به نام خدا

نام: مهدی حسینی

شماره دانشجویی: ۹۶۳۶۶۳۰۱۱

درس: آزمایشگاه سیستم عامل ها

عنوان: وی پی ان سرور ها

فهرست مطالب

فهرست

تاریخچه ۵

مقدمه ٦

مختصری از یک داستان بلند ۷

وی پی ان چیست؟ ۱۱

همبندی شبکه ۱۲

انواع همبندی ۱۲

محیط انتقال ۱٤

خط انتقال ۱۵

رمزنگاری ۱۵

نظریه اطلاعات ۱٦

فیلتر شکن ۱۷

جمع بندی و تعریف کامل وی پی ان؟ ۱۸

اصول کاری وی پی ان ۲٦

اف تی پی ۲٦

قرارداد هدایت انتقال/قرارداد اینترنت ۲۷

اصول کار وی پی ان ۲۸

امنیت در وی پی ان ۳۱

دیوار آتش ۳۲

تاریخچه ۳۳

انواع فایروال ۳٤

مزایا و معایب ۳٦

نحوه عملکرد فایروال های پکت فیلترینگ ۳۷

امکانات ۳۸

رمز نگاری ۳۹
رمز نگاری کد گزاری پنهان گذاری ٤٠
اصول شش گانه کرشهف ٤١
رمزگذاری پیشرفته ٤٢
تعاریف و اصطلاحات: ٤٢
کاربرد های رمزنگاری ٤٣
پروتکل رمزنگاری: ٤٤
الگوریتم رمز نگاری ٤٥
رمزگذاری کلید متقارن ٤٦
رمزگذاری کلید نامتقارن ٤٧
مقایسه رمزنگاری کلید های متقارن و نا متقارن ٤٧
تجزیه و تحلیل: ٤٨
رمزنگاری کلید عمومی ٤٩
آی پی سک ٤٩
مزایا ٥٠
حالت انتقال ٥٠
حالت تونل ٥١
آی پی سک و وی پی ان ٥١
VPN-IP-sec فقط برای اینترنت ٥٢
ویژگی های امنیتی در IP-sec ٥٣
آی پی سک بدون تونل ٥٤
جریان یک ارتباط IP-sec ٥٤
مدیریت کلید های رمز IP-sec ٥٥
پروتکل Ike ٥٦
سرویس دهنده AAA: ٥٧
انواع وی پی ان و پروتکل های آن ٥٨
شبکه وی پی ان سایت به سایت ٥٩

بر پایه اینترنت: ۵۹
بر پایه اکسترانت: ۵۹
شبکه وی پی ان دستیابی از راه دور ٦۰
انواع پروتکل های وی پی ان ٦۱
پروتکل PPTP(Point To Point Tunneling Protocol) ٦۱
پروتکل L2TP/IPsec(Layer 2 Tunneling protocol) ٦۳
پروتکل OpenVPN ٦٤
پروتکل IKEv2(Internet Key Exchange version 2) ٦۷
پروتکل SSTP(Secure Socket Tunneling Protocol) ٦۹
تونل زنی روی وی پی ان ۷۰
تونل زدن چیست ۷۱
پروتکل های درون وی پی ان ۷۳
وی پی ان در ایران و ساخت یک وی پی ان ساده در ویندوز ۷۵
وی پی ان در ایران ۷٦
ساخت یک وی پی ان در ویندوز ۷۷
تنظیمات روتر وای فای ۸۰
طریقه اتصال به وی پی ان سرور خود ۸۰

تاریخچه

مقدمه

بیشتر ابزارهای امنیتی که در طول روز استفاده می‌کنیم در مسیر تکاملشان دستخوش تغییراتی بودند. از صخره‌های بزرگی که نیاکان ما برای بستن ورودی غارها استفاده می‌کردند تا گوشی‌هههای هوشمند که با تصدیق بیولوژیکی کار می‌کنند.از لباس‌های پنهانی که برای محافظت در برابر سرما استفاده می‌شوند تا وسایل گرمایشی که شما را در مناطق سردسیر، گرم نگه می‌دارند. از داروهای گیاهی برای درمان سرفه تا تشریح ژنتیک که قادر است عامل سرطان را از درون DNA شما ریشه‌کن کند.

با تحولات عظیم در عرصه ارتباطات، اغلب سازمان‌ها و موسسات ارائه‌دهنده کالا و خدمات که در گذشته بسیار محدود و منطقه‌ای مسائل را دنبال می‌کردند، امروزه بیش از گذشته نیازمند تفکر در سطح جهانی برای ارائه خدمات و کالای تولیده شده را دارند. به عبارت دیگر، تفکرات منطقه‌ای و محلی حاکم بر فعالیت‌های تجاری جای خود را به تفکرات جهانی و سراسری داده‌اند. امروزه سازمان‌های زیادی وجود دارند که در سطح یک کشور دارای دفاتر فعال و حتی در سطح دنیا دارای دفاتر متفاوتی می‌باشند. تمام سازمان‌های فوق به‌دنبال یک روش سریع، ایمن و قابل اعتماد به منظور برقراری ارتباط با دفاتر و نمایندگی‌های خود در اقصی نقاط یک کشور یا در سطح دنیا هستند.

اکثر سازمان‌ها و موسسات به منظور ایجاد یک به با سرعت ۱۲۸کیلوبیت در ثانیه) با سرعت ۱۵۵ مگابیت در ثانیه). یک شبکه گسترده دارای مزایای عمده‌ای نسبت به یک شبکه عمومی نظیر اینترنت از بعد امنیت و کارایی است. اما پشتیبانی و نگهداری یک شبکه گسترده در عمل و زمانی‌که از خطوط اختصاصی استفاده می‌گردد، مستلزم صرف هزینه بالائی است.

جای دیگری از زندگی که امنیت در آن‌یک نگرانی بزرگ محسوب می‌شود، ارتباطات آنلاین و فضای مجازی است. گرچه عمق تاریخچه ابزارهای امنیت اینترنت در مقایسه با مثال‌هایی که در بالا گفتیم کمتر است (با توجه به سن اینترنت که ۲۸ سال است). اما از جذابیت بالایی برخوردار است. مشاهده می‌شود که چگونه شبکه خصوصی مجازی (VPN) یکی از کارآمدترین و رایج‌ترین ابزارهای محافظت امنیت و حریم خصوصی در اینترنت است. امروز قصد داریم تاریخچه کوتاهی از پیشرفت‌های آن را برای شما ارائه دهیم.

مختصری از یک داستان بلند

سرانجام درسال ۱۹۶۱ میلادی تعداد ۴ کامپیوتر در ۲ ایالت مختلف با موفقیت ارتباط برقرار کردند و با اضافه شدن واژه نت به طرح اولیه، نام آرپانت (ArpaNet) برای آن منظور شد.

در دهه ۱۹۷۰ میلادی با تعریف پروتکل‌های جدیدتر از جمله TCP که تا به امروز رواج دارد و نیز مشارکت کامپیوترهای میزبان (Host) بیشتر به آرپانت و حتی گسترده شدن آن به برخی نواحی فراتر از مرزهای ایالات متحده، آرپانت شهرت بیشتری یافت و ایده اینترنت همراه با جزییات بیشتر راجع به شبکه‌های کامپیوتری مطرح گشت تا اینکه طی سال‌های پایانی دهه ۱۹۷۰ شبکه‌های مختلف تصمیم گرفتند به صورت شبکه‌ای با یکدیگر ارتباط برقرار نمایند و آرپانت را بعنوان هسته اصلی انتخاب کردند.

بعدها در سال ۱۹۹۳ میلادی نام اینترنت روی این شبکه بزرگ گذاشته شد. وب یا همان WWW که مخفف World Wide Web (به فارسی: تار جهان‌گستر) می‌باشد توسط آزمایشگاه اروپایی فیزیک ذرات CERN بخاطر نیاز آنها به دسترسی مرتب‌تر و آسان‌تر به اطلاعات موجود روی اینترنت ابداع گشت. در این روش اطلاعات به صورت مستنداتی صفحه‌ای بر روی شبکه اینترنت قرار می‌گیرند و بوسیله یک مرورگر وب قابل مشاهده هستند و هم اکنون کارکردهای بسیاری دارند.

همزمان با عمومیت یافتن اینترنت ، اغلب سازمان‌ها و موسسات ضرورت توسعه اختصاصی خود را به درستی احساس کردند. درابتدا شبکه های اینترانت مطرح گردیدند. این نوع شبکه‌ها به صورت کاملاً اختصاصی بوده و کارمندان یک سازمان بااستفاده از گذرواژه تعریف شده، قادر به ورود به شبکه و استفاده از منابع موجود می‌شوند

اینترانت خود تاریخچه‌ای مستقل ندارد، زیرا یکی از دستاوردهای اینترنت به‌شمار می‌رود و در واقع چند سالی پس از آنکه اینترنت پا به عرصه جهانی گذاشت، اینترانت و اکسترانت نیز پدید آمد.

در ایران، از اواسط سال ۱۳۷۴ که نرم‌افزار سیستم عامل شبکه (NT SERVER) شرکت رایانه‌ای نت اسکیپ (Netscape) وارد کشور شد، به سبب سهولت نصب اینترانت‌ها بر روی این سیستم عامل شبکه، نصب اینترانت‌ها آغاز گردید و از آن زمان تاکنون، این جریان در دنیا و ایران رشد فزاینده‌ای داشته است. به‌طور مثال، وزارت کشاورزی ایران در همان سال توانست از خدمات شبکه اینترانت استفاده کند.

اطلاع‌رسانی، ارتباطات، بازاریابی و فروش، آموزش از راه دور، کار از راه دور، تصمیم‌گیری بهینه مدیریت بانکداری و اقتصاد و کار و کاریابی، کاربردهای اصلی اینترانت‌ها هستند. در زمینه اطلاع‌رسانی با توجه به قابلیت چند رسانه‌ای‌ها و ارائه اطلاعات روزآمد، می‌توان به ارائه اطلاعات در زمینه‌های مختلف از جمله نشریات، اطلاعیه‌ها، بخشنامه‌ها، پرونده‌های کاری، اطلاعات تخصصی، اطلاعات مشتریان، رقبا و کاربران، اخبار، و جز آن اشاره کرد. ارائه الکترونیکی این اطلاعات خود موجب کاهش استفاده از کاغذ می‌شود و در نهایت کاهش هزینه و زمان را برای شرکت‌ها به دنبال خواهد داشت. از این روش می‌توان برای توزیع اطلاعات به‌دست آمده از اینترنت استفاده کرد.

در زمینه ارتباطات، اینترانت‌ها باعث تسهیل ارتباطات میان اعضای یک سازمان با مشتریان و رقبا و سازمان‌های بیرونی خواهند شد که به‌طور نمونه می‌توان به جمع‌آوری نظرات، شکایات، و آگاه کردن مدیران از مسائل را نام برد؛ یا ارتباط افراد هم اندیشه در موضوعات خاص که خود باعث ایجاد نوآوری‌ها، خلاقیت‌ها، و ابتکارها در زمینه‌های مختلف می‌شود.

در زمینه بازاریابی و فروش می‌توان تبلیغات جهت معرفی محصولات، در نهایت سفارش از مشتری، دریافت پیشنهادات و انتقادات از مشتری، انجام و پیگیری عملیات فروش، ارائه خدمات پس از فروش،

انجام هماهنگی‌های لازم با مشتری و گزارش پیشرفت سفارش به مشتری و به‌طور کلی فروش از راه دور را نام برد.

ولی به تازگی، موسسات و سازمان‌ها با توجه به مطرح شدن خواسته‌های جدید (کارمندان و ادارات از راه دور) اقدام به ایجاد شبکه‌های اختصاصی مجازی نموده‌اند. یک وی‌پی‌ان شبکه‌ای اختصاصی است که از یک شبکه برای ارتباط با شبکه‌ای دیگر از راه دور و ارتباط کاربران با شبکه سازمان خود استفاده می‌نماید. این نوع شبکه‌ها به جای استفاده از خطوط واقعی نظیر خطوطLeased ، از یک ارتباط مجازی به اینترنت برای ایجاد شبکه اختصاصی استفاده می‌کنند. نیاز به نگهداری از اطلاعات حساس آنلاین به‌صورت خصوصی و ایمن به‌طور بحث‌برانگیزی از وقتی اینترنت به وجود آمد احساس می‌شد. در آغاز، این نگرانی بیشتر در کسب‌وکارها و دولت‌ها مشاهده می‌شد. بااین‌حال، با افزایش جرائم اینترنتی که نتیجه یک سری رخنه‌های امنیتی در دهه اول قرن ۲۱ بود، هر روز کاربران بیشتری نسبت به خطرات دنیای آنلاین باخبر می‌شوند. این شد که VPN و استفاده از آن تبدیل به یک جواب نهایی برای احتیاجات آن‌ها شد. زیرا به صرفه و قابل دسترس است.فیلتر شکن به آن‌ها اجازه داد تا از راه دور به یک شبکه خصوصی در یک اتصال عمومی متصل شوند، همچنین به آن‌ها سطح بالایی از حفاظت حریم خصوصی را هدیه داد.

از سال ۲۰۰۵ تاکنون دیگر پروتکل VPN جدیدی به بازار معرفی نشده است. اکثر توسعه‌دهندگان ترجیح می‌دهند با نمونه‌های مرجع باز یا اوپن سورس کار کنند و تلاش برای ارتقای آن‌ها دارند. پروتکل‌های Openvpn و IKEv2 برای اطمینان از بهترین تعادل بین محافظت، حریم خصوصی و کارایی برای کاربران ما استفاده می‌شوند. همچنین نکته شایان‌ذکر، Keep solid wise است. این یک فناوری پیچیده است که برای قابلیت اعتماد بیشتر و بهره‌گیری از یک پهنای باند بدون مسدود شدن، توسعه‌یافته است.در کل، امنیت اینترنت در حال حاضر موضوع جذابی بوده و از دید فنی درحال‌توسعه پایدار است و به‌آرامی به سمتی پیش می‌رود که امنیتی در سطح شبکه‌های نظامی باقیمت‌های معقول را برای ما به ارمغان آورد.

از سوی دیگر، به‌هرحال به دلیل رقابت همیشگی، که بسیار شبیه به زندگی در اینترنت است، گاهی پی گرفتن یک مسیر برای نوآوری بسیار سخت و رنج‌آور می‌شود. ما امیدواریم که این متن به شما کمک کرده باشد تا تصویر واضحی از توسعه ابزارهای امنیت اینترنت دیده باشید.

وی پی ان چیست؟

همبندی شبکه

هم‌بندی یا توپولوژی شبکه یک آرایش از المان‌های مختلف از شبکه ای رایانه ای (نظیر گره، پیوند و ...) است .اساساً ساختار توپولوژیکی از شبکه، که ممکن است از لحاظ فیزیکی یا منطقی به تصویر کشیده شود. همبندی یک شبکه بر اساس چیدمان سیستم‌ها نیست بلکه بسته به تنوع کابل کشی می‌باشد.

انواع همبندی

توپولوژی خطی :(bus) در این نوع توپولوژی سیستم‌ها به یک سیم ارتباطی قوی به نام کواکسیال مرتبط هستند و کانکتور و ترمیناتورهای متصل به پیام‌ها را منتقل می‌کنند. یکی از پرکاربردترین توپولوژِی‌ها می‌باشد از مزایای ان می‌توان به پیکربندی اشاره ان کرد. در این نوع همبندی سیستم‌ها از ارسال broadcast استفاده می‌کنند همانند اترنت و کابل آن که بسته را پخش و توسط آدرس mac و ip بسته برای ان سیستم باز می‌شود. از معایب هزینه زیاد سیم کسی و امنیت کمتر نسبت به نوع‌های دیگر می‌باشد.

توپولوژی حلقوی : سیستم‌ها به صورت یک حلقه می‌باشد و این نوع سیستم از نوع token ring می‌باشند یعنی بسته به صورت حلقه ای چرخش و با توجه به token ان بسته به سیستم مقصدش می رسد. مزایای ان سیم کشی کم و هزینه کم و معایب ان این است که اگر در یک رابط مشکل ایجاد شود در کل سیستم مشکل ایجاد می‌شود.

توپولوژی ستاره ای : به صورتی است که در میان دو سیستم متصل یک سیستم سروری که مبادله ان به دیگر سیستم توسط token ring کمک می‌کند . حداقل سیستم استفاده شده در این نوع توپولوژی ۳ عدد می‌باشد و ماز مزایای ان امنیت نسبی خوب و معایب سختی در عیب یابی هنگام بروز مشکل است.

توپولوژی درختی : همانند درخت می‌باشد و مانند شبکه ستاره ای اما حداقل باید از چهار سیستم باشد که از سیستم سرور فرمان می گیرد . این نوع سیستم بیشتر در مکان‌های توزیع اطلاعات مانند شرکت‌ها مورد استفاده قرار می گیرد و مسیر رسیدن بسته به مقصد طی یک چرخش می‌باشد همانند توپولوژی حلقوی اما از لحاظ امنیتی مناسب و از لحاظ سیم کشی مطلوب می‌باشد.

توپولوژی تکامل یافته : این نوع همبندی مانند یک چند ضلعی می‌باشد که به تمام راس‌هایش متصل است و اطلاعات بدون گذر از گذرگاهی و به طوری مستقیم به مقصد می رسد . این نوع توپولوژی با کوتاه کردن مسیر ارتباطی مناسب تر است اما سیم کشی هزینه گزافی دارد. این نوع توپولوژی بر خلاف بیشتر توپولوژی‌ها از روترها استفاده می‌کنند که امنیت را بالا می برد و از نوع پخش داده Unicast بهره می برد که از لحاظ امنیتی بسیار مطلوب می‌باشد.

توپولوژی تکامل نیافته: این نوع همبندی که از توپولوژی تکامل یافته سرچشمه گرفته‌است به سیستم‌های متعدد و مختلفی ارتباط دارد و نظم و قانون خاصی در ارتباط با سیستم‌ها ندارد این نوع سیستم خودجوش به وجود می ایند و قصد خاصی در وجود اوردن آن‌ها نمی‌باشد مثلاً وصل کردن دو کامپیوتر به یک دیگر در یک دانشگاه که ارتباط با بقیهٔ سیستم‌ها ندارد.

توپولوژی ترکیبی:(hybrid) این نوع توپولوژی متشکل از چندین نوع همبندی در نوع خود می‌باشد . همبندی شبکه‌های امروزی براساس این نوع همبندی تشکیل می‌شود و به از سرور اصلی فرمان می‌گیرند.

محیط انتقال

محیط انتقال به مسیر فیزیکی‌ای گفته می‌شود که کارش حمل سیگنال ها از مکانی به مکان دیگر است. درارتباطات داده ای محیط انتقال ممکن است یک خط انتقال ساده یا یک شبکه پیچیده باشد که مبدأ را به مقصد متصل می‌کنددر شبکه‌های رایانه‌ای انتقال اطلاعات بین فرستده و گیرنده در محیط انتقال و با استفاده از امواج الکترومغناتیسی یا ولتاژهای الکتریکی انجام می‌شوددر این شبکه‌ها محیط انتقال نقش متصل‌کننده گره‌های شبکه به هم را بر عهده دارد کارایی شبکه تا حد زیادی به محیط انتقال آن بستگی خواهد داشت

به محیط‌های انتقال سیمی، محیط انتقال کران‌دار یا هدایت‌شده و به محیط‌های انتقال بی‌سیم محیط انتقال بی‌کران یا هدایت‌نشده گفته می‌شود. برای انتقال در سرعت‌های مختلف از محیط‌های انتقال گوناگون استفاده می‌شود و پهنای باند ، نویز ، تضعیف و تابش از عوامل تأثیرگذار در انتخاب محیط انتقال هستند .

زوج به هم تابیده، کابل هم محور و فیبر نوری نمونه‌هایی از یک محیط انتقال کران‌دار هستند. این محیط‌های انتقال را به عنوان محیط‌های انتقال باسیم می‌شناسند. در مقابل محیط‌های انتقال بی‌کران از فناوری‌های ریز موج و فروسرخ برای انتقال استفاده می‌کنند

خط انتقال

کابل‌های برق معمولی برای حمل فرکانس پایین جریان متناوب(AC) ، مانند برق قدرت ، که ۱۰۰ تا ۱۲۰ بار در ثانیه تغییر جهت می‌دهند، و سیگنال‌های صوتی مناسب است. ولی نمی‌تواند به عنوان حامل جریان در محدوده فرکانس رادیویی یا بالاتر باشد. که در ثانیه میلیون‌ها تا میلیاردها بار تغییر جهت می‌دهد. , به این دلیل که انرژی تمایل دارد از خود پرتو ساطع کند استفاده از کابل به عنوان حامل امواج رادیویی ، باعث تلفات توان می‌شود. جریان‌های فرکانس رادیویی نیز تمایل به منعکس شدن از ناپیوستگی‌ها در کابل مانند اتصالات الکتریکی و مفاصل، وحرکت در کابل به سمت منبع دارد. این بازتاب‌ها به عنوان گلوگاه‌ها عمل می‌کنند، مانع از رسیدن قدرت سیگنال به مقصد می‌شود. خطوط انتقال به صورت مخصوص ساخته می‌شود، و از تطبیق امپدانس استفاده می‌شود، تا حمل سیگنال الکترومغناطیسی با حداقل بازتاب و تلفات توان انجام شود. از بارزترین ویژگی‌های خطوط انتقال این است که آن‌ها ابعاد مقطعی یکنواختی در طول خط دارند،

نتیجتاً امپدانس الکتریکی یکنواختی، امپدانس مشخصه‌دارند .تا از بازتاب پیشگیری شود. از انواع خطوط انتقال می‌توان به خطوط موازی خط نردبانی ,زوج به هم تابیده کابل کوسیکال ,استریپ لاین، و میکرو استریپ اشاره کرد.

رمزنگاری

رمزنگاری استفاده از روش‌های ریاضی، برای برقراری امنیت اطلاعات است. دراصل، رمزنگاری دانش تغییر دادن متن پیام یا اطلاعات به کمک کلید رمز و با استفاده از یک الگوریتن رمز است. به صورتی که تنها شخصی که از کلید و الگوریتم آگاه است می‌تواند اطلاعات اصلی از اطلاعات رمزگذاری،

استخراج کند و شخصی که از یکی یا هر دوی آن‌ها اطلاع ندارد نمی‌تواند به اطلاعات دسترسی پیدا کند. دانش رمزنگاری بر پایه اصولی مانند نظریه اطلاعات، نظریه اعداد و آمار بنا شده‌است و امروزه به‌طور خاص در علم مخابرات مورد بررسی و استفاده قرار می‌گیرد. برابر رمزنگاری در زبان انگلیسی واژه Cryptography است، که برگرفته از دو واژه زبان یونانی Kryptos به مفهوم «محرمانه» و Graphien به معنای «نوشتن» است

نظریه اطلاعات

نظریه اطلاعات به مقداردهی ذخیره و انتقال اطلاعات می‌پردازد. این نظریه، مدل ریاضی از شرایط و عوامل مؤثر در پردازش و انتقال اطلاعات (داده‌ها) به‌دست می‌دهد. تمرکز این نظریه بر محدودیت‌های بنیادین ارسال و پردازش اطلاعات است، و کمتر به چگونگی عملکرد و پیاده‌سازی روش‌های انتقال و پردازش اطلاعات می‌پردازد. پیدایش این نظریه در پی کارهای کلود شانون در ۱۹۴۸ بوده‌است.

نظریه اطلاعات مورد استفاده خاص مهندسان مخابرات است، هرچند برخی از مفاهیم آن در رشته‌های دیگری مانند روان شناسی ، زبان شناسی ، کتابداری و اطلاع رسانی ، و علوم شناختی نیز استفاده می‌شود

مفهوم «اطلاعات» که شانون پیش نهاد، از دیدگاه آمار و احتمالات بوده و لزوماً با مفهوم رایج اطلاعات به معنی «دانش» یا دیگر استفاده‌های روزمره از آن در زبان محاوره‌ای مانند «بازیابی اطلاعات»، «تحلیل اطلاعات»، «چهارراه اطلاعات» و غیره یکی نیست. اگر چه نظریه اطلاعات بر رشته‌های دیگر مانند روان‌شناسی و فلسفه اثر گذاشته، ولی اثرش به علت مشکل تبدیل «مفهوم آماری اطلاعات» به «مفهوم معنایی دانش و محتوا» بیشتر از نوع القای احساساتی نسبت به مفهوم اطلاعات بوده‌است

فیلتر شکن

فیلترشکن در اصطلاح عامیانه به مجموعه‌ای از روش‌ها و نرم‌افزارهای مختلف گفته می‌شود که برای عبور از سد فیلترینگ و یا دور زدن تحریم اینترنتی از آن استفاده می‌کنند. جستجوی کلمه فیلتر شکن و vpn از پر کاربرد ترین و بیشترین جستجو در گوگل و سایت های جستجو مشابه در کشور ایران را دارا می باشد. وزیر ارتباطات دولت دوازدهم از تجارت چند صد میلیاردی خرید و فروش فیلترشکن، پروکسی و vpn خبر داده است که خود رقم بالایی در دنیا برای این تجارت محسوب می گردد

به دلیل گستردگی فیلترینگ و سانسور اینترنت در ایران ، بسیاری از کاربران ایرانی از این روش‌ها و نرم‌افزارها بهره می‌گیرند. البته بعضی از فیلترشکن‌ها کاربرد امنیتی دارند یعنی با عوض‌کردن آی پی آدرس فرد مورد نظر جلوی هک شدن را می‌گیرند.

فیلتر سایت در ایران را تنها کشور دانست که حتی شبکه های اجتماعی و پیام رسان
نظیر فیسبوک ،تویتر ، وایبر و... فیلتر می باشند. دولت ایران در طی سال ۱۳۹۲ قدم را فراتر گذاشته و سرویس ارسال ایمیل گوگل یعنی جیمیل را نیز فیلتر کرد. که با اعتراضات در فضای مجازی و شکایت سرویس جیمیل باز شد

سازمان

گزارشگران بدون مرز ایران را به‌دلیل سانسور گسترده اینترنت در رده ۱۳ کشور دشمن اینترنت آزاد دسته‌بندی کرده‌است

برخی از روش‌ها و نرم‌افزارهایی که برای عبور از فیلترینگ و سانسور اینترنت وجود دارند قابل اعتماد هستند، و تعداد زیادی از آن‌ها را می توان بدون نگرانی استفاده کرد اما در این بین برخی از

نرم‌افزارهای با امنیت کم ممکن است خطراتی برای کاربران استفاده‌کننده در پی داشته باشند. برای مطمئن‌شدن از امنیت آن‌ها می توان از شرکت یا فرد تولیدکننده فیلترشکن و نرم‌افزار مورد استفاده، گواهی های امنیتی و مورد استفاده را درخواست کنید بعضی فیلترشکن‌ها ممکن است حاوی ، ردیابی کاربران، دسترسی شرکت‌های شخص ثالث به داده‌های کاربران، دزدی پهنای باند، ربود مرورگر و نشت داده هستند که ممکن است از جمله این خطرات می‌باشند .

مجله آنلاین TechCrunch اولین مرجعی بود که متوجه پاک شدن Onavo از گوگل‌پلی شده بود. در حال حاضر این برنامه بر روی دستگاه کاربران فعلی به حیات خود ادامه می دهد؛ اما انتظار میرود در طول زمان به کلی تعطیل شود.

در پاسخ به وبسایت Gizmodo برای شفاف سازی بیشتر این مسئله یکی از سخن گویان شرکت فیسبوک اعلام داشت: " تحقیقات بازاری به تولید محصولات بهتر برای مشتریان کمک میکند. در حال حاضر سعی بر روی پیاده سازی یک مدل تحقیقاتی پاداش محور هستیم که به این معناست که برنامه به زودی تعطیل خواهد شد".

مانند هر سرویس VPN دیگری، Onavo Protectبه وسیله تغییر مسیر فعالیت وبگردی کاربران در یک سرور شخص ثالث، آدرس IP و موقعیت مکانی آنها را از دید ردیاب ها مخفی نگه می داشته است. کاربران ممکن است از این طریق اطلاعات شخصی خود را از شرکتی مانند Camcast دور نگه داشته باشند، اما این را فراموش کرده اند که در مقابل، دسترسی اختصاصی به فعالیت های وبگردی خود را به یکی از بزرگترین (و بدنام ترین) شرکت های فناوری داده محور سپرده اند.

جمع بندی و تعریف کامل وی پی ان؟

زمانی که به اینترنت وصل می‌شود، از سرویسی استفاده می‌کنید که شرکت ارتباطات در اختیار شما قرار می‌دهد. شما برای دسترسی به اینترنت به مودم/روتر نیاز دارید. کامپیوتر شما توسط اترنت به روتر وصل می‌شود و برای اتصال لپ‌تاپ و گوشی هوشمند خود به اینترنت از وای فای استفاده می‌کنید. حتی اگر برای وصل شدن به اینترنت از دیتای سیمکارت استفاده کنید، تفاوتی در نحوه عملکرد اینترنت ایجاد نمی‌شود. این روند برای باز کردن یک صفحه و یا دانلود تکرار می‌شود. برای اینکه این اطلاعات توسط اینترنت جابه‌جا شوند، نیاز به آدرس دهی است تا معلوم شود این اطلاعات از کجا آمده و به کجا می‌روند. با توجه به اطلاعاتی که جابه‌جا می‌شوند، شیوه‌های آدرس‌دهی متفاوتی وجود دارد؛ با این حال در بالاترین سطح آدرسی وجود دارد که به آن آدرس IP یا نشانی IP گفته می‌شود.

مخفف کلمات Virtual Private Networkیا به زبون خودمونی شبکه خصوصی مجازی است که ارتباط بین کاربران را در یک فضای خاص ایجاد می کند.واسهٔ توضیحش یه مثال میزنم.فرض کنیم که یک شرکت بزرگ داریم که شعبه هایی توی شهرهای مختلف داره، وقتی کامپیوترهای این شرکت ها بخوان با هم اطلاعات رد و بدل کنن یا حتی از یه اتوماسیون اداری یکسان استفاده کنن باید از طریق شبکه این کارو رو انجام بدن. امّا استفاده از شبکهٔ جهانی مثل اینترنت امنیت نداره و ترافیک بالایی هم داره و همچنین ما آدرس هایی که در شبکه داخلیمون استفاده میکنیم در شبکه اینترنت معتبر نیست که بخوان از مسیریاب ها رد بشن . از شبکه های گستردهٔ دیگه ای مثل ISDN و OC3 هم می شه استفاده کرد اما زیر ساخت های زیادی لازم داره و هزینهٔ بالایی هم باید پرداخت بشه. پس ما از یک راه میانبر به نام VPN استفاده میکنیم.

در واقع vpn یک شبکهٔ خصوصی در دل شبکهٔ WAN به وجود می یاره که ترافیک بالای اینترنت رو نداره و سرعت بالاتر و امنیت بیشتری داره. این یک کانال خصوصی برای ارتباط راحت تر و سریع تره. اصلا بزارید مفهوم راحتتر رو براتون بگم ، VPNیک تونل ایجاد میکنه یعنی چی ؟ شما وقتی تو جاده از تونل رد میشین در حقیقت دارید از بستر کوه عبور میکنین اما محتواتون با محتوای کوه فرق داره ، شما از هوا دارید رد میشید نه سنگ و این برای کوه قابل درک نیست و به همین دلیل اطلاعات شما هم توی اینترنت به همین شکل خواهد بود ، شما فرض کنید اطلاعاتتون رو دارید با شکل مثلث ارسال میکنید و این در حالی هست که اطلاعات در اینترنت به شکل مستطیل هستن و این باعث میشه که

اطلاعات شما برای دیگران که در اینترنت هستند غیر قابل درک و نامفهوم باشه که این خودش میشه امنیت ... حالا جلوتر بیشتر براتون توضیح میدم.

یک شبکه خصوصی را از طریق شبکه‌های عمومی مانند اینترنت گسترش می‌دهد. مثلاً فرض کنید که شبکه خصوصی شرکتی در داخل ساختمان آن شرکت محدود شده و برای دسترسی به آن باید به داخل ساختمان برویم. اما در مواقعی ما دسترسی فیزیکی به آن مکان را نداریم ولی باید به شبکه خصوصی آن جا وصل شده و با آن کار کنیم. مثلاً زمانی که شما در مسافرت هستید و اتفاقی می‌افتد که سریعاً باید به شبکه وصل شوید یا امروزه که اصطلاح کار از راه دور مطرح است، کاربران با استفاده از اتصالات VPN به شبکه وصل شده و کار خود را انجام می‌دهند. اتصالات وی‌پی‌ان کاملاً امن بوده و غیرقابل شنود و رمزگشایی هستند.

در گذشته برای گسترش داده شبکه‌های خصوصی از اینترانت (Intranet) استفاده می‌شد. اینترانت نوعی شبکه است که برای ارتباط و تبادل داده از اینترنت استفاده نکرده و یک شبکه کاملاً اختصاصی بین شرکت‌ها است. اینترانت‌ها بدون واسط اکسترانت هیچ ارتباطی با شبکه اینترنت ندارند. یعنی می‌توان اینترانت را مانند یک اینترنت شخصی برای شرکت‌ها تعریف کرد که از پروتکل و استانداردهای اینترنت استفاده می‌کند اما بسیار محدود تر و دسترسی به آن تنها برای افراد تایید شده امکان پذیر است. مثلاً شبکه بانک‌ها، دانشگاه‌ها و ... اغلب از نوع اینترانت هستند.

راه اندازی اینترانت بسیار پر هزینه بوده و برای اغلب شرکت‌ها امکان پذیر نیست. از طرفی امنیت آن و امکان دسترسی افراد غیر مجاز همیشه تهدیدی بزرگ برای شبکه‌های اینترانت به حساب می‌آید. به همین دلیل روش ارتباط وی‌پی‌ان مطرح شد که کم هزینه تر، امن تر، قابل انعطاف تر و فرایند خطایابی آن نیز سریع تر است.

واژه vpn را امروزه بسیار می شنویم. این واژه تقریبا به طور شکست ناپذیری به عنوان یک راه حل سازمانی در صنعت شبکه در گوش مدیران فناوری اطلاعات تکرار می شود. تعاریف بسیار متعددی از یک شبکه وی پی ان وجود دارد، اما صرف نظر از تمام این ها، تنها یک چیز می تواند تعریف درستی از

وی پی ان به ما بدهد، و آن این است که بدانیم وی پی ان چگونه کار می کند.

دنیا در دهه های اخیر با تغییرات زیادی روبه رو شده است. به جای سر و کار داشتن با دغدغه های محلی، بسیاری از مشاغل امروزه به بازار جهانی می اندیشدند، اقتصاد جهان به بدنه ای یک پارچه تبدیل شده است و هر اتفاقی در این بدنه رخ بدهد، تاثیر آن را همگان خواهند دید. بسیاری از شرکت ها، تاسیسات خود را در جاهای مختلف دنیا نهادینه کرده اند و این ها همه به یک چیز نیاز دارند: راهی برای ایجاد اتصال سریع، امن و قابل اطمینان میان این مراکز، صرف نظر از مکان آن مرکز.

تا همین چند وقت پیش، اگر یک شرکتی می خواست برای خود شبکه ای تولیدکند، مجبور بود با عقد قرارداد با مخابرات سرویس دهنده محل، نسبت به خرید یک خط شخصی اقدام می کرد و از طریق این خطوط شخصی، یک شبکه wan راه اندازی می کرد. یک راه دیگر تولید شبکه ای است که از طریق تونل زدن یا رمزگذاری روی خط یا شبکه ای عمومی، به گونه ای بتواند از آن استفاده شخصی کند. البته که می توانید برای راه اندازی یک شبکه خصوصی از خطوط اتصالی خودتان استفاده کنید. اما در این صورت هزینه بسیار بالایی را باید متقبل شوید. تفاوت این دو مثل اجاره کردن یک لیموزین در خیابان شهر است، و یا ایجاد یک سری خیابان های جدید برای حرکت ماشین های مان.

برای درک بهتر این موضوع، ما مثالی را برای شما خواهیم زد: فرض کنید شما صاحب یک شرکت بزرگ هستید که دارای دفاتر متعددی در مکان ها و مناطق مختلف می باشد. شما برای اتصال کامپیوترهای موجود در دفاتر مختلف به یکدیگر و ایجاد یک شبکه واحد، نیاز دارید تا همه این سیستم ها را از روش های گوناگون به یکدیگر متصل سازید که ممکن هزینه بسیار زیادی را متحمل شوید. از طرفی می توانید از شبکه اینترنت نیز برای اتصال سیستم ها به یکدیگر استفاده کنید که این کار هزینه بسیار کمتری دارد، اما امنیت آن بسیار پایین است و ممکن است اطلاعات حیاتی شما بر بستر شبکه اینترنت، مورد شنود واقع شود.

در چنین شرایطی VPN ها به کمک شما خواهند آمد و با استفاده از آن ها می توانید یک شبکه امن و ارزان قیمت را برای تعداد نامحدودی از سیستم های خود، ایجاد کنید. وی پی ان ها به شما کمک می

کنند تا یک شبکه مجازی ایمن را در دل شبکه عمومی اینترنت ایجاد کنید و به این ترتیب علاوه بر این که میزان هزینه ها را کاهش می دهید، موفق می شوید تا میزان امنیت را نیز بالا ببرید.

در پاسخ به پرسش وی پی ان چیست می‌توان به صورت مختصر گفتVPN ، یک شبکه کامپیوتری منتقل‌کننده اطلاعات از طریق یک شبکه عمومی مانند اینترنت است، اما به لطف بهره بردن از الگوریتم‌های رمزنگاری، این ارتباط‌ها همچنان خصوصی باقی می‌مانند. با در نظر گرفتن هزینه‌های سرسام‌آور راه‌اندازی شبکه‌های محلی، وی پی ان راهکاری فوق‌العاده برای اتصال کامپیوترها به یکدیگر محسوب می‌شود.

در تعریفی ساده می توانیم اینگونه بگوییم که وی پی ان به جای اینکه شما را به یک فضای نا امن و شلوغ در اینترنت متصل کند شما را به یک شبکه خصوصی از اینترنت انتقال میدهد گه تنها به خودتان اختصاص دارد. وی پی ان ها به این صورت هستند که مکان یابی شما را با توجه به آی پی به جای وصل می کنند که اصلا به شما تعلق نداشته است. پس با توجه به این مورد می توانیم بگوییم که شما با استفاده کردن از VPN می توانید امنیت خودتان را در فضای اینترنت به وجود بیاورید.

فرض کنید در جزیره‌ای در اقیانوسی بزرگ، زندگی می‌کنید. هزاران جزیره در اطراف جزیره شما وجود دارد. برخی از جزایر به شما نزدیک و برخی دور هستند. متداول‌ترین روش به منظور مسافرت به جزیره دیگر، استفاده از یک کشتی مسافربری است. مسافرت با کشتی مسافربری، به منزله عدم وجود امنیت است، بدین معنی که هر کاری را که شما انجام دهید، توسط سایر مسافرین قابل مشاهده خواهد بود

.

در این مثال هر یک از جزایر مورد نظر را می‌توان مشابه یک شبکه محلی به :شبکه محلی دانست، اقیانوس به مثابه اینترنت است و مسافرت با یک کشتی مسافربری مشابه برقراری ارتباط با یک سرویس دهنده وب یا سایر دستگاه‌های موجود در اینترنت خواهد بود.

شما دارای هیچگونه کنترلی بر روی کابل‌ها و روتر موجود دراینترنت نیستید (مشابه عدم کنترل شما به عنوان مسافر کشتی مسافربری بر روی سایر مسافرین حاضر در کشتی). در صورتی‌که تمایل به ارتباط بین دو شبکه اختصاصی از طریق منابع عمومی وجود داشته باشد، اولین مسئله‌ای که با

چالش‌های جدی برخورد خواهد کرد، امنیت خواهد بود. فرض کنید، جزیره شما قصد ایجاد یک پل ارتباطی با جزیره مورد نظر را داشته باشد. مسیر ایجاد شده یک روش ایمن، ساده و مستقیم برای مسافرت ساکنین جزیره شما به جزیره دیگر را فراهم می‌آورد. همان‌طور که حدس زده‌اید، ایجاد و نگهداری یک پل ارتباطی بین دو جزیره مستلزم صرف هزینه‌های بالائی خواهد بود. (حتی اگر جزایر در مجاورت یکدیگر باشند). با توجه به ضرورت و حساسیت مربوط به داشتن یک مسیر ایمن و مطمئن، تصمیم به ایجاد پل ارتباطی بین دو جزیره گرفته شده‌است. در صورتی‌که جزیره شما قصد ایجاد یک پل ارتباطی با جزیره دیگر را داشته باشد که در مسافت بسیار طولانی نسبت به جزیره شما واقع است، هزینه‌های مربوط بمراتب بیشتر خواهد بود. وضعیت فوق، نظیر استفاده از یک خط Leased اختصاصی است. ماهیت پل‌های ارتباطی (خطوط اختصاصی) از اقیانوس (اینترنت) متفاوت بوده و کماکان قادر به ارتباط جزایر (شبکه‌های محلی) خواهند بود.

سازمان‌ها و موسسات متعددی از رویکرد فوق (استفاده از خطوط اختصاصی) استفاده می‌نمایند. مهم‌ترین عامل در این زمینه وجود امنیت و اطمینان برای برقراری ارتباط هر یک سازمان‌های مورد نظر با یکدیگر است. در صورتی‌که مسافت ادارات یا شعب یک سازمان از یکدیگر بسیار دور باشد، هزینه مربوط به برقراری ارتباط نیز افزایش خواهدیافت.

با توجه به مقایسه انجام شده در مثال فرضی، می‌توان گفت که بااستفاده از وی‌پی‌ان به هر یک از ساکنین جزیره یک زیردریائی داده می‌شود. زیردریائی فوق دارای خصایص متفاوت زیر است:

- دارای سرعت بالایی است.
- هدایت آن ساده است.
- قادر به استتار (مخفی نمودن) شما از سایر زیردریایی‌ها و کشتی‌ها است.
- قابل اعتماد است.

پس از تأمین اولین زیردریائی، افزودن امکانات جانبی و حتی یک زیردریائی دیگر مقرون به صرفه خواهد بود.

در مدل فوق، باوجود ترافیک در اقیانوس، هر یک از ساکنین دو جزیره قادر به تردد در طول مسیر در زمان دلخواه خود با رعایت مسایل ایمنی می‌باشند. مثال فوق بیانگر نحوه عملکرد وی‌پی‌ان است. هر یک از کاربران از راه دور شبکه قادر به برقراری ارتباطی امن و مطمئن بااستفاده از یک محیط

انتقال عمومی (نظیر اینترنت) با شبکه محلی موجود در سازمان خود خواهند بود. توسعه یک وی‌پی‌ان (افزایش تعداد کاربران از راه دور یا افزایش مکان‌های مورد نظر) بمراتب آسان‌تر از شبکه‌هایی است که از خطوط اختصاصی استفاده می‌نمایند. قابلیت توسعه فراگیر از مهم‌ترین ویژگی‌های یک وی‌پی‌ان نسبت به خطوط اختصاصی است.

با توجه به اینکه در یک شبکه وی‌پی‌ان به عوامل متفاوتی نظیر: امنیت، اعتمادپذیری، مدیریت شبکه و سیاست نیاز خواهد بود. استفاده از وی‌پی‌ان برای یک سازمان دارای مزایای متعددی است:

- گسترش محدوده جغرافیائی ارتباطی
- بهبود وضعیت امنیت
- کاهش هزینه‌های عملیاتی در مقایسه با روش‌های سنتی نظیرWAN
- کاهش زمان ارسال و حمل اطلاعات برای کاربران از راه دور
- بهبود بهره وری
- توپولوژی آسان،... است.

وی‌پی‌ان نسبت به شبکه‌های پیاده‌سازی شده با خطوط استیجاری، در پیاده‌سازی و استفاده، هزینه کمتری صرف می‌کند. اضافه و کم کردن گره‌ها یا شبکه‌های محلی به وی‌پی‌ان، به خاطر ساختار آن، با هزینه کمتری امکان‌پذیر است. در صورت نیاز به تغییر همبندی شبکه خصوصی ، نیازی به راه‌اندازی مجدد فیزیکی شبکه نیست و به صورت نرم‌افزاری، همبندی شبکه قابل تغییر است.

پس به اختصار میتوان گفت: شبکه‌ای است که اطلاعات در آن از طریق یک شبکه عمومی مانند اینترنت جابه‌جا می‌شود اما در عین حال با استفاده از الگوریتم‌های رمز نگاری و با احراز هویت این ارتباط هم‌چنان اختصاصی باقی می‌ماند

شبکه خصوصی مجازی به‌طور عمده برای ایجاد ارتباط بین شعبه‌های مختلف شرکت‌ها یا فعالیت از راه دور مورد استفاده قرار می‌گیرد.

اصول کاری وی پی ان

اف تی پی

درمیان رایانه‌های میزبان، اف‌تی‌پی به‌طور ویژه یک قراردادِ متداول برای دادوستد فرمان ها و پرونده‌ها در هر شبکه پشتیبان از قرارداد اینترنت و قرارداد هدایت انتقال (TCP/IP) مانند اینترنت و اینترانت

است .پیش‌فرض برای خدمات قاپ، درگاه ۲۱ TCP/و برای انتقال داده از درگاه ۲۰ TCP/استفاده می‌کند.

در یک انتقال اف‌تی‌پی دو رایانه دخیل است، یک کارساز و یک کاربر. کارساز (سرور) قاپ، برنامه‌های کارساز اف‌تی‌پی را اجرا می‌کند، و درخواست پذیرش در شبکه را رایانهٔ دیگر (یعنی کاربر) مطرح می‌کند. رایانه کاربر برنامه‌های کاربری اف‌تی‌پی را اجرا و یک ارتباط با کارساز بر قرار می‌کند.

هنگامی که یک ارتباط برقرار می‌شود کاربر می‌تواند تعدادی از برنامه‌ها را تغییر دهد (دستکاری محدود)، مانند بارگذاری پرونده در کارساز و باگیری پرونده از آن، یا بازنامیدن یا حذف پرونده‌ها در کارساز و مانند این‌ها.

هر شخص یا شرکت برنامه‌ساز می‌تواند یک کارساز قاپ یا برنامه‌های کاربری ایجاد کند، چرا که این قراردادی آزاد است.

در واقع همه بسترهای رایانه‌ای از اف‌تی‌پی پشتیبانی می‌کنند و به هر ارتباط رایانه‌ای که بر اساس قرارداد هدایت انتقال/قرارداد اینترنت باشد صرف‌نظر از این که از چه سامانه عاملی استفاده می‌شود، اگر رایانه‌ها اجازه دسترسی به قاپ را داشته باشند، این اجازه را می‌دهد که در پرونده‌های رایانه دیگر در این شبکه تغییراتی ایجاد کند.

قرارداد هدایت انتقال/قرارداد اینترنت

مدل TCP/IP یا مدل مرجع اینترنتی که گاهی به مدل DOD (وزارت دفاع)، مدل مرجع ARPANET نامیده می‌شود، یک توصیف خلاصه لایه TCP/IP برای ارتباطات و طراحی پروتکل شبکه کامپیوتری است TCP/IP .در سال ۱۹۷۰ بوسیله DARPA ساخته شده که برای پروتکل‌های اینترنت در حال توسعه مورد استفاده قرار گرفته‌است، ساختار اینترنت دقیقاًبوسیله مدل TCP/IP منعکس شده‌است.

مدل اصلی TCP/IP از ۴ لایه تشکیل شده‌است. سازمان IETF استانداردی که یک مدل ۵ لایه‌ای است را قبول نکرده است و پروتکل‌های لایه فیزیکی ولایه پیوند داده‌ها به وسیلهIETFاستاندارد نشده‌اند. سازمان IETF تمام مدل‌های لایه فیزیکی را تأیید نکرده است. با پذیرفتن مدل ۵ لایه‌ای در بحث اصلی بامسولیت فنی برای نمایش پروتکل می‌باشد این امکان هست که راجع به پروتکل‌های غیر IETFدر لایه فیزیکی صحبت کنیم. این مدل قبل از مدل مرجع OSI گسترش یافته و واحد وظایف مهندسی اینترنت(IETF) ، برای مدل و پروتکل‌های گسترش یافته تحت آن پاسخگو است، هیچ‌گاه خود را ملزم ندانست که توسط OSI تسلیم شود. درحالی که مدل بیسیک OSI کاملاً در آموزش استفاده شده است و OSI به یک مدل ۷ لایه‌ای معرفی شده‌است، معماری یک پروتکل واقعی RFC ۱۱۲۲مورد استفاده در محیط اصلی اینترنت خیلی منعکس نشده است. حتی یک مدرک معماری IETFکه اخیراً منتشر شده یک مطلب با این عنوان دارد: " لایه بندی مضر است ". تأکید روی لایه بندی به عنوان محرک کلیدی معماری یک ویژگی از مدل TCP/IP نیست، اما نسبت به OSI بیشتر است. بیشتر اختلال از تلاش‌های واحد OSI می‌آید لایه شبیه داخل یک معماری است که استفاده آن‌ها را به حداقل می‌رساند.

اصول کار وی پی ان

شبکه‌های رایانه‌ای به شکل گسترده‌ای در سازمان‌ها و شرکت‌های اداری و تجاری مورد استفاده قرار می‌گیرند. اگر یک شرکت از نظر جغرافیایی و در فضای کوچک متمرکز باشد، ارتباطات بین بخش‌های مختلف آن را می‌توان با یک شبکه محلی برقرار کرد. اما برای یک شرکت بزرگ که دارای فضای گسترده جغرافیایی و شعب مختلف در نقاط مختلف یک کشور یا در نقاط مختلف دنیا است و این بخش‌ها یا شعب نیاز دارند که با هم ارتباطاتِ اطلاعاتیِ امن داشته باشند، بایستی یک شبکه گسترده خصوصی بین نقاط آن ایجاد گردد. شبکه‌های اینترانت که فقط محدود به یک سازمان یا یک شرکت می‌باشند، به دلیل محدودیت‌های گسترشی نمی‌توانند چندین سازمان یا شرکت را تحت پوشش قرار دهند. شبکه‌های گسترده نیز که با خطوط استیجاری راه‌اندازی می‌شوند، در واقع شبکه‌های گسترده‌ٔ امنی هستند که بین مراکز سازمان‌ها ایجاد شده‌اند. پیاده‌سازی این شبکه‌ها علی‌رغم درصد پایین بهره‌وری، نیاز به هزینه زیادی دارد زیرا این شبکه‌ها به دلیل عدم اشتراک منابع با دیگران، هزینه مواقع عدم استفاده از منابع را نیز بایستی پرداخت کنند. راه‌حل غلبه بر این مشکلات، راه‌اندازی یک وی‌پی‌ان است.

فرستادن حجم زیادی از داده از یک رایانه به رایانه دیگر مثلاً در به‌هنگام‌رسانی بانک اطلاعاتی یک مشکل شناخته‌شده و قدیمی است. انجام این کار از طریق ایمیل به دلیل محدودیت گنجایش سرویس‌دهندگان ایمیل نشدنی است.

استفاده از اف تی پی هم به سرویس‌دهنده مربوطه و همچنین ذخیره‌سازی موقت روی فضای اینترنت نیاز دارد که قابل اطمینان نیست.

یکی از راه حل‌ها، اتصال مستقیم به کامپیوتر مقصد به کمک مودم است که در اینجا هم علاوه بر مودم، پیکربندی کامپیوتر به عنوان سرویس‌دهنده Remote Access Service لازم خواهد بود. از این گذشته، هزینه ارتباط تلفنی راه دور برای مودم هم قابل تأمل است.

اما اگر دو کامپیوتر در دو جای مختلف به اینترنت متصل باشند می‌توان از طریق سرویس به اشتراک‌گذاری فایل در ویندوز به سادگی فایل‌ها را رد و بدل نمود. در این حالت، کاربران می‌توانند به دیسک سخت کامپیوترهای دیگر همچون دیسک سخت کامپیوتر خودشان دسترسی داشته باشند. به این ترتیب بسیاری از راه‌های خرابکاری برای نفوذکنندگان بسته می‌شود.

شبکه‌های شخصی مجازی یا وی‌پی‌ان‌ها برای حل این‌گونه مشکلات مناسب هستند. وی‌پی‌ان به کمک رمزگذاری روی داده‌ها، درون اینترنت یک شبکه کوچک می‌سازد و تنها کسانی که آدرس‌های لازم و گذر واژه را در اختیار داشته باشد می‌توانند به این شبکه وارد شوند.

مدیران شبکه‌ای که بیش از اندازه وسواس داشته و محتاط هستند می‌توانند وی‌پی‌ان را حتی روی شبکه محلی هم پیاده کنند. اگر چه نفوذ کنندگان می‌توانند به کمک برنامه‌های Packet sniffer جریان داده‌ها را دنبال کنند اما بدون داشتن کلید رمزنگاری نمی‌توانند آن‌ها را بخوانند.

امنیت در وی پی ان

دیوار آتش

دیوار آتش Firewallبرابر فرهنگستان ادب و زبان فارسی :بارو تاربارو یا فایروال نام عمومی برنامه هایی است که از دستیابی غیرمجاز به یک سیستم رایانه جلوگیری می‌کنند. در برخی از این نرم افزار ها ، برنامه‌ها بدون اخذ مجوز قادر نخواهند بود از یک رایانه برای سایر رایانه‌ها، داده ارسال کنند. به این گونه نرم‌افزارها، تاربارو‌ی دو طرفه گویند، زیرا علاوه بر درگاه ورودی(Incoming) ، درگاه های خروجی (Outing) هم کنترل می‌شوند. بسته‌های اطلاعاتی که حاوی اطلاعات بدون مجوز هستند، به وسیله تاربارو متوقف می‌شوند .نوع دیگری از فایروال نیز وجود دارد که به آن فایروال معکوس می‌گویند. فایروال معکوس ترافیک خروجی شبکه را فیلتر می‌کند، برخلاف فایروال معمولی که ترافیک ورودی را فیلتر می‌کند. در عمل، فیلتر کردن برای هر دوی این مسیرهای ورودی و خروجی، احتمالاً توسط دستگاه یا نرم‌افزار یکسانی انجام می‌شود فایروال‌ها صرفاً پورت‌های ضروری برای کاربران یا سایر برنامه‌های موجود در خارج از شبکه را در دسترس و قابل استفاده می‌کنند. برای افزایش ایمنی، سایر پورت‌ها غیرفعال می‌گردد تا امکان استفاده از آنان توسط هکرها وجود نداشته باشد. در برخی موارد و با توجه به نیاز یک برنامه می‌توان موقتاً تعدادی از پورت‌ها را فعال و پس از اتمام کار مجدداً آنان را غیرفعال نمود. اگر برای اتصال به اینترنت از وسیله‌ای مانند روتر بیسیم، دستگاهی که به شما امکان می‌دهد تا از اینترنت بیسیم استفاده کنید، داشته باشید احتمالاً هم‌اکنون نیز دیوار آتش دارید و نیازی به نصب جداگانه آن بر روی سیستم در بسیاری از مواقع وجود ندارد

تاریخچه

اولین دیوار آتش در سال ۱۹۸۹ با ایجاد مفهوم پکت فیلترینگ متولد شد و فایروال ها به عنوان یک proxyبین شبکه داخلی و خارجی تعریف شدند.

در سال ۱۹۹۴ یک شرکت امنیتی اسرائیلی برای اولین بار در جهان اولینstateful inspection های مبتنی بر دیوار آتش را معرفی کرد.

در سال ۱۹۹۵ مفهوم دیوار های آتش حالت دار رشد قابل توجه ای داشت و این فایروال ها با اضافه شدن ویژگی های پیشرفته تری همچون وی پی ان و فانکشن هایی از جمله Access Control Methodها کامل تر شدند

در سال ۲۰۰۴ مفهوم یو تی ام یا مدیریت یمپارچه ی تهدید شکل گرفت و معرفی شد که در واقع ترکیبی از دیوار های آتش های سنتی یا ، سیستم تشخیص نفوذ یاIDS ، قابلیت آنتی ویروس ، قابلیت ایمیل فیلترینگ و سایر قابلیت ها در یک فایروال بودند .هر چند شرکتی همچون فورتینت در سال ۲۰۰۲ اولین محصول از یو تی ام های سری فورتی گیت را خود را ایجاد کرد ولی این محصول در آن سال مشخصاً نام یو تی ام نداشت

در سال ۲۰۰۸ مفهوم ان جی اف دابلیو یا دیوار های آتش نسل بعد شکل گرفت و معرفی شد و اولین ان جی اف دابلیو توسط یک شرکت کالیفرنیایی منتشر شد شد. تمرکز ان جی اف دابلیو ها بر روی Performance Degradationموقع فعالسازی همزمان چندین قابلیت و مدیریت بهتر کاربر ها،

اپلیکیشن ها و محتوا بود. همچنین در سال ۲۰۰۹ موسسه گارتنر نیز" ان جی اف دابلیو "را به به دیوار های آتش بحرانی معرفی کرد.

بعد از سال ۲۰۰۸ رشد و پیشرفت ان جی اف دابلیو ها و یو تی ام ها ادامه داشت تا در سال ۲۰۱۹ دسته جدیدی از فایروال ها تحت عنوان دیوار های آتش مبتنی بر سرویس یاService-Defined Firewall ها شکل گرفته و معرفی شدند. این دسته از فایروال ها که به صورت دیوار های آتش حالت دار لایه ۷ی هستند ترکیب هوش مصنوعی یا و هوش انسانی یا جهت بررسی مدل رفتار اپلیکیشن های مورد استفاده قرار می گیرند.

این فایروال ها با ترکیب سازه های شبکه-محوری همچون L7 packet inspection و AppID و حتی تکمیل شدن با استراتژی های فایروال های سنتی همچون دیوار های آنش مبتنی بر هویت و پ وضعیت کلی امنیت را در محیط شبکه تقویت می کنند. همچنین این فایروال ها جلوگیری از حرکات مشکوک انواع حملات نیز مورد استفاده قرار می گیرند. لازم به ذکر است فایروال ها را می توان در شبکه های داخلی به صورت- اجازه ای یا در شبکه SDDC و حتی چند ابری ها نیز استفاده نمود.

انواع فایروال

فایر وال پکت فیلترینگ:

فیلترینگ فایروال همان‌طور که از نامش پیداست فیلترینگ را بر اساس بسته‌های شبکه، ارزیابی بسته‌ها بر اساس آدرس‌های مقصد و مبدأ و برنامه‌های مختلف انجام می‌دهد و در لایه سوم شبکه کار می‌کند. این نوع فیلترینگ فایروال، دیتای موجود در بسته را ارزیابی نمی‌کند و فقط بر اساس آدرسِ قرار گرفته در بسته اجازه یا عدم اجازه ورود و یا خروج به شبکه را این به بسته خواهد داد از این رو این فایروال‌ها بسیار شبیه به ACL هاست. مثلا اگر می‌خواهید شبکه شما به وب‌سایت‌های بیرون از شبکه دسترسی داشته باشند باید پورت ۸۰ را روی فایروال باز بگذارید در غیر این صورت کاربران نمی‌توانند به هیچ وب‌سایتی به طور معمول دسترسی داشته باشند.

فایروال‌های Packet Filtering به No Stateful Packet و Stateful Packet تقسیم می‌شوند. در نوع No Stateful Packetیا بدون حالت، فیلترینگ بر اساس آدرس مشخص شده در بسته انجام می‌شود اما در حالت Stateful Packet علاوه بر ارزیابی آدرس، تمامی دیگر اطلاعات بسته در بانک اطلاعاتی فایروال ذخیره شده و بسته‌های بعدی با همین مشخصات را نیز بر اساس قانون در نظر گرفته شده برای قبلی‌ها رفتار می‌کند

فایروال circuit level gateway:

فایروال‌های Circuit level Gateway به‌عنوان یک میانجی در ارتباط تی سیپی قرار می‌گیرند و تا زمانی که ارتباط یا Session به صورت امن و کامل برقرار نشود اجازه دسترسی و اتصال نشست به سیستم مقصد را نمی‌دهند. در این نوع از ارتباط‌ها شما قابلیت بررسی معتبر بودن نشست را دارید و چون این نوع از فایروال‌ها دسترسی به تمامی داده‌های بسته ندارد و فقط قسمت‌هایی از آن را بررسی می‌کنند و بعد اجازه یا عدم اجازه را صادر می‌کنند، سرعت خوبی دارند.

فایر وال اپلیکیشن فیلترینگ:

این نوع فایروال معمولا به عنوان سیستم میانی بین سیستم شما و اینترنت قرار می‌گیرد و درخواست‌های شما را دریافت و به جای اینکه شما مستقیم به اینترنت دسترسی داشته باشید خود دیتای مورد درخواست شما را ارسال و جواب را از سرویس‌دهنده گرفته و پس از بررسی و صحت داده‌ها به سمت شما ارسال می‌کند و اگر کسی قبلا این داده‌ها را درخواست کرده باشد به جایی اینکه دوباره به سرویس‌دهنده مراجعه کند می‌تواند با قابلیت نگه‌داری از درخواست‌های قبلی از دیتای ذخیره‌شده در حافظه خود به شما پاسخ دهد. به این ترتیب سرعت پاسخ‌گویی شبکه شما را افزایش می‌دهد.
همان‌طور که از نام این مورد پیداست در لایه ۷ مدل OSI یعنی لایه Application فعالیت می‌کند.

فایر وال های هیبرید:

این نوع فایروال معمولا چند یا همه موارد بالا را در کنار دیگر محصولات امنیتی فراهم می‌کند و می‌تواند امنیت بالاتری برای شبکه شما به ارمغان بیاورد ولی باید این نکته را در نظر داشت که به‌کارگیری این نوع نیاز به فرد متخصص و نیز هزینه‌های بیشتری دارد.

مزایا و معایب

سخت افزاری:

مزایای استفاده از فایروال های سخت افزاری:

- از تمام شبکه محافظت می کند و مختص به یک سیستم نیست.
- محافظت جامع تر و کامل تری انجام می دهد و از این نظر دارای امنیت بیشتری است.
- تا زمانی که بر روی سیستم اجرا نشده اند هیچ تاثیری بر روی عملکرد سیستم ندارند.
- مستقل از سیستم عامل و نرم افزار های آن عمل می کنند و دارای سیستم عامل مجزایی برای خود هستند.

معایب استفاده از فایروال های سخت افزاری:

- هزینه ی بیشتری نسبت به فایروال های نرم افزاری دارند.
- به علت وجود سخت افزار نیاز به فضای جداگانه دارند و همچنین به کابل کشی های پیچیده بین شبکه نیاز خواهد بود.
- فایروال های سخت افزاری با مودم Dialup کار نمی کنند.

نصب و راه اندازی اولیه و همچنین Upgradeکردن آنها دشوار خواهد بود.

نرم افزاری

مزایای استفاده از firewall نرم افزاری:

- این فایروال ها بر روی کامپیوتر های شخصی و سرور ها استفاده می شوند در نتیجه بر روی هر سیستم عاملی قابل راه اندازی هستند.
- به صورت جداگانه و مستقل قابل نصب هستند.
- معمولا به صورت بسته ی نرم افزاری ارائه می شوند که شامل آنتی ویروس و آنتی اسپم نیز هست.
- به راحتی بروز رسانی می شوند.

معایب استفاده از firewall نرم افزاری:

- برای هر کامپیوتر موجود در شبکه می بایست جداگانه نصب شوند در نتیجه زمان بر خواهد بود.
- گاهی Uninstall کردن و حذف کامل آن ها با مشکل رو به رو می شود.
- به دلیل وابسته بودن به سیستم عامل در زمان های بحرانی مناسب نیستند.
- از پردازنده و مموری خود سیستم برای پردازش ها استفاده می کنند.

نحوه عملکرد فایروال های پکت فیلترینگ

packet filteringاز مجموعه قوانین ساده استفاده می کند ، بسته در هنگام ورود یا خروجی از یک اینترفیس ، جایی که ACL برای فیلتر کردن اعمال شده است توسط این ACL چک می شود و اینکار به

ترتیب از بالای لیست به سمت پایین لیست انجام می گیرد تا با یک ACE مطابقت پیدا کند به این ترتیب باقی لیست ACL بررسی نمی شود و نوع action مورد نظر مانند permit یا deny برای آن اعمال می شود. یک extended ACL در روتر سیسکو می تواند از معیارهای مختلفی در هدر لایه سه و چهار برای بررسی بسته ها استفاده کند که شامل مورد زیر می باشد:

- آدرس آی پی مبدا
- آدرس آی پی مقصد
- درگاه یا پورت ورودی
- درگاه یا پورت خروجی
- اطلاعات همگام سازی تی سی پی

امکانات

یکی از کاربردهای معمول فایروال واگذاری اختیار ویژه به گروهی خاص از کاربران جهت استفاده از یک منبع بوده، و همچنین بازداشتن کسانی که از خارج از گروه خواهان دسترسی به منبع هستند می‌باشد. استفاده دیگر فایروال جلوگیری از ارتباط مستقیم یک سری از رایانه‌ها با دنیای خارج می‌باشد. هر چند فایروال بخش مهمی از سیستم امنیتی را تشکیل می‌دهد ولی طراحان به این نکته نیز توجه می‌ورزند که اکثر حملات از درون شبکه می‌آیند و نه از بیرون آن

نحوه عملکرد بسیاری از سیستم‌های فایروال اینگونه‌است تمامی ارتباطات از طریق یک سرویس دهنده پروکسی به سمت فایروال هدایت شده و همین سرویس دهنده درباره‌ٔ امن بودن یا نبودن عبور یک پیام یا یک فایل از طریق شبکه تصمیم گیری می‌کند

این سیستم امنیتی معمولاً ترکیبی از سخت افزار و نرمافزار است. با توجه به ضرورت‌های استاندارد ISO27001 فایروالها جزء لاینفک شبکه های کامپیوتری قرارگرفته‌اند و یکی از دغدغه‌های اصلی مسئولین شبکه شده‌اند، در این میان با توجه به حساسیت هر سازمان لایه بندی و قدرت فایروال‌ها در نظر گرفته می‌شود. مثلاً در بانک‌ها به لحاظ اهمیت و ارزش اطلاعات فایروال‌ها جایگاه حساسی دارند و مسئولین شبکه بانک‌ها همواره دقت بسیاری را در این ارتباط به خرج می‌دهند. برخی از شرکت‌های بزرگی که در این ارتباط با مهم‌ترین بانک‌های بین‌المللی همکاری دارند عبارت‌اند از Cisco, Juniper, Securepointو...

رمز نگاری

رمزنگاری استفاده از روش‌های ریاضی، برای برقراری امنیت اطلاعات است. دراصل، رمزنگاری دانش تغییر دادن متن پیام یا اطلاعات به کمک کلید رمز و با استفاده از یک الگوریتن رمز است. به صورتی که تنها شخصی که از کلید و الگوریتم آگاه است می‌تواند اطلاعات اصلی از اطلاعات رمزگذاری، استخراج کند و شخصی که از یکی یا هر دوی آن‌ها اطلاع ندارد نمی‌تواند به اطلاعات دسترسی پیدا کند. دانش رمزنگاری بر پایه اصولی مانند نظریه اطلاعات، نظریه اعداد و آمار بنا شده‌است و امروزه به‌طور خاص در علم مخابرات مورد بررسی و استفاده قرار می‌گیرد. برابر رمزنگاری در زبان

انگلیسی واژه Cryptography است، که برگرفته از دو واژه زبان یونانی Kryptos به مفهوم «محرمانه» و Graphien به معنای «نوشتن» است

رمز نگاری کد گزاری پنهان گذاری

در رمزنگاری، وجود اطلاعات یا فرستادن پیام به هیچ وجه مخفی نیست، بلکه ذخیره اطلاعات یا فرستاده پیام مشخص است، اما تنها افراد مورد نظر می‌توانند اطلاعات اصلی را بازیابی کنند. بالعکس در پنهان گذاری ، اصل وجود اطلاعات یا فرستاده پیام محرمانه، مخفی نگاه داشته می‌شود و غیر از طرف فرستنده و طرف دریافت‌کننده کسی از فرستاده پیام آگاه نمی‌شود.

در رمزنگاری محتویات یک متن به صورت حرف به حرف و در بعضی موارد بیت به بیت تغییر داده می‌شود و هدف تغییر محتوای متن است نه تغییر ساختار زبان‌شناختی آن. در مقابل، کد گذاری تبدیلی است که واژه‌ای را با یک واژه یا نماد دیگر جایگزین می‌کند و ساختار زبان‌شناختی متن را تغییر می‌دهد.

ریشه واژه Cryptography برگرفته از یونانی به معنای «محرمانه نوشتن متون» است. رمزنگاری پیشینه طولانی و درخشان دارد که به هزاران سال پیش برمی‌گردد. کارشناسان رمزنگاری بین رمز و کد تمایز قائل می‌شوند. رمز عبارت است از تبدیل کاراکتر به کاراکتر یا بیت به بیت بدون آن که به محتویات زبان شناختی آن پیام توجه شود. در طرف مقابل، کد تبدیلی است که واژه‌ای را با یک واژه یا علامت دیگر جایگزین می‌کند. امروزه از کدها استفاده چندانی نمی‌شود اگر چه استفاده از آن پیشینه طولانی و پرسابقه‌ای دارد. موفق‌ترین کدهایی که تاکنون نوشته شده ابداع شده‌اند توسط ارتش ایالات متحده و در خلال جنگ جهانی دوم در اقیانوس آرام بکار گرفته شد.

اصول شش گانه کرشهف

آگوست کرشهف شهرت خود را از پژوهش‌های زبانشناسی و کتاب‌هایی که در این خصوص و زبان ولاپوک نوشته بود بدست آورد. او در سال ۱۸۸۳ دو مقاله با عنوان «رمزنگاری نظامی» منتشر کرد. در این دو مقاله، شش اصل پایه‌ای وجود داشتند که اصل دوم آن به عنوان یکی از قوانین رمزنگاری هنوز هم مورد استفاده دانشمندان رمزنگاری پیشرفته‌است:

- سامانه رمزنگاری نه فقط به لحاظ تئوری که در عمل هم باید غیرقابل شکست باشد.
- سامانه رمزنگاری نباید هیچ نکته پنهان و محرمانه‌ای داشته باشد. بلکه تنها چیزی که سری است کلید رمز است.
- کلید رمز باید به گونه‌ای قابل انتخاب شود که ۱) بتوان به راحتی آن را عوض کرد و ۲) بتوان آن را به خاطر سپرد و نیازی به یاداشت کردن کلید رمز نباشد.
- متون رمزنگاری باید از طریق خطوط تلگراف قابل مخابره باشند.
- دستگاه رمزنگاری یا اسناد رمزگذاری‌شده باید توسط یک نفر قابل حمل و نقل باشد.
- سامانه رمزنگاری باید به سهولت قابل راه‌اندازی باشد.

به چند دلیل عمده کلید رمز باید تنها اطلاعات محرمانه در یک سامانه رمزنگاری باشد:

۱. محرمانه نگه داشتن یک رشته بیت ۵۱۲ تایی (به‌طور معمول) بسیار ساده‌تر و عملی تر از محرمانه نگه داشتن یک الگوریتم یا روش پیاده‌سازی است.
۲. اگر کلید رمز افشا شود تنها با اتخاذ یک کلید تازه می‌توان دوباره به یک سامانه رمزنگاری تازه و امن دست پیدا کرد در صورتی‌که اگر امنیت سامانه رمزنگاری وابسته به الگوریتم و روش پیاده‌سازی باشد با افشای این اطلاعات بازتولید یک سامانه رمزنگاری تازه و امن بسیار دشوار خواهد بود.
۳. وقتی که کلید رمز تنها اطلاعات محرمانه یک سامانه رمزنگاری باشد می‌توان از یک سامانه مشترک (با کلیدهای متفاوت) برای ارتباط با گیرنده/فرستنده‌های گوناگون استفاده کرد در

صورتی که اگر غیر از این می‌بود برای ارتباط با هر فرستنده/گیرنده به یک الگوریتم و روش پیاده‌سازی تازه نیاز می‌بود.

٤. وقتی که الگوریتم و روش پیاده‌سازی برای همگان قابل دسترسی باشد مشکلات و حفره‌های امنیتی الگوریتم پیش از آنکه توسط یک حمله گر مورد سوء استفاده قرار بگیرد توسط محققان امنیتی مورد بررسی قرار گرفته و رفع می‌شود و بنابراین سامانه‌های رمزنگاری که بر پایه الگوریتم‌های روشن و قابل دسترسی عمل می‌کنند معمولاً قابل اعتمادتر هستند

رمزگذاری پیشرفته

با پدید آمدن رایانه‌ها و افزایش قدرت محاسباتی آنها، دانش رمزنگاری وارد زمینه علوم رایانه شد و این پدیده، موجب بروز سه تغییر مهم در مسائل رمزنگاری شد:

١. وجود قدرت محاسباتی بالا این امکان را پدیدآورد که روش‌های پیچیده‌تر و مؤثرتری برای رمزنگاری به وجود آید.
٢. روش‌های رمزنگاری که تا پیش از آن اصولاً برای رمزکردن پیام به کار می‌رفتند، کاربردهای تازه و زیادی پیدا کردند.
٣. تا پیش از آن، رمزنگاری عمدتاً روی اطلاعات متنی و با استفاده از حروف الفبا انجام می‌گرفت؛ اما ورود رایانه باعث شد که رمزنگاری روی انواع اطلاعات و بر مبنای بیت انجام شود.

تعاریف و اصطلاحات:

عناصر مهمی که در رمزنگاری مورد استفاده قرار می‌گیرند به شرح زیر است:

- **متن آشکار :**پیام و اطلاعات را در حالت اصلی و پیش از تبدیل شدن به حالت رمز، متن آشکار یا اختصاراً پیام می‌نامند. در این حالت اطلاعات قابل فهم توسط انسان است.
- **متن رمز :**به پیام و اطلاعات پس از تبدیل شدن به حالت رمز، گفته می‌شود. اطلاعات رمزگذاری‌شده توسط انسان قابل فهم نیست.
- **رمزگذاری (رمزکردن) :**عملیاتی است که با استفاده از کلید رمز، پیام را به رمز تبدیل می‌کند.
- **رمزگشایی (بازکردن رمز) :**عملیاتی است که با استفاده از کلید رمز، پیام رمزگذاری‌شده را به پیام اصلی بازمی‌گرداند. از نظر ریاضی، این الگوریتم عکس الگوریتم رمزکردن است.
- **کلید رمز :**اطلاعاتی معمولاً عددی است که به عنوان پارامتر ورودی به الگوریتم رمز در نظر گرفته می‌شود و عملیات رمزگذاری و رمزگشایی با استفاده از آن انجام می‌گیرد. انواع گوناگونی از کلید های رمز در رمزنگاری تعریف و استفاده می‌شود.

کاربرد های رمزنگاری

پیش از ورود رایانه‌ها به زمینه رمزنگاری، تقریباً کاربرد رمزنگاری محدود به رمزکردن پیام و پنهان کردن مفاد آن می‌شده‌است. اما در رمزنگاری پیشرفته سرویس‌های گوناگونی از جمله موارد زیر ارائه شده‌است:

- حفظ محرمانگی یا امنیت محتوا فرستاده یا ذخیره اطلاعات به نحوی که تنها افراد مجاز بتوانند از محتوای آن مطلع شوند، که همان سرویس اصلی و اولیه پنهان کردن مفاد پیام است.
- حفظ صحت داده ها یا سلامت محتوا: به معنای ایجاد اطمینان از صحت اطلاعات و عدم تغییر محتوای اولیه آن در حین فرستاده‌است. تغییر محتوای اولیه اطلاعات ممکن است به صورت اتفاقی (در اثر مشکلات مسیر ارسال) یا به صورت عمدی باشد.
- احراز هویت یا اصالت سنجی محتوا: به معنای تشخیص و ایجاد اطمینان از هویت فرستنده اطلاعات و عدم امکان جعل هویت افراد است.

- عدم انکار : به این معنی است که فرستنده اطلاعات نتواند در آینده فرستاده آن را انکار یا مفاد آن را تکذیب نماید.

چهار مورد بالا، کاربردهای اصلی رمزنگاری تلقی می‌شوند و دیگر اهداف و کاربردهای رمزنگاری، با ترکیب چهار مورد بالا قابل حصول هستند.

این کاربردها مفاهیم جامعی هستند و می‌توانند برای کاربردهای گوناگون پیاده‌سازی و استفاده شوند. برای نمونه سرویس اصالت محتوا هم در معاملات تجاری اهمیت دارد و هم در مسائل نظامی و سیاسی مورد استفاده قرار می‌گیرد. برای ارائه کردن هر یک از سرویس‌های رمزنگاری، بسته به نوع کاربرد، از پروتکل‌های گوناگون رمزنگاری استفاده می‌شود.

پروتکل رمزنگاری:

به‌طور کلی، یک پروتکل رمزنگاری، مجموعه‌ای از قواعد و روابط ریاضی است که چگونگی ترکیب کردن الگوریتم‌های رمزنگاری و استفاده از آن‌ها به منظور ارائهٔ یک سرویس رمزنگاری خاص در یک کاربرد خاص را فراهم می‌سازد.

معمولاً یک پروتکل رمزنگاری مشخص می‌کند که:

- اطلاعات موجود در چه قالبی باید قرار گیرند
- چه روشی برای تبدیل اطلاعات به عناصر ریاضی باید اجرا شود
- کدامیک از الگوریتم‌های رمزنگاری و با کدام پارامترها باید مورد استفاده قرار گیرند
- روابط ریاضی چگونه به اطلاعات عددی اعمال شوند
- چه اطلاعاتی باید بین طرف فرستنده و دریافت‌کننده رد و بدل شود
- چه مکانیسم ارتباطی برای انتقال اطلاعات مورد نیاز است.

برای نمونه می‌توان به پروتکل تبادل برای ایجاد و تبادل کلید رمز مشترک بین دو طرف اشاره نمود.

الگوریتم رمز نگاری

الگوریتم رمزنگاری، به هر الگوریتم یا تابع ریاضی گفته می‌شود که به علت دارا بودن خواص مورد نیاز در رمزنگاری، در پروتکل های رمز گذاری مورد استفاده قرار گیرد. اصطلاح الگوریتم رمزنگاری یک مفهوم جامع است و لازم نیست هر الگوریتم از این دسته، به‌طور مستقیم برای رمزگذاری اطلاعات مورد استفاده قرار گیرد، بلکه صرفاً وجود کاربرد مربوط به رمزنگاری مد نظر است.

در گذشته سازمان‌ها و شرکت‌هایی که نیاز به رمزگذاری یا سرویس‌های دیگر رمزنگاری داشتند، الگوریتم رمزنگاری منحصربه‌فردی را طراحی می‌نمودند. به مرور زمان مشخص شد که گاهی ضعف‌های امنیتی بزرگی در این الگوریتم‌ها وجود دارد که موجب سهولت شکسته شدن رمز می‌شود. به همین دلیل امروزه رمزنگاری مبتنی بر پنهان نگاه داشتن الگوریتم رمزنگاری منسوخ شده‌است و در روش‌های تازه رمزنگاری، فرض بر این است که اطلاعات کامل الگوریتم رمزنگاری منتشر شده‌است و آنچه پنهان است فقط کلید رمز است.

بنا بر این تمام امنیت حاصل شده از الگوریتم‌ها و پروتکل‌های رمزنگاری استاندارد ، متکی به امنیت و پنهان ماندن کلید رمز است و جزئیات کامل این الگوریتم‌ها و پروتکل‌ها برای عموم منتشر می‌شود.

بر مبنای تعریف فوق، توابع و الگوریتم‌های مورد استفاده در رمزنگاری به دسته‌های کلی زیر تقسیم می‌شوند:

- توابع بدون کلید
  - توابع درهم ساز
  - تبدیل‌های یک‌طرفه

- توابع مبتنی بر کلید
  - الگوریتم های کلید متقارن
    - الگوریتم‌های رمز قالبی
    - الگوریتم‌های رمز دنباله ای
    - توابع تصدیق پیام
  - الگوریتم های کلید نامتقارن
    - الگوریتم‌های مبتنی بر تجزیه اعداد صحیح
    - الگوریتم‌های مبتنی بر لگاریتم گسسته
    - الگوریتم‌های مبتنی بر منحنی های بیضوی
  - الگوریتم‌های امضای رقومی

الگوریتم‌های رمزنگاری بسیار زیاد هستند، اما تنها شمار اندکی از آن ها به صورت استاندارد درآمده‌اند.

رمزگذاری کلید متقارن

رمزنگاری کلید متقارن *یا *تک کلیدی*، به آن دسته از الگوریتم‌ها، پروتکل‌ها و سامانه‌های رمزنگاری گفته می‌شود که در آن هر دو طرف رد و بدل اطلاعات از یک کلید رمز یکسان برای عملیات رمزگذاری و رمزگشایی استفاده می‌کنند. در این قبیل سامانه‌ها، یا کلیدهای رمزگذاری و رمزگشایی یکسان هستند یا با رابطه‌ای بسیار ساده از یکدیگر قابل استخراج هستند و رمزگذاری و رمزگشایی اطلاعات نیز دو فرایند معکوس یکدیگر هستند.

واضح است که در این نوع از رمزنگاری، باید یک کلید رمز مشترک بین دو طرف تعریف شود. چون کلید رمز باید کاملاً محرمانه باقی بماند، برای ایجاد و رد و بدل کلید رمز مشترک باید از کانال امن

استفاده نمود یا از روش‌های رمزنگاری نامتقارن استفاده کرد. نیاز به وجود یک کلید رمز به ازای هر دو نفرِ درگیر در رمزنگاری متقارن، موجب بروز مشکلاتی در مدیریت کلیدهای رمز می‌شود

رمزگذاری کلید نامتقارن

رمزنگاری کلید نامتقارن در ابتدا با هدف حل مشکل انتقال کلید در روش متقارن و در قالب پروتکل های تبادل کیلی دهلمن پیشنهاد شد. در این نوع از رمزنگاری، به جای یک کلید مشترک، از یک زوج کلید به نام‌هایکلید عمومی و کلید خصوصی استفاده می‌شود. کلید خصوصی تنها در اختیار دارنده آن قرار دارد و امنیت رمزنگاری به محرمانه بودن کلید خصوصی بستگی دارد. کلید عمومی در اختیار کلیه کسانی که با دارنده آن در ارتباط هستند قرار داده می‌شود.

به مرور زمان، به غیر از حل مشکل انتقال کلید در روش متقارن، کاربردهای زیادی برای این نوع از رمزنگاری مطرح شده‌است. در سامانه‌های رمزنگاری نامتقارن، بسته به کاربرد و پروتکل مورد نظر، گاهی از کلید عمومی برای رمزگذاری و از کلید خصوصی برای رمزگشایی استفاده می‌شود و گاهی نیز، بر عکس، کلید خصوصی برای رمزگذاری و کلید عمومی برای رمزگشایی به کار می‌رود.

دو کلید عمومی و خصوصی با یکدیگر متفاوت هستند و با استفاده از روابط خاص ریاضی محاسبه می‌شوند. رابطه ریاضی بین این دو کلید به گونه‌ای است که کشف کلید خصوصی با در اختیار داشتن کلید عمومی، عملاً ناممکن است.

مقایسه رمزنگاری کلید های متقارن و نا متقارن

اصولاً رمزنگاری کلید متقارن و کلید نامتقارن دارای دو ماهیت متفاوت هستند و کاربردهای متفاوتی نیز دارند؛ بنابراین مقایسه این دو نوع رمزنگاری بدون توجه به کاربرد و سامانه مورد نظر کار دقیقی نخواهد بود. اما اگر معیار مقایسه، به‌طور خاص، حجم و زمان محاسبات مورد نیاز باشد، باید گفت که با در نظر گرفتن مقیاس امنیتی معادل، الگوریتم‌های رمزنگاری متقارن خیلی سریع‌تر از الگوریتم‌های رمزنگاری نامتقارن هستند

تجزیه و تحلیل:

تجزیه و تحلیل رمز یا شکستن رمز، به کلیه اقدامات مبتنی بر اصول ریاضی و علمی اطلاق می‌شود که هدف آن از بین بردن امنیت رمزنگاری و در نهایت بازکردن رمز و دستیابی به اطلاعات اصلی باشد. در تجزیه و تحلیل رمز، سعی می‌شود تا با بررسی جزئیات مربوط به الگوریتم رمز یا پروتکل رمزنگاری مورد استفاده و به کار گرفتن هرگونه اطلاعات جانبی موجود، ضعف‌های امنیتی احتمالی موجود در سامانه رمزنگاری یافته شود و از این طریق به نحوی کلید رمز به دست آمده یا محتوای اطلاعات رمزگذاری‌شده استخراج شود.

تجزیه و تحلیل رمز، گاهی به منظور شکستن امنیت یک سامانه رمزنگاری و به عنوان خرابکاری و یک فعالیت ضد امنیتی انجام می‌شود و گاهی هم به منظور ارزیابی یک پروتکل یا الگوریتم رمزنگاری و برای کشف ضعف‌ها و آسیب‌پذیری‌های احتمالی آن صورت می‌پذیرد. به همین دلیل، تجزیه و تحلیل رمز، ذاتاً یک فعالیت خصومت‌آمیز به حساب نمی‌آید؛ اما معمولاً قسمت ارزیابی و کشف آسیب‌پذیری را به عنوان جزئی از عملیات لازم و ضروری در هنگام طراحی الگوریتم‌ها و پروتکل‌های تازه به حساب می‌آورند و در نتیجه *تجزیه و تحلیل رمز* بیشتر فعالیت‌های خرابکارانه و ضد امنیتی را به ذهن متبادر می‌سازد. با توجه به همین مطلب از اصطلاح *حملات تحلیل رمز* برای اشاره به چنین فعالیت‌هایی استفاده می‌شود.

تحلیل رمز، در اصل اشاره به بررسی ریاضی الگوریتم (یا پروتکل) و کشف ضعف‌های احتمالی آن دارد؛ اما در خیلی از موارد فعالیت خرابکارانه، به جای اصول و مبنای ریاضی، به بررسی یک پیاده‌سازی خاص

آن الگوریتم (یا پروتکل) در یک کاربرد خاص می‌پردازد و با استفاده از امکانات گوناگون سعی در شکستن رمز و یافتن کلید رمز می‌نماید. به این دسته از اقدامات خرابکارانه، *حملات جانبی* گفته می‌شود.

رمزنگاری کلید عمومی

در رمزنگاری عمومی از ترکیب یک کلید خصوصی و یک کلید عمومی استفاده می‌شود. کلید خصوصی صرفاً برای کامپیوتر شما (ارسال‌کننده) قابل شناسایی و استفاده‌است. کلید عمومی توسط کامپیوتر شما در اختیار تمام کامپیوترهای دیگری که قصد ارتباط با آن را داشته باشند گذاشته می‌شود. به منظور رمزگشایی یک پیام رمز شده، یک کامپیوتر می‌بایست با استفاده از کلید عمومی (ارائه شده توسط کامپیوتر ارسال‌کننده) و کلید خصوصی مربوط به خود اقدام به رمزگشایی پیام ارسالی نماید. یکی از متداول‌ترین ابزارهای رمز نگاری کلید عمومی ، روشی با نام پی جی پی است. با استفاده از این روش می‌توان اقدام به رمزنگاری اطلاعات دلخواه خود نمود.

آی پی سک

IPsecیا همان Internet Protocol security عبارت است از مجموعه‌ای از چندین پروتکل که برای ایمن‌سازی پروتکل اینترنت در ارتباطات به وسیله احراز هویت و رمزگذاری در هر بسته (packet) در یک سیر داده به کار می‌رود. این پروتکل محصول مشترک مایکروسافت و سیسکو سیستمز است که در نوع خود جالب توجه است.

مزایا

- IPsecبر خلاف دیگر پروتکلهای امنیتی نظیر SSL, TSL, SSH که در لایه انتقال (لایه ۴) به بالا قرار دارند در لایه شبکه یا همان لایه ۳ مدل مرجع کار می‌کند یعنی لایه که آی پی در آن قرار دارد که باعث انعطاف بیشتر این پروتکل می‌شود به‌طوری‌که می‌تواند از پروتکل‌های لایه ۴ نظیر تی سی پی و یو دی پی محافظت کند.
- مزیت بعدی IPsec به نسبت بقیه پروتکل‌های امنیتی نظیر اس اس ال این است که: نیازی نیست که برنامه بر طبق این پروتکل طراحی شود

حالت های عمل

IPSECمی‌تواند حالت انتقال هاست به هاست را در شبکه و درمد تونل پیاده‌سازی کند.

حالت انتقال

در مد انتقال تنها پیلود بسته‌های IP معمولاً به صورت رمزگذاری شده یا معتبر است از آنجایی که هدر IP نه تغییر داده شده و نه رمز شده‌است، با این حال زمانی که هدر احراز هویت می‌شود، IP آدرس را نمی‌تواند ترجمه کند که این مقدار هش بی‌اعتبار است .لایه انتقال و لایه کاربرد معمولاً به وسیله hash امن می‌شوند؛ بنابراین آن‌ها نمی‌توانند به هیچ وجه تغییر پیدا کنند به عنوان مثال با ترجمه شماره پورت

حالت تونل

در مد تونل تمام بسته‌های اطلاعاتی IP رمزگذاری و احراز هویت می‌شوند. پس از آن در یک بسته IP جدید با یک سرآیند جدید کپسوله می‌شوند. حالت تونل برای ایجاد شبکه خصوصی مجازی در ارتباطات شبکه به شبکه (به عنوان مثال بین روتر و لینک سایت)، ارتباطات هاست به شبکه (مانند دسترسی به کاربر از راه دور) و ارتباطات هاست به هاست (مانند چت خصوصی) استفاده می‌شود.

آی پی سک و وی پی ان

پروتکل آی پی سک یکی از امکانات موجود برای ایجاد امنیت در ارسال و دریافت اطلاعات است. قابلیت این روش در مقایسه با الگوریتم‌های رمزنگاری بمراتب بیشتر است. پروتکل فوق دارای دو روش رمزنگاری است .Tunnel, Transport: در روشtunel ، هدر و Payload رمز شده درحالیکه در روش transport صرفاً payload رمز می‌گردد. پروتکل فوق قادر به رمزنگاری اطلاعات بین دستگاه‌های متفاوت است:

۱. روتر به روتر
۲. فایروال به روتر
۳. کامپیوتر به روتر
٤. کامپیوتر به سرویس‌دهنده

VPN-IP-sec فقط برای اینترنت

Ipsecبرخلاف PPTPوL2TP روی لایه شبکه یعنی لایه سوم کار می‌کند. این پروتکل داده‌هایی که باید فرستاده شود را همراه با همه اطلاعات جانبی مانند گیرنده و پیغام‌های وضعیت رمزگذاری کرده و به آن یک IP Header معمولی اضافه کرده و به آن سوی تونل می‌فرستد.

کامپیوتری که در آن سو قرار داردIP Header را جدا کرده، داده‌ها را رمز گشایی کرده و آن را به کامپیوتر مقصد می‌فرستد Ipsec.را می‌توان با دو شیوه Tunneling پیکر بندی کرد. در این شیوه انتخاب اختیاری تونل، سرویس گیرنده نخست یک ارتباط معمولی با اینترنت برقرار می‌کند و سپس از این مسیر برای ایجاد اتصال مجازی به کامپیوتر مقصد استفاده می‌کند. برای این منظور، باید روی کامپیوتر سرویس گیرنده پروتکل تونل نصب شده باشد. معمولاً کاربر اینترنت است که به اینترنت وصل می‌شود. اما کامپیوترهای درون LAN هم می‌توانند یک ارتباط VPN برقرا کنند. از آنجا که ارتباطIP از پیش موجود است تنها برقرار کردن ارتباط VPN کافی است.

در شیوه تونل اجباری، سرویس گیرنده نباید تونل را ایجاد کند بلکه این کار به عهده فراهم ساز است. سرویس گیرنده تنها باید به ISP وصل شود. تونل به‌طور خودکار از فراهم ساز تا ایستگاه مقصد وجود دارد. البته برای این کار باید هماهنگی‌های لازم باISP انجام بگیرد.

ویژگی های امنیتی در IP-sec

Ipsecاز طریق AH مطمئن می‌شود کهPacket های دریافتی از سوی فرستنده واقعی نه از سوی یک نفوذکننده (که قصد رخنه دارد) رسیده و محتویات شان تغییر نکرده AH.اطلاعات مربوط به تعیین اعتبار و یک شماره توالی در خود دارد تا از حملات Replay جلوگیری کند. اما AH رمزگذاری نمی‌شود. رمزگذاری از طریق Encapsulation Security Header یا ESH انجام می‌گیرد. در این شیوه داده‌های اصلی رمزگذاری شده وVPN اطلاعاتی را از طریق ESH ارسال می‌کند.

ESHهمچنین کارکردهایی برای تعیین اعتبار و خطایابی دارد. به این ترتیب دیگر به AH نیازی نیست. برای رمزگذاری و تعیین اعتبار روش مشخص و ثابتی وجود ندارد اما با این همه، IETFبرای حفظ سازگاری میان محصولات مختلف، الگوریتم‌های اجباری برای پیاده‌سازی Ipsec تدارک دیده. برای نمونه می‌توان بهMD5 ، DESیا Secure Hash Algorithm اشاره کرد. مهم‌ترین استانداردها و روش‌هایی که در Ipsec به کار می‌روند عبارتنداز:

- Diffie-Hellmanبرای مبادله کلیدها میان ایستگاه‌های دو سر ارتباط.
- رمزگذاری Public Key برای ثبت و اطمینان از کلیدهای مبادله شده و همچنین اطمینان از هویت ایستگاه‌های سهیم در ارتباط.
- الگوریتم‌های رمزگذاری مانند DES برای اطمینان از درستی داده‌های انتقالی.
- الگوریتم‌های درهم ریزی (Hash) برای تعیین اعتبار تک تکPacket ها.
- امضاهای دیجیتال برای تعیین اعتبارهای دیجیتالی.

آی پی سک بدون تونل

Ipsecدر مقایسه با دیگر روش‌ها یک برتری دیگر هم دارد و آن اینست که می‌تواند همچون یک پروتکل انتقال معمولی به کار برود.

در این حالت برخلاف حالت Tunneling همه IP packet رمزگذاری و دوباره بسته بندی نمی‌شود. به جای آن، تنها داده‌های اصلی رمزگذاری می‌شوند و Header همراه با آدرس‌های فرستنده و گیرنده باقی می‌ماند. این باعث می‌شود که داده‌های سرباز (Overhead) کمتری جابجا شوند و بخشی از پهنای باند آزاد شود. اما روشن است که در این وضعیت، خرابکاران می‌توانند به مبدأ و مقصد داده‌ها پی ببرند. از آنجا که در مدل OSI داده‌ها از لایه ۳ به بالا رمزگذاری می‌شوند خرابکاران متوجه نمی‌شوند که این داده‌ها به ارتباط با سرویس دهنده Mail مربوط می‌شود یا به چیز دیگر.

جریان یک ارتباط IP-sec

بیش از آن که دو کامپیوتر بتوانند از طریق Ipsec داده‌ها را میان خود جابجا کنند باید یکسری کارها انجام شود.

- نخست باید ایمنی برقرار شود. برای این منظور، کامپیوترها برای یکدیگر مشخص می‌کنند که آیا رمز گذاری، تعیین اعتبار و تشخیص خطا یا هر سه آن‌ها باید انجام بگیرد یا نه.
- سپس الگوریتم را مشخص می‌کنند، مثلاً DEC برای رمزگذاری و MD5 برای خطایابی.
- در گام بعدی، کلیدها را میان خود مبادله می‌کنند.

Ipsecبرای حفظ ایمنی ارتباط از SA استفاده می‌کند SA .چگونگی ارتباط میان دو یا چند ایستگاه و سرویس‌های ایمنی را مشخص می‌کندSA.ها از سوی SPI شناسایی می‌شوند SPI.از یک عدد تصادفی و آدرس مقصد تشکیل می‌شود. این به آن معنی است که همواره میان دو کامپیوتر دو SPI وجود دارد:
یکی برای ارتباط A و B و یکی برای ارتباط B به .A اگر یکی از کامپیوترها بخواهد در حالت محافظت شده داده‌ها را منتقل کند نخست شیوه رمزگذاری مورد توافق با کامپیوتر دیگر را بررسی کرده و آن شیوه را روی داده‌ها اعمال می‌کند. سپس SPI را در Header نوشته و Packet را به سوی مقصد می‌فرستد.

مدیریت کلید های رمز IP-sec

اگر چه Ipsec فرض را بر این می‌گذارد که توافقی برای ایمنی داده‌ها وجود دارد اما خودش برای ایجاد این توافق نمی‌تواند کاری انجام بدهد.
Ipsecدر این کار به IKE تکیه می‌کند که کارکردی همچون IKMP دارد. برای ایجاد SA هر دو کامپیوتر باید نخست تعیین اعتبار شوند. در حال حاضر برای این کار از راه‌های زیر استفاده می‌شود:

- Pre shared keys:روی هر دو کامپیوتر یک کلید نصب می‌شود که IKE از روی آن یک عدد Hash ساخته و آن را به سوی کامپیوتر مقصد می‌فرستد. اگر هر دو کامپیوتر بتوانند این عدد را بسازند پس هر دو این کلید دارند و به این ترتیب تعیین هویت انجام می‌گیرد
- رمزگذاری:Public Key هر کامپیوتر یک عدد تصادفی ساخته و پس از رمزگذاری آن با کلید عمومی کامپیوتر مقابل، آن را به کامپیوتر مقابل می‌فرستد. اگر کامپیوتر مقابل بتواند با کلید شخصی خود این عدد را رمز گشایی کرده و باز پس بفرستد برا ی ارتباط مجاز است. در حال حاضر تنها از روش RSA برای این کار پیشنهاد می‌شود.
- امضاء دیجیتال:در این شیوه، هر کامپیوتر یک رشته داده را علامت‌گذاری (امضاء) کرده و به کامپیوتر مقصد می‌فرستد. در حال حاضر برای این کار از روش‌های RSA و DSS استفاده می‌شود. برای امنیت بخشیدن به تبادل داده‌ها باید هر دو سر ارتباط نخست بر سر یک یک کلید به توافق برسند که برای تبادل داده‌ها به کار می‌رود. برای این منظور می‌توان همان کلید به دست آمده از طریق Diffie Hellman را به کاربرد که سریع تر است یا یک کلید دیگر ساخت که مطمئن تر است.

پروتکل Ike

پروتکلی که امروزه استفاده از آن رایج است مبادله کلید اینترنت به انگلیسی Internet Key : Exchange، به اختصار IKEنام دارد. نسخه اول آن در سال ۱۹۹۸ به بازار آمد و اسم رایج آن IKEv1 است. به دلیل این که اولین نسخه از IKE توسط IPsec به‌عنوان پیش‌فرض استفاده شد. خصوصیات IKEv1بخش‌های پنهان آن را ارتقا داد. برای ارتقای آن در ۲۰۰۵، IKEv2ایجاد شد. با این به‌روزرسانی، این پروتکل قابل‌اعتمادتر شد و در مقابل حملات DOS منعطف‌تر شد.

سرویس دهنده AAA:

سرویس دهندگان AAA به منظور ایجاد امنیت بالا در محیط‌های وی‌پی‌ان از نوع دستیابی از راه دور استفاده می‌گردند. زمانیکه کاربران با استفاده از خط تلفن به سیستم متصل می‌شوند، سرویس دهنده AAAدرخواست آن‌ها را اخذ و عملیات زیر را انجام خواهد داد:

- شما چه کسی هستید(authentication)
- شما مجاز به انجام چه کاری هستید(authorization)
- حسابداری شما چه کار هایی را انجام داده اید؟(accounting)

انواع وی پی ان و پروتکل های آن

شبکه وی پی ان سایت به سایت

نوعی از وی پی ان با نام Site to site VPN امکان این را فراهم می کند که شعبه‌هایی از یک شرکت با یکدیگر در تعامل باشند . این نوع از وی‌پی‌ان vpnهنگامی اهمیت خود را نمایش می دهد که صدها نفر قصد این را داشته باشند که با سرور ارتباط داشته باشند . بجای این که هر یک از این ها از نوع "وی‌پی‌ان دسترسی از راه دور" استفاده نمایند ، به گروه‌هایی تقسیم می‌گردند که به عنوان شعبه‌هایی از شرکت مورد نظر ، از طریق "وی‌پی‌ان مکان به مکان" به هم متصل گشته و اجازه استفاده از منابع همدیگر را می‌دهند . اجزای مورد احتیاج جهت راه اندازی این نوع وی‌پی‌ان همانند نوع قبلی می باشد . تفاوت بسیار مهم این هست که معمولا ، دیگر احتیاجی به داشتن کلاینت بر روی هر رایانه نخواهد بود .

بر پایه اینترنت:

چنانچه شرکت یک یا چند مکان دور داشته باشد که قصد داشته باشند به همدیگر متصل شده و شبکه محلیشان را در اختیار همدیگر قرار بدهند ، از طریق وی‌پی‌ان بر پایه اینترنت نیز می توانند استفاده کنند.

بر پایه اکسترانت:

چنانچه شرکت‌ها یا سازمان‌های و موسساتی قصد این را داشته باشند که با یکدیگر در ارتباط باشند ولی نیازی به اینترنت نداشته باشند کافیست شبکه اینترانت خود را با امکان دستیابی به وی‌پی‌ان بر پایه اکسترانت ، به شبکه اینترانت دیگر شرکت یا موسسه متصل نمایند . بدین ترتیب امکان کار کردن با یکدیگر فراهم شده و از طرفی می توانند از شبکه اینترانت خود نیز محافظت نمایند.

شبکه وی پی ان دستیابی از راه دور

این نوع از وی پی ان با نام Remote Access VPN اجازه می‌دهد که افراد حقیقی (منظور از از افراد حقیقی شرکت‌ها ، سازمان ها و ... نیستند) به شبکه یا شبکه های خصوصی یک شرکت متصل شوند . این کاربران قادرند با متصل شدن به سرور VPN شرکت مورد نظر ، از منابع آن استفاده نمایند . اشخاصی که از وی پی ان شرکت استفاده می کنند افرادی هستند که جزو کارکنان هستند که از راه دور کارهای شرکت را انجام می دهند.

جهت ایجاد ارتباط در این نوع وی‌پی‌ان به دو جزء حیاتی احتیاج است:

۱ : NAS -مخفف عبارت Network Access Server بوده است که ارتباط را از سمت سرور کنترل می نماید NAS . امکان دارد به عنوان یک سرور اختصاصی در سمت شبکه شرکت فعالیت نموده یا به عنوان یک نرم افزاری که بروی شبکه‌های اشتراکی کار می نماید ، اطلاعات احراز هویت کاربر را دریافت کرده و با بررسی دقیق آن‌ها به وی اجازه متصل شدن به شبکه شرکت را فراهم کند

.۲ -برنامه سمت کاربر : کاربر جهت متصل شدن به سرور وی‌پی‌ان می بایست از نرم افزاری استفاده نماید که علاوه بر برقراری ارتباط و احراز هویت آن ، داده‌های ارسالی را رمزگذاری نموده و داده‌های دریافتی را نیز رمزگشایی نماید . بسیاری از سیستم عامل‌ها (از جمله ویندوز، لینوکس ، مکینتاش و ...) برنامه‌های تهیه شده ای جهت متصل شدن به سرور وی‌پی‌ان در اختیار کاربران قرار می‌دهند.

کانکشن های مورد استفاده در وی پی ان رمزگذاری را توسط پروتکل های مخصوص تونل سازی انجام می دهند . تا جایی به امکان داشته باشد اندک توضیحاتی همراه با جزییات تقریبا کاملی درباره پروتکل

های مورد استفاده توسط ارایه دهنده های اینترنت نموده و مقایساتی ما بین پروتکل ها در مبحث امنیتی ، سرعت این سرویس و سازگاری آن با سیستم عامل های مختلف انجام می دهیم.

انواع پروتکل های وی پی ان

پروتکل PPTP(Point To Point Tunneling Protocol)

PPTPیکی از رایج ترین و البته ضعیف ترین پروتکل‌هایی است که در ارتباطات VPN استفاده می‌شود . PPTPمخفف Point-to-Point Tunneling Protocol است توسط شرکت مایکروسافت ایجاد شده است که برای تونلینگ استفاده شده و با پروتکل MPPE رمزگذاری می‌شود.

این پروتکل آسیب پذیری‌های امنیتی مختلفی دارد که ارتباط و داده‌های ارسالی را در خطر لو رفتن توسط سازمان های امنیتی قرار می‌دهد ولی چون در اکثر سیستم عامل‌ها تعبیه می‌شود و از طرفی استفاده از آن آسان و سریع است، به یکی از رایج ترین پروتکل‌ها تبدیل شده. اگر امنیت ارتباطتان اهمیت ندارد PPTPمی‌تواند بهترین گزینه برای شما باشد.

Point-to-Point Tunneling Protocolیا به اختصار PPTP از دهه‌ی ۱۹۹۰ مورد استفاده قرار می‌گرفته است و در ابتدا در محصولات مایکروسافت ویندوز بسیار پیاده‌سازی می‌شد (از بروزرسانی ۱.۳ ویندوز ۹۵ به بعد) PPTP .از چند پروتکل دیگر استفاده می‌کند تا راهکاری کامل، شامل Point-to-Point Protocolیا به اختصار PPP و نسخه‌ی بهبود یافته‌ی GRE فراهم شود.

برای کارکرد PPTP باید در ابتدا یک کانال کنترلی راه‌اندازی شود که برای ایجاد یک Tunnel داده مورد استفاده قرار گیرد. این Tunnel داده باGRE ، Encapsulateمی‌گردد که یک PPP Frame را حمل می‌کند ؛ PPP از حمل چندین پروتکل از جمله IP پشتیبانی می‌نماید. همچنین PPP از احراز هویت، رمزگذاری و فشرده‌سازی پشتیبانی می‌کند.

PPTPاز نظر پیکربندی یکی از ساده‌ترین پروتکل‌هاست، اما از نظر محرمانه بودن دارای نقاط ضعف شناخته‌شده‌ای می‌باشد. دلیل این امر این است که PPTP برای پشتیبانی از رمزگذاری RC4 که دارای آسیب‌پذیری‌های شناخته شده است عمدتا از Microsoft Point-to-Point Encryption یا به اختصار MPPEاستفاده می‌نماید.

پروتکل PPTP دارای متد رمزنگاری و یاد احرازهویت نیست، بصورت point to point پیاده سازی میشود. موارد امنیتی میتواند در مبدا و مقصد پیاده سازی شود. ین پروتکل رایج ترین پروتکل انتقال اطلاعات در ابزارهای Microsoft می باشد. از لحاط امنیتی و سطوح دسترسی راه دور مانند VPN می باشد.
پروتکل روی پورت TCP 1723 فعالیت میکند و پس از برقراری کانکشن TCP مدیریت تونل برعهده GREخواهد بود.

راه اندازی و استفاده از این پروتکل آسان است، PPTPدارای مشکلات و آسیب پذیری های بسیاری است، بیشترین آسیب پذیری ها مربوط به احراز هویت می باشد.

پروتکل L2TP/IPsec(Layer 2 Tunneling protocol)

پروتکل L2TP با همکاری چندین شرکت ایجاد شده‌است. این پروتکل از ویژگی‌های PPTP و L2F استفاده کرده‌است. پروتکل L2TP به صورت کامل آی پی سک را حمایت می‌کند. از پروتکل فوق به منظور ایجاد تونل بین موارد زیر استفاده می‌گردد:

- سرویس گیرنده و روتر
- NASو روتر
- روتر و روتر

عملکرد تونل‌زنی مشابه حمل یک کامپیوتر توسط یک کامیون است. فروشنده، پس از بسته‌بندی کامپیوتر (پروتکل مسافر) درون یک جعبه (پروتکل کپسوله‌سازی) آن را توسط یک کامیون (پروتکل حمل‌کننده) از انبار خود (اینترفیس ورودی تونل) برای متقاضی ارسال می‌دارد. کامیون (پروتکل حمل‌کننده) از طریق بزرگراه (اینترنت) مسیر خودرا طی، تا به منزل شما (اینترفیس خروجی تونل) برسد. شما در منزل جعبه (پروتکل کپسول سازی) را باز و کامیون (پروتکل مسافر) را از آن خارج می‌نمایید.

پروتکل L2TP مخفف Internet Protocol Security بوده و پروتکلی برای امن کردن شبکه عمومی اینترنت است. این پروتکل علاوه بر قابلیت رمزگذاری، می‌تواند تونل نیز بزند. این پروتکل در دوحالت Transport Modeکه فقط اطلاعات موجود در قسمت داده بسته IP را رمزگذاری می‌کند و حالت Tunnel Modeکه کل بسته IP (داده و سربرگ (هدر)) را رمزگذاری می‌کند.

این پروتکل در کانکشن‌های VPN در کنار پروتکل L2TP کار می‌کند.

L2TPمخفف Layer 2 Tunneling بوده، برای تونلینگ استفاده می‌شود، بر پایه PPP بوده و قابلیت رمزگذاری ندارد. با این حال در ترکیب با IPSec می‌تواند بسیار مناسب باشد.

ترکیب پروتکل L2TP/IPSec در سیستم عامل‌های جدید بصورت تعبیه شده پشتیبانی می‌شود. یعنی راه اندازی آن آسان بوده و از طرفی امنیت بالایی هم دارد. ولی چون قابلیت کانفیگ یا پیکربندی زیادی ندارد نسبت به OpenVPN در رده پایین تری قرار می‌گیرد.

پروتکل OpenVPN

اوپن وی پی ان (Openvpn) در حال حاظر مشهورترین و محبوب‌ترین پروتکل به عنوان VPN مورد استفاده قرار می‌گیرد و شما هر ارائه‌دهنده وی پی ان را که بررسی کنید (در داخل و خارج از کشور)، قطعا این سرویس را در لیست پروتکل‌های خود دارند. حتی ارائه دهندگانی هم در خارج از کشور وجود دارند که تنها به همین پروتکل اکتفا کرده و تنها Openvpn را ارائه می‌دهند.

در ادامه به برتری‌ها و دلایلی که باعث می‌شود آن را نسبت به دیگر پروتکل‌ها ترجیح دهند، صحبت خواهیم کرد.

Openvpn برخلاف سایر پروتکل‌های تونل سازی مبتنی بر IPSec (مانند L2tp)، برای تأیید اعتبار و رمزنگاری اطلاعات، به SSL / TLS تکیه می‌کند.

این فناوری امنیتی استاندارد، برای ایجاد اتصالات ایمن و از راه دور از مکانی به مکان دیگر یا از نقطه‌ای به نقطه دیگر است. استفاده ازSSL برای محافظت از معاملات مالی، انتقال داده‌ها، ایمیل و موارد دیگر بسیار معروف و شناخته شده است.

OpenVPN تقریبا با تمامی سیستم‌عامل‌های اصلی مانند ویندوز، اندروید، IOS، مک و لینوکس سازگار است. این VPN، استانداردهای قدرتمند رمزنگاری را ارائه می‌دهد و برای شکستن محدودیت‌های جغرافیایی بسیار عالی عمل می‌کند.

Openvpn اوپن سورس (Open Source) است و از رمزگذاری حداکثر ۲۵۶ بیتی پشتیبانی می‌کند.

اوپن سورس بودن دارای مزایای بسیاری است که به صورت تخصصی وارد این مبحث نمی‌شویم ولی به عنوان مثال به دلیل آن که ساختار آن در اختیار همه قرار می‌گیرد، آسیب‌پذیری‌های امنیتی توسط افراد مختلف مورد بررسی قرار گرفته و حل می‌شوند.

به عبارت ساده‌تر، OpenVPNیک ایجاد کننده‌ی ارتباط خصوصی یا تونل بین کاربر و سرور VPN است. ترافیکی که از طریق آن عبور می‌کند با رمزگذاری کاملاً محافظت می‌شود و در نهایت داده‌های شما در برابرISP ها Internet Service Providerیا ارائه دهنده اینترنت هکرها و شخص ثالث محافظت می‌شود.

هر فعالیتی که با دستگاه‌تان بر روی اینترنت انجام می‌دهید (حتی یک کلیک برای وارد شدن به سایت)، داده‌هایی به اینترنت ارسال می‌شود که پکت (Packet) نام دارند، این بسته‌ها ابتدا توسط اپلیکیشن OpenVPN رمزنگاری شده و سپس عملیات ارسال به سمت سرور Openvpn انجام می‌شود.

داده‌های ارسالی به همراه کلید رمزگشایی، توسط سرور دریافت و رمزگشایی می شوند. سپس درخواست یا همان پکت شما، به وب سرور (اینترنت) ارسال می‌شود و مجددا از سمت وب سرور، داده‌های درخواستی شما (مثلا اجرای سایت گوگل) به سرور Openvpn ارسال می شود.

داده‌های بازگشتی توسط سرور Openvpn برای بار دیگر رمزنگاری شده و سپس به دستگاه یا رایانه شما ارسال می‌شود و عملیات رمزگشایی صورت می‌گیرد.

حالا این پروسه تحت دو حالت و توسط دو پروتکل می‌تواند انجام شود. UDP و TCP که در مورد تفاوت‌های آن‌ها در به صورت تخصصی پرداختیم. در ادامه توضیح کوتاه و ساده‌ای از عملکرد این دو پروتکل ارائه خواهیم داد.

در اینجا برخی از مزایای استفاده از OpenVPN می‌پردازیم:

- بسیار امن

برای محافظت از داده‌های خود در برابر اشخاص ذینفع، پروتکل OpenVPN گزینه‌ی بسیار مناسبی است. این برنامه از رمزنگاری‌های سطح بالا و رمزگذاری ۲۵۶ بیتی استفاده می‌کند. این امر باعث می‌شود که سرقت اطلاعات شما توسط حملات مجرمان سایبری غیرممکن شود.

- سازگاری با چندین سیستم‌عامل

یکی از بهترین ویژگی‌های OpenVPN، قابلت نصب آن در تمام سیستم‌عامل‌های رایج دسکتاپ و موبایل است. همچنین از سیستم‌عامل‌های با محبوبیت کمتر مانند FreeBSD،OpenBSD و Solaris پشتیبانی می‌کند.

- مسدود کردن آن سخت است

تشخیص و مسدود کردن اتصالات OpenVPN کار ساده‌ای نیست. آن‌ها می‌توانند از پورت‌های TCP و همچنین UDP استفاده کنند. علاوه بر این، پیکربندی OpenVPN در پورت ۴۴۳ شما را قادر می‌سازد تا هرگونه فایروال را به اشتباه وادارید، زیرا همان پورتی است که توسط ترافیک HTTPS استفاده می‌شود.

- کنترل کامل اتصالات

برخلاف پروتکل‌های دیگر، OpenVPN به شما آزادی انتخاب بین TCP و UDP را برای انتقال داده‌های خود می‌دهد. کنترل بیشتر بر روی اتصالات، تطبیق آن‌ها را با نیازهای شما آسان‌تر می‌کند.

- پشتیبانی کامل از محرمانگی پیشرو

این اقدام امنیتی فوق‌العاده مفید احتمال به خطر افتادن اطلاعات شخصی شما را به میزان قابل توجهی کاهش می‌دهد. دلیل این امر آن است که کلیدهای منحصر به فرد برای هر بخش تولید می‌شود.

در اینجا چند مورد از ویژگی‌های منفی استفاده از OpenVPN می‌پردازیم:

- راه‌اندازی اولیه

راه‌اندازی و اتصال به Openvpn برای بار اول ممکن است کمی پیچیده‌تر از دیگر سرویس‌ها باشد (شاید دو مرحله بیشتر نیاز دارد) که آموزش تصویری و ویدیویی آن در صفحه برای تمامی سیستم‌عامل‌ها درج شده است و با توجه به مزایای آن، قابل چشم پوشی است. در Openvpn تنها مرحله‌ای که با دیگر سرویس‌ها متفاوت است قسمت وارد کردن سرور مورد نظر می‌باشد که به جای وارد کردن سرور، می‌بایست فایل سرور را فراخوانی کنید.

- نیاز به نصب اپلیکیشن

OpenVPN با هیچ سیستم‌عاملی ادغام نمی‌شود. بنابراین برای استفاده از آن باید اپلیکیشن آن را نصب کنید.

- افت سرعت ناچیز

OpenVPN به‌عنوان امن‌ترین پروتکل VPN در نظر گرفته می‌شود. اما این پروسه رمزنگاری که در بالا به آن اشاره کردیم، ممکن است افت سرعت ناچیزی داشته باشد (قابل چشم پوشی است).

پروتکل IKEv2(Internet Key Exchange version 2)

ikev2در واقع از دو عبارت ike و v2 تشکیل شده است. منظور از ike مخفف Internet Key *Exchange*بوده و v2 نشان‌دهنده نسخه دوم از این پروتکل است که در این نسخه، به یک پروتکل پیشرفته وی پی ان تبدیل شد. به طوری که تعادلی در امنیت و سرعت ایجاد کرد ikev2 .حاصل همکاری و توسعه دو شرکت سیسکو و مایکروسافت است.

در مورد پروسه رمزنگاری VPNها آن پرداختیم. ولی اگر بخواهیم آن را به صورت جمع بندی شده در نظر بگیریم، هرچه پروسه رمزنگاری اطلاعات پیچیده‌تر و قوی‌تر باشد، سرعت اتصال، کاهش پیدا می‌کند. چرا که با هر درخواستی که شما در فضای اینترنت ارسال می‌کنید، وی پی ان ابتدا آن را رمزنگاری کرده و سپس اجازه ارسال صادر می‌شود.

با توجه به آماری که در فیت نت بدست آوردیم، ۹۹ درصد کاربران، نیازی به رمزنگاری اطلاعات در سطح بسیار بالا ندارند.

برای مثال زمانی که شما قصد وب گردی و یا تماشای ویدیو دارید، آیا واقعا نیاز است که اطلاعات شما به صورت ۲۵۶ بیتی رمزنگاری شود؟ از طرفی پروتکل‌هایی مانند PPTP هستند که سطح رمزنگاری بسیار پایینی دارند و طبیعتاً سرعت بالاتر.

در ikev2 هر دو مورد در نظر گرفته شده و امنیت تا حد مناسبی ارتقا یافته و همچنین باعث افت سرعت محسوس نمی‌شود.

IKEv2مانند هر پروتکل وی پی ان دیگر، مسئولیت ایجاد تونل ایمن بین کاربر و سرور VPN را بر عهده دارد. در این پروسه، ابتدا با تأیید اعتبار کاربر و سرور انجام می‌شود (تایید اعتبار نام کاربری و رمز عبوری که پس از خرید اشتراک دریافت می‌کنید). سپس توافق می‌شود از کدام روش رمزگذاری استفاده شود.

IKEv2یک پروتکل رمزنگاری ریکوئست و ریسپانس هاست .(Request – Response)این وی‌پی‌ان، مشخصه SA یا Security Association را ایجاد کرده و کنترل می‌نماید.

به عبارت ساده، ikev2وظیفه ایجاد امنیت بین دو نهاد را دارد. در این مورد، کاربر و سرور VPN این دو نهاد را تشکیل می‌دهند. این کار با تولید کلید رمزنگاری متقارن یکسان برای هر دو نهاد انجام می‌شود و کلید یاد شده برای رمزنگاری و رمزگشایی کلیه داده‌هایی که از طریق VPN عبور می‌کنند، استفاده می شود.

در اینجا به تعدادی از تفاوت‌های اصلی بین IKEv2 و IKEv1 می‌پردازیم:

- IKEv2 به کمک تأیید هویت EAP، از دسترسی از راه دور به صورت پیش فرض پشتیبانی می‌کند.
- IKEv2 برای پهنای باند کمتر از IKEv1 در نظر گرفته شده است.
- پروتکل IKEv2 VPN از کلیدهای رمزنگاری برای هر دو طرف استفاده می‌کند و باعث ارتقا امنیت آن نسبت به IKEv1 می‌شود.
- IKEv2 از پشتیبانی MOBIKE برخوردار است. این به آن معنی است که می‌تواند در برابر تغییرات شبکه مقاوم باشد.
- بر خلاف IKEv1، نسخه دوم آن می تواند تشخیص دهد که آیا اتصال وی پی ان برقرار است یا خیر. این ویژگی به IKEv2 امکان برقراری مجدد اتصال قطع شده را می‌دهد.
- رمزنگاری IKEv2 از الگوریتم‌های بیشتری نسبت به IKEv1 پشتیبانی می‌کند.

پروتکل SSTP(Secure Socket Tunneling Protocol)

SSTPمخفف Secure Socket Tunneling Protocolاست و پروتکلی برای تونلینگ است با اینحال در کنار پروتکل SSL برای رمزگذاری، برای کانکشن‌های VPN بسیار مناسب است SSTP .از ویندوز ویستا سرویس پک ۱ به بعد بصورت تعبیه شده توسط این سیستم عامل‌ها پشتیبانی می‌شود و به دلیل همین پشتیبانی اغلب بهتر ازOpenVPN است. با کانفیگ کردن این پروتکل برای استفاده از رمزگذاری AES یک کانکشن قوی خواهید داشت. استفاده از SSTP بیشتر از سایر پروتکل‌ها پیشنهاد می‌شود.

تونل زنی روی وی پی ان

تونل زدن چیست

در شبکه‌های رایانه‌ای به کاربر اجازه می‌دهد تا به سرویس‌هایی که در شبکه‌اش ارائه نمی‌شوند، دسترسی پیدا کند. یکی از استفاده‌های مهم پروتکل‌های تونل‌زنی اجرای یک پروتکل خارجی برروی شبکه‌ایست که آن پروتکل را پشتیبانی نمی‌کند؛ برای مثال استفاده از IPv6 برروی شبکه مبتنی بر. IPv4

این روش ها کاربران و یا شبکه های IPV6 را روی بستر IPV4 به یکدیگر متصل می کند. تصور کنید دفاتر یک سازمان در نقاط مختلف کشور به آدرس و سرویس های IPV6 تجهیز شده اند اما بستر ارتباطی بین دفاتر، اینترنت و یا ISP ای است که صرفا ترافیک IPV4 عبور می دهند. در چنین شرایطی مدیر شبکه قادر خواهد بود با بکارگیری روش هایTunneling ، دفاتر IPv6 را روی بستر IPV4 به یکدیگر متصل کند و کاربران IPV6 بدون اطلاع از بستر ارتباطی به راحتی از سرویس های IPV6 استفاده کنند. علاوه بر مثال فوق ایجاد ارتباط کاربر یا سایت با اینترنت IPV6 روی بستر IPV4 نیز با روش های Tunneling امکان پذیر می باشد که در ادامه جزئیات آن را بررسی خواهیم کرد.

بدین معنی که اگر سازمانی تصمیم بگیرد که به اینترنت IPV6 متصل شود اما تنها روش اتصال اینترنتی آن IPV4 باشد،این روش امکان ایجاد ارتباط با اینترنت IPV6 را فراهم می کند که در ادامه به آن خواهیم پرداخت.

در روش های IPV6 Tunneling ایده بدین صورت است که محدوده آدرس IPV6 هر سایت با توجه به آدرس بیرونی روتر مرزی آن سایت که از نوع IPV4 است، انتخاب می شود. به عبارت دیگر آدرس بیرونی روتر مرزی که از نوع IPV4 است در داخل محدوده آدرس IPV6 هر سایت گنجانده می شود. بدین ترتیب وقتی از یک سایت IPV6 ارتباطی با سایت مقصد IPV6 ایجاد می کنیم، روتر مرزی سایت مبدا با توجه به آدرس مقصدIPV6 ، آدرس بیرونی IPV4 روتر مرزی سایت مقصد را بدست می آورد.

سپس روتر مرزی سایت مبدا به صورت اتوماتیک تونلی با سایت مقصد روی بستر IPV4 ایجاد می کند و ترافیک روی آن تونل ارسال می کند.

پورتکل‌های تونل‌زنی با استفاده از قرار دادن بسته درخواست سرویس در درون قسمت داده یک پروتکل دیگر عمل می‌کنند. تونل‌زنی نیز مانند TCP/IP از مدل لایه‌ای استفاده می‌کند اما معمولاً لایه‌های با حمل بسته سرویس در درون بدنه یک بسته دیگر، لایه‌بندی شبکه حمل‌کننده را به‌هم می‌زند. عموماً پروتکل مقصد در لایه‌هایی بالاتر از پروتکل حمل‌کننده قرار می‌گیرند.

اکثر شبکه‌های وی‌پی‌ان به منظور ایجاد یک شبکه اختصاصی با قابلیت دستیابی از طریق اینترنت از امکان تونل‌زنی استفاده می‌نمایند. در روش فوق تمام بسته اطلاعاتی در یک بسته دیگر قرار گرفته و از طریق شبکه ارسال خواهد شد. پروتکل مربوط به بسته اطلاعاتی خارجی (پوسته) توسط شبکه و دو نقطه (ورود و خروج بسته اطلاعاتی) قابل فهم است. دو نقطه فوق را *اینترفیس‌های تونل* می‌گویند.
تونل‌زنی مستلزم استفاده از سه پروتکل است:

۱. پروتکل حمل‌کننده: پروتکلی است که شبکهٔ حامل اطلاعات استفاده می‌نماید.
۲. پروتکل کپسوله سازی از پروتکل‌هایی نظیر IPSec,L2F,PPTP,L2TP یا GRE استفاده می‌گردد.
۳. پروتکل مسافر:از پروتکل‌هایی نظیر IPX,IP یا NetBeui به منظور انتقال داده‌های اولیه استفاده می‌شود

با استفاده از روش تونل‌زنی می‌توان عملیات جالبی را انجام داد. مثلاً می‌توان از بسته‌ای اطلاعاتی که پروتکل اینترنت را حمایت نمی‌کند نظیرNetBeui درون یک بسته اطلاعاتی آی‌پی استفاده و آن را از طریق اینترنت ارسال نمود یا می‌توان یک بسته اطلاعاتی را که از یک آدرس آی پی غیرقابل روت (اختصاصی) استفاده می‌نماید، درون یک بسته اطلاعاتی که از آدرس‌های معتبر آی‌پی استفاده می‌کند، مستقر و از طریق اینترنت ارسال نمود.

در شبکه‌های وی‌پی‌ان نوع سایت به سایت، از پروتکل جی‌آرای (به انگلیسی GRE :یا generic routing encapsulation)به عنوان پروتکل کپسوله‌سازی استفاده می‌گردد. فرایند فوق نحوه استقرار و

بسته‌بندی *پروتکل مسافر* از طریق پروتکل *حمل‌کننده* برای انتقال را تبین می‌نماید. پروتکل حمل‌کننده، عموماً آی‌پی است. این فرایند شامل اطلاعاتی در رابطه با نوع بسته‌های اطلاعاتی برای کپسوله نمودن و اطلاعاتی در رابطه با ارتباط بین سرویس گیرنده و سرویس دهنده‌است. در برخی موارد از پروتکل آی پی سک (در حالت تونل) برای کپسوله‌سازی استفاده می‌گردد. پروتکل آی‌پی‌سک، قابل استفاده در دو نوع شبکه وی‌پی‌ان (سایت به سایت و دستیابی از راه دور) است. اینترفیس‌های تونل می‌بایست دارای امکانات حمایتی از آی‌پی‌سک باشند.

در شبکه‌های وی‌پی‌ان نوع دستیابی از راه دور، تونل‌زنی با استفاده از PPP انجام می‌گیرد. پروتکل نقطه به نقطه به عنوان حمل‌کننده سایر پروتکل‌های آی‌پی در زمان برقراری ارتباط بین یک سیستم میزبان و یک سیستم ازه دور، مورد استفاده قرار خواهد گرفت. هر یک از پروتکل‌های زیر با استفاده از ساختار اولیه PPP ایجاد و توسط شبکه‌های وی‌پی‌ان دستیابی از راه دور استفاده می‌گردند:

پروتکل های درون وی پی ان

تونل‌زنی را می‌توان روی دو لایه از لایه‌های OSI پیاده کرد PPTP .و L2TP از لایه ۲ یعنی پیوند داده استفاده کرده و داده‌ها را در قالبFrame های پروتکل نقطه به نقطه (PPP) بسته‌بندی می‌کنند. در این حالت می‌توان از ویژگی‌های PPP همچون تعیین اعتبار کاربر، تخصیص آدرس پویا مانندDHCP فشرده سازی داده‌ها یا رمزگذاری داده‌ها بهره برد.

با توجه به اهمیت ایمنی انتقال داده‌ها در وی‌پی‌ان، در این میان تعیین اعتبار کاربر نقش بسیار مهمی دارد. برای این کار معمولاً از CHAP استفاده می‌شود که مشخصات کاربر را در این حالت رمزگذاری شده جابه‌جا می‌کند Call back .هم دسترسی به سطح بعدی ایمنی را ممکن می‌سازد. در این روش پس از

تعیین اعتبار موفقیت‌آمیز، ارتباط قطع می‌شود. سپس سرویس دهنده برای برقرار کردن ارتباط جهت انتقال داده‌ها شماره‌گیری می‌کند. هنگام انتقال داده‌ها، Packetهای IP, IP X یا NetBEUI در قالب Frameهای PPP بسته‌بندی شده و فرستاده می‌شوند PPTP .هم Frame های PPP را پیش از ارسال روی شبکه بر پایه IP به سوی کامپیوتر مقصد، در قالبPacket های IP بسته‌بندی می‌کند. این پروتکل در سال ۱۹۹۶ از سوی شرکت‌هایی چون مایکروسافت ، Ascend، ۳ com و Robotics US پایه‌گذاری شد. محدودیت PPTP در کار تنها روی شبکه‌های IP باعث ظهور ایده‌ای در سال ۱۹۹۸ شد L2TP .روی X.25,Frame Relayیا ATM هم کار می‌کند. برتری L2TP در برابر PPTP این است که به‌طور مستقیم روی رسانه‌های گوناگون WAN قابل انتقال است.

پروتکل L2F توسط سیسکو ایجاد شده‌است. در این پروتکل از مدل‌های تعیین اعتبار کاربر که توسط PPPحمایت شده‌اند استفاده شده‌است پروتکل PPTP توسط کنسرسیومی متشکل از شرکت‌های متفاوت ایجاد شده‌است. این پروتکل امکان رمزنگاری ۴۰ بیتی و ۱۲۸ بیتی را دارا بوده و از مدل‌های تعیین اعتبار کاربر که توسط PPP حمایت شده‌اند، استفاده می‌نماید.

پروتکل L2TP با همکاری چندین شرکت ایجاد شده‌است. این پروتکل از ویژگی‌های PPTP و L2F استفاده کرده‌است. پروتکل L2TP به صورت کامل آی پی سک را حمایت می‌کند. از پروتکل فوق به منظور ایجاد تونل بین موارد زیر استفاده می‌گردد:

- سرویس گیرنده و روتر
- NASو روتر
- روتر و روتر

عملکرد تونل‌زنی مشابه حمل یک کامپیوتر توسط یک کامیون است. فروشنده، پس از بسته‌بندی کامپیوتر (پروتکل مسافر) درون یک جعبه (پروتکل کپسوله‌سازی) آن را توسط یک کامیون (پروتکل حمل‌کننده) از انبار خود (اینترفیس ورودی تونل) برای متقاضی ارسال می‌دارد. کامیون (پروتکل حمل‌کننده) از طریق بزرگراه (اینترنت) مسیر خودرا طی، تا به منزل شما (اینترفیس خروجی تونل) برسد. شما در منزل جعبه (پروتکل کپسول سازی) را باز و کامیون (پروتکل مسافر) را از آن خارج می‌نمایید.

وی پی ان در ایران و ساخت یک وی پی ان ساده در ویندوز

وی پی ان در ایران

در حدود سال ۱۳۹۱ طرح ایجاد VPNبومی در ایران مطرح شد اما مسئولان بعدها اعلام کردند که این طرح از نظر اقتصادی با شکست مواجه شده‌است

اگرچه وی‌پی‌ان کاربردهای بسیاری دارد، اما یکی از کاربردهای اصلی وی‌پی‌ان در ایران استفاده از آن به عنوان فیلتر شکن است. برای دسترسی به وی‌پی‌ان در ایران می‌توان از طریق برخی شرکت‌های سرویس‌دهنده اقدام کرد. اخباری از ایرنا درباره وی پی ان:

دبیر شورای عالی فضای مجازی در جمع خبرنگاران به اعلام جزئیات فیلترشکن‌های قانونی پرداخت و گفت: ما نیز در مرکز ملی فضای مجازی کشور موافق این مسئله هستیم که با توجه به نیازهایی که در مشاغل گوناگون و بین افراد وجود دارد، سطوح مختلف دسترسی به اینترنت را در نظر بگیریم.
در این رابطه، پیشنهادات لازم به کارگروه تعیین مصادیق مجرمانه داده شده و در حال تهیه آیین نامه و دستورالعمل این کار هستیم.

وی اشاره کرد: ما دوست داشتیم این آیین نامه طی دو یا سه ماه قبل آماده می‌شد اما متاسفانه جلسات کارگروه دیر به دیر تشکیل می‌شود و این مسئله موجب کندی در تصمیم‌گیری می‌شود اما امیدواریم در اسرع وقت به نتیجه برسیم.
فیروزآبادی در خصوص ارائه و فروش وی پی ان قانونی در کشور گفت: این بحث از گذشته در شورای عالی فضای مجازی مطرح بوده اما اجرایی نشده است. امیدواریم با توجه به این که هم اکنون اقتصاد وی پی ان اقتصاد بزرگی شده است با مسئولیت پذیری دادستانی و وزارت ارتباطات، شاهد شکل‌گیری اپراتورهای وی پی ان رسمی در کشور باشیم.

او اشاره کرد: فیلترشکن ها باید طبق مقررات، با نظم مشخص و برای مواردی که نیاز است از طریق این اپراتورها به صورت رسمی واگذار شود و مورد استفاده قرار گیرد .
وی درباره این که ارائه این فیلترشکن‌ها شرایط خاصی دارد، گفت: بله نیاز به ساز وکار دارد. مثلا سازمان‌هایی هستند که به دلیل برخی مسایل امنیتی نیاز به استفاده از وی پی ان دارند، این موارد هم در کارهای دولتی و بانکی وجود دارد. ضمن اینکه در بعضی حوزه‌ها شاهد تحریم وسیع سایت‌های آمریکایی هستیم. این کشور دسترسی ما به بسیاری از اپلیکیشن‌ها را تحریم کرده و کسب و کارهایی برای دسترسی به این اپلیکیشن‌های تحریم شده، نیاز به استفاده از وی پی ان دارند.

آیین نامه مورد استفاده در این زمینه در حال تهیه در کارگروه تعیین مصادیق است. ما نیز نه به عنوان عضو این کارگروه بلکه در کنارشان حضور داریم و امیدواریم زودتر تنظیم شود تا مسئله ساماندهی وی پی ان در کشور به نتیجه برسد .

او درباره جرایمی مانند استفاده و فروش وی پی ان نیز افزود: طرحی در حال تدوین در مجلس است که می تواند در این مسئله کمک کننده باشد. متولی تهیه طرح، مرکز پژوهش های مجلس است البته از مرکز ملی هم نظر گرفته شده است. این طرح آماده رفتن به صحن علنی مجلس است.
فیروزآبادی در خصوص این که سیستم عامل بومی به کجا رسیده است، گفت: ما با همراهی وزارت ارتباطات و معاونت علمی و فناوری ریاست جمهوری یک توافق و تقسیم کار سه جانبه تهیه کرده‌ایم که انشاءالله طی مراسمی از این توافق نامه رو نمایی خواهیم کرد .

طرح‌هایی که الان در زمینه سیستم عامل بومی اندروید هم از آن صحبت می‌شود، می‌تواند یک بخشی از این توافق باشد، ولی حرکت اصلی ما به سمت ملی شدن است.

ساخت یک وی پی ان در ویندوز

ویندوز دارای امکان جنبی و توانایی سرخود عمل به عنوان VPNسرور است که از پروتکل تانلینگ سر به سر(PPTP) استفاده می کند. این امکان جنبی مخفی می باشد و همانند سایر امکانات جنبی ویندوز ۱۰ می توانید آن را فعال نموده یا مدیریت نمایید. در اینجا طریقه پیدا کردن پروتکل تونلینگ سر به سر ویندوز ۱۰ و نصب وی پی ان سرور بحص میشود بحث می شود.

نصب کردن و ایجاد VPNسرور برای اتصال به شبکه خانگی خود در جاده، بازی کردن گیم به صورت شبکه با LAN یا بالا بردن امنیت جستجوی وب بخصوص در زمان استفاده از اتصال وایفای عمومی و دلایل زیاد دیگری؛ مفید است. این روش در ویندوز ۸، ویندوز ۷ و ویندوز ۱۰ قابل استفاده است و کار می کند. این سرور از پروتکل تونلی کردن سر به سر (PPTP) استفاده می کند.

توجه :در بعضی از نسخه های آپریت ویندوز ۱۰ مثل آپدیت خالقین ویندوز ۱۰ Windows 10 Creators Updateممکن است در ایجاد VPNسرور مشکلی ایجاد شود که بخاطر عدم استارت سرویس های مسیریابی (Routing) و دسترسی دور (Remote Access Service) است. این یک مشکل شناخته شده است که هنوز در آپدیت های ویندوز رفع نشده است. هرچند می توان با ادیت چند کلید رجیستری ویندوز این مشکل را بطور موقت رفع کرد.

هرچند امکان **ایجاد VPN سرور در ویندوز** یک خصیصه جالب است اما ایجاد VPNسرور به این شیوه یک گزینه ایده آل نیست و محدودیت هایی دارد، از جمله:

- به امکان فوروارد کردن پورت ها از روتر خود نیاز خواهید داشت

مجبورید پورت ویندوز و پورت PPTP VPN سرور را مستقیما در اینترنت افشا کنید که از نقطه نظر امنیتی کار ایده آلی نیست. بایستی از پسوردهای قوی استفاده کرده و از پورتی استفاده کنید که از پورت های پیش فرض نباشد.

- نصب VPN سرور و استفاده از نرم افزارهایی مثل LogMeIn Hamachi و TeamViewer آسان نیست. در صورت نیاز به این نرم افزارها بهتر است برای ایجاد VPNسرور از نرم افزارهای مخصوص این کار استفاده کنید.

۱. برای ایجاد VPN سرور در ویندوز، ابتدا بایستی پنجره Network Connections را باز کنید. سریعترین راه باز کردن این استفاده از سرچ استارت ویندوز یا زدن شورت کات یا کلید میانبر Win + Rو باز کردن دیالوگ Run است. می توانید دیالوگ Run را از منوی دسترسی ویندوز ۱۰ باز کنید. سپس دستور ncpa.cplرا تایپ کرده و دکمه Enterویندوز را بزنید.
۲. در پنجره اتصالات شبکه (Network Connections) دکمه Altکیبورد را بزنید تا منوی کامل نمایش یابد. سپس از منوی فایل گزینه New Incoming Connection را انتخاب کنید.
۳. در مرحله بعد حساب کاربری را انتخاب کنید که می تواند بطور ریموت به ویندوز کامپیوتر یا لپ تاپ وصل شود. برای افزایش امنیت سیستم خود بهتر است یک حساب کاربری جدید با محدودیت ههای دسترسی و پسوورد قوی بسازید بجای اینکه از حساب کاربری اصلی خود یعنی حساب با مجوز مدیر استفاده کنید. می توانید ساخت حساب کاربری را با زدن دکمه Add someoneانجام دهید. به هر حال از هر حساب کاربری که استفاده می کنید اطمینان حاصل کنید که رمزعبور قوی داشته باشد. زیرا رمزعبور ضعیف خیلی سریع با استفاده از دیکشنری حملات هک شکسته و کرک می شود.
٤. وقتی حساب کاربری مورد نظر را انتخاب کردید، دکمه Next را بزنید
٥. در پنجره بعدی که باز می شود گزینه Through the Internet را تیک بزنید تا امکان اتصال به وی پیا ان از طریق اینترنت فراهم شود. احتمالا فقط همین یک گزینه را خواهید دید اما اگر از سخت افزار dial-up استفاده می کنید ممکن است گزینه های دیگری هم وجود داشته باشد.
٦. حالا می توانید پروتکل شبکه ای که برای اتصالات ورودی بایستی فعال باشد را انتخاب کنید. برای مثال، اگر نمی خواهید افرادی که به VPN سرور شما وصل می شوند به فایل های اشتراکی و پرینتر شبکه محلی دسترسی داشته باشند، می توانید گزینه File and Printer Sharing for Microsoft Networksرا غیرفعال کنید.
۷. وقتی تنظیمات را انجام دادید، دکمه Allow Access را بزنید
۸. در مرحله بعد ویندوز شروع به پیکربندی و راه اندازی حساب کاربری انتخابی شما می پردازد که ممکن است چند ثانیه تا دقیقه طول بکشد.

۹. در این نقطه VPNسرور شما و آماده و در حال اجرا است و می تواند درخواست های اتصال ورودی را دریافت نماید. اگر خواستید VPN سرور خود را غیرفعال کنید، به سادگی می توانید به پنجره Network Connections برگشته و آیتم Incoming Connections را حذف کنید.

تنظیمات روتر وای فای

اگر از طریق اینترنت به VPN سرور جدید خود وصل می شوید، لازم است که پورت فروارد‌ینگ وایفای و روتری که ترافیک از طریق آن به سیستم شما ارسال می شود را فعال کنید. بنابراین وارد صفحه تنظیمات پیش فرض وایفای خود شده و پورت ۱۷۲۳ را به آدرس آی پی کامپیوتری که VPN سرور را روی آن نصب کرده اید، ست کنید.

برای بیشترین امنیت ممکن، می توانید قانونی برای فوروارد پورت ایجاد کنید و از پورت تصادفی خارجی مثل ۲۳۲۴۳ استفاده کنید بجای اینکه از پورت داخلی ۱۷۲۳ استفاده کنید. اینکار موجب امنیت بیشتر اتصال شما بر روی VPN سرور و امنیت سیستم کامپیوتر یا لپ تاپ شما می شود.

همچنین می توانید از روتر یا فایروال استفاده کرده و تنها اتصالات ورودی (incoming connections) آدرس IP های خاصی که مشخص می کنید را قبول کند.

اگر می خواهید اطمینان حاصل کنید که همیشه می توانید به VPN سرور خود وصل شوید، می توانید یک سرویس DNS دینامیک از قبیل سرویس DynDNS روی روتر خود نصب کنید.

طریقه اتصال به وی پی ان سرور خود

برای وصل شدن به وی پی ان سرور شخصی خود، لازم است که کامپیوتر شما دارای یک آدرس آی پی عمومی باشد آدرس IP شبکه شما بر روی اینترنتو یا از آدرس DNS دینامیک آن استفاده کنید اگر سرویس DNS دینامیک را نصب کرده اید.

صرفنظر از نسخه ویندوزی که می خواهید از آن به VPN سرور خود وصل شوید، می توانید در کادر سرچ استارت خود عبارت vpn را تایپ کرده و دیالوگ اتصال باز می شود و مشخصات مورد نیاز را وارد کنید. در ویندوز ۱۰ این دیالوگ به نام Change Virtual Private Networks (VPN)خواهد بود اما در ویندوز ۷ نام آن Set up a virtual private network (VPN)است.

در دیالوگی که باز می شود از شما نام اتصال (هر نامی که دوست دارید) را به همراه آدرس اینترنت (نام دامنه یاآدرس آی پی مشخص شده) می خواهد.

منابع

۱. https://fa.wikipedia.org/wiki/%D8%B4%D8%A8%DA%A9%D9%87_%D8%AE%D8%B5%D9%88%D8%B5%DB%8C_%D9%85%D8%AC%D8%A7%D8%B2%DB%8C

۲. https://fa.wikipedia.org/wiki/%D9%87%D9%85%E2%80%8C%D8%A8%D9%86%D8%AF%DB%8C_%D8%B4%D8%A8%DA%A9%D9%87

۳. https://fa.wikipedia.org/wiki/%D9%85%D8%AD%DB%8C%D8%B7_%D8%A7%D9%86%D8%AA%D9%82%D8%A7%D9%84

۴. https://fa.wikipedia.org/w/index.php?title=%D8%A7%D8%B1%D8%AA%D8%A8%D8%A7%D8%B7%D8%A7%D8%AA_%D8%AF%D8%A7%D8%AF%D9%87%E2%80%8C%D8%A7%DB%8C&action=edit&redlink=1

۵. https://fa.wikipedia.org/wiki/%D8%AE%D8%B7_%D8%A7%D9%86%D8%AA%D9%82%D8%A7%D9%84

۶. https://fa.wikipedia.org/wiki/%D9%86%D8%B8%D8%B1%DB%8C%D9%87_%D8%A7%D8%B7%D9%84%D8%A7%D8%B9%D8%A7%D8%AA

۷. https://fa.wikipedia.org/wiki/%D9%BE%D8%B1%D9%88%D8%AA%DA%A9%D9%84_%D8%A7%D9%86%D8%AA%D9%82%D8%A7%D9%84_%D9%81%D8%A7%DB%8C%D9%84

۸. https://fa.wikipedia.org/wiki/%D9%85%D8%AC%D9%85%D9%88%D8%B9%D9%87_%D9%BE%D8%B1%D9%88%D8%AA%DA%A9%D9%84_%D8%A7%DB%8C%D9%86%D8%AA%D8%B1%D9%86%D8%AA

۹. https://fa.wikipedia.org/wiki/%D8%AF%DB%8C%D9%88%D8%A7%D8%B1_%D8%A2%D8%AA%D8%B4

۱۰. https://kaliboys.com/firewalls/

۱۱. https://iranhost.com/blog/%DA%86%D9%87%D8%A7%D8%B1-%D8%AF%D8%B3%D8%AA%D9%87-%D8%A7%D8%B5%D9%84%DB%8C-%D9%81%D8%A7%DB%8C%D8%B1%D9%88%D8%A7%D9%84-%D9%87%D8%A7-%D9%88-%D8%A8%D8%B1%D8%B1%D8%B3%DB%8C-%D9%85%D8%B2%D8%A7%DB%8C%D8%A7/

۱۲. https://iranhost.com/blog/%DA%86%D9%87%D8%A7%D8%B1-%D8%AF%D8%B3%D8%AA%D9%87-%D8%A7%D8%B5%D9%84%DB%8C-%D9%81%D8%A7%DB%8C%D8%B1%D9%88%D8%A7%D9%84-%D9%87%D8%A7-%D9%88-%D8%A8%D8%B1%D8%B1%D8%B3%DB%8C-%D9%85%D8%B2%D8%A7%DB%8C%D8%A7/

۱۳. https://server.ir/%D9%85%D9%82%D8%A7%D9%84%D8%A7%D8%AA/%D8%A8%D8%B1%D8%B1%D8%B3%DB%8C-%D9%88-

%D9%85%D9%82%D8%A7%DB%8C%D8%B3%D9%87-%D9%85%D8%B2%D8%A7%DB%8C%D8%A7-%D9%88-%D9%85%D8%B9%D8%A7%DB%8C%D8%A8-%D9%81%D8%A7%DB%8C%D8%B1%D9%88%D8%A7%D9%84-%D9%87%D8%A7/

۱۴. https://firewall.tosinso.com/fa/tips/32719/static-packet-filtering-%DA%86%DB%8C%D8%B3%D8%AA-%D9%88-%DA%86%D9%87-%D9%85%D8%B2%D8%A7%DB%8C%D8%A7-%D9%88-%D9%85%D8%B9%D8%A7%DB%8C%D8%A8%DB%8C-%D8%AF%D8%A7%D8%B1%D8%AF%D8%9F

۱۵. https://falnic.com/blog/what-is-firewall.html

۱۶. https://fa.wikipedia.org/wiki/%D8%B1%D9%85%D8%B2%D9%86%DA%AF%D8%A7%D8%B1%DB%8C

۱۷. https://fa.wikipedia.org/wiki/%D8%A2%DB%8C%E2%80%8C%D9%BE%DB%8C%E2%80%8C%D8%B3%DA%A9

۱۸. https://digiato.com/article/2019/01/18/%D8%AA%D9%81%D8%A7%D9%88%D8%AA-%D8%A2%DB%8C-%D9%BE%DB%8C-%D8%B9%D9%85%D9%88%D9%85%DB%8C-%D9%88-%D8%AE%D8%B5%D9%88%D8%B5%DB%8C/

۱۹. https://www.datisnetwork.com/vpn-types.html

۲۰. http://avrmicro.blog.ir/post/%D8%A7%D9%86%D9%88%D8%A7%D8%B9-VPN-%D9%88-%DA%86%DA%AF%D9%88%D9%86%DA%AF%DB%8C-%DA%A9%D8%A7%D8%B1%DA%A9%D8%B1%D8%AF-%D8%A2%D9%86%D9%87%D8%A7

۲۱. https://www.datisnetwork.com/vpn-protocols-types.html

۲۲. https://koneshtech.academy/which-vpn-protocol-is-the-best/

۲۳. https://wiki.serversetup.co/tag/%D9%BE%D8%B1%D9%88%D8%AA%DA%A9%D9%84-pptp-%DA%86%DB%8C%D8%B3%D8%AA/

۲۴. https://www.datisnetwork.com/l2tp-protocol.html

۲۵. https://virgool.io/@fitnet/openvpn-%DA%86%DB%8C%D8%B3%D8%AA-%D9%88-%DA%86%D8%B1%D8%A7-%D8%A8%D9%87-%D8%B9%D9%86%D9%88%D8%A7%D9%86-%D8%A8%D9%87%D8%AA%D8%B1%DB%8C%D9%86-vpn-%D8%A7%D8%B2-%D8%A2%D9%86-%DB%8C%D8%A7%D8%AF-%D9%85%DB%8C-%D8%B4%D9%88%D8%AF-wfpyq2hjdjsg

۲۶. https://network.tosinso.com/fa/tips/34328/%D9%85%D8%B9%D8%B1%D9%81%DB%8C-%D8%A7%D9%86%D9%88%D8%A7%D8%B9-%D9%BE%D8%B1%D9%88%D8%AA%DA%A9%D9%84-%D9%87%D8%A7%DB%8C-vpn-%D9%82%D8%B3%D9%85%D8%AA-4-openvpn-%DA%86%DB%8C%D8%B3%D8%AA%D8%9F

۲۷. https://www.datisnetwork.com/ikev2-protocol.html

۲۸. https://virgool.io/@fitnet/ikev2-%DA%86%DB%8C%D8%B3%D8%AA-k8cusxxzpiuc

۲۹. https://www.datisnetwork.com/sstp-protocol.html

۳۰. https://fa.wikipedia.org/wiki/%D8%A7%D8%B3%E2%80%8C%D8%A7%D8%B3%E2%80%8C%D8%AA%DB%8C%E2%80%8C%D9%BE%DB%8C

۳۱. https://nextadmin.net/tag/%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-sstp/

۳۲. https://nextadmin.net/vpn-virtual-private-network/

۳۳. https://www.datisnetwork.com/sstp-protocol.html

۳۴. http://ysorkh.net/home/articles/tunneling/

۳۵. http://sisco.blogfa.com/post/5/%D9%86%D8%B5%D8%A8-%D9%88-%D8%B1%D8%A7%D9%87-%D8%A7%D9%86%D8%AF%D8%A7%D8%B2%DB%8C-vpn-server%D8%A7%D8%B2-%D8%A7%D8%A8%D8%AA%D8%AF%D8%A7-%D8%AA%D8%A7-%D8%A7%D8%AE%D8%B1-%D9%86%D8%B8%D8%B1-%D9%8A%D8%A7%D8%AF%D8%AA%D9%88%D9%86-%D9%86%D8%B1%D9%87

۳۶. https://ciscohome.ir/%D8%A2%D9%85%D9%88%D8%B2%D8%B4-%D9%86%D8%B5%D8%A8-%D8%B1%D8%A7%D9%87-%D8%A7%D9%86%D8%AF%D8%A7%D8%B2%DB%8C-vpn-%D9%88%DB%8C%D9%86%D8%AF%D9%88%D8%B2-%D8%B3%D8%B1%D9%88%D8%B1-%DB%B2/

۳۷. https://teeteel.ir/%D8%B1%D9%88%D8%B4-%D8%B1%D8%A7%D9%87-%D8%A7%D9%86%D8%AF%D8%A7%D8%B2%DB%8C-vpn-server.html

۳۸. https://fa.wikipedia.org/wiki/%D9%81%DB%8C%D9%84%D8%AA%D8%B1%D8%B4%DA%A9%D9%86

۳۹. http://pictocademy.ir/word/%D9%81%D8%A7%D8%B1%D8%B3%DB%8C-%D9%88-%D9%84%D8%A7%D8%AA%DB%8C%D9%86-%DA%A9%D8%B1%D8%AF%D9%86-%D8%A7%D8%B9%D8%AF%D8%A7%D8%AF-%D9%88%D8%B1%D8%AF/

۴۰. https://www.irna.ir/news/83549937/%D8%B4%DA%A9%D9%84-%DA%AF%DB%8C%D8%B1%DB%8C-%D8%A7%D9%BE%D8%B1%D8%A7%D8%AA%D9%88%D8%B1%D9%87%D8%A7%DB%8C-%D8%B1%D8%B3%D9%85%DB%8C-%D9%88%DB%8C-%D9%BE%DB%8C-%D8%A7%D9%86-%D8%AF%D8%B1-%DA%A9%D8%B4%D9%88%D8%B1

۴۱. https://easy.parastar.info/index.php/win10-help-system/458-create-a-vpn-server-on-your-windows-computer

۴۲. https://it.iut.ac.ir/net-tel

۴۳. https://www.easy.parastar.info/index.php/win10-help-system/458-create-a-vpn-server-on-your-windows-computer