ACTIVIDAD 06
Implementación IPSec VPN

Pedro Damian Jasso Dávila - 176658
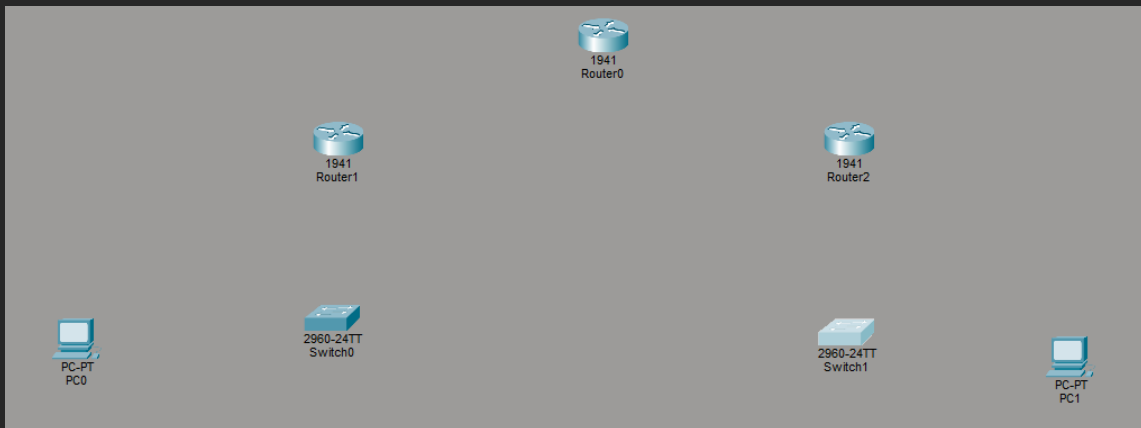
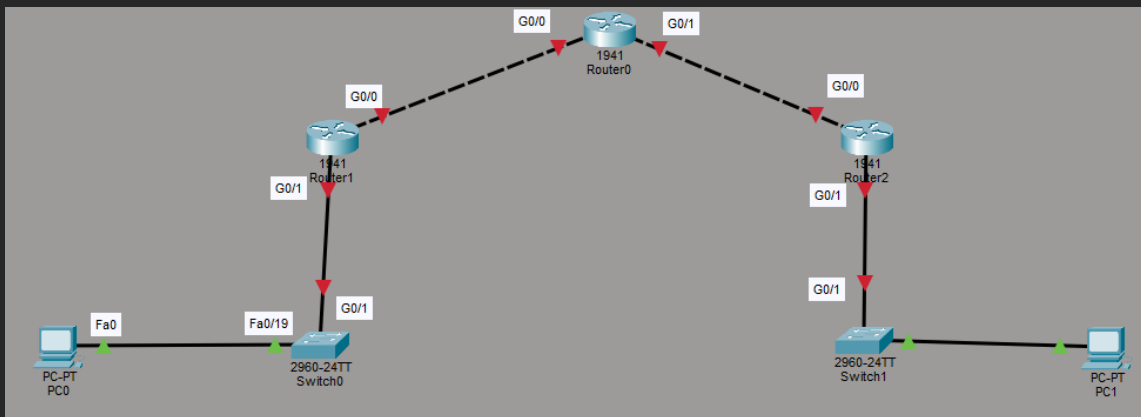*CNO V: Seguridad Informática*

16/02/2026

Mtro. Servando López Contreras

1) Configuración Inicial

Para hacer la configuración inicial en packet Tracer usamos 3 Routers 1941, 2 Switches 2960 y dos PC's para iniciar.

Ahora conectamos de la siguiente manera.

Ahora desde la terminal del Router 1 vamos a hacer la siguiente configuración inicial.

```
Press RETURN to get started!


Router>en
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname R1
R1(config)#interface G0/1
R1(config-if)#ip address 192.168.1.1 255.255.255.0
R1(config-if)#no shut

R1(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to up

R1(config-if)#interface G0/0
R1(config-if)#ip address 209.165.100.1 255.255.255.0
R1(config-if)#no shut

R1(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up
ip route 0.0.0.0 0.0.0.0 209.165.100.2
R1(config)#
```
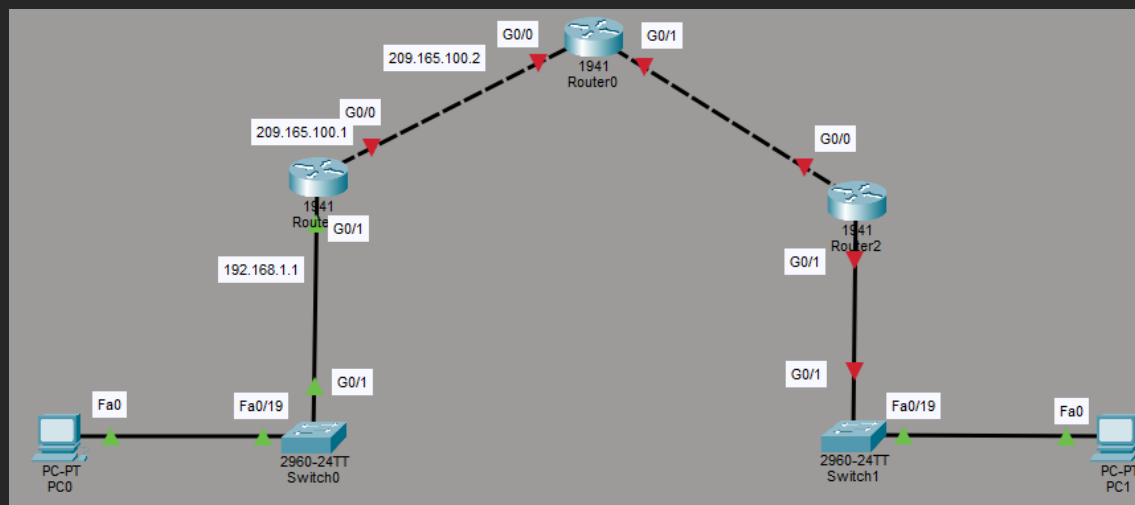
Copy   Paste

Quedando de la siguiente manera.

Ahora vamos con la configuración del Router 2.

```
Press RETURN to get started!


Router>en
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname R2
R2(config)#Interface G0/1
R2(config-if)#ip address 192.168.3.1 255.255.255.0
R2(config-if)#no shut

R2(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to up

R2(config-if)#interface G0/0
R2(config-if)#ip address 209.165.200.1 255.255.255.0
R2(config-if)#no shut

R2(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up

R2(config-if)#ip route 0.0.0.0 0.0.0.0 209.165.200.2
R2(config)#
```
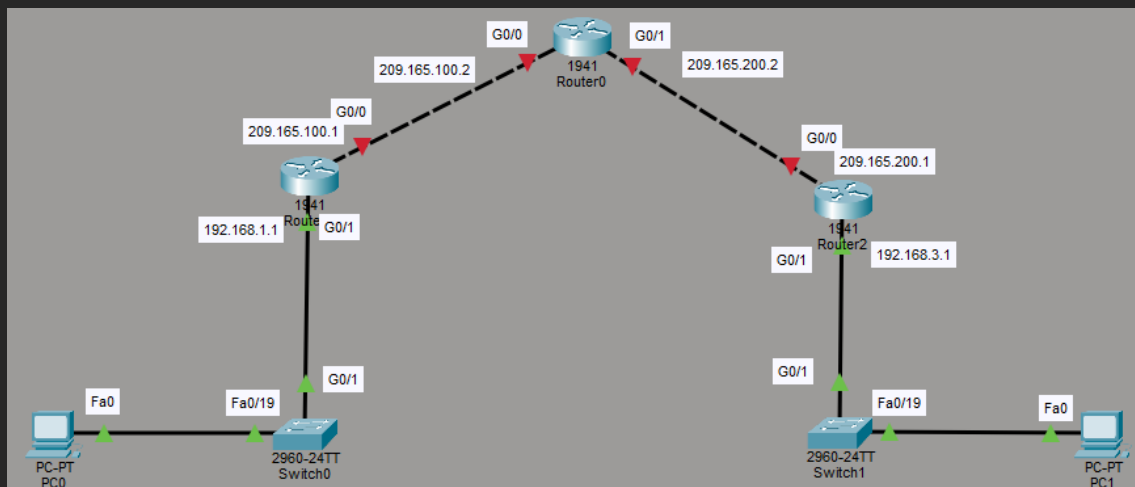
Copy   Paste

Top

Ahora quedando de la siguiente manera.

Ahora vamos a configurar el router ISP (Router 0).

```
        --- System Configuration Dialog ---

Would you like to enter the initial configuration dialog? [yes/no]: n


Press RETURN to get started!



Router>en
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname ISP
ISP(config)#interface G0/0
ISP(config-if)#ip address 209.165.100.2 255.255.255.0
ISP(config-if)#no shut

ISP(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to up

ISP(config-if)#interface G0/1
ISP(config-if)#ip address 209.165.200.2 255.255.255.0
ISP(config-if)#no shut

ISP(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to up

ISP(config-if)#ip route 0.0.0.0 0.0.0.0 209.165.200.1
ISP(config)#
```

Copy   Paste

Al final quedando así.
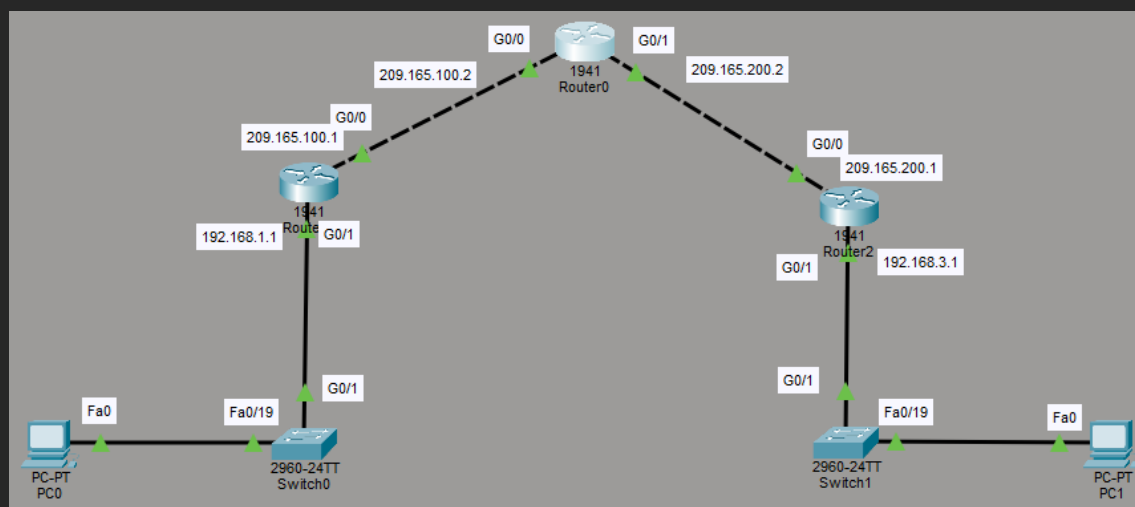
2) Licencia de seguridad Habilitada

Estas licencias se activan en el router 1 y router 2 con el siguiente comando

#license boot module c1900 technology-package securityk9

R1

```
R1>en
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#license boot module c1900 technology-package securityk9
PLEASE  READ THE  FOLLOWING TERMS  CAREFULLY. INSTALLING THE LICENSE OR
LICENSE  KEY  PROVIDED FOR  ANY CISCO  PRODUCT  FEATURE  OR  USING SUCH
PRODUCT  FEATURE  CONSTITUTES  YOUR  FULL ACCEPTANCE  OF  THE FOLLOWING
TERMS. YOU MUST NOT PROCEED FURTHER IF YOU ARE NOT WILLING TO  BE BOUND
BY ALL THE TERMS SET FORTH HEREIN.

Use of this product feature requires  an additional license from Cisco,
together with an additional  payment.  You may use this product feature
on an evaluation basis, without payment to Cisco, for 60 days. Your use
of the  product,  including  during the 60 day  evaluation  period,  is
subject to the Cisco end user license agreement
http://www.cisco.com/en/US/docs/general/warranty/English/EU1KEN_.html
If you use the product feature beyond the 60 day evaluation period, you
must submit the appropriate payment to Cisco for the license. After the
60 day  evaluation  period,  your  use of the  product  feature will be
governed  solely by the Cisco  end user license agreement (link above),
together  with any supplements  relating to such product  feature.  The
above  applies  even if the evaluation  license  is  not  automatically
terminated  and you do  not receive any notice of the expiration of the
evaluation  period.  It is your  responsibility  to  determine when the
evaluation  period is complete and you are required to make  payment to
Cisco for your use of the product feature beyond the evaluation period.

Your  acceptance  of  this agreement  for the software  features on one
product  shall be deemed  your  acceptance  with  respect  to all  such
software  on all Cisco  products  you purchase  which includes the same
software.  (The foregoing  notwithstanding, you must purchase a license
for each software  feature you use past the 60 days evaluation  period,
so  that  if you enable a software  feature on  1000  devices, you must
purchase 1000 licenses for use past  the 60 day evaluation period.)
```

```
Use of this product feature requires  an additional license from Cisco,
together with an additional  payment.  You may use this product feature
on an evaluation basis, without payment to Cisco, for 60 days. Your use
of the  product,  including  during the 60 day  evaluation  period,  is
subject to the Cisco end user license agreement
http://www.cisco.com/en/US/docs/general/warranty/English/EU1KEN_.html
If you use the product feature beyond the 60 day evaluation period, you
must submit the appropriate payment to Cisco for the license. After the
60 day  evaluation  period,  your  use of the  product  feature will be
governed  solely by the Cisco  end user license agreement (link above),
together  with any supplements  relating to such product  feature.  The
above  applies  even if the evaluation  license  is  not  automatically
terminated  and you do  not receive any notice of the expiration of the
evaluation  period.  It is your  responsibility  to  determine when the
evaluation  period is complete and you are required to make  payment to
Cisco for your use of the product feature beyond the evaluation period.

Your  acceptance  of  this agreement  for the software  features on one
product  shall be deemed  your  acceptance  with  respect  to all  such
software  on all Cisco  products  you purchase  which includes the same
software.  (The foregoing  notwithstanding, you must purchase a license
for each software  feature you use past the 60 days evaluation  period,
so  that  if you enable a software  feature on  1000  devices, you must
purchase 1000 licenses for use past  the 60 day evaluation period.)

Activation  of the  software command line interface will be evidence of
your acceptance of this agreement.


ACCEPT? [yes/no]: y
% use 'write' command to make license boot config take effect on next boot

R1(config)#: %IOS_LICENSE_IMAGE_APPLICATION-6-LICENSE_LEVEL: Module name = C1900 Next
reboot level = securityk9 and License = securityk9

R1(config)#exit
R1#
%SYS-5-CONFIG_I: Configured from console by console
```

```
copy run start
Destination filename [startup-config]?
Building configuration...
[OK]
R1#reload
```

```
R1>en
R1#show version
Cisco IOS Software, C1900 Software (C1900-UNIVERSALK9-M), Version 15.1(4)M4, RELEASE
SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2007 by Cisco Systems, Inc.
Compiled Wed 23-Feb-11 14:19 by pt_team

ROM: System Bootstrap, Version 15.1(4)M4, RELEASE SOFTWARE (fc1)
cisco1941 uptime is 1 minutes, 1 seconds
System returned to ROM by power-on
System image file is "flash0:c1900-universalk9-mz.SPA.151-1.M4.bin"
Last reload type: Normal Reload

This product contains cryptographic features and is subject to United
States and local country laws governing import, export, transfer and
use. Delivery of Cisco cryptographic products does not imply
third-party authority to import, export, distribute or use encryption.
Importers, exporters, distributors and users are responsible for
compliance with U.S. and local country laws. By using this product you
agree to comply with applicable laws and regulations. If you are unable
to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html
 --More--
```

R2

```
R2>en
R2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#license boot module c1900 technology-package securityk9
PLEASE  READ THE  FOLLOWING TERMS  CAREFULLY. INSTALLING THE LICENSE OR
LICENSE  KEY  PROVIDED FOR  ANY CISCO  PRODUCT  FEATURE  OR  USING SUCH
PRODUCT  FEATURE  CONSTITUTES  YOUR  FULL ACCEPTANCE  OF  THE FOLLOWING
TERMS. YOU MUST NOT PROCEED FURTHER IF YOU ARE NOT WILLING TO  BE BOUND
BY ALL THE TERMS SET FORTH HEREIN.

Use of this product feature requires  an additional license from Cisco,
together with an additional  payment.  You may use this product feature
on an evaluation basis, without payment to Cisco, for 60 days. Your use
of the  product,  including  during the 60 day  evaluation  period,  is
subject to the Cisco end user license agreement
http://www.cisco.com/en/US/docs/general/warranty/English/EU1KEN_.html
If you use the product feature beyond the 60 day evaluation period, you
must submit the appropriate payment to Cisco for the license. After the
60 day  evaluation  period,  your  use of the  product  feature will be
governed  solely by the Cisco  end user license agreement (link above),
together  with any supplements  relating to such product  feature.  The
above  applies  even if the evaluation  license  is  not  automatically
terminated  and you do  not receive any notice of the expiration of the
evaluation  period.  It is your  responsibility  to  determine when the
evaluation  period is complete and you are required to make  payment to
Cisco for your use of the product feature beyond the evaluation period.

Your  acceptance  of  this agreement  for the software  features on one
product  shall be deemed  your  acceptance  with  respect  to all  such
software  on all Cisco  products  you purchase  which includes the same
software.  (The foregoing  notwithstanding, you must purchase a license
for each software  feature you use past the 60 days evaluation  period,
so  that  if you enable a software  feature on  1000  devices, you must
purchase 1000 licenses for use past  the 60 day evaluation period.)

Activation  of the  software command line interface will be evidence of
your acceptance of this agreement.
```

```
ACCEPT? [yes/no]: y
% use 'write' command to make license boot config take effect on next boot

R2(config)#: %IOS_LICENSE_IMAGE_APPLICATION-6-LICENSE_LEVEL: Module name = C1900 Next
reboot level = securityk9 and License = securityk9

R2(config)#copy run start
                 ^
% Invalid input detected at '^' marker.

R2(config)#reload
```

```
R2(config)#exit
R2#
%SYS-5-CONFIG_I: Configured from console by console
copy run start
Destination filename [startup-config]?
Building configuration...
[OK]
R2#reload
```

```
R2>en
R2#show version
Cisco IOS Software, C1900 Software (C1900-UNIVERSALK9-M), Version 15.1(4)M4, RELEASE
SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2007 by Cisco Systems, Inc.
Compiled Wed 23-Feb-11 14:19 by pt_team

ROM: System Bootstrap, Version 15.1(4)M4, RELEASE SOFTWARE (fc1)
cisco1941 uptime is 1 minutes, 6 seconds
System returned to ROM by power-on
System image file is "flash0:c1900-universalk9-mz.SPA.151-1.M4.bin"
Last reload type: Normal Reload

This product contains cryptographic features and is subject to United
States and local country laws governing import, export, transfer and
use. Delivery of Cisco cryptographic products does not imply
third-party authority to import, export, distribute or use encryption.
Importers, exporters, distributors and users are responsible for
compliance with U.S. and local country laws. By using this product you
agree to comply with applicable laws and regulations. If you are unable
to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html
 --More--  |
```

3) Implementación ACLs

```
R1>en
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#access-list 100 permit ip 192.168.1.0 0.0.0.255 192.168.3.0 0.0.0.255
R1(config)#|
```

```
R2>en
R2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#access-list 100 permit ip 192.168.3.0 0.0.0.255 192.168.1.0 0.0.0.255
R2(config)#|
```

4) Phase 01: ISAKMP policy

```
R1>en
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#access-list 100 permit ip 192.168.1.0 0.0.0.255 192.168.3.0 0.0.0.255
R1(config)#crypto isakmp policy 10
R1(config-isakmp)#encryption aes 256
R1(config-isakmp)#authentication pre-share
R1(config-isakmp)#group 5
R1(config-isakmp)#exit
R1(config)#crypto isakmp key secretkey address 209.165.200.1
R1(config)#|
```

```
R2>en
R2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#access-list 100 permit ip 192.168.3.0 0.0.0.255 192.168.1.0 0.0.0.255
R2(config)#crypto isakmp policy 10
R2(config-isakmp)#encryption aes 256
R2(config-isakmp)#authentication pre-share
R2(config-isakmp)#group 5
R2(config-isakmp)#exit
R2(config)#crypto isakmp key secretkey address 209.165.100.1
R2(config)#
```

5) Phase 02: IPSec transform-set

```
R1(config)#crypto ipsec transform-set R1->R3 esp-aes 256 esp-sha-hmac
R1(config)#
```

```
R2(config)#
R2(config)#crypto ipsec transform-set R3->R1 esp-aes 256 esp-sha-hmac
R2(config)#
```

6) Crear el mapa criptográfico

```
R1(config)#
R1(config)#crypto map IPSEC-MAP 10 ipsec-isamkp
                                          ^
% Invalid input detected at '^' marker.

R1(config)#crypto map IPSEC-MAP 10 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 209.165.200.1
R1(config-crypto-map)#set pfs group5
R1(config-crypto-map)#
```

```
R2(config)#
R2(config)#crypto map IPSEC-MAP 10 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)#set peer 209.165.100.1
R2(config-crypto-map)#set pfs group5
R2(config-crypto-map)#
```

```
R2(config-crypto-map)#set pfs group5
R2(config-crypto-map)#
R2(config-crypto-map)#set security-association lifetime seconds 86400
R2(config-crypto-map)#set transform-set R3->R1
R2(config-crypto-map)#match
% Incomplete command.
R2(config-crypto-map)#match address 100
R2(config-crypto-map)#
```

7) Aplicar el mapa criptográfico

```
R1(config-crypto-map)#set pfs group5
R1(config-crypto-map)#
R1(config-crypto-map)#exit
R1(config)#int g0/0
R1(config-if)#crypto map IPSEC-Map
ERROR: Crypto Map with tag IPSEC-Map does not exist.

R1(config-if)#crypto map IPSEC-MAP
*Jan  3 07:16:26.785: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
R1(config-if)#
```

```
R2(config-crypto-map)#match address 100
R2(config-crypto-map)#
R2(config-crypto-map)#exit
R2(config)#int g0/0
R2(config-if)#crypto map IPSEC-MAP
*Jan  3 07:16:26.785: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
R2(config-if)#
```