دانشکده مهندسی کامپیوتر

آزمایشگاه شبکه‌های کامپیوتری

فعالیت پژوهشی گزارش اولیه

عنوان آزمایش : آشنایی با شبکه‌های خصوصی مجازی
Virtual Private Network (VPN)

دکتر بردیا صفایی

سارا آذرنوش — ۹۸۱۷۰۶۶۸

کهبد آئینی — ۹۸۱۰۱۲۰۹

پارسا محمدیان — ۹۸۱۰۲۲۸۴

۱۶ اسفند ۱۴۰۲

فهرست مطالب

۱ توضیح پروژه ۲

۲ خلاصه‌ی مقاله‌ی مروری در حوزه‌ی VPN ۲

۳ Vpn ۲

۱.۳ ریسک ها و تهدیدها ۲

۱.۱.۳ احراز هویت کاربران معتبر ۲

۲.۱.۳ خطرات در سمت مشتری ۲

۳.۱.۳ آلودگی های ناشی از ویروس یا بدافزار ۳

۲.۳ انواع ۳

۱.۲.۳ OVPN(Optical Virtual Private Networks) ۳

۲.۲.۳ IPsec ۳

۳.۲.۳ PPTP (Point to Point Tunnel Protocol) ۵

۴.۲.۳ L2TP (Layer 2 Tunneling Protocol) ۵

۱ توضیح پروژه

۲ خلاصه‌ی مقاله‌ی مروری در حوزه‌ی VPN

در این پروژه تصمیم داریم مرور و پژوهشی در حوزه‌ی شبکه‌های خصوصی مجازی یا Virtual Private Network (VPN) داشته باشیم.
روند انتخاب این حوزه از شبکه‌های اینترنتی به عنوان موضوع این پژوهش، بارش فکری اعضای گروه بوده. پس از انتخاب فیلد کلی پژوهش به انتخاب مقاله از بین گزینه‌های مد نظر خواهیم پرداخت.
همانطور که ذکر شد حوزه‌ی اصلی این پژوهش شبکه‌های خصوصی مجازی می‌باشد و مقالات و مقاله‌های مروری از این بخش انتخاب شده‌اند. از کلمات کلیدی این پژوهش می‌توان VPN, Tunneling, Protocols, IPsec, Firewall, L2TP نام برد.

۳ Vpn

شبکه های خصوصی مجازی (Virtual Private Networks)
VPN یک شبکه خصوصی است که در یک زیرساخت شبکه عمومی مانند اینترنت جهانی ساخته شده است.
یک شبکه شامل هر تعداد دستگاهی است که می توانند از طریق روش های دلخواه ارتباط برقرار کنند. دستگاه هایی از این نوع شامل رایانه ها، چاپگرها، روترها و غیره هستند و ممکن است در مکان های جغرافیایی متنوعی قرار گیرند. روش‌هایی که در آنها ممکن است ارتباط برقرار کنند، بسیار زیاد است، زیرا تعداد بیشماری دستگاه وجود دارد.
در ساده‌ترین تعریف، «خصوصی» به این معناست که ارتباطات بین دو (یا چند) دستگاه، به نوعی مخفی است (این که دستگاه‌هایی که در ماهیت «خصوصی» ارتباطات شرکت نمی‌کنند، در محتوای ارتباطی محرمانه نیستند.)
مجازی به معنی شبیه سازی شده است. انجام کارکردهای چیزی که واقعاً وجود ندارد.

۱.۳ ریسک ها و تهدیدها

امنیت از مهم ترین ویژگی ها است که باید نگهداری شود و مورد خطرات بسیاری مانند زیر قرار میگیرد.

۱.۱.۳ احراز هویت کاربران معتبر

احراز هویت کاربر در VPN قوی نیست. از آنجایی که اتصال VPN توسط کاربران مجاز برقرار می شود، فرض بر این است که کاربران در VPN کاربران تأیید شده هستند. به دلیل این آسیب‌پذیری، دسترسی غیرمجاز به شبکه وجود خواهد داشت و ممکن است سرقت داده، از دست دادن داده‌ها و غیره رخ دهد.

۲.۱.۳ خطرات در سمت مشتری

کاربران مشتری ممکن است دو اتصال داشته باشند، یعنی اتصال اینترنت و اتصال VPN به یک شبکه خصوصی. این امر خطر و تهدیدی را برای شبکه خصوصی ایجاد می کند، زیرا کاربران شبکه خصوصی را در معرض شبکه عمومی، که اینترنت است، قرار می دهند. یک سیستم کلاینت همچنین ممکن است از نظر امنیت در شبکه با یک سیستم در معرض خطر مرتبط باشد.

۳.۱.۳ آلودکی های ناشی از ویروس یا بدافزار

اگر یک سیستم کلاینت توسط ویروس یا بدافزار آلوده شود، کل شبکه برای حمله فوری در معرض خطر قرار می گیرد. مهاجم ممکن است بتواند رمز عبور اتصال VPN را بدزدد. ویروس یا بدافزار موجود در یک سیستم کلاینت ممکن است به صورت سیستمی به سیستم های دیگر در شبکه سرایت کند و در نتیجه شبکه را آسیب پذیر و مستعد خطر کند. بنابراین، یک سیستم ضد ویروس موثر باید در شبکه گنجانده شود.

۲.۳ انواع

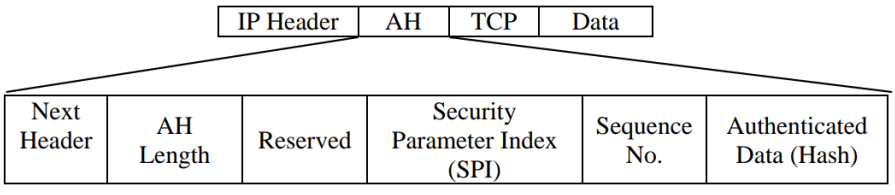
۱.۲.۳ OVPN(Optical Virtual Private Networks)

خدماتی را در قالب اتصال نوری به مشتری ارائه می دهد که انتظار می رود یکی از کاربردهای اصلی در شبکه های نوری آینده باشد. OVPN می تواند رویکرد مطلوبی برای تحقق خدمات شبکه خصوصی مجازی (VPN) نسل بعدی باشد.
انتظار می رود که آنها یکی از کاربردهای اصلی در شبکه های نوری آینده باشند. بنابراین، over OVPN IP (پروتکل اینترنت)/GMPLS (تعمیم چند پروتکل برچسب سوئیچینگ) بر روی فناوری DWDM (تقسیم طول موج متراکم) به عنوان یک رویکرد مطلوب برای تحقق خدمات VPN نسل بعدی پیشنهاد شده است.

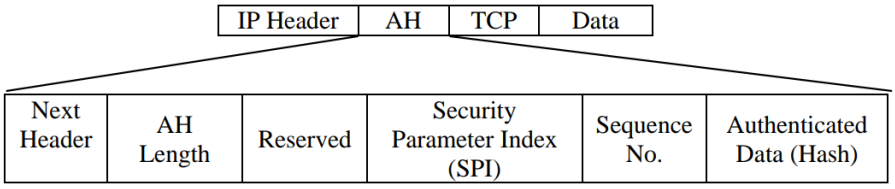
۲.۲.۳ IPsec

IPSec یکی از کامل ترین، ایمن ترین و در دسترس ترین استانداردهای مبتنی بر پروتکل های توسعه یافته برای انتقال داده ها است. در لایه شبکه عمل می کند. IPSec حاوی پروتکل هایی است که به ایجاد احراز هویت متقابل بین دو طرف در ارتباط در ابتدای جلسه و مذاکره درباره کلیدهای رمزنگاری برای استفاده در جلسه کمک می کند. IPSec مجموعه ای از پروتکل های امنیتی است که به سیستم اجازه می دهد پروتکل های امنیتی مناسب را در حین انتقال داده انتخاب کند. IPSec می تواند برای محافظت از انتقال داده بین دو میزبان یا بین یک جفت دروازه امنیتی (مانند فایروال ها یا روترها) استفاده شود. IPSec احراز هویت کاربران، رمزگذاری داده ها و یکپارچگی داده ها را در حین انتقال داده ها بین فرستنده و گیرنده فراهم می کند. از سه پروتکل اصلی به نام‌های هدر احراز هویت، محفظه‌ی بار امنیتی و تبادل کلید اینترنت برای برقراری ارتباط و انتقال داده‌ها به شیوه‌ای امن استفاده می‌کند.

1) Authentication Header (AH):
این پروتکل احراز هویت گره های منبع، یکپارچگی داده ها را فراهم می کند. رمزگذاری داده ها را ارائه نمی دهد. تمام بسته های IP حاوی AH در قالب بسته بندی شده خود هستند. AH حاوی داده های هش شده، شماره دنباله، شاخص پارامتر امنیتی و غیره است.



2) Encapsulated Security Payload (ESP):
پروتکل امنیتی کپسوله شده سه سرویس عمده یعنی محرمانه بودن داده ها، یکپارچگی داده ها و احراز هویت منبع را ارائه می دهد. از الگوریتم های رمزگذاری متقارن برای تامین حریم خصوصی و امنیت داده ها استفاده می کند. فرستنده و گیرنده باید از یک الگوریتم رمزگذاری استفاده کنند.



تمامی پروتکل های امنیتی در دو حالت عملیاتی اجرا می شوند:

۱) حالت تونل:
عملیات حالت تونل به عنوان حالت کار پایان به انتها نیز نامیده می شود. یک تونل دو نقطه از VPN را در زیرساخت شبکه مشترک به هم متصل می کند. در حالت تونل، نقاط انتهایی تونل گره های مشترک VPN و زیرساخت شبکه مشترک هستند. حالت تونل امنیت داده ها را فراهم می کند. بسته داده شامل هدر IP جدید علاوه بر هدر ESP و تریلر، هدر IP اصلی، داده های رمزگذاری شده و احراز هویت ESP است. هدر IP جدید حاوی آدرس نقطه پایانی تونل است. هنگامی که بسته داده رمزگذاری شده به نقطه پایانی تونل می رسد، توسط نقطه پایانی تونل رمزگشایی می شود تا آدرس مقصد را پیدا کند. با یافتن آدرس مقصد، نقطه تونل بسته داده اصلی را در شبکه به مقصد هدایت می کند.

New IP Header	ESP Header	Original IP Header	Encrypted Data	ESP Trailer	ESP Authentication

۲) حالت حمل و نقل:
نام دیگر حالت حمل و نقل حالت عملیات میزبان به میزبان است. بسته داده شامل هدر و تریلر ESP، احراز هویت ESP، سرصفحه IP و غیره است. هدر IP رمزگذاری نشده است. از این رو امکان استشمام آدرس توسط مهاجمان وجود دارد. همچنین برای مهاجمان امکان تجزیه و تحلیل ترافیک داده وجود دارد زیرا اطلاعات هدر به راحتی در دسترس آنها است .

Original IP Header	ESP Header	TCP	Encrypted Data	ESP Trailer	ESP Authentication

3) Key Exchange and Management:
IPSec دو نوع مدیریت کلید را برای شبکه خصوصی مجازی از طریق شبکه عمومی ارائه می دهد.

۱) مدیریت کلید دستی:
در مدیریت دستی کلید، کلیدهای مخفی بین فرستنده و گیرنده قبل از برقراری ارتباط بین آنها رد و بدل می شود. مقادیر کلیدهای مخفی و ارتباطات امنیتی فقط برای فرستنده و گیرنده شناخته شده است. این نوع مدیریت کلید را می توان در یک محیط شبکه کوچک و ثابت استفاده کرد. کلیدهای مخفی بین گره های ارتباطی رد و بدل می شوند و قبل از انتقال واقعی داده ها به یکدیگر شناخته می شوند. از این رو، شبکه نمی تواند پویا و مقیاس پذیر باشد. عیب اصلی این روش این است که اگر کلیدهای مخفی توسط شخص ثالثی که می تواند مهاجم باشد دستگیر شود، هر احتمالی وجود دارد که امنیت شبکه به خطر بیفتد.

۲) مدیریت خودکار کلید:
مدیریت خودکار کلید که با نام عمومی تبادل کلید اینترنت (IKE) شناخته می شود، پروتکل پیش فرضی است که در IPSec برای تولید و مدیریت کلیدهای مخفی بین گره های ارتباطی در شبکه استفاده می شود. برخلاف مدیریت کلید دستی، شبکه ای که از این نوع مدیریت کلید استفاده می کند می تواند پویا و مقیاس پذیر باشد.

۳.۲.۳ PPTP (Point to Point Tunnel Protocol)

پروتکل Point to Point Tunneling Protocol یک پروتکل OSI لایه دو است که در بالای پروتکل نقطه به نقطه (PPP) ساخته شده است. PPTP با ایجاد یک شبکه مجازی برای هر مشتری راه دور به شبکه هدف متصل می شود. اتصال کنترل PPTP پیام کنترل و مدیریت تماس PPTP را حمل می کند که برای نگهداری تونل PPTP استفاده می شود.

IP Header	GRE Header	PPP Header	Encrypted PPP Data

۴.۲.۳ L2TP (Layer 2 Tunneling Protocol)

L2TP (Layer 2 Tunneling Protocol) در لایه پیوند داده مدل OSI عمل می کند و یک شبکه خصوصی مجازی امن (VPN) را بین دو دستگاه از طریق یک شبکه نامعتبر فراهم می کند. این کار با کپسوله کردن بسته داده اصلی در بسته دیگری و اضافه کردن هدرهای اضافی به آن کار می کند.

IP Header	UDP Header	L2TP Header	PPP Header	Encrypted PPP Data

Classical layer structure	VPNs
Application	
Presentation	
Session layer	SOCKs
Transport layer	
Network layer	IPSec, Layer 3 VPN
MAC layer	ATM, FR, Layer 2 VPN
Physical layer	OVPN, Layer 1 VPN