تسلط بر مفاهیم پایه شبکه منطبق با استانداردهای بین‌المللی

آموزش رایگان دوره Network+ آشنایی با پروتکل‌های دسترسی از راه دور،FTP و... (بخش 46)

در شماره گذشته آموزش نتورک‌پلاس با انواع مختلف داده‌ها، مکانیزم‌ها و پروتکل‌هایی که برای محافظت از داده‌ها از آن‌ها استفاده می‌شود آشنا شدیم. در ادامه به‌طور اجمالی دو پروتکل پر کاربرد این حوزه را بررسی کرده و در انتها مقدمه‌ای در ارتباط با دسترسی از راه دور ارائه کردیم. همان‌گونه که وعده دادیم در این شماره جزییات بیشتری در ارتباط با دسترسی از راه دور یاد خواهیم گرفت.

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

در شماره قبلی آموزش **نتورک‌پلاس** با فناوری دسترسی از راه دور که یک کلاینت بر مبنای آن قادر است به شبکه و منابع آن دسترسی داشته باشد آشنا شدیم. همان‌گونه که اشاره کردیم روش‌های مختلفی برای دسترسی از راه دور به منابع در اختیار ما قرار دارند که سه روش دسترسی از راه دور نقطه به نقطه، شبکه اختصاصی مجازی و شبیه‌سازی ترمینال پر کاربردتر از سایر روش‌ها هستند. امنیت و حریم اختصاصی در هنگام مدیریت و استفاده از مکانیزم دسترسی از راه دور بسیار مهم است. برای این منظور، قبل از انتقال داده‌ها از طریق یک ارتباط از راه دور، داده‌ها اغلب رمزگذاری می‌شوند. برخی از پروتکل‌های دسترسی از راه دور به‌طور خاص قابلیت رمزگذاری را برای محافظت از داده‌ها ارائه می‌کنند، در حالی که برخی دیگر این‌گونه نیستند و باید پیش از ارسال داده‌ها به رمزنگاری آن‌ها بپردازیم.

پروتکل‌های دسترسی راه دور نقطه به نقطه

کلاینت‌ها و سرورهای دسترسی از راه دور برای برقراری ارتباط و تبادل اطلاعات به یک پروتکل واحد نیاز دارند. پروتکل سریال خطی اینترنت SLIP سرنام (Serial Line Internet Protocol) یکی از پروتکل‌های قدیمی این حوزه است که امروزه به ندرت استفاده می‌شود. این پروتکل از رمزگذاری پشتیبانی نکرده و تنها قادر به ارسال بسته‌های آی‌پی (و نه بسته‌های دیگر پروتکل‌های لایه شبکه) بوده و بیشتر روی ارتباطاتی همچون Dial-up یا DSL کار می‌کند. SLIP در نهایت توسط PPP به عنوان یک پروتکل ارتباطی برای دسترسی از راه دور مبتنی بر رویکرد نقطه به نقطه جایگزین شد. PPP (پروتکل نقطه به نقطه) یک پروتکل لایه پیوند داده است که به‌طور مستقیم دو نقطه انتهایی WAN را به یکدیگر متصل می‌کند. یک مثال زمانی است که یک مودم DSL یا مودم کابلی را به یک سرور در ISP متصل می‌کنید. سرآیندها و دنباله فریم‌های PPP یک فریم PPP ایجاد می‌کنند که بسته‌های لایه شبکه را کپسوله می‌کنند. فریم‌ها در مجموع فقط 8 یا 10 بایت طول دارند و تفاوت اندازه‌ها به فیلد FCS بستگی دارد.

نکته امتحانی: هنگامی که PPP روی یک شبکه اترنت (نوع اتصال اهمیتی ندارد) استفاده می‌شود، به عنوان پروتکل نظیر به نظیر روی اترنت (PPPoE) سرنام PPP over Ethernet شناخته می‌شود. به‌طور مثال، PPPoE می‌تواند برای اتصال یک کامپیوتر به مودم با استفاده از یک آداپتور شبکه اترنت و پچ کابل استفاده شود. به همین شکل PPPoA نیز پروتکل نظیر به نظیر روی ATM است (حالت انتقال آسنکرون) که یک فناوری WAN بوده و در مقاله‌های

آتی آن‌را بررسی خواهیم کرد.

شبیه‌ساز ترمینال

شبیه‌ساز ترمینال که برخی مواقع رایانش مجازی از راه دور نیز نامیده می‌شود، اجازه می‌دهد یک کاربر روی یک کامپیوتر که کلاینت نامیده می‌شود کامپیوتر دیگری که میزبان یا سرور نامیده می‌شود را بر مبنای یک ارتباط تحت شبکه کنترل کند. نرم‌افزارهای خط فرمانی شبیه به تلنت، SSH و برخی از نرم‌افزارهای دارای رابط گرافیکی همچون Remote Desktop برای ویندوز، join.me، VNC و TeamViewer از جمله نرم‌افزارهای این حوزه هستند. یک میزبان ممکن است به کلاینت‌ها مجموعه‌ای از مجوزها را تنها برای مشاهده صفحه و برنامه‌های در حال اجرا یا ویرایش داده‌هایی که درون فایل‌ها و روی هارددیسک میزبان قرار دارند تخصیص دهد. پس از اتصال، اگر به کاربر از راه دور مجوزهای سطح بالایی تخصیص داده شود کنترل ماوس و صفحه‌کلید میزبان نیز در اختیار کلاینت قرار می‌گیرد، درست مثال آن‌که کاربر به شکل فیزیکی در مقابل صفحه‌نمایش کامپیوتر میزبان قرار گرفته است. به‌طور مثال، کارمند یک شرکت می‌کند از طریق لپ‌تاپ و قابلیت اتصال از راه دور به دسکتاپ کامپیوتر خودش در شرکت متصل شود. به این ترتیب، او می‌تواند از راه دور و از طریق به‌کارگیری نرم‌افزارهایی شبیه به اکسل به ویرایش و به‌روزرسانی اسناد خود بپردازد.

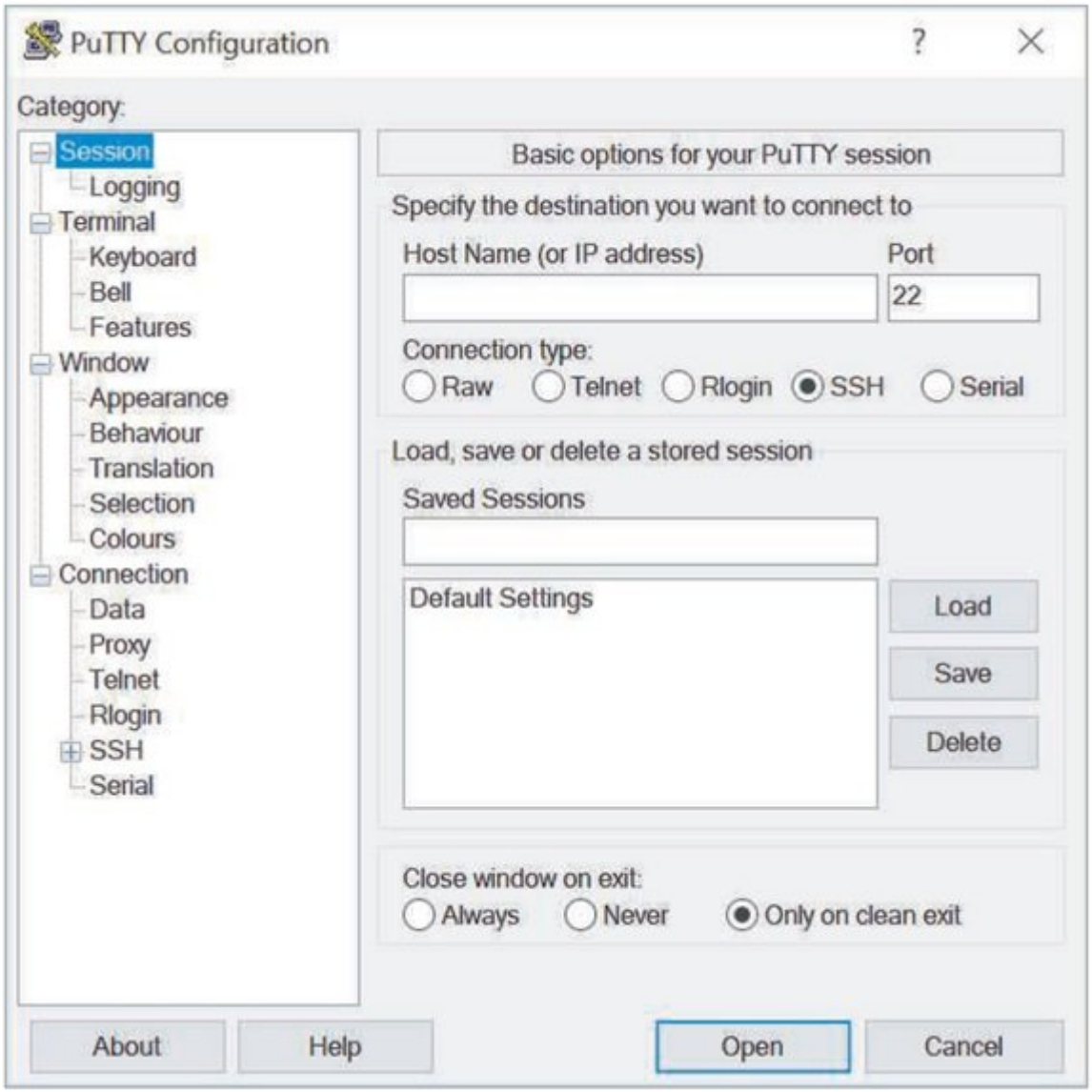
تلنت

همان‌گونه که یاد گرفتید، Telnet یک ابزار شبیه‌ساز ترمینال است که توسط برنامه‌های کاربردی سرویس‌گیرنده/سرویس‌دهنده Telnet استفاده شده و به مدیر یا کاربری اجازه می‌دهد از راه دور به کنترل یک کامپیوتر بپردازند. به‌طور مثال، اگر مدیر شبکه‌ای هستید که در یک ساختمان اداری قرار دارید و مجبور هستید تنظیمات روتر را در ساختمان دیگری تغییر دهید، شما می‌توانید از Telnet برای دسترسی به روتر استفاده کرده و دستورات را برای تغییر تنظیمات پیکربندی اجرا کنید. با این حال، تلنت برای برقراری یک ارتباط به منظور انتقال اطلاعات حساس مناسب نیست، زیرا امنیت آن در حد پایینی است و از رمزنگاری داده‌ها استفاده نمی‌کند.

Secure Shell

پروتکل پوسته امن SSH سرنام (Secure Shell) مجموعه‌ای از پروتکل‌هایی است که هر دو رویکرد احراز هویت و رمزگذاری را ارائه می‌کند. با استفاده از SSH، شما می‌توانید به‌طور ایمن به یک میزبان متصل شده، دستورات را روی میزبان اجرا کرده و فایل‌ها را به میزبان یا از میزبان کپی کنید. SSH در مدت زمان یک نشست داده‌های در حال تبادل را رمزنگاری می‌کند. این پروتکل در برابر دسترسی‌های غیر مجاز به یک میزبان، جعل آی‌پی، رهگیری داده‌ها در مدت زمان انتقال (حتی زمانی که داده‌ها از میزبان‌های میانی عبور می‌کنند) و DNS spoofing از داده‌ها محافظت می‌کند. بسته به نسخه SSH این پروتکل ممکن است از سه‌گانه الگوریتم‌های DES، AES، Blowfish یا سایر الگوریتم‌های کمتر رایج رمزنگاری استفاده کند. دوره سکوریتی‌پلاس به شکل دقیق‌تری مباحث این پروتکل را تشریح می‌کند.

SSH توسط سازمان SSH Communications Security توسعه داده شده است. شما برای استفاده از این پروتکل باید مجوز مربوطه را خریداری کنید، با این حال، نسخه متن‌باز آن همچون OpenSSH برای اکثر پلتفرم‌های کامپیوتری در دسترس است. برای ایجاد یک اتصال امن، SSH باید در هر دو طرف سرویس‌دهنده و سرور اجرا شود. همانند تلنت، سرویس گیرنده SSH ابزاری است که می‌تواند در محیط خط فرمان در پلتفرم‌های ویندوزی، لینوکیسی یا یونیکس اجرا شود. البته نسخه‌های مبتنی بر رابط گرافیکی نیز در دسترس قرار دارند. مجموعه پروتکل‌های SSH با تمامی توزیع‌های جدید یونیکس و لینوکس و با MacOS Server و MacOS ارائه شده‌اند، اما کامپیوترهای ویندوزی باید میان‌افزار کلاینت SSH شبیه به PuTTY که در سایت putty.org قرار دارد را دانلود کنند. اگر در شکل زیر دقت کنید مشاهده می‌کنید که PuTTY از انواع مختلفی از اتصالات همچون SSH و تلنت پشتیبانی می‌کند.



PuTTY همچنین از طریق خط فرمان نیز اجرا می‌شود. شما می‌توانید از SSH برای تعیین اعتبار گذرواژه‌ها یا احراز هویت با استفاده از کلیدهای عمومی و اختصاصی استفاده کنید. برای احراز هویت با استفاده از کلیدها، شما ابتدا باید یک کلید عمومی و یک کلید اختصاصی روی ایستگاه کاری کلاینت خودتان با اجرای دستور ssh-keygen (این‌کار از طریق برنامه گرافیکی SSH نیز امکان‌پذیر است) ایجاد کنید. کلیدها در دو فایل مختلف رمزگذاری شده روی هارد دیسک ذخیره می‌شوند. در مرحله بعد، باید کلید عمومی در یک فایل تایید هویت قرار گرفته و به میزبانی که می‌خواهید به آن متصل شوید انتقال پیدا کند. هنگامی که شما از طریق SSH به میزبان متصل می‌شوید، کلاینت و میزبان کلیدهای عمومی را مبادله کرده و اگر فرآیند تأیید هویت را به درستی پشت سربگذارند، اتصال کامل می‌شود. SSH به پورت 22 که به خوبی قابل پیکربندی است گوش می‌کند. این قابلیت پیکربندی به شما اجازه می‌دهد از میان انواع مختلف روش‌های رمزنگاری گزینه مدنظر خود را انتخاب کرده و همچنین پیکربندی پورت فورواردینگ را به گونه‌ای انجام دهید که ترافیک شبکه را به سمت پورت ایمن شده با SSH هدایت کنید. این رویکرد به شما این امکان را می‌دهد که از SSH برای کارهای بیشتری نسبت به یک لاگین ساده به میزبان و ویرایش فایل‌ها استفاده کنید. با پورت فورواردینگ، شما می‌توانید ترافیک HTTP با یک وب‌سرور را از طریق یک اتصال ایمن SSH مدیریت کنید.

Remote Desktop Protocol و Virtual Network Computing

اگر به خاطر داشته باشید به شما گفتیم که پروتکل رومیزی از راه دور RDP سرنام (Remote Desktop Protocol) یک پروتکل اختصاصی ارائه شده از سوی مایکروسافت است. پروتکلی که ابزارهای Windows Remote Desktop و Remote Assistance client/server برای اتصال به یک کامپیوتر و کنترل از راه دور کامپیوتر از آن استفاده می‌کنند. به‌طور مشابه، VNC سرنام (Virtual Network Computing یا Virtual Network Connection)

از پروتکل چندسکویی RFB سرنام (remote frame buffer) برای کنترل از راه دور یک ایستگاه کاری یا سرور استفاده می‌کند. VNC کندتر از Remote Desktop بوده و نیاز به پهنای باند بیشتری دارد. با این حال، به دلیل این‌که VNC متن‌باز است، بسیاری از شرکت‌ها نسخه‌های خاص خود را بر مبنای این پروتکل توسعه داده‌اند. نرم‌افزارهایی که قادر به انجام کارهای زیر هستند:

- اجرای سیستم‌عامل روی کامپیوترهای کلاینت
- دسترسی از راه دور به کامپیوترها، تبلت‌ها و گوشی‌های هوشمند
- کنترل از راه دور تجهیزات رسانه‌ای و سامانه‌های نظارتی

مدیریت خارج از باند

Telnet، SSH، RDP، VNC و مدیریت یک آدرس اینترنتی (URL) همگی با اتکا بر زیرساخت جاری شبکه به مدیر شبکه اجازه می‌دهند از راه دور به کنترل یک دستگاه بپردازد. قبل از آن‌که مدیر بتواند دستگاه‌ها را به این شکل پیکربندی کند، دستگاه‌ها باید بوت شده و نرم‌افزار پیکربندی از قبل روی آن‌ها نصب شده باشد. این فرآیند، "مدیریت درون گروهی" نام داشته و اساسا قابلیت‌های عیب‌یابی را محدود می‌کند. با این وجود، مدیریت خارج از باند با اتکا بر یک اتصال اختصاصی (یا سیم یا بی سیم) بین کامپیوتر مدیر شبکه و هرگونه دستگاه مهم شبکه همچون روتر، دیوارآتش، سرور، منبع تغذیه، برنامه‌ها و دوربین‌های امنیتی کار می‌کند. ارتباطات ویژه به مدیران شبکه اجازه می‌دهد از راه دور:

- دستگاهی را روشن کنند
- تنظیمات میان‌افزار را تغییر دهند
- سیستم‌عامل را دومرتبه نصب کنند
- بر حس‌گرهای سخت‌افزاری نظارت داشته باشند
- به عیب‌یابی مشکلات راه‌اندازی بپردازند
- دسترسی کاربران شبکه به عملکردهای مدیریتی را محدود کنند
- دستگاه‌های تحت شبکه حتا زمانی که سایر قسمت‌های شبکه در دسترس نیستند را مدیریت کنند

راه‌حل‌های مدیریت خارج از باند مجموعه‌ای از گزینه‌ها، از توانایی راه‌اندازی مجدد گرفته تا مدیریت کامل یک دستگاه را شامل می‌شوند. یک کارت مدیریت کنترل از راه دور به پورت کنسول دستگاه شبکه متصل شده یا گاهی اوقات کارت کنترل از راه دور به شکل از پیش ساخته شده درون دستگاه قرار گرفته است. یک مودم دایال‌آپ از طریق یک خط تلفن سیمی یا از طریق یک اتصال سلولی - ممکن است به دستگاهی متصل شود تا در صورت بروز مشکلات حاد برای شبکه همچون خاموش شدن کامل شبکه دسترسی به نسخه پشتیبان CLI را فراهم کند. یک دستگاه واحد، مانند یک کنسول سرور یا کنسول روتر می‌توانند یک مدیریت متمرکز روی تمام دستگاه‌های مرتبط با شبکه را ارائه کنند.

دسترسی به فایل از راه دور

درست است به لحاظ فنی شکلی از شبیه‌سازی ترمینال نیست، اما پروتکل انتقال فایل (FTP) دسترسی از راه دور به فایل‌ها را فراهم می‌کند. اکنون که اطلاعات بیشتری در مورد چگونگی رمزگذاری و انتقال داده‌ها به دست آورده‌اید، بهتر است با برخی از گزینه‌های دسترسی از راه دور به فایل‌ها از طریق پروتکل FTP آشنا شوید. اگر به خاطر داشته باشید به شما گفتیم که FTP ابزاری است که می‌تواند فایل‌ها را به/از یک کامپیوتر میزبان با استفاده از نرم‌افزار سرور FTP انتقال دهد. در دنیای شبکه سه فناوری مرتبط با FTP وجود دارند که به شرح زیر هستند:

- FTPS سرنام (FTP Security یا FTP Secure) – یک لایه حفاظتی مضاعف برای FTP ارائه کرده که این لایه

محافظ از پروتکل SSL / TLS برای رمزگذاری کانال و داده استفاده می‌کند. همان‌گونه که پیش‌تر اشاره کردیم FTP به پورت 21 که یک کانال فرمان است گوش می‌دهد. داده‌ها از طریق پورت 20 که کانال داده‌ها است انتقال پیدا می‌کنند. FTPS معمولا به گونه‌ای پیکربندی می‌شود که شبیه به FTP به پورت 21 گوش دهد، با این وجود به دو کانال داده‌ای هم نیاز دارد. به‌طور پیش‌فرض کانال‌های داده‌ای در پورت‌های 989 و 990 قرار دارند. با این حال، FTPS نیز می‌تواند به گونه‌ای پیکربندی شود که در محدوده از پیش تعریف شده به پورت‌های داده‌ای دسترسی داشته و با آن پورت‌ها ارتباط برقرار کند. شما می‌توانید برنامه vsftpd که پیش‌تر با آن آشنا شدید را برای پشتیبانی از FTPS پیکربندی کنید، زیرا هر دو بر اساس استانداردهای اصلی FTP هستند.

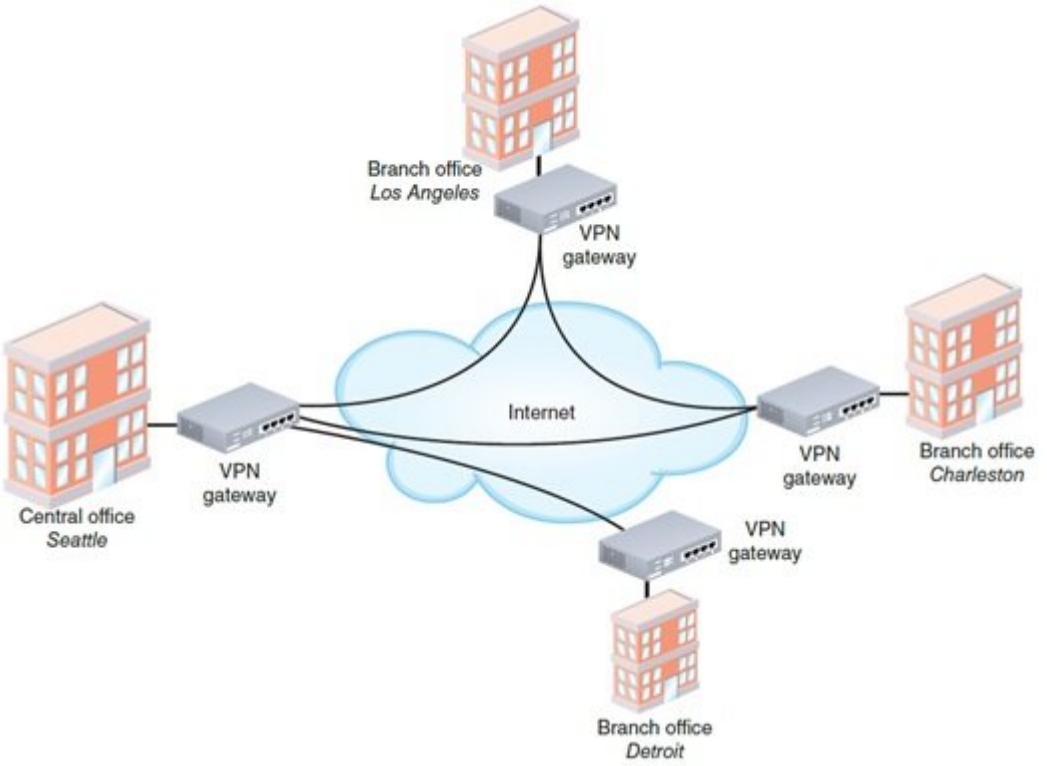
• SFTP سرنام (FTP Secure) –پروتکلی برای انتقال فایل‌ها است که بر مبنای پروتکل SSH دو رویکرد رمزگذاری و احراز هویت را ارائه می‌کند. دقت کنید SFTP یک پروتکل توسعه یافته از پروتکل SSH است و نباید آن‌را یک پروتکل توسعه یافته از FTP توصیف کنید. برخلاف FTP یا FTPS که از یک کانال کنترل و یک یا دو کانال داده استفاده می‌کنند، SFTP تنها از یک اتصال استفاده کند. در این پروتکل ارتباطات وارد و خارج شونده به آن معمولا پیکربندی می‌شوند. این پروتکل برای تبادل اطلاعات از پورت 22 پروتکل SSH استفاده می‌کند. SFTP و FTPS با یکدیگر ناسازگار هستند. در حالی که SFTP از واژگان مشابهی برای vsftpd استفاده می‌کند، اما این دو استاندارد نیز با یکدیگر سازگاری ندارند. با این حال، SFTP از سوی سرورهای لینوکس و یونیکس پشتیبانی می‌شود.

• TFTP سرنام (Trivial FTP) - نسخه ساده FTP است که هیچ‌گونه احراز هویت یا امنیتی در زمان انتقال فایل‌ها ارائه نکرده و از پروتکل UDP در لایه انتقال برای تبادل داده‌ها استفاده می‌کند. (برعکس FTP که بر مبنای پروتکل TCP در لایه انتقال کار می‌کند). TFTP نیاز به حافظه بسیار کمی دارد و اغلب توسط دستگاه‌های پشت صحنه برای انتقال فایل‌های بوت یا فایل‌های پیکربندی استفاده می‌شود. در نتیجه پروتکل فوق برای برقراری ارتباط ایمن در اینترنت مناسب نیست، کاربران نمی‌توانند به اطلاعات دایرکتوری دسترسی پیدا کنند و محدودیت انتقال فایل 4 گیگابایت را دارد. TFTP به پورت 69 گوش می‌دهد و یک کانال داده‌ای برای هر ارتباط ایجاد می‌کند.

Virtual Private Network

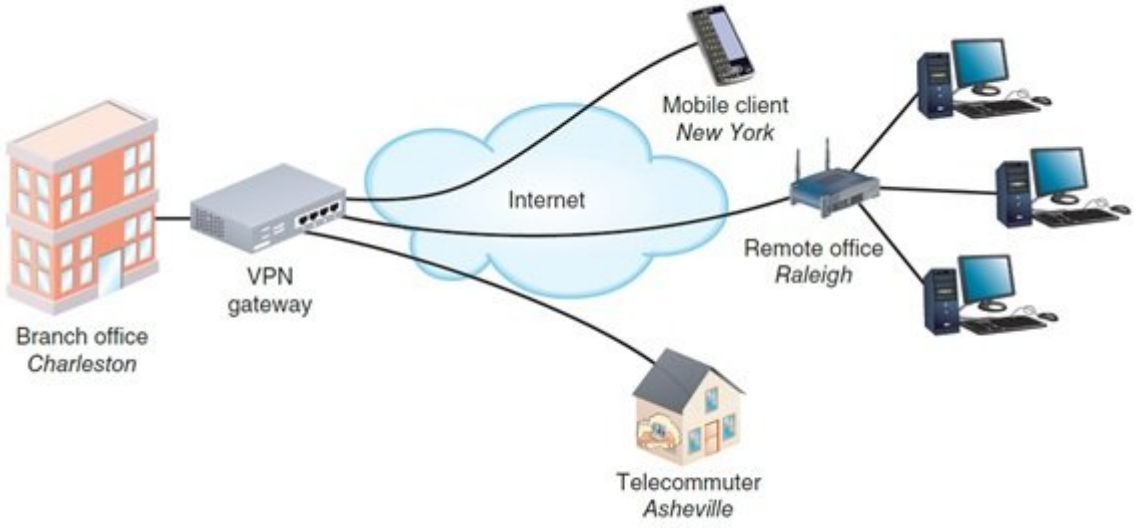
یک شبکه اختصاصی مجازی یا به اختصار VPN یک ارتباط رمزگذاری شده شبکه‌ای را ارائه می‌کند. یک ارتباط اختصاصی که از ابتدا تا انتهای مسیر برای دسترسی به یک شبکه راه دور همه چیز را رمزگذاری می‌کند. شبکه اختصاصی مجازی گاهی اوقات به عنوان یک تونل نیز شناخته می‌شود. به‌طور مثال، یک ارائه‌دهنده خدمات بیمه از شبکه‌های اختصاصی مجازی استفاده می‌کند تا به سایر دفاتر عامل خود را در سراسر کشور اجازه دهد با پایگاه‌های داده‌ای دفتر مرکزی در ارتباط باشند. با اساس تنوع نقاط انتهایی که به شبکه‌های اختصاصی متصل می‌شوند این شبکه‌ها به‌طور خلاصه به سه مدل client-to-site VPN، site-to-site VPN و host-to-host VPN طبقه‌بندی می‌شوند.

• شبکه اختصاصی مکان به مکان site-to-site VPN- تونل‌ها چندین مکان درون WAN را به یکدیگر متصل می‌کنند، شبیه به آن‌چه در تصویر زیر نشان داده شده است.



در هر مکان، یک گیت‌وی شبکه اختصاصی مجازی در لبه هر شبکه محلی یک ارتباط امن را ارائه می‌کند. هر گیت‌وی شامل یک روتر یا سرور دسترسی از راه دور همراه با نرم‌افزار شبکه اختصاصی مجازی نصب شده‌ای است که فرآیند رمزگذاری و کپسوله کردن داده‌ها به منظور تبادل درون تونل را امکان‌پذیر می‌کنند. در همین حال، کلاینت‌ها، سرورها و سایر میزبان‌ها در شبکه‌های محلی محافظت شده از طریق گیت‌وی‌های شبکه اختصاصی مجازی به شرطی که همگی روی شبکه یکسانی قرار داشته باشند با یکدیگر در ارتباط هستند. در این مدل شبکه‌های اختصاصی هر مکان باید یک آدرس آی‌پی عمومی ایستا در اختیار داشته باشد.

• شبکه اختصاصی مجازی (client-to-site)، این شبکه‌ها که به نام host-to-site یا remote-access VPN نیز شهرت دارند بر پایه این اصل کار می‌کنند که یک سرور شبکه اختصاصی مجازی در مرکز زیرساخت قرار گرفته و کاربران می‌توانند از هر مکانی با سرور فوق از طریق VPN ارتباط برقرار کرده و اطلاعات را به شکل ایمن دریافت کرده یا ارسال کنند. شکل زیر نحوه عملکرد این مدل را نشان می‌دهد. هر کلاینت را ه دور روی یک چنین مدلی باید نرم‌افزار شبکه اختصاصی مجازی را برای اتصال به گیت‌وی شبکه اختصاصی مجازی اجرا کند.



• host-to-host VPN- دو کامپیوتر یک تونل را با هدف ایجاد یک شبکه اختصاصی مجازی میان خودشان به شکل مستقیم ایجاد می‌کنند. در این مدل هر دو کامپیوتر باید نرم‌افزار مناسب را نصب کرده باشند، اما دو کامپیوتر به عنوان یک دروازه برای سایر میزبان‌ها در شبکه‌های مرتبط به ایفای نقش نخواهند پرداخت. در یک شبکه اختصاصی مجازی میزبان به میزبان، معمولا مکانی که اتصال VPN را دریافت می‌کند (مانند یک شبکه خانگی) نیاز به یک آدرس آی‌پی عمومی ایستا دارد. البته روش دیگری نیز برای دسترسی به این شبکه‌ها وجود دارد که بر مبنای پرداخت حق اشتراک و عضویت در سرویسی شبیه به Dynamic DNS by Oracle است که به‌طور خودکار اطلاعات IP پویا را برای مشترکین ردیابی می‌کند. برای اطلاعات بیشتر درباره شبکه‌های اختصاصی مجازی به مقاله Virtual Private Network (VPN): Everything You Need to Know مراجعه کنید.

نکته: با توجه به این‌که در آزمون نتورک‌پلاس و همچنین دوره‌های سیسکو مبحث شبکه‌های اختصاصی مجازی به شکل جدی مورد توجه قرار می‌گیرد، پیشنهاد می‌کنم از منابع دیگری برای کسب اطلاعات بیشتر در این خصوص استفاده کنید.

در شماره آینده آموزش **نتورک‌پلاس** مبحث شبکه‌های اختصاصی مجازی را ادامه خواهیم کرد.

تاریخ انتشار:
14 اردیبهشت 1398

نشانی منبع:
https://www.shabakeh-mag.com/networking-technology/15150/%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-network-%D8%A2%D8%B4%D9%86%D8%A7%DB%8C%DB%8C-%D8%A8%D8%A7-%D9%BE%D8%B1%D9%88%D8%AA%DA%A9%D9%84%E2%80%8C%D9%87%D8%A7%DB%8C-%D8%AF%D8%B3%D8%AA%D8%B1%D8%B3%DB%8C-%D8%A7%D8%B2-%D8%B1%D8%A7%D9%87-%D8%AF%D9%88%D8%B1%D8%8Cftp-%D9%88