نویسنده

زهرا مرشدی

۲۲ | ۰ | ۷ | ۷۳

وقتی باختم مسیر را یافتم.راهی جز موفقیت ندارم پس راهی میشوم.



# VPN چگونه امن می شود؟ بررسی امنیت در شبکه های VPN

۲۴۹۲ | ۵ | ۱۶

در این مقـاله و در ادامه مقـاله قبلیم که در خصوص معرفی شـبکه هـای خصوص مجـازی یا [illegible] راجع به امنیت در این نوع شـبکه های صـحبت کنم ، شاید اکثر شما دوستان فکر کنید که VPN که خودش برای امنیت ساخته شـده ، مگه خودش ایمن نیست ؟ جوابش رو در این مثاله بهتون می دم ، هر سیستم امنیتی برحسب نوع پارامترهای امنیتی که در داخلش استفاده شده ممکن هست که مورد هجوم و در نهایت بهش نفوذ بشه و VPN هم از این قضیه خارج نیست .

VPN هم برای خودش تنظیمات ویژه امنیتی داره که میتونه توانایی های حفظ محرمانگی و امنیت اطلاعات ما رو بالا ببره و کمتر بشه بهش نفوذ کرد .باید باور کنیم که این شـبکه هم مثل شبکه های دیگه قابل نفود هست و ما تنها کاری که میتونیم انجام بدیم این هست که تا جای ممکن امنیتش رو بالا ببریم . در ادامه مطلب روش هایی رو که ما میتونیم از طریق اونها این شبکه رو ایمن سازی کنیم و تا حد زیادی امنیت اطلاعاتمون رو بالا ببریم رو عنوان میکنیم ، روش های اصلی به شکل زیر هستند :

## فایروال ، دیوراه آتش یا Firewall

همونطور که از اسـمش مشـخص به معنی دیواره آتش.آتشـی که جنبه ی محافظت داره و مانع نفوذ غیرمجاز میشه.وقتی تعـداد سیسـتم های متصل به شـبکه خصوصـی زیاد میشه،به طبع محافظت از منابع سیستم هم مشکل میشه.firewall یک دیوار امنیتی بین شـبکه ی اختصاصی و اینترنت ایجاد میکنه و با محدود کردن دسترسی افراد خارجی به سیستم امکان حمله به سیستم رو کم میکنه.همچنین دسترسی از داخل به خارج شبکه رو هم میتونیم با اون محدود کنیم،مثلا بعضی پورت ها رو ببندیم.دیوار آتش هم میتونه نرم افزاری بـاشه هم سـخت افزاری. اگر دوست داشتین تو همین وب سایت تفاوت فایروال نرم افزاری و سـخت افزاری رو می تونین مطالعه کنید.این هم لینک مطلبش :

- تفاوت فایروال نرم افزاری و سخت افزاری

## Fire wall برای جلوگیری از حملاتی مثل:

۱. دسترسی غیرمجاز به منابع شبکه یا Unauthorized Access (که با نفوذ مداخله گر از طریق رایانه اتفاق می افته)
۲. عدم سرویس دهی و تقاضای بیش از حد سرویس ها یا DOS Attack(طوری که سرویس دهی به بقیه غیرممکن بشه)
۳. نقاب زدن یا Spoofing (جا زدن به جای یک فرد دیگه،مثلا تغییر آدرس فرستنده ی پست الکترونیکی)

## از راهکارهایی مثل:

۱. محدود کردن دسترسی
۲. جلوگیری از استفاده ی بعضی سرویس ها
۳. و ارتباط بین بعضی سیستمها، استفاده میکنه

## رمزنگاری (encryption)

رمزنگـاری فرآینـد حفظ امنیت داده هاست،کامپیوتر مبـداء داده ها یا بسـته رو رمزگـذاری میکنه و به سـمت مقصـد میفرسـته و کامپیوتری که مجاز به رمزگشایی هست وقتی بسته رو دریافت کرد اون رو رمزگشایی میکنه.دو نوع رمزنگاری داریم:

۱. رمزنگاری کلید متقارن (secret +key )
۲. رمزنگاری کلید عمومی (public +key )

توی رمزنکاری متقارن هر کدوم از کامپیوترها یک کلید(کد) دارن که برای رمزکذاری بسته ی اطلاعاتی از اون استفاده میکنن.کلید رمزگذاری بین فرستنده و گیرنده مشترک،فرستنده با استفاده از کلیدی که داره متن اصلی رو با الگوریتم مشخصی رمز و ارسال میکنه و گیرنده با الگوریتم رمزگشایی که عکس عمل رمزنگاری هست،داده ی دریافتی رو رمزگشایی میکنه به شرطی که با الگوریتم رمزگشایی آشنایی داشته باشه.اگه پیام یا بسته به دست نفوذگرها بیفته به دلیل اینکه از کلید آگاهی ندارن نمی تونن اون رو رمزگشایی کنن.

توی رمزنگاری کلید عمومی هر کاربر یک زوج کلید(کلیدخصوصی و کلیدعمومی) داره.کلید خصوصی برای کامپیوتر ارسال کننده قابل شناسایی و استفاده ست و کلید عمومی هر فرد به بقیه ارسال میشه یا توی یک جای عمومی ذخیره میشه تا کاربرهای دیگه بتونن از اون استفاده کنن.تو این روش هر کاربری که بخواد پیامی برای شخص دیگه ارسال کنه با کلید عمومی شخص گیرنده،پیام موردنظر رو ارسال میکنه و این پیام تنها به وسیله ی کلید خصوصی به کار رفته توی رمزنگاری،قابل رمزگشایی هست.

## AAA (Authentication Authorization Accounting) چیست؟

این سه کار در واقع سه نوع سرویس هستند که معمولا هم بصورت نرم افزاری و هم بصورت سخت افزاری انجام میشن . به این سه تا در اصطلاح AAA یا تریپل A هم گفته میشه ، معمولا وقتی سه تا حرف کنار هم در انگلیسی میاد اینطوری خونده می شه مثلا IEEE خونده میشه آی تریپل E . بهر حال ما بحثمون چیز دیگه ای هست . این سروس ها برای حفظ امنیت در دسترسی های از راه دور استفاده می شن .وقتی به کاربری نام کاربری و رمز عبور میدین و یک Connection برای VPN به محض برقراری اتصال اول درخواستش به این سرویس منتقل می شه . بعد به شکل زیر هر کدوم از این A ها کار خودشون رو انجام میدن :

۱. شما چه کسی هستید؟(Authentication)
۲. شما مجاز به انجام چه کاری هستید؟(Authorization)
۳. چه کارهایی رو انجام داده اید؟(Accounting)

با این فرآیند بعد از مشخص شدن هویت کاربر،یجورایی برای کاربر مجاز محدوده ی استفاده رو مشخص کنه.

## IPSEC(Internet Protocol Security) چیست؟

یکی از راه های ایجاد امنیت،به وجود آوردن امنیت در سطح IP هست.پروتکل IPSEC هم یکی از امکانات موجود برای برای ایجاد امنیت و ارسال اطلاعات در سطح پروتکل IP هست . بسته ها در شبکه ی LAN به صورت معمولی منتقل میشن،یعنی هر بسته یک بدنه ی IP و یکheader یا Header IP داره.ولی وقتی اون بسته میخواد از شبکه ی LAN به یک شبکه ی دیگه منتقل بشه,بسته ها تغییر میکنن و به اونا Header IP SEC اضافه میشه.IP SEC شامل دوتا Sub protocol هست که برای امن کردن بسته ها توی شبکه ی vpn به کار میره.

## ESP (Encapsulated security payload) چیست؟

برای محرمانگی محتوای پیام و به صورت محدود برای محرمانگی جریان ترافیک استفاده میشه، کار ESP اینه که Payload بسته ای رو که در حال انتقال هست رو به وسیله ی کلید متقارن رمزگذاری کنه.

## AH (Authentication header) چیست؟

سرآیه ی احراز اصالت AH برای حفظ تمامیت و احراز اصالت بسته های IP استفاده میشه.برای پنهان کردن اطلاعات بسته ها مثل(هویت ارسال کننده ها) قبل از اینکه به مقصد برسن رویheader بسته به کار میره تا امنیتش رو حفظ کنه.

## IP SEC میتونه داده های بین دستگاه های مختلف مثل:

۱. Router به Router
۲. Router به Firewall
۳. Router به Desktop
۴. Desktop به Server

رو رمز نگاری کنه.

## SSL(Secure Socket Layer) چیست؟

لایه ی سوکت امن اجازه میده که بین کاربر و سرور یک نشست ایجاد بشه و از این طریق هر تعداد اتصال امن امکانپذیر میشه.در واقع مجموعه ای از پارامترهای امنیتی رو تعریف میکنه،که به صورت اشتراکی توی اتصالات مربوط به این جلسه استفاده میشن.از نظر تئوری بین کاربر و سرور میتونه بیشتر از یک نشست وجود داشته باشه ولی در عمل فقط یک جلسه به وجود میاد.

نویسنده : زهرا مرشدی

منبع : جزیره امنیت اطلاعات و ارتباطات وب سایت توسینسو



### ۵ نظر

محمد نصیری ۸۹ ماه قبل

ممنونم مقالتون بسیار خوب و عالی بود فقط جند نکته برام ابهام پیش اومده :

۱. تفاوت رمزنگاری با رمزگذاری در چی هست ؟
۲. در رمزنگاری کلید متقارن یا Symmetric Algorithms Encryption فرمودید که این کلید رو قبلا به اشتراک میگذارند ، البته در مورد کلید نامتقارن هم همینطور بود ، اما میخام بدوم این کلید چطور منتقل میشه ؟ خوب شما هرچقدر هم امنیت اکلوریتمتون بالا باشه اما این کلید اصلیه لو بره اطلاعات ما هم لو میره ، آیا تمهیدات امنیتی خاصی برای انتقال این کلیدها وجود داره ؟

ممنونم از راهنماییتون.

پسندها (۲)

فاطمه قرباوی ۸۹ ماه قبل

سلام .. ممنون از مقاله ی خوبت :)

یه سوال داشتم : میشه در مورد payload بسته ها یه توضیحی بدی ؟

موفق باشی

پسندها (۲)

زهرا مرشدی ۸۹ ماه قبل

سلام.متشکرم از نظرات و سوالاتتون که باعث میشه مطلب برای همه مون بهتر جا بیفته.

۱.رمزنگاری (cryptography)علم مطالعه درباره ی مهارت های پنهان نویسی پیام و رمزگذاری سیستم هاست و به طورکلی منجر به تغییرشکل اصل اطلاعات به صورت اطلاعات رمزشده میشه،اما رمزگذاری(encryption)،تکنیک ها یا الگوریتم های ست که برای پنهان سازی اطلاعات متن اصلی یا رمز کردن اون ها به کار میره.

۲.برای مبادله ی کلید اگر فرض بشه کاربران قبلا کلید مشترکی داشتن،کلید جدید میتونه به وسیله ی کلید مشترک رمز و ارسال بشه و در غیر اینصورت مبادله ی کلید به صورت فیزیکی انجام میشه.برای توزیع کلید بین کاربران فرض میکنیم گره ی مطمئنی مثل c توی شبکه وجود داره و میتونیم کلید ارتباطی بین کاربرها رو به وسیله ی این گره تولید کنیم و مثلا هر گره مثل A یک کلید اصلی با گره C به اشتراک میذاره .حرف شما کاملا درسته, ارسال کلید یک نقطه ضعف امنیتی به حساب میاد،اما روش

هایی برای حفاظت وجود داره. توی رمزگذاری ها برای حفظ امنیت کلید،یکی از راه ها اینه که مسیر انتقال پیام رمز میشه و از اون جایی که توی رمزگذاری لازمه که کلید رو فقط فرستنده و گیرنده بدونه پس کلید از طریق کانال امن ارسال میشه.روش دیگه اینه که اغلب برای تبادل کلیدها الگوریتم های متفاوتی از الگوریتمهای رمزکردن پیام ها استفاده میشه.مفهوم (key domain)برای محدود کردن میدان کلیدها ومحافظت از کلیدها استفاده میشه.دامنه یک سیستم کامپیوتری هست که می تونه به صورت فیزیکی و منطقی محافظت بشه.کلیدهای استفاده شده توی یک دامنه به وسیله ی یک کلید رمزکننده ی کلید محلی ذخیره میشن.وقتی این کلیدها میخوان به یک کامپیوتر دیگه فرستاده بشن،رمزگشایی میشن و تحت یک کلید جدید رمز میشن که اغلب به عنوان کلید کنترل ناحیه(zone control key)شناخته میشن،با دریافت این کلیدها در طرف دیگه تحت کلید محلی سیستم جدید رمز میشن.روش دیگه استفاده از اجازه دهنده ی گواهینامه ی دیجیتال،که به عنوان واسطی عمل میکنه که هردو رایانه به اون اعتماد دارن،این واسط مشخص میکنه که آیا هرکدوم از رایانه های مبدا یا مقصد همونی هست که باید باشه یا خیر،بعد از اون امکان استفاده ی کلید عمومی هر یک از کامپیوترها رو برای رایانه های مجاز فراهم میکنه.

امیدوارم که ابهامتون رفع شده باشه.

پسندها (۲)

زهرا مرشدی ۸۹ ماه قبل

سلام.مرسی ، payloadبسته همون اطلاعات خام بسته ست،محتوای بسته بدون اینکه بخوایمheaderها رو درنظر بگیریم.درواقع همون بار بسته اطلاعاتی که بعدا کپسوله میشه و منتقل میشه.

پسندها (۴)

محمد نصیری ۸۹ ماه قبل

البته من هم چند مرد رو جستجو کردم و برخی مسائل رو به این صورت بیشتر متوجه شدم :

۱. رمزنگاری یعنی داده ها رو رمز کنیم ، کل داده رمز میشه و غیر قابل فهم ، رمزگذاری مثل یک فایل میمونه که براش رمز عبور گذاشتیم ، شما در این حالت اطلاعاتتون رو رمز نگاری نمیکنید فقط یک رمز عبور براش تعریف کردید و داده های شما شکل اولیه خودشون رو دارند .
۲. برای مبادله کلید کاملا درست می فرمایید ، ما در بسیار مواقع از طریق تلفن ، پیامک و ایمیل این رمز ها رو اگر بصورت متقارن یا نا متقارن باشند انتقال می دیم ، برای انتقال کلیدها در الگوریتم های نامتقارن از الگوریتم هایی استفاده می کنیم که کارشون انتقال کلید هست ، مثلا الگوریتمی به نام الگامال El-Gammal برای انتقال کلید های PKI وجود داره .

موفق باشید

پسندها (۱)

## نظر شما

برای ارسال نظر باید وارد شوید.

## از سرتاسر توسینسو