بست

علمي او څېړنيزه مجله

ټوک : څلورم

گڼه: لومړی

کال: ۱۴۰۴

بسم الله الرحمن الرحيم

بُست علمي او څېړنيزه مجله

بُست پوهنتون

څلورم ټوک – لومړی ګڼه

کال – ۱۴۰۴

بُست علمی او څېړنیزه مجله

بُست پوهنتون

د امتیاز خاوند: بُست پوهنتون

مسئول مدیر: ډاکټر ذبیح الله انوري

سردبیران: پوهندوی دوکتور علي احمد احمدي او خان محمد وفا

ډیزاین: د بُست پوهنتون د خپرنیزو او فرهنګي چارو مدیریت

د خپرولو کال: ۱۴۰۴

درک: بُست پوهنتون، لښکرګاه، هلمند، افغانستان

د بُست پوهنتون د رئیس پیغام

په ننې ژوند کې د یوې علمي مؤسسې یو له مسؤلیتونو څخه دا دی ، چې نه یوائې خپل محصلان د پوهې په ګانه سمبال کړي، بلکې د پوهنتون د لوړو زده کړو لرونکو پوهانو او استادانو د علمي زیرمتون څخه داسي څه وخت په وخت راوباسي، چې د ټولنې د ژوند د اړتیاوو د پوره کولو لپاره او یا لږ تر لږه د ټولنې د لوستې قشر د خبرولو او که وکولای شي له هغوی څخه د عمل په ډګر کې د ګټې اخیستنې په موخه ، په کار واچول شي.

و دې موخې ته د رسیدلو لپاره پوهنتون باید یو داسې علمي خپرندویه ارګان ولري، چې په هغه کې د پوهنتون ټول با صلاحیته منسوبین که هغه استاد وي، که کارکوونکی او که زده کړه یال ، خپلې علمي او څېړنیزې مقالې او لیکنې د کاغذ پر مخ باندې کښیښودلای شي.

زما په شخصي آند پدې مجله کې لکه له نوم څخه چې یې ښکاري، باید داسي مسائل را برسیره شي، چې نه یوائې په پوهنتون پورې راګیر پاتې شي، بلکې په عام ډول سره د افغانې ټولنې او په ځانګړي ډول سره د هلمند ولایت د اوسیدونکو و ننې او سبا ژوند ته په کتلو سره، بریالیتونونه، ستونزې ، وړاندیزونه او د حل لارې-چارې ، وړاندې کړل شي.هغه وخت به د بُست پوهنتون علمي مجله یوائې د بست پوهنتون نه، بلکې د ټول هلمند ولایت ، آن د سیمې او ټول افغانستان په کچه د پوهې او څېړنې په برخه کې د وخت د غوښتنو سره سم ، د پاملرنې وړ او و ځوان نسل ته د یوې سمې لارې د ښودلو په موخه ، یوه محبوبه او پر زیاتو خلکو باندې ګرانه مجله وي او په ټول هیواد کې به خپل مینه وال ولري.

دا مجله به د بُست پوهنتون د مشرتابه، استادانو ، محصلانو ، فارغانو او ټولو مینه د علمي او څېړنیزو مقالو د خپرولو لپاره که هغوی د پوهې په هر ډګر کې چې وي، یو خپرنیز ارګان وي،چې و خپریدلو ته به یې ټول مینه وال په تمه ناست وي.ځومره به پرځای او ښه خبر وي، چې د ټولنې لوستی قشر په تیره بیا د بست پوهنتون محترم استادان ، فارغ شوي او بر حاله محصلان د علمي او څېړنیزو مقالو و لیکلو ته و هڅول شي.

زه د بُست پوهنتون د ټولو منسوبینو په استازیتوب ویاړ لرم ، چې د بُست پوهنتون د علمې مجلې د خپریدلو له امله د محترم مؤسس، محترم علمي مرستیال او د څېړنې له محترم آمر او همدا رنګه د مجلې له ټولو کارکوونکو او پرسونل څخه د زیار او زحمت په ګاللو سره چې مجله یې و خپریدلو ته چمتو کړې ده ، مننه او قدرداني وکړم، ټولو ته د زړه له کومې مبارکي وایم او هیله لرم چې د بُست پوهنتون د علمي مجلې کارکوونکي به خپل رسالت د پوهنتون او ټول هلمندې ولس او په اخری تحلیل کې د ټول افغان ملت پر وړاندې په پوره او ټینګ عزم سره سرته ورسوي.

په درنښت

ډیپلوم انجنیر محمود سنګین

د بُست پوهنتون رئیس

سریزه

بُست پوهنتون ویاړ لري چې د خپل علمي پرمختګ په لاره کې يې يو بل ډير مهم او اړين ګام پورته کړ او هغه د بُست د علمي او څېړنيزي مجلې د څلورم ټوک، لومړی ګڼې خپرېدل دي . تر هر څه دمخه د پوهنتون ټولو استادانو، محصلانو او د علم او پوهې د لوی کور مينه والو ته د بُست د علمي او څېړنيزي مجلې د خپرېدلو مبارکي وړاندې کوم او ددې سره جوخت د ټولو ملګرو څخه چې ددې مجلې د جواز په تر لاسه کولو، ترتيبولو او خپرولو کې يې نه ستړې کېدونکې ونډه اخيستې ده د زړه له کومې مننه کوم.

د علمي کور کهول او اړوند کسانو ته ښکاره ده او پوره باور لري چې د ننني نړۍ هر اړخيزه پر مختګ د پوهانو د علمي څېړنو د زيار له برکته ممکن سوی او د لوړو زده کړو مؤسسې، اکادميک انستيتوتونه او څېړنيز علمي مرکزونه پکښې مرکزي او پريکنده رول لوبولی دی.

همدې اصل او ارزښت ته په کتو سره بُست پوهنتون غواړي د پرمختللو اکاډميکو نورمونو په رعايت د تدريس، علميڅېړنو او نوښتونو له لارې مسلکي کادرونه وروزي او د معياري تحصيلي اسانتياوو او زمينو په برابرولو سره د ټولنې ځوانانو ته معياري او د لوړ کيفيت لوړې زده کړې وړاندی او د علميڅېړنو پر بنسټ د کره پوهنيزو اثارو د توليد زمينه برابره کړي ، ترڅو د لوړو زده کړو او مسلکي پوهې په ډګر کې د ګټوړو مهارتونو په تر لاسه کولو او د خپلو رښتينو اهدافو په لاسته راوړلو سره د ټولنې او هيواد په پرمختګ او رغونه کې رغنده ونډه واخلي او د رښتيني خدمت جوګه شي.

ژمن يو چې د هلمند ولايت، ګاونډيو ولايتونو او په ټول هيواد کې ځوان نسل ته د اسلامي ، ملي او کلتوري ارزښتونو په رڼا کې معياري د علمي او مسلکي لوړو زده کړو او پراخو علمي څېړونو زمينه برابره او ټولنې او هيواد ته ژمن او روزل سوي کادرونه وړاندې کړو.

د اوس لپاره د بُست علمي او څېړنيزه مجله يوازې د **سائينسي علومو** په برخه کې علمي او څېړنيزې مقالې او ليکنې د چاپ او نشر د تګلارې سره سم مني او خپروي او هيله مند يو چې په راتلونکې کې به نورې برخې هم ور زياتې کړل سي.

ډاډ لرم چې د بُست پوهنتون استادان، محصلان او علمي کارمندان به انشاألله، نن، سبا او په راتلونکې کې د خپلې علمي څېړنيزې مجلې د خپرولو له لارې خپل دغه دروند خو ويارلی دين (پور) ادأ کړي. همدا ډول ټولو د علم او پوهې څښتنانو او مينه والو ته په مينه سره بلنه ورکوو چې ددی علمي او څېړنيزې مجلې او د بُست پوهنتون د پرمختګ په لاره کې خپلې علمي او څېړنيزې ليکنې، آندونه، وړاندیزونه او رغنده نيوکې او مرستې د تل په شان راولورو. او د علم ددې ستر کور په ودانولو کې د خپلې دينې، او ملي برخې د ادايې ويار راوبښې.

مور هوډ کړيدي او هيله مند يو چې انشآ الله د وخت په تيريدو سره به د خپل هيواد و بچيانو او ځوان نسل ته د تدريس ، ښه روزنې او څېړنيز هاند لپاره اړيني او د پام وړاسانتياوې برابرې کړو تر څو په لومړي پړاو کښې خپلو هلمندوالو بيا د سهيل لويديځې حوزې او په پای کښې و ټولو هيوادوالو ته د يو داسې چوپړ مصدر وګرځي چې زمور د ځوريدلي اولس او ويجاړشوي هيواد اقتصادي، فرهنګي، سياسي او ټولنيزې ستونزې حل او افغانستان د نړۍ د پرمختللوهيوادونو په ليکه کې ودريږي.

لړليک

د مجازي شخصي شبکې د امنيت تطبيق او ډيزاين

خان محمد وفا

د کمپيوټر ساينس پوهنځی رئيس او استاد، بُست پوهنتون

د مسوُل ايميل ادرس: khanmohammad_wafa@yahoo.com

لنډيز

د IP آدرسونو د کمښت له امله د IPv6 پروتوکول ته د مهاجرت يوه حياتي اړتيا ګرځېدلې ده. اوسنیIPv4، چې د NAT (Network Address Translation)له لاري کار کوي، د شبکي د فعاليت او نړيوال لاسرسي پر وړاندي محدوديتونه رامنځته کوي. دا محدوديتونه د نړيوالو پيرودونکو سره د اړيکو ټينګولو او د ويب‌سايټونو د نړيوال ليدلو مخه نيسي. راپورونه ښيي چې د IPv4 آدرسونه د ختمېدو په حال کي دي او هره ورځ د دوی کارېدنه زياتيږي، چې دا يوه جدي اندېښنه ده. که څه هم دا ستونزه له پخوا راهيسي پېژندل سوې، خو بيلابيل حل‌لاري هم وړاندي سوي دي. د دې اړتيا له امله زيات شمېر سازمانونه او پراخي شبکې هڅه کوي، چې د IPv4 څخه IPv6 ته تدريجي مهاجرت ترسره کړي. سره له دې، چې دا مهاجرت ځيني تخنيکي ننګونې لري، خو د دواړو پروتوکولونو هممهاله کارول کولای سي د انتقال بهير اسان کړي. دا مقاله د IPv6 ته د مهاجرت اړتيا، خنډونه او ممکنه حل‌لاري تر څېړني لاندي نيسي.

کليدي کليمې:IPv4 ، IPv6، مهاجرت، NAT، نړيوال لاسرسی

سریزه

مجازي شخصي شبکه (VPN) په حقیقت کي تاسو ته دا وړتیا درکوي، چي خپل آله په انټرنیټ کي د مقابل شبکي سره په یوه امن تونل کي وصل کړئ. په دې شکل چي ستاسو ډیتا به هیڅاته د لاسرسي وړ نه وي. یو ساده مثال دلته غواړم چي وړاندي کړم: مثال په توګه تاسو پوهنتون ته کله چي داخلېږئ، نو د پوهنتون کارت به حتمي درسره وي او په کارت کي ستاسو معلومات شتون لري که چیرته کارت نه وي درسره نو تاسو نه سئ داخلیداي. همداسې په (VPN) شبکه کي همدې مثال ته ورته ویلی سو، چي (VPN) شبکه د دوه نقطو ترمنځ یو امن تونل رامنځته کوي، چي د لاسرسي وړ ندي هغه معلومات چي له دې تونل څخه تیریږي یا هم انتقالیږي د اطمنیان وړ دی او په مکمل ډول خوندی سوی دی. کله چي تاسو په مجازي سرور کي (VPN) سیستم جوړ کړي تاسو به ډېرې ګټې ترلاسه کړې، نو په دې اساس موږ هم تاسو ته دا سپارښتنه کوو، چي د (VPN) جوړول په مجازي سرور کي زده کړئ. ځینې ګټې یې په لاندي ډول سره دي: د ارتباط رامنځته کولو لپاره د ځای انتخاب، په مسلسله توګه ارتباط او د ارتباطاتو پر مهال لوړ امنیت(Fortinet, 2025).

تر ټولو لومړي باید تاسو ددې پام ولري، چي د کارونکي او سرور ترمنځ ډیتا باید خوندي سي. همدارنګه پام مو وي چي شخصي (VPN) په مجازي سرور کي، لکه پروکسي په شکل عمل ترسره کوي آن د انټرنیټ خدماتو وړاندي کونکي هم د ویب برخي له معلومات څخه بې خبره دي، په آخر کي مو پام وي چي تاسو دریم (VPN) سرور ته اړتیا نه لرئ، چي خپل معلومات شریک کړئ. د نورو سره په عمومي توګه د شخصي (VPN) جوړښت لپاره یو مجازي سرور او (SSH) کلاینت ته اړتیا لیدل کېږي. پام مو وي چي د مجازي سرور لپاره ۱۲۸ میګابایټ رم حافظې ته اړتیا ده. که چیرته غواړي چي با کیفیت (VPN) خدمات ترلاسه کړئ، نو پرمختللي مجازي سرور انتخاب کړئ، چي CentOS 6 32 یا هم ۶۴ بیټ وي. هغه کارونکي چي د مک او لینوکس عامل سیستم څخه ګټه اخلي مخکي له مخکي د کلاینټ ټرمینال سره وصل دي، خو د ویندوز کارونکي باید د لاسرسي لپاره د PuTTy سافټویر نصب کړي د سافټویر نصب څخه ورسته موږ مجازي سرور ته لاسرسي امکان لري او د مجازي (VPN) سرور کار پیلیږي چي ټولې مرحلې باید په پوره دقت سره ترسره کړل سي (NordVPN, 2025).

مواد او کړنلاره

د دې څېړنیزې مقالې لپاره کتابتون محوره (Library-based) څېړنیزه تګلاره غوره سوې ده، چي له لارې یې د موضوع اړوند موُثق او مستند معلومات راټول سوي دي. د معلوماتو راټولو لپاره له بیلابیلو علمي سرچینو، لکه علمي مقالو، درسي کتابونو، تخنیکي راپورونو او معتبرو ویب‌سایټونو څخه استفاده سوې ده. د څېړني تمرکز د یو خوندي VPN سیستم ډیزاین او تطبیق باندي دی، چي د دې هدف لپاره د VPN ځانګړتیاوي، امنیتي پروتوکولونه او د امنیت ارزوني معیارونه څېړل سوي دي. سربېره پر دې د معلوماتو د تحلیل لپاره توصیفي (descriptive) تحلیل کارول سوی، ترڅو د راټول سویو معلوماتو څخه د معنا لرونکي پایلو راایستلو ته لاره هواره سي.

د څېړني موندنې

د شخصي مجازي شبکي (Virtual Private Network) پیژندنه:

مجازي شخصي شبکه یا (VPN)چي مخفف یې عبارت دی له ( ) Virtual Private Network څخه په حقیقت کي تاسو ته دا وړتیا درکوي، چي خپل آله په انټرنیټ کي د مقابل شبکې سره په یوه امن تونل کي وصل کړئ. په دې شکل چي ستاسو معلومات به هیڅاته د لاسرسي وړ نه وي یوه ساده مثال دلته غواړم چي وړاندي کړم: مثال په توګه تاسو پوهنتون ته کله چي داخلیږي، نو د پوهنتون کارت به حتمي درسره وي او په کارت کي ستاسو معلومات شتون لري که چیرته کارت نه وي درسره، نو تاسو نه سئ داخلیدای. همداسي په (VPN) شبکه

کي همدې مثال ته ورته ويلای سو، چې (VPN) شبکه د دوه نقطو ترمنځ يو امن تونل رامنځته کوي، چې د لاسرسي وړ نه دی. هغه معلومات چې له دې تونل څخه تيريږي يا هم انتقاليږي د اطمنيان وړ دي او په مکمل ډول خوندي (Encrypt) سوي دي (Palo Alto Networks, 2025).

۱ شکل : د VPN شبکه

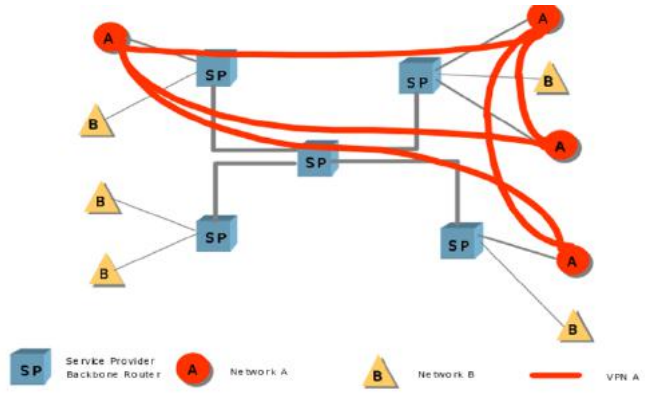
VPN همدارنګه discrete نيټورک هم ويل کېږي discrete شبکه تاسو ته دا اجازه درکوي، چې د privacy او virtualization وکاورئ. په خپله شبکه کي (Mozilla. (n.d.)

د VPN څخه ګټه اخستنه په دوه حالتونو کي ګټور تمامياي سي لومړي تاسو د مجازي شبکې (VPN) په فعالولو سره کولای سي د بيلابيلو هيوادونو سرورونو ته داخل سئ او ګټه ترې واخلئ. د انټرنيټ په مرسته په عمومي ډول د (VPN) څخه د هغه معلوماتو لاسرسي لپاره ګټه اخستل کېږي، چې د لاسرسي وړ نه وي په هغه ساحه کي مثال په توګه: د نټفليکيس ليکنو ته په ډيرو هيوادونو کي لاسرسي نه کېږي، چې د لاسرسي لپاره يې د(VPN) څخه ګټه اخستل کېږي. دوهمه ګټه دا ده چې کله تاسو د(VPN) څخه ګټه اخلي ستاسو تعقيب هيڅوک نه سي کولای. په انټرنيت کي په همدې اساس ستاسو د انټرنيټ امنيت هم ورسره اطميناني کېږي. حتا که چيرته تاسو د وای فای څخه هم ګټه اخلئ (Palo Alto Networks, 2025).

VPN په شبکه کي د دوه لوريو ترمنځ د امن ارتباط رامنځته کولو لپاره کارول کېږي دغه ارتباط کيداي سي په محلي شبکه کي وي، په يو شبکه کي وي يا هم په پراخه شبکه کي وي. عموما درې ډوله VPN () شتون لري، چې په لاندي دول سره تشريح کېږي.

1. **Intranet:** د يوه شرکت په برخي سره يو ځای کوي د مثال په ډول: د شرکت مرکزي نماينده ګي د شرکت بلي نمايندګۍ سره دغه ډول ارتباط ته Site to Site يا هم LAN to LAN ويل کېږي.
2. **Extra Net:** يو سازمان د بل سازمان سره وصل کول.
3. **Remote Access:** د يوه کوچني دفتر کارکونکي د يو يوه لوی شرکت سره وصل کول، د ليري ساحي څخه.

VPN هغه تګلاره ده، چې د ټرافيک جلا کولو لپاره په شبکه کي کارول کېږي، لکه تحقيق او توليد په نيږدې او ليري ساحه کي. په اصل کي يوه ساحه ده خو جلا دغه تګلاره په (MORPHnet) کي هم شتون لري. په VPN شبکه کي ټرافيک په يوه ځانګړي ټونل کي انتقاليږي، چې ډير ګټور دی نسبت نورو تګلارو ته. تر ټولو عام ټونل چې GRE په نوم سره يادېږي. (Hanks،1994)



۲ شکل : د VPN شبکي ساختمان

په اصل کي tunneling د پيل او پای روټر ترمنځ ترسره کېږي چې (د کوربه څخه تر کوربه او د روټر څخه روټر) ټونلينګ پروتوکول هم شتون لري، لکه L2TP پروتوکول PPTP پروتوکول، چې مخفف يې عبارت دی له (Point-to-Point Tunneling Protocol) څخه DVMRP پروتوکول چې مخفف يې عبارت دی له (Distance

Vector Multicast Routing Protocol) څخه چې دا ټول د ټونلینګ پروتوکول په نوم سره یادېږي. (Waitzman et al., 1988)

GRE ټونل یو په یو ټونل دی، چې دلته یوازي یو د پیل آدرس او یو د پای آدرس ته اړتیا لیدل کېږي. همدارنګه ځینې تنظیمات هم پکاریږي، تر څو یو په یو ټونل کې عیار کړل سي. همدارنګه یا ټونل کولای سو د یو څخه ډېرو ته هم عیار کړو، لکه د NHRP پروتوکول چې مخفف یې عبارت دی له (Next-hop Routing Protocol) څخه. (Luciani et al., 1998)

په VPN کې Encryption هم ډېره مهمه او اړینه ټکنالوژي شمېرل کېږي، کله چې موږ د(VPN)څخه ګټه اخلو، نو ځینې پروتوکولونه شتون لري، چې د Encryption دنده پر مخ وړي د نیټورک لایر Encryption لپاره تر ټولو مشهوره پروتوکول IPSec دی. (Kent & Atkinson, 1998)

د مجازی شخصي شبکې تاریخچه (VPN) :

د ۲۱ یویشتم پیړۍ په دوهمه نیمایي کې امنیتي پېښې ډېرې سوې، چې انټرنیټ جرمونه هم ورسره مل وو، چې ډېرو کارونکو په انټرنیټ کې د خطر احساس کولو د VPN په رامنځته کیدو سره دغه امنیتي ستونزې ورسره حل سوې او کارونکو ته په اطمینانې توګه لاسرسي وړاندې کړل سو. VPN د لیرې ساحې څخه د لاسرسي تګلاره وه، چې وړاندې کړل سوه، چې کارونکي په لوړ امنیت سره وکولای سي خپل کارونه ترسره کړي او د دوی ډیټا خوندي پاتې سي. په VPN کې بیلابیل پروتوکولونه هم کارول کېږي چې ورسته به تر بحث لاندې ونیول سي خو د ۲۰۰۵م کال ورسته نوی پروتوکول بازار ته وړاندې نه سو (Security.org, 2025).

۳ شکل : د VPN تاریخچه

د مجازی شخصي شبکې (VPN) ځانګړتیاوي:

د VPN څخه د ګټې اخستنې یو لوی علت ممکن دا وي، چې دوی پر ISP اعتبار نه لري. په دې سره تاسو باید پوه سئ، چې کوم VPN ښه دی او کوم یو ښې ځانګړتیاوي لري.

د ای پی آدرس خوندي (Encrypt) کول:

د VPN ای پی آدرس باید ISP او ویب سایټونو څخه پټ وي په دې سره تاسو کولای سي، چې په آسانۍ سره خپل معلومات ولیږئ او ترلاسه کړئ بغیر له کوم محدودیت څخه او همدارنګه د لوړ امنیت خاوند به هم وي.

د پروتوکول خوندي (Encrypt) کول:

VPN باید وکولای سي چې ستاسو د پلټنې ساحې پټې کړي. د مثال په توګه: ویب سایټ که د پلټنې په برخه کې (کوکی) د کوکی خوندي کول کولای سي، چې ستاسو د پلټنې معلومات پټ کړي او د لاسرسي وړ نه سي، نو ځکه د ډېر اهمیت وړ خبره ده(NYM, 2025)

د هویت پېژندل په دوه مرحلو کې:

په اصل کې یو پیاوړی VPN په بیلابیلو لارو سره د هویت پیژندل ترسره کوي او سیستم ته لاسرسي برابروي.

د مجازي شخصي شبکې (VPN) عملي کولو تګلاري:

د VPN د عملي کولو لپاره لاندې تګلاري کارول کېږي.

1. GRE (Generic Route encapsulation)
2. PPTP (Point to Point Tunneling Protocol)

3. L2TP (Layer 2 Tunneling Protocol)

4. IPSEC (IP Security)

5. SSL (Secure Socket Layer-CISCO's solution is called WEBVPN) (رستم،۱۳۸۱)

په مجازي شخصي شبکې (VPN)کي پروتوکولونه:

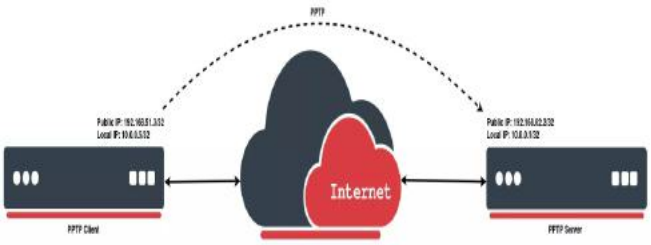
په VPN کي بيلابيل پروتوکولونه شتون لري، چې د VPN سره يو ځای د امنيت په برخه کي فعاليت ترسره کوي او بيلابيل خدمات وړاندي کوي، چې ځينې پروتوکولونه په لاندي ډول سره دي. (رستم،۱۳۸۱)

۴ شکل : په VPN کي پروتوکولونه

په مجازي شخصي شبکې (VPN) کي د PPTP پروتوکول :

د PPTP مخفف عبارت دی له Point-to-Point Tunneling Protocol څخه، هغه پروتوکول دی، چې په (VPN) ټکنالوژۍ کي کارول کېږي. دغه پروتوکول په(VPN)کي د لومړيو څخه کارول کېده او د پخواني پروتوکول په حيث پېژندل کېږي دغه پروتوکول د ۱۲۸ بيټ Encrption څخه ګټه اخلي، چې د استندرد پر اساس يو کمزوري پروتوکول پېژندل کېږي. PPTP ساده شکل لري او لاسرسي ورته په آساني سره کېږي، که څه PPTP پروتوکول يو ساده پروتوکول په حيث پېژندل کېږي، خو بيا خپلي ګټې لري سرعت يې لوړ دي .

(Rubens et al., 1998)



۵ شکل : په VPN کي د PPTP پروتوکول

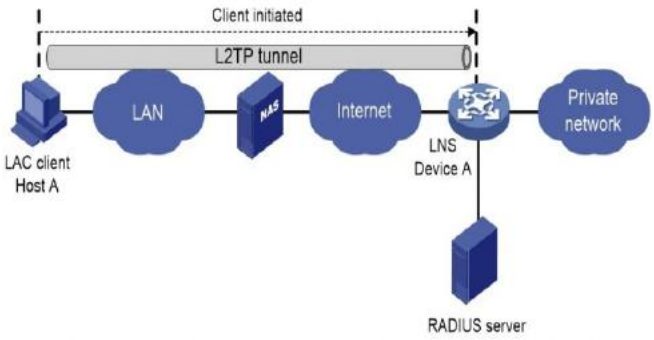
د PPTP پروتوکول کار په دې ډول سره دی، چې لومړي آله خپله غوښتنه سرور ته لېږي. کله چې د هويت پېژندل ترسره کړل سي PPTP پروتوکول د کارونکي او سرور ترمنځ تونل رامنځته کوي، معلومات پکښې ليږل په خوندي ډول يعني د کلاينټ او سرور ترمنځ معلومات ليږل کېږي. (رستم،۱۳۸۱)

د PPTP ګټې او نيمګړتياوي:

د PPTP پروتوکول تر ټولو مهمه ګټه سرعت دی، چې په بيلابيلو آلو کي يې لري. ټيټ امنيت، کرک کيدل او د ځينو فايروالو لخوا بند کيدل يې لويي نيمګړتياوي شمېرل کېږي.(رستم،۱۳۸۱)

په مجازي شخصي شبکې (VPN)کي د IPSEC/L2TP پروتوکول:

په VPN کي يو بل پروتوکول، چې نسبت PPTP ته يې امنيت ډېر دی، خو سرعت يې لږ دی IPsec ورته ويل کېږي. دغه پروتوکول هم د کارونکي او سرور ترمنځ د تونل په رامنځته کولو کي بريالي دی. په اصل کي په IPsec کي د هويت پېژندل او Encryption دواړه صورت نيسي. آله خپله غوښتنه (VPN) سرور ته انتقالوي ورسته سرور د کارونکي نوم او پاسورډ دواړه چک کوي تر تاييد څخه ورسته د آلې او کارونکي ترمنځ تونل رامنځته کېږي چې معلومات پکښې انتقال سي IPsec د هويت پېژندل او ډيټا Encryption دنده پر غاړه لري او د امنيت رامنځته کولو لپاره بيلابيل پروتوکول کاروي. (رستم،۱۳۸۱)



٦ شکل : په VPN کي د IPSEC/L2TP پروتوکول

د TCP/IP په هر لایر کي بیلابیل پروتوکولونه شتون لري، چې خپلې دندې لري، نو په دې اساس هر لایر لپاره پروتوکولونه رامنځته سوي، چې امنیت رامنځته کړي. په دې ډول د امنیت لپاره پروتوکولونه ایجاد سوي، تر څو امنیت رامنځته کړي. په شبکه کي د ورکړل سویو اصولو له مخې په هر لایر کي پروتوکول کولای سي یو ځانګړی قرارداد ولري. د ځانګړي دندې ترسره کولو لپاره، چې په همدې اساس IPsec په نیټورک لایر کي خپله دنده ترسره کولای سي. دغه پروتوکول په پراخه پیمانه سره په (VPN) شبکو کي استعمالیږي، چې اساس یې په دوه طرفه ارتباطاتو باندې ولاړ دی. په (VPN) شبکه کي امنیت کولای سي بیلابیل روسونه یا تګلاري ولري، لکه د فایروال شتون، AAA Server، IPsec او کپسولیټ ترسره کول، خو د IPsec روش مطمعین، ثابت، ارزانه، انعطاف پذیره، لوړ مدیریت او داسي نوري ځانګړتیاوو درلودونکي دي.

دغه پروتوکول لاندې دوه پروتوکول لري:

- **Authentication Header یا AH:** په دغه برخه کي د پاکټ فارمټ او هویت پېژندل تر بحث لاندې نیول کېږي.
- **Encryption Algorithm:** په دغه برخه کي بیا د ESP په واسطه Encryption تر بحث لاندې نیول کېږي.
- **Key Management:** دغه برخه کي بیا د کیلي مدیریت تر بحث لاندې نیول کېږي.
- **Domain of Inter Predation:** دغه برخه کي د کیلي مدیریت یعني د کیلي د عمر اندازه معلومول بیلابیل الګوریتم کارول بیلابیل پارامتر استعمالول او د دوی د تعامل پایله پکښې لیدل کېږي.

د AH او ESP پروتوکول یوازې د Encryption دنده پر مخ وړي او ESP بیا د هویت پېژندلو پروسه مخ ته بیایي. په حقیقت کي IPsec یو پرمختللي پروتوکول دی، چې د IP پروتوکول پر اساس خپل کار ترسره کوي او په نړۍ کي د امنیت په برخه کي کار ته دوام ورکوي، چې IPsec تر څنګ دوه نور پروتوکولونه هم شتون لري، چې په ګډه کار ترسره کوي د هویت او محرمیت لپاره. همدارنګه په IPsec پروتوکول کي دوه حالتونه یا موډونه هم شتون لري، چې لومړي ته یې د Tunnel موډ او دوهم ته یې د Transport موډ ویل کېږي، چې دا حالتونه د امنیتي برخه کي کارول کېږي(Waitzman et al., 1988)

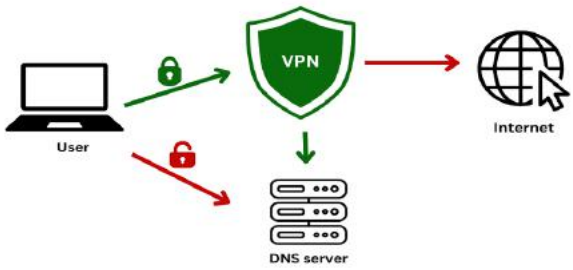
په Tunnel حالت د IP ډیټاګرام په مکمل ډول د نوي IP ډیټاګرام په واسطه کپسول کېږي او دغه کار د IPsec پروتوکول لپاره ترسره کوي، خو په Transport موډ کي بیا د پیلوډ په واسطه ډیټاګرام IPsec ته ورپېژندل کېږي، تر څو د IP په پورتني برخه کي اضافه سي. د Tunnel حالت ګټه دا ده چې معمولا د Gateway آدرسونه بیرته ترلاسه کوي، چې دغه موضوع په شبکه کي د بریدونه څخه مخنیوي کوي او دوهمه ګټه یې دا ده، چې مسیریابي یا لاره پېژندل یې په واسطه ترسره کېږي. په Transport حالت کي هویت پېژندنه مستقیم د سرور او کلاینټ ترمنځ ترسره کېږي. په دغه حالت کي واقعا دوه کمپیوټر په یوه محلي شبکه کي قرار نه لري، خو په Tunnel حالت کي بیا د Gateway په واسطه خدماتو دا ثابته کړي ده، چې هویت پېژني دواړه حالتونه د Transport mode Manuel mode څخه د استخراج لپاره کارول کېږي.

IPSEC کولای سي په محلي شبکه کي په مجازي شخصي شبکه په پراخه شبکه او آن په انټرنیټ کي مطمین ارتباطات رامنځته کړي. د IPSEC مثالونه په لاندې ډول سره دي: (Waitzman et al., 1988)

- د انټرنیټ په واسطه د اداري لپاره ارتباط رامنځته کول

- انترنیټ ته په مطمینه توګه لاسرسي.
- د داخلي او بهرني انترنیټ سره ارتباط رامنځته کول، چې انټرانیټ او اکسټرانیټ ورته ویل کېږي.
- په الکترونیکي تجارت کې پرمختګ رامنځته کول،

تر ټولو مهمه ځانګړتیا چې IPSEC پروتوکول یې لري کولای سي، چې د IP پروتوکول پر سطحه باندې ټرافیک شکل بدل کړي، تر څو د لوستلو وړ نه سي. همدارنګه د اعتبار او هویت پیژندنه ترسره کړي، چې په پایله کې ټول ټرافیک د امنیت خاوندان کیدای سي، لکه ایمیل سرور، فایلونه، سرور، ویب پرخه او داسې نور. لاندې تصویر کې تاسو لیدلاي سئ هغه نیټورک، چې د IPSEC پروتوکول څخه یې ګټه اخستې ده او یو سازمان کولای سي په بیلابیلو موقیعتونو کې ارتباطات سره رامنځته کړي، چې د هر LAN لپاره یو IP په نظر کې نیول سوي دي، خو ټرافیک د شبکې څخه بهر د IPSEC پروتوکول څخه ګټه اخلي او دغه پروتوکول بیلابیل ډول خدمات وړاندې کوي، لکه فایروال، مسیر یابي لاره پیدا کول امنیت او داسي نور. (Waitzman et al., 1988)



۷ شکل : سرور او مجازی VPN

IPsec پروتوکول د انټرنیټ په لایر کې کار ترسره کوي IPsec کولای سي د دوه کمپیوټرو دوه استعمالونکو ترمنځ دوه شبکو ترمنځ یو امنیتي میزبان په شکل رول ولوبوي. همدارنګه IPsec پروتوکول په پراخه پیمانه په امنیتي پرخه کې کارول کېږي، لکه د SSL لایر، د SSH لایر او TLS لایر کې کار کوي. په داسي حال کې چې IPsec پروتوکول په هر ډول ټرافیک کې کار ترسره کوي. همدارنګه GRE پروتوکول هم د IPsec څنګ کې کار ترسره کوي. ددې لپاره چې په IPsec کې په ډول سره کار ترسره کړي تاسو باید یعني دواړه لوري کیلی ولري او د یو بل سره یې شریکه کړي، چې دې پروسې ته د کیلي مدیریت ویل کېږي. دغه پروتوکول ترسره کوونکي ته دا وړتیا ورکوي، چې یوه عمومي کیلي ترلاسه کړي او په واسطه یې د هویت پیژندل ترسره کړي. (Hamzeh et al., 1997)

د ای پي سیکورټي وي پي این (IPsec VPN) ځانګړتیاوي:

د Replay برید مخنیوي

IPsec د replay څخه مخنیوی کوي. که چیرته هر پاکټ ته مسلسله شمیره ورکړل سي، نو ورسته د تکراري پاکټ مخنیوی کیدای سي او کولای سي تکراري پاکټ حذف کړي. د (Hash (HMAC څخه د هویت پیژندلو لپاره ګټه اخستل کېږي.

د معلوماتو محرمیت:

PFS پروتوکول کولای سي د (VPN) ترڅنګ پیاوړي امنیت رامنځته کړي، چې هر ارتباط لپاره ځانګړي کیلي ایجادوي، یعني ځانګړي سوي کیلي. (Hamzeh et al., 1997)

شفافیت:

IPsec د انتقال لایر لاندې کار ترسره کوي، نو په دې اساس د استعمالونکو لپاره شفافیت ډېر اړین دی، چې په پایله کې فایروال، یا هم مسیر یابي پروتوکولونو ته اړتیا نه پیدا کېږي.

Encapsulation ترسره کول:

Encapsulation ترسره کول د بیلابیلو بریدونو مخنیوي کوي. ځکه د کیلي څخه ګټه اخلي د هویت پیژندلو لپاره تر څو هکر ونه سي کولای معلومات غلا کړي.

محرمیت رامنځته کول:

پاکټ مخکې له دې چې انتقال سي Encapsulation کېږي، چې په پایله کې لیږونکي Encapsulation سوي پاکټ ترلاسه کوي(Hamzeh et al., 1997)

په AH کې د تونل او انتقال حالتونه:

AH په IP پاکټ کي د ساتني او تمامیت لپاره د Hash Message Authentication Code څخه ګټه اخلي. په دغه پروتوکول کي چې په لنډ ډول HMAC هم ورته ویل کېږي د HMAC لپاره IPsec پروتوکول د SHA څخه ګټه اخلي د هش لپاره، تر څو وکولای سي کیلي امنیت خوندي کړي. یعني د secret key د محتویات څخه ګټه واخلي په اصل کي په دغه پروتوکول کي د hash برخي کود په ترلاسه کیدونکي پاکټ کي موجود دي، چې کیلي ته لاسرسي برابرولي سي او نور د IP ډیټاګرام محرمیت په برخه کي د IPsec پروتوکول د الګوریتمونو په برخه کي او همدارنګه د Symmetric Encryption Algorithm لپاره کارول کېږي(Hamzeh et al., 1997)

IPsec پروتوکول د بریدونو مخنیوي لپاره د Denial of services څخه په sliding windows کي ګټه اخلي په دغه روش کي پاکټ ته مسلسله شمېره ورکول کېږي، چې هر نوي پاکټ یوه نوې شمیره ترلاسه کړي. که چیرته کوم پاکټ شمیره تکراري سوه هغه پاکټ dispatched کېږي. دغه روش د اکثره بریدونو په مقابل کي پیاوړې تګلاره ده.

د SA امنیتي ټولګه لاندي درې پارامتر لري:

1. **Security Parameter Index:** دغه پارامتر ۳۲ بایټ محلي ذخیره لري. دغه پارامتر بیا HA او ESP هم انتقالوي تر څو سیستم وکولای سي، چې اړونده SA انتخاب کړي.
2. **security Parameter Identifier:** دغه پارامتر د SA اړوند دی، چې امنیتي SA انتخابوي په دغه پارامتر کي دواړه پروتوکولونه یو ځای کار نه سي ترسره کولای.
3. **د مقصد IP :** دغه آدرس عموما په شبکه کي یو مقصد مورِ ته معلوموي هغه که کمپیوټر وي یا هم روټر یا هم نوري آلې.

د SA امنیتي برخه کي لاندي معلومات شتون لري:

1. د پیل او پای آدرس.
2. د ESP په باره کي معلومات، IPsec ، AH اړونده الګوریتمونو په باره کي.
3. د پاکټ انتقال لپاره د Transport او Tunnel موډ شتون.
4. د Sliding windows ویندوز اندازې شتون، چې د بریدونو په مخنیوي کي کارونه ورځخه کېږي.
5. د SA لپاره د حیات وخت هغه وخت دی، چې بل نوي SA پکښې پیلیږي.
6. په IPsec پروتوکول کي په تونل او انتقال موډونو کي wildcard هم مشخصیږي.
7. د Sequence Number caurter شتون.
8. د sequence caunter interflow شتون.
9. د Path Maximum Transportation limit شتون (رستم،۱۳۸۱)

په SP کي بیا لاندي معلومات شتون لري:

1. د ساتل سوي پاکټ د پیل او پای آدرس.
2. د پروتوکول او پورت ساتنه ترسره کول.
3. د Security Associate رامنځته کول د امنیتي برخي لپاره په Security Associate یا لاسي ډول د امنیتي برخې تنظیم تل د ستونزو سره مخ وي. ځکه خطا او غلطي پکښې ترسره کېږي. له بلي خوا باید په دغه ډول شبکو کي د (VPN) څخه کارونه وسي. ځکه (VPN) د خپل ځان سره بیلابیل الګوریتمونه کارونه کوي، چې دا خپله د یو امنیتي پرمختګ دی. یعني د مثال په ډول دوه طرفه غواړي د یو بل سره ارتباط رامنځته کړي، نو د یو بل سره باید Key Exchange ترسره کړي. یعني تر څو یو بل وپېژني. د کیلي حافظت او ساتني لپاره بیلابیل الګوریتم شتون لري چې یو یې د Diffle – Hellman key exchange الګوریتم دي.(Hamzeh et al., 1997)

د ای پي سیکورټي (IPsec) حالتونه:

په IPsec کي حالتونه په دوه پروتوکولو پوري اړه لري، چي مرکزي پروتوکول هم ورته ویل کېږي. لومړي Encapsulating Security Payload او دوهم Authentication Header په نوم باندې یادیږي. دواړه پروتوکول د Header برخي ته ډیاګرام اضافه کوي، ددغه دواړو پروتوکولو توپیر په Encapsulation کي دی، چي ډیاګرام په بیلابیلو اشکالو اضافه کوي. همدارنګه IPsec پروتوکول د Transport او tunnel حالت څخه هم ګټه اخلي.(Luciani et al., 1998)

۸ شکل : د IPsec حالت

Transport حالت

په دغه حالت کي Payload بغیر له دې چي په Header کي کوم تغیرات رامنځته کړي Encapsulation ترسره کوي، چي همدې په خاطر ورته Encapsulating Security Payload ویل کېږي. په دغه روش کي دواړه لوري د هویت پېژندلو پروسه تیروي او همدارنګه د معلوماتو Encapsulation هم ترسره کوي. په دغه حالت کي NAT هم کار کولای سي VPN د NAT سره په ګډه شبکه کي د امنیت رامنځته کولو لپاره کوښښ کوي(Luciani et al., 1998)

Tunnel حالت:

په دغه حالت کي Payload په Header کي تغیرات رامنځته کړي، تر څو وکولای سي مطمعین ارتباط رامنځته کړي tunnel حالت د Authentication Header په نوم هم مشهوره دی. په دغه حالت کي IPsec ډیټا بیرته Decapsulat کوي، تر څو وکولای سي بیرته د معلوماتو څخه ګټه واخلي(Luciani et al., 1998)

د P2TP/IPSec پروتوکول ګټي او نیمګړتیاوي:

د IPSec پروتوکول مناسب سرعت خاوند دی، چي او په هر ډول عامل سیستم کي کار ترسره کولای سي. هغه کارونکي چي فلتر څخه بغیر انټرنیټ کارول غواړي کولای سي له دې پروتوکول څخه ګټه واخلي. همدارنګه د IPSec پروتوکول نیمګړتیاوي هم لري په دوامداره توګه د فایروال په واسطه قطع کېږي او امنیت یې هم لږ دي. (Aiken et al., 1997)

د ای پي سیکورټي وي پي این (IPsec VPN) ګټي:

- د بیلابیلو ډیوایسونو سره کار ترسره کول.
- تر ټولو بهترینه امنیت وړاندي کوي.
- د کارکونکي وړتیاوې لوړ وي او هر وخت او هر ځای د شرکت منابعو ته لاسرسي موندلاي سي.
- د کار کولو وړتیا لوړوي او په شبکه کي مدیریت رامنځته کوي او مصارف کموي.
- ثابت دی څکه که چیرته په شبکه کي تغیرات رامنځته کېږي د قطع کیدو څخه ورسته بیرته وصل کېږي.
- په شبکه کي عمل کوي یعني کوم سافټویر پوري وصل نه دي.

د ای پي سیکورټي وي پي این (IPsec VPN) نیمګړتیاوي:

- د فایروال په واسطه کولای سي محدودیتونه لمنځه یوسي.
- تر ټولو چټک پروتوکول نه دی، لکه L2TP / IPsec چي ډیټا دوباره یا دوه ځلي کپسولیټ کړي.
- د پروسس لپاره ډېر باندویټ ته اړتیا لري.

په مجازي شخصي شبکه (VPN) کي IKE پروتوکول:

IKE هغه پروتوکول دی، چي څو مهمي مسئلې د امنیت په اړوند تنظیموي، د هویت تشخیص د کیلي تبادله د امنیت په اړوند ټولګه وړاندي کول د Security Association data base رامنځته کول شامل دي پکښې، چي عموما د استعمالونکو اکثره اړتیاوي پوره کوي

او په عامل سيستم باندي يې عملي کوي. د IKE پروتوکول د UDP د ۵۰۰ پورت څخه ګټه اخلي.

ددې پروتوکول مکمل نوم IKEv2/IPSec دی، چې د VPN امنيتي پروتوکولونو څخه شمېرل کېږي. ددې پروتوکول امنيت هم د IPSec پر غاړه دی. همدارنګه د ويندوز ۷ څخه وروسته ورژنو لپاره مناسب بلل کېږي. دغه پروتوکول امنيت ډېر پياوړی دی، خو ډېر ښه نه بلل کېږي. همدارنګه د اندوراید او IOS عامل سيستمونه هم ګټه تړي اخستی سي. IKE پروتوکول نسبت P2TP ته مشهوره نه دی، خو امنيت يې ډېر پياوړي دی. دغه پروتوکول د AES الګوريتم څخه ګټه اخلي د Encrytpion لپاره(Aiken et al., 1997)

۹ شکل : په VPN کې IKE پروتوکول

IKE دوه مرحلې لري، چې لومړۍ يې د ISAKMP SA په نوم باندي يادېږي او دوهمه يې د ISAKMPSA په نوم چې د SA او IPsec سره د مذاکرات او تنظيم په برخه کې مرسته کوي.

لومړۍ مرحله د دوه حالتونو څخه پيشتباني کوي main mode يا اصلي موډ دوهم د aggressive mode يا تهاجمي موډ په نوم باندي يادېږي، چې په دواړو حالتونو کې د هويت پېژندنه د ISAKMP SA په واسطه تنظيمېږي. په بريدکونکي موډ کې يوازي نيمايي پيامونه تر خپل پوښښ لاندي راولي. په هر حال دا خپله يو ډول شکل دی. ځکه دغه حالت نه سي کولای، چې د هويت ساتنه او حمايت ترسره کړي. ددې له لحاظ د man-in-the-middle تر برید لاندي راځي. په اصلي حالت کې نه يوازي چې د هويت څخه ساتنه نه ترسره کېږي، بلکې حمايت يې هم نه کوي. ځکه نه پېژني او په بريدکونکي حالت کې هم د دوی څخه حمايت نه کوي. په دوهم حالت کې د IKE پروتوکول د SA څخه حمايت ترسره کوي او د ISAKMP سره د SA په برخه کې په توافق رسيدلی دی ISAKMP SA د هويت پېژندلو لپاره او د هغوي د ساتنې لپاره د برید کونکي لاري څخه ګټه اخلي. دوهمه مرحله ډېره چټکه ده، ځکه چې SAKMP د SA سره په توافق رسيدلی دی (Hanks et al., 1994)

د IKE پروتوکول ګټې او نيمګړتياوي:

لوړ امنيت، دوامداره ارتباطات بغير له قطع کيدو څخه لوړ سرعت په بانډويټ کې لږ بيروبار او نيمګړتيا يې دا ده، چې د ټولو سيستمونو سره کار نه سي ترسره کولای.

په مجازي شخصي شبکه(VPN) کې د SSL پروتوکول:

د SSL مخفف عبارت دی له Secure Socket Layer څخه چې د امن پروتوکول لاير په نوم باندي يادېږي او نور نومونه يې په دې دول سره دي: Https ، S-HTTP ، Secure HTTP. SSL په اصطلاح کې د امن سيستم ته ويل کېږي، چې پکښې معلومات په خوندي ډول انتقاليږي SSL په کال ۱۹۹۶م کې د Netscape شرکت لخوا د ډېتا انتقال لپاره کارول کېږي او اوس مهال اکثره بروزر ددې پروتوکول څخه ګټه اخلي، لکه فايرفاکس، اپرا، انټرنيټ اکسپلور، ګوګل کروم او سافاري څخه حمايت کولای سي. همدارنګه دا شرکت د ssl ګواهينامه هم وړاندي کوي. لومړی د SSL.com تعريف ته ورځو، چې SSL يې څنګه تعريف کړی دی؟ SSL هغه امنيتي ټکنالوژي ده، چې د ارتباط برقرارولو لپاره کارول کېږي. د سرور او ويب بروزر ترمنځ دغه ارتباط په منځ کې چې د سرور او ويب بروزر ترمنځ واقع سوي دي، معلومات په محرم ډول انتقاليږي او تضمين يې ترسره کوي. کله چې تاسو پاڼې ته داخليږئ، چې فرم پکښې موجود وي، کله چې تاسو فرم ته داخل سئ، نو فرم به ډکوئ وروسته به ليږل کېږي. دغه پاڼه د SSL ګواهينامه ونه لري، نو ټول معلومات به هکر ترلاسه کړي. (رستم،۱۳۸۱) دغه ډېتا کيدای سي، چې

بیلابیل ډول معلومات پکښې شتون ولري. اکثره بانکي سیستمونه د دغه برخي څخه ګټه اخلي. اکثره بریدکونکي د همدې برخي څخه کارونه کوي او د man-in-the-middle attack برید ترسره کوي. برید کونکي کوښښ کوي، چې یو کوچنی مقدار پروګرام په هغه سرور کي ځای پر ځای کړي، چې ویب سایټ پکښې شتون لري دغه پروګرام منتظر پاتي کېږي، تر څو ډیټا په فارم کي ورته داخل سي وروسته دغه معلومات ددې پروګرام په واسطه غلا کېږي، خو کله چې تاسو د SSL پروتوکول څخه ګټه واخلئ، نو د تاسو بروزر د SSL په واسطه پېژندل کېږي. وروسته د بروزر او سرور ترمنځ ارتباط د SSL په واسطه لیدل کېږي او امنیت یې برقراره کېږي. په دغه حالت کي هیڅوک نه سي کولای، چې د تاسو معلومات وګوري. نن سبا د SSL ارتباطات ډیر چټک دي او سرعت یې هم ډیر زیات ښودل سوی دی. نو ددې لپاره چې استعمالونکي وکولای سي د پیاوړي ارتباطاتو څخه ګټه واخلي دې ته اړتیا ده، چې لومړی د https:// څخه په لومړی قدم کي کارونه ورځخه وکړای سي. ځکه چې د SSL ګواهینامه لري چې تر ټولو معتبره ګواهینامه ده د ارتباطات په برخه کي(Hanks et al., 1994)

د SSL ګټې:

نن ورځ هر ویب سایټ لپاره که شخصي دی یا تجارتي د SSL اړتیا ډېره زیاته ده. ځکه چې داسي ګټې لري، چې سترګي ترې څوک نه سي پټولای. ځکه اکثره خلک د SSL له ګټو څخه خبر سول، نو په دې اساس د SSL استعمال ډېر پراخ سو.

د معلوماتو ساتنه کوي:

د SSL اصلي دنده د معلوماتو ساتنه ده، چې د سرور او بروزر ترمنځ تبادله کېږي. SSL د معلومات هر بیټ (Encrypt) کوي. په ساده ډول ووایو یعني قفل کوي، تر څو د بیرته خلاصولو لپاره کیلي ته اړتیا پیدا سي. همدارنګه SSL په بیلابیلو برخو کي کارول کېږي، چې بانکي کارت یې یو مثال ښودلای سو، لکه څنګه چې SSL متن داسي یو فارمټ ته بدلوي چې د ویلو وړ نه وي، نو ډېر اړین دی (Hanks et al., 1994)

SSL د هویت تایید ترسره کوي:

د SSL دوهمه دنده دا ده، چې د ویب اعتبار تایید کړي شک نسته، چې په انټرنیټ کي ډېر زیات داسي ویب سایټونه شتون لري، چې هکرانو مربوط دي، چې دغه کار خلکو ته بیلابیل ډول مالی زیانونه رسوي. اوس مهال د SSL اړتیا ډېر سوې ده او باید په هر برخه کي کارونه ورځخه وسي، تر څو د ویب سایت تایید ورسته تاسو ګټه تري واخلئ ()

SSL لپاره لوګو یوه اړتیا ده د ملګرتیا لپاره:

د کاروبار یانو یوه نمونه دا ده، چې لوګو د ځان پېژندلو لپاره یوه لوګو استعمالوي. نن سبا که چیرته د تاسو شرکت کومه لوګو ونه لرئ، نو څوک اعتماد نه درباندي کوي. اوس مهال د ستوري لوګو په انټرنیټ کي شتون لري، یعني یو ستوري، دوه ستوري او درې ستوري. دغه ددې معنا لري، چې تاسو د SSL یو کلن اعتبار ترلاسه کړی دی. دقت باید ولري چې تاسو دوه ستوري لوګو هیڅ کله په وړیا توګه د SSL څخه نه سئ ترلاسه کولای. (رستم،۱۳۸۱)

SSL د مشتري اعتماد ډېروي:

نن سبا اکثره مشتریان که چیرته کومه برخه د SSL څخه کارونه نه کوي اعتبار پرې نه کوي. ځکه چې د معلومات غلا کولو لپاره پر دوی باندي اعتماد نه سي کولای. عموما نن سبا اکثره کارونه د انټرنیټ په واسطه ترسره کېږي، نو که چیرته څوک SSL ونه لري، نو څوک اعتبار هم نه پرې کوي او نه هم دوی په خپل کارو بار کي پرمختګ کولای سي(DigiCert, 2021).

SSL د پلټنې په موتور کي د تاسو د پرمختګ باعث کېږي:

ګوګل کروم په رسمي ډول اعلان وکړ که چیرته دوه دانې ویبسایټونه د یو بل سره برابر وي هر یو، چې SSL اعتبار نامه ولري هغې ته اولویت

ورکول کېږي، چې دغه کار د پلټنې په برخه کې هم ډېر مفید ښکاره سو.(DigiCert, 2021).

۱۰ شکل : د SSL پروتوکول

په مجازي شخصي شبکه (VPN) کې د OpenVPN پروتوکول:

OpenVPN یو خلاص متن پروتوکول دی، چې لوړ امنیت خدمات وړاندې کوي. همدارنګه د SSL/TLS خدماتو څخه هم ګټه اخلي. د Encryption په برخه کې دغه پروتوکول کارونکي ته اجازه ورکوي، تر څو وکولای سي یاد پروتوکول د خپلې خوښې مطابق عیار کړي. دغه پروتوکول د ښه امنیت خاوند دی، چې په بیلابیلو چلیزو سیستمونو کې کار ترسره کولای سي، لکه ویندوز، مک، لینوکس، اندوراید او IOS، د OpenVPN پروتوکول سبک پروتوکول دی، چې کولای سو په ارتباطاتو کې ترې ګټه واخلو. ددې پروتوکول اصلي ګټه دا ډېتا Encryption دی په بیلابیلو تګلارو سره(DigiCert, 2021).

د OpenVPN ګټې او نیمګړتیاوې:

OpenVPN یو خلاص متن پروتوکول دی، کولای سو پکښې په خپله خوښه تغیرات راولو او عیار یې کړو. د هر ډول چلیز سیستم سره کار ترسره کولای سي، امنیت یې لوړ دی او په آسانې سره ارتباطاتو لپاره کارول کېږي او تر ټولو لویه نیمګړتیا یې دا ده چې په لاره اچول یې ستونزمن دي. (DigiCert, 2021).

په مجازي شخصي شبکه (VPN) کې د SSTP پروتوکول:

Secure Socket Tunneling Protocol | SSTP په VPN کې یو بل امنیتي پروتوکول دی، چې د مایکروسافټ کمپنۍ لخوا وړاندې کړل سوي دی او ډېرو سیستمونو څخه حمایت ترسره کوي. دغه پروتوکول د SSL/TLS خدماتو د Encrypt کولو لپاره رامنځته سوي دی. SSTP پروتوکول خلاص متن نه دی، که څه په مک عامل سیستم کې شتون لري، خو د ویندوز سره هم کولای سي ښه ډول کار ترسره کړي، خو په اصل کې ددې پروتوکول کار د PPTP په نسبت ښه دی او همدارنګه د man-in-the-middle بریدونو په مقابل کې پیاوړی دی او ډېرو سیستمونو سره کار ترسره کولای سي. دغه پروتوکول د ارتباطاتو لپاره پیاوړی دی او همدارنګه د اعتماد وړ هم بلل کېږي .(SwissSign. (n.d.).

د SSTP ګټې او نیمګړتیاوې:

SSTP پروتوکول په اصل کې د مایکروسافټ کمپنۍ لخوا وړاندې کړل سوي دی، چې لویه ګټه یې همدا د بل لوري په ویندوز عامل سیستم کې په ښه ډول کار ترسره کولای سي او ډېرو سافټویرو سره یو ځای عمل کوي. د ښه امنیت او سرعت خاوند هم دی او همدارنګه په مسلسله توګه خپل خدمات وړاندې کوي. تر ټولو لویه نیمګړتیا یې دا ده چې یوازې په ویندوز کورنۍ کې ښه کار ترسره کولای سي، پیچلتیا او د کارولو تګلاره یې نورې نیمګړتیاوې دي .(SwissSign. (n.d.).

په مجازي شخصي شبکه (VPN) کې د WireGuard پروتوکول:

WireGuard پروتوکول هم نوی دی او هم یې سرعت لوړ دی. ددې پروتوکول پرمختللي Encrytpion د ډېرو توجه ځانته راګرځولې ده، خو په د VPN ډېرې ځانګړتیاوې اوس هم نه حمایت کوي، خو اټکل کېږي، چې په نیږدې راتلونکي کې دغه پروتوکول ډېرې ځانګړتیاوې حمایت کړي. دغه پروتوکول هم خلاص متن دی او کولای سو هر ډول تغیرات پکښې په آسانۍ سره راولو. له بل لوري نوی پرمختللي هم دی، خو مکمل نه دی. ځکه چې اوس مهال ځینې نیمګړتیاوې له ځانه سره لري، خو بیا هم د امنیت لرونکو پروتوکولونو څخه شمېرل کېږي .(SwissSign. (n.d.).

۱۱ شکل : په VPN کې د WireGuard پروتوکول

د مجازي شخصي شبکې (VPN) ګټې او نیمګړتیاوي:

د مجازي شخصي شبکې (VPN) ګټې:

- د ټرافیک Encrypt کول او امنیت رامنځته کول د VPN په ګټې اخستنې سره.
- د ځینو ویب سایټونو قوانین لیري کول.
- د ډیټا انتقال په غیر مستقیم ډول او په لوړ امنیت سره
- ستاسو د جغرافیاوي ساحې څخه ساتنه ترسره کول او د ویب سایټونو لخوا د نه پېژندلو امکانات برابرول.

د مجازي شخصي شبکې (VPN) نیمګړتیاوي:

- په ځینو هیوادونو کې د VPN پر استعمال بندیز.
- د VPN لوړ قیمت نسبت وړیا VPN ته.
- د VPN قطع کیدو څخه وروسته د انټرنیټ سره د ټرافیک مستقیم وصل کیدل.
- په وړیا سرورونو کې ځینې محدودیتونه او د قطع کیدو امکان (GoDaddy. (n.d.).

ولې موږ شخصي VPN جوړو؟

ددې سوال ځواب لپاره باید د VPN لاسرسي درې تګلارې په نظر کې ونیول سي، چې په لاندې ډول سره دي.

1. سرویس (خدمات) یا وړیا اپلیکیشن.
2. د سرویس اخستل.
3. د VPN جوړول په مجازي سرور کې.

لومړي وړیا اپلیکیشن ډېر مناسب نه ښکاري. ځکه چې وړیا اپلیکیشن د ځینو محدودیتونو او امنیتي ستونزو سره مخ وي. دوهم د سرویس اخستل هم د کافي امنیت خاوند دی، امنیتي ستونزې پکښې شتون لري، نو په همدې اساس موږ دا سپارښتنه کوو چې په مجازي سرور کې VPN جوړ کړل سي، تر څو امنیت لرونکي VPN سیستم ولرو.

۱۲ شکل : ولې موږ شخصی VPN جوړو؟

د مجازي شخصي شبکې (VPN) جوړلو ګټې په مجازي سرور کې:

کله چې تاسو په مجازي سرور کې VPN سیستم جوړ کړئ، تاسو به ډېرې ګټې ترلاسه کړئ، نو په دې اساس موږ هم تاسو ته دا سپارښتنه کوو، چې د VPN جوړول په مجازي سرور کې زده کړئ. ځینې ګټې یې په لاندې ډول سره دي.

د ارتباط رامنځته کولو لپاره د ځای انتخاب:

که چیرته تاسو د وړیا اپلیکیشن څخه ګټه اخلئ باید له هغه ساحې سره یو ځای سئ، چې جوړونکي مشخصي کړي دي. په ځینو سافټویرو کې د ساحې محدودیتونه هم شتون لري. که چیرته غواړئ د یوه ځانګړي هیواد سره وصل سئ نو باید ځانګړي کځوړي واخلي .GoDaddy) (n.d.).

په مسلسله توګه ارتباط:

په VPN سافټویرو کې یوه لویه ستونزه د ارتباط پر مهال محدودیت (Connection Time Out) دی، چې په ډېرو سافټویرو کې شتون لري، نو د ارتباطاتو پر مهال د قطع کیدو ستونزه ډېره ستونزمنه ده، چې ددې لپاره هم د VPN څخه ګټه اخستل کېږي، تر څو مسلسل ارتباط وړاندې کړي.

د ارتباطاتو پر مهال لوړ امنیت:

کله چې VPN سیستم په مجازي سرور کې جوړیږي د سرور او کارونکي ترمنځ معلومات (Encrypt) کېږي، چې هیڅکله د دریم ګړي لخوا د لاسرسي وړ نه دي، نو دا تر ټولو لوړه ګټه شمېرل کېږي. ځکه هیڅ هکر یا برید کونکي نه سي کولای چې ستاسو معلوماتو ته لاسرسي ولري. .(GoDaddy. (n.d.)

د مجازي شخصي شبکې (VPN) شخصي امنیت:

تر ټولو لومړي باید تاسو ددې پام ولرئ، چې د کارونکي او سرور ترمنځ ډیټا باید Encrypt سي. همدارنګه پام مو وي، چې شخصي VPN په مجازي سرور کې لکه پروکسي په شکل عمل ترسره کوي. آن د انټرنیټ خدماتو وړاندي کوونکي هم د ویب برخي له معلوماتو څخه بې خبره دی. په آخر کې مو پام وي چې تاسو دریم VPN سرور ته اړتیا نه لرئ، چې خپل معلومات شریک کړئ د نورو سره .(GlobalSign. (n.d.)

د VPN په برخه کې تر ټولو مشهوره سافټویر (اپلیکیشن):

ProtonVPN سافټویر:

دغه VPN هغه کسانو ته ډېر د اهمیت وړ دی، چې په مجازي نړۍ کې امنیت ته ډېر پام کوي. ددې شرکت اصلي سیستم په سویس هیواد کې موقیعت لري او د امنیت په برخه کې فعالیت ترسره کوي. ProtonVPN کوم محدودیت نه لري، خو تاسو کولای سئ، چې یوازي یو ډیوایس کې ترې ګټه واخلئ او د سرور انتخاب لپاره درې آپشن تاسو ته درکول کېږي. ProtonVPN د ثبت په برخه کې سخت نه دی او د کار پیل لپاره یوازي یو ایمیل آدرس ته اړتیا لیدل کېږي. په ویب سایټ کې یې هیڅ ډول تبلیغات شتون نه لري. کله چې مصرف یې ډېر سي سرعت یې کمیږي او د P2P څخه هم حمایت نه ترسره کوي. په ویندوز، مک، اندوراید او iOS کې دغه پروګرام شتون لري .(GlobalSign. (n.d.)

Hotspot Shield VPN سافټویر:

Hotspot Shield VPN د وړیا VPN په برخه کې تر ټولو بهترینه پروګرام بلل کېږي، چې په اندوراید، مک، ویندوز او iOS کې شتون لري په وړیا اپلیکیشن کې یې تاسو کولای سئ په میاشتني توګه ۵۰۰ میګابایټ ډیټا وکاروئ، چې ۱۵ ګیګابایټ کېږي او همدارنګه نوري وړتیاوي، لکه په یوه وخت کې د پنځو ډیوایسونو سره وصلیدل په یوه کلیک سره تاسو ګټه واخلئ .(Mozilla. (n.d.)

پایله

مجازی شخصي شبکه (VPN) په حقیقت کې تاسو ته دا وړتیا درکوي، چې خپل ډیوایس په انټرنیټ کې د مقابل شبکې سره په یوه امن تونل په مرسته وصل کړئ، په دې شکل چې ستاسو ډیټا به هیڅاته د لاسرسي وړ نه وي. یو ساده مثال دلته غواړم چې وړاندي کړم: د مثال په توګه تاسو پوهنتون ته کله چې داخلیږئ، نو د پوهنتون کارت به حتمي درسره وي او په کارت کې ستاسو معلومات شتون لري. که چیرته کارت نه وی درسره، نو تاسو نه سي داخلیدای. همداسي په VPN شبکه کې همدې مثال ته ورته ویلای سو، چې VPN شبکه د دوه نقطو ترمنځ یو امن تونل رامنځته کوي، چې د لاسرسي وړ نه دی. هغه معلومات چې له دې تونل څخه تیریږي یا هم انتقالیږي د اطمنیان وړ دي او په مکمل ډول Encrypt سوي دي. کله چې تاسو په مجازي سرور کې VPN سیستم جوړ کړئ تاسو به ډېرې ګټې ترلاسه کړئ، نو په دې اساس مونږ هم تاسو ته دا سپارښتنه کوو، چې د VPN جوړول په مجازي سرور کې زده کړئ. ځینې ګټې یې په لاندې ډول سره دي: د ارتباط رامنځته کولو لپاره د ځای انتخاب، په مسلسله توګه ارتباط او د ارتباطاتو پر مهال لوړ امنیت. تر ټولو لومړی باید تاسو ددې پام ولرئ، چې د کارونکي او سرور ترمنځ ډیټا باید Encrypt سي. همدارنګه پام مو وي، چې شخصي VPN په مجازي سرور کې، لکه پروکسي په شکل عمل ترسره کوي. آن د انټرنیټ خدماتو وړاندي کونکي هم د ویب برخي له

معلومات څخه بې خبره دی. په آخر کې مو پام وي چې تاسو دریم VPN سرور ته اړتیا نه لرئ، چې خپل معلومات شریک کړي د نورو سره. په عمومي توګه د شخصي VPN جوړښت لپاره یو مجازي سرور او SSH کلاینت ته اړتیا لیدل کېږي. پام مو وي چې د مجازي سرور لپاره ۱۲۸ میګابایټ رم حافظې ته اړتیا ده. که چیرته غواړئ چې با کیفیت VPN خدمات ترلاسه کړئ، نو پرمختللی مجازي سرور انتخاب کړئ، چې CentOS 6 32 یا هم ۶۴ بیټ وي. هغه کارونکي چې د مک او لینوکس عامل سیستم څخه ګټه اخلي مخکې له مخکې د کلاینټ ټرمینال سره وصل دي، خو د ویندوز کارونکي باید د لاسرسي لپاره د PuTTy سافټویر نصب کړي. د سافټویر د نصب څخه وروسته موږ مجازي سرور ته لاسرسی امکان لري او د مجازي VPN سرور کار پیلیږي، چې ټولې مرحلې باید په پوره دقت سره ترسره کړل سي.

اخځلیکونه

1. Aiken, R., Carlson, R., Foster, I., Kuhfuss, T., Stevens, R., & Winkler, L. (1997, January). *Architecture of the Multi-Modal Organizational Research and Production Heterogeneous Network (MORPHnet)*. U.S. Department of Energy.
2. DigiCert. (2021). *New DigiCert Smart Seal displays identity and improves trust with industry-first verified logos*. DigiCert. https://www.digicert.com/news/new-digicert-smart-seal-displays-identity-and-improves-trust-with-industry-first-verified-logos
3. Fortinet. (n.d.). *Benefits of VPN*. Fortinet CyberGlossary. Retrieved May 8, 2025, from https://www.fortinet.com/resources/cyberglossary/benefits-of-vpn
4. GlobalSign. (n.d.). *What is an SSL Certificate?*. GlobalSign. https://www.globalsign.com/en/ssl-information-center/what-is-an-ssl-certificate
5. GoDaddy. (n.d.). *What is an SSL certificate?*. GoDaddy. https://www.godaddy.com/help/what-is-an-ssl-certificate-611
6. Hamzeh, K., Pall, G. S., Verthein, W., Taarud, J., & Little, W. A. (1997, July). *Point-to-Point Tunneling Protocol (PPTP)* (draft-ietf-pppext-pptp-02.txt). IETF. https://datatracker.ietf.org/doc/html/draft-ietf-pppext-pptp-02
7. Hanks, S., Li, T., Farinacci, D., & Traina, P. (1994, October). *Generic Routing Encapsulation over IPv4 networks*. IETF.
8. Hanks, S., Li, T., Farinacci, D., & Traina, P. (1994, October). *RFC 1701: Generic Routing Encapsulation (GRE)*. IETF. https://datatracker.ietf.org/doc/html/rfc1701
9. Kent, S., & Atkinson, R. (1998, March). *Security Architecture for the Internet Protocol (IPSec)*. IETF. https://datatracker.ietf.org/doc/html/rfc2401
10. Luciani, J., Katz, D., Piscitello, D., Cole, B., & Doraswamy, N. (1998, February). *NBMA Next Hop Resolution Protocol (NHRP)* (draft-ietf-rolc-nhrp-15.txt). IETF.

https://datatracker.ietf.org/doc/html/draft-ietf-rolc-nhrp-15

11. Mozilla. (n.d.). *Security/Certificate Authority*. Mozilla Wiki. https://wiki.mozilla.org/CA
12. NordVPN. (n.d.). *Benefits of using a VPN*. NordVPN Blog. Retrieved May 8, 2025, from https://nordvpn.com/blog/benefits-of-vpn
13. NYM. (n.d.). *VPN tunneling explained*. NYM Blog. Retrieved May 8, 2025, from https://nym.com/blog/vpn-tunnels
14. Palo Alto Networks. (n.d.). *VPN benefits*. Cyberpedia. Retrieved May 8, 2025, from https://www.paloaltonetworks.com/cyberpedia/vpn-benefits
15. Rubens, A., Kolar, T., Littlewood, M., Townsley, W. M., Taarud, J., Pall, G. S., Palter, B., Verthein, W., Valencia, A., & Hamzeh, K. (1998, March). *Layer Two Tunneling Protocol (L2TP)* (draft-ietf-pppext-l2tp-10.txt). IETF. https://datatracker.ietf.org/doc/html/draft-ietf-pppext-l2tp-10
16. Security.org. (n.d.). *How VPN encryption works*. Retrieved May 8, 2025, from https://www.security.org/vpn/encryption
17. SwissSign. (n.d.). *Trust logo*. SwissSign AG. https://www.swisssign.com/en/trust-logo.html
18. Waitzman, D., Partridge, C., & Deering, S. (1988, November). *RFC 1075: Distance Vector Multicast Routing Protocol*. IETF. https://datatracker.ietf.org/doc/html/rfc1075
19. Webster's Revised Unabridged Dictionary. (1913). *Hypertext Webster Gateway*. https://www.webster-dictionary.org

قدیر پور، رستم (۱۳۸۱) مدل های اعتماد بر بسلتر کلید عمومی کتاب های مقالات چهارمین همایش ملی انجمن کمپیوتر کاران ایران.

Design and implementation of a secure VPN system

Khan Mohammad Wafa
Lecturer and Dean of Computer Science Faculty, Bost University
Corresponding Author Email: khanmohammad_wafa@yahoo.com

Abstract

A Virtual Private Network (VPN) essentially allows you to connect your device securely to a remote network over the internet through a secure tunnel, ensuring that your data remains inaccessible to unauthorized parties. Every research arises from a need, and the extent of that need reflects the importance of the study. Whether the research is quantitative or qualitative, it carries its own value. Therefore, I decided to conduct a comprehensive study on "Secure VPN System Design and Implementation." The main research question is: *How can we design and implement a secure VPN system?* The primary objective of this research is to understand the design and implementation of a secure VPN system. This study uses a literature review approach, including academic articles, books, and websites as key sources of information. The Internet provides vast resources on this topic. However, like any research, this one also faces limitations, such as the lack of reference books in Lashkargah city, limited internet access, and the absence of well-equipped libraries in universities.

Keywords: Virtual Network, VPN, Tunnel, Data.

BOST

Academic & Research National Journal

Volume: 4 Issue: 1

Year: 2025