شبکه خصوصی مجازی(VPN) شبکه ای است که در آن از طریق یک شبکه عمومی مانند اینترنت اطلاعات جابه جا می شود و در عین حال با استفاده از سخت افزار و نرم افزار می توان همچنان این ارتباط را اختصاصی و ایمن نگه داشت.

این راهکار بطور عمده جهت ارتباط ایمن بین شعبه های مختلف شرکت ها یا ارتباط از راه دور کاربرد دارد و این در حالی است که در ایران اصلی ترین استفاده از VPN به عنوان فیلترشکن بوده که با استفاده از آن می توان به سرویس دهندگان اینترنت در خارج از ایران متصل شده و از آنها سرویس اینترنت بدون فیلترینگ ایران دریافت نمود.

در گذشته برای انتقال اطلاعات شرکت ها ازLeased Line ، Modem جهت ارتباط RAS، E-Mail ،FTP و . . . استفاده می شد ،که VPN می تواند جایگزین مناسب و ایمنی جهت برقراری این ارتباط به صورت امن و با قابلیت های فراتر نسبت به روش های قبلی ایفاء نقش نماید.

VPN باعث می شود امنیت ،اعتماد پذیری، مدیریت و سیاست گذاری شبکه به صورت متمرکز بوده و دارای مزایایی نظیر بهبود وضعیت امنیت،گسترش به روز ،ایجاد محدوده ی ارتباطی بزرگتر از لحاظ جغرافیایی ، کاهش هزینه ها نسبت به روش های قبلی ،کاهش زمان ارسال اطلاعات و . . . بوده و این در حالی است که تغییرات در توپولوژی و سیاست شبکه نسبت به روش های قبلی با هزینه پایین تر و معمولا به صورت نرم افزاری می باشد.

VPN برخلاف خود اینترنت کار نفوذ را برای خرابکاران خیلی سخت کرده زیرا جهت تامین امنیت داده ها و اطلاعات از روش هایی نظیر دیواره ی آتش ، رمز نگاری ، IPSec، AAA استفاده می کند.

با استفاده از دیواره ی آتش می توان در تعداد پورت های فعال یا پروتکل های خاص و . . . محدودیت ایجاد نمود.

در رمزنگاری همانطور که مشخص است اطلاعات در کامپیوتر مبداء رمز شده و در سایر کامپیوتر هابه صورت رمز قابل مشاهده است، در این صورت کامپیوتر های مجاز، قادر به رمز گشایی اطلاعات ارسالی می باشند.بدین ترتیب اطلاعات بدون رمزگشایی قابل استفاده نمی باشد.

الگوریتم های رمز نگاری در کامپیوتر ها دارای دو نوع کلید متقارن و کلید عمومی می باشد.

پروتکل IPSec(IP Security) قابلیت های بیشتری نسبت به الگوریتم های رمزنگاری دارد که خود دارای دو روش Tunnel: که در آن Header و Payload رمز شده و دیگری Transport: که صرفا Payload رمز می گردد.

IPSec بر خلاف دیگر پروتکل های امنیتی نظیر SSH, TCL, SSL که در لایه ٤ به بالا(مدل OSI) و پروتکل های PPTP و L2TP(بصورت کامل IPSec را حمایت می کند) که در لایه ۲ هستند، این پروتکل در لایه ی ۳ کار می کند و می تواند از پروتکل های TCP,UDP حفاظت کند و مزیت آن نسبت به پروتکل های لایه بالاتر این است که نیاز به طراحی برنامه بر طبق این پروتکل نمی باشد.

پروتکل IPSec قابلیت رمزنگاری بین روتر ، دیواره آتش ، کامپیوتر و سرویس دهنده ها را دارد.

AAA (Authentication, Authorization, Accounting): یکی دیگر از راههای بالابردن امنیت در VPN است که می توان با استفاده از آن شخص را در استفاده از منابع شبکه محدود نمود که معمولا در جاهایی که VPNاز نوع دستیابی از راه دور است مورد استفاده قرار می گیرد.