باسمه تعالی

درس: آزمایشگاه امنیت شبکه

نام و نام خانوادگی: تینا توکلی

شماره دانشجویی: 9922762220

شماره تمرین :06

---

1. انواع شبکه‌های خصوصی مجازی (VPN)

انواع مختلفی از VPN ها وجود دارد که هر کدام مزایا و معایب خاص خود را دارند. رایج ترین انواع VPN ها عبارتند از:

1. VPN های نقطه به نقطه (Point-to-Point VPN):

این نوع VPN ساده ترین نوع VPN است و برای اتصال دو نقطه مانند دو دفتر یا یک کامپیوتر به یک شبکه استفاده می شود. پیاده سازی VPN های نقطه به نقطه به طور معمول آسان است و به تجهیزات تخصصی کمی نیاز دارد.

نحوه پیاده سازی:

- برای راه اندازی VPN نقطه به نقطه، به یک روتر یا مودم در هر دو انتهای اتصال نیاز دارید.
- هر روتر یا مودم باید برای استفاده از پروتکل VPN مانند PPTP یا L2TP پیکربندی شود.
- آدرس IP و اطلاعات دیگر را برای هر اتصال VPN پیکربندی کنید.

2. VPN های دسترسی از راه دور (Remote Access VPN):

این نوع VPN به کاربران از راه دور اجازه می دهد تا به طور امن به شبکه شرکتی خود متصل شوند. VPN های دسترسی از راه دور به طور معمول توسط شرکت ها برای ارائه دسترسی به کارمندان دورکار، پیمانکاران و شرکا استفاده می شود.

نحوه پیاده سازی:

- برای راه اندازی VPN دسترسی از راه دور، به یک سرور VPN در شبکه شرکتی خود نیاز دارید.
- سرور VPN باید برای استفاده از پروتکل VPN مانند PPTP، L2TP یا OpenVPN پیکربندی شود.
- کاربران از راه دور باید برای اتصال به سرور VPN، نرم افزار VPN را روی رایانه های خود نصب کنند.

3. VPN های مبتنی بر وب (Web-Based VPN):

این نوع VPN به کاربران اجازه می دهد تا با استفاده از مرورگر وب خود به شبکه شرکتی خود متصل شوند. VPN های مبتنی بر وب نیازی به نصب نرم افزار VPN روی رایانه های کاربران ندارند، که آنها را به گزینه ای آسان برای استفاده تبدیل می کند.

نحوه پیاده سازی:

- برای راه اندازی VPN مبتنی بر وب، به یک پورتال وب VPN در شبکه شرکتی خود نیاز دارید.
- پورتال وب VPN باید برای استفاده از پروتکل VPN مانند SSL یا OpenVPN پیکربندی شود.
- کاربران برای اتصال به شبکه شرکتی خود، به سادگی باید به پورتال وب VPN در مرورگر وب خود مراجعه کنند.

4. VPN های Site-to-Site:

این نوع VPN دو شبکه کامل را به هم متصل می کند، مانند دو دفتر یا یک شبکه شرکتی و یک شبکه ابری. VPN های Site-to-Site به طور معمول توسط شرکت ها برای اتصال چندین مکان یا برای گسترش شبکه های خود به ابر استفاده می شود.

نحوه پیاده سازی:

- برای راه اندازی VPN Site-to-Site، به یک روتر یا فایروال در هر دو شبکه ای که می خواهید متصل کنید نیاز دارید.
- هر روتر یا فایروال باید برای استفاده از پروتکل VPN مانند IPSec یا OpenVPN پیکربندی شود.
- آدرس IP و اطلاعات دیگر را برای هر اتصال VPN پیکربندی کنید.

5. VPN های مش (Mesh VPN):

این نوع VPN شبکه ای از دستگاه های VPN را ایجاد می کند که با یکدیگر ارتباط برقرار می کنند. VPN های مش به طور معمول برای ارائه دسترسی به اینترنت امن و قابل اعتماد استفاده می شود.

نحوه پیاده سازی:

- برای راه اندازی VPN Mesh، به چندین دستگاه VPN مانند روتر یا مودم نیاز دارید.
- هر دستگاه VPN باید برای استفاده از پروتکل VPN مانند OpenVPN یا WireGuard پیکربندی شود.
- دستگاه های VPN را طوری پیکربندی کنید که با یکدیگر ارتباط برقرار کنند و شبکه مش را تشکیل دهند.

2. تفاوت بین IPSec و GRE

IPSec (Internet Protocol Security) و **GRE** (Generic Routing Encapsulation) دو پروتکل شبکه هستند که برای انتقال داده ها از طریق شبکه های IP استفاده می شوند. تفاوت های کلیدی بین این دو پروتکل وجود دارد:

هدف:

- **IPSec:** یک پروتکل امنیتی است که برای رمزگذاری و احراز هویت ترافیک IP استفاده می شود. این پروتکل برای محافظت از داده ها در برابر شنود و دستکاری طراحی شده است.
- **GRE:** یک پروتکل تونل سازی است که برای انتقال بسته های IP از طریق شبکه های IP دیگر استفاده می شود. این پروتکل برای گسترش شبکه های IP یا اتصال شبکه های جداگانه استفاده می شود.

امنیت:

- **IPSec:** یک پروتکل امن است که از رمزگذاری و احراز هویت برای محافظت از داده ها استفاده می کند.
- **GRE:** یک پروتکل ناامن است که هیچ امنیتی ارائه نمی دهد. داده های منتقل شده از طریق تونل GRE می توانند توسط هر کسی که به شبکه دسترسی دارد، شنود و دستکاری شوند.

کاربرد:

- **IPSec:** به طور معمول برای VPN ها، ارتباطات نقطه به نقطه و سایر برنامه هایی که نیاز به امنیت بالایی دارند استفاده می شود.
- **GRE:** به طور معمول برای تونل سازی IP، اتصال شبکه های جداگانه و سایر برنامه هایی که نیاز به امنیت بالایی ندارند استفاده می شود.

پروتکل های زیربنایی:

- **IPSec:** می تواند بر روی IPv4 و IPv6 اجرا شود.
- **GRE:** می تواند بر روی IPv4 و IPv6 اجرا شود.

مقایسه:

ویژگی	IPSec	GRE
هدف	امنیت	تونل سازی
امنیت	امن	ناامن
کاربرد	VPN ها، ارتباطات نقطه به نقطه	تونل سازی IP، اتصال شبکه های جداگانه
پروتکل های زیربنایی	IPv6 ،IPv4	IPv6 ،IPv4

توپولوژی:

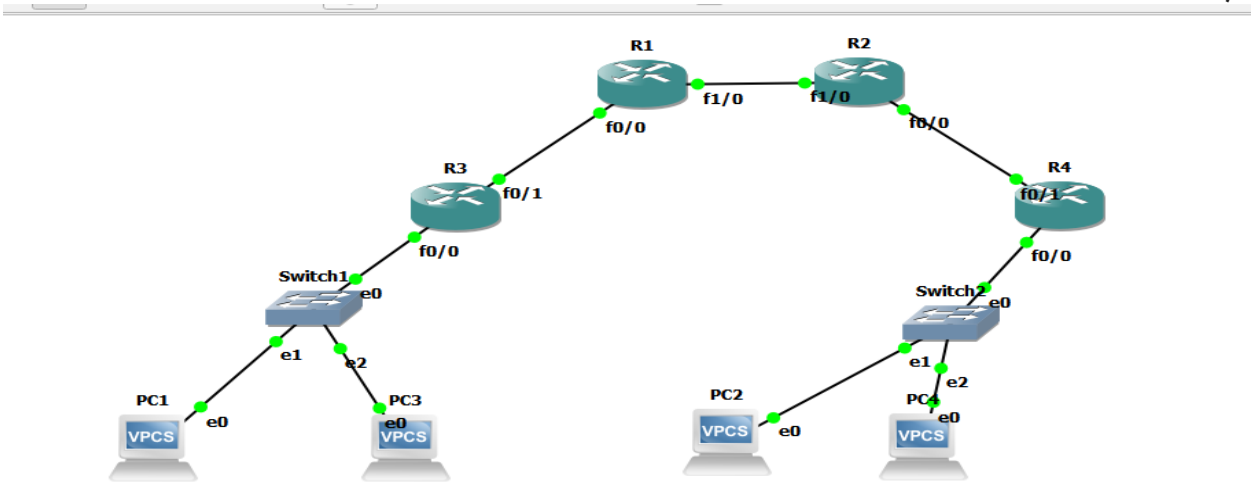

Figure 1-حالت tunnle بین R3,R4

تنظیمات روتر ها و ... همه مانند فعالیت کلاسی است و تنها تفاوت در تنظیم IPها در پایین آمده:

Pc1: ip 192.168.1.1/24 192.168.1.2

Pc3: ip 192.168.1.3/24 192.168.1.2

Pc2: ip 192.168.2.1/24 192.168.2.2

Pc4: ip 192.168.2.4/24 192.168.2.2

3. Site to Site VPN Between Cisco Routers:

این نوع VPN به شما امکان می دهد دو شبکه خصوصی را از طریق اینترنت به هم متصل کنید .این کار با ایجاد یک تونل رمزگذاری شده بین دو روتر انجام می شود .تمام ترافیک بین دو شبکه از طریق این تونل عبور می کند و از آن محافظت می شود.

مزایا:

- امنیت :ترافیک بین دو شبکه را رمزگذاری می کند و از آن در برابر هکرها محافظت می کند.
- حریم خصوصی :از داده های حساس شما در برابر رهگیری و نظارت محافظت می کند.
- کاهش هزینه ها :می توانید از خطوط اختصاصی گران قیمت اجتناب کنید.

مراحل:

- ایجاد توپولوژی: در GNS3، دو روتر و دو شبکه را راه اندازی کنید.
- **تنظیم روترها:**

رابط های روترها را پیکربندی کنید.

پروتکل مسیریابی (مانند BGP یا OSPF) را بین روترها پیکربندی کنید.

مسیرهای لازم برای رسیدن به شبکه دیگر را اضافه کنید.

- **تنظیم شبکه ها:**

آدرس های IP و subnet mask های شبکه ها را پیکربندی کنید.

پیاده سازی:

برای router 3:

```
configure terminal
crypto isakmp policy 1
encryption aes
hash md5
authentication pre-share
group 2
lifetime 80000
exit
crypto isakmp key tinatvk81 address 192.168.34.4
ip access-list extended IPSEC_List
permit ip 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255
```

```
crypto ipsec transform-set TSET esp-aes esp-md5-hmac
crypto map CMAP 1 ipsec-isakmp
set peer 192.168.34.4
set transform-set TSET
exit
interface FastEthernet 0/1
crypto map CMAP
exit
access-list 100 deny ip 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255
access-list 100 permit ip 192.168.1.0 0.0.0.255 any
ip nat inside source list 100 interface FastEthernet 0/1 overload
in FastEthernet0/1
ip nat outside
in FastEthernet0/0
ip nat inside
```

برای router 4:

```
configure terminal
crypto isakmp policy 1
encryption aes
hash md5
authentication pre-share
group 2
lifetime 80000
exit
crypto isakmp key tinatvk81 address 192.168.12.1
crypto ipsec transform-set TSET esp-aes esp-md5-hmac
ip access-list extended IPSEC_List
permit ip 192.168.2.0 0.0.0.255 192.168.1.0 0.0.0.255
crypto map CMAP 1 ipsec-isakmp
```

set peer 192.168.12.1

set transform-set TSET

match address IPSEC_List

exit

interface FastEthernet 0/1

crypto map CMAP

access-list 100 deny ip 192.168.2.0 0.0.0.255 192.168.1.0 0.0.0.255

access-list 100 permit ip 192.168.2.0 0.0.0.255 any

ip nat inside source list 100 interface FastEthernet 0/1 overload

in FastEthernet0/1

ip nat outside

in FastEthernet0/0

ip nat inside

حال تنظیمات انجام شده و میتوان به راحتی پینگ گرفت(به طور ایمن):

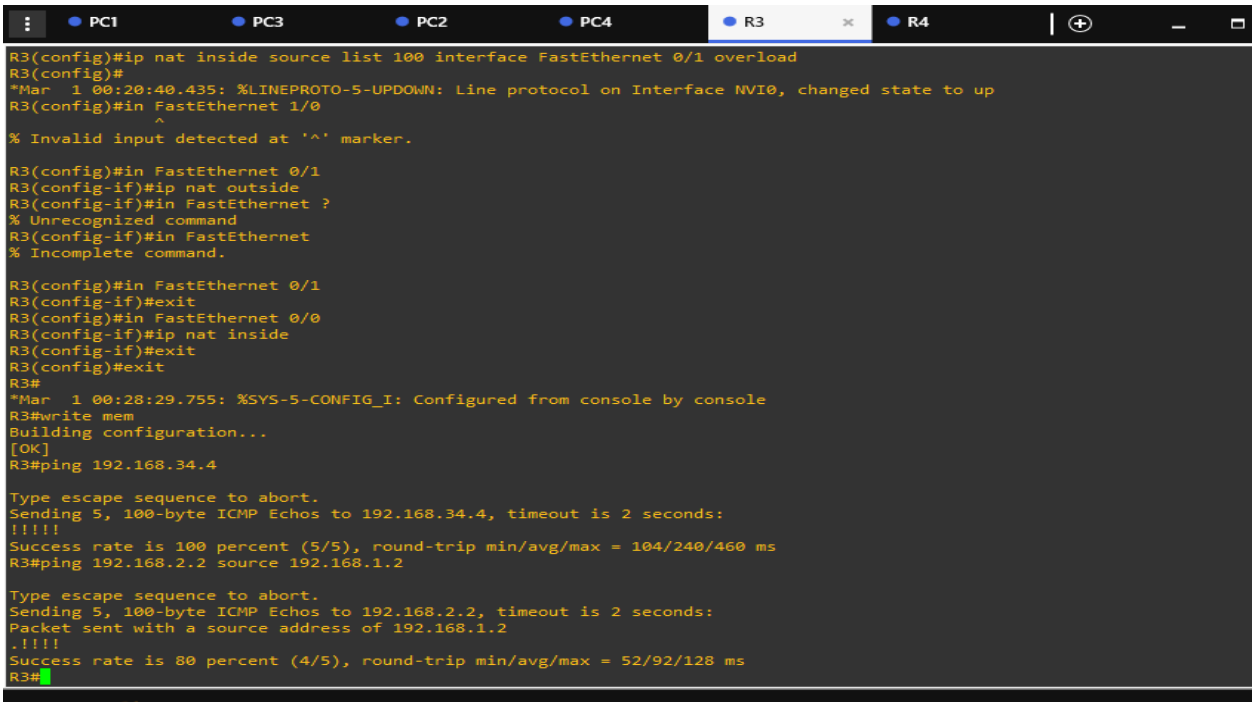

Figure 2-پینگ روتر دیگر را گرفته

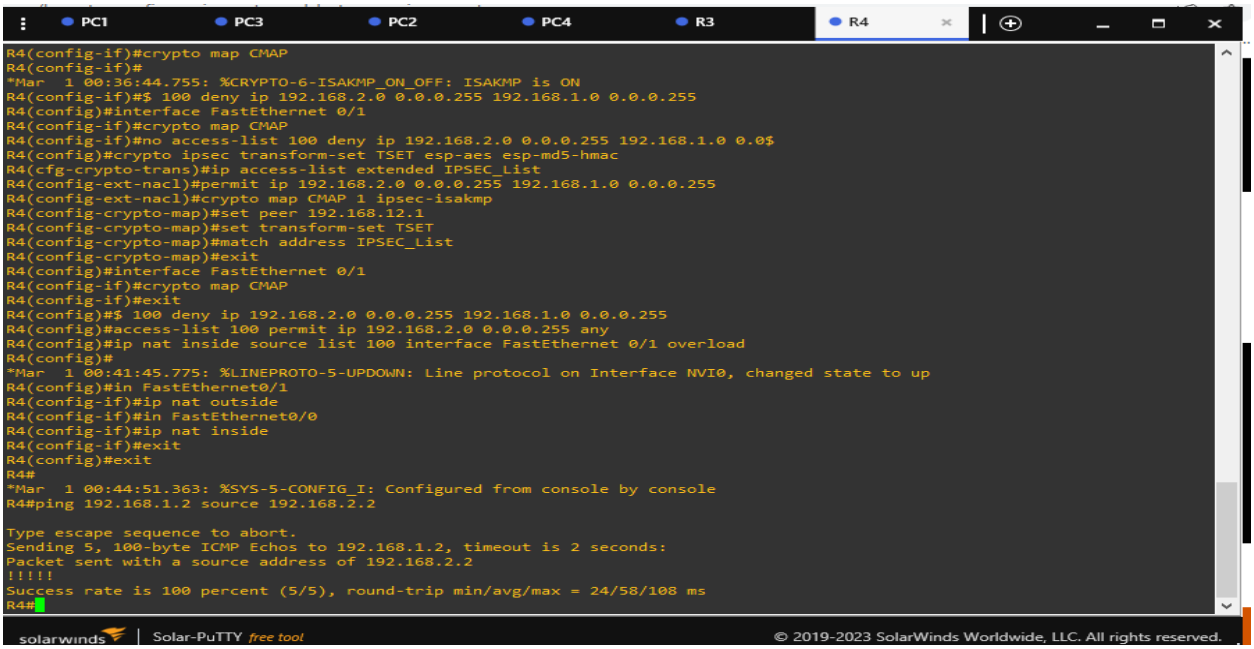

Figure 3-پینگ روتر دیگر را گرفته

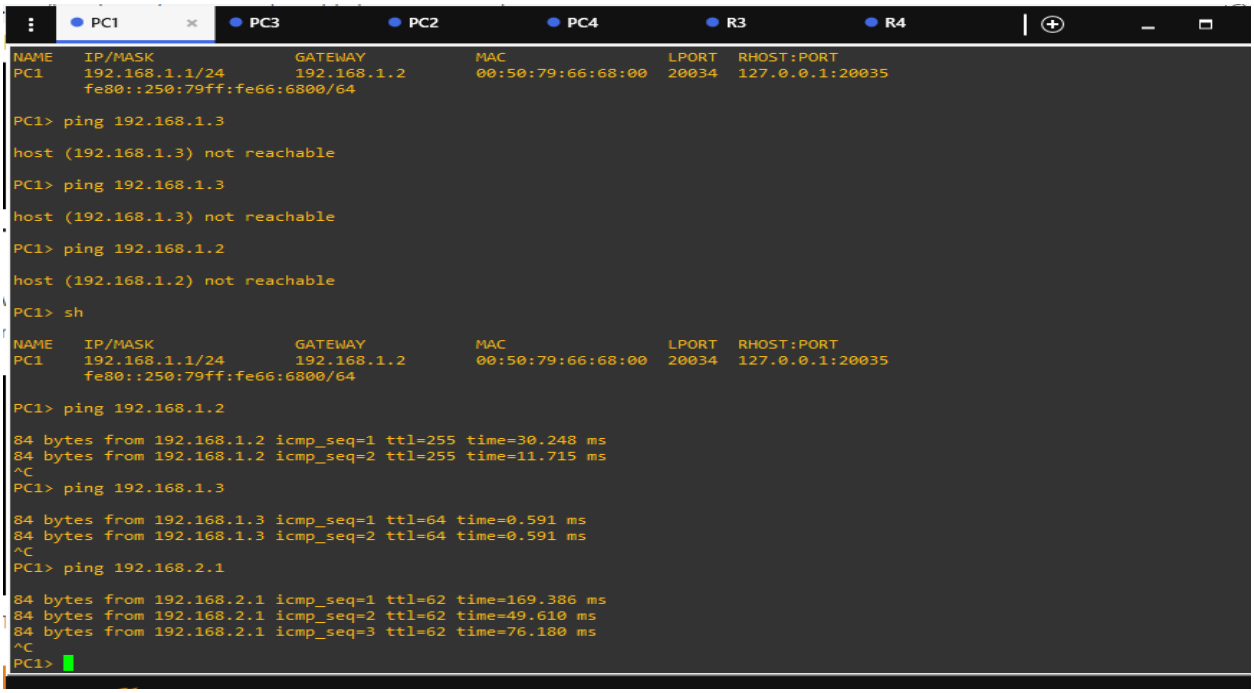

Figure 4-پینگ pc روبه رو را گرفته

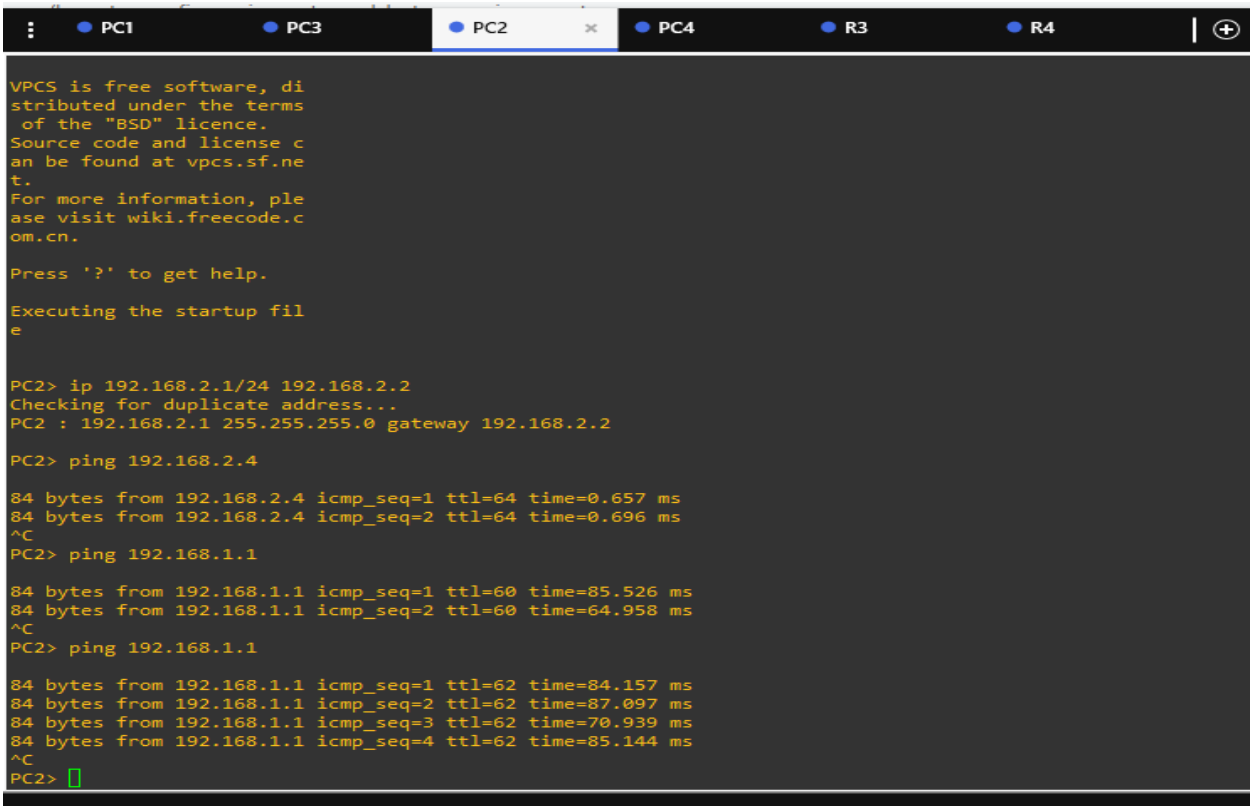

Figure5--پینگ pc روبه رو را گرفته

سپس برای نشان دادن اینکه به طور ایمن پکت ها جا به جا میشوند از wireshark استفاده میکنیم:

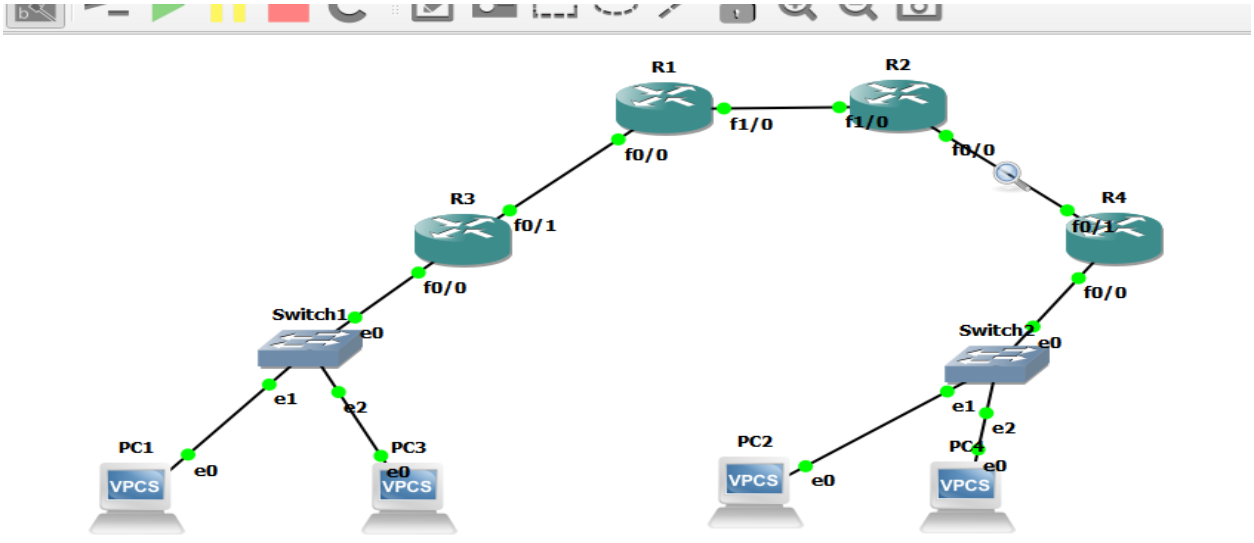

Figure 6-نشان دادن توپولوژی

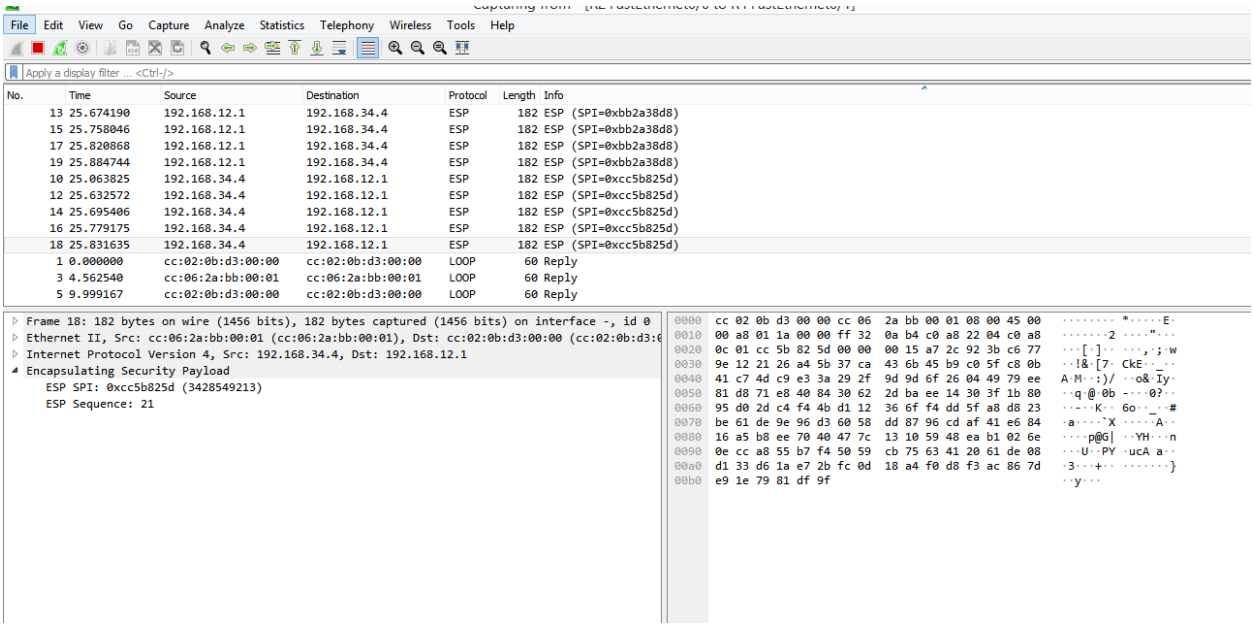

Figure 7- به طور ایمن فرستاده شده

منبع:

https://www.gns3network.com/how-to-configure-ipsec-tunnel-between-cisco-routers

4. host to Network VPN:

این نوع VPN به شما امکان می دهد از طریق اینترنت به طور امن به یک شبکه خصوصی یا سرور شخص ثالث متصل شوید .این کار با ایجاد یک تونل رمزگذاری شده بین دستگاه شما و سرور VPN انجام می شود .تمام ترافیک اینترنتی شما از طریق این تونل عبور می کند و از آن محافظت می شود.

مزایا:

- **امنیت :**ترافیک شما را رمزگذاری می کند و از آن در برابر هکرها محافظت می کند.
- **حریم خصوصی :**آدرس IP شما را پنهان می کند و فعالیت آنلاین شما را ناشناس می کند.
- **دسترسی به محتوای محدود :**می توانید به وب سایت ها و خدماتی که در منطقه شما مسدود شده اند دسترسی پیدا کنید.

مراحل:

- ایجاد توپولوژی: در GNS3، روتر، سرور VPN و کلاینت را راه اندازی کنید.
- **تنظیم روتر:**

رابط های روتر را پیکربندی کنید.

مسیرهای لازم را برای رسیدن به شبکه VPN یا سرور شخص ثالث اضافه کنید.

- **تنظیم سرور VPN:**

نوع سرور VPN را انتخاب کنید .

گواهینامه های SSL/TLS را پیکربندی کنید.

کاربران و مجوزهای دسترسی را تنظیم کنید.

- **تنظیم کلاینت:**

کلاینت VPN را نصب و پیکربندی کنید.

آدرس سرور VPN و گواهی SSL/TLS را وارد کنید.

نام کاربری و رمز عبور خود را وارد کنید.

پیاده سازی: