باسمه تعالی

درس: آزمایشگاه امنیت شبکه

نام و نام خانوادگی: هادی امینی

شماره دانشجویی: 9912762370

شماره آزمایش : 06

تاریخ تحویل: 1403/03/18

موضوع: **شبکه خصوصی مجازی (VPN)**

❖ انواع شبکه های خصوصی مجازی را بیان و نحوه پیاده سازی هر یک را شرح دهید.

شبکه‌های خصوصی مجازی (VPN) به طور کلی به دو دسته اصلی تقسیم می‌شوند:

1- VPNدسترسی از راه دور (Remote Access VPN)

این نوع VPN برای اتصال کاربران فردی به شبکه شرکت یا سازمان از مکان‌های مختلف استفاده می‌شود. این کاربران معمولاً از طریق اینترنت به سرور VPN شرکت متصل می‌شوند. کاربران از طریق نرم‌افزارهای کلاینت VPN بر روی دستگاه‌های خود به سرور VPN متصل می‌شوند تا به منابع شبکه داخلی مانند ایمیل‌ها، فایل‌ها و برنامه‌های کاربردی دسترسی پیدا کنند.

ویژگی‌ها:

- **کاربردها** :مناسب برای کارمندان دورکار، کارکنان فروش در حال حرکت، و هر کسی که نیاز به دسترسی امن به شبکه سازمانی دارد.
- **امنیت** :استفاده از پروتکل‌های امنیتی و رمزنگاری برای حفاظت از داده‌ها.
- **انعطاف‌پذیری** :امکان اتصال از هر نقطه‌ای که دسترسی به اینترنت وجود دارد.

نحوه پیاده‌سازی:

1. **انتخاب سرویس‌دهنده VPN :** انتخاب یک نرم‌افزار یا سرویس‌دهنده VPN مانندOpenVPN ، Cisco AnyConnectیا دیگر سرویس‌های مشابه.
2. **نصب و تنظیمات سرور VPN** : نصب نرم‌افزار VPN بر روی سرور یا استفاده از روترهای VPN و تنظیمات مربوطه برای دسترسی کاربران.
3. **توزیع کلاینت VPN به کاربران** :نصب و پیکربندی نرم‌افزار کلاینت VPN بر روی دستگاه‌های کاربران.

4. **تنظیمات امنیتی** :تعریف پروتکل‌های امنیتی و رمزنگاری برای ارتباط امن.
5. **اتصال کاربران** :کاربران می‌توانند از طریق نرم‌افزار کلاینت به سرور VPN متصل شوند و به منابع شبکه داخلی دسترسی پیدا کنند.

2- vpn سایت به سایت(Site-to-Site VPN)

این نوع VPN برای اتصال دو یا چند شبکه محلی (LAN) در مکان‌های جغرافیایی مختلف به کار می‌رود. معمولاً بین دفاتر یک سازمان که در نقاط مختلف قرار دارند استفاده می‌شود. این نوع VPN معمولاً بین روترها یا فایروال‌های هر شبکه تنظیم می‌شود تا یک ارتباط امن و دائمی بین شبکه‌ها برقرار شود.

ویژگی‌ها:

- **کاربردها** :مناسب برای سازمان‌هایی که دارای دفاتر متعدد در مکان‌های مختلف هستند و نیاز به ارتباط دائم و امن بین این دفاتر دارند.
- **امنیت** :استفاده از پروتکل‌های رمزنگاری و احراز هویت برای اطمینان از امنیت ارتباط.
- **پایداری** :ارتباط دائمی و پایدار بین شبکه‌ها، بدون نیاز به اتصال مجدد توسط کاربران.

نحوه پیاده‌سازی:

1. **انتخاب روتر یا فایروال مناسب** :اطمینان از اینکه روتر یا فایروال‌های موجود از قابلیت VPN پشتیبانی می‌کنند.
2. **پیکربندی روترها** :تنظیمات روترها برای ایجاد تونل VPN بین سایت‌ها. این شامل تنظیمات IPsec یا پروتکل‌های مشابه می‌شود.
3. **تعریف سیاست‌های مسیریابی** :تنظیمات مسیریابی برای اطمینان از اینکه ترافیک بین شبکه‌ها از طریق تونل VPN عبور می‌کند.
4. **تنظیمات امنیتی** :تعیین کلیدهای رمزنگاری و پروتکل‌های امنیتی برای اطمینان از امنیت تونل.VPN
5. **تست اتصال** :بررسی و تست اتصال بین شبکه‌ها و اطمینان از کارکرد صحیح تونل.VPN

❖ تفاوت بین دو پروتکل IPSec و GRE را توضیح دهید.

در حوزه شبکه‌های کامپیوتری، پروتکل‌های GRE (Generic Routing Encapsulation) و IPSec (IP Security) هر دو نقشی اساسی در انتقال داده‌ها ایفا می‌کنند .با این وجود، هریک از آن‌ها اهداف و عملکردهای متمایزی را دنبال می‌کنند که در ادامه به بررسی تفصیلی آنها می‌پردازیم.

GRE:

- **GRE**به عنوان یک پروتکل **تونل‌سازی** شناخته می‌شود که وظیفه **کپسوله کردن و انتقال بسته‌های سایر پروتکل‌ها** را در بستر شبکه IP بر عهده دارد.

- از این پروتکل می‌توان برای **انتقال ترافیک IPX** بر روی شبکه‌های IP و یا **ایجادVPN های ساده** بهره برد.
- **GREفاقد هرگونه مکانیزم امنیتی** بوده و به طور پیش‌فرض، بسته‌های GRE **بدون رمزنگاری** ارسال می‌شوند.
- ماهیت **بدون حالت** این پروتکل ایجاب می‌کند که هر بسته به طور مستقل مسیریابی شده و هیچ ارتباطی بین بسته‌ها حفظ نگردد.

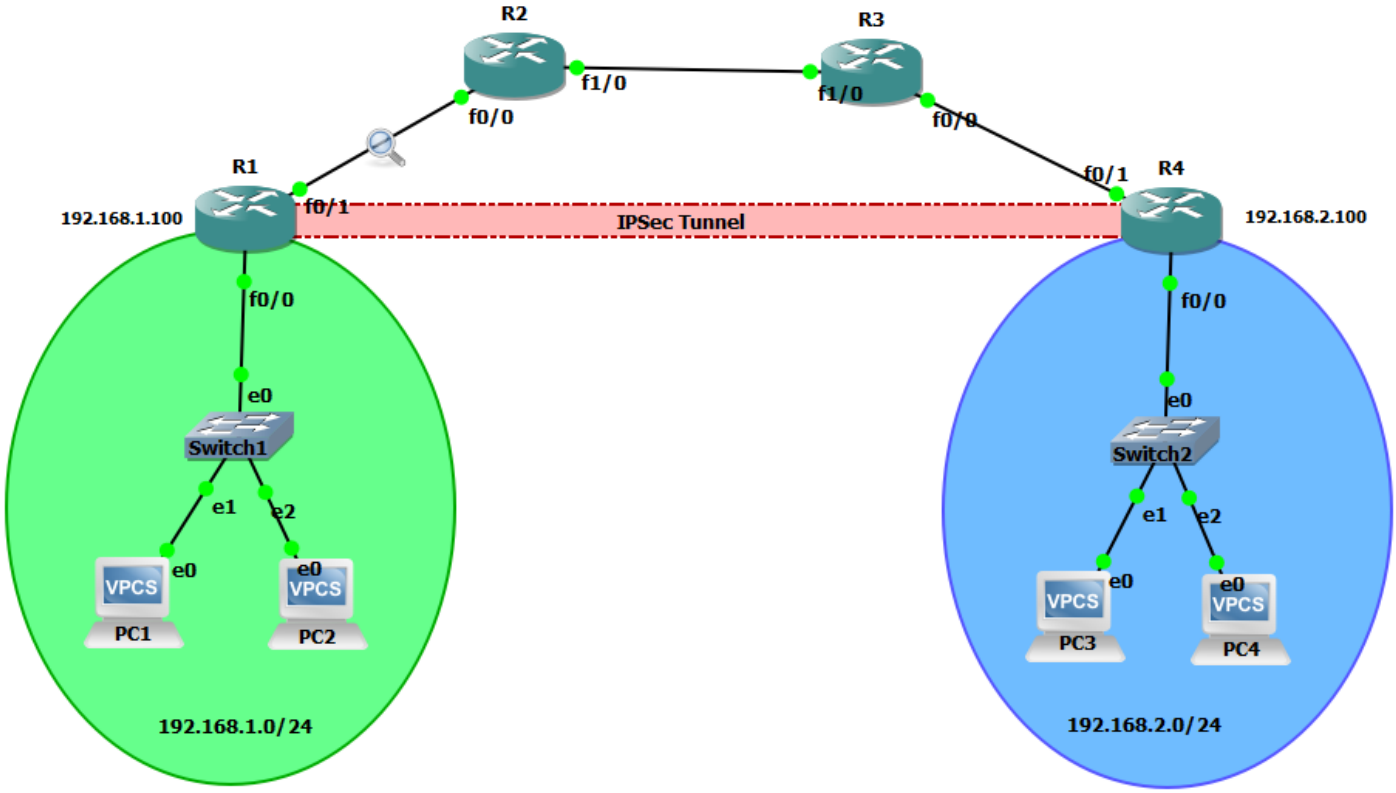
IPSec:

- **IPSec**مجموعه‌ای از **پروتکل‌های امنیتی** است که با هدف **محرمانه کردن، احراز هویت و حفظ یکپارچگی داده‌ها** در حین انتقال آنها از طریق شبکه‌های IP طراحی شده است.
- کاربرد برجسته **IPSec**در **ایجادVPN های امن** بین دو نقطه انتهایی است.
- این پروتکل قادر به کار در **دو حالت حمل و نقل و تونل** می‌باشد:
  - در **حالت حمل و نقل** تنها **هدرهای IP** رمزگذاری می‌شوند، در حالی که **حالت تونل** کل بسته IP را در یک بسته IP جدید کپسوله می‌کند.
- **IPSec**با استفاده از **الگوریتم‌های رمزنگاری قدرتمند**، از داده‌ها در برابر **استراق سمع و دستکاری** محافظت می‌کند.
- ماهیت **با حالت** این پروتکل ایجاب می‌کند که از **انجمن‌های امنیتی** برای حفظ ارتباط بین بسته‌ها و پیگیری وضعیت تبادل اطلاعات استفاده شود.

مقایسه نهایی:

- **GRE**برای **تونل‌سازی و انتقال بسته‌های سایر پروتکل‌ها** کاربرد دارد، در حالی که **IPSec**بر **امن‌سازی ارتباطات IP**تمرکز دارد.
- **GREفاقد هرگونه تمهیدات امنیتی** است، در حالی که **IPSec**با اتکا به **رمزنگاری قوی** از داده‌ها محافظت می‌کند.
- **GRE**یک پروتکل **بدون حالت** است، در حالی که **IPSec**از نوع **با حالت** می‌باشد.

بخش عملی:



دستورات مربوط به فاز ISAKMP 1 در روتر R1 :

```
R1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#crypto isakmp policy 1
R1(config-isakmp)#encryption 3des
R1(config-isakmp)#hash md5
R1(config-isakmp)#authentication pre-share
R1(config-isakmp)#group 2
R1(config-isakmp)#lifetime 86400
```

تعریف کلید مشترک :

```
R1(config)#crypto isakmp key hadi address 192.168.34.4
```

تنظیم پارامتر های فاز ISAKMP 2 :

```
R1(config)#crypto ipsec transform-set TSET esp-3des esp-md5-hmac
```

تنظیم Extended ACL و Crypto MAP:

در این مرحله، برای مطابقت با ترافیک شبکه، نیاز به پیکربندی «فهرست کنترل دسترسی توسعه‌یافته» (Extended ACL) و «نگاشت رمزنگاری» (Crypto Map) داریم.

```
R1(config)#ip access-list extended IPSEC_List
R1(config-ext-nacl)#permit ip 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255
R1(cfg-crypto-trans)#crypto map CMAP 1 ipsec-isakmp
R1(config-crypto-map)#set peer 192.168.34.4
R1(config-crypto-map)#set transform-set TSET
R1(config-crypto-map)#match address IPSEC_List
```

اعمال crypto Map به اینترفیس خروجی:

```
R1(config)#interface FastEthernet 0/1
R1(config-if)#crypto map CMAP
```

مستثنی کردن ترافیک VPN IPSec از NAT :

```
R1(config)#access-list 100 deny ip 192.168.1.0 0.0.0.255 192.168.2.0
0.0.0.255
R1(config)#access-list 100 permit ip 192.168.1.0 0.0.0.255 any
```

```
R1(config)#ip nat inside source list 100 interface FastEthernet 0/1 over-
load
```

```
R1(config)#in FastEthernet0/1
R1(config-if)#ip nat outside
R1(config-if)#in FastEthernet0/0
R1(config-if)#ip nat inside
```

پیکربندی روتر R4:

```
R4#configure terminal
R4(config)#crypto isakmp policy 1
R4(config-isakmp)# encryption 3des
R4(config-isakmp)# hash md5
R4(config-isakmp)# authentication pre-share
R4(config-isakmp)# group 2
R4(config-isakmp)# lifetime 86400
```

```
R4(config)#crypto isakmp key hadi address 192.168.12.1
```

```
R4(config)#crypto ipsec transform-set TSET esp-3des 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 CMAP 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)#interface FastEthernet 0/0

R4(config-if)#crypto map CMAP
```

```
R4(config)#access-list 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 0/0 over-
load

R4(config)#in FastEthernet0/0

R4(config-if)#ip nat outside

R4(config-if)#in FastEthernet1/0

R4(config-if)#ip nat inside
```

```
R1(config)#crypto isakmp policy 1
R1(config-isakmp)#encryption 3des
R1(config-isakmp)#hash md5
R1(config-isakmp)#authentication pre-share
R1(config-isakmp)#group 2
R1(config-isakmp)#lifetime 86400
R1(config-isakmp)#exit
R1(config)#crypto isakmp key hadi address 192.168.34.4
R1(config)#crypto ipsec transform-set TSET esp-3des esp-md5-hmac
R1(cfg-crypto-trans)#exit
R1(config)#ip access-list extended IPSEC_List
R1(config-ext-nacl)#permit ip 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255
R1(config-ext-nacl)#exit
R1(config)#crypto ipsec transform-set TSET esp-3des esp-md5-hmac
R1(cfg-crypto-trans)#crypto map CMAP 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)#set peer 192.168.34.4
R1(config-crypto-map)#set transform-set TSET
R1(config-crypto-map)#match address IPSEC_List
R1(config-crypto-map)#interface FastEthernet 0/1
R1(config-if)#crypto map CMAP
R1(config-if)#
*Mar  1 00:20:51.995: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
R1(config-if)#$ 100 deny ip 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255
R1#
R1#
*Mar  1 00:21:46.983: %SYS-5-CONFIG_I: Configured from console by console
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#access-list 100 deny ip 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255
R1(config)#access-list 100 permit ip 192.168.1.0 0.0.0.255 any
R1(config)#ip nat inside source list 100 interface FastEthernet 0/1 overload
R1(config)#
*Mar  1 00:25:37.871: %LINEPROTO-5-UPDOWN: Line protocol on Interface NVI0, changed state to up
```

تصویر 1 - انجام کانفیگ در روتر

```
R1(config)#in FastEthernet0/1
R1(config-if)#ip nat outside
R1(config-if)#in FastEthernet0/0
R1(config-if)#
R1(config-if)#
R1(config-if)#
R1(config-if)#
R1(config-if)#
R1(config-if)#
R1(config-if)#exit
R1(config)#in FastEthernet0/0
R1(config-if)#ip nat inside
R1(config-if)#exit
```

تصویر 2 - تنظیم اینترفیس ورودی و خروجی NAT

```
R1#ping 192.168.2.100 source 192.168.1.100

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.2.100, timeout is 2 seconds:
Packet sent with a source address of 192.168.1.100
.....
Success rate is 0 percent (0/5)
R1#ping 192.168.2.100 source 192.168.1.100

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.2.100, timeout is 2 seconds:
Packet sent with a source address of 192.168.1.100
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 36/44/52 ms
R1#write mem
R1#write memory
Building configuration...
[OK]
R1#ping 192.168.14.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.14.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 44/59/84 ms
R1#
```

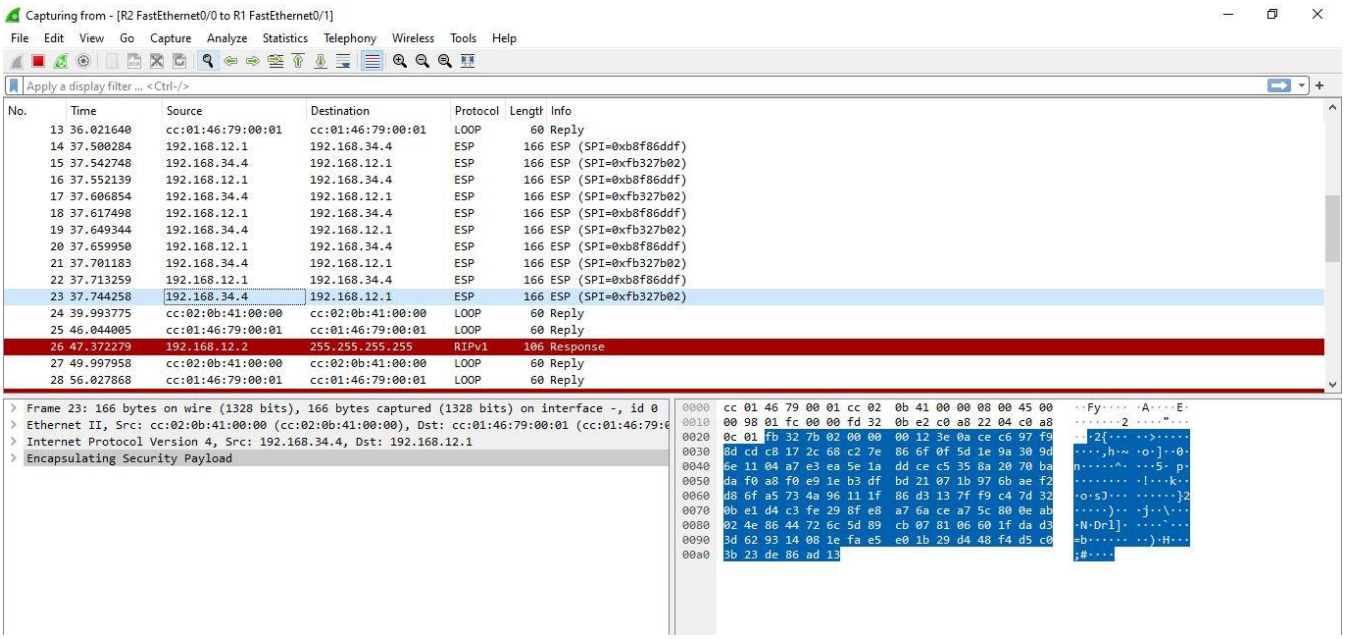
تصویر 3 - پینگ در روتر 1

```
R4#ping 192.168.1.100 source 192.168.2.100

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.100, timeout is 2 seconds:
Packet sent with a source address of 192.168.2.100
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 52/84/116 ms
R4#ping 192.168.14.4

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.14.4, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 16/32/44 ms
R4#
```

تصویر 4- پینگ در روتر 4



تصویر 5- تحلیل ترافیک در وایرشارک