دانشکده مهندسی کامپیوتر

آزمایشگاه شبکه‌های کامپیوتری

فعالیت پژوهشی گزارش دوم

عنوان آزمایش : آشنایی با شبکه‌های خصوصی مجازی
Virtual Private Network (VPN)

دکتر بردیا صفایی

سارا آذرنوش — ۹۸۱۷۰۶۶۸

کهبد آئینی — ۹۸۱۰۱۲۰۹

پارسا محمدیان — ۹۸۱۰۲۲۸۴

۱۶ اسفند ۱۴۰۲

فهرست مطالب

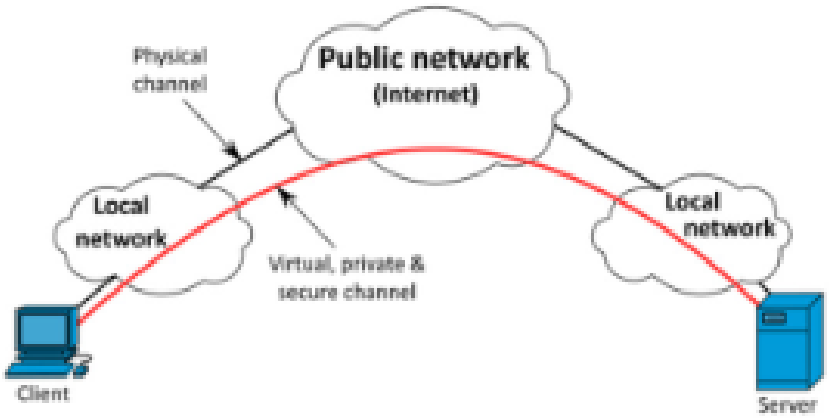
۱ توضیح پروژه

۲ خلاصه‌ی مقاله‌ی مروری در حوزه‌ی VPN

در این پروژه تصمیم داریم مرور و پژوهشی در حوزه‌ی شبکه‌های خصوصی مجازی یا Virtual Private Network (VPN) داشته باشیم.
روند انتخاب این حوزه از شبکه‌های اینترنتی به عنوان موضوع این پژوهش، بارش فکری اعضای گروه بوده. پس از انتخاب فیلد کلی پژوهش به انتخاب مقاله از بین گزینه‌های مد نظر خواهیم پرداخت.
همانطور که ذکر شد حوزه‌ی اصلی این پژوهش شبکه‌های خصوصی مجازی می‌باشد و مقالات و مقاله‌های مروری از این بخش انتخاب شده‌اند. از کلمات کلیدی این پژوهش می‌توان VPN, Tunneling, Protocols, IPsec, Firewall, L2TP نام برد.

۳ Vpn

شبکه های خصوصی مجازی (Virtual Private Networks)
VPN یک شبکه خصوصی است که در یک زیرساخت شبکه عمومی مانند اینترنت جهانی ساخته شده است.
یک شبکه شامل هر تعداد دستگاهی است که می توانند از طریق روش های دلخواه ارتباط برقرار کنند. دستگاه هایی از این نوع شامل رایانه ها، چاپگرها، روترها و غیره هستند و ممکن است در مکان های جغرافیایی متنوعی قرار گیرند. روش‌هایی که در آنها ممکن است ارتباط برقرار کنند، بسیار زیاد است، زیرا تعداد بیشماری دستگاه وجود دارد.
در ساده‌ترین تعریف، «خصوصی» به این معناست که ارتباطات بین دو (یا چند) دستگاه، به نوعی مخفی است (این که دستگاه‌هایی که در ماهیت «خصوصی» ارتباطات شرکت نمی‌کنند، در محتوای ارتباطی محرمانه نیستند.)
مجازی به معنی شبیه سازی شده است. انجام کارکردهای چیزی که واقعاً وجود ندارد.



۱.۳ تاریخچه

فناوری اجرای VPN ها مدتی است که وجود داشته است. منشا آنها را می توان در مدار مجازی یافت. پیاده سازی مدارهای مجازی در شبکه های با اتصال بالا و همچنین مقرون به صرفه بودن آسان است. مدار مجازی در ابتدا در اواخر دهه هفتاد و اوایل دهه هشتاد تولید شد.
ساختار اصلی مدار مجازی ایجاد یک مسیر منطقی از پورت مبدأ به درگاه مقصد است. این مسیر ممکن است پرش های زیادی را بین مسیریاب ها برای تشکیل مدار ترکیب کند. مسیر نهایی و منطقی یا مدار مجازی به همان شیوه ای که ارتباط مستقیم بین دو پورت برقرار می کند عمل می کند.
به این ترتیب، دو برنامه می توانند از طریق یک شبکه مشترک ارتباط برقرار کنند.
فناوری مدارهای مجازی با اضافه شدن تجهیزات رمزگذاری به سیستم های روتر پیشرفت کرد. این تجهیزات جدید اطلاعات را بین پورت های مدار مجازی رمزگذاری می کرد. این بدان معناست که مهاجمان نمی توانند به اطلاعات در حال انتقال بین نهادهای ارتباطی دسترسی داشته باشند.
بعدها فناوری های امنیتی دیگری مانند احراز هویت توکن اضافه شد. متأسفانه خطوط ارتباطی همچنان برای حمله باز بودند و این منجر به توسعه ارتباطات ایمن از طریق یک شبکه عمومی، VPN شد.

۲.۳ ساختار

سیستم VPN معمولی در درجه اول از تونل ها و گاهی اوقات فایروال ها و سرورهای پراکسی استفاده می کند.

۳.۳ tunnel

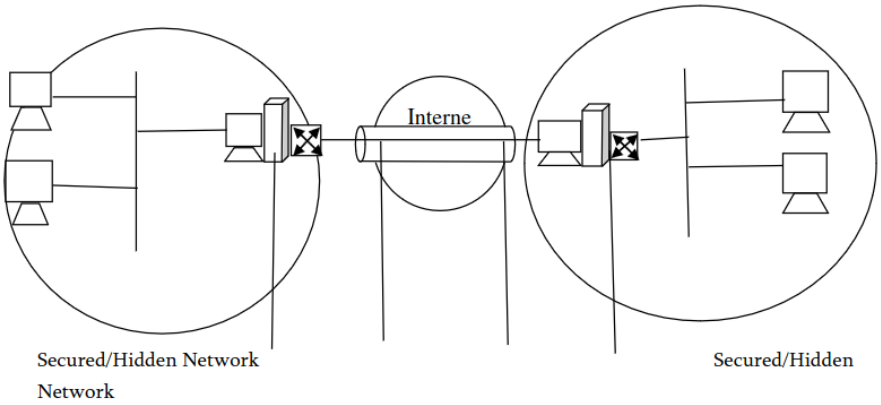
تونل سازی یا کپسوله سازی تکنیکی برای بسته بندی یک بسته شبکه در داخل بسته دیگر است. بسته محصور شده بسته تونلی شده و بسته بیرونی، بسته بندی، بسته حمل و نقل نامیده می شود. تمام اطلاعات بسته در پایین ترین سطح رمزگذاری می شود که سطح پیوند مدل OSI است.
مانند VPN ها، مفهوم کپسوله سازی برای سال ها در دسترس بوده است. از آن برای پل زدن بخش هایی از اینترنت که دارای قابلیت ها یا خط مشی های متفاوتی هستند استفاده شده است. این تونل به عنوان یک روتر در بالای پروتکل اینترنت عمل می کند.
روش کپسوله سازی بسیار ساده است. یک هدر IP خارجی به هدر اصلی اضافه می شود و بین این دو هدر اطلاعات امنیتی مخصوص تونل قرار دارد. هدر بیرونی منبع و مقصد یا "نقاط پایانی" تونل را مشخص می کند در حالی که هدر داخلی فرستنده اصلی و گیرنده بسته را مشخص می کند.

۴.۳ VPN access Remote

اتصال VPN با دسترسی از راه دور توسط یک سرویس گیرنده دسترسی از راه دور ایجاد می شود. کلاینت دسترسی از راه دور یک کاربر کامپیوتری است که از یک مکان راه دور به یک شبکه خصوصی متصل می شود. سرور VPN دسترسی به منابع شبکه ای را که سرور VPN به آن متصل است، فراهم می کند.
بسته های ارسال شده از طریق اتصال VPN از مشتری VPN منشا می گیرند. سرویس گیرنده VPN خود را به سرور VPN احراز هویت می کند و برای احراز هویت متقابل، سرور VPN خود را به مشتری VPN احراز هویت می کند.

VPN Site-to-site ۵.۳

اتصال VPN سایت به سایت دو بخش از یک شبکه خصوصی یا دو شبکه خصوصی را به هم متصل می کند.
به عنوان مثال، این به یک سازمان اجازه می دهد تا با دفاتر جداگانه، یا با سازمان های دیگر، از طریق اینترنت ارتباط مسیریابی داشته باشد. یک اتصال VPN روت شده در سراسر اینترنت به طور منطقی به عنوان یک پیوند اختصاصی شبکه گسترده (WAN) عمل می کند.



نحوه ی کار ۶.۳

برای استفاده از اینترنت به عنوان یک شبکه گسترده خصوصی، سازمان ها ممکن است مجبور باشند بر دو مانع اصلی غلبه کنند.
اول اینکه، شبکه ها اغلب با استفاده از پروتکل های مختلفی مانند IPX و NetBEUI ارتباط برقرار می کنند، اما اینترنت فقط می تواند ترافیک IP را مدیریت کند. بنابراین، VPN ها ممکن است نیاز به ارائه راهی برای انتقال پروتکل های غیر IP از یک شبکه به شبکه دیگر داشته باشند.
دوم، بسته‌های داده‌ای که به اینترنت سفر می‌کنند در متن شفاف منتقل می‌شوند. در نتیجه، هر کسی که بتواند ترافیک اینترنت را ببیند، می‌تواند داده‌های موجود در بسته‌ها را نیز بخواند. اگر شرکت‌ها بخواهند از اینترنت برای انتقال اطلاعات مهم و محرمانه تجاری استفاده کنند، این به وضوح یک مشکل است.
VPN ها با استفاده از استراتژی به نام تونل سازی بر این موانع غلبه می کنند. به جای اینکه بسته ها در فضای باز از اینترنت عبور کنند، بسته های داده ابتدا برای امنیت رمزگذاری می شوند و سپس توسط VPN در یک بسته IP محصور می شوند و از طریق اینترنت تونل می شوند. برای نشان دادن مفهوم، فرض کنید ما NetWare را در یک شبکه اجرا می کنیم، و یک کلاینت در آن شبکه می خواهد به یک سرور NetWare راه دور متصل شود.

ریسک ها و تهدیدها ۷.۳

امنیت از مهم ترین ویژگی ها است که باید نگهداری شود و مورد خطرات بسیاری مانند زیر قرار میگیرد.

۱.۷.۳ احراز هویت کاربران معتبر

احراز هویت کاربر در VPN قوی نیست. از آنجایی که اتصال VPN توسط کاربران مجاز برقرار می شود، فرض بر این است که کاربران در VPN کاربران تأیید شده هستند. به دلیل این آسیب‌پذیری، دسترسی غیرمجاز به شبکه وجود خواهد داشت و ممکن است سرقت داده، از دست دادن داده‌ها و غیره رخ دهد.

۲.۷.۳ خطرات در سمت مشتری

کاربران مشتری ممکن است دو اتصال داشته باشند، یعنی اتصال اینترنت و اتصال VPN به یک شبکه خصوصی. این امر خطر و تهدیدی را برای شبکه خصوصی ایجاد می کند، زیرا کاربران شبکه خصوصی را در معرض شبکه عمومی، که اینترنت است، قرار می دهند. یک سیستم کلاینت همچنین ممکن است از نظر امنیت در شبکه با یک سیستم در معرض خطر مرتبط باشد.

۳.۷.۳ آلودکی های ناشی از ویروس یا بدافزار

اگر یک سیستم کلاینت توسط ویروس یا بدافزار آلوده شود، کل شبکه برای حمله فوری در معرض خطر قرار می گیرد. مهاجم ممکن است بتواند رمز عبور اتصال VPN را بدزدد. ویروس یا بدافزار موجود در یک سیستم کلاینت ممکن است به صورت سیستمی به سیستم های دیگر در شبکه سرایت کند و در نتیجه شبکه را آسیب پذیر و مستعد خطر کند. بنابراین، یک سیستم ضد ویروس موثر باید در شبکه گنجانده شود.

۴.۷.۳ برنامه‌های قدیمی

این برنامه‌ها برنامه‌هایی هستند که معمولاً برای اتصال سرورها/سرویس‌های شبکه مختلف بدون هیچ گونه ممیزی یا به‌روزرسانی نسخه مانند Putty و غیره استفاده می‌شوند. تقریباً هر کاربر ویندوزی که روی تنظیمات سرور کار می‌کند با این برنامه‌ها آشنا است. با این حال، سران فناوری اطلاعات کمترین نگرانی را در مورد نگرانی‌های امنیتی آن دارند، نسخه‌ای که استفاده می‌شود، از سایت‌های قانونی دانلود می‌شود، یا این است که درهای پشتی را باز می‌کند و به سازمان‌های مادر یا هکرها امتیاز می‌دهد. این یکی از رایج‌ترین راه‌ها برای ربودن VPN است و می‌تواند از هر منبعی که کاربر نهایی یک سازمان به آن دسترسی دارد، سوء استفاده کند.

۸.۳ پروتکل های امنیت

یک VPN اتصال به میزبان های پایانی یا زیرشبکه هایی که به عنوان اعضای VPN شناسایی شده اند را فراهم می کند. VPN برای اینکه یک شبکه موثر باشد، الزامات زیر را برآورده می کند.

۱.۸.۳ Authentication

VPN با ارائه احراز هویت داده ها، فرستنده را تأیید می کند .

۲.۸.۳ Integrity Data

داده ها در حین انتقال تغییر یا تغییر نمی کنند.

Confidentiality ۳.۸.۳

داده ها به گونه ای رمزگذاری می شوند که داده ها برای سایر کاربران شبکه شفاف شود. داده ها را می توان فقط فرستنده و گیرنده مشاهده کرد.

Protection Replay ۴.۸.۳

محافظت از پخش مجدد: VPN تضمین می کند که مهاجمان نمی توانند داده ها را رهگیری کرده و در زمان دیگری پخش کنند.

Interoperability ۵.۸.۳

قابلیت همکاری با سایر شبکه های VPN به دلیل فناوری های مبتنی بر استاندارد مورد استفاده در VPN امکان پذیر است.

۹.۳ انواع

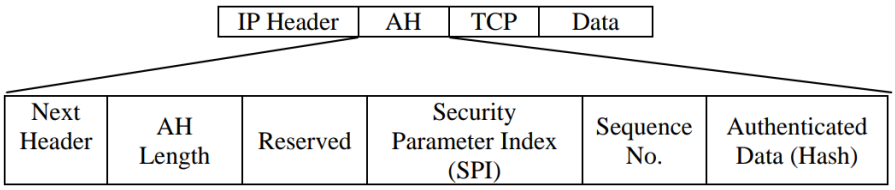
OVPN(Optical Virtual Private Networks) ۱.۹.۳

خدماتی را در قالب اتصال نوری به مشتری ارائه می دهد که انتظار می رود یکی از کاربردهای اصلی در شبکه های نوری آینده باشد. OVPN می تواند رویکرد مطلوبی برای تحقق خدمات شبکه خصوصی مجازی (VPN) نسل بعدی باشد.
انتظار می رود که آنها یکی از کاربردهای اصلی در شبکه های نوری آینده باشند. بنابراین، over OVPN IP (پروتکل اینترنت)/GMPLS (تعمیم چند پروتکل برچسب سوئیچینگ) بر روی فناوری DWDM (تقسیم طول موج متراکم) به عنوان یک رویکرد مطلوب برای تحقق خدمات VPN نسل بعدی پیشنهاد شده است.

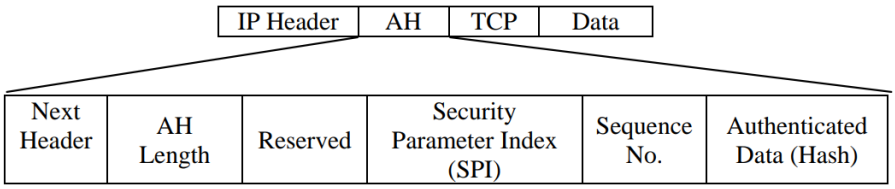
IPsec ۲.۹.۳

IPSec یکی از کامل ترین، ایمن ترین و در دسترس ترین استانداردهای مبتنی بر پروتکل های توسعه یافته .برای انتقال داده ها است. در لایه شبکه عمل می کند
IPSec حاوی پروتکل هایی است که به ایجاد احراز هویت متقابل بین دو طرف در ارتباط در ابتدای جلسه و مذاکره درباره کلیدهای رمزنگاری برای استفاده در جلسه کمک می کند. IPSec مجموعه ای از پروتکل های امنیتی است که به سیستم اجازه می دهد پروتکل های امنیتی مناسب را در حین انتقال داده انتخاب کند. IPSec می تواند برای محافظت از انتقال داده بین دو میزبان یا بین یک جفت دروازه امنیتی (مانند فایروال ها یا روترها) استفاده شود.
IPSec احراز هویت کاربران، رمزگذاری داده ها و یکپارچگی داده ها را در حین انتقال داده ها بین فرستنده و گیرنده فراهم می کند.
از سه پروتکل اصلی به نام‌های هدر احراز هویت، محفظه‌ی بار امنیتی و تبادل کلید اینترنت برای برقراری ارتباط و انتقال داده‌ها به شیوه‌ای امن استفاده می‌کند.

Authentication Header (AH)
این پروتکل احراز هویت گره های منبع، یکپارچگی داده ها را فراهم می کند. رمزگذاری داده ها را ارائه نمی دهد. تمام بسته های IP حاوی AH در قالب بسته بندی شده خود هستند. AH حاوی داده های هش شده، شماره دنباله، شاخص پارامتر امنیتی و غیره است.



Encapsulated Security Payload (ESP)
پروتکل امنیتی کپسوله شده سه سرویس عمده یعنی محرمانه بودن داده ها، یکپارچگی داده ها و احراز هویت منبع را ارائه می دهد. از الگوریتم های رمزگذاری متقارن برای تامین حریم خصوصی و امنیت داده ها استفاده می کند. فرستنده و گیرنده باید از یک الگوریتم رمزگذاری استفاده کنند.



تمامی پروتکل های امنیتی در دو حالت عملیاتی اجرا می شوند:

۱) حالت تونل:
عملیات حالت تونل به عنوان حالت کار پایان به انتها نیز نامیده می شود. یک تونل دو نقطه از VPN را در زیرساخت شبکه مشترک به هم متصل می کند. در حالت تونل، نقاط انتهایی تونل گره های مشترک VPN و زیرساخت شبکه مشترک هستند.
حالت تونل امنیت داده ها را فراهم می کند. بسته داده شامل هدر IP جدید علاوه بر هدر ESP و تریلر، هدر IP اصلی، داده های رمزگذاری شده و احراز هویت ESP است. هدر IP جدید حاوی آدرس نقطه پایانی تونل است. هنگامی که بسته داده رمزگذاری شده به نقطه پایانی تونل می رسد، توسط نقطه پایانی تونل رمزگشایی می شود تا آدرس مقصد را پیدا کند. با یافتن آدرس مقصد، نقطه تونل بسته داده اصلی را در شبکه به مقصد هدایت می کند.

New IP Header	ESP Header	Original IP Header	Encrypted Data	ESP Trailer	ESP Authentication

۲) حالت حمل و نقل:
نام دیگر حالت حمل و نقل حالت عملیات میزبان به میزبان است. بسته داده شامل هدر و تریلر ،ESP احراز هویت ،ESP سرصفحه IP و غیره است. هدر IP رمزگذاری نشده است. از این رو امکان استشمام آدرس توسط مهاجمان وجود دارد. همچنین برای مهاجمان امکان تجزیه و تحلیل ترافیک داده وجود دارد زیرا اطلاعات هدر به راحتی در دسترس آنها است .

Original IP Header	ESP Header	TCP	Encrypted Data	ESP Trailer	ESP Authentication

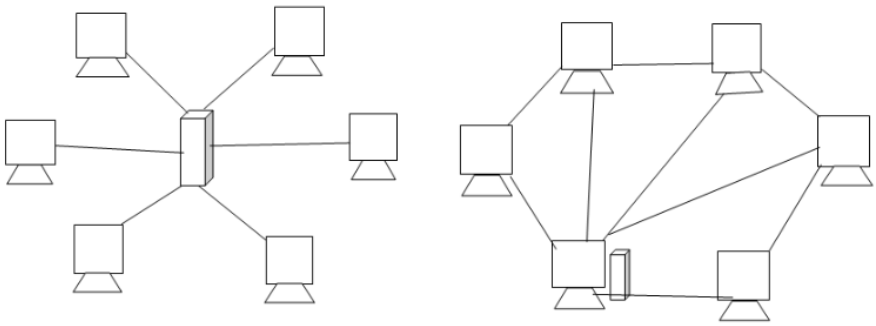
Key Exchange and Management
IPSec دو نوع مدیریت کلید را برای شبکه خصوصی مجازی از طریق شبکه عمومی ارائه می دهد.

۱) مدیریت کلید دستی:
در مدیریت دستی کلید، کلیدهای مخفی بین فرستنده و گیرنده قبل از برقراری ارتباط بین آنها رد و بدل می شود. مقادیر کلیدهای مخفی و ارتباطات امنیتی فقط برای فرستنده و گیرنده شناخته شده است. این نوع مدیریت کلید را می توان در یک محیط شبکه کوچک و ثابت استفاده کرد.
کلیدهای مخفی بین گره های ارتباطی رد و بدل می شوند و قبل از انتقال واقعی داده ها به یکدیگر شناخته می شوند. از این رو، شبکه نمی تواند پویا و مقیاس پذیر باشد. عیب اصلی این روش این است که اگر کلیدهای مخفی توسط شخص ثالثی که می تواند مهاجم باشد دستگیر شود، هر احتمالی وجود دارد که امنیت شبکه به خطر بیفتد.

۲) مدیریت خودکار کلید:
مدیریت خودکار کلید که با نام عمومی تبادل کلید اینترنت (IKE) شناخته می شود، پروتکل پیش فرضی است که در IPSec برای تولید و مدیریت کلیدهای مخفی بین گره های ارتباطی در شبکه استفاده می شود. برخلاف مدیریت کلید دستی، شبکه ای که از این نوع مدیریت کلید استفاده می کند می تواند پویا و مقیاس پذیر باشد.

P2P (Peer-Peer) ۳.۹.۳

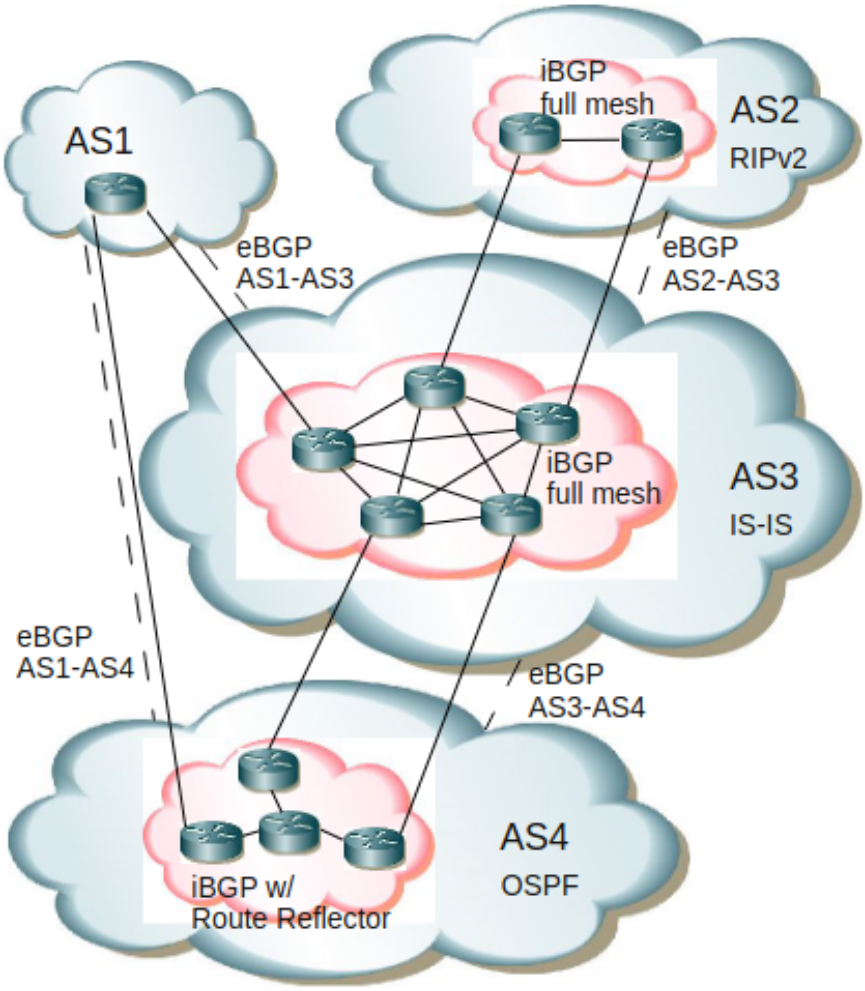
سیستم‌های Peer-Peer VPN (P۲P) که فقط به همتایان مورد اعتماد اجازه مشارکت می‌دهد. این را می توان با استفاده از یک سرور مرکزی مانند یک اتصال هاب برای احراز هویت مشتریان به دست آورد. از طرف دیگر، کاربران می توانند رمزهای عبور یا کلیدهای رمزنگاری را با دوستان خود مبادله کنند تا یک شبکه غیرمتمرکز تشکیل دهند.
تونل زنی که امکان کپسوله کردن یک نوع بسته پروتکل در داخل را فراهم می کند دیتاگرام یک پروتکل متفاوت به عنوان مثال، اتصالات VPN ویندوز می‌توانند از بسته‌های پروتکل تونل زنی نقطه به نقطه (PPTP) برای کپسوله‌سازی و ارسال ترافیک شبکه خصوصی، مانند ترافیک TCP/IP روی یک شبکه عمومی مانند اینترنت استفاده کنند. سرور VPN را می توان به گونه ای پیکربندی کرد که از Windows یا Service User Dial-In Authentication Remote به عنوان ارائه دهنده احراز هویت استفاده کند. اگر Windows به‌عنوان ارائه‌دهنده احراز هویت انتخاب شود، اعتبار کاربری ارسال شده توسط کاربرانی که سعی در اتصال VPN دارند با استفاده از مکانیزم‌های معمولی احراز هویت Windows تأیید می‌شوند و تلاش برای اتصال با استفاده از ویژگی‌های حساب کاربری مشتری VPN و خط‌مشی‌های دسترسی از راه دور محلی مجاز است.



Centralized Decentralized

BGP (Border Gateway Protocol) ۴.۹.۳

مسیریابی اینترنت بر اساس یک سیستم توزیع شده متشکل از روترهای زیادی است که در حوزه های مدیریتی به نام سیستم های خودمختار (ASes) گروه بندی شده اند. اطلاعات مسیریابی بین AS ها در پیام های به روز رسانی پروتکل دروازه مرزی (BGP) مبادله می شود.



۵.۹.۳ MPLS (Multi-Protocol Label Switchin)

چند پروتکل سوئیچینگ برچسب (MPLS) VPN یک روش انعطاف پذیر برای انتقال و مسیریابی چندین نوع ترافیک شبکه با استفاده از ستون فقرات MPLS است. VPN MPLS ها قدرت MPLS و Border را با هم ترکیب می کنند پروتکل مسیریابی Protocol Gateway .(BGP) MPLS برای ارسال بسته ها بر روی ستون فقرات شبکه ارائه دهنده استفاده می شود و BGP برای توزیع مسیرها بر روی ستون فقرات استفاده می شود.

یک شبکه خصوصی مجازی MPLS (VPN) از تجهیزات زیر در خطر است:
۱) روترهای لبه مشتری :(CE) این روترها در محل قرار می گیرند و معمولاً متعلق به مشتری سازمانی هستند. برخی از ارائه دهندگان خدمات نیز تجهیزات CE را با هزینه اجاره اندکی تامین می کنند.

۲) روترهای لبه ارائه دهنده :(PE) اینها روترهای لبه ارائه دهنده هستند که روترهای CE به آنها متصل می شوند. روترهای PE همیشه متعلق به ارائه دهنده خدمات هستند.

۳) روترهای ارائه دهنده :(P) این روترها معمولاً به عنوان "روترهای ترانزیت" شناخته می شوند و در شبکه اصلی ارائه دهنده خدمات قرار دارند. اطلاعات مسیریابی از مسیریاب CE به روتر PE با استفاده از مسیرهای ثابت یا پروتکل مسیریابی مانند BGP منتقل می شود. روتر PE یک جدول ارسال در هر سایت را نگه می دارد که به عنوان جدول مسیریابی و انتقال مجازی (VRF) نیز شناخته می شود.

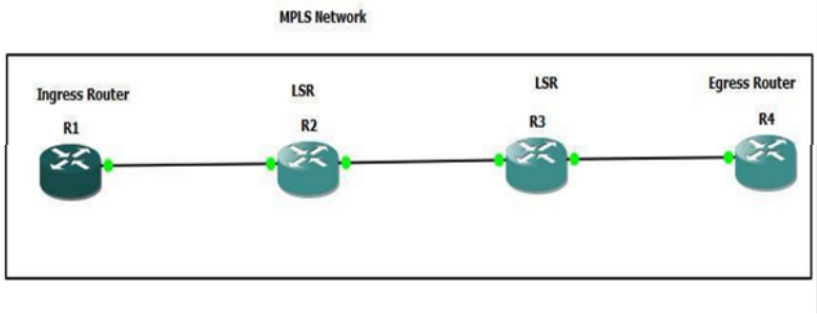


Figure 5: MPLS network.

۶.۹.۳ PPTP (Point to Point Tunnel Protocol)

پروتکل Point to Point Tunneling Protocol یک پروتکل OSI لایه دو است که در بالای پروتکل نقطه به نقطه (PPP) ساخته شده است. PPTP با ایجاد یک شبکه مجازی برای هر مشتری راه دور به شبکه هدف متصل می شود. اتصال کنترل PPTP پیام کنترل و مدیریت تماس PPTP را حمل می کند که برای نگهداری تونل PPTP استفاده می شود.

IP Header	GRE Header	PPP Header	Encrypted PPP Data

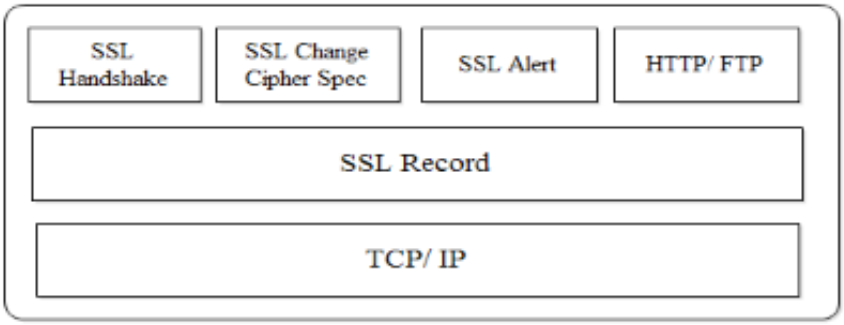
۷.۹.۳ L2TP (Layer 2 Tunneling Protocol)

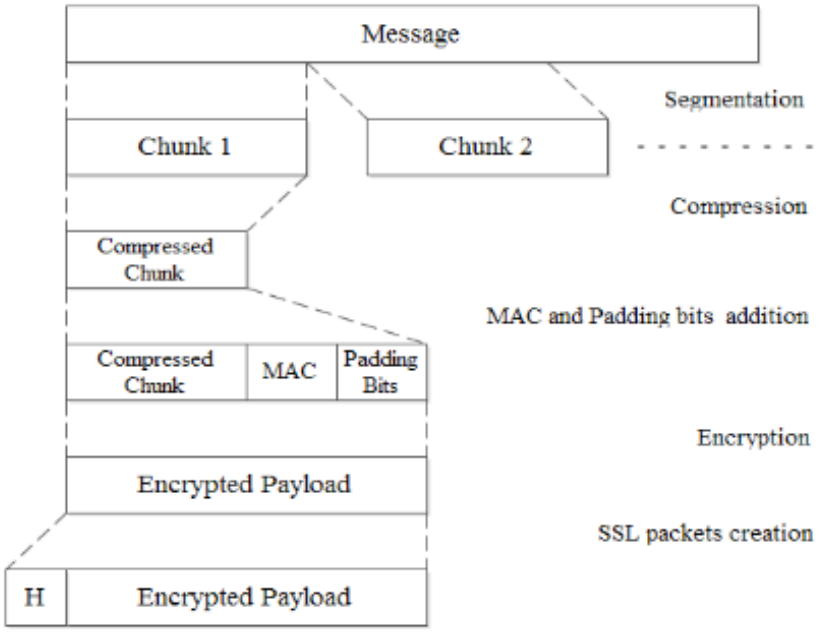
L2TP (Layer 2 Tunneling Protocol) در لایه پیوند داده مدل OSI عمل می کند و یک شبکه خصوصی مجازی امن (VPN) را بین دو دستگاه از طریق یک شبکه نامعتبر فراهم می کند. این کار با کپسوله کردن بسته داده اصلی در بسته دیگری و اضافه کردن هدرهای اضافی به آن کار می کند.

IP Header	UDP Header	L2TP Header	PPP Header	Encrypted PPP Data

۸.۹.۳ SSL (Secure Socket Layer)

پروتکل های لایه سوکت ایمن برای(SSL) ارائه خدمات قابل اعتماد در پروتکل لایه انتقال استفاده می شود.
SSL ترکیبی از چهار پروتکل است که امنیت پروتکل های لایه بالایی مانند ،FTP HTTP و هر پروتکل لایه کاربردی را فراهم می کند. آنها به دو لایه تقسیم می شوند.





۹.۹.۳ TLS (Transport Layer Security)

TLS نسخه ارتقا یافته SSL است، معماری و پروتکل های مشابهی دارد به جز اینکه تغییراتی در پارامترهای امنیتی و محاسبات ،MAC امضای دیجیتال و بلوک کلید وجود دارد. همچنین برخی از پیام های هشدار جدید و عملکرد شبه تصادفی را برای تقویت امنیت در مقایسه با SSL معرفی می کند.

۱۰.۹.۳ ATM (Asynchronous Transfer Mode)

شبکه‌های خصوصی مجازی (VPN) به عنوان ابزاری حیاتی برای ارائه خدمات ارزش افزوده بر روی شبکه‌های IBC مبتنی بر ATM در آینده شناخته شده‌اند.
منشاء آن به عنوان یک فناوری سوئیچینگ و مالتی پلکس مناسب برای طراحی سوئیچ های با ظرفیت بالا بود. ویژگی های ضروری ATM یک بسته با طول ثابت (به نام سلول) است که بر اساس یک شناسه مدار مجازی در هدر سلول سوئیچ می شود. میزبان‌های پایانی درخواست می‌کنند که شبکه یک مدار مجازی را از طریق یک پروتکل سیگنالینگ (کنترل) راه‌اندازی کند که به آنها امکان می‌دهد کیفیت خدمات مورد نظر را مشخص کنند.
شبکه ATM یک شبکه اتصال گرا مبتنی بر سلول است.

۱۱.۹.۳ FR (Frame relay)

پیش‌بینی می‌شود که در آینده نزدیک کارکرد رله‌ی فریم ظاهر شود. شبکه FR یک شبکه اتصال گرا مبتنی بر فریم است.

Classical layer structure	VPNs
Application	
Presentation	
Session layer	SOCKs
Transport layer	
Network layer	IPSec, Layer 3 VPN
MAC layer	ATM, FR, Layer 2 VPN
Physical layer	OVPN, Layer 1 VPN

[۲]
[۱۰]
[۸]
[۷]
[۶]
[۴]
[۵]
[۹]
[۳]

[۱]

مراجع

[۱] Implementation VPN based “MPLS Siddiqui. UA and Butt، ZU Ahmed، F & Technology Information of Journal In: Environment”. Corporate a in .۷–۱ pp. ،(۲۰۱۶) ۶,۵ Engineering Software

[۲] .(۱۹۹۸) In: VPN؟” a is “What Huston. Geoff and Ferguson Paul

[۳] Communica- In: networks”. private virtual “ATM al. et Fotedar Shivi .۱۰۹–۱۰۱ pp. ،(۱۹۹۵) ۳۸,۲ ACM the of tions

[۴] with vpn host-to-site and Site-to-site “P۴-ipsec: al. et Hauser Frederik .۱۳۹۵۸۶–۱۳۹۵۶۷ pp. ،(۲۰۲۰) ۸ Access IEEE In: sdn”. p۴-based in ipsec

[۵] BGP—A “Securing Armitage. Grenville and Rossi، Mattia Huston، Geoff ۱۳,۲ Tutorials & Surveys Communications IEEE In: survey”. literature .۲۲۲–۱۹۹ pp. ،(۲۰۱۰)

[۶] on Report Survey “A Bai. Thulasi V DR and Jayanthi Gokulakrishnan Sci- Computer of Journal Indian In: Technologies”. its & Security VPN .(۲۰۱۴) ۵,۴ (IJCSE) Engineering and ence

[۷] net- private virtual on “Study Reddy. Indira B and Jyothi Karuna K of Journal International In: security”. and protocols VPN’s (VPN)، work Information and Engineering Science، Computer in Research Scientific .۹۳۲–۹۱۹ pp. ،(۲۰۱۸) ۳,۵ Technology

[۸] Multi- Guaranteed QoS for Mechanism “Control al. et Kim Jeong-Mi ۲,۱ Commun. J. In: DWDM.” over IP/GMPLS over OVPN in Service cast .۵۱–۴۴ pp. ،(۲۰۰۷)

[۹] Sur- Comprehensive “A al. et Livingston، Jenila Satapathy، Ashutosh of Journal International In: Vulnerabilities”. their and SSL/TLS on vey .۳۸–۳۱ pp. ،(۲۰۱۶) ۱۵۳,۵ Applications Computer

[۱۰] (VPN): network private virtual of overview “An al. et Zhang Zhensheng ،(۲۰۰۴) ۷ communications network Photonic In: VPN”. optical and VPN IP .۲۲۵–۲۱۳ pp.