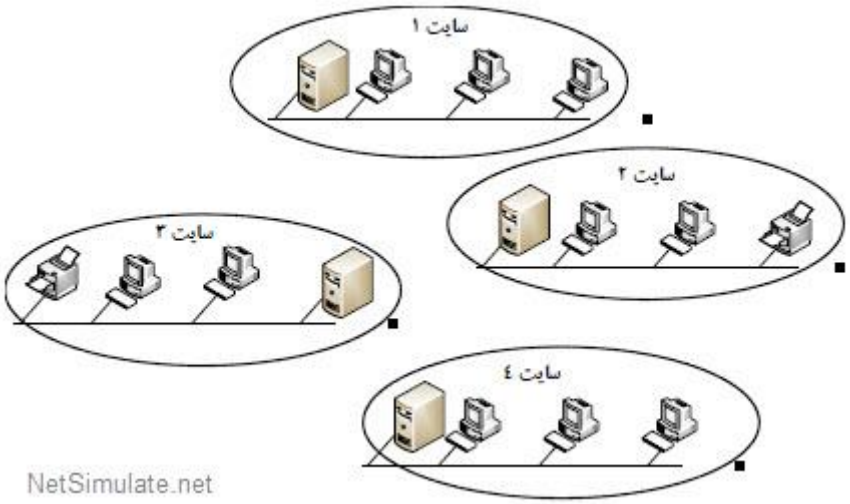
شبکه های خصوصی مجازی VPN

در این بخش از مقاله سعی کردیم مطالبی کوتاه در مورد شبکه های خصوصی مجازی VPN ارائه دهیم و شما را با مفاهیم اولیه و شیوه کارکرد این نوع شبکه آشنا سازیم، پس با ما همراه باشید تا در زیر مفصل به این موضوع بپردازیم.

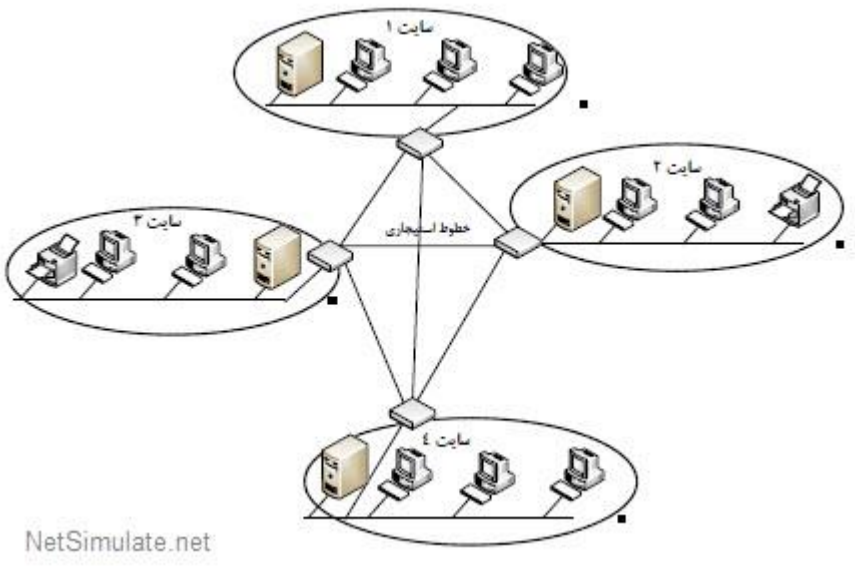
مقدمه مقاله :

در چند ساله اخیر، شرکت های چند ملیتی به مزایای استفاده اشتراکی از داده ها از طریق شبکه های کامپیوتری گسترده پی برده اند. امروزه با استفاده از فن آوری VPN ها امکان استفاده از مزایای استفاده اشتراکی داده ها برای کلیه شرکت ها، حتی شرکت های کوچک فراهم شده است. درحالت عادی، چنانچه شرکتی دارای سایت های کامپیوتری متعدد در نقاط مختلفی از دنیا باشد، امکان استفاده اشتراکی از داده ها بین شعبات مختلف شرکت وجود ندارد. به عنوان مثال در شکل زیر چهار سایت کامپیوتری مختلف یک شرکت که در نقاط گوناگون قرار دارند، نشان داده شده است.



سایت های کامپیوتری مجزا از یکدیگر

به خاطر عدم وجود اتصال های لازم بین سایت های کامپیوتری فوق، امکان استفاده اشتراکی از داده ها برای سایت های کامپیوتری وجود ندارد. با استفاده از خطوط استیجاری، مبادله مستقیم داده ها بین کامپیوتر های مختلف سایت های کامپیوتری فراهم می آید. این مسئله در شکل زیر نشان داده شده.

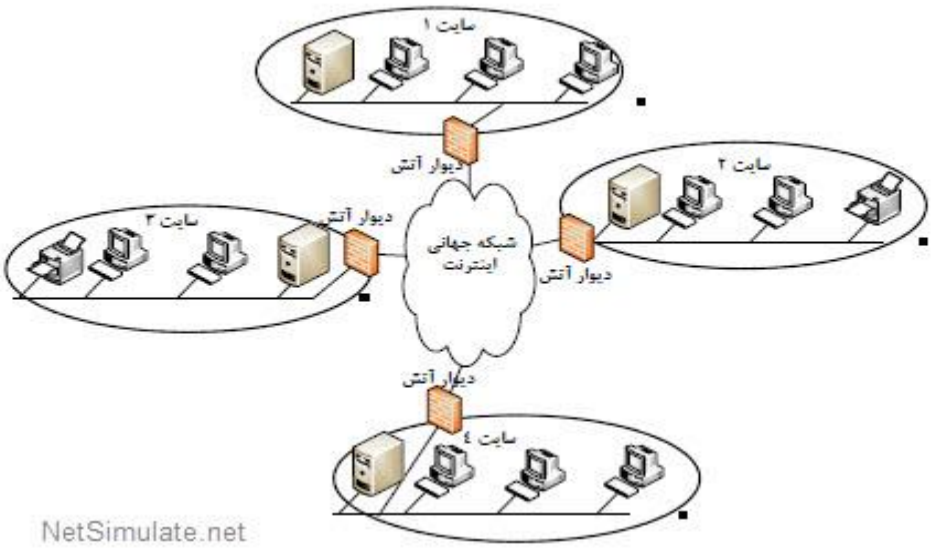


اتصال سایت های کامپیوتری مجزا از یکدیگر به وسیله خطوط استیجاری

حتی بعد از گسترش اینترنت و امکان استفاده از آن به خاطر قیمت پایین تر نسبت به خطوط استیجاری، به خاطر مشکلات امنیتی موجود دراتصال های اینترنتی، شرکت ها همچنان مایل به استفاده از خطوط گران قیمت استیجاری برای مبادلات داده های خود بودند. اخیراً با استفاده از فن آوری VPN امکان مبادلات تجاری امن بین کامپیوتر های شبکه با استفاده از بستر اینترنت فراهم شده است.

VPN ها قادر به برقراری اتصالات خصوصی تونل بین سایت های کامپیوتری مختلف شرکت ها در بستر اینترنت می باشند. تونل های فوق درست مشابه خطوط استیجاری می باشند با این تفاوت که هزینه تونل های خصوصی VPN به مراتب کمتر از خطوط استیجاری است. طبق آمار موجود VPN ها باعث صرفه جویی ۳۰ تا ۷۰ درصدی هزینه نسبت به خطوط استیجاری می شوند. برخلاف خطوط استیجاری گران قیمت، با استفاده از رمزنگاری های قوی داده های کامپیوتر ها به طور امن از طریق VPN ها مبادله می شود، طوری که نه تنها نفوذگران این ترنت بلکه خود ISP ها نیز قادر به استراق سمع داده ها نخواهند بود. امروزه سازمان های مختلف با استفاده از دیواره های آتشین از دسترسی غیرمجاز افراد خارج از شبکه به منابع کامپیوتری سازمان خود جلوگیری می کنند. البته دیواره های آتشین قادر به تشخیص و جدا سازی افر اد خارجی مجاز و همچنین کارمندان و همکاران تجاری شرکت ها از افراد خارجی غیرمجاز نمی باشند.

مطابق با شکل بالا دیواره های آتشین مدرن، بدون آن که امنیت داده های سایت های کامپیوتری به خطر بیافتد قادر به برقراری ارتباط های VPN بین سایت های مختلف می باشند. فن آوری های مدرن VPN با استفاده از روش های رمز نگاری جدید قادر به اتصال سایت های کوچک و بزرگ به یکدیگر از طریق اینترنت می باشد طوری که کاربران راه دور به همان کیفیت کاربران محلی قادر به استفاده از منابع شبکه می باشند. به عنوان مثال کاربران راه دور مشابه کاربران محلی قادر به استفاده از داده های موجود در سرویس دهنده های وب هستند.



اتصال سایت های کامپیوتری مجزا از یکدیگر به وسیله VPN

با استفاده از رمزنگاری، امکان مخفی سازی اطلاعات محرمانه نظیر رمز عبور و داده های داخل پست های الکترونیکی وجود دارد رمز نگاری VPN شامل دو قسمت است که عبارتند از :

۱. الگوریتم رمزنگاری
۲. کلید رمزنگاری

معمولاً الگوریتم رمزنگاری دانش عمومی بوده و همه از روش آن آشنا هستند، ولی کلید رمزنگاری همواره مخفی می باشد. الگوریتم های رمزنگاری نوین مثل DES از کلید رمز ۱۱۲ بیتی یا بیشتر استفاده می کنند. امنیت داده های رمز شده به امنیت کلید رمز بستگی دارد. هنگامی که دو سایت در مورد پیاده سازی VPN به توافق رسیدند، کلیدهای رمز خود ارتباط های مطمئن امکان تبادل داده های تجاری و محرمانه وجود دارد VPN های مدرن امروزه نیازی به فن آوری های محرمانه ندارند، بلکه با استفاده از سخت افزار ها و نرم افزار هایی که به راحتی قابل نصب می باشند، امکان استفاده از VPN وجود دارد همچنین نصب VPN نیازی به تغییر در پیکره بندی سرویس دهنده های شبکه ندارد. سربار اضافی عملیات رمز نگاری VPN در شبکه به دیواره های آتش و مسیریاب های شبکه منتقل می شود و به سرویس دهنده شبکه بار اضافی تحمیل نمی شود.

پروتکل امنیتی اینترنت IPSEC

امروزه در اکثر محصولات VPN ، از پروتکل امنیتی IPSEC برای افزایش اطمینان شبکه استفاده می شود. IPSEC از فناوری امنیتی جامعی استفاده می کند IPSEC برای برنامه های کاربردی موجود امکانات محافظتی شفافی فراهم

می آورد، طوری که بدون نیاز به اعمال تغییرات نرم افزاری در برنامه های کار بردی موجود، امکان محافظت پیام های آنها وجود در شکل زیر جایگاه پروتکل IPSEC در معماری TCP/ IP نشان داده شده است.

جایگاه پروتکل IPSEC

IPSEC برای تمام پیام های ارسالی، سه قابلیت حفاظتی زیر را فراهم می سازد :

۱. رمزنگاری
۲. تصدیق هویت
۳. حفظ تمامیت و درستی داده ها

همان طور که قبلاً اشاره شد، رمزنگاری باعث پنهان ساختن محتویات پیام می گردد. تصدیق هویت باعث می شود که هویت فرستنده پیام مورد تایید و تصدیق گیرنده قرار گیرد. حفظ تمامیت و درستی داده ها، مانع دست کاری کردن تمام یا بخشی از پیام توسط افراد غیرمجاز می شود. این سه قابلیت حفاظتی IPSEC مانع از دزدی و سرقت داده ها می شود.

بر اساس میزان گستردگی شبکه، نحوه استفاده از محصولات IPSEC متفاوت می باشد. سایت های بزرگ از پروتکل IPSEC که در داخل دیواره آتشین قرار دارد، برای محافظت اتصال های اینترنتی خود استفاده می کنند. سایت های کوچکتر می توانند از پروتکل IPSEC که داخل مسیریاب شبکه مخفی شده است، استفاده نمایند. کاربران انفرادی در ادارات کوچک و یا منازل می توانند از نسخه های رومیزی ، پروتکل IPSEC برروی کامپیوتر های خود استفاده کنند. تنها در صورتی که ترافیک ورودی به شبکه از یک کاربر و یا سایت مورد تأیید تولید شده باشد، IPSEC اجازه ورود آن را به شبکه سازمان می دهد.

سیر تکاملی IPSEC

امروزه IPSEC، به یکی از مهمترین پروتکل های امنیتی رایج مورد استفاده در صنعت تبدیل شده است در سال ۱۹۸۰ آژانس امنیتی ملی آمریکا، به منظور توسعه و ایجاد پروتکل های همه منظوره امنیتی شبکه، شروع به اجرای پروژه ای به نام SDNS نمود. در اوایل سال ۱۹۹۰ چندین شریک اولیه SDNS با همکاری یکدیگر اقدام به توسعه و طراحی پروتکل امنیتی جدیدی برای IPV6 نمودند، به خاطر رواج بیشتر IPV4 نسبت به IPV6 پروتکل امنیتی طراحی شده برای استفاده در IPV4 وفق داده شد. در سال ۱۹۹۰پروتکل IPSEC ارائه گردید. بعد از آن تحقیقات ومطالعات زیادی برای تجدید نظر و توسعه و تکامل بیشتر پروتکل IPSEC انجام شد پروتکل IKE برای مدیریت اتوماتیک کلیدهای رمز نگاری در IPSEC مورد تائید قرار گرفت. تمام باز نگری های اعمال شده بر روی پروتکل IPSEC از طریق کمیته های استاندارد گزاری کنترل و

نظارت می شود. IPSEC قادر به استفاده در دیواره های آتشین و مسیریاب های متعدد می باشد. برای بررسی سازگاری محصولات، اکثر تولیدکنندگان دیواره آتشین و مسیریاب های شبکه اقدام به برگزاری آزمایش های تست سازگاری محصولات خود می نمایند. امروزه از IPSEC درسیستم عامل های ویندوز ۲۰۰۰ استفاده می شود.

پیاده سازی IPSEC VPN

شکل های مختلف پیاده سازی IPSEC VPN به صورت زیر می باشد :

۱. سایت به سایت
۲. سرویس گیرنده /سرویس دهنده
۳. ترکیب هر دو روش

VPN های سایت به سایت از دو یا چند سایت جدا از هم که با استفاده از VPN به یکدیگر متصل شده و از داده های یکدیگر به صورت اشتراکی استفاده می کنند، تشکیل شده است. VPN های مبتنی بر برمدل سرویس گیرنده / سرویس دهنده از

تعدادی کاربر راه دور که از طریق اینترنت به سایت مرکزی (سرویس دهنده) متصل هستند، تشکیل می شوند.

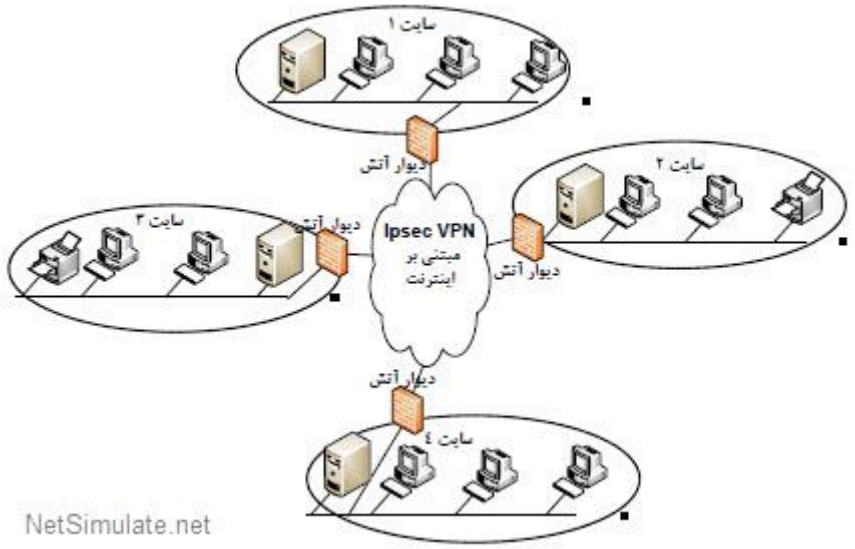
مطابق با شکل زیر در VPN های سایت به سایت هرسایت از طریق یک دیواره آتشین به اینترنت اتصال یافته

از دیواره آتشین به همراه Ipsec برای محافظت داده های مبادله شده بین سایت ها استفاده می شود.

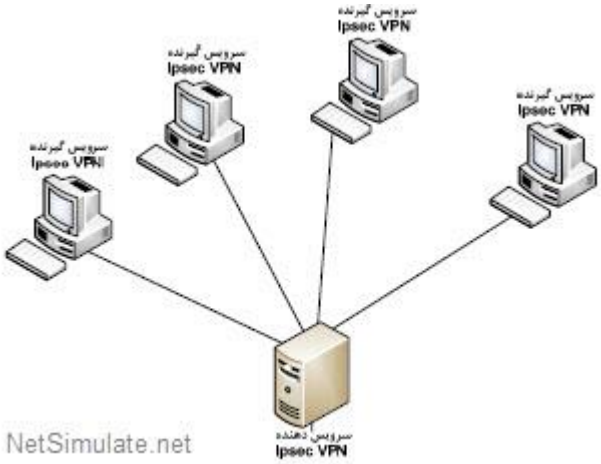
برای برقراری VPN های سایت به سایت، هر سایت نیاز به اتصال اینترنت به همراه دیواره های آتشین با قابلیت IPSEC VPN دارد . برای برقراری اتصال های رمز شده مطمئن بین سایت ها، براساس پروتکل IKE سایت ها باید اعتبارنامه های رمزنگاری خود را بین یکدیگر مبادله نمایند.

در شکل زیر ساختار VPN های مبتنی بر مدل سرویس گیرنده /سرویس دهنده نشان داده شده است . در این ساختار یک سایت VPN با استفاده از پروتکل IPSEC اقدام به برقراری ارتباط های مطمئن با یک یا چند سرویس گیرنده

انفرادی می کند. هر دو طرف سرویس دهنده و سرویس گیرنده باید مجهز به نرم افزار انفرادی می کند IPSEC باشند.



اتصال سایت های کامپیوتری مجزا از یکدیگر به وسیله IPSEC VPN مبتنی بر اینترنت



VPN از نوع سرویس گیرنده / سرویس دهنده