



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 GRE و IPSec

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:

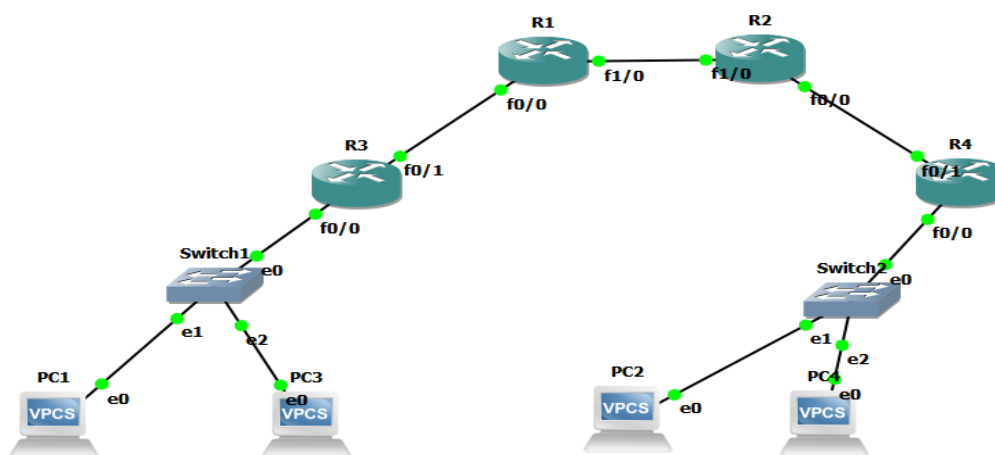


Figure 1- حالت tunnel بین R3,R4

تنظیمات روتر ها و ... همه مانند فعالیت کلاسی است و تنها تفاوت در تنظیم IP ها 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 3 router:

```
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 4 router:

```
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):

```

R3(config)#ip nat inside source list 100 interface FastEthernet 0/1 overload
R3(config)#
*Mar  1 00:20:40.435: %LINEPROTO-5-UPDOWN: Line protocol on Interface NVI0, changed state to up
R3(config)#in FastEthernet 1/0
^
% Invalid input detected at '^' marker.

R3(config)#in FastEthernet 0/1
R3(config-if)#ip nat outside
R3(config-if)#in FastEthernet ?
% Unrecognized command
R3(config-if)#in FastEthernet
% Incomplete command.

R3(config)#in FastEthernet 0/1
R3(config-if)#exit
R3(config)#in FastEthernet 0/0
R3(config-if)#ip nat inside
R3(config-if)#exit
R3(config)#exit
R3#
*Mar  1 00:28:29.755: %SYS-5-CONFIG_I: Configured from console by console
R3#write mem
Building configuration...
[OK]
R3#ping 192.168.34.4

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.34.4, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 104/240/460 ms
R3#ping 192.168.2.2 source 192.168.1.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.2.2, timeout is 2 seconds:
Packet sent with a source address of 192.168.1.2
!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 52/92/128 ms
R3#

```

Figure 2-پینگ روتر دیگر را گرفته

```
PC1 PC3 PC2 PC4 R3 R4
R4(config-if)#crypto map CHAP
R4(config-if)#
*Mar 1 00:36:44.755: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
R4(config-if)#$ 100 deny ip 192.168.2.0 0.0.0.255 192.168.1.0 0.0.0.255
R4(config)#interface FastEthernet 0/1
R4(config-if)#crypto map CHAP
R4(config-if)#no access-list 100 deny ip 192.168.2.0 0.0.0.255 192.168.1.0 0.0.0.255
R4(config)#crypto ipsec transform-set TSET esp-aes esp-md5-hmac
R4(cfg-crypto-trans)#ip access-list extended IPSEC_List
R4(config-ext-nacl)#permit ip 192.168.2.0 0.0.0.255 192.168.1.0 0.0.0.255
R4(config-ext-nacl)#crypto map CHAP 1 ipsec-isakmp
R4(config-crypto-map)#set peer 192.168.12.1
R4(config-crypto-map)#set transform-set TSET
R4(config-crypto-map)#match address IPSEC_List
R4(config-crypto-map)#exit
R4(config)#interface FastEthernet 0/1
R4(config-if)#crypto map CHAP
R4(config-if)#exit
R4(config)#$ 100 deny ip 192.168.2.0 0.0.0.255 192.168.1.0 0.0.0.255
R4(config)#access-list 100 permit ip 192.168.2.0 0.0.0.255 any
R4(config)#ip nat inside source list 100 interface FastEthernet 0/1 overload
R4(config)#
*Mar 1 00:41:45.775: %LINEPROTO-5-UPDOWN: Line protocol on Interface NVI0, changed state to up
R4(config)#in FastEthernet0/1
R4(config-if)#ip nat outside
R4(config-if)#in FastEthernet0/0
R4(config-if)#ip nat inside
R4(config-if)#exit
R4(config)#exit
R4#
*Mar 1 00:44:51.363: %SYS-5-CONFIG_I: Configured from console by console
R4#ping 192.168.1.2 source 192.168.2.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.2, timeout is 2 seconds:
Packet sent with a source address of 192.168.2.2
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 24/58/108 ms
R4#
```

Figure 3-پینگ روتر دیگر را گرفته

```
PC1 PC3 PC2 PC4 R3 R4
NAME IP/MASK GATEWAY MAC LPORT RHOST:PORT
PC1 192.168.1.1/24 192.168.1.2 00:50:79:66:68:00 20034 127.0.0.1:20035
fe80::250:79ff:fe66:6800/64

PC1> ping 192.168.1.3
host (192.168.1.3) not reachable
PC1> ping 192.168.1.3
host (192.168.1.3) not reachable
PC1> ping 192.168.1.2
host (192.168.1.2) not reachable
PC1> sh
NAME IP/MASK GATEWAY MAC LPORT RHOST:PORT
PC1 192.168.1.1/24 192.168.1.2 00:50:79:66:68:00 20034 127.0.0.1:20035
fe80::250:79ff:fe66:6800/64

PC1> ping 192.168.1.2
84 bytes from 192.168.1.2 icmp_seq=1 ttl=255 time=30.248 ms
84 bytes from 192.168.1.2 icmp_seq=2 ttl=255 time=11.715 ms
^C
PC1> ping 192.168.1.3
84 bytes from 192.168.1.3 icmp_seq=1 ttl=64 time=0.591 ms
84 bytes from 192.168.1.3 icmp_seq=2 ttl=64 time=0.591 ms
^C
PC1> ping 192.168.2.1
84 bytes from 192.168.2.1 icmp_seq=1 ttl=62 time=169.386 ms
84 bytes from 192.168.2.1 icmp_seq=2 ttl=62 time=49.610 ms
84 bytes from 192.168.2.1 icmp_seq=3 ttl=62 time=76.180 ms
^C
PC1>
```

Figure 4-پینگ pc روبه رو را گرفته

```

PC1 PC3 PC2 PC4 R3 R4
VPCS is free software, distributed under the terms of the "BSD" licence. Source code and license can be found at vpcs.sf.net. For more information, please visit wiki.freecode.com.cn.
Press '?' to get help.
Executing the startup file
PC2> ip 192.168.2.1/24 192.168.2.2
Checking for duplicate address...
PC2 : 192.168.2.1 255.255.255.0 gateway 192.168.2.2
PC2> ping 192.168.2.4
84 bytes from 192.168.2.4 icmp_seq=1 ttl=64 time=0.657 ms
84 bytes from 192.168.2.4 icmp_seq=2 ttl=64 time=0.696 ms
^C
PC2> ping 192.168.1.1
84 bytes from 192.168.1.1 icmp_seq=1 ttl=60 time=85.526 ms
84 bytes from 192.168.1.1 icmp_seq=2 ttl=60 time=64.958 ms
^C
PC2> ping 192.168.1.1
84 bytes from 192.168.1.1 icmp_seq=1 ttl=62 time=84.157 ms
84 bytes from 192.168.1.1 icmp_seq=2 ttl=62 time=87.097 ms
84 bytes from 192.168.1.1 icmp_seq=3 ttl=62 time=70.939 ms
84 bytes from 192.168.1.1 icmp_seq=4 ttl=62 time=85.144 ms
^C
PC2>

```

Figure 5--پینگ pc روبه روبرو گرفته

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

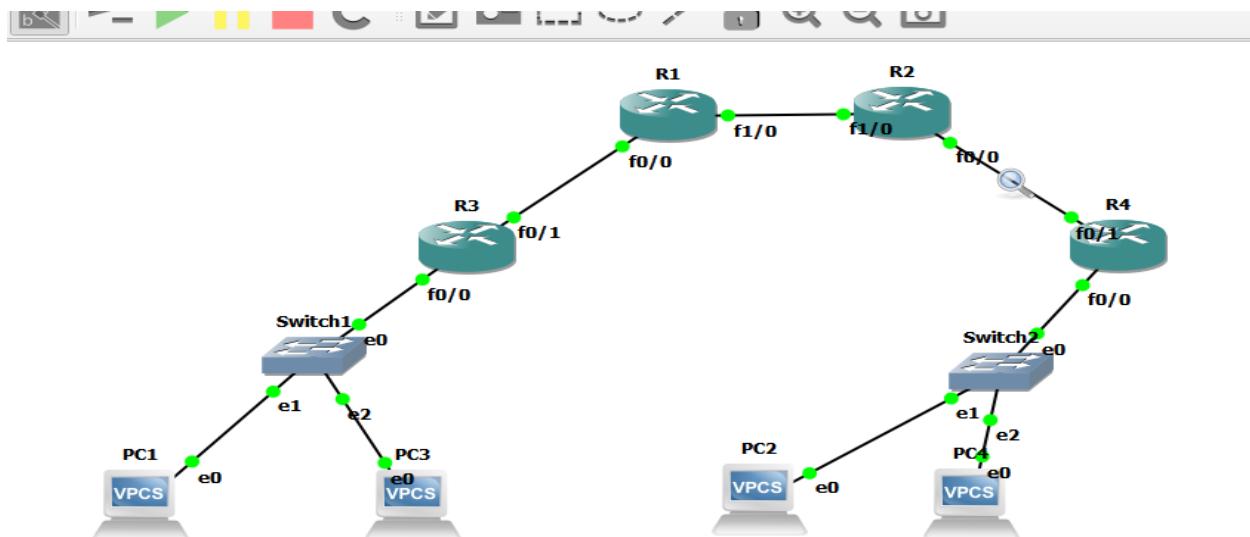


Figure 6-نشان دادن توپولوژی

No.	Time	Source	Destination	Protocol	Length	Info
13	25.674190	192.168.12.1	192.168.34.4	ESP	182	ESP (SPI=0xb2a38d8)
15	25.758046	192.168.12.1	192.168.34.4	ESP	182	ESP (SPI=0xb2a38d8)
17	25.820868	192.168.12.1	192.168.34.4	ESP	182	ESP (SPI=0xb2a38d8)
19	25.884744	192.168.12.1	192.168.34.4	ESP	182	ESP (SPI=0xb2a38d8)
10	25.063825	192.168.34.4	192.168.12.1	ESP	182	ESP (SPI=0xcc5b825d)
12	25.632572	192.168.34.4	192.168.12.1	ESP	182	ESP (SPI=0xcc5b825d)
14	25.695406	192.168.34.4	192.168.12.1	ESP	182	ESP (SPI=0xcc5b825d)
16	25.779175	192.168.34.4	192.168.12.1	ESP	182	ESP (SPI=0xcc5b825d)
18	25.831635	192.168.34.4	192.168.12.1	ESP	182	ESP (SPI=0xcc5b825d)
1	0.000000	cc:02:0b:d3:00:00	cc:02:0b:d3:00:00	LOOP	60	Reply
3	4.562540	cc:06:2a:bb:00:01	cc:06:2a:bb:00:01	LOOP	60	Reply
5	9.999167	cc:02:0b:d3:00:00	cc:02:0b:d3:00:00	LOOP	60	Reply

Frame 18: 182 bytes on wire (1456 bits), 182 bytes captured (1456 bits) on interface -, id 0 Ethernet II, Src: cc:06:2a:bb:00:01 (cc:06:2a:bb:00:01), Dst: cc:02:0b:d3:00:00 (cc:02:0b:d3:00:00) Internet Protocol Version 4, Src: 192.168.34.4, Dst: 192.168.12.1 Encapsulating Security Payload ESP SPI: 0xcc5b825d (3428549213) ESP Sequence: 21	<pre> 0000 cc 02 0b d3 00 00 cc 06 2a bb 00 01 08 00 45 00*....E- 0010 00 a8 01 1a 00 00 ff 32 0a b4 c0 a8 22 04 c0 a82..... 0020 0c 01 cc 5b 82 5d 00 00 00 15 a7 2c 92 3b c6 77 ...[]...;w 0030 9e 12 21 26 a4 5b 37 ca 43 6b 45 b9 c0 5f c8 0b ...!&[7- CkE... 0040 41 c7 4d c9 e3 3a 29 2f 9d 9d 6f 26 04 49 79 ee A-M-:/-o&Iy- 0050 81 d8 71 e8 40 84 30 62 2d ba ee 14 30 3f 1b 80 ...q @-b-...0?.. 0060 95 00 2d c4 f4 4b d1 12 36 6f f4 dd 5f a8 d8 23 ...-K-6o-...# 0070 be 61 de 9e 96 d3 60 58 dd 87 96 cd af 41 e6 84 ...a-X-A-... 0080 16 a5 b8 ee 70 40 47 7c 13 10 59 48 ea b1 02 6e ...-p@G -YH-...n 0090 0e cc a8 55 b7 f4 50 59 cb 75 63 41 20 61 de 08 ...U-PY-ucA a-... 00a0 d1 33 d6 1a e7 2b fc 0d 18 a4 f0 d8 f3 ac 86 7d ...3-++-...} 00b0 e9 1e 79 81 df 9fy... </pre>
--	--

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: