تدوین راهکارهای امنیتی شبکه های خصوصی مجازی

نویسنده: امیرعباس برادران –a.baradaran24@yahoo.com

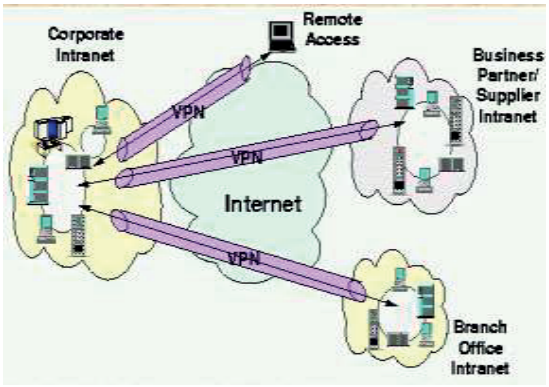
چکیده: *VPN*، شبکه‌ای اختصاصی بوده که از یک شبکه عمومی برای ارتباط با سایت‌های راه دور و ارتباط کاربران با یکدیگر استفاده می‌نماید. این نوع شبکه‌ها به جای استفاده از خطوط واقعی مثل خطوط اجاره‌ای، از یک ارتباط مجازی به کمک اینترنت برای شبکه اختصاصی به منظور ارتباط با سایت‌ها استفاده می‌کنند. استفاده از این نوع شبکه در سازمان‌های مختلف می‌تواند روش‌های متفاوتی داشته باشد. به طور کلی سازمان‌های مجری باید به طور کامل با ساختار این نوع شبکه آشنایی کامل داشته باشند. استفاده وسیع این نوع شبکه، به خصوص در محیط‌هایی که انتقال داده حساس است، روزبه‌روز در حال افزایش است. درنتیجه طرحی جامع از ساختار کلی این شبکه، ضروری به نظر می‌رسد. در این تحقیق برآنیم تا به طور کامل ساختار این نوع شبکه را مورد واکاوی قرار داده تا رویکردهای جدیدی برای حل مشکلات این نوع شبکه ارائه دهیم. هدف اصلی این تحقیق، ارائه ساختاری جامع از شبکه *VPN* و تبیین یک راهکار امنیتی می‌باشد که به کمک این ساختار سازمان‌های درخواست‌کننده بتوانند شبکه مورد نظر و ایمن خود را راه‌اندازی کنند.

کلیدواژه: شبکه‌های خصوصی مجازی، امنیت، معماری *VPN*، نفوذ

۱- مقدمه

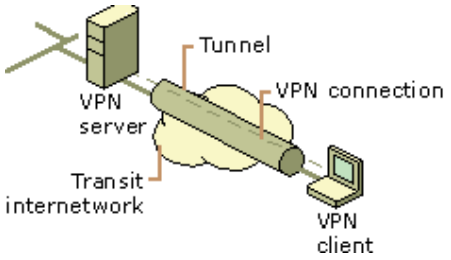
در طی سال‌های گذشته دنیا دستخوش تحولات فراوانی در عرصه ارتباطات بوده است. اغلب سازمان‌ها و موسسات ارائه دهنده کالا و خدمات که در گذشته بسیار محدود و منطقه‌ای مسائل را دنبال و در صدد ارائه راهکارهای مربوطه بودند، امروزه بیش از گذشته نیازمند تفکر در محدوده جهانی برای ارائه خدمات و کالای تولیده شده هستند. اکنون با سازمانهای بسیاری برخورد می‌نمائیم که در سطح یک کشور یا دنیا دارای دفاتر فعال و متفاوتی می‌باشند. همه این سازمانها قبل از هر چیز به دنبال یک اصل بسیار مهم و آن پیداکردن یک روش سریع، ایمن و قابل اعتماد به منظور برقراری ارتباط با دفاتر و نمایندگی‌های خود می‌باشند. اکثر سازمان‌ها و مؤسسات به منظور ایجاد یک شبکه WAN از خطوط اختصاصی یا استیجاری استفاده می‌نمایند. این خطوط دارای انواع متفاوتی می‌باشند. بعنوان مثال، ISDN با سرعت ۱۲۸ کیلو بیت در ثانیه یا OC3 با سرعت ۱۵۵ مگابیت در ثانیه، دامنه وسیع خطوط اختصاصی را پشتیبانی می‌کنند. یک شبکه WAN دارای مزایای عمده‌ای نسبت به یک شبکه عمومی نظیر اینترنت از بعد امنیت وکارآئی است. پشتیبانی و نگهداری یک شبکه WAN در عمل و زمانی که از خطوط اختصاصی استفاده می‌گردد ، مستلزم صرف هزینه بالائی است[1,2,3]. همزمان با عمومیت یافتن اینترنت، اغلب سازمانها و مؤسسات، ضرورت توسعه شبکه اختصاصی خود را به درستی احساس کرده‌اند. در ابتدا «شبکه‌های اینترانت» مطرح شدند. این نوع شبکه بصورت کاملا اختصاصی بوده و کارمندان یک سازمان با استفاده از رمز عبور تعریف شده، قادر به ورود به شبکه و استفاده از منابع موجود بودند. اخیراً، تعداد زیادی از مؤسسات و سازمان‌ها با توجه به مطرح شدن خواسته‌های جدید (کارمندان از راه دور، ادارات از راه دور) اقدام به ایجاد شبکه‌های اختصاصی مجازی یا VPN نموده‌اند. دو نوع عمده شبکه‌های VPN بنام دستیابی از راه دور و سایت به سایت وجود دارد[1,4,5]. در VPN دسترسی از راه دور شبکه از مدل ارتباط کاربر به یک شبکه محلی استفاده می‌شود. سازمان‌هایی که از این مدل استفاده می‌کنند، به دنبال ایجاد تسهیلات لازم برای ارتباط پرسنل (عموماً کاربران از راه دور که در هر مکانی می‌توانند حضور داشته باشند) به شبکه سازمان می‌باشند. سازمان‌هایی که

تمایل به برپاسازی یک شبکه بزرگ دستیابی از راه دور دارند، می‌بایست از امکانات یک مرکز ارائه‌دهنده خدمات اینترنت جهانی ISP استفاده نمایند. سرویس دهنده ISP، برای نصب و پیکربندی VPN، یک NAS را پیکربندی کرده و نرم‌افزاری را در اختیار کاربران از راه دور برای ارتباط با سایت قرار خواهد داد. کاربران در ادامه با برقراری ارتباط قادر به دستیابی به NAS و استفاده از نرم افزار مربوطه به منظور دستیابی به شبکه سازمان خود خواهند بود[6,8,10]. در VPN سایت به سایت، یک سازمان با توجه به سیاست‌های موجود، قادر به اتصال چندین سایت ثابت از طریق یک شبکه عمومی نظیر اینترنت می‌باشد. شبکه‌های VPN که از این روش استفاده می‌کنند ، دارای انواع خاصی در این زمینه می‌باشند که عبارتند از: مبتنی بر اینترانت، مبتنی بر اکسترانت. چنانچه سازمانی دارای یک و یا بیش از یک محل (راه دور) بوده و تمایل به الحاق آنها در یک شبکه اختصاصی داشته باشد، می‌تواند یک اینترانت VPN را به منظور برقراری ارتباط هر یک از شبکه‌های محلی با یکدیگر ایجاد کند. در مواردی که سازمانی در تعامل اطلاعاتی بسیار نزدیک با سازمان دیگر باشد، می‌تواند یک اکسترانت VPN را به منظور ارتباط شبکه‌های محلی هر یک از سازمان‌ها ایجاد کند. شکل ۱ معماری کلی VPN مبتنی بر اینترانت را نشان می‌دهد[7,11,12,13].



شکل۱: شبکه VPN مبتنی بر اینترانت

VPN دارای سرور، سرویس‌گیرنده و تونل می‌باشد. سرور VPN درخواست مشتریان VPN و سرویس‌گیرنده‌ی VPN خدمات سرور VPN که می‌تواند یک مسیریاب یا PC نیز باشد را دریافت می‌کنند. تونل VPN نیز قسمتی از اتصال است که داده‌ها در آن بسته بندی می‌شوند. به عبارت دیگر، تونل، داده‌ها را به صورت مجازی کوتاه می‌کند. شکل ۲ اجزای VPN بهمراه ارتباط آنها با یکدیگر را نشان می‌دهد.



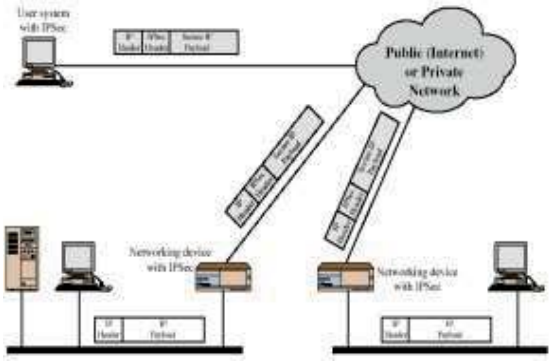
شکل۲: اجزاء VPN

۲- سیاست‌های امنیتی VPN

شبکه‌های VPN به منظور تأمین امنیت داده‌ها و ارتباطات از روشهای متعددی استفاده می‌کنند. یکی از این روش‌ها استفاده از «دیواره آتش» است. دیواره آتش یک دیواره مجازی بین شبکه اختصاصی یک سازمان و اینترنت ایجاد می‌کند. با استفاده از دیواره آتش می‌توان عملیات متفاوتی را جهت اعمال سیاست‌های امنیتی یک سازمان انجام داد. ایجاد محدودیت در تعداد پورت‌های فعال، پروتکل‌های خاص و نوع بسته‌های اطلاعاتی، نمونه‌هایی از عملیاتی است که می توان با استفاده از یک دیواره آتش انجام داد. یکی دیگر از این سیاست‌ها استفاده از رمزنگاری است. رمزنگاری فرآیندی است که با استفاده از آن کامپیوتر مبدأ، اطلاعاتی رمزشده را برای کامپیوتر دیگر ارسال می‌کند[14,15,16]. سایر کامپیوترهای مجاز، قادر به رمزگشایی اطلاعات ارسالی خواهند بود. بدین ترتیب پس از ارسال اطلاعات توسط فرستنده، دریافت‌کنندگان، قبل از استفاده از اطلاعات می‌بایست اقدام به رمزگشائی اطلاعات ارسال شده نمایند. سیستم‌های رمزنگاری به دو گروه رمزنگاری کلید متقارن و رمزنگاری کلید عمومی تقسیم می‌شوند. روش دیگر امنیتی، استفاده از پروتکلهای امنیتی می‌باشد [17,18,19,20,21,22]. این پروتکل‌ها شامل پروتکل‌های IPSec، SSL VPN، PPTP، PPP و L2TP می‌باشند.

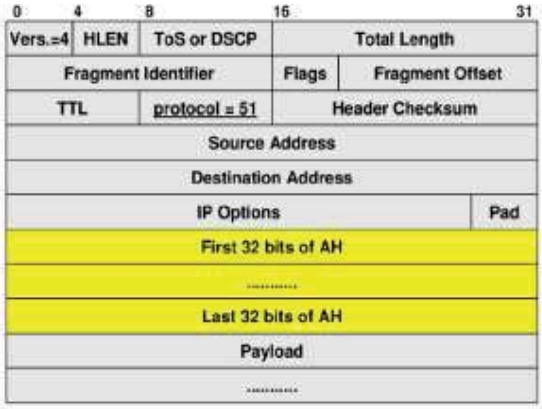
۲-۱- پروتکل IPSec

IPSec یک پروتکل تونل‌زنی لایه سوم است که از روش ESP برای بسته بندی کردن و رمزنگاری اطلاعات IP برای تبادل امن اطلاعات از طریق یک شبکه کاری IP عمومی یا خصوصی استفاده می‌کند. IPSec با استفاده از روش ESP می‌تواند اطلاعات IP را به صورت کامل بسته بندی و رمزنگاری کند. به محض دریافت اطلاعات رمزگذاری شده، تونل سرور، سرایند اضافه‌شده به IP را پردازش کرده و سپس کنار می‌گذارد و بعد از آن رمزهای ESP و بسته را باز می‌کند. بعد از این مراحل است که بسته IP به صورت عادی پردازش می‌شود. پردازش عادی ممکن است شامل مسیریابی و ارسال بسته به مقصد نهایی آن باشد. به طور کلی IPSec یک پروتکل تنها نیست بلکه مجموعه‌ای از الگوریتم‌های امنیتی می‌باشد که چارچوبی کلی فراهم می‌کند تا به کمک آن بتواند ارتباط امنی را برقرار کند. سرویس‌های امنیتی فراهم شده توسط IPSec، هویت‌شناسی به همراه کنترل جامعیت داده‌ها، محرمانگی بسته‌ها و مدیریت کلید(تبادل امن کلید) می‌باشند[22,23,15,16]. از کاربردهای این پروتکل می‌توان به مواردی از قبیل ایجاد VPN برای قسمت‌های مختلف یک سازمان از طریق اینترنت، دسترسی امن کارمندان شرکت به منابع شبکه از طریق اینترنت، امکان ارتباط امن بین چند سازمان و به وجود آوردن خدمات امنیتی برای کاربردهای دیگر(مثل تجارت الکترونیک) اشاره کرد. شکل ۳ نحوه استفاده از این پروتکل را نشان می‌دهد[24,25].

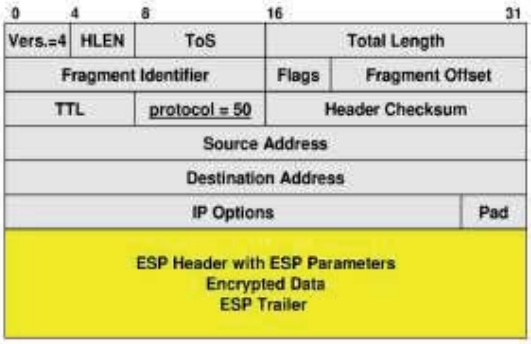


شکل ۳: نحوه استفاده از پروتکل IPSec

از مزایای مهم این پروتکل می‌توان به تأمین امنیت قوی بین داخل و خارج LAN در صورت به‌کارگیری در مسیریاب‌ها و دیواره آتش‌ها، عدم سربار رمزنگاری در نقاط انتهایی، شفافیت از دید کاربران و برنامه‌های کاربردی لایه‌های بالاتر و ایجاد ارتباط امن بین کارکنان سازمان از خارج به داخل اشاره کرد. این پروتکل دارای توصیف نسبتاً مشکلی است و در IPV6 الزامی و در IPV4 اختیاری است. این پروتکل در سرآیندهای توسعه یافته و بعد از سرآیند اصلی IP پیاده‌سازی می‌شود و مستندات آن بسیار حجیم بوده و به اجزای معماری، ESP، AH و مدیریت کلید دسته‌بندی می‌شود. شکل ۴ جایگاه AH در بسته IPV4 و شکل ۵ جایگاه ESP در IPV4 را نشان می‌دهد[26,27,28].



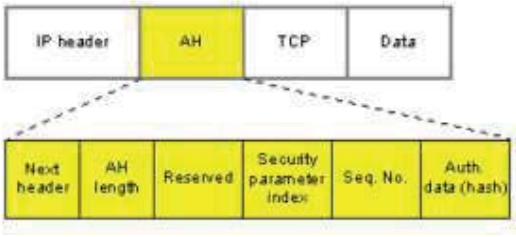
شکل ۴: جایگاه AH در IPV4



شکل ۵: جایگاه ESP در IPV4

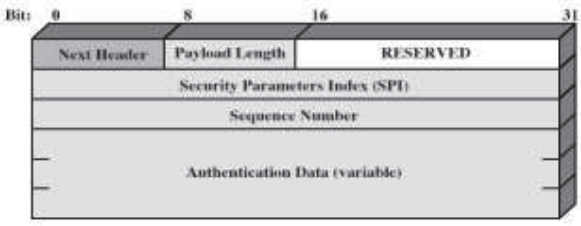
ESP برای رمزنگاری بسته‌هاست که احراز هویت در آن اختیاری است. همچنین AH تشخیص هویت بسته‌ها می‌باشد. به

طورکلی IPSec یک سیستم را قادر می‌سازد تا پروتکل‌های امن و مورد نیاز و مواردی از این قبیل را برای ارتباطات خود انتخاب کند که این کار را به وسیله دو پروتکل AH و ESP انجام می-دهد که AH سندیّت و صحت منبع و بسته‌های IP را فراهم می‌کند. شکل ۶ ساختار پروتکل IPSec را به همراه AH نشان می‌دهد[30,31,32].



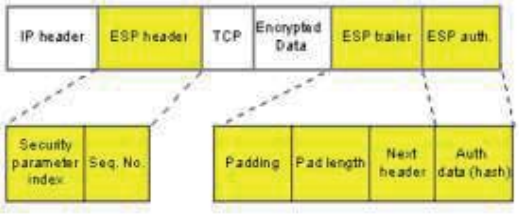
شکل۶: پروتکل IPSec به همراه AH

طول بسته AH، ۳۲ بیت می‌باشد. Next Header نوع سرآیند بعدی موجود در بسته و AH Length طول AH می‌باشد که هرکدام ۸ بیتی می‌باشند. SPI نیز پارامتر امنیت می‌باشد که ۳۲ بیتی است. Seq.No شمارنده ۳۲ بیتی و AD نیز دربرگیرنده MAC یا ICV می‌باشد. همچنین فیلد Reserved نیز برای استفاده‌های آتی است که ۱۶ بیتی است. شکل ۷ نوع دیگری از ساختار AH را نشان می‌دهد[7,32,34,35].



شکل ۷: ساختار AH

پروتکل ESP محرمانگی داده را فراهم می‌کند و توسط آن جامعیت و درستی منبع تایید می‌شود و در هر بار فقط قادر است یکی از این موارد را پشتیبانی کند. ESP از الگوریتم‌های رمزنگاری متقارن مانند 3DES استفاده می‌کند تا داده‌ها مخفی شوند. شکل ۸ ساختار این پروتکل را نشان می‌دهد[7,36,37,38].



شکل۸: پروتکل IPSec به همراه ESP

در AH و ESP دو حالت انتقال و تونل وجود دارد. در حالت انتقال تغییرات تنها روی محتوای بسته صورت می‌گیرد (بدون تغییر سرآیند IP) و در حالت تونل تغییرات روی کل بسته IP (سرآیند به همراه Payload) انجام می‌شود. IPSec می‌تواند خدماتی مانند کنترل دسترسی، تضمین صحت داده‌ها در ارتباطات بدون اتصال، احراز هویت منبع داده‌ها، تشخیص بسته-های دوباره ارسال شده و عدم پذیرش آنها، محرمانگی بسته‌ها و محرمانگی جریان ترافیک را فراهم کند. جدول ۱ مقایسه بین دو پروتکل AH و ESP و جدول۲ مقایسه بین دو حالت انتقال و تونل در AH و ESP را نشان می‌دهد[1,5,7,9].

جدول ۱: مقایسه بین AH و ESP در IPSec

	AH	ESP (encryption only)	ESP (encryption plus authentication)
کنترل دسترسی	✓	✓	✓
صحت connectionless	✓		✓
احراز اصالت منبع داده	✓		✓
رد بسته‌های بازارسال شده	✓	✓	✓
محرمانگی بسته‌ها		✓	✓
محرمانگی جریان ترافیک		✓	✓

جدول۲: مقایسه بین دو حالت انتقال و تونل در AH و ESP

	مد انتقال	مد تونل
AH	احراز بخش داده‌ای IP و بخشهایی از سرآیند IP	احراز اصالت کل بسته IP داخلی به انضمام بخشهایی از سرآیند IP بسته بیرونی
ESP	رمز بخش داده‌ای IP که به دنبال سرآیند ESP قرار دارد	رمز کل بسته IP داخلی
ESP with Authentication	رمز بخش داده‌ای IP که به دنبال سرآیند ESP قرار دارد. احراز اصالت بخش داده‌ای IP و نه سرآیند آن	رمز کل بسته IP داخلی. احراز اصالت بسته IP داخلی

۲-۲- پروتکل PPP

PPP امکان استفاده از TCP/IP بر روی کابل‌های سریال مثل خطوط تلفن را فراهم می‌نماید. با استفاده از این پروتکل، کاربران می‌توانند توسط یک کامپیوتر و مودم به اینترنت متصل شوند. PPP دارای مزایایی از قبیل امکان مبادله اطلاعات به صورت همزمان و غیرهمزمان، ارائه امکانات لازم برای تصحیح خطا، فشرده‌سازی، نسبت‌دهی آدرسها به صورت پویا و استفاده از چندین پروتکل بر روی لینکهای PPP می‌باشد. در هنگام استفاده از این پروتکل، به مواردی از قبیل اکانتی از نوع PPP ، نصب نرم‌افزارهای TCP/IP و PPP بر روی کامپیوتر کاربر و آدرس IP (دائم یا پویا) نیاز است.

۲-۳- پروتکل PPTP

این پروتکل طبق پروتکل PPP ایجاد شد. PPTP یک پروتکل چندگانه می‌باشد که کاربران راه دور به وسیله PPP به یک شبکه خصوصی دسترسی دارند. به طور کلی چون PPP فقط ارتباط بین دو نقطه را برقرار می‌کند و نمی تواند چندین کاربر راه دور را پشتیبانی کند، برای حل این مشکل از PPTP استفاده می‌شود. PPTP اجازه یک نشست PPP را بدون پروتکل TCP/IP می‌دهد (مثلاً IPX و یا NetBeuI). این پروتکل در RFC2637 به‌عنوان یک پیش‌نویس اطلاعاتی مستند شد که از مکانیسم تصدیق هویت مشابهی برای اتصالات PPP در یک ارتباط VPN مبتنی بر PPTP پشتیبانی می‌کند. این مکانیسم شامل پروتکل تصدیق توسعه‌پذیر یا EAP، پروتکل احراز هویت (MSCHAP یا CHAP)، پروتکل تصدیق رمز Shiva (SPAP) و پروتکل تصدیق رمز (PAP) می‌باشد.

۲-۴- پروتکل L2TP

این پروتکل ترکیبی از پروتکل‌های PPTP و L2F (ارسال دولایه) می‌باشد. L2TP می‌تواند به‌عنوان یک پروتکل تونل‌زنی برای بسته بندی کردن قاب‌های PPP استفاده شود تا قاب‌ها سرتاسر یک شبکه ATM ، X.25 یا Frame Relay ارسال شوند. به وسیله این پروتکل، ارتباطات چندگانه از طریق یک تونل انجام می‌شوند. مشابه L2F و PPTP، پروتکل L2TP روی دو لایه OSI کار می‌کند. پروتکل‌های VPN دولایه، داده‌ها را در قاب‌های PPP بسته بندی می‌کنند و قادر به انتقال بسته‌های بدون IP سرتاسر یک شبکه مبتنی بر IP هستند. این پروتکل در RFC3931 مستند شد. ارتباطات L2TP از برخی مکانیسم‌های تصدیق پروتکل PPP مانند CHAP، MS-CHAP، EAP، PAP و SPAP استفاده می‌کند. تونل‌زنی L2TP از طریق سطوح چندگانه فرایند بسته بندی انجام می‌شود. داده PPP داخل یک سرایند PPP و یک سرایند L2TP بسته بندی می‌شود. بسته L2TP، بیشتر با یک سرایند UDP با پورتهای منبع و مقصد پوشش داده می‌شود. آخرین بسته با یک سرایند IP شامل آدرس‌های IP منبع و مقصد سرویس‌دهنده و سرویس‌گیرنده VPN کپسوله می‌شود. به دلیل فقدان محرمانگی L2TP، اغلب به صورت ترکیبی با IPSec استفاده می‌شود که به این حالت عموماً L2TP/IPsec گفته می‌شود. هنگامی که L2TP سرتاسر IPSec در حال اجرا می‌باشد، خدمات و سرویس‌های امنیتی توسط IPSec فراهم می‌شوند (AH و ESP) و همه کنترل‌ها و داده‌های L2TP به‌عنوان بسته‌های داده IP همگن برای سیستم IPSec آشکار می‌شوند.

۲-۵- پروتکل SSL

SSL راه‌حلی برای برقراری ارتباطات ایمن میان یک سرویس‌دهنده و یک سرویس‌گیرنده می‌باشد که توسط شرکت Netscape ارائه شده است. در واقع SSL پروتکلی است که پایین‌تر از لایه کاربرد قرار می‌گیرد. مزیت استفاده از این پروتکل بهره‌گیری از موارد امنیتی تعبیه شده‌ی آن برای امن کردن پروتکل‌های ناامن لایه کاربرد مثل ، LDAP و IMAP می‌باشد که براساس آن الگوریتم‌های رمزنگاری روی داده‌های خام که قرار است از یک کانال ارتباطی غیرامن مثل اینترنت عبور کنند، اعمال می‌شود و محرمانه بودن داده‌ها را در طول کانال انتقال تضمین می‌کند. به بیان دیگر شرکتی که صلاحیت صدور و اعطاء گواهی‌های دیجیتال SSL را دارد برای هر کدام از دو طرفی که قرار است ارتباطات میان شبکه‌ای امن داشته باشند، گواهی‌های مخصوص سرویس‌دهنده و سرویس‌گیرنده را صادر می‌کند و با مکانیزم‌های احراز هویت خاص خود، هویت هر کدام از طرفین را برای طرف مقابل تأیید می‌کند. به علاوه باید تضمین کند که اگر اطلاعات حین انتقال مورد سرقت قرار گرفت، برای رباینده قابل درک و استفاده نباشد که اینکار را با کمک الگوریتم‌های رمزنگاری و کلیدهای رمزنگاری متقارن و نامتقارن انجام می‌دهد. برای داشتن ارتباطات امن مبتنی بر SSL عموماً به دو

نوع گواهی دیجیتال SSL یکی برای سرویس‌دهنده و دیگری برای سرویس‌گیرنده و یک مرکز صدور و اعطای گواهینامه دیجیتال یا CA نیاز می‌باشد. وظیفه CA این است که هویت طرفین ارتباط، نشانی‌ها، حساب‌ها و تاریخ انقضای گواهینامه را بداند و براساس آن هویت‌ها را تعیین نماید. پروتکل SSL دارای دو زیر پروتکل بنام SSL Record و SSL Handshake می‌باشد. تفکیک پروتکل SSL به دو زیر پروتکل دارای مزایای متعددی است. اولاً در ابتدای کار و طی مراحل اولیه ارتباط، هویت سرویس‌دهنده برای سرویس‌گیرنده مشخص می‌گردد. و ثانیا در همان ابتدای شروع تبادلات، سرویس‌دهنده و سرویس‌گیرنده بر سر نوع الگوریتم رمزنگاری تبادلی توافق می‌کنند. همچنین در صورت لزوم، هویت سرویس‌گیرنده نیز برای سرویس‌دهنده احراز می‌گردد و در صورت استفاده از تکنیک‌های رمزنگاری مبتنی بر کلید عمومی، می‌توانند کلیدهای اشتراکی مخفی را ایجاد نمایند. ارتباطات بر مبنای SSL رمزنگاری می‌شوند. الگوریتم‌های رمزنگاری پشتیبانی شده در SSL از اغلب الگورتیم‌های عمومی رمزنگاری و تبادل کلید مثل DES، DSA، KEA، MD5، RC2،RC4، RSA، RSA Key Exchange، SHA-1، Skipjack و DES3 پشتیبانی می‌کنند و بسته به اینکه نرم‌افزارهای سمت سرویس‌دهنده و سرویس‌گیرنده نیز از موارد مذکور پشتیبانی میکنند، ارتباطات SSL می‌توانند بر اساس هر کدام از این الگوریتم‌ها انجام شوند. البته بسته به طول کلید مورد استفاده در الگوریتم و قدرت ذاتی الگوریتم، می‌توان آن‌ها را در رده‌های مختلفی قرار داد که توصیه می‌شود با توجه به سناریوهای مورد نظر، از الگوریتم‌های قوی‌تر نظیرDes3 با کلید ۱۶۸ بیتی برای رمزنگاری داده‌ها و همچنین الگوریتم SHA-1 برای مکانیزم‌های تأیید پیغام MD5 استفاده شود و یا این‌که اگر امنیت در این حد مورد نیاز نبود، می‌توان در مواردی خاص از الگوریتم رمزنگاری RC4 با کلید ۴۰ بیتی و الگوریتم تأیید پیغام MD5 استفاده نمود. SSL می‌تواند از ترکیب رمزنگاری متقارن و نامتقارن استفاده کند. رمزنگاری کلید متقارن سریع‌تر از رمزنگاری کلید عمومی است و از طرف دیگر رمزنگاری کلید عمومی تکنیک‌های احراز هویت قوی‌تری را ارائه می‌کند. یک نشست SSL با یک تبادل پیغام ساده تحت عنوان SSL Handshakeشروع می‌شود. این پیغام اولیه به سرویس‌دهنده این امکان را می‌دهد تا خودش را به سرویس‌دهنده دارای کلید عمومی معرفی نماید و سپس به سرویس‌گیرنده و سرویس‌دهنده این اجازه را می‌دهد که یک کلید متقارن را ایجاد نمایند تا برای رمزنگاری‌ها و رمزگشایی سریع‌تر در جریان ادامه مبادلات مورد استفاده قرار گیرد. جداول ۳، ۴ و ۵ به ترتیب دسته‌بندی VPN براساس رمزنگاری، پیاده‌سازی لایه‌ای و پروتکلها را نشان می-دهند.

۳- مخاطرات VPN

حملاتی که ممکن است در یک شبکه مبتنی بر VPN رخ دهند شامل حملات هک، تصدیق کاربر، سرویس‌گیرنده، ویروسها (کرمها) و حملات ناشی از قوانین نادرست دسترسی به شبکه می‌باشند. ممکن است درون یک شبکه ارتباطی، ماشین سرویس‌گیرنده یا مشتری، هدف حمله قرار گیرد یا یک نقطه جاسوسی برای مهاجم تلقی شود. یک مهاجم یا هکر می‌تواند به طور مخفیانه از شبکه استفاده کند و یا پیکربندی نامناسبی را برای سرویس‌گیرنده ایجاد کند. همچنین هکر می‌تواند انواع مختلفی از ابزارهای هک و نفوذ را برای یک حمله به کار گیرد. حملات نفوذ به دو دسته‌ی سرقت VPN و man-in-the-middle تقسیم می‌شوند. سرقت VPN، تسخیر کامل یک ارتباط قانونی VPN از یک سرویس‌گیرنده راه دور و جعل هویت آن می‌باشد. حملاتی که به واسطه انسان ایجاد می‌شوند، ترافیک بین گروههای ارتباطی را تحت تاثیر قرار داده و شامل قطع، الحاق، حذف و اصلاح پیامها، بازگشت به فرستنده و ارسال مجدد آنها می‌باشد. یک ارتباط VPN باید به وسیله یک کاربر تأیید شده و مجاز، قانونی شود.

جدول۳: دسته‌بندی VPN براساس رمزنگاری

شبکه	وظایف	انواع
VPN رمزشده	استفاده از رمزنگاری برای انتقال امن اطلاعات	شبکه‌های خصوصی مجازی به کمک IPSEC
VPN رمزنشده	اتصال دو یا چند شبکه خصوصی به منظور استفاده از منابع شبکه، عدم اهمیت چندان امنیت در حین تبادل و	روش تفکیک مسیریابی (فقط اطلاعات در حال تبادل بین دو شبکه-ی خصوصی به هر

	ایجاد امنیت با روشهایی غیر از رمزنگاری	یک از آنها مسیردهی می‌شوند)

جدول ۴: دسته‌بندی VPN بر اساس لایه‌های پیاده‌سازی

نام لایه	مشخصات	معایب
پیوند داده	ایجاد دو شبکه خصوصی با استفاده از پروتکل‌های ATM و Frame relay	استفاده از ATM و Frame relay هزینه بالایی دارد، نیاز به مسیر اختصاصی، امنیت پایین، عدم رمزنگاری توسط ATM و Frame relay
شبکه	استفاده از تونل‌زنی و تکنیکهای رمزنگاری مثل IPSec، GRE و L2TP، بهترین لایه برای رمزنگاری	-
کاربرد	هدف اصلی ایجاد کار با برنامه‌های کاربردی است، SSH و SSL VPN نمونه‌های مناسبی از این روش می‌باشند.	با افزایش خدمات و برنامه-های جدید، نیاز به فرایندهای پشتیبانی جدید نیز می‌باشد.

اگر تصدیق برای دسترسی محدود به اندازه کافی قوی نباشد، هر کسی می‌تواند به ارتباطات شبکه و منابع آن دسترسی داشته باشد. اکثر پیاده‌سازی‌های VPN، روشهای محدودی از تصدیق و سندیّت را فراهم می‌کنند. به عنوان مثال، پروتکل PAP مورد استفاده در PPTP، نام کاربری و رمز عبور را در قالب یک متن واضح و آشکاری انتقال می‌دهد. طرف ثالثی می‌تواند این اطلاعات را تسخیر کرده و آنها را برای دسترسی‌های بعدی به شبکه به کار گیرد.

سرویس‌گیرنده VPN که اغلب کاربران خانگی هستند ممکن است به وسیله اینترنت و یا ارتباط WAN در تماس باشند که ممکن است این ارتباطات صورت گرفته از طریق VPN منجر به خطراتی شود. همچنین یک سرویس‌گیرنده ممکن است با سایر گروه‌هایی که از سیاست‌های امنیتی اطلاعات کافی ندارند، اطلاعاتی را به اشتراک بگذارد و یا از اطلاعات به صورت مشترک استفاده کند. بنابراین تمهیدات امنیتی برای اغلب کاربردهای مبتنی بر VPN کافی نیستند. حتی اگر سرویس‌گیرنده VPN، قبل یا در طول ارتباط بر روی سیاست‌های امنیتی خاصی نیز توافق کند، باز هم وقوع تهدیدات امنیتی دور از ذهن نیست. اگر یک شبکه ارتباطی تحت تأثیر ویروس‌ها یا کرم‌ها قرار گیرد، ممکن است رمز VPN برای مهاجمان آشکار شود. به طورکلی اگر یک VPN اکسترانت یا اینترانت تحت تأثیر ویروس‌هایی قرار گیرد که خیلی زود در سطح شبکه توزیع شوند، آنگاه سیستم‌های ضدویروس و حفاظت از ویروس نیز مؤثر نخواهند بود.

جدول۵: دسته‌بندی VPN بر اساس نوع پروتکل

نوع پروتکل	وظایف و مشخصات
PPP VPN	- امکان مبادله اطلاعات به صورت همزمان و غیر همزمان و استفاده از چندین پروتکل بر روی لینکهای PPP - ارائه امکانات لازم به منظور تصحیح خطا، فشرده‌سازی، نسبت‌دهی آدرسها به صورت پویا - عملکرد کند پروکسی به علت رمزگذاری ، رمزگشایی و بازرسی محتویات - AT نیاز به موتور مترجم دارد.
PPTP VPN	- مناسب برای انتقال NetBEUI روی یک شبکه بر پایهIP و پیاده سازی روی لایه پیوند داده - نگهداری و مدیریت تونل به وسیله مکانیزم نگهداری فعال(KA) و توسعه یافته پروتکل PPP - رمزگذاری اطلاعات با نرخ ۱۲۸ بیت و ارتباط به صورت TCP، استفاده از PPP برای ارتباطات WAN - دارای قابلیت فشرده سازی سرایند(سرایند ۶ بایتی فشرده شده)، استانداردهای امنیتی پایین - فقط روی شبکه‌های مبتنی بر IP کار می‌کند، نرخ انتقال و امنیت پایین(در گذشته) - PPTP بدون IPSec ، امنیت کمتری نسبت به L2TP دارد. - نداشتن مکانیزمی برای حفظ تمامیت و تصدیق اطلاعات مبداء - کارایی پایین در شبکه‌های ناپایدار، استفاده از رمزگذاریPPP - پشتیبانی توسط دیوارهای اتش ISA Sever یا Cisco PIX و Sonic Wall
L2TP VPN	- ترکیبی است از بهترین خصوصیات موجود در L2F وPPTP - مناسب برای شبکه های مبتنی بر IP و مبتنی برX.25 ، Frame Relayو یاATM - استفاده از اتصال UDP و دارای قابلیت فشرده سازی سرایند(سرایند ۴ بایتی فشرده شده) - برخورداری از ویژگی های امنیتی بیشتری نسبت بهPPTP ، استفاده از پروتکل IPSec برای رمزنگاری - سرعت کمتر نسبت به PPTP به علت افزایش امنیت و طولانی شدن مراحل امنیتی - نیاز به انجام تنظیمات رجیستری در برخی سیستم عاملها مثل Server 2008 و Vista - عدم تطابق بین کلیدهای امنیتی و ناسازگاری با NAT ، مناسب برای زمانیکه امنیت مهم است نه سرعت
SSL VPN	- برقراری ارتباط بین سرور و کلاینت و انجام درخواستهای داخلی و ترجمه و عبور اطلاعات به سرورهای دیگر - ترجمه اطلاعات از یک پروتکل به پروتکل دیگر، ارتباط ایمن با چندین سرور - توسعه شبکه، کارکرد در لایه انتقال داده و پورت TCP443 - مراحل پیاده‌سازی شامل ، شناسایی نیازهای سازمان، طراحی راه‌حل، پیاده‌سازی و تست نمونه اولیه، مدیریت راه‌حل اجراشده - سازگار با مرورگرهایی که بتوانند از محتوی فعال (Active) پشتیبانی کنند. مانند : Flash, Java Script, Java ActiveX - دارای دو نوع Full Tunnel و Split Tunnel می باشد.
IPSec VPN	- ارسال اطلاعات به صورت رمزگذاری به همراه یک سرایند IP ، تعیین اعتبار توسط AH ، رمزگذاری از طریق ESP - استفاده از Diffie-Hellman برای مبادله کلیدها میان ایستگاههای دو سر ارتباط - استفاده از امضاهای دیجیتال برای تعیین اعتبارهای دیجیتالی، پیاده‌سازی IKE سخت - مراحل پیاده‌سازی شامل، طی کردن پارامترهای پروتکل، مبادله کلیدهای عمومی، تایید هویت هر دو طرف، مدیریت کلیدها پس از مبادله - پیاده‌سازی و کارکرد روی لایه شبکه، تونل‌زنی به شیوه اجباری و اختیاری - رمز گذاری Public Key برای ثبت و اطمینان از کلیدهای مبادله شده و همچنین اطمینان از هویت ایستگاههای سهیم در ارتباط - استفاده از الگوریتم‌های رمز گذاری مانند DES برای اطمینان از درستی داده‌های انتقالی - استفاده از الگوریتم‌های درهم ریزی (Hash) برای تعیین اعتبار تک تکPacket ها - پیاده سازی های دستی و غیر قابل تغییرIPSec که توسط IKE قابل حل است.

۴- ملاحظات امنیتی در VPN

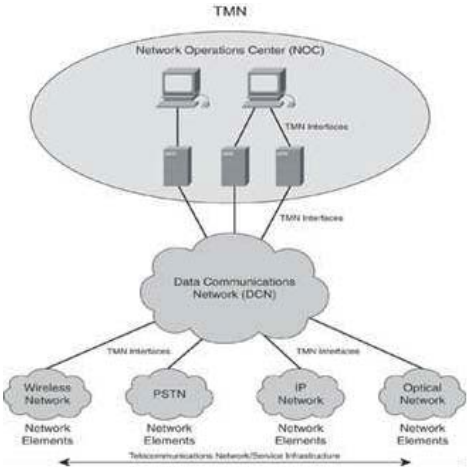
ملاحظات امنیتی در VPN به سه دسته: ۱) عمومی، ۲) اکسترانت و ۳) ملاحظات سرویس‌گیرنده دسته‌بندی می‌شوند. این ملاحظات بیشتر در هنگام انتخاب و یا استفاده از یکی از محصولات یا تولیدات VPN مطرح می‌شوند. یک VPN به منظور حفظ امنیت باید سه وظیفه مهم را انجام دهد. ابتدا باید اعتبار کاربر تأیید شود. این عمل، تأیید ارتباط رمزنگاری‌شده نام دارد. ثانیاً داده‌هایی که تبادل می‌شوند باید با کدگذاری اطلاعات در زمان بارگذاری، ایمن شوند. ثالثاً، VPN باید ترافیک شبکه را بین شبکه‌های ایمن حفظ کند. به این عمل بسته بندی کردنIP گفته می‌شود.

۴-۱- کیفیت سرویس در VPN مبتنی بر IP

به طور کلی کیفیت سرویس(QoS) به معنای کم‌ترین تأخیر یا گم‌شدن بسته‌ها است که برای انواع مشخصی از کاربردها یا ترافیک تعریف شود. شبکه‌های سنتی می‌توانستند سطوح ثابتی را برای در دسترس بودن منابع در همه وضعیت‌ها تضمین کنند که این تضمین با استفاده از مدارهای اجاره‌ای اختصاصی صورت می‌گرفت. VPNهای دولایه می‌توانند کارایی قابل قبول و قابل مقایسه با راه‌حل‌های خطوط اختصاصی، ایجاد کنند. همچنین انتظار می‌رود که تهیه‌کنندگان سرویس IPVPN نیز QoS را به همین شکل پشتیبانی کنند. به وسیله IETF دو چارچوب به عنوان معماری QoS در شبکه‌های مبتنی بر IP به وجود آمده است که عبارتند از: سرویس‌های مجتمع یا IntServ و سرویس‌های متمایز یا DiffServ. همچنین MPLS همراه با مدیریت ترافیک و مسیریابی مبتنی بر محدودیت نیز ابزارهای جدیدی را برای مدیریت و کنترل QoS تهیه می‌کنند که این روش‌ها قابل استفاده در VPNهای مبتنی بر IP نیز هستند.

۴-۲- نیازمندیهای مدیریت QOS در VPN

از آنجا که VPNها معمولا ارتباطات شبکه خصوصی امنی هستند که روی یک زیرساخت قابل دسترس عمومی مانند اینترنت یا شبکه تلفن عمومی ایجاد می‌شوند، بنابراین یک VPN باید شبیه به یک شبکه خصوصی رفتار کند. به طور معمول بر طبق مدل TMN، رفتار جداگانه‌ای برای مدیریت شبکه و کنترل آن در نظر گرفته می‌شود. شکل ۹ یک شبکه TMN را نشان می‌دهد.



شکل ۹: شبکه TMN

توابع مدیریتی اغلب به صورت یک لایه پوششی که عملیات مخصوص FCAPS را انجام می‌دهند، پیاده‌سازی می‌شوند. امروزه این جداسازی واضح بین سطح کنترلی و سطح مدیریتی چندان آشکار نیست. انواع ویژه‌ای از مدیریت شبکه تاکنون در پروتکل‌ها (مخصوصا در لایه بالا) قرار گرفته‌اند و حرکت آنها به سمت سرمایه‌گذاری بالا در مدیریت خدمات و توسعه مکانیزم‌های مدیریتی سطح بالا برای خودکار کردن زیربرنامه‌های خاص مدیریتی و کاهش زمان تحویل می‌باشد. یکی از موضوعات کلیدی برای موفقیت VPN، مساله کیفیت سرویس است. ترکیب VPN با QoS منجر به محصولاتی با قابلیت رقابتی بالا می‌شود. بنابراین هم VPNو هم QoS باید بصورت ترکیبی مدیریت شوند، بدون توجه به اینکه چه نوع معماری برای VPN انتخاب می‌شود یا چه فناوری، QoS را پشتیبانی می‌کند. سرویس‌های IPVPN (VPN مبتنی برIP) فرصت خوبی را برای فراهم‌کنندگان خدمات فراهم می‌کنند تا منافع جدید و بیش‌تری را دریافت کنند. فراهم‌کنندگانی که بتوانند سرویس‌های IPVPN قابل مدیریت و به سرعت قابل گسترشی را عرضه کنند، سود رقابتی بالایی را به دست خواهند آورد. کلید موفقیت خدمات IPVPN را می‌توان به طور ساده در فناوری ایجاد شده جست‌وجو کرد. مدیریت‌پذیری سرویس و مدیریت کل دوره‌ی زمانی یعنی برنامه‌ریزی، تدارک، مانیتورینگ، عملیات و صورت‌حساب، مهم هستند. تهیه‌کنندگان سرویس، دیگر روی قیمت با یکدیگر رقابت نمی‌کنند بلکه بر روی زمان تحویل سرویس

رقابت می‌کنند. بنابراین کلید گسترش سودآور سرویس VPN، مدیریت است.

۴-۳- قابلیتهای عمومی مدیریت QOS برای تدارک IP-VPN

قابلیتهای عمومی مدیریت QoS برای تدارک IPVPN شامل پشتیبانی از نیازمندی‌های گوناگون ترافیک کاربر، ارائه، پشتیبانی و نگه‌داری سطوح توافق شده سرویس (مثل پیکربندی، خرابی، کارآیی، امنیت و...) می‌باشند. هر FCAPS باید با SLA مقایسه شود و هر تخطی از QoS و SLA باید به طور خودکار کشف شود. فراهم‌سازی هر نوع اطلاعاتی باید متناسب با نیازمندی‌های QoS و SLA باشد. برخی از قابلیت‌های مدیریتی باید در SLAها قرار گیرند و مدیریت SLA باید چنان باشد که سطح خدمات (مثل قابلیت انتقال IP، پارامترهای QoS، در دسترس بودن، اطمینان‌پذیری، تثبیت و تایید تحویل، پشتیبانی پویا و قابلیت حمل ونقل، امنیت، پهنای باند، اولویتها، تشخیص هویت، پروتکل‌های پشتیبانی شده، گسترش انعطاف‌پذیری و متصل بودن و مدت زمان SLA) مشخص باشد. همچنین مانیتورینگ QoS باید با اهداف فوق، ردیابی جریان ترافیکی، تهیه و ارائه گزارش‌های مورد نیاز، سود و زیان مالی، صورت‌حساب، جریمه‌ها، قیمت‌گذاری و هزینه‌های خاتمه‌ی زود هنگام سرویس و موارد مشابه همسو باشد. برای این که بتوانیم به طور واقعی مدیریت SLA را انجام دهیم، لازم است تا در همه سرویس‌های وابسته و اطلاعات مشتریان، یک مدیریت مؤثر داشته باشیم. توابع مدیریت SLAباید گستره وسیعی از منابع داده را ترکیب، وابستگی آنها را پیدا و در نهایت این موارد را ارزیابی و مدیریت کنند تا بتوانند به گونه‌ای مؤثر، حصول SLA ها را مدیریت و ضمانت کنند. مدل لایه‌ای به عنوان روشی اساسی برای مدیریت شبکه و QoS مناسب است. با این مدل، مدیریت شبکه، QoS، کارآیی و مانیتورینگ می‌تواند بر اساس اهداف مورد نظر کاربر انتخاب شوند. سیستم‌های مدیریت QoSباید برای انواع مختلف ترافیک انتها به انتها و برای ویژگیهای ارتباطی VPNها طراحی شوند.

۵- مدل‌های پیشنهادی

برای پیاده‌سازی، مدیریت، مستندسازی، ذخیره‌سازی و نیز پردازش داده‌ها باید یک پایگاه داده‌ی استاندارد به کار گرفته شود و سیستم‌های پایگاه داده پشتیبان عملیات و مدیریت باید به صورت مجتمع وجود داشته باشند. برای مدیریت خرابی‌ها، پیاده‌سازی ثبت رخدادها و مانیتور کردن وضعیت، علاوه بر سطوح هشدار، مجتمع‌سازی گزارش خرابی و سیستمهای trouble ticket نیز پیشنهاد می‌شود. برای پشتیبانی از خودکارسازی مدیریت پیکربندی، مدل تحویل سرویس IPVPN بر مبنای مدل ارائه‌ی اصلی پیشنهاد می‌شود. عملیاتی از قبیل پیش بینی ترافیک (مثل ظرفیت و نوع ترافیکی که قرار است انتقال یابد)، تقاضا در رزرو منابع و تغییرات موجود در آن، توجه به کاربر و رسیدگی به دستورات سیستم پشتیبانی از زمان تحویل سرویس، به صورت ترکیبی می‌توانند بر مبنای این مدل انجام شوند. پیاده‌سازی سیستمهای پشتیبانی استاندارد که برای اهدافی نظیر تشخیص هویت و مدیریت حسابرسی به کار برده می‌شوند نیز می‌تواند موثر باشد. همچنین استفاده از معماری مبتنی بر امنیت برای پیاده‌سازی یا ایجاد زیرساختهای امنیتی نیز مناسب می‌باشد. طبق استاندارد IETFچهار گزینه برای گسترش سیستم‌های مدیریت VPNو سیستم‌های پشتیبانی QoS برای تحویل سرویس VPNوجود دارد که عبارتند از:

- استفاده از یک مدل call-centre برای کنترل مشتری
- گسترش سیستم‌های مدیریتی سفارشی و اغلب اختصاصی
- کنترل سیستم‌ها، مانیتورکردن راه‌حل‌های پیاده‌سازی شده برای مدیریت backbone شبکه IPVPN و تحویل سرویس
- پیاده‌سازی استانداردها و نیز راه حل‌های مدیریت VPN بر اساس سیاست‌های شبکه

۶- خلاصه و نتیجه‌گیری

در این تحقیق، مروری کلی بر VPN و معماری آن داشتیم و پروتکلهای امنیتی و مورد استفاده در VPN را مورد نقد

و بررسی قرار دادیم. پروتکل‌هایی مانند IPSec ، PPTP ، PPP و L2TP به همراه ویژگی‌های آنها معرفی شدند و در انتها پروتکل SSL تعریف و نقاط قوت آن ارائه شد. سپس مخاطرات امنیتی در VPN را بیان کردیم و در یک تقسیم-بندی مجزا، ملاحظات امنیتی را به سه دسته عمومی، اکسترانت و سرویس‌گیرنده تقسیم و برای هر یک به طور جداگانه، موارد امنیتی بیان شد. در انتها نیز سیاست‌های کلی امنیتی در VPN مطرح شدند. همچنین در بخشی مجزا، نفوذ و روشهای تشخیص نفوذ ارائه و مواردی از قبیل انواع سیستم‌های تشخیص نفوذ، مدل فرایندی برای تشخیص نفوذ معرفی و بیان شدند. در انتها نیز مفاهیم مدیریتی و راهکار پیشنهادی ارائه شد.

مراجع

[1] T. Braun, M. Günter, M. Kasumi, I. Khalil,"Virtual Private Network Architecture", Institut für Informatik und Angewandte Mathematik (IAM), Uni Bern Neubrückstr. 10, CH-3012 Bern,1999

[2] Michael Stines,"Remote Access VPN – Security Concerns and Policy Enforcement", GSEC Practical 1.4b – option 1,2003

[3] Abd Karim Bin Md Sah,"A Study of Scalability Over MPLS VPN,In Partial Fulfillment of Requirement for the Bachelor of Science (hons)",In Data Communication and Networking, April 2005

[4] Vertical Systems Group,"Enterprise VPNs:Choose performance and Reliability and Low Cost", 2008

[5] Chen Lin , Wang Guowei, "Security Research of VPN Technology Based on MPLS", Proceedings of the Third International Symposium on Computer Science and Computational Technology(ISCSCT '10) Jiaozuo, P. R. China, 14-15,August 2010, pp. 168-170

[6] Jared Lewis and Devin Kahrs , "An Analysis of Virtual Private Networks", June 6, 2004

[7] Mark Bouchard ,"SSL VPN: The Ideal Approach for Establishing Secure Access to Virtual Desktop Infrastructure Solutions", Juniper Networks,2009

[8] Roy Hills, NTA Monitor Ltd, "Common VPN Security Flaws"

[9] Anwar Haque, Pin-Han Ho," Design of Survivable Optical Virtual Private Networks (O-VPNs)", School of Computer Science University of Waterloo Ontario, Canada, N2L 3G1,2009

[10] Akira Misawa, Satoru Okamoto,Masaru Katayama,Naoaki Yamanaka," Optical VPN Service Using OUNI/GMPLS Signaling for Service Assignment With HIKRAI Router ",ECOC IOOC 2003 Proceedings,VOL.3,2008

[11] Hamid Ould-Brahim, Yakov Rekhter, Luyuan Fang and etc," Service Requirements for Optical VPNs", 51th IETF, London, August 2001

[12] Mira Yun ," Differentiated Optical QoS Service Framework in Next Generation Optical VPN", Thesis for Degree of Master of Engineering, Department of Telematics Engineering, Pukyong National University, February 2004

[13] Timothy K. Shih," Advanced Penetration Testing Methodology for VPN", Journal of Security Engineering,2008

[14] Priyanka Gupta, Ashok Verma," Establishing a Service Model of Private Elastic VPN for cloud computing", International Journal of Computer Science and Network (IJCSN) Volume 1, Issue 4, August 2012

[15] Sanjay Jha,Anil Sood,"A Framework for QOS Enabled IP-VPN Management ",2009

[16] Isaias Martinez-Yelmo, David Larrabeiti, Ignacio Soto, Piotr Pacyna," Multicast Traffic Aggregation in MPLS-based VPN networks", Departamento de Ingenier´ıa Telem´atica Universidad Carlos III de Madrid,2010

[17] Pham Ngoc Thanh, Keecheon Kim," A methodology for implementation and integration Two-Factor Authentication into VPN",2012

[18] Yue Tian, Xiangqing Tian, Lufeng Leng, Tong Ye, Yikai Su," Optical VPN Connecting ONUs in Different PONs", State Key Lab of Advanced Optical Communication Systems and Networks,2007

[19] Bill Uliasz," Verizon Optical Network Strategic Vision", Verizon – Core Network & Technology Director – Access & Transport Network Architecture, February 25, 2008

[20] D. Papadimitriou, E. Mannie, D. Brungard, S. Dharanikota, J. Lang, G.

[21] Li, B. Rajagopalan, and Y. Rekhter, "Analysis of Generalized MPLS-based RecoveryMechanisms (including Protection

and Restoration)", Internet Draft, working in progress, May 2003.
[21] K. Sriram, D. Griffith, S. Lee, and N. Golmie, "Backup Resource Pooling in (M:N)n Fault Recovery Schemes in GMPLS Optical Networks", Opticomm 2003.
[22] P. –H. Ho and H. T. Mouftah, "Reconfiguration of Spare Capacity for MPLS-based Recovery in the Internet Backbone Networks", IEEE/ACM Transaction on Networking, Vol. 12, No. 1, Feb. 2004.
[23] P. –H. Ho and H. T. Mouftah, "A Framework of a Survivable Optical Internet using Short Leap Shared Protection (SLSP)", IEEE Workshop on High Performance Switching and Routing (HPSR 2001), Dallas, May, 2001
[24] B. Ramamurthy and A. Ramakrishnan, "Design of Virtual Private Networks (VPNs) over Optical Wavelength Division Multiplexed (WDM) Networks", SPIE Optical Networks Magazine, Vol. 3, Issue 1, Jan./Feb. 2002
[25] P. –H. Ho and H. T. Mouftah, "On Optimal Diverse Routing for Shared Protection in Mesh WDM Networks", IEEE Transactions on Reliability (to appear in March 2004).
[26] Yang Qin, K. M. Sivalingam and Bo Li, " QoS for Virtual Private Networks (VPN) over Optical WDM Networks ",Optical Communications and Networking Conference, (Dallas, TX), Oct. 2000
[27] D. Xu, C. Qiao, and Y Xiong, "An Ultra-fast Shared Path Protection Scheme Distributed Partial Information Management, Part II", Proceedings IEEE International Conference on Network Protocols (ICNP 2002), Paris, France , Nov. 2002.
[28] S. Ramamuthy and B. Mukherjee, "Survivable WDM mesh networks: Part I-Protection," Infocom'99, New York, Mar. 1999.
[29] R. R. Iraschko and W. D. Grover, "A Highly Efficient Path-Restoration Protocol for Management of Optical Network TransportIntegrity", IEEE Journal on Selected Areas in Communications (JSAC), vol. 18, no. 5, May 2000, pp.779-793.
[30] Jian C, Chin L, "A restorable MPLS-based hose-model VPN network, " Computer Networks, vol. 5l, pp. 4836- 4848, 2007
[31] Myoungju Y, Jongmin L, Tai-Won U, "A new mechanism for seamless mobility based on MPLS LSP in BCN," IEICE Transactions on Communications, vol. 91, pp. 593- 596, 2008.
[32] Rosen E, Rekhter Y, RFC 4364 BGP/MPLS IP Virtual Private Networks (VPNs)[S], IETF, 2006.
[33] Yang Yanyan, Martel Charles U, Fu Zhi, Wu Shyhtsun Felix, "IPSec/VPN security policy correctness and assurance," Journal of High Speed Networks, vol. 15, pp. 275-289, 2006.VPN Consortium,
[34] "VPN Technologies: Definitions and Requirements", 2008. http://www.vpnc.org/vpntechnologies.html
[35] H. Hiroaki, Y. Kamizuru, A. Honda, T. Hashimoto, K. Shimizu, and H.Yao, "Dynamic IP-VPN architecture for cloud computing", in nformation and Telecommunication Technologies (APSITT), 2010 8th Asia-Pacific Symposium on, 2010.
[36] S. Yasukawa, Signaling Requirements for Point-to-Multipoint Traffic-Engineered MPLS Label Switched Paths (LSPs), RFC 4461 (Informational), Apr. 2006. [Online]. Available: http: //www.ietf.org/rfc/rfc4461.txt