (Internet Protocol Security) بسته‌ای متشکل از پروتکل‌های رمزگذاری است که مجموعه‌ای از قواعدی که برای رمزنگاری، احراز هویت، و مدیریت کلید در زمان فرآیند انتقال داده‌ها بر مبنای پروتکل TCP / IP از آن‌ها استفاده می‌شود را تعریف می‌کند. IPsec در لایه شبکه از مدل OSI کار کرده و اطلاعات امنیتی را به سرباره همه بسته‌های آی‌پی اضافه کرده و بارداده‌ها را نیز رمزگذاری می‌کند. IPsec ارتباطات ایمن را در پنج مرحله‌ای که به آن‌ها اشاره خواهد شد ایجاد می‌کند:

1. IPsec initiation- ترافیک مهم و حائز اهمیت بر مبنای خط‌مشی‌های امنیتی تعریف شده و پس از آن فرآیند رمزگذاری IPsec آغاز می‌شود.

2. *key management*- در فرآیند مدیریت کلید، دو گره روی پارامترهای مشترک کلیدهایی که قرار است از آن‌ها استفاده کنند به توافق می‌رسند. این مرحله در درجه اول شامل دو سرویس/پروتکل زیر است:

• پروتکل مبادله کلید اینترنتی IKE (Internet Key Exchange) – در این سرویس کارهای مختلفی همچون تأیید اعتبار کلیدها انجام می‌شود. نسخه فعلی این سرویس IKEv2 نام دارد که در شماره‌های آتی به بررسی آن خواهیم پرداخت.

• پروتکل مدیریت کلید و تشکیل مجمع امنیت اینترنت Internet Security Association and Key) Management Protocol) ISAKMP – این سرویس در فرآیند مبادله کلید اینترنتی با هدف ایجاد خط‌مشی‌هایی برای مدیریت کلیدها استفاده می‌شود.

3. security negotiations – سرویس مبادله کلید اینترنت همچنین برای ایجاد پارامترهای امنیتی که برای حفاظت از داده‌ها در هنگام انتقال از آن‌ها استفاده می‌شود کاربرد دارد.

4. data transfer- پس از تنظیم پارامترها و تکنیک‌های رمزنگاری، یک کانال امن ایجاد می‌شود که می‌تواند برای انتقال ایمن تا زمانی که کانال شکسته شود استفاده شود. در این حالت داده‌ها رمزگذاری شده و سپس منتقل می‌شوند. این کانال ممکن است برای رمزگذاری سرباره احراز هویت (authentication header) AH یا رمزگذاری ESP سرنام (Encapsulating Payload Security) نیز استفاده شود. هر دو نوع رمزگذاری، یک مکانیزم تأیید اعتبار را برای بار داده بسته‌های آی‌پی از طریق به‌کارگیری تکنیک‌های کلید عمومی ارائه می‌کنند. علاوه بر این، ESP یک بسته کامل آی‌پی را با هدف افزایش امنیت رمزگذاری می‌کند.

5. termination- IPsec با هدف کم کردن چالش‌های استنتاج و نفوذ به یک ارتباط به‌طور منظم به بازبینی مجدد یک ارتباط می‌پردازد. یک ارتباط می‌تواند پیش از آن‌که جلسه فعلی به اتمام برسد، بازنگری شده و ارتباط دومرتبه برقرار شده یا خاتمه پیدا کند.

IPsec می‌تواند در یکی از دو وضعیت حالت انتقال (transport mode) که هر بسته را در بار داده و بدون دست زدن به سرآیند رمزنگاری می‌کند (اتصال دو میزبان) یا حالت تونل (tunnel mode) که هم بار داده و هم سرآیند را رمزنگاری می‌کند (روی روترها یا دستگاه‌های ارتباطی در زمینه شبکه خصوصی مجازی اجرا می‌شود) استفاده شود.

Secure Sockets Layer و Transport Layer Security

پروتکل لایه سوکت‌های امن SSL سرنام (Secure Sockets Layer) و پروتکل امنیت لایه انتقالTLS سرنام

(Transport Layer Security) هر دو با هدف رمزگذاری داده‌ها در فرآیند انتقال مبتنی بر پروتکل TCP / IP و در مواردی همچون رمزگذاری صفحات وب و اطلاعات وارد شده به فرم‌های وب، برقراری ارتباط میان سرویس گیرنده و سرور با استفاده از فناوری رمزگذاری کلید عمومی استفاده می‌شوند. دو پروتکل را می‌توان در کنار یکدیگر استفاده کرد. در این حالت دو پروتکل فوق به صورت SSL / TLS یا TLS / SSL نوشته می‌شوند. تمام مرورگرهای مدرن برای ایمن ساختن یک نشست HTTP از دو پروتکل SSL / TLS پشتیبانی می‌کنند.

شرکت نت‌اسکیپ در سال 1995 میلادی پروتکل SSL که در لایه کاربرد از آن استفاده می‌شود را توسعه داد. در سال 1999 نت‌اسکیپ کنترل کامل این پروتکل را به سازمان استانداردسازی داوطلبانه وب (IETF) واگذار کرد. سازمان IETF پروتکلی مشابه با SSL را با نام TLS نسخه 1 ارائه کرد. پروتکلی که در لایه انتقال کار می‌کند و از الگوریتم‌های رمزنگاری کمی متفاوت‌تر از SSL استفاده می‌کند. اما در اصل نسخه به‌روز شده‌ای از پروتکل SSL است. SSL در حال حاضر منسوخ شدن است و انتظار می‌رود به مرور زمان کاملا از دور خارج شده و جای خود را به پروتکل ایمن‌تر TLS بدهد. تنها دلیلی که باعث شده است از هر دو پروتکل پشتیبانی به عمل آید بحث سازگاری است. لازم به توضیح است که سازمان IETF در سال 2006 میلادی، نسخه 1.1، در سال 2008 نسخه 1.2 و در سال 2018 نسخه 1.3 پروتکل TLS را منتشر کرد.

همان‌گونه که می‌دانید، HTTP از پورت 80 و TCP استفاده می‌کند، در حالی که پروتکل HTTPS از رمزگذاری / SSL TLS و پورت TCP 443 به جای پورت 80 استفاده می‌کند. هر بار یک سرویس‌دهنده و سرور یک اتصال SSL / TLS برقرار می‌کنند، آن‌ها نشست منحصر به فردی ایجاد می‌کنند که هر دو بر سر تکنیک‌های رمزنگاری خاصی که از آن استفاده می‌کنند به توافق رسیده‌اند. این نشست به کلاینت و سرور اجازه می‌دهد به شکل محرمانه به مبادله داده‌ها بپردازند. یک نشست میان کلاینت و سرور بر مبنای یک دست‌دهی ساخته شده و یکی از چند پروتکل درون / SSL TLS و شاید مهم‌ترین آن‌ها برای این منظور استفاده می‌شود. همان‌گونه که از نامش پیدا است، پروتکل دست‌دهی به کلاینت و سرور اجازه می‌دهد خودشان را به دیگری معرفی کرده و شرایط را برای چگونگی مبادله ایمن داده‌ها آماده کنند. این رویکرد شبیکه به دست‌دهی سه وضعیتی TCP است که قبلا با آن آشنا شدید. با توجه به سناریوی یک مرورگر برای دسترسی به یک وب سایت ایمن، دست‌دهی SSL / TLS به شرح زیر عمل می‌کند:

مرحله 1 - مرورگر، در این سناریو کامپیوتر کلاینت بوده و یک پیام client_hello را به وب‌سروری می‌فرستد که حاوی اطلاعاتی درباره سطح امنیتی است که مرورگر قادر به قبول آن بوده و همچنین نوع رمزگذاری که مرورگر قادر به رمزگشایی پیام‌ها است را مشخص می‌کند. پیام client_hello یک عدد تصادفی تولید شده را منتشر کرده که شناسه کلاینت و همچنین شماره شناسایی نشست را نشان می‌دهد.

مرحله 2- سرور با یک پیام server_hello پاسخ می‌دهد. این پیام اطلاعات دریافت شده از مرورگر را تایید کرده و بر مبنای این اطلاعات شرایط لازم برای رمزگذاری را مهیا می‌کند. بسته به روش رمزگذاری پیشنهادی وب‌سرور، سرور ممکن است تصمیم بگیرد یک کلید عمومی یا یک گواهی دیجیتال برای مرورگر ارسال کند.

مرحله 3: اگر سرور از مرورگر یک گواهی درخواست کند، مرورگر آن‌را ارسال می‌کند. هر داده‌ای که مرورگر به سرور ارسال می‌کند با استفاده از کلید عمومی سرور رمزگذاری می‌شود. کلیدهای جلسه استفاده شده تنها برای این جلسه ایجاد شده و دارای ارزش هستند.

پس از اینکه مرورگر و سرور بر سر شرایط رمزنگاری توافق کردند، کانال امن ایجاد شده و تبادل اطلاعات آغاز می‌شود.

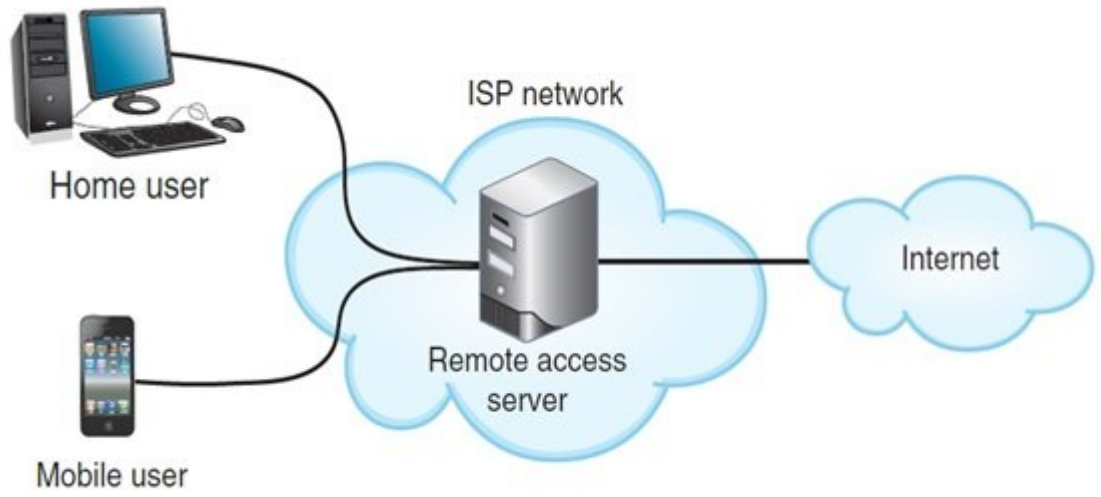
نوع خاصی از پروتکل ارتباطی مبتنی بر TLS به نام DTLS سرنام (Datagram Transport Layer Security) طراحی شده که به‌طور ویژه برای استریم کردن ارتباطات از آن استفاده می‌شود. همان‌گونه که از نامش بر می‌آید، DTLS به جای TCP از UDP استفاده می‌کند تا تاخیر را به حداقل برساند. با این حال، برنامه‌های کاربردی که از DTLS استفاده می‌کنند باید برای مرتب‌سازی مجدد بسته‌ها، کنترل جریان و قابلیت اطمینان از رویکردهای خاص خود استفاده کنند. DTLS شامل سطوح امنیتی قابل قیاس با TLS است و معمولا توسط برنامه‌های کاربردی حساس به زمان تاخیر مانند VoIP و برنامه‌های تونل‌زنی مانند VPN استفاده می‌شود.

دسترسی راه دور

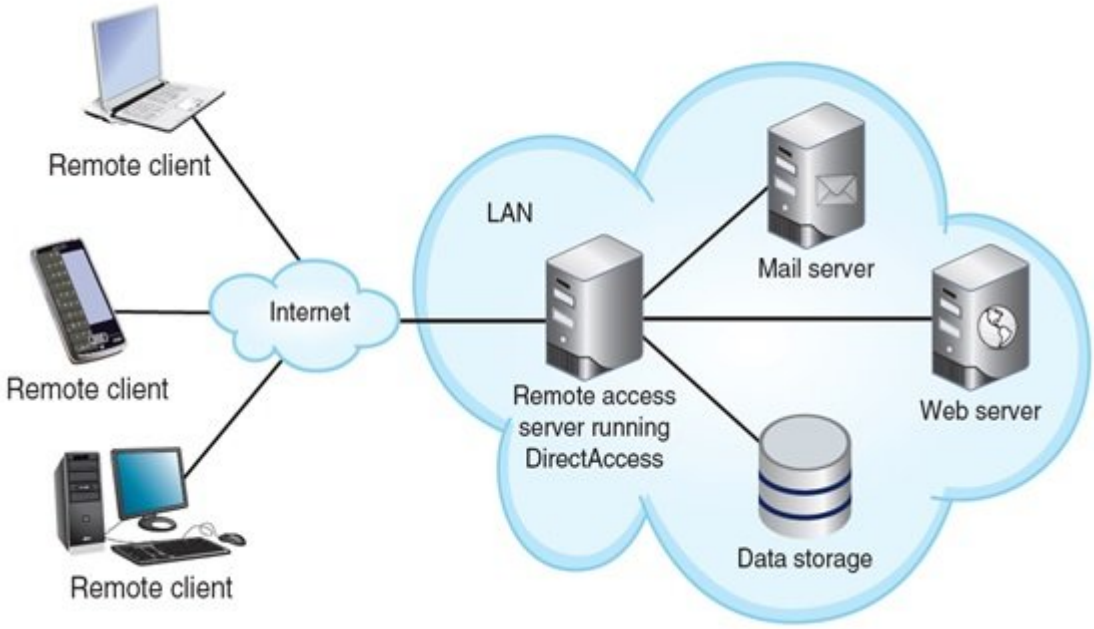
به عنوان یک کاربر از راه دور، شما می‌توانید بر مبنای فناوری دسترسی از راه دور به یک شبکه و منابع آن متصل شوید. سرویس دسترسی از راه دور به یک کلاینت اجازه می‌دهد به یک سرور، شبکه محلی یا WAN که در یک منطقه جغرافیایی مختلف قرار دارند متصل شود. پس از اتصال، یک کلاینت راه دور می‌تواند به فایل‌ها، برنامه‌ها و سایر منابع به‌اشتراک قرار گرفته همچون پرینترها یا هر نوع دستگاه کلاینت دیگری متصل شده و از آن‌ها استفاده کند. برای برقراری ارتباط و دسترسی از راه دور، کلاینت و میزبان به یک مسیر انتقال و نرم‌افزار مناسب برای تکمیل اتصال و تبادل داده‌ها نیاز دارند.

همه تکنیک‌های دسترسی از راه دور که به شبکه متصل می‌شوند، به نوعی به سرور دسترسی از راه دور RAS سرنام remote access server نیاز دارند تا یک اتصال از راه دور به دسترسی ایجاد شده و دسترسی به منابع شبکه امکان‌پذیر شود. همچنین، نرم‌افزار مربوطه باید روی سرویس گیرنده از راه دور و سرور دسترسی از راه دور برای برای برقراری ارتباط نصب شده باشد. دو نوع سرور دسترسی از راه دور وجود دارد:

• دستگاه‌های اختصاصی - دستگاه‌هایی مانند سرورهای AS5800 سیسکو که تنها به عنوان RAS بوده و برای اجرای نرم‌افزاری که برای برقراری ارتباط با سیستم‌عامل و احراز هویت کلاینت‌ها از آن استفاده می‌شود را میزبانی می‌کنند. یک ISP ممکن است از یک دستگاه اختصاصی برای تأیید اعتبار کامپیوترهای کلاینت یا روترهای خانگی برای دسترسی به منابع ISP و اینترنت استفاده کند. شکل زیر این موضوع را نشان می‌دهد.



• نرم‌افزار در حال اجرا روی سرور - سرویس دسترسی از راه دور ممکن است تحت یک سیستم‌عامل شبکه اجرا شود تا اجازه ورود به سیستم را به یک شبکه سازمانی ارائه کند. به‌طور مثال، DirectAccess سرویسی است که ابتدا در ویندوز سرور R2 2008 معرفی شد. سرویسی که می‌تواند به‌طور خودکار کاربران و کامپیوترهای راه دور را به دامنه ویندوز و منابع شبکه متصل کند. شکل زیر این مسئله را نشان می‌دهد.



روش‌های مختلفی برای دسترسی از راه دور به شبکه‌ها و منابع وجود دارد که سه مورد از رایج‌ترین این روش‌ها را در شماره آینده بررسی خواهیم کرد.

در شماره آینده آموزش **نتورک‌پلاس** مبحث محاسبات ابری را ادامه خواهیم کرد.

تاریخ انتشار:
11 اردیبهشت 1398

نشانی منبع:
https://www.shabakeh-mag.com/networking-technology/15095/%D8%A2%D9%85%D9%88%D8%B2%D8%B4-%D8%B1%D8%A7%DB%8C%DA%AF%D8%A7%D9%86-%D8%AF%D9%88%D8%B1%D9%87-%D9%86%D8%AA%D9%88%D8%B1%DA%A9%E2%80%8C%D9%BE%D9%84%D8%A7%D8%B3%D8%8C-%D8%B1%D9%85%D8%B2%D9%86%DA%AF%D8%A7%D8%B1%DB%8C%D8%8C-%D9%BE%D8%B1%D9%88%D8%AA%DA%A9%D9%84-ipsec%D8%8C-ssl-%D8%A8%D8%AE%D8%B4-45