SSL VPN
vs
IPSec VPN

TryHackBox

TLS vs. IPsec VPN Comparison

مقایسه فنی و تحلیلی بین شبکه‌های VPN مبتنی بر SSL/TLS وIPsec

تهیه شده توسط تیم TryHackBox

The Chaos

لینک زیر جهت حمایت از جامعه آموزش رایگان :

https://daramet.com/TryHackBox

ما را به دوستانتان معرفی کنید .

دیگر کانال ها و شبکه های اجتماعی ما را دنبال کنید:

کانال های تلگرام ما

آموزش تست نفوذ و Red Team :

@TryHackBox

رودمپ های مختلف:

@TryHackBoxOfficial

داستان های هک:

@TryHackBoxStory

آموزش برنامه نویسی:

@TryCodeBox

رادیو زیروپاد (پادکست ها):

@RadioZeroPod

اینستاگرام :

http://www.instagram.com/TryHackBox

یوتیوب:

https://youtube.com/@tryhackbox

بخش اول: مقدمه‌ای بر شبکه‌های خصوصی مجازیVPN ها و اهمیت آنها

۱.۱ مقدمه کلی: شبکه‌های خصوصی مجازی به عنوان پلی امن

در جهانی که به طور فزاینده‌ای در حال اتصال است، شبکه‌های خصوصی مجازیVPN ها به عنوان ابزاری ضروری برای ایجاد یک کانال ارتباطی امن و رمزگذاری شده روی شبکه‌های عمومی غیرقابل اعتماد مانند اینترنت عمل می‌کنند. هدف اصلی این شبکه‌ها فراتر از پنهان‌سازی هویت یا تغییر موقعیت جغرافیایی است و بر محافظت از داده‌های حساس و تضمین محرمانگی و یکپارچگی آن‌ها در هنگام انتقال متمرکز شده استVPN .ها جزئی حیاتی از استراتژی‌های امنیت سایبری سازمان‌ها محسوب می‌شوند و به کارمندان—به ویژه در محیط‌های کاری دورکارامکان دسترسی امن به منابع داخلی شرکت را می‌دهند، گویی که به شبکه محلی متصل هستند. این امر به عاملی اساسی برای تضمین تداوم کسب‌وکار و انعطاف‌پذیری عملیاتی در برابر چالش‌های امنیتی رو به رشد تبدیل شده است.

۲.۱ انگیزه پشت استفاده از پروتکل‌های SSL/TLS و IPsec در VPNها

انگیزه اساسی ظهور پروتکل‌هایی مانند SSL/TLS و IPsec، ناشی از یک ضعف ذاتی در طراحی پروتکل‌های هسته‌ای اینترنت است. پروتکل اینترنت (IP) که ستون فقرات شبکه جهانی است، در ابتدا بدون اولویت دادن به رمزنگاری طراحی شده بود. این پروتکل بر مسیریابی و تحویل سریع داده‌ها متمرکز است، جایی که بسته‌های داده به صورت «شفاف» (متنی ساده) در سراسر شبکه منتقل می‌شوند.

این ضعف، داده‌ها را در برابر رهگیری، استراق سمع، دستکاری و همچنین حملات «مرد میانی» آسیب‌پذیر می‌کند، جایی که یک مهاجم می‌تواند داده‌ها را در حین انتقال بین فرستنده و گیرنده بخواند یا تغییر دهد. برای رفع این آسیب‌پذیری امنیتی اساسی، توسعه پروتکل‌های امنیتی

اضافی که داده‌ها را «کپسوله‌سازی» و رمزگذاری می‌کنند، ضروری شد تا آن را برای افراد غیرمجاز غیرقابل خواندن و دستکاری کند.

اگرچه هر دو پروتکل SSL/TLS و IPsec اهداف یکسانی را در تأمین محرمانگی، یکپارچگی و احراز هویت برای داده‌ها دنبال می‌کنند، اما لایه‌های عملیاتی متفاوت آن‌ها در مدل ارتباطی (مدل OSI) منجر به تفاوت‌هایی در عملکرد، سهولت استفاده و سناریوهای کاربردی می‌شود. درک این تفاوت اساسی در لایه‌های عملیاتی آن‌ها، کلید فهم تمایزات فنی و عملکردی این پروتکل‌ها است.

بخش دوم: توضیح عمیق در مورد VPNهای مبتنی بر پروتکل SSL/TLS

۱.۲ مبانی و اصول: تکامل SSL به TLS

VPNهای مبتنی بر SSL/TLS گسترش منطقی پروتکل‌هایی هستند که وب مدرن را امن کرده‌اند. این مسیر با پروتکل SSL (لایه سوکت‌های امن) آغاز شد که پیشگام در رمزگذاری ارتباطات بین مرورگر وب و سرور بود. با گذشت زمان، این پروتکل تکامل یافت و توسط پروتکل جدیدتر و امن‌تر TLS (امنیت لایه انتقال) جایگزین شد که در واقع امروزه در تمام ارتباطات امن اینترنتی مورد استفاده قرار می‌گیرد. با وجود این تکامل، اصطلاح "SSL" همچنان رایج است و اغلب به جای TLS استفاده می‌شود، زیرا نام آن در consciousness جمعی جامعه فناوری تثبیت شده است.

انعطاف‌پذیری VPNهای SSL/TLS در این واقعیت نهفته است که آن‌ها عمدتاً در لایه انتقال (لایه ۴) مدل OSI عمل می‌کنند، اما به طور مؤثر برای ارائه دسترسی امن در لایه کاربردی

(لایه ۷) مورد استفاده قرار می‌گیرند که به آن‌ها مزیت منحصر به فرد سهولت استفاده و سازگاری می‌بخشد. این شبکه‌ها از پروتکل‌های TLS که از قبل در تمام مرورگرهای مدرن تعبیه شده‌اند، بهره می‌برند که استقرار آن‌ها را آسان کرده و اغلب نیاز به نصب برنامه کلاینت اختصاصی توسط کاربر نهایی را مرتفع می‌سازد. این رابطه نزدیک بین پروتکل و برنامه‌های وب، ویژگی‌های متمایز کننده VPNهای SSL/TLS را تشکیل می‌دهد.

۲.۲ مکانیسم‌های فنی Handshake و رمزگذاری داده‌ها

مکانیسم عملیاتی یک VPN مبتنی بر SSL/TLS بر اساس یک فرآیند پیچیده اما کارآمد به نام "Handshake"است. این فرآیند شامل یک سری مراحل است که از طریق آن یک کانال ارتباطی امن بین کلاینت (دستگاه کاربر) و سرور درگاه VPN برقرار می‌شود. فرآیند زمانی آغاز می‌شود که کلاینت یک پیام "Client Hello"برای سرور ارسال می‌کند که حاوی اطلاعاتی درباره الگوریتم‌های رمزگذاری پشتیبانی شده است. سرور با یک پیام "Server Hello" پاسخ می‌دهد که شامل گواهی دیجیتال آن (برای اثبات هویت) و انتخاب بهترین الگوریتم رمزگذاری مشترک است.

مهم‌ترین مرحله در این فرآیند، تبادل کلید است که از یک مدل رمزگذاری ترکیبی استفاده می‌کند. در ابتدا از رمزگذاری نامتقارن برای تبادل امن یک "کلید جلسه "بین کلاینت و سرور استفاده می‌شود. رمزگذاری نامتقارن از دو کلید عمومی و خصوصی استفاده می‌کند. کلید عمومی سرور برای رمزگذاری کلید جلسه استفاده می‌شود و فقط با کلید خصوصی سرور قابل رمزگشایی است که این امر از رهگیری کلید مخفی جلوگیری می‌کند. پس از تبادل موفقیت‌آمیز کلید جلسه، اتصال به رمزگذاری متقارن تغییر می‌کند که از یک کلید یکسان برای رمزگذاری و رمزگشایی داده‌ها استفاده می‌کند. این مدل هوشمندانه، امنیت رمزگذاری نامتقارن در مرحله راه‌اندازی را با کارایی فوق‌العاده رمزگذاری متقارن در مرحله انتقال داده ترکیب می‌کند و در عین حفظ امنیت قوی، عملکرد بالایی را تضمین می‌کند.

۳.۲ مدل‌های دسترسی اصلی: پورتال و تونل

VPNهای SSL/TLS دو مدل دسترسی اصلی ارائه می‌دهند که انعطاف‌پذیری زیادی برای پاسخگویی به نیازهای کاربران و سازمان‌ها فراهم می‌کنند:

- **SSL Portal VPN** این مدل به عنوان "VPNبدون کلاینت "شناخته می‌شود زیرا به کاربران اجازه می‌دهد از طریق یک پورتال وب امن به منابع خاصی در شبکه داخلی (عمدتاً برنامه‌های تحت وب) دسترسی پیدا کنند. این مدل نیاز به نصب هیچ نرم‌افزاری روی دستگاه کاربر ندارد و آن را به گزینه‌ای بسیار convenient برای کارمندانی تبدیل می‌کند که از دستگاه‌های شخصی خود (BYOD) استفاده می‌کنند. با این حال، عملکرد آن 仅限于به دسترسی به برنامه‌های مبتنی بر وب محدود شده و ممکن است سایر انواع اتصالات را شامل نشود.

- **SSL Tunnel VPN** برخلاف مدل پورتال، این مدل requires به نصب یک برنامه کلاینت VPN روی دستگاه کاربر برای ایجاد یک تونل امن نیاز دارد. این تونل دسترسی گسترده‌تر به شبکه را فراهم می‌کند، از جمله برنامه‌های غیر وب‌بیس مانند برنامه‌های اشتراک‌گذاری فایل یا کلاینت‌های ایمیل. اگرچه مزیت "بدون کلاینت "را از دست می‌دهد، اما یک تجربه اتصال عمیق‌تر و جامع‌تر مشابه اتصال به شبکه محلی را برای کاربران فراهم می‌کند.

وجود این دو مدل به سازمان‌ها این توانایی را می‌دهد که اصل "کمترین امتیاز Least-Privilege "را اعمال کنند، جایی که کاربران فقط دسترسی دقیق و محدود به منابع مورد نیاز خود را دارند که این امر significantly سطح حمله بالقوه را کاهش می‌دهد.

بخش سوم: توضیح عمیق VPN های مبتنی بر پروتکل IPsec

۱.۳ مبانی و اصول: یک پروتکل در لایه شبکه (لایه ۳)

VPNهای مبتنی بر IPsec رویکردی کاملاً متفاوت برای ایمن‌سازی ارتباطات ارائه می‌دهند. در حالی که SSL/TLS به پروتکل‌های برنامه‌های وب متکی است، IPsecاساساً مجموعه‌ای از پروتکل‌ها است که برای ایمن‌سازی خود پروتکل اینترنت (IP) طراحی شده است. مهم‌ترین تفاوت در موقعیت عملیاتی آن نهفته است؛ IPsec در لایه شبکه (لایه ۳) مدل OSI عمل می‌کند.

این موقعیت در معماری شبکه به IPsec یک مزیت منحصر به فرد می‌دهد: توانایی ایمن‌سازی تمام بسته‌های IP بدون در نظر گرفتن منشأ برنامه‌ای آنها. به عبارت دیگر، این پروتکل "محافظت جامع "برای تمام ارتباطات در سطح شبکه ارائه می‌دهد، نه فقط برای برنامه‌های خاص مانند مرورگرهای وب. این قابلیت، IPsecرا به انتخابی ایده‌آل برای اتصال شبکه‌های مختلف (Site-to-Site) یا ارائه دسترسی کامل و جامع به یک شبکه داخلی تبدیل می‌کند. با این حال، ماهیت ریشه‌دار آن در معماری شبکه، راه‌اندازی را پیچیده‌تر می‌کند و نیاز به پیکربندی دقیق در سطح سیستم عامل و زیرساخت شبکه دارد.

۲.۳ مکانیسم‌های فنی IKE و امنیت ارتباطات (SA)

مکانیسم عملیاتی IPsec به یک فرآیند پیچیده و چندمرحله‌ای برای ایجاد یک تونل امن متکی است. برخلاف فرآیند نسبتاً ساده handshake درSSL/TLS ، IPsecنیاز به پیکربندی دقیق سیاست‌های امنیتی در هر دو انتها (کلاینت و سرور) دارد.

فرآیند برقراری اتصال IPsec در دو فاز اصلی انجام می‌شود:

- **فاز ۱:** تبادل کلید :(IKE) در این فاز، از پروتکل IKE (تبادل کلید اینترنتی) برای ایجاد یک کانال ارتباطی امن و احراز هویت دو طرف استفاده می‌شود. هدف این فاز، تبادل کلیدهای لازم برای رمزگذاری داده‌ها در فاز دوم است.

- **فاز ۲:** امنیت ارتباطات :(SA) یک "امنیت ارتباطات "نشان‌دهنده توافق یک‌طرفه بین دو نقطه پایانی درباره پارامترهای امنیتی است که برای جلسه استفاده خواهد شد، مانند الگوریتم‌های رمزگذاری، کلیدهای جلسه و تنظیمات احراز هویت. یک اتصال دوطرفه بین دو دستگاه، نیاز به SA در هر دو جهت دارد.

این پیچیدگی در راه‌اندازی، یک چالش فنی significant محسوب می‌شود، زیرا پیکربندی نادرست می‌تواند منجر به آسیب‌پذیری‌های امنیتی شود. با این حال، این پیچیدگی به administratorsکنترل بیشتری بر نحوه عملکرد تونل می‌دهد و امنیت را قوی‌تر و مقاوم‌تر در برابر تهدیدات می‌سازد.

۳.۳ پروتکل‌ها و مؤلفه‌های هسته‌ای AH و ESP

مجموعه پروتکل IPsec از چندین مؤلفه کلیدی تشکیل شده است که برای دستیابی به امنیت جامع با هم همکاری می‌کنند:

-هدر احراز هویت (Authentication Header) این پروتکل، احراز هویت مبدأ داده، یکپارچگی داده و محافظت در برابر حملات بازپخش را فراهم می‌کند. نکته مهم این که این پروتکل محرمانگی را ارائه نمی‌دهد، به این معنی که داده‌ها رمزگذاری نشده و به صورت متن آشکار ارسال می‌شوند. اگرچه این پروتکل کمتر در برنامه‌های VPN متداول است،

سناریوهایی مفید است که نیاز به تأیید منبع و یکپارچگی داده بدون نیاز به رمزگذاری آن وجود دارد.

-محموله امنیت کپسوله‌سازی (Encapsulating Security Payload)

این پروتکل پرکاربردترین پروتکل در VPN های مبتنی بر IPsec است. این پروتکل علاوه بر احراز هویت، یکپارچگی داده و محافظت در برابر حملات بازپخش، محرمانگی (رمزگذاری) نیز ارائه می‌دهد. این پروتکل داده اصلی را کپسوله‌سازی و رمزگذاری کرده و سپس یک هدر جدید اضافه می‌کند که این امر محرمانه ماندن داده را در حین انتقال تضمین می‌کند.

۳.۴ حالت‌های عملیاتی: تونل و ترابری (Tunnel and Transport)

IPsecدر دو حالت اصلی که سطوح مختلفی از حفاظت را ارائه می‌دهند، عمل می‌کند:

-حالت Tunnel: این رایج‌ترین حالت برای VPN ها است. در این حالت، کل بسته IPشامل هدر و payload رمزگذاری شده و سپس درون یک بسته IP جدید کپسوله می‌شود. این حالت برای اتصال شبکه‌ها (Site-to-Site) یا دسترسی از راه دور از طریق شبکه‌های عمومی ایده‌آل است، زیرا اطلاعات شبکه داخلی را به طور کامل از دید طرف‌های خارجی پنهان می‌کند.

-حالت Transport: در این حالت، فقط payload بسته داده رمزگذاری می‌شود، در حالی که هدر IP اصلی بدون تغییر باقی می‌ماند. این امر به روترها اجازه می‌دهد آدرس را خوانده و بسته را مسیریابی کنند. این حالت معمولاً برای ایمن‌سازی ارتباط بین دو دستگاه در یک شبکه قابل اعتماد یا داخلی یکسان استفاده می‌شود.

۵.۳ مزایا و محدودیت‌ها

مزایا:

- عملکرد بالا: به دلیل عملکرد در لایه شبکه (لایه ۳)، VPNهای مبتنی بر IPsec می‌توانند عملکرد برتر و سرعت انتقال داده بالاتری نسبت به VPNهای SSL/TLS ارائه دهند.

- امنیت جامع: IPsec حفاظت robust و جامع در سطح کل بسته‌های IP ارائه می‌دهد و امنیت تمام ارتباطات را صرف نظر از برنامه‌ای که از آن نشأت گرفته‌اند، تضمین می‌کند.

- دسترسی کامل به شبکه: این پروتکل به کاربران اجازه می‌دهد به تمام منابع شبکه داخلی همانطور که از نظر فیزیکی به شبکه محلی متصل هستند دسترسی داشته باشند که آن را برای کار دورکاری که نیاز به دسترسی به چندین برنامه دارد ایده‌آل می‌کند.

- ایده‌آل برای اتصالات Site-to-Site: IPsec انتخاب ترجیحی برای اتصال ایمن شبکه‌های دفاتر شعبه یک شرکت به یکدیگر از طریق اینترنت عمومی و ایجاد یک شبکه گسترده امن (WAN) است.

محدودیت‌ها:

- نیاز به کلاینت: IPsec نیاز به یک برنامه کلاینت اختصاصی روی هر دستگاه دارد که استقرار را پیچیده‌تر و مدیریت را سخت‌تر می‌کند.

- راه‌اندازی پیچیده: راه‌اندازی IPsec پیچیده است و نیاز به تخصص فنی عمیق دارد که احتمال خطاهای پیکربندی نادرست را افزایش داده و می‌تواند منجر به آسیب‌پذیری‌های امنیتی شود.

- چالش‌های عبور از فایروال: VPNهای مبتنی بر IPsec ممکن است در عبور از فایروال‌هایی که می‌توانند پورت‌های مورد استفاده آن‌ها را مسدود کنند، با مشکل مواجه شوند که نیاز به پیکربندی اضافی دارد.

بخش چهارم: مقایسه تحلیلی جامع و توصیه‌های راهبردی

۱.۴ مقایسه فنی مستقیم: جدول مقایسه جامع

تفاوت‌های اساسی بین VPN های SSL/TLS و VPN های IPsec را می‌توان در جدول زیر خلاصه کرد:

ویژگی	VPNهای SSL/TLS	VPNهای IPsec
لایه OSI	انتقال (لایه ۴) / کاربردی (لایه ۷)	شبکه (لایه ۳)
نیاز به کلاینت	مرورگر وب (برای حالت پورتال) یا برنامه کلاینت	همیشه نیاز به برنامه کلاینت اختصاصی دارد
نوع دسترسی	دانه‌بندی شده و محدود (برای برنامه‌های خاص)	جامع (برای کل شبکه)
سهولت راه‌اندازی	آسان و سریع	پیچیده و نیاز به تخصص فنی دارد
سازگاری	بسیار گسترده (وابسته به مرورگر)	نیاز به پیکربندی خاص برای هر دستگاه دارد
عملکرد	کندتر (به دلیل سربار رمزگذاری)	به طورکلی سریع‌تر و کارآمدتر
عبور از فایروال	عالی (عملکرد روی پورت ۴۴۳)	دشوار (ممکن است برخی پورت‌ها مسدود شوند)
موارد استفاده متداول	دسترسی از راه دور برای برنامه‌های وب، سیاست‌های BYOD	اتصالات site-to-site ، دسترسی کامل به شبکه

۲.۴ تحلیل راهبردی: انتخاب راه‌حل بهینه برای سازمان

بین VPNهای SSL/TLS و VPNهای IPsec هیچ راه‌حل «بهتری» وجود ندارد؛ بلکه یک راه‌حل «مناسب‌تر» وجود دارد که به نیازهای خاص سازمان بستگی دارد. این انتخاب یک تصمیم راهبردی است که باید بر اساس درک عمیقی از موارد استفاده مورد نیاز صورت گیرد.

چه زمانی از VPN SSL/TLS استفاده کنیم؟

این گزینه ایده‌آل برای سازمان‌هایی است که بر انعطاف‌پذیری و سهولت استفاده تمرکز دارند. در موارد زیر ترجیح داده می‌شود:

- دسترسی از راه دور انعطاف‌پذیر: برای کارمندان و پیمانکارانی که نیاز به دسترسی به برنامه‌های خاص از دستگاه‌های شخصی مختلف (BYOD) دارند بدون نیاز به نصب نرم‌افزارهای پیچیده.

- کنترل دسترسی دانه‌بندی شده: هنگامی که نیاز به اعمال اصل کمترین امتیاز وجود دارد و کاربران فقط دسترسی دقیق و محدود به منابع مورد نیاز خود را دارند که به طور مؤثر سطح حمله را کاهش می‌دهد.

- محیط‌های کاری نیازمند عبور از فایروال: هنگامی که دسترسی از شبکه‌های محدود شده مانند کافی‌شاپ‌ها یا هتل‌ها انجام می‌شود، جایی که گاهی اوقات تنها پورت 443 باز است.

چه زمانی از VPN IPsec استفاده کنیم؟

این گزینه بهینه برای سازمان‌هایی است که عملکرد و دسترسی جامع را در اولویت قرار می‌دهند. در موارد زیر ترجیح داده می‌شود:

- اتصالات Site-to-Site: برای اتصال ایمن شبکه‌های دفاتر شعبه یک شرکت از طریق اینترنت عمومی و ایجاد یک شبکه گسترده خصوصی (WAN).

- عملکرد بالا: برای محیط‌هایی که نیاز انتقال مقادیر زیادی داده یا وظایفی که لازمه تاخیر کم هستند، مانند انتقال فایل‌های بزرگ یا اتصال به سرورهای پایگاه داده.

- دسترسی کامل به شبکه: هنگامی که کاربران نیاز دسترسی به تمام منابع و برنامه‌های شبکه داخلی، نه فقط برنامه‌های مبتنی بر وب.

۳.۴ نتیجه‌گیری و توصیه‌های نهایی

در نتیجه، تحلیل دقیق نشان می‌دهد که VPNهای SSL/TLS و IPsec راه‌حل‌های رقیبی نیستند، بلکه فناوری‌های مکملی هستند که هریک در سناریوهای مختلف کار می‌کنند. تفاوت اصلی بین آنها در لایه‌ای است که هریک فناوری در آن عمل می‌کند، که بر ویژگی‌های اصلی آن از نظر عملکرد، دسترسی و سهولت استقرار تأثیر می‌گذارد.

قبل از تصمیم‌گیری در مورد مناسب‌ترین فناوری، بسیار توصیه می‌شود که سازمان‌ها ارزیابی جامعی از نیازهای خاص خود انجام دهند. عوامل زیر باید در نظر گرفته شوند:

1. حوزه دسترسی مورد نیاز: آیا کاربران نیاز دسترسی کامل به شبکه یا دسترسی محدود به برنامه‌های خاص دارند؟
2. دستگاه‌های مورد استفاده: آیا سازمان به سیاست BYOD یا دستگاه‌های استاندارد شده متکی است؟
3. عملکرد مورد نیاز: آیا اولویت با سرعت انتقال داده یا سهولت استفاده است؟
4. تخصص فنی: آیا تیم فناوری اطلاعات دارای تخصص لازم برای مدیریت پیکربندی‌های پیچیده IPsec است؟
5. بودجه: آیا هزینه مجوزهای نرم‌افزار کلاینت اختصاصی با بودجه سازگار است؟

در بسیاری از موارد، سازمان‌ها می‌توانند از استفاده همزمان از هر دو فناوری در راه‌حل‌های ترکیبی بهره‌مند شوند. به عنوان مثال، از یک VPN IPsec برای اتصال شعب اصلی به یکدیگر (Site-to-Site) استفاده می‌شود، درحالی که از یک VPN SSL/TLS برای اعطای دسترسی امن و محدود به کارمندان دورکار به برنامه‌های وب داخلی استفاده می‌شود. این رویکرد قدرت IPsec در زیرساخت را با سهولت SSL/TLS برای کاربر نهایی ادغام می‌کند.

با تکامل مستمر landscape امنیت سایبری، راه‌حل‌های جدیدی در حال ظهور هستند، مانند SASE (Secure Access Service Edge) ، که شبکه و امنیت را در یک سرویس ابری واحد integrates می‌کند. این راه‌حل‌ها ممکن است در آینده یک جایگزین جامع‌تر ارائه دهند، که تأکید می‌کند استراتژی‌های امنیتی باید پویا باشند و با آخرین تحولات فناوری سازگار کنند.