موضوع : **VPN**

ترجمه :

لیلی نادری – فرزانه نوری

استاد:

جناب آقای مهندس فیروزبخت

منبع : اینترنت

تکنولوژی VPN

۱- تعاریف

این گزارش رسمی تکنولوژی‌های اصلی را برای شبکه‌های خصوصی مجازی راشرح بدهد،که امروزه دراینترنت کاربرد دارند. تجارت (NPV) درعرض ۱۰ سال چنان تغییر می یابد که رشدآن مانند اینترنت بوده است.ومثل کمپانی‌های به طور وسیع جهت ارتباطات بیشتر روی اینترنت تکیه میکنند. محصولات وتصورات (NPV) پیشنهاد میشود به وسیله پهنه وسیعی از فروشنده‌ها که جهت تکامل آن می کوشند.(NPV) سیستمی است که این مسائل را پیشنهاد میکند. توضیحات وتعاریف دراین گزارش رسمی به مشتریان درفهم بهتر (NPV) و رهایی ازسردرگمی کمك بسیار بزرگی میکند و به همین اندازة به فروشنده‌ها در شرح دادن پیشنهادهایی جهت استفاده بهتراز آنها کمك بکند.

۲- ملزومات

یك شبکه‌ای خصوصی مجازی((NPV)) یك شبکة داده‌ای خصوصی که است اززیرساختار مخابرات تلفنی دورعمومی استفاده می‌کند،نگهداری کننده خطوط بوسیله قراردادها و رویه‌های امنیتی.

یك شبکه‌ای خصوصی مجازی است که می تواند مقایسه شود با خطوط یك سیستم شخصی یا اجاره ای که می تواند فقط بوسیله یك کمپانی استفاده شود. هدف اصلی یك (NPV) این است که به کمپانی همان توانایی‌های خطوط اجاره‌ای خصوصی با قیمت خیلی پایین‌تربااستفاده کردن زیرساختارعمومی اشتراکی را بدهد.

تلفن کمپانی‌ها منابع اشتراکی خصوصی جهت پیغامهای صوتی برای بیش ازیك پیغام را فراهم می کند. یك شبکه‌ای خصوصی مجازی امکان حفاظت ازاشتراك منابع عمومی برای داده‌ها را فراهم می کند.

امروزکمپانی‌ها به دنبال استفاده ازیك شبکه‌ای مجازی خصوصی برای عریض کردن و گستردن شبکه های اینترانت می باشند.

این متن سه تکنولوژی مهم(vpn)راشرح می‌دهد:

- مطمئن (VPNs)
- محفوظ (VPNs)
- دورگه (VPNs)

این مهم است جهت یادداشت برداری ازvpn محفوظ (sNPV) و مطمئن است که مربوط به امورغیرفنی و آیا اینکه آیا آنها می توانن دریك بسته واحد موجود باشند؟

تقریباً پیش ازآنکه اینترنت به صورت جامع وعمومی شود یك شبکه‌ای خصوصی مجازی ازیك یا چند مدارکه ازتولید کننده های ارتباطات اجاره می شداستفاده می گردید.هرمدار اجاره‌ای شبیه یك تك‌سیم در یك شبکه که به وسیله مشتری کنترل می‌شد رفتار می کرد.

فروشندة ارتباطات بعضی وقت‌ها به مدیریت شبکه مشتریان کمك میکند اما ایدة اساسی که یك مشتری می‌توانست استفاده بکند این است که مدارات را به همان شکل اجاره دهند که آنها سیمهای فیزیکی را در شبکة محلی‌شان استفاده کنند.

حاصل پوشیدگی توسط (sNPV)میرا فقط این بود که ارتباطات مطمئن مشتری را فراهم کند که درغیراین صورت هیچ کس دیگرنمی توانست از این مدارات استفاده بکند.

این اجازه را می داد که مشتریان خود را ملزوم به داشتن آدرس IP وسیاستهای امنیتی جهت رویه‌هایشان بکنند. یك مداراجاره‌ای ازآغازتا پایان یك یا بیش ازچند گزینه ارتباطی را اجرا می کرد.

vpn مشتری مطمئن ، تهیه کننده ای است که به درستی از مدارات مجتمع نگهداری می کند وجهت استفاده بهترازشبکه معاملات بازرگانی وجلوگیری ازترافیك شبکه ازتجسس و جاسوسی بی مورد جلوگیری می کند.

بطوریکه اینترنت بیشترملی ومردمی شده است بطوریکه محیط هماهنگ ویکپارچه ای جهت ارتباطات پدیدآورده است. امنیت خیلی بیشترازیك موضوع دیگرهم به مشتری وهم تهیه کننده فشارمی آورد.

دیدی که VPNs مطمئن پیشنهاد می کندامنیت واقعی نیست ، فروشنده شروع به خلق پروتکل هایی می کند که اجازه دهد اطلاعات در بخش آغازین شبکه و یا در یك کامپیوتر به کد درآید وآن را مانند سایر داده ها دراینترنت انتقال دهد و سپس آنها پس از رسیدن به مقصد از حالت رمزو کد خارج کرده و به صورت اولیه درآورد.

عمل عبور و مرور رمزها مانند یك تونل که بین دو شبکه است می باشد:

حتی اگر یك حمله عبور و مرور اطلاعات رخ دهد آنها می توانند آن را بخوانند و نمی توانند شلوغی عبور و مرور را تغییر دهند . بدون تغییر که مشاهده شود بوسیله دریافت بخشی و بنابراین رد کرد ن انها شبکه هایی ایجاد می شوند که بصورت پنهانی استفاده می شوند این شبکه ها VPNs نامیده میشود.

اخیرا تولیدکننده های سرویس شروع به پیشنهاد دادن یك نوع جدید از VPNs مورد اعتماد کرده است. دراین مرتبه استفاده کننده اینترنت به جای سیستم تلفن خام به عنوان زیربنایی برای ارتباطات استفاده می شد.

این VPNs مطمئن جدید هنوز امنیتی را پیشنهاد نکرده اند اما به آسانی آنها به مشتریان یك راه بدهندکه قطعه‌های شبکه‌ای را برای مساحت عریض شبکه‌ها به وجود می‌آورند((sNAW).)

به علاوه،VPN مطمئن قطعه‌هایی است که می‌توانند از یك مکان کنترل‌شوندواغلب با ضمانت کردن کیفیت سرویس گارانتی از-خدمات((SoQ)) تهیه‌کننده استفاده کنند.

یك VPNمحفوظ می تواند به عنوان بخشی از VPN مطمئن اجرا شود (خالق یك سوم نوع VPN که در تجارت دورگه VPN خیلی جدید است.

برخی اوقات یك vpn دورگه به طور کامل بوسیله یكvpn محفوظ محافظت میشود، اما معمولا فقط یك بخش از آن محافظت می شود.

۳. کاربرد سناریوها برای محفوظ (VPNs) و به (VPNs) مطمئن

دلیل اصلی آنکه کمپانی‌ها از vpn محفوظ استفاده میکند همین است برای اینکه آنها اطلاعات حساس را روی اینترنت بدون نگرانی اینکه کسی آنها را ببیند روی اینترنت منتقل کنند. هر چیزی که روی یك vpn محفوظ قرار دارد در یك سطح دسترسی میباشد و حتی اگر کسی یك نسخه‌از این اطلاعات را ضبط کند، بازهم این اطلاعات قابل خواندن نمی باشند حتی اگر آنهااز ارزش صدها میلیون دلاری ازکامپیوترها استفاده کنند.

به علاوه، استفاده‌از یك vpn محفوظ به کمپانی این اجازه را میدهدکه یك حمله‌کننده به اطلاعات را شناسایی کند و او نمی تواند محتویات این اطلاعات را تغییر بدهد.

کمپانی هایی که از vpns مطمئن استفاده می کنند نیز به همین ترتیت می باشندزیرا آنها می خواهند که بدانند که داده های آنها روی یك مسیر مشخص شده منتقل می شوندکه

خصوصیات مخصوص به خود را دارند و توسط یك ISP یا یك کنفدراسیون مطمئن (isps) کنترل می شوند.

این به مشتری اجازه می‌دهدکه از IP خصوصی خودشان استفاده کنند و محتملاً به مسیرمخصوص به خودشان دسترسی داشته باشند.

این راهها بر اساس توافق مشتری می باشد اما نمی توان به برخی افراد مانند هکرها اعتماد داشت ، زیرا آنها به این خطوط دسترسی می یابند و اطلاعات را تغییر می دهند.

برای یك مشتری تقریبا غیر ممکن است که بتواند تمام راههای ورود به اطلاعات را شناسایی کندو بنا براین باید به تهیه‌کنندهشان اعتماد بکنند.

واضح است که vpns محفوظ و vpns مطمئن دارای ویژگیهای متفاوتی هستند.

vpns محفوظ امنیت را فراهم میکند اما هیچ اطمینانی به راه‌ها نیست.

vpns مطمئن امکان اطمینان ازراههای انتقال اطلاعات را فراهم می‌کند مانندQOs اما بازهم هیچ امنیتی از فضولی کردن و یا تجسس در اطلاعات نیست.

به دلیل این نقاط ضعف و قدرت ،vpns دورگه ایجاد شد اگرچه که به نظرمیرسند که این سناریوها هنوز به مطلوبیت خود نرسیده و جای تکامل دارد.

یك نمونة بارزازاین وضعیت برای (vpn) دورگه زمانی است که یك کمپانیvpn مطمئن رادرمحل دارد وهمچنین بخشهایی ازاین کمپانی به امنیت روی بخش دیگر vpn احتیاج دارند.

٤. ملزومات برای(vpn)

یك ازملزومات مهم که معمولا برای vpns محفوظ ،vpns مطمئن و vpns دورگه وجود دارد این است که آیا مدیرvpn باید نوع آن را بشناسد علیرغم استفاده ازاین نوع vpn یك vpn باید تواناییهایی را داشته باشد که یك شبکه معمولی آنها را ندارد.بنابراین یك مدیر vpn در هر زمان باید بدند که از کدام نوع vpn باید استفاده کند.

هریك ازاین چهار نوع vpns ملزومات مربوط به خودشان را دارند.

- ٤/١ ملزومات vpn محفوظ

همه عبور و مرور نقل و انتقال روی vpn محفوض باید به صورت رمز شده و درستی آن تصدیق شود.خیلی از پروتکلها جهت استفاده برای خلق vpns محفوظ استفاده میشوند که تصحیح در آنها بدون رمزسازی صورت میگیرد.

اگرچه یك چنین شبکه‌ای بیشتر محفوظ است نسبت به یك شبکه بدون سندیت و درستی اما یك vpnنیست چون هیچ سطحی از پوشیدگی و امنیت در آن نیست.

ویژگیهای امنیت در vpn باید توسط بخشهایی از vpn موافقت شود.vpns محفوظ یك یا بیش از یك تونل دارد و هر تونل دو انتها دارد.

مدیران دو انتها از هر تونل باید در امنیت دارایی‌های تونل توانایی داشته باشند.

هیچ کس در خارج از vpn نمی تواند روی آن موثر باشد.

- ٤/٢ملزوماتvpn مطمئن

هیچ کس به غیر از تولید کننده vpn نمی تواند روی ایجاد آن ویا ویرایش آن موثر باشد.

ارزش کاملvpn مطمئن آن است که مشتری می‌تواند اعتماد بکند وتهیه‌کننده میتواند آن را نظارت و کنترل کند.بنابراین هیچ کس خارج از قلمرو vpn نمی تواند آن را تغییر دهد. یادداشت آن مقداری (sNPV) فاصله بیش از یك تهیه‌کننده؛ در این موضوع، مشتری به گروه تهیه‌کننده‌ها اعتماد می‌کند مثل اینکه آنها یك تهیه‌کننده تك بودند.

هیچ کس به غیر از تهیه‌کنندهvpn مطمئن نمی تواند داده‌ها را تغییربدهد، داده‌ها را وارد بکند یا داده‌ها را در یك مسیر مشخصvpn حذف می‌کند.

یك vpn مطمئن بیش از یك راه است : بنابراین داده ها در چندین مسیر جریان دارند. اگرچه به طور نمونه راه‌ها میان خیلی از مشتریهای یك تهیه‌کننده اشتراکی هستند،اما مسیر هر مشتری باید خاص خودش باشد و هیچ کس نتواند روی داده های آن موثر باشد.

آیا مسیریابی و مخاطب قرار دادن به کاررفته دریك (NPV) مطمئن باید قبل ازتحقق یك (NPV) به وجودآمده باشد؟

مشتری باید بداند که چه اندازه باید منتظر مشتری و چه اندازه باید منتظر خدمت تهیه کننده باشد بنابراین باید برای نگهداری از شبکه خریداری شده برنامه ریزی کنند.

- ٤/٣ملزومات دورگه ها

مرزهای vpn محفوظ وvpn مطمئن باید کاملا مشخص و روشن و واضح باشد.

در یك (vpn) دورگه،vpn محفوظ یك زیرمجموعه ازvpn مطمئن می باشد ، از قبیل اگر یك قسمت در یك شرکت محفوظ خودش را اجراء بکند باید به متحد کردن آن اعتماد کرد.

برای هر نشانی معین در یك (vpn) دورگه، مدیر(vpn) بایداین توانایی را داشته باشد که در نهایت بله یا خیرگوید حمل ونقل بین آن دو نشانی بخشی ازvpn محفوظ هستند.

٥. تکنولوژی هایی که توسط vpnc پشتیبانی می شوند:

- ٥/١تکنولوژی vpn محفوظ

Ipsec با رمزی‌سازی درهرتونل ویا سبك انتقال.امنیت انجمن‌ها می تواند به صورت دستی و یا با استفاده کردن از گواهی‌نامه‌های محرمانه . Ipsec در خیلی از RFC ها شرح داده می شود وشامل ۲٤۰۱، ۲٤۰٦، ۲٤۰۷، ۲٤۰۸ و ۲٤۰۹می باشد.

cesPI درون L2TPپردازش از دور(به عنوان شرحRFC ۳۱۹۳) آیا در دسترسی و دستیابی به سرور و کلاینت تفاوتی وجود دارد.

هردوی این تکنولوژی‌ها در (IETF) استاندارد شده‌اند وبسیاری از مشتریان محصولات خود را در این زمینه به خوبی به نمایش می گذارند.

- ۲/٥تکنولوژی vpn مطمئن

تهیه کننده های سرویسهای جدید انواع متفاوتی از این نوع را پیشنهاد می کنند.اینها عموما به لایه ۲ و لایه ۳ جدا میشوند.

✓ **تکنولوژی لایه دوم شامل:**

دستگاه بانك اتوماتیك مدارات

رله قاب مدارات که فریم لایه دوم را روی Mplsانتقال می دهد.به عنوان توضیح این مورد پیش نویس draft-martini-I2circuittrans-mplsمطرح میشود.

✓ **تکنولوژی لایه سوم شامل:**

Mpls با در فشار گذاشتن اطلاعات از میان (BGP)، .به عنوان توضیح این مورد پیش نویسdraft-ietf-ppvpn-rfc2547bi s مطرح میشود.

هیچیك ازمبانی تکنولوژی Mpls درIETF استاندارد نشده اند اما درآینده هردو استانداردها خواهد شد.

همچنین، صنعت وابسته به خدمات تهیه‌کننده یکی از این تکنولوژی‌ها را بیشتر از دیگری در بر نگرفته است.

- ۳/۵تکنولوژی vpn دورگه

هراجرای vpn محفوظ پس از پشتیبانی تکنولوژی vpn مطمئن پشتیبانی میشود. مهم این امر جهت یادداشت مهم است که ه یك (vpn) دورگه فقط محفوظ است در بخشهایی که مبنی بر vpn محفوظ است.

یعنی، اضافه کردنvpn محفوظ به یكvpn مطمئن موجب افزایش اطمینان امنیتی در سایر بخشها نمی شود و فقط روی قسمت مورد نظر موثر است.

vpnمحفوظ مزیتهایی بر vpn مطمئن دارد از جمله شناسایی QOS.

6. درباره vpnc :

انجمن تجارت بین المللvpn جهت تهیه کنندگان vpn میباشد. مقصودهای اولیه ما:

محصولات اعضای آنرا به مطبوعات ترویج بدهید و به عامل بالقوه مشتریان توانایی استفادة مفید بین اعضا با نشان دادن به محصولات جایی که مثل میدان عمومی رم قدیم برای (vpn) سازندهها سرتاسر جهان مطبوعات و عامل بالقوه مشتریان را تکنولوژیها بفهمد و استانداردها از توانایی و شهرت استفادة مفید پشتیبانی میکنند اتفاقات آزمایش شده آن باید یادداشتشده باشندو جریان استانداردها رادر آینده پشتیبانی بکند.

VPN PROTOCOLS

پروتکل VPN واژه ای است که در سالهای اخیر معانی متفاوتی دارد VPN یک گزارش رسمی در باره تکنولوژی VPN را دارد که خیلی از واژه هایی که درتجارتVPN استفاده می شود را شرح می دهدوتوصیف می کند .

د راین خصوص میان VPNS محفوظ و VPNS مورد اعتماد کامپیوتر تفاوت وجود دارد .

تکنولوژی VPNS محفوظ بگونه ای است که دو حالت زیر را پشتیانی می کند :

۱- رمز سازی IP در ثانیه

۲- L2TP از درون پروتکل های VPNS

VPNS مورد اعتماد تکنولوژی است که دو مورد زیر را پشتیبانی کند :

۱- MPLS با توزیع فشار از اطلاعات روتینگ به واسطه BGP

۲- انتقال از لایه دو فریم بالای MPLS (لایه دو VPNS)

IPSEC بطو خیلی متفاوت مسلط ترین قرارداد برای VPNS محفوظ است L2TP تحت نظارت کم IPSEC اجرا می شود اما گسترش و آرایش آن مهم است .

برای VPNS تحت اعتماد بازار و تجارت به دو پروتکل MPLS پایه تقسیم شده است . سپس کمپانی ها مسیر یابی خودشان را جهت استفاده از لایه دو انجام می دهند. کمپانی ها تمایل داشتند و می خواستند که از لایه سوم استفاده کنند . پروتکل های مختلف VPNS بوسیله اعداد بزرگی از استانداردها و توصیه هایی که بوسیله مهندسین اینترنت (IETF) به رمز در می آیند تعریف می گردند .

حالتهایی متعددی از این استانداردهای IETF وجود دارد که شامل توصیه نامه ها ، احکام رویه عرف و مواردی دیگر می باشد .

برخی از پروتکل ها در IPSEC که سراسر از استانداردهای IETF استفاده می کنند وجود دارند . اگر چه اغلب آنها مفید می باشند و به اندازه کافی باثبات می باشند که استاندارد تلقی می شود و بوسیله مردم این نرم افزارها و استانداردها اجرا می شود .

هنوز هیچیک از تکنولوژی های VPN استاندارد تحت IETF مورد تایید کامل نیستند اگر چه تعداد بسیار زیادی از کارها انجام شده اند ولی هنوز به استانداردهای واقعی تبدیل نشده اند .

RFSC

RFSC تصمیمات را به صورت رمزی در متون در می آورد که در خواست برای توضیح وتفسیر نامیده می شود.

بسیاری ازRFCSها استانداردی روی اینترنت هستند.

سطح استاندارد سازی RFC

بسیاری از سطوح استاندارد سازی RFC به شکل دو وجهه هستند .سطحهای استاندارد سازی که یک RFC به آن می رسد به گونه ای وسیع تست و اجرا می شوند.

سطحی از استاندارد سازی RFC در نظر دارد که فقط به خوب بودن استاندارد توجهی ندارد بلکه تنها به تست و اجرا و و رفع اشکالات آن متکی است.

برخی از RFCاستانداردها یی قابل اطمینان نیستند اما استانداردهایی قابل اطمینان نیستند اما تکنولوژی هایی وجود دارند ک ارزش زیادی در اینترنت دارند که جهت اجرا وتکمیل vpns به کار می روند.

به منظور تعریف VPNS هر قرارداد یک در خواست IETF برای توضیح وتفسیر متوفی دارد که می تواند تا حدی یک استاندارد تلقی شود.

مطمنا هر RFC وابسته به IPSCE است که دارای توازن IETF می باشد که استانداردهایی دقیق و صحیح می باشند.

INTERNET DRAFTS

قبل از آنکه یک متن RFC شود به عنوان یک پیش نویس اینترنت مطرح می شود. IDS ها پیش نویسهای ناهماهنگ وتاحدی نادرست هستند و غالبا برای مقاصد مهم به وجود نمی آیند بلکه به وجود می آیند تا بگویند نویسنده چگونه باید فکر کند.

به بیان دیگر اغلب اطلاعات خوب در IDS ها موجود است و به طور اختصاصی پوششی است که جریان استانداردهها را به سمت صحیح هدایت می کند.بسیاری از پیشنویسها در اینترنت برای مدت طولانی کاربرد دارند اما پس ازمدتی رها می شوند ویا کارآیی آنها پایین می آید.

پایه بسیاری ازتصمیمات برنامه ریزی روی اطلاعات حاصل از پیش نویسهای اینترنتی می باشند که عملی غیر عاقلانه محسوب می شود.

امروزه اغلب IDS ها به سمت تکامل پیش می روند و بعد ار تکامل به شکل پروتکلهایی در پیش نویسها توصیف می شوند وبسیاری از آنها هم به سادگی از بین می روند.

لیستی از آنها وابسته به پست الکترونیکی می باشد .بعضی از آنها به RFC ها تبدیل می شوند و برخی متروکه شدده از بین می روند.

لیست پروتکلها

IETF های مربوط به گروههای مختلف کاری برای VPNS های ایمن و محفوظ به کار می روند که شامل:

۱.قرارداد امنیت گروه کاری

۲.قرارداد سیاست امنیت کاری

۳.لایه دو گروهها ی کاری شبکه های اختصاصی مجازی

۴.لایه سوم

۵.شبکه گروههای کاری نزدیک به هم

مدارک به وسیله طبقات عمومی مرتب شده اند که این طبقات شامل:

VPNS محفوظ:

۱.پروتکلهای عمومی

۲ .رمز سازی و اثبات در ستی سر صفحه ها

۳.تعویض کلیدها

۴. الگوریتم پوشیده

۵. پروتکلهای بررسی سیاست و روش اداره

۶. دسترسی از دور

VPNS مورد اعتماد

۱.MPLS عمومی

۲.MPLS تحت فشار به وسیله مسیر یابی BGP

۳.انتقال از فریم لایه دو روی MPLS

۴ .روتر مجازی

پروتکلها ی عمومی

RFC2401 :

پروتکل امنیت برای اینترنت ،هدف از این استاندارد به روز رسانی نسخه ثانی است.

:RFC2411

پروتکل طرح مسیر متن امنیتی

:RFC2521

ICPM امنیت شکست پیغامها

:RFC2709

الگوی ایمنی با TUNNEL مدل IP برای قلمرو و حوضه NAT

: RFC2764

چارچوبی برای پایه شبکه اختصاصی مجازی

چارچوب پیش نویس IETF-NAT-RSIP

حوزه ویژه IP : FRAMWORK

پروتکل پیش نویس IETF-NAT-RSIP

حوزه ویژه IP : مشخصه قرارداد

پیش نویس IETF-NAT-RSIP-IPSEC

جهت پشتیبانی بی نهایت تا بی نهایت (فواصل دور)

پیش نویس IETF-IPSEC-SCTP

برای استفاده از SCTP با ISPCE به عنوان یک استاندارد تصویب شده

ویژگیهای پیش نویس IETF-IPSEC

ویژگیهای امنیت از موقعیت پروتکلهای IPSEC

پیش نویس WARD-BGP-IPSEC

امنیت BGPV4 در استفاده ازIPSEC امنیت بلاکهای ذخیره شده قراردادها روی IP

پیش نویس SANKER-IMP-SCTP

مکانیزم امنیت خط در دقیقه

پیش نویس IETF-IPSEC-DPD

روش ترافیک پایه از تصحیح خطا

کاغذهای سفید vpn

اعضاء vpnc اغلب گزارشها و کاغذهای سفید در مورد موضوعات مختلف وابسته به تکنولوژی vpn را ایجاد می کنند.

این مقاله در مورد مو ضوعات تجاری vpn می باشد. البته این گزارشها توسط کمپانی ها نوشته می شود.هر کمپانی از نگاه خود موضوعات تجاری vpn را بررسی می کند و نگاه هر کمپانی به سوی این موضوع با نگاه کمپانی دیگر متفاوت است. Vpn گزارش رسمی مخصوص به خود در مورد تکنولوژی vpn را دارد که vpnc را دارد کهvpns را تعریف و تشریح می کند.

- ✓ دید بالاتری از vpn

- ✓ درك شبكه های خصوصی مجازی
- ✓ دید بالایی از Ipsecاز cisco
- ✓ کیفیت سرویسهای شبکه های خصوصی مجازی
- ✓ شرح vpn از پورتهای ورودی باز
- ✓ سیر تکاملی پروتکلهای vpns از تکنولوژیهای انباشته

تکنولوژی vpn و رمز نگاری

- ✓ سیاست میکروسافت دستیابی شبکه را محافظت می کند:
- ✓ شبکه خصوصی مجازی و امنیت در اینترنت
- ✓ کنترل پهنای باند و تغییر شکل مسیر عبور و مرور برای شیوه های محرك
- ✓ امنیت و ذخیره کردن با شبکه های مجازی خصوصی

موارد تجاری برای vpns

- ✓ شرح آدرس یك سرویس گزینه محرك از تکنولوژی های درخواستی
- ✓ امنیت و اجرا(کاربرد) پیوندهای منتشر شده همراه با صدا و تصویر از پروتکلهای اینترنتی
- ✓ ەموضوع با گستردگی زمینه رقابت شبکه ، از قسمتهای باز قابل دسترسی
- ✓ مهاجرت از سیستمهای میرا و کاربرد (استفاده از) در جهت پهنای باند آدرس پیدایش vpn Vpns و دستیابی از دور
- ✓ استفاده از پروتکلها ی نقطه به نقطه (استفاده مرحله به مرحله)

- ✓ موضوع اجرای vpn های دور
- ✓ امنیت دستیابی دور با پروتکلهای vpns
- ✓ تکامل vpn های موبایل و مفهوم آن در جهت امنیت از سوی شرکت نوکیا

توازن و هماهنگی میان جلسه ها و گفتگو ها در مورد vpn

عالم vpn فضای زیادی را پوشش میدهد و فروشنده های vpn را تمایل دارند بسیاری از رخدادهای متفاوت مانند اینکه ، نمایش تجاری ، رخدادهای فنی و غیره .

پیروان این فهرستها پراهمیت ترین جلسات و کنفرانس ها را در این مورد برگزار می کنند.

اگر می خواهید راجع به بقیه موارد رخدادهای این موضوع پی ببرید به سایت زیر مراجعه کنید :

Paul hoffman @ vpnc.org

این ارجاع خوب پروتکلهای اینترنتی v6 بسیاری از رخدادهای در این موضوع را با یکدیگر توام می کند به طوریکه بسیاری از شرکت کنندگانی را که دارای سیستمهایی با پروتکل v6 هستند را با یکدیگر آشنا می کند.

فروشنده های پروتکلهای sec که v6 را حمایت و پشتیبانی می کنند ، می توانند پروتکلهای sec و کدهای v6 را با یکدیگر مطابقت داده و استفاده مفید می کنند.

این کنفرانسهای طولانی و مداوم و نمایشگاههای همه جانبه ، همه جوانب Mpls را می پوشانند که شامل : استفاده از vpn s و به عنوان هسته تکنولوژی ISPs است .

نوع گران آن شامل توانایی استفاده مفید در سازمانها بوسیله Mpls و توانایی تقویت کردن فریمها می باشد.

این کنفرانس روی امنیت همه انواع تکنولوژی ها تمرکز می کند اما با vpn s فقط روی یك جنبه متمرکز است.

اطلاعات درباب vpn در شبکه جهانی اینترنت

خبر : توصیه نامه ها را از فهرستهای ایمیل vpn که بهترین آدرس ارجاع کتابها هستند رزرو بکنید.

Vpn چیست؟

شبکه های خصوصی مجازی اتصالات شبکه ای خصوصی حفاظت شده را گویند که آشکارا روی زیرساختارهای قابل دسترسی از قبیل اینترنت یا شبکه تلفنی همگانی ساخته شده اند .

به طور نمونه vpns اغلب رمزسازی ، گواهی نامه های دیجیتالی ، اثبات درستی کاربر را جهت کنترل دستیابی به آنها و نقل و انتقال این اطلاعات روی شبکه ، با یکدیگر ترکیب می کند.

Vpn ها با Ipsec شروع شده اند ، مدتها بود که از اعضاء انجمن های فعلی Vpn می خواستند آنها را شروع کنند اما نمی دانستند باید از کجا شروع بکنند.

پراهمیت ترین تهدید امنیتی در هر Vpn وضع شخص دور است یك نفر از خانه و یك کارمند یا مسافر با لپ تاپ در مسافرت می توانند ارتباط برقرار کنند و جهت اتصال و متصل شدن به شبکه باید با دفتر Vpn تماس بگیرند.