گزارش ششم

نظری

انواع شبکه های خصوصی مجازی

سایت به سایت :

یک VPN سایت به سایت با IPSec یک تونل امن و رمزگذاری شده بین دو شبکه فیزیکی جداگانه ایجاد می کند و به آنها اجازه می دهد تا با هم ارتباط برقرار کنند، گویی که به طور مستقیم روی یک خط اختصاصی متصل هستند، حتی اگر از اینترنت عمومی در بین آنها استفاده می شود. در اینجا نحوه عملکرد آن آمده است:

رمزگذاری و تونل سازی:

IPsec (امنیت پروتکل اینترنت): مجموعه ای از پروتکل ها است که پایه و اساس اتصال امن را فراهم می کند. این بسته های داده ای را که بین شبکه ها حرکت می کنند رمزگذاری می کند و آنها را برای هر کسی که آنها را رهگیری می کند غیرقابل خواندن می کند.

تونل سازی: تصور کنید تونلی زیرزمینی ساخته شده است که دو مکان را به هم متصل می کند. یک VPN سایت به سایت یک تونل مجازی مشابه در داخل اینترنت ایجاد می کند. بسته های داده در بسته های جدید با هدرهای جدید قرار می گیرند و سپس از طریق این تونل رمزگذاری شده ارسال می شوند.

احراز هویت:

هر دو طرف اتصال VPN برای جلوگیری از دسترسی غیرمجاز باید هویت یکدیگر را تأیید کنند. این معمولاً با استفاده از کلیدهای از پیش به اشتراک گذاشته شده (PSK) یا گواهی های دیجیتال حاصل می شود.

مسیریابی:

از پروتکل های مسیریابی برای هدایت بسته های داده به سمت تونل VPN و اطمینان از رسیدن آنها به مقصد مورد نظر در شبکه دیگر استفاده می شود.

میزبان به سایت :

یک VPN میزبان به سایت با IPSec یک تونل امن و رمزگذاری شده بین یک دستگاه (میزبان) و یک شبکه راه دور (سایت) ایجاد می کند. این به میزبان اجازه می دهد تا به طور ایمن به منابع موجود در شبکه راه دور دسترسی داشته باشد، گویی که به طور مستقیم متصل است، حتی اگر از اینترنت عمومی در بین آنها استفاده می شود. در اینجا نحوه مقایسه آن با VPN های سایت به سایت آمده است:

شباهت ها:

IPsec: هر دو از مجموعه پروتکل های IPSec برای رمزگذاری و ارتباط امن استفاده می کنند.

تونل سازی: داده ها کپسوله شده و از طریق یک تونل مجازی درون اینترنت ارسال می شوند.

احراز هویت: از پیش به اشتراک گذاشته شده (PSK) یا گواهی های دیجیتال برای تایید اعتبار استفاده می شود.

تفاوت های کلیدی:

دامنه: سایت به سایت کل شبکه ها را متصل می کند، در حالی که میزبان به سایت اتصال یک دستگاه واحد را ایمن می کند.

کاربردها: برای کاربران راه دور که نیاز به دسترسی ایمن به شبکه شرکت یا منابع ابری از رایانه های شخصی یا لپ تاپ های خود دارند، ایده آل است.

پیچیدگی: به طور کلی راه‌اندازی آن نسبت به VPN های سایت به سایت ساده‌تر است، زیرا تنها یک دستگاه نیاز به پیکربندی دارد.

در اینجا نحوه عملکرد یک VPN میزبان به سایت IPSec آمده است:

آغاز(Initiation): میزبان یک درخواست اتصال به نقطه انتهایی VPN شبکه راه دور (معمولاً فایروال یا سرور VPN) ارسال می کند.

مذاکره(Negotiation): هر دو طرف پارامترهای امنیتی مانند الگوریتم های رمزگذاری و روش های تأیید اعتبار را تعیین می کنند.

احراز هویت: میزبان و نقطه انتهایی VPN با استفاده از PSK یا گواهی، هویت یکدیگر را تأیید می کنند.

ایجاد تونل: یک تونل رمزگذاری شده بین میزبان و شبکه راه دور ایجاد می شود.

ارتباط امن: اکنون میزبان می تواند از طریق تونل به طور ایمن داده ها را ارسال و دریافت کند و به منابع موجود در شبکه راه دور دسترسی داشته باشد، گویی که به طور مستقیم متصل است.

تفاوت بین پروتکل IPSec و GRE

IPsec و GRE هر دو پروتکل‌هایی هستند که در شبکه‌های کامپیوتری استفاده می‌شوند، اما اهداف متفاوتی دارند:

IPsec (امنیت پروتکل اینترنت):

پروتکل امنیتی: بر ارائه ارتباط امن در سراسر شبکه تمرکز دارد.

رمزگذاری و احراز هویت: بسته‌های داده را رمزگذاری می‌کند و دستگاه‌های ارتباطی را تأیید می‌کند تا از حریم خصوصی محافظت کند و از دسترسی غیرمجاز جلوگیری کند.

تونل‌سازی (اختیاری): می‌تواند همراه با پروتکل‌های تونل‌سازی برای ایمن‌سازی داده‌ها درون یک تونل استفاده شود.

مناسب برای: ایجاد اتصالات امن مانند VPN های سایت به سایت یا دسترسی کاربران راه دور به شبکه شرکتی.

GRE (Generic Routing Encapsulation - کپسوله‌سازی مسیریابی عمومی):

پروتکل تونل‌سازی: یک تونل مجازی درون شبکه دیگری برای انتقال داده ایجاد می‌کند.

بدون امنیت: خود بسته‌های داده را رمزگذاری نمی‌کند. امنیت داده‌های کپسوله‌شده به شبکه زیربنایی یا پروتکل‌های اضافی بستگی دارد.

پشتیبانی از پروتکل‌های مختلف: می‌تواند پروتکل‌های مختلفی مانند IP، IPX (پروتکل شبکه قدیمی‌تر) و AppleTalk را کپسوله‌سازی کند.

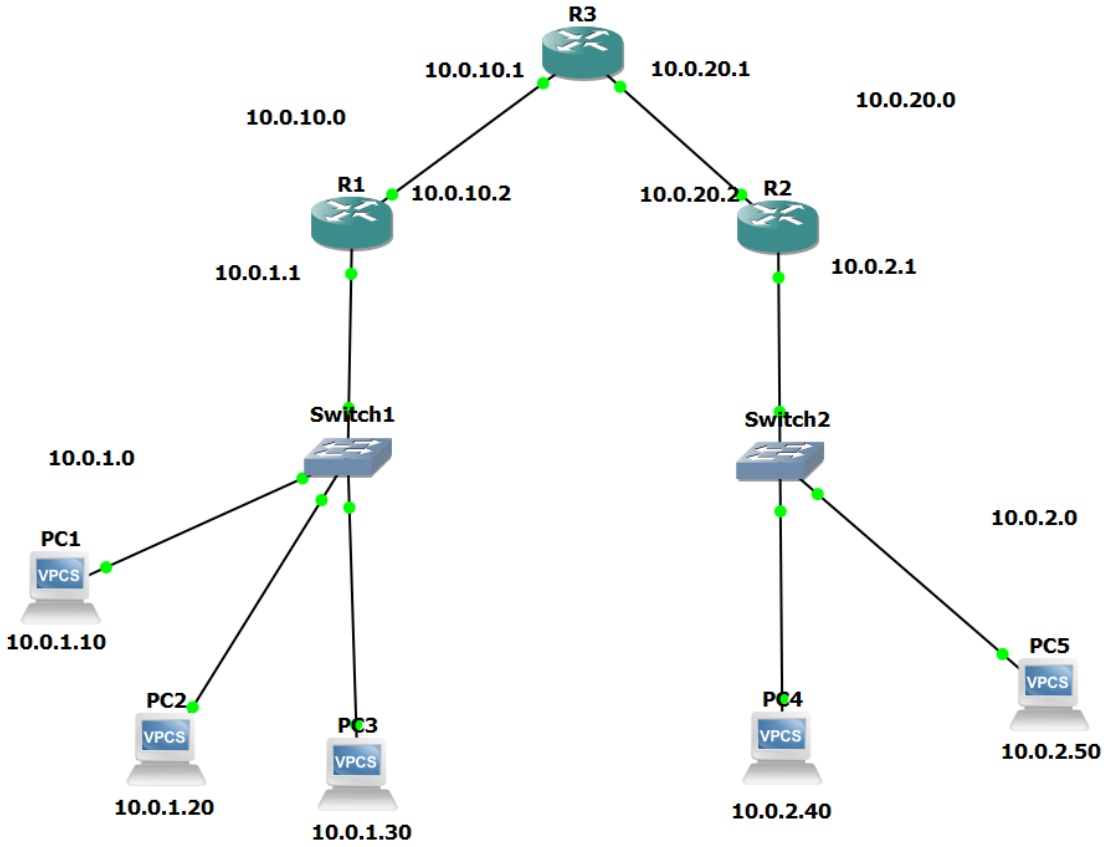
مناسب برای: گسترش شبکه‌های خصوصی روی شبکه‌های عمومی یا کپسوله‌سازی ترافیک غیر IP روی شبکه‌های IP.

مقایسه پروتکل های IPsec و GRE به صورت خلاصه در جدول زیر آورده شده است.

PARAMETER	GRE	IPSec
Full Form	Generic Routing Encapsulation	IP Security
Purpose	GRE is a protocol that encapsulates packets in order to route other protocols over IP networks.	The IP Security (IPsec) Protocol is a standards-based method of providing privacy, integrity, and authenticity to information transferred across IP networks.
Usage	GRE is used when IP packets need to be sent from one network to another, without being parsed or treated like IP packets by any intervening routers.	IPsec ESP is used when IP packets need to be exchanged between two systems while being protected against eavesdropping or modification along the way.
Modes	Single mode – GRE Tunnel	Two Modes – Tunnel Mode and Transport Mode
Privacy, integrity and authenticity of information	Not Supported	Supported
Encapsulation	Encapsulation of Payload	Tunnel Mode – Entire packet is encapsulated Transport Mode – Only payload is protected.
Standard	GRE is defined in RFC 2784 standard	IPSEC ESP is defined in RFC2406
Protocol & Port	GRE use IP Protocol number 47	IPSec uses ESP (IP protocol number 50) and AH (IP Protocol number 51). In addition IPSec uses IKE for negotiations (UDP Port number 500).
IP Header	4 Bytes additional IP Header	Additional bytes not used.
Multicast , Routing Protocol and Routed protocol support	Supported	Not Supported
Simplicity	Simpler and faster	Complex

عملی:

در این قسمت هدف پیاده سازی site-to-site vpn از طریق پروتکل IPsec می باشد. توپولوژی در نظر گرفته شده برای این آزمایش مطابق تصویر زیر است.



ابتدا برای pc ها و اینترفیس های روترها ip ست می کنیم.

```
PC1> ip 10.0.1.10 255.255.255.0 10.0.1.1
Checking for duplicate address...
PC1 : 10.0.1.10 255.255.255.0 gateway 10.0.1.1
```

```
PC2> ip 10.0.1.20 255.255.255.0 10.0.1.1
Checking for duplicate address...
PC2 : 10.0.1.20 255.255.255.0 gateway 10.0.1.1
```

```
PC3> ip 10.0.1.30 255.255.255.0 10.0.1.1
Checking for duplicate address...
PC3 : 10.0.1.30 255.255.255.0 gateway 10.0.1.1
```

```
PC4> ip 10.0.2.40 255.255.255.0 10.0.2.1
Checking for duplicate address...
PC4 : 10.0.2.40 255.255.255.0 gateway 10.0.2.1
```

```
PC5> ip 10.0.2.50 255.255.255.0 10.0.2.1
Checking for duplicate address...
PC5 : 10.0.2.50 255.255.255.0 gateway 10.0.2.1
```

در دستورات زیر ابتدا برای روترها ip ست می کنیم سپس اینترفیس ها را up کرده و مسیریابی انجام می دهیم.

```
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#int f0/0
R1(config-if)#ip addr 10.0.1.1 255.255.255.0
R1(config-if)#no shut
R1(config-if)#exit
R1(config)#
*Mar  1 00:03:06.619: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state to up
*Mar  1 00:03:07.619: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
R1(config)#int f0/1
R1(config-if)#ip addr 10.0.10.2 255.255.255.0
R1(config-if)#no shut
R1(config-if)#exit
R1(config)#
*Mar  1 00:03:44.351: %LINK-3-UPDOWN: Interface FastEthernet0/1, changed state to up
*Mar  1 00:03:45.351: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up
R1(config)#router eigrp 1
R1(config-router)#network 0.0.0.0
R1(config-router)#exit
```

```
R3#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)#int f0/0
R3(config-if)#ip addr 10.0.10.1 255.255.255.0
R3(config-if)#no shut
R3(config-if)#exit
R3(config)#
*Mar  1 00:06:47.387: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state to up
*Mar  1 00:06:48.387: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
R3(config)#int f0/1
R3(config-if)#ip addr 10.0.20.1 255.255.255.0
R3(config-if)#no shut
R3(config-if)#exit
R3(config)#
*Mar  1 00:07:12.939: %LINK-3-UPDOWN: Interface FastEthernet0/1, changed state to up
*Mar  1 00:07:13.939: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up
```

```
R3(config)#router eigrp 1
R3(config-router)#network 0.0.0.0
R3(config-router)#
*Mar  1 00:08:23.351: %DUAL-5-NBRCHANGE: IP-EIGRP(0) 1: Neighbor 10.0.10.2 (FastEthernet0/0) is up: new adjacency
R3(config-router)#exit
```

```
R2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#int f0/0
R2(config-if)#ip addr 10.0.2.1 255.255.255.0
R2(config-if)#no shut
R2(config-if)#exit
R2(config)#
*Mar  1 00:08:50.451: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state to up
*Mar  1 00:08:51.451: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
R2(config)#int f0/1
R2(config-if)#ip addr 10.0.20.2 255.255.255.0
R2(config-if)#no shut
R2(config-if)#exit
R2(config)#
*Mar  1 00:09:19.003: %LINK-3-UPDOWN: Interface FastEthernet0/1, changed state to up
*Mar  1 00:09:20.003: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up
R2(config)#router eigrp 1
R2(config-router)#network 0.0.0.0
R2(config-router)#exit
R2(config)#
*Mar  1 00:09:47.599: %DUAL-5-NBRCHANGE: IP-EIGRP(0) 1: Neighbor 10.0.20.1 (FastEthernet0/1) is up: new adjacency
```

برای بررسی درستی تنظیمات پینگ می گیریم.

```
PC1> ping 10.0.2.40

10.0.2.40 icmp_seq=1 timeout
84 bytes from 10.0.2.40 icmp_seq=2 ttl=61 time=84.165 ms
84 bytes from 10.0.2.40 icmp_seq=3 ttl=61 time=90.142 ms
84 bytes from 10.0.2.40 icmp_seq=4 ttl=61 time=89.369 ms
84 bytes from 10.0.2.40 icmp_seq=5 ttl=61 time=93.168 ms
```

```
PC2> ping 10.0.1.10

84 bytes from 10.0.1.10 icmp_seq=1 ttl=64 time=1.572 ms
84 bytes from 10.0.1.10 icmp_seq=2 ttl=64 time=1.880 ms
84 bytes from 10.0.1.10 icmp_seq=3 ttl=64 time=1.941 ms
84 bytes from 10.0.1.10 icmp_seq=4 ttl=64 time=2.100 ms
84 bytes from 10.0.1.10 icmp_seq=5 ttl=64 time=2.237 ms
```

```
PC5> ping 10.0.1.10

84 bytes from 10.0.1.10 icmp_seq=1 ttl=61 time=91.847 ms
84 bytes from 10.0.1.10 icmp_seq=2 ttl=61 time=90.904 ms
84 bytes from 10.0.1.10 icmp_seq=3 ttl=61 time=91.429 ms
84 bytes from 10.0.1.10 icmp_seq=4 ttl=61 time=91.672 ms
84 bytes from 10.0.1.10 icmp_seq=5 ttl=61 time=91.183 ms
```

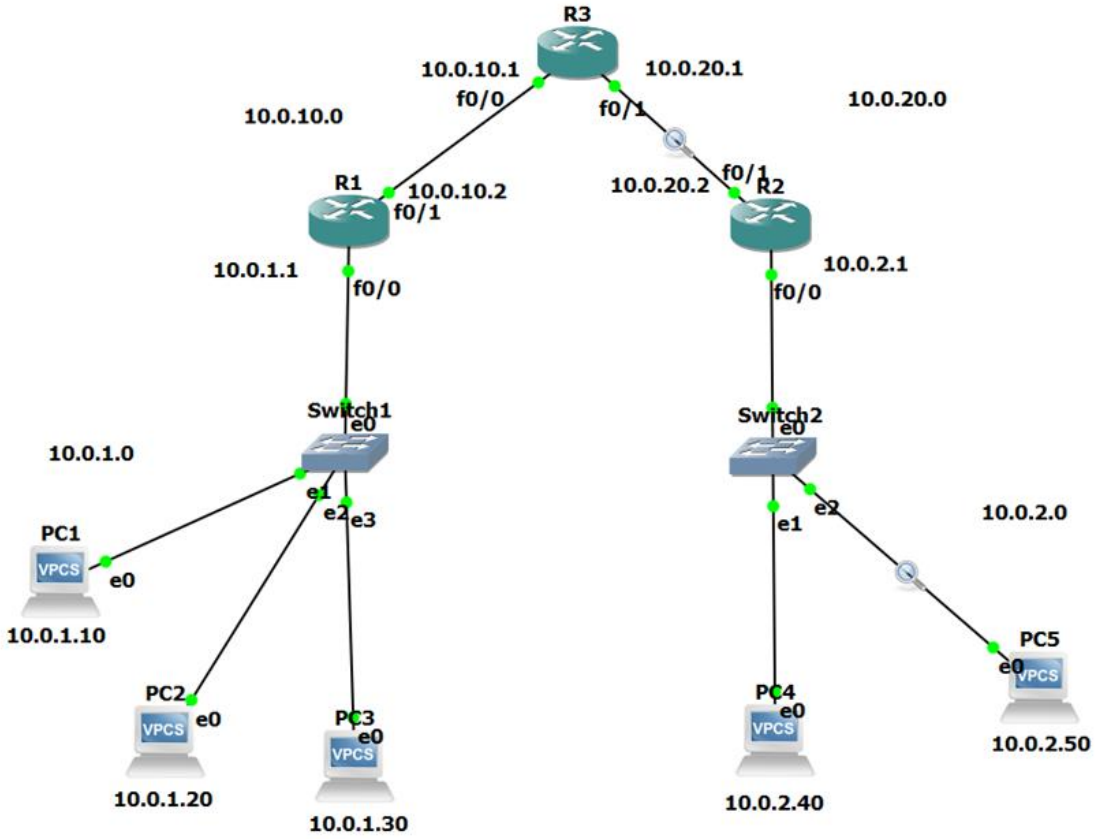
سپس بین روترهای R1 و R2 با استفاده از دستورات زیر تونل می زنیم با استفاده ازدستور crypto isakmp policy پارامترهای مورد نیاز برای رمزنگاری در SA و سیستم مدیریت کلید را مشخص می کنیم.

```
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#crypto isakmp policy 1
R1(config-isakmp)#encryption aes 128
R1(config-isakmp)#authentication pre-share
R1(config-isakmp)#group 2
R1(config-isakmp)#hash sha
R1(config-isakmp)#crypto isakmp key 6 referux123 address 0.0.0.0
A pre-shared key for address mask 0.0.0.0 0.0.0.0 already exists!

R1(config)#crypto ipsec transform-set MYSET esp-aes 128 esp-sha-hmac
R1(cfg-crypto-trans)#exit
R1(config)#ip access-list extended 100
R1(config-ext-nacl)#permit ip 10.0.1.0 0.0.0.255 10.0.2.0 0.0.0.255
R1(config-ext-nacl)#exit
R1(config)#crypto map MYMAP 1 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
        and a valid access list have been configured.
R1(config-crypto-map)#match address 100
R1(config-crypto-map)#set peer 10.0.20.2
R1(config-crypto-map)#set transform-set MYSET
R1(config-crypto-map)#exit
R1(config)#int f0/1
R1(config-if)#crypto map MYMAP
R1(config-if)#
*Mar  1 00:27:03.891: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
R1(config-if)#end
R1#
*Mar  1 00:27:09.323: %SYS-5-CONFIG_I: Configured from console by console
```

```
R2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#crypto isakmp policy 1
R2(config-isakmp)#encryption aes 128
R2(config-isakmp)#authentication pre-share
R2(config-isakmp)#group 2
R2(config-isakmp)#hash sha
R2(config-isakmp)#crypto isakmp key 6 referux123 address 0.0.0.0
R2(config)#crypto ipsec transform-set MYSET esp-aes 128 esp-sha-hmac
R2(cfg-crypto-trans)#exit
R2(config)#ip access-list extended 100
R2(config-ext-nacl)#permit ip 10.0.2.0 0.0.0.255 10.0.1.0 0.0.0.255
R2(config-ext-nacl)#exit
R2(config)#crypto map MYMAP 1 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
        and a valid access list have been configured.
R2(config-crypto-map)#match address 100
R2(config-crypto-map)#set peer 10.0.10.2
R2(config-crypto-map)#set tranform-set MYSET
                              ^
% Invalid input detected at '^' marker.

R2(config-crypto-map)#set transform-set MYSET
R2(config-crypto-map)#exit
R2(config)#int f0/1
R2(config-if)#crypto map MYMAP
R2(config-if)#e
*Mar  1 00:26:53.927: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
R2(config-if)#end
R2#
*Mar  1 00:26:57.539: %SYS-5-CONFIG_I: Configured from console by console
```

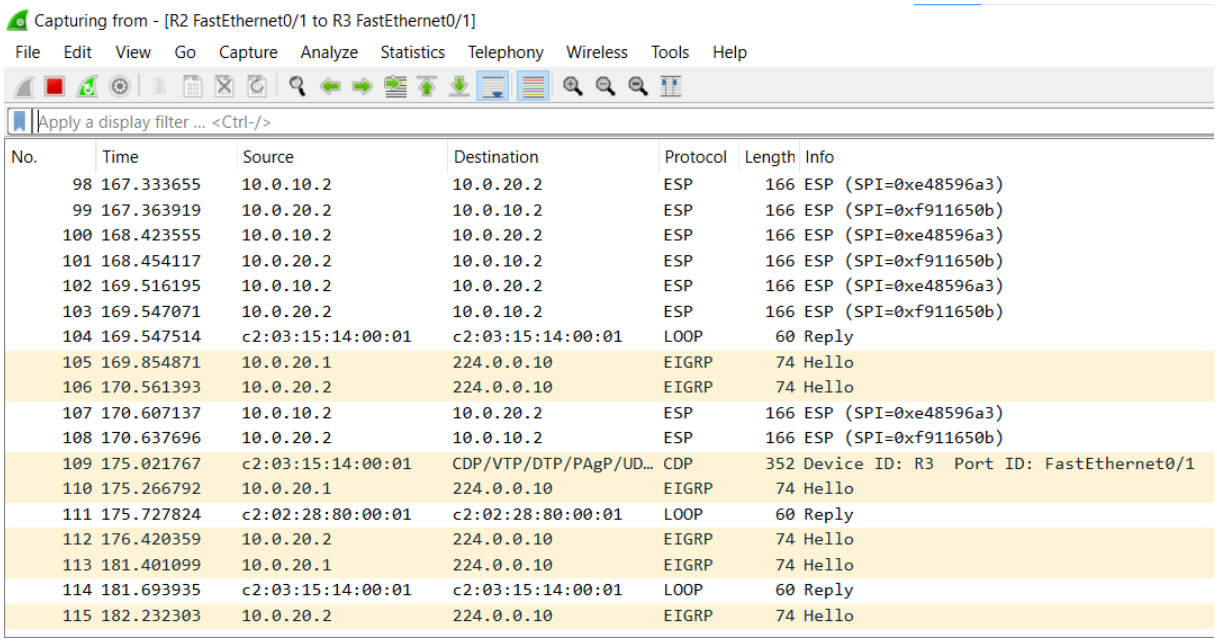
پس از تنظیم کردن تونل، نودهای بین دو روتر نمی توانند ترافیک شبکه را آنالیز کنند و آنالیز ترافیک شبکه فقط برای سایت هایی که روترهای R1 و R2 در آن قرار دارند ممکن است. این موضوع با آنالیز پکت هایی که از روتر R3 به R2 و از روتر R2 به PC5 می روند، قابل مشاهده است.

ابتدا از PC1 ، PC5 را پینگ می کنیم و سپس ترافیک شبکه را در مسیرهای ذکر شده بررسی می کنیم.



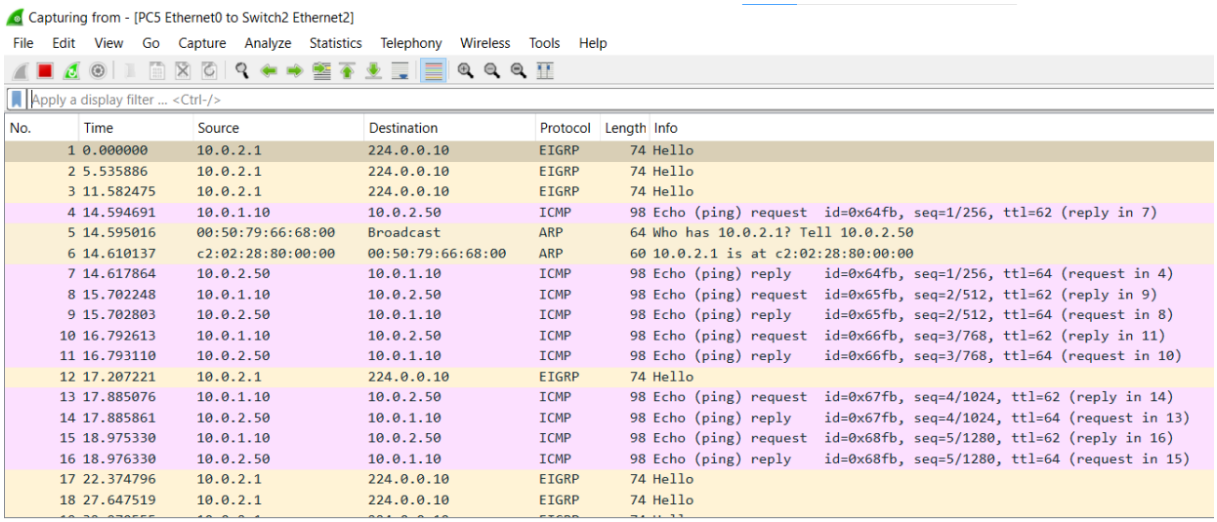

```
PC1> ping 10.0.2.50

84 bytes from 10.0.2.50 icmp_seq=1 ttl=62 time=107.076 ms
84 bytes from 10.0.2.50 icmp_seq=2 ttl=62 time=90.425 ms
84 bytes from 10.0.2.50 icmp_seq=3 ttl=62 time=90.102 ms
84 bytes from 10.0.2.50 icmp_seq=4 ttl=62 time=91.365 ms
84 bytes from 10.0.2.50 icmp_seq=5 ttl=62 time=89.516 ms
```

همانطور که در تصویر زیر مشاهده می شود ترافیک شبکه از روتر R3 به R2 قابل مشاهده نیست و توسط esp رمز شده است همچنین آدرس ip مبدا و مقصد، آدرس واقعی نیست و آدرس های روترها (gateway) هستند



No.	Time	Source	Destination	Protocol	Length	Info
98	167.333655	10.0.10.2	10.0.20.2	ESP	166	ESP (SPI=0xe48596a3)
99	167.363919	10.0.20.2	10.0.10.2	ESP	166	ESP (SPI=0xf911650b)
100	168.423555	10.0.10.2	10.0.20.2	ESP	166	ESP (SPI=0xe48596a3)
101	168.454117	10.0.20.2	10.0.10.2	ESP	166	ESP (SPI=0xf911650b)
102	169.516195	10.0.10.2	10.0.20.2	ESP	166	ESP (SPI=0xe48596a3)
103	169.547071	10.0.20.2	10.0.10.2	ESP	166	ESP (SPI=0xf911650b)
104	169.547514	c2:03:15:14:00:01	c2:03:15:14:00:01	LOOP	60	Reply
105	169.854871	10.0.20.1	224.0.0.10	EIGRP	74	Hello
106	170.561393	10.0.20.2	224.0.0.10	EIGRP	74	Hello
107	170.607137	10.0.10.2	10.0.20.2	ESP	166	ESP (SPI=0xe48596a3)
108	170.637696	10.0.20.2	10.0.10.2	ESP	166	ESP (SPI=0xf911650b)
109	175.021767	c2:03:15:14:00:01	CDP/VTP/DTP/PAgP/UD…	CDP	352	Device ID: R3 Port ID: FastEthernet0/1
110	175.266792	10.0.20.1	224.0.0.10	EIGRP	74	Hello
111	175.727824	c2:02:28:80:00:01	c2:02:28:80:00:01	LOOP	60	Reply
112	176.420359	10.0.20.2	224.0.0.10	EIGRP	74	Hello
113	181.401099	10.0.20.1	224.0.0.10	EIGRP	74	Hello
114	181.693935	c2:03:15:14:00:01	c2:03:15:14:00:01	LOOP	60	Reply
115	182.232303	10.0.20.2	224.0.0.10	EIGRP	74	Hello

اما در تصویر زیر ترافیک شبکه از روتر R2 به PC5 قابل مشاهده است که در آن رمزنگاری صورت نگرفته و آدرس ip مبدا و مقصد، آدرس PC1 ip و PC5 می باشد.



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	10.0.2.1	224.0.0.10	EIGRP	74	Hello
2	5.535886	10.0.2.1	224.0.0.10	EIGRP	74	Hello
3	11.582475	10.0.2.1	224.0.0.10	EIGRP	74	Hello
4	14.594691	10.0.1.10	10.0.2.50	ICMP	98	Echo (ping) request id=0x64fb, seq=1/256, ttl=62 (reply in 7)
5	14.595016	00:50:79:66:68:00	Broadcast	ARP	64	Who has 10.0.2.1? Tell 10.0.2.50
6	14.610137	c2:02:28:80:00:00	00:50:79:66:68:00	ARP	60	10.0.2.1 is at c2:02:28:80:00:00
7	14.617864	10.0.2.50	10.0.1.10	ICMP	98	Echo (ping) reply id=0x64fb, seq=1/256, ttl=64 (request in 4)
8	15.702248	10.0.1.10	10.0.2.50	ICMP	98	Echo (ping) request id=0x65fb, seq=2/512, ttl=62 (reply in 9)
9	15.702803	10.0.2.50	10.0.1.10	ICMP	98	Echo (ping) reply id=0x65fb, seq=2/512, ttl=64 (request in 8)
10	16.792613	10.0.1.10	10.0.2.50	ICMP	98	Echo (ping) request id=0x66fb, seq=3/768, ttl=62 (reply in 11)
11	16.793110	10.0.2.50	10.0.1.10	ICMP	98	Echo (ping) reply id=0x66fb, seq=3/768, ttl=64 (request in 10)
12	17.207221	10.0.2.1	224.0.0.10	EIGRP	74	Hello
13	17.885076	10.0.1.10	10.0.2.50	ICMP	98	Echo (ping) request id=0x67fb, seq=4/1024, ttl=62 (reply in 14)
14	17.885861	10.0.2.50	10.0.1.10	ICMP	98	Echo (ping) reply id=0x67fb, seq=4/1024, ttl=64 (request in 13)
15	18.975330	10.0.1.10	10.0.2.50	ICMP	98	Echo (ping) request id=0x68fb, seq=5/1280, ttl=62 (reply in 16)
16	18.976330	10.0.2.50	10.0.1.10	ICMP	98	Echo (ping) reply id=0x68fb, seq=5/1280, ttl=64 (request in 15)
17	22.374796	10.0.2.1	224.0.0.10	EIGRP	74	Hello
18	27.647519	10.0.2.1	224.0.0.10	EIGRP	74	Hello