عنوان مقاله : مقدمه ای بر پروتکل IP sec

گروه مطالعاتی : امنیت

گروه کاری : امنیت

ارائه دهنده: افسانه کربلائي زاده

تاریخ ارائه: ۸۳/۱۱/۱۳

سرپرست گروه کاری: طیبه میرزائی

تاریخ اصلاح: ۸۳/۱۱/۱۵

اصلاح کننده : افسانه کربلائي زاده

مرجع: اینترنت

IP Security یا IPSec رشته ای از پروتکلهاست که برای ایجاد VPN مورد استفاده قرار می گیرند. مطابق با تعریف IETF (Internet Engineering Task Force) پروتکل IPSec به این شکل تعریف می شود:
یک پروتکل امنیتی در لایه شبکه تولید خواهد شد تا خدمات امنیتی رمزنگاری را تامین کند. خدماتی که به صورت منعطفی به پشتیبانی ترکیبی از تایید هویت ، جامعیت ، کنترل دسترسی و محرمانگی بپردازد.
در اکثر سناریوها ،IPSec به شما امکان می دهد تا یک تونل رمزشده را بین دو شبکه خصوصی ایجاد کنید.همچنین امکان تایید هویت دو سر تونل را نیز برای شما فراهم می کند.اما IPSec تنها به ترافیک مبتنی بر IP اجازه بسته بندی و رمزنگاری می دهد و درصورتی که ترافیک غیر IP نیز در شبکه وجود داشته باشد ، باید از پروتکل دیگری مانند GRE در کنار IPSec استفاده کرد.
IPSec به استاندارد de facto در صنعت برای ساخت VPN تبدیل شده است.بسیاری از فروشندگان تجهیزات شبکه ، IPSec را پیاده سازی کرده اند و لذا امکان کار با انواع مختلف تجهیزات از شرکتهای مختلف ، IPSec را به یک انتخاب خوب برای ساخت VPN مبدل کرده است.

انواع IPSec VPN

شیوه های مختلفی برای دسته بندی IPSec VPN وجود دارد اما از نظر طراحی ، IPSec برای حل دو مسئله مورد استفاده قرار می گیرد

۱- اتصال یکپارچه دو شبکه خصوصی و ایجاد یک شبکه مجازی خصوصی
۲- توسعه یک شبکه خصوصی برای دسترسی کاربران از راه دور به آن شبکه به عنوان بخشی از شبکه امن

بر همین اساس ، IPSec VPN ها را نیز می توان به دو دسته اصلی تقسیم کرد:

۱- پیاده سازی LAN-to-LAN IPSec

این عبارت معمولا برای توصیف یک تونل IPSec بین دو شبکه محلی به کار می رود. در این حالت دو شبکه محلی با کمک تونل IPSec و از طریق یک شبکه عمومی با هم ارتباط برقرار می کنند به گونه ای که کاربران هر شبکه محلی به منابع شبکه محلی دیگر، به عنوان عضوی

از آن شبکه، دسترسی دارند. IPSec به شما امکان می دهد که تعریف کنید چه داده ای و چگونه باید رمزنگاری شود.

۲- پیاده سازی Remote-Access Client IPSec

این نوع از VPN ها زمانی ایجاد می شوند که یک کاربر از راه دور و با استفاده از IPSec client نصب شده بر روی رایانه اش، به یک روتر IPSec یا Access server متصل می شود. معمولا این رایانه های دسترسی از راه دور به یک شبکه عمومی یا اینترنت و با کمک روش dialup یا روشهای مشابه متصل می شوند. زمانی که این رایانه به اینترنت یا شبکه عمومی متصل می شود، IPSec client موجود بر روی آن می تواند یک تونل رمز شده را بر روی شبکه عمومی ایجاد کند که مقصد آن یک دستگاه پایانی IPSec ،مانند یک روتر، که بر لبه شبکه خصوصی مورد نظر که کاربر قصد ورود به آن را دارد، باشد.

در روش اول تعداد پایانه های IPSec محدود است اما با کمک روش دوم می توان تعداد پایانه ها را به ده ها هزار رساند که برای پیاده سازی های بزرگ مناسب است.

ساختار IPSec

IPSec برای ایجاد یک بستر امن یکپارچه ، سه پروتکل را با هم ترکیب می کند :

۱- پروتکل مبادله کلید اینترنتی (Internet Key Exchange یا IKE)

این پروتکل مسئول طی کردن مشخصه های تونل IPSec بین دو طرف است. وظایف این پروتکل عبارتند از:

- ☐ طی کردن پارامترهای پروتکل
- ☐ مبادله کلیدهای عمومی
- ☐ تایید هویت هر دو طرف
- ☐ مدیریت کلیدها پس از مبادله

IKE مشکل پیاده سازی های دستی و غیر قابل تغییر IPSec را با خودکار کردن کل پردازه مبادله کلید حل می کند. این امر یکی از نیازهای حیاتی IPSec است. IKE خود از سه پروتکل تشکیل می شود :

- ☐ SKEME : مکانیزمی را برای استفاده از رمزنگاری کلید عمومی در جهت تایید هویت تامین می کند.

- Oakley : مکانیزم مبتنی بر حالتی را برای رسیدن به یک کلید رمزنگاری، بین دو پایانه IPSec تامین می کند.
- ISAKMP : معماری تبادل پیغام را شامل قالب بسته ها و حالت گذار تعریف می کند.

IKE به عنوان استاندارد RFC 2409 تعریف شده است. با وجودی که IKE کارایی و عملکرد خوبی را برای IPSec تامین می کند، اما بعضی کمبودها در ساختار آن باعث شده است تا پیاده سازی آن مشکل باشد، لذا سعی شده است تا تغییراتی در آن اعمال شود و استاندارد جدیدی ارائه شود که IKE v2 نام خواهد داشت.

۲- پروتکل Encapsulating Security Payload یا ESP

این پروتکل امکان رمزنگاری ، تایید هویت و تامین امنیت داده را فراهم می کند.

۳- پروتکل سرآیند تایید هویت (Authentication Header یا AH)

این پروتکل برای تایید هویت و تامین امنیت داده به کار می رود.