بهبود امنیت و بالابردن دسترسی ipsec-vpn با استفاده از نرم افزار GNS3

چکیده

VPN ارتباط امن از راه دور برای کلاینت ها مهیا می کند تا با شبکه های شرکت ها تبادل اطلاعات داشته باشد.این مقاله به صورت SITE TO SITE IPSEC-VPN راه اندازی شده و این شبکه از پروتکل های امنیتی برای مدیریت ، مبادله کلید،احراز هویت و صداقت با استفاده از نرم افزار GNS3 پیاده سازی شده است. در این مقاله ما برای به دست اوردن تمام دسترسی در شبکه از پروتکل HSRPاستفاده میکنیم، به طوری که این پروتکل UPTIME بودن شبکه را تقریبا نزدیک به ۱۰۰ درصد می رساند و از نظر دسترسی در شبکه بهبود حاصل می شود. برای ارتباط کلاینتها هم نیاز به تانل زدن بین انها داشتیم که توسط تانل IPIP و GRE این هدف تحقق پیدا کرد و تفاوت انها نیز بیان شده است و از طریق تانل gre بهبود هایی ایجاد کردیم که در نتیجه عنوان میشه.حال برای امن کردن این تانل ها نیز از کدهای IPSEC استفاده شده و همچنین تست و تجزیه و تحلیل بسته داده ها با استفاده از دستور PING و نرم افزار wireshark انجام شده تا از رمزگذاری بسته های داده در هنگام تبادل اطلاعات بین سایت های مختلف متعلق به یک شرکت اطمینان حاصل شود و بهبودی برای ارسال امن بسته ها نیز حاصل شد.

کلمات کلیدی : احراز هویت، تانل،پروتکل،GRE،HSRP،UPTIME

۱- مقدمه

سازماندهی امنیت یکی از مهمترین مسائل در این روزها است . به نظر میرسد یک شبکه خصوصی مجازی (VPN) روشی عالی برای خدمات توزیع شده در ساختار شبکه عمومی باشد و از احراز هویت برای اطمینان از تمامیت داده ها و محرمانه بودن انها استفاده می کند.به طورکلی VPNرا میتوان با توجه به مساله امنیت، tunneling، انواع اتصال , مکانیسمهای امنیتی ، و انواع پروتکلهای ارتباطی طبقه بندی نمود و

از ویژگی های شبکه مجازی خصوصی میتوان به :

هزینه پایین , استفاده موثر از پهنای باند , مقیاس پذیر و انعطافپذیر , ارتباطات امن و خصوصی اشاره کرد..

VPNاین اتصالات بین تجهیزات شبکه را از طریق یک تانل فراهم میکند یعنی یک خط خصوصی مجازی بین دو محل شبکه ایجاد میکند که ترافیک شبکه از آن عبور میکند،اصولا از تانل پویا برای استفاده از پهنای باند کارآمد و انعطاف پذیری برای ایجاد و حذف تانل ها در هر زمان استفاده می کند و در اصل تانل در روتر ها پایه ریزی شده است و آدرسIP مسیریاب را ارایه میدهد و در انتهای تانل، درون بسته های اطلاعاتی ادرس IP مقصد گنجانده شده است و هر دو نقطه پایانی باید از یک پروتکل تانلینگ مشابه استفاده کنند. این تانل های منطقی که بسته IP را حمل می کنند مستقل از بار هستن و با توجه به پروتکل اجرا شده دارای سرصفحه های مختلف می باشند.[1]

این مقاله پروتکل های تانل زنی VPN را تجزیه و تحلیل می کند و به صورت SITE TO SITE شبکه مجازی را راه اندازی کرده و در نهایت از پروتکل IPIP و GRE برای تانل زدن استفاده میکند..بعد از انجام تانلینگ ما نیاز به برقراری امنیت در این تانلها داریم تا داده های ما به صورت امن در این مسیر رفت و امد کنند و بسته ها رمزنگاری و رمزگشایی شوند.برای این کار اومدیم از کدهای IPSEC استفاده کردیم بر روی تانل ها، که این کد

ها توانایی تضمین هر نوع فعالیت بر روی سیستمهای مبتنی بر IP مانند اینترنت را میدهند و میتواند کل مسیر بین دو عنصر را تضمین کند. و با اینکار ما امنیت شبکه رو بهبود بخشیدیم و در نهایت برای بالابردن دسترسی در شبکه و از کار نیفتادن روترها و ادامه کار انها از پروتکلی به نام HSRP استفاده نمودیم که در صورت خرابی روتر اول ،انتقال اطلاعات را به روتر دوم واگذار کرده و کارایی و اطمینان شبکه رو بالا می برد. به طوری که uptime بودن شبکه را تقریبا نزدیک به ۱۰۰ درصد می رساند. یعنی هیچ گاه دسترسی شبکه ما به شبکه مورد نظر قطع نمی شود و بهبود دسترسی پیدا کردیم نسبت به قبل.

۲- شبکه خصوصی مجازی (VPN)

VPN یک شبکه (data and speech networks) است که از زیرساخت ارتباطی عمومی و در عین حال حفظ حریم خصوصی با استفاده از پروتکل security وtunneling استفاده میکند . انرا میتوان در دو نوع مهم site to site VPNوRemote Access VPN تقسیم کرد و در حالت کلی VPNبه روشهای تانلی برای انتقال داده تکیه دارد واین پروتکلهای تانل سازی در لایه هایOSI مختلف، مانند لایه پیوند داده , لایه شبکه و یا لایه نشست کار میکنند.

رایجترین پروتکلهای مربوط به توسعه VPN در حالت SITE TO SITEپروتکل (GRE ,IPSEC,SSL) می باشد ودر حالت دسترسی از راه دور پروتکلهای (L2TP,PPTP,MPLS)هستند که این پروتکل ها رمزنگاری و رمزگشایی داده را فراهم میکنند.[1]

VPN دارای ویژگی های امنیتی زیر می باشد:

- حریم خصوصی: جلوگیری از مشاهده، تغییر و یا حذف داده ها در بسته انتقال داده شده از طریق کانال توسط کاربران واسطه
- تأیید اعتبار: تأیید می کند که بسته VPN توسط یک کاربر مجاز ارسال می شود
- یکپارچگی داده ها: اطمینان حاصل می کند که بسته های داده در حین انتقال، باقی می مانند
- ضد انتشار: جلوگیری از کپی و ارسال مجدد بسته های فرستاده شده توسط کاربر مجاز

فن آوری VPN نقش حیاتی در محیط های مختلف ارتباطی مانند کسب و کار،سازمان های نظامی، موسسات آموزشی و حتی افراد دارد.آمار نشان می دهد که ۶۳ درصد از شرکت ها از سایت به سایت VPN برای اتصال به شعبات خود استفاده می کنند که در آن ۹۰ درصد از کارکنان و ۷۹ درصد کارکنان مسافر از VPN به دسترسی از راه دور برای برقراری ارتباط با دفتر مرکزی استفاده میکنند.

SSL مبتنی بر وب مبتنی بر تکنولوژی VPN است که دارای ضعف امنیتی است،و عملکرد ضعیفی دارد و بار کاریش بالاست و از سیستم عاملهای دیگر نیز پشتیبانی نمیکند.

MPLS VPN برای راه اندازی سخت گیر است، اغلب وابسته به ارائه دهنده سرویس اینترنت (ISP) می باشد، و برای برنامه های بزرگ استفاده می شود.

از سوی دیگر، پروتکل هایی مانند GRE، IPSec، PPTP و L2TP با IPSec ارزان تر هستند و آسان تر از دیگران پیکربندی و نگهداری می شوند.[2]

۳- پروتکل IPSEC

یک معماری هست که خدمات امنیتی را برای شبکه های IP فراهم می کند و توابع احراز هویت و رمزگذاری را که می توان در شبکه های IP استفاده کرد را تعریف می کند.

رمزگذاری IPSec با استفاده از یک جفت الگوریتم رمزنگاری برای رمزگذاری و رمزگشایی داده ها صورت می گیرد.یعنی یک الگوریتم برای رمزگذاری استفاده می شود و دیگری برای رمزگشایی داده ها استفاده می شود . از چندین الگوریتم رمزگذاری می تواند پشتیبانی کند از قبیل : DES ,3DES,AES, که برای رمزگذاری و رمزگشایی داده ها استفاده می شود.

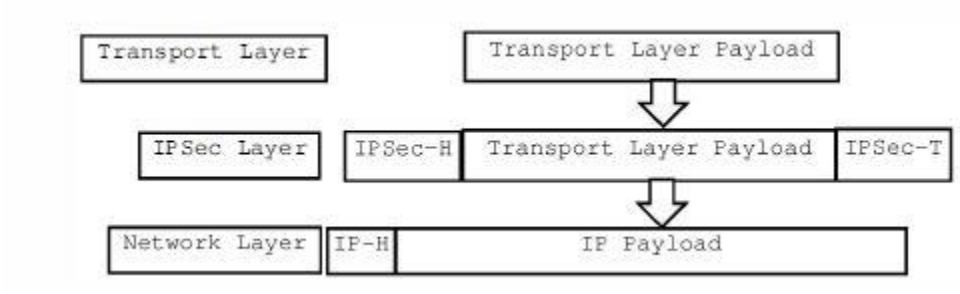
اثر AES بیشتر از DES است و حافظه بزرگتر مورد نیاز است و زمان شبیه سازی در AES در مقایسه با DES بیشتر است.[3]

این پروتکل بسیار امن تر و قابل اطمینان تر از پروتکلهای تانلینگ VPN می باشد که می تواند در هر دو سایت به VPN دسترسی پیدا کرده و REMOTE هم بزند.در اینجا تانل زنی IPSec برای ایجاد دسترسی به سایتهای VPN استفاده می شود و مجموعه ای از پروتکل ها در تانل IPSec ترکیبی است که امنیت در بسته ی لایه IP را فراهم می کند.

دو پروتکل امنیتی مانند احراز هویت (A H) و بارگیری امنیت Encapsulating Security (ESP) نیز بخشی جدایی ناپذیر از تانل IPSec هستند. در پروتکل AH ، یکپارچگی داده ها و تأیید هویت مبدأ نگهداری می شود اما این امر حریم خصوصی را تضمین نمی کند.در پروتکل ESP ،یکپارچگی داده و تأیید هویت و حریم خصوصی حفظ می شود. انجمن امنیت اینترنت (SA) یک مسئله اساسی تانل زنی در IPSec است که کانال امن بین دو طرف ایجاد می کند. پروتکل کلیدی اینترنت (IKE) پروتکل مورد نیاز برای IPSec را ایجاد می کند که کلید ها را بین طرفین مبادله می کند.

انجمن امنیت اینترنت و پروتکل مدیریت کلید (ISAKMP) چارچوبی را برای تبادل IKE و ایجاد SA و کلید رمزنگاری ارائه می دهد.

شکل ۱ فرمت بسته ی تانل IPSEC را نشان می دهد:



شکل ۱. فرمت بسته ی IPSEC

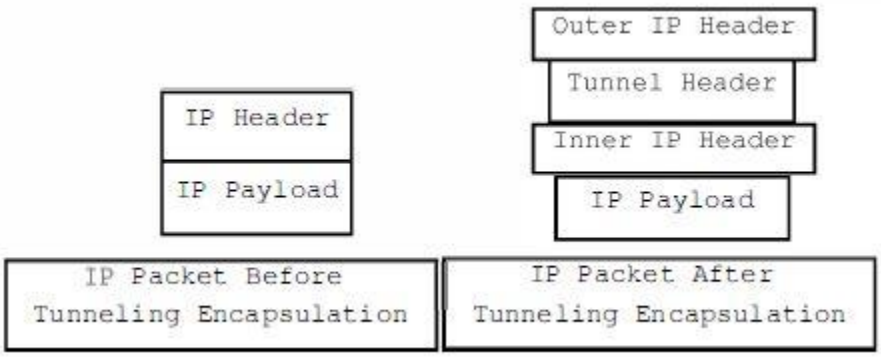
این پروتکل از دو مد تشکیل شده : ۱-مد انتقال ۲-مد تانل که در مد انتقال بار لایه حمل و نقل برای حصول اطمینان از حفاظت در IPSec کپی شده است. حالت حمل و نقل IPSec فقط پرونده اصلی را محافظت می کند،و هیچ حفظتی برای هدر IP ارائه نمی کند.در مد تانل کل بسته شامل هدر IP در حالت تانل IPSec محافظت می شود و لایه IP لایه شبکه با هدر AH یا ESP و سپس هدر اضافی محصور شده است.[5][2]

۴- پروتکل GRE

پروتکل مسیریابی عام(GRE) یک پروتکل ارتباطی است که توسط سیستمهای سیسکو ایجاد شده است که میتواند طیف گستردهای از پروتکلهای لایه شبکه را در درون یک شبکه پروتکل اینترنت به طور خلاصه بیان کند .. عمدتا این تانل برای حمل بسته های IP یا بسته های غیر IP از طریق شبکه عمومی IP استفاده می شود و به طور معمول به عنوان یک encapsulation پیچیده درپروتکل های سطح بالا استفاده می شود. این تانل

همچنین می تواند برای encapsulation با هر پروتکل لایه ۳ OSI استفاده شود. بسته های اصلی داده به سادگی در داخل هدر GRE که از حملات مختلف اینترنت محافظت می شود.

شکل ۲ بسته بندی GRE را نشان می دهد :



شکل ۲. فرمت GRE

مسیر ارتباطی مانند IPSec امن نیست زیرا GRE ویژگی های امنیتی قوی مانند رمزگذاری،احراز هویت و توالی را تولید نمی کند. این تکنیک بسیار ساده اما قدرتمند برای تانل زنی است. تانل GRE می تواند برای انجام سریع، ارتباطات قابل اعتماد و آسان از طریق شبکه عمومی مورد استفاده قرار گیرد. در تانل سایت فرستنده ، بسته داده ها توسط روترهای انتهای نقطه GRE دریافت می شود و سپس بسته با سرصفحه GRE همراه با آدرس مقصد تانل ارسال می شود، در تانل سایت گیرنده بسته های ENCAPSULE را دریافت کرده و DECAPSULE میکند و به مقصد دلخواه ارسال می کند.[2]

در کل GREبه عنوان یک مکانیزم قابل استفاده برای تانل است که از IP به عنوان پروتکل Transport استفاده می کند و می توان از آن برای حمل پروتکل های مختلف استفاده کرد تانل مانند یک لینک مجازی

Point to Pointعمل می کند که دارای دو نقطه انتهای است که توسط tunnel source و tunnel destinationدرهردوسمت آن شناسایی می شود .

یک مثال برای تانل این است که ما یک سازمان با دفتر مرکزی و چند شعبه داریم برای این سازمان می خواهیم یک پروتکل مسیریابی مانند RIP ، OSPF یا EIGRP اجرا کنیم که بین شعبه ها و دفتر مرکزی عملی مسیریابی انجام شود. لینک ارتباطی بین دفتر مرکزی و شعبه ها از چند روتر Service Provider عبور می کند. در نتیجه با توجه به اینکه برای برقراری همسایگی پروتکل های مسیریابی ذکر شده به یک ارتباط مستقیم نیاز داریم همسایگی بین روترهای دفتر مرکزی و شعبه ها برقرار نمی شود. اما استفاده از تانل این مشکل را برطرف می کند .استفاده از تانل مانند این است که یک ارتباط Point to Point بین دو دستگاه ایجاد کنیم در نتیجه دو روتر می توانند رابطه همسایگی خود را برقرار کنند GRE .یک تکنیک تانل زنی ساده است که این کار را به راحتی برای ما انجام می دهد.

۵- پروتکل HSRP

در دسترس بودن و امنیت سرویس ها عامل بسیار مهمی برای شبکه متقابل است. به منظور دستیابی به نتیجه مورد نظر،ما در حال بررسی پروتکل اول فرعی مانند (FHRP) هستیم که این پروتکل ها از قبیل : پروتکل (GLBP) پروتکل(HSRP) و پروتکل مجازی (VRRP)، می باشد. این پروتکل ها باعث اضافه کاری و قابلیت اطمینان در لایه پیوند داده ها از مدل سیستم ارتباطات (OSI) می شود و اجازه میدهند به میزبان های متعدد که یک گروه در میانشان ایجاد کنند برای توزیع بار و قرار گرفتن به صورت یک لینک مجازی.

ما نیاز به لینک های اضافی و توزیع بار در میان روترها در شبکه های اینترنت داریم،برای همین میتوان از پروتکلهایHSRP ,GLBP,VRRP استفاده کنیم. پروتکل های FHRP قادر به این هستن که اگر روتر اصلی نتواند خدماتی ارائه دهد به طور خودکار مسیر دیگری در شبکه محلی (LAN) برای مسیریابی انتخاب کنند. این پروتکل ها را می توان در شبکه طراحی شده مستقر کرد بدون اینکه هیچ گونه تغییر فیزیکی در دستگاه های ما ضروری باشد و تنها لازم است که به صورت منطقی در لایه شبکه، یک گروهی از روترها را ایجاد کنیم و یک پروتکل مجازی (VIP) به انها اختصاص دهیم و DEGFAULT GETWAY کلاینتهارا به اینها دهیم.

پروتکل Routing Hot Standby (HSRP) HOT یک پروتکل اختصاصی سیسکو است که برای ایجاد یک دروازه پیش فرض برطرف کننده خطا ازش استفاده میشه. HSRP در دروازه پیش فرض ،تضمین میکنه که سریع به رفع خطا می پردازد که کمتر از ۱۰ ثانیه هم طول می کشد تا مسیر پیش فرض مسیر دیگری را در یک گروه مشابه تغییر دهد.[4]

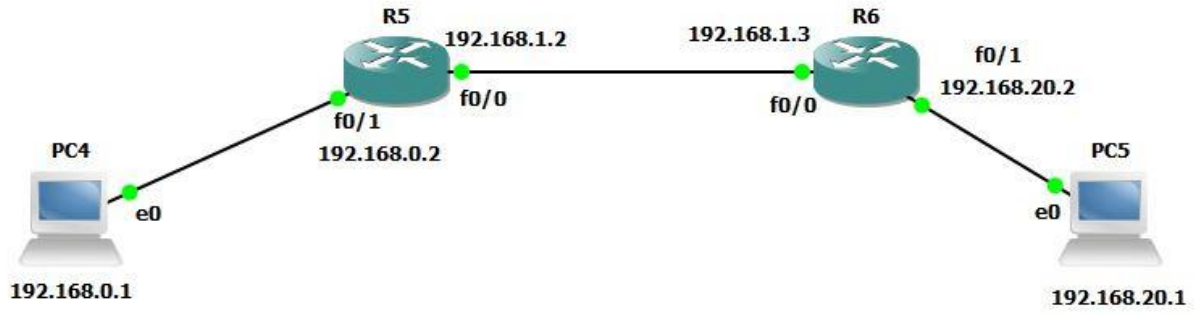
۶- تانل IPIP

در این نوع تانل از هیچ نوع فشرده سازی و کد گزاری استفاده نمیشود بلکه تنها یک header به پکت مربوطه اضافه شده و در مقصد برداشته میشود.لازم به ذکر است که استاندارد این نوع تانل متعلق به شرکت Cisco System میباشد که بعضی روتر های دیگر نظیر Mikrotik نیز از آن پیروی میکنند.

۷- پیاده سازی **تانل IPIP**

ما در این مقاله اول یک سناریو کوچک رو با استفاده از تانل IPIP پیاده کردیم که ویژگی های تانل GRE را ندارد و دارای محدودیتهای امنیتی و غیره می باشد که بعدا با تانل GRE بهبود درش حاصل کردیم و گام به گام سناریو رو گسترش دادیم و امنیت در شبکه برقرار کردیم.

شکل ۳ سناریو برای تانل IPIP می باشد



شکل ۳. تانل IPIP

در اینجا ما دوتا روتر داریم که دوتا کلاینت به ان متصل هستن.حال برای اینکه بتونیم ارتباط بین کامپیوتر ۴و۵ رو برقرار کنیم باید ابتدا IP هارو تنظیم کنیم در شبکه و سپس یک تانل بین دو روتر بزنیم که زمینه را برای برقراری ارتباط کلاینتها فراهم کند و پکت از این مسیر عبور کند.

تنظیمات انجام شده در روتر ۶ به صورت شکل ۴ نشان داده شده است:

```
R6
interface Tunnel0
 ip address 172.16.0.2 255.255.0.0
 tunnel source 192.168.1.3
 tunnel mode ipip
 tunnel destination 192.168.1.2
!
interface FastEthernet0/0
 ip address 192.168.1.3 255.255.255.0
 speed auto
 duplex auto
!
interface FastEthernet0/1
 ip address 192.168.20.2 255.255.255.0
 speed auto
 duplex auto
!
ip forward-protocol nd
!
!
no ip http server
no ip http secure-server
```

شکل ۴. تنظیمات روتر و تانل IPIP

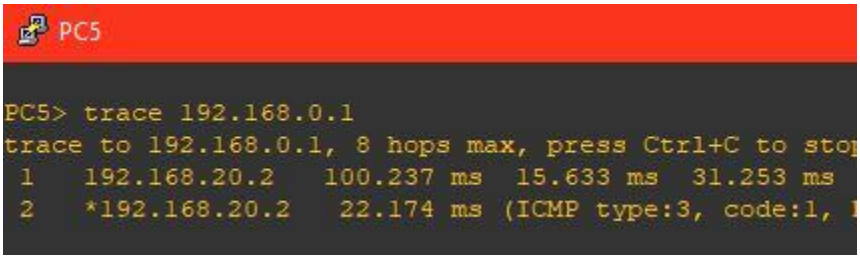
بعد از اینکه تنظیمات انجام شد نوبت به تست ارتباط بین کلاینها می باشد تا ببینیم ارتباط دارن یا خیر برای اینکار از دستور PING استفاده میکنیم که در صورت برقراری ارتباط ۵ رپلای داده میشود.اینکار .در شکل ۵ نشان داده شده:

```
PC5
PC5> ping 192.168.0.1
*192.168.20.2 icmp_seq=1 ttl=255 time=15.615 ms
*192.168.20.2 icmp_seq=2 ttl=255 time=46.843 ms
*192.168.20.2 icmp_seq=3 ttl=255 time=15.607 ms
*192.168.20.2 icmp_seq=4 ttl=255 time=22.160 ms
*192.168.20.2 icmp_seq=5 ttl=255 time=15.625 ms

PC5>
```

شکل ۵ . تست ارتباط از سمت کلاینت ۵ با کلاینت ۴

حال نوبت به این میرسه که ببینیم تانلی که زدیم کار میکنه یا خیر؟ در شکل ۶ نشان داده شده. برای همین از دستور TRACE استفاه میکنیم و ای پی مقصد رو میدیم تا ببینیم مسیر عبوری از کجاست؟با توجه به شکل از کلاینت ۵ بسته ما حرکت کرده و وارد روتر ۶ شده و درون تانل قرار گرفته و به دست کلاینت ۴ رسیده.

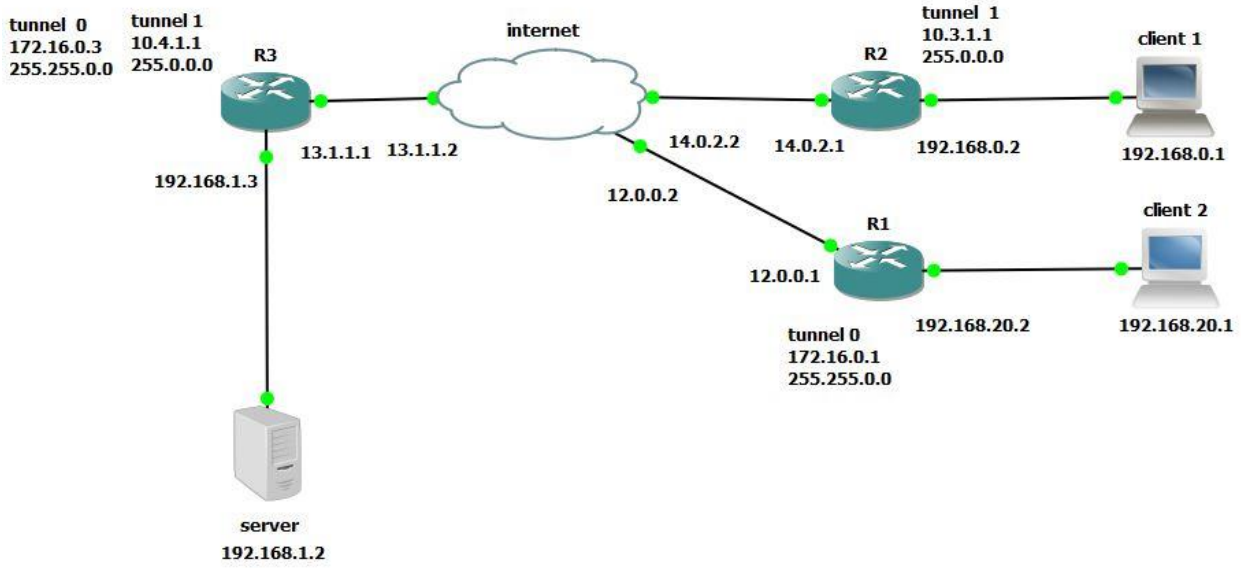


شکل ۶. تست مسیریابی تانل IPIP

در اخر نتایج رو بررسی میکنیم و شاهد و بهبود عملکرد سیستم خواهیم بود.

۸-پیاده سازی تانل GRE,IPSEC

ما در این قسمت میخواییم بسته هایی که بین کلاینت و سرور و کلاینت و کلاینت جابه جا میشود رمزنگاری و رمزگشای شود و امنیت شبکه ما بالابره و هرکسی اجازه دسترسی به بسته ها و تغییرات اونهارو نداشته باشه.برای برقراری امنیت لازم هست که پس از اتصال اجزا مانند شکل ۷ , آدرس IP را برای هر اترنت سریع پیکربندی کردیم .



شکل ۷. پیاده سازی IPSEC ,GRE

مولفه اینترنت ما در اصل یک روتر است و ما فقط نماد را برای یک ابر عوض کرده ایم و آن را اینترنت نامگذاری کردیم که این شبیه سازی اینترنت به ما کمک میکند تا راحتتر عمل کنیم و اگر روتری نمیدونست مقصد بسته کحاست به اینترنت میفرسته و از اینترنت به دست گیرنده واقعی میرسه. IP های موجود در این سناریو شامل 2 نوع , خصوصی و عمومی است.

IP هایی مانند13.1.1.1 که برای روتر۳ ما پیکربندی شده است , عمومی هستند , اما IP های کلاینت و سرور مانند 192.168.20.2خصوصی هستند . تفاوتشون در اینه که سمت اینترنت ما با IP PUBLIC کار میکنیم.حال ما باید واسطهایی را در بخش اینترنتی خود پیکربندی کنیم و اجازه دهیم که بداند کدام اجزا به آن متصل هستند , در اینجا دارای سه اترنت سریع است که روتر ها را به آن متصل میکند . وقتی مسیریابها میخواهند بسته ها را ارسال کنند اگر مقصد ناشناخته

باشد , ما یک IP ROUTE را برای روتر ها تعریف میکنیم تا بسته ها را به اینترنت ارسال کنیم و سپس اینترنت آن را برای سرور ارسال خواهد کرد که هیچ بستهای از بین نخواهد رفت . در حال حاضر باید اطمینان حاصل کنیم که همه اتصالات به طور کامل کار میکنند , اطمینان حاصل کنیم که آیا امکان ارسال یک بسته از مشتریان به سرور وجود دارد , بنابراین لازم است که ما یک تانل بین روتر ها داشته باشیم . در اینجا دو تانل ایجاد کردیم , تانل 0 که نقطه شروع آن R1 و نقطه پایانی R3 است . همچنین تانل 1 که نقطه شروع R2 و نقطه پایانی R3 است.این تانلها از نوع , GRE بوده و برای اتصال مشتریان و سرور به ارسال و دریافت بسته ها لازم است . اکنون با داشتن این تانلها , ما به راحتی میتوانیم تجهیزات را پینگ کرده و از اتصال مناسب بین مشتریان و سرور مطمئن شویم. حال کدهای مربوط به تنظیم تانل GRE در روتر۳ را در شکل ۸ نشان میدهیم:

```
Int f0/0
Ip add 192.168.1.2 255.255.255.0
Int f0/1
Ip add 13.1.1.1 255.0.0.0
Ip route 0.0.0.0
0.0.0.0 13.1.1.2
Int tunnel 0
Ip add 172.16.0.3 255.255.0.0
Tunnel source f0/1
Tunnel des 12.0.0.1
Tunnel mode gre ip
Do sh run int tun 0
Access-list 117 permit gre host 13.1.1.1 host
12.0.0.1
Router eigrp 10
Network 192.168.0.0
Network 172.16.0.3
No auto-summary
Exit
```

شکل ۸. تنظیمات تانل GRE بر روی روتر ۳

حالا برای اینکه این تانل امن بشه لازم هست که کدهای IPSEC رو در این تانل بزنیم تا بسته ها رمز گذاری شوند.شکل ۹ تنظیمات لازم بر روی روتر ۱ رو نشون میده:

```
Crypto isakmp policy 10
  encr aes 256
 authentication pre-share
  group 5
Crypto isakmp key cisco address 13.1.1.1
Crypto isakmp keep alive 10
!
!
Crypto ipsec transform-set esp-aes 256 esp-sha-
hmac
!
Crypto map cmap 10 ipsec-isakmp
  set peer 13.1.1.1
  set transform-set esp-aes256-sha
  match address 121
!
```

شکل ۹. تنظیم کد IPSEC

حال به تست این سناریو میپردازیم و ارتباط بین کلاینت و سرور را در شکل ۱۰ نسان میدهیم که اتصال برقرار است:

```
client 1

VPCS> ping 192.168.1.2
84 bytes from 192.168.1.2 icmp_seq=1 ttl=62 time=100.266 ms
84 bytes from 192.168.1.2 icmp_seq=2 ttl=62 time=100.261 ms
84 bytes from 192.168.1.2 icmp_seq=3 ttl=62 time=84.640 ms
84 bytes from 192.168.1.2 icmp_seq=4 ttl=62 time=100.264 ms
84 bytes from 192.168.1.2 icmp_seq=5 ttl=62 time=100.261 ms
```

شکل ۱۰. PING و تست گرفتن بین کلاینت و سرور

همانطور که در شکل ۱۱ نشان داده شده ، ما تست میکنیم که بسته های ارسالی ما رمزنگاری و رمزگشایی میشوند یا خیر؟ که با توجه به مقدار CAPSULE و ENCAPSULE متوجه صحت این موضوع میشویم و اینکه نشان میده کدهای IPSEC در این روتر تنظیم شده است.

```
R1
R1#show crypto ipsec sa

interface: Tunnel0
    Crypto map tag: Tunnel0-head-0, local addr 12.0.0.1

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (12.0.0.1/255.255.255.255/47/0)
   remote ident (addr/mask/prot/port): (13.1.1.1/255.255.255.255/47/0)
   current_peer 13.1.1.1 port 500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 219, #pkts encrypt: 219, #pkts digest: 219
    #pkts decaps: 287, #pkts decrypt: 287, #pkts verify: 287
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0

     local crypto endpt.: 12.0.0.1, remote crypto endpt.: 13.1.1.1
     path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet0/1
     current outbound spi: 0x260965EB(638150123)
     PFS (Y/N): N, DH group: none

     inbound esp sas:
      spi: 0x22AEA429(581870633)
        transform: esp-3des esp-sha-hmac ,
        in use settings ={Transport, }
        conn id: 1, flow_id: 1, sibling_flags 80000000, crypto map: Tunnel0-head-0
        sa timing: remaining key lifetime (k/sec): (4363553/2752)
        IV size: 8 bytes
        replay detection support: Y
        Status: ACTIVE(ACTIVE)
      spi: 0x15620EF(22421743)
        transform: esp-3des esp-sha-hmac ,
        in use settings ={Transport, }
        conn id: 3, flow_id: 3, sibling_flags 80004000, crypto map: Tunnel0-head-0
        sa timing: remaining key lifetime (k/sec): (4312861/2756)
        IV size: 8 bytes
        replay detection support: Y
        Status: ACTIVE(ACTIVE)
```

شکل ۱۱. تست رمزنگاری و رمزگشایی داده ها

در شکل ۱۲ مجموع رمزنگاری و رمزگشایی ها نشان داده شده و معلوم میشه از چه الگوریتمی برای رمز نگاری استفاده شده است.

```
R1#show crypto engine connection active
Crypto Engine Connections

   ID  Type    Algorithm          Encrypt  Decrypt LastSeqN IP-Address
    1  IPsec   3DES+SHA                 0        9        9 12.0.0.1
    2  IPsec   3DES+SHA                 9        0        0 12.0.0.1
    3  IPsec   3DES+SHA                 0      156      156 12.0.0.1
    4  IPsec   3DES+SHA                87        0        0 12.0.0.1
 1001  IKE     MD5+3DES                 0        0        0 12.0.0.1
 1002  IKE     MD5+3DES                 0        0        0 12.0.0.1
```

شکل ۱۲. تست مجموع رمزنگاری ها و الگوریتم مورد استفاده

همانند تستی که در تانل IPIP گرفیتم در شکل ۱۳ هم تست میکنیم که بسته ارسالی ما از کجا عبور میکند و درون تانل قرلر میگیرد یا خیر؟که نشان داده شده از از روتر ۲گذشته و داخل تانل شده و به سرور رسیده بسته.

client 1

```
VPCS> trace 192.168.1.2
trace to 192.168.1.2, 8 hops max, press Ctrl+C to stop
 1   192.168.0.2   15.622 ms  15.625 ms  15.627 ms
 2   10.4.1.1   84.642 ms  84.639 ms  84.638 ms
 3   *192.168.1.2   84.639 ms (ICMP type:3, code:3, Destination port unreachable)
```

شکل ۱۳. تست مسیریابی تانل GRE

در شکل ۱۴ نشان داده شده که ISAKMP فعال هست و این ارتباط امن بین کدام روترها با چه مبدا و مقصدی برقراره؟

```
R1#show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id status
13.1.1.1        12.0.0.1        QM_IDLE           1002 ACTIVE
12.0.0.1        13.1.1.1        QM_IDLE           1001 ACTIVE

IPv6 Crypto ISAKMP SA
```

شکل ۱۴. تست ISAKMP POLICY

و در نهایت در شکل ۱۵ با نرم افزار wireshark نشان دادیم که رمزنگاری رو بسته ها صورت گرفته و از پروتکل esp استفاده شده و در پایین شکل هم بسته ها رمز شده اند.

Capturing from Standard input

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
21	17.993605	13.1.1.1	12.0.0.1	ESP	158	ESP (SPI=0x015620ef)
22	17.993605	13.1.1.1	12.0.0.1	ESP	158	ESP (SPI=0x015620ef)
23	18.410275	12.0.0.1	13.1.1.1	ESP	134	ESP (SPI=0x260965eb)
24	18.964978	12.0.0.1	13.1.1.1	ESP	158	ESP (SPI=0x260965eb)
25	18.996226	13.1.1.1	12.0.0.1	ESP	158	ESP (SPI=0x015620ef)

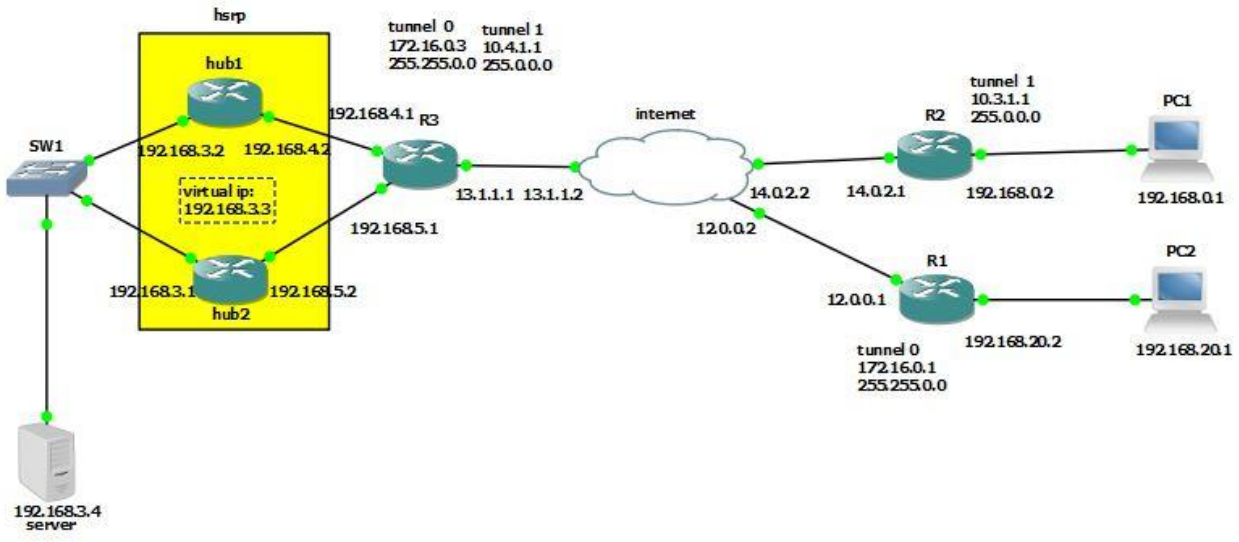
```
> Frame 1: 134 bytes on wire (1072 bits), 134 bytes captured (1072 bits) on interface 0
> Ethernet II, Src: ca:09:19:6c:00:1c (ca:09:19:6c:00:1c), Dst: ca:08:37:60:00:06 (ca:08:37:60:00:06)
> Internet Protocol Version 4, Src: 12.0.0.1, Dst: 13.1.1.1
> Encapsulating Security Payload
```

```
0000  ca 08 37 60 00 06 ca 09  19 6c 00 1c 08 00 45 c0   ··7`···· ·l····E·
0010  00 78 00 9e 00 00 fe 32  a0 f3 0c 00 00 01 0d 01   ·x·····2 ........
0020  01 01 26 09 65 eb 00 00  00 96 41 4b b8 9e 88 29   ··&·e··· ··AK···)
0030  04 f6 53 71 9c a4 98 10  06 fd 81 2b 11 53 d3 6b   ··Sq···· ···+·S·k
0040  e2 21 cd 45 6c fa 43 e8  b5 d5 74 79 20 bb 36 62   ·!·El·C· ··ty ·6b
0050  69 2d a8 5f b6 7a f1 0e  7d 90 dd 07 99 e3 0d 04   i-·_·z·· }·......
0060  58 73 fe 67 59 d6 74 d0  8a 86 1e 37 3c 5f b9 70   Xs·gY·t· ···7<_·p
0070  ea 51 4a 67 6e 9f 9e 92  33 30 40 65 ba 87 d1 50   ·QJgn··· 30@e···P
```

شکل ۱۵. تست ipsec با wireshark

۹- پیاده سازی HSRP

حالا ما تمامی کارهای لازم بابت رمزنگاری و رمزگشایی و بهبود امنیت رو انجام دادیم .نوبت به این میرسه که دسترسی و بهبود بدیم و جلوگیری کنیم از اینکه اگر یه هاب از کار بیفته کل شبکه مختل بشه و با اینکار کارایی شبکه رو هم افزایش دادیم و به نوعی امنش کردیم در مقابل خرابی و قطعی روترها.پس به نسبت قبل سناریو رو گسترش میدیم و به ان هاب های HSRP را اضافه می کنیم. در شکل ۱۶



شکل ۱۶. پیاده سازی HSRP

در این سناریو ما همه ی کارهای قبلی و انجام دادیم بجز استفاده از تانل IPIP، و حالا لازمه که در هاب ۱و۲ دستورات HSRP رو بزنیم و هاب ۱ رو به عنوان هاب ACTIVE در نظر بگیریم.یعنی اولویت اول برای مسیریابی و میذاریم از هاب۱ بگذره.و اگر این هاب به مشکل خورد در عرض چندثانیه هاب ۲ جایگزین بشه و بسته ها از هاب ۲ به سرور برسن و بالعکس. نحوه ی کار HSRP بدین شکل است که با اجرای این پروتکل روتر ها در یک

گروه قرار میگیرد که این گروه را روتر مجازی می نامیم . توجه داشته باشید که IP این روتر مجازی را که virtual ip می نامیم ، باید به عنوانDefault gateway به station های شبکه خودمان بدهیم . طبق شکل ۱۷ تنظیمات در روتر ۱ به این صورت می باشد و IPمجازی ما شمارش 192.168.3.3 می باشد:

```
hub1
interface FastEthernet0/0
 ip address 192.168.4.2 255.255.255.0
 speed auto
 duplex auto
!
interface FastEthernet0/1
 ip address 192.168.3.2 255.255.255.0
 standby 1 ip 192.168.3.3
 standby 1 priority 105
 standby 1 preempt
 standby 1 track 1 decrement 10
 speed auto
 duplex auto
!
ip forward-protocol nd
!
!
no ip http server
no ip http secure-server
ip route 0.0.0.0 0.0.0.0 192.168.4.1
!
!
!
```

شکل ۱۷. تنظیمات HSRP در هاب ۱

بر اساس شکل ۱۸ وضعیت active ,standby بودن روتر ها به نمایش گذاشته میشه و نشون میده ترافیک واقعا بر دوش هاب۱ می باشد:

```
hub1
hub1#show standby br
                    P indicates configured to preempt.
                    |
Interface   Grp  Pri P State   Active          Standby         Virtual IP
Fa0/1       1    105 P Active  local           192.168.3.1     192.168.3.3
hub1#
hub1#
```

شکل ۱۸. وضعیت active ,standby

ما میتونیم یکی از پورتهای متصل به هاب ۱ رو خاموش کنیم ،در اینصورت اگه دوباره دستور قبل و تکرار کنیم نتیجه به این صورت میشه که هاب ۱ به حالت standby میره و هاب ۲ active میشه.شکل ۱۹ نشان دهنده این وضعیت می باشد.

```
hub1#show standby br
                    P indicates configured to preempt.
                    |
Interface   Grp  Pri P State   Active          Standby         Virtual IP
Fa0/1       1    95  P Standby 192.168.3.1     local           192.168.3.3
```

شکل ۱۹. تغییر وضعیت هاب ۱

۱۰- نتیجه گیری

با توجه به پیاده سازی های انجام شده و تست های گرفته شده، ما به این نتیجه رسیدیم که تانل IPIP یک تانل ساده و پیش پا افتاده است که امکان رمزنگاری اطلاعات و فشرده سازی بسته ها را در خودش ندارد و نمیتوان ان را گسترش داد و پارامترهای بیشتری را درش لحاظ کرد.برای همین اومدیم از تانل GREاستفاده

کردیم برای بهبود تانل به روش قبلی و با استفاده از GRE امکانات زیادی شامل حال شبکه ما شده و بهبودهایی از نظر :

۱- می تواند پروتکل های مختلف لایه شبکه را در داخل یک لینک Point to Point روی بستر IP کپسوله کند. تانل Generic Routing Encapsulation (GRE) همانطور که از نامش پیداست می تواند تقریبا هر نوع دیتایی را encapsulate کرده و آنرا روی اینترفیس های فیزیکی روتر ارسال کند. در واقع GRE می تواند انواع پروتکل های لایه ۳ را encapsulate کند که باعث می شود GRE بسیار انعطاف پذیر شود.برخلاف تانل IPIP

۲- بسته های GRE را می توان روی یک IPsec VPN ارسال کرد که باعث می شود بسته های GRE به صورت امن ارسال شوند.برخلاف IPIP

۳- IPSEC تنها می تواند از بسته های unicast حفاظت کند.اما وقتی از تانل GRE استفاده بشه ،می تواند بسته های IP Multicast را encapsulate کند. در نتیجه بسته های unicast و multicast توسط تانل GRE کپسوله می شوند و همچنین بسته های unicast توسط تانل IPsec محافظت می شوند.

۴- تانل GRE اجازه برقراری VPN را روی شبکه های WAN را می دهد.

۵- راه حلی برای شبکه هایی که از پروتکل هایی که محدودیت تعداد hop دارند مانند پروتکل RIP

۶- تانل GRE امکان انتقال ترافیک IPv6 را علاوه بر IPV4 دارد.که در IPIP شاهد همچین مزایایی نبودیم و بعد از استفاده از GRE این بهبودها حاصل شد.به طور مثال در این تست شاهد استفاده از IPV6 هستیم :

```
R1#show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id status
13.1.1.1        12.0.0.1        QM_IDLE           1002 ACTIVE
12.0.0.1        13.1.1.1        QM_IDLE           1001 ACTIVE

IPv6 Crypto ISAKMP SA
```

بهبود بعدی که رو کل شبکه ما حاصل شد ،استفاده از پروتکل HSRP بود. یعنی با این پروتکلی که استفاده کردیم هیچ گاه دسترسی شبکه ما به شبکه مورد نظر قطع نمی شود. همانطور که می دانید برای دسترسی به شبکه ای دیگر نیاز به روتر داریم. اگر این روتر به هر دلیلی ارتباطش با ما یا با شبکه مقصد قطع شود دسترسی به شبکه نداریم. اینجاست که اهمیت پروتکلHSRP مشخص می شود. و ماهم بجای یک روتر از دو روتر برای اتصال و دسترسی به شبکه ی مورد نظر استفاده کردیم تا به محض قطع شدن و از دسترس خارج شدن روتر اولیه ، روتر بعدی active شود. بحث دیگه ای که وجود دارد این است که HSRP باعث به وجود آمدن افزونگی(Redundancy) در ip networks و دستگاه روتر می شود . با استفاده از این افزونگی می توان ویژگی high availability را به وجود آورد .حالا ما با تستی که در قسمت پیاده سازی HSRP در شکل ۱۸و۱۹ انجام دادیم شاهد این HIGH AVALABILITY دز شبکه بودیم یعنی هاب ۱ رو پورتش رو قطع کردیم و بسته ارسال کردیم.بعد شاهد این بودیم که هاب ۱ از وضعیت ACTIVE به STANDBY رفت و هاب۲ سریعا جایگزین شد تا شبکه مختل نشه و این بهبود در کل شبکه ما را نشان می دهد.

منابع

[1] Fatimah Abdulnabi Salman, Implementation of IPsec-VPN Tunneling using GNS3, Indonesian Journal of Electrical Engineering and Computer Science, ijeecs, September 2017, 855 ~ 860

[2] Sohety Jahan, Md. Saifur Rahman, Sajeeb Saha, Application Specific Tunneling Protocol Selection for Virtual Private NetworkS, Department of Computer Science and Engineering Jagannath University,IEEE, January 2017

[3] Dnyanesh Deshmukh and Brijesh Iyer, Design of IPSec Virtual Private Network For Remote Access, IEEE,2017

[4] Mohammad Hamid Ibrahimi, Komil B. Vora, Kunal Khimani, Deploy Redundancy of Internet using First Hop Redundancy Protocol and Monitoring it using IP Service Level Agreements,IGESC,2017

[5] Engr. Maria Abdullah† and Najeed Ahmed Khan††, Shariq Mahmood Khan††, Domineering Analysis & Mitigation of IP-SEC VPN Using GNS3, IJCSNS,2017