

COURSE: CLOUD AND NETWORK SECURITY

NAME: DENISE SOPHY ONDISO MUTAYI

STUDENT NO: CS-CN09-25047

CONFIGURING SITE-TO-SITE VPNS

Table of contents

| | |
|---|----|
| INTRODUCTION..... | 3 |
| PART 1: CONFIGURE IPSEC PARAMETERS ON R1..... | 4 |
| Step 1: Test connectivity..... | 4 |
| Step 2: Enable the Security Technology package. | 4 |
| Step 3: Identify interesting traffic on R1..... | 6 |
| Step 4: Configure IKE Phase 1 (ISAKMP) on R1 | 6 |
| Step 5: Configure IKE Phase 2 (IPsec) on R1 | 7 |
| Step 6: Apply the Crypto Map to the Interface..... | 7 |
| Part 2: Configure IPsec on R3..... | 8 |
| Step 1: Enable the Security Technology package. | 8 |
| Step 2: Configure router R3 to support a site-to-site VPN with R1. | 8 |
| Step 3: Configure the IKE Phase 1 ISAKMP properties on R3. | 9 |
| Step 4: Configure the IKE Phase 2 IPsec policy on R3. | 9 |
| Step 5: Configure the crypto map on the outgoing interface..... | 10 |
| Part 3: Verify the IPsec VPN..... | 10 |
| Step 1: Verify the tunnel prior to interesting traffic..... | 10 |
| Step 2: Create interesting traffic..... | 11 |
| Step 3: Verify the tunnel after interesting traffic. | 11 |
| Step 4: Create uninteresting traffic. | 12 |
| Step 5: Verify the tunnel..... | 12 |
| Step 6: Check results..... | 13 |
| CONCLUSION..... | 14 |

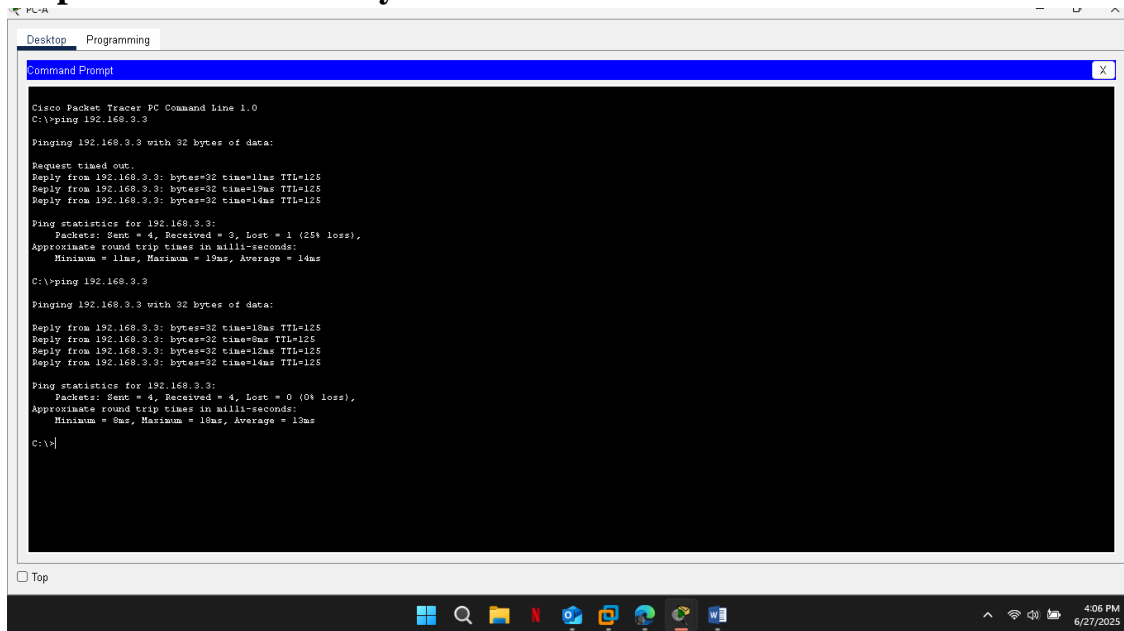
INTRODUCTION

This Packet Tracer activity involved the configuration and verification of a site-to-site IPsec VPN between two routers, R1 and R3, which were connected through an intermediary router, R2, acting as a simple pass-through with no VPN awareness. The primary goal was to secure communication between the LANs of R1 (192.168.1.0/24) and R3 (192.168.3.0/24) by using IPsec to encrypt traffic across the untrusted transit network.

The task included enabling the securityk9 license package on both R1 and R3, defining interesting traffic using ACL 110, configuring IKE Phase 1 (ISAKMP) policies with AES-256 encryption and DH Group 5 key exchange, and setting up IPsec Phase 2 with ESP using AES and SHA-HMAC for authentication. The VPN configuration was finalized using crypto maps, which were applied to the appropriate serial interfaces. Throughout the process, commands such as `show crypto isakmp sa` and `show crypto ipsec sa` were used to verify tunnel establishment and packet encryption.

PART 1: CONFIGURE IPSEC PARAMETERS ON R1

Step 1: Test connectivity.



```
Command Prompt

Cisco Packet Tracer PC Command line 1.0
C:\>ping 192.168.3.3

Pinging 192.168.3.3 with 32 bytes of data:

Request timed out.
Reply from 192.168.3.3: bytes=32 time=11ms TTL=125
Reply from 192.168.3.3: bytes=32 time=19ms TTL=125
Reply from 192.168.3.3: bytes=32 time=14ms TTL=125

Ping statistics for 192.168.3.3:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 11ms, Maximum = 19ms, Average = 14ms

C:\>ping 192.168.3.3

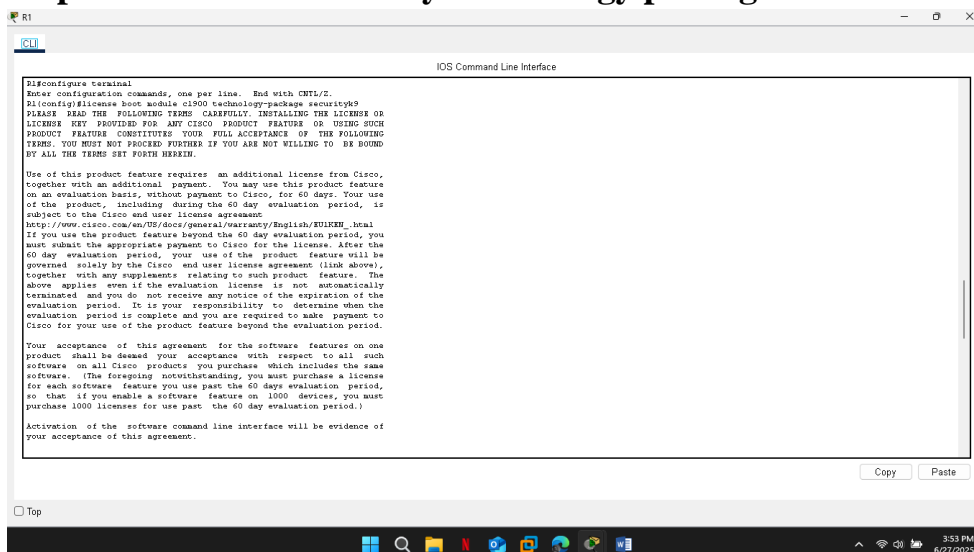
Pinging 192.168.3.3 with 32 bytes of data:

Reply from 192.168.3.3: bytes=32 time=10ms TTL=125
Reply from 192.168.3.3: bytes=32 time=8ms TTL=125
Reply from 192.168.3.3: bytes=32 time=12ms TTL=125
Reply from 192.168.3.3: bytes=32 time=14ms TTL=125

Ping statistics for 192.168.3.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 8ms, Maximum = 14ms, Average = 13ms

C:\>
```

Step 2: Enable the Security Technology package.



```
R1
CLI

R1#configure terminal
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/EULKEN.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.

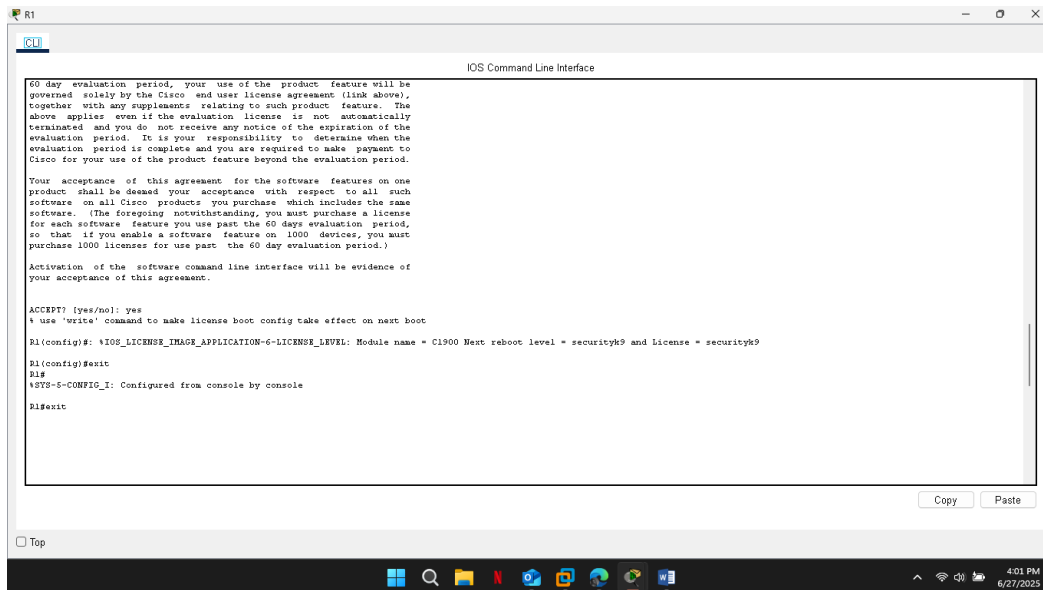
Your acceptance of this agreement for the software features on one
product shall be deemed your acceptance with respect to all such
software on all Cisco products you purchase which includes the same
software. (The foregoing notwithstanding, you must purchase a license
for each software feature you use 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.

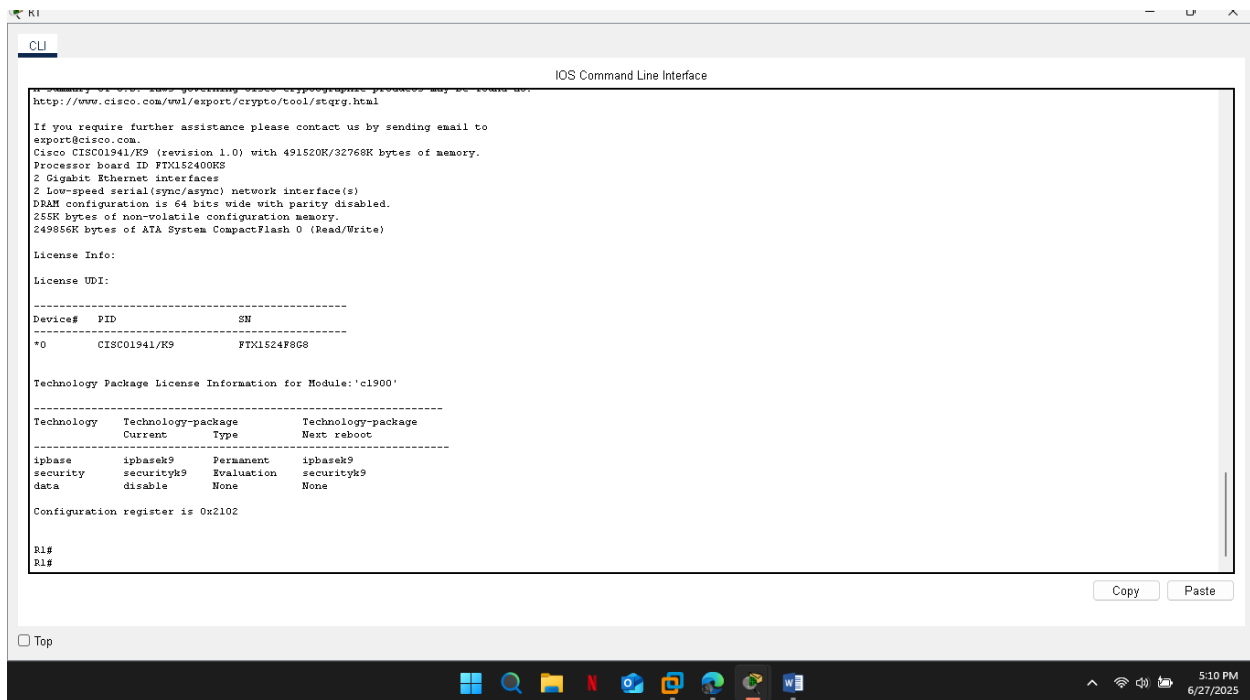
Copy Paste
```

Enable the security technology package by using the following command to enable the package.

R1(config)# license boot module c1900 technology-package securityk9

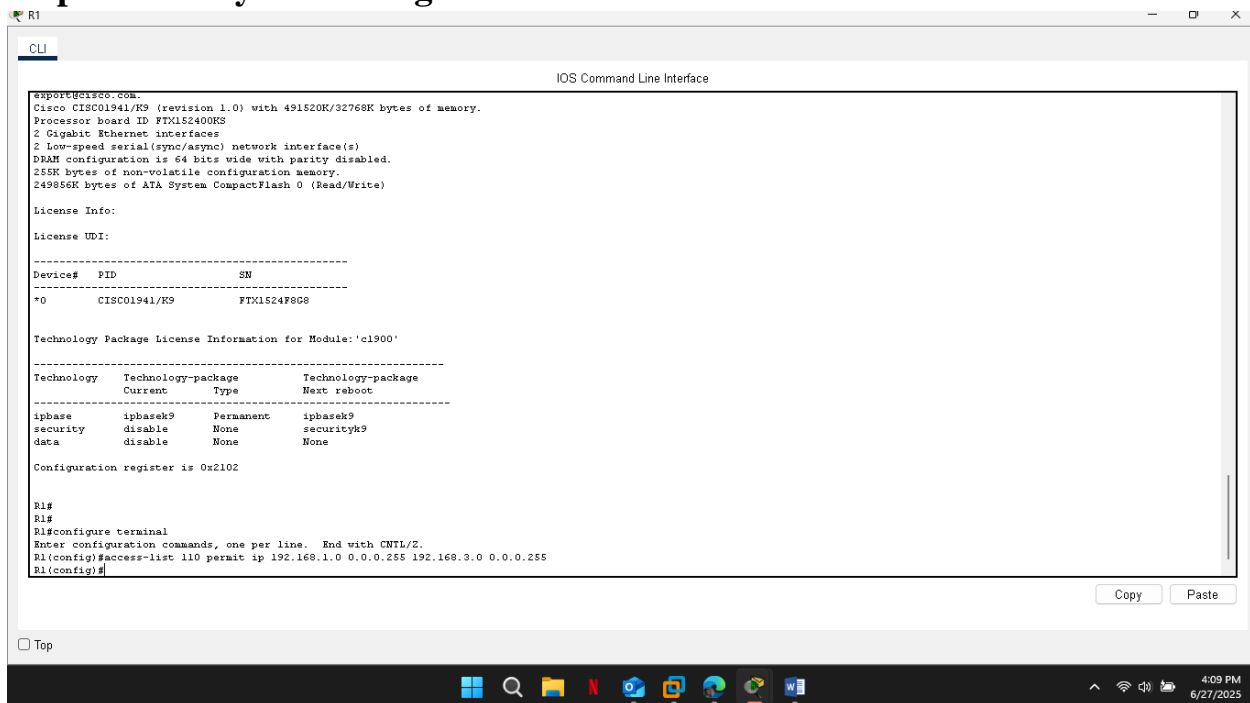


Accept the end-user license agreement.



Verified that the Security Technology package has been enabled by using the show version command

Step 3: Identify interesting traffic on R1.



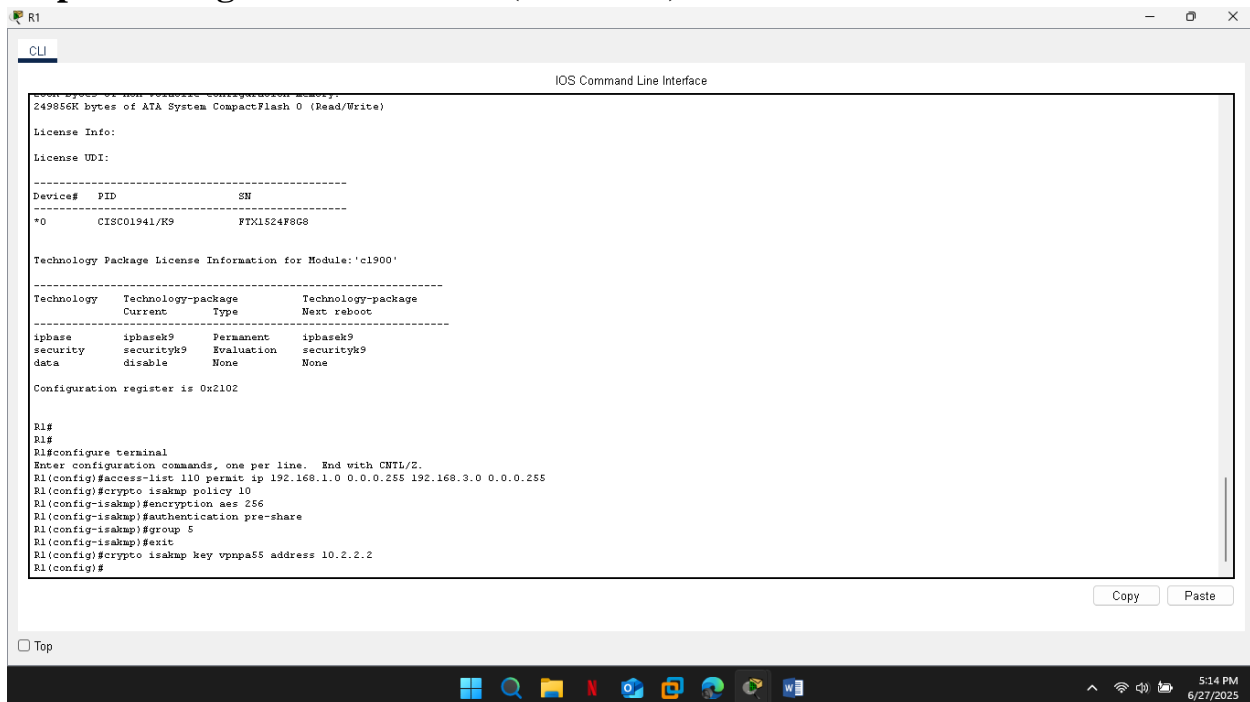
The screenshot shows the Cisco IOS Command Line Interface (CLI) for router R1. The output of the 'show version' command is displayed, providing details about the hardware, software, and license. The system is a Cisco CISC01941/K9 with 491520K/32768K bytes of memory. It features 2 Gigabit Ethernet interfaces and 2 Low-speed serial(sync/async) network interface(s). The RAM configuration is 64 bits wide with parity disabled. The configuration register is 0x2102. The license information is as follows:

```
License Info:
License UDI:
-----
Device#  PID          SN
-----
*0        CISC01941/K9        FTX1524F8G8

Technology Package License Information for Module:'c1900'
-----
Technology  Technology-package  Type  Technology-package
Current      Type               Next reboot
-----
ipbase      ipbasek9            Permanent  ipbasek9
security    disable             None       securityk9
data        disable             None
```

The configuration register is 0x2102. The prompt is R1#. The user has entered 'configure terminal' and is now in configuration mode. The prompt is R1(config)#. The user has entered 'access-list 110 permit ip 192.168.1.0 0.0.0.255 192.168.3.0 0.0.0.255' and the prompt is R1(config)#.

Step 4: Configure IKE Phase 1 (ISAKMP) on R1



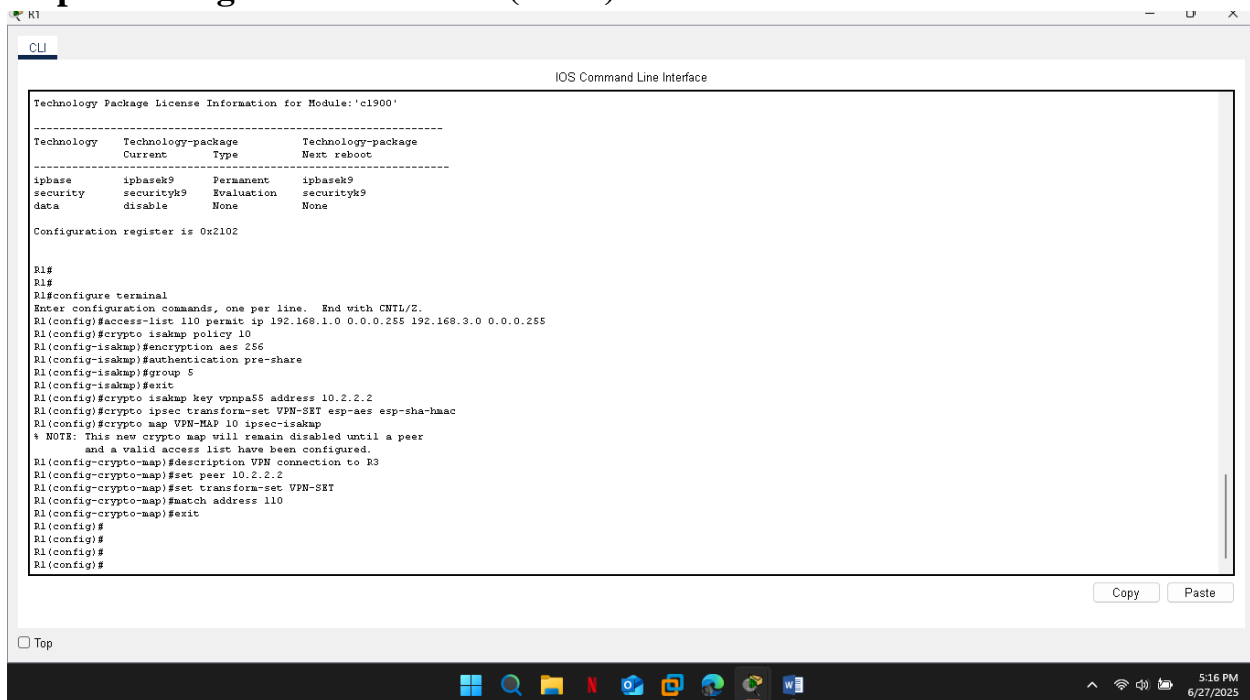
The screenshot shows the Cisco IOS Command Line Interface (CLI) for router R1. The output of the 'show version' command is displayed, providing details about the hardware, software, and license. The system is a Cisco CISC01941/K9 with 491520K/32768K bytes of memory. It features 2 Gigabit Ethernet interfaces and 2 Low-speed serial(sync/async) network interface(s). The RAM configuration is 64 bits wide with parity disabled. The configuration register is 0x2102. The license information is as follows:

```
License Info:
License UDI:
-----
Device#  PID          SN
-----
*0        CISC01941/K9        FTX1524F8G8

Technology Package License Information for Module:'c1900'
-----
Technology  Technology-package  Type  Technology-package
Current      Type               Next reboot
-----
ipbase      ipbasek9            Permanent  ipbasek9
security    securityk9          Evaluation  securityk9
data        disable             None
```

The configuration register is 0x2102. The prompt is R1#. The user has entered 'configure terminal' and is now in configuration mode. The prompt is R1(config)#. The user has entered 'access-list 110 permit ip 192.168.1.0 0.0.0.255 192.168.3.0 0.0.0.255' and the prompt is R1(config)#. The user has entered 'crypto isakmp policy 10' and the prompt is R1(config-isakmp)#. The user has entered 'encryption aes 256' and the prompt is R1(config-isakmp)#. The user has entered 'authentication pre-share' and the prompt is R1(config-isakmp)#. The user has entered 'group 5' and the prompt is R1(config-isakmp)#. The user has entered 'exit' and the prompt is R1(config)#. The user has entered 'crypto isakmp key vpnpa55 address 10.2.2.2' and the prompt is R1(config)#.

Step 5: Configure IKE Phase 2 (IPsec) on R1



The screenshot shows the R1 CLI interface with the following commands and output:

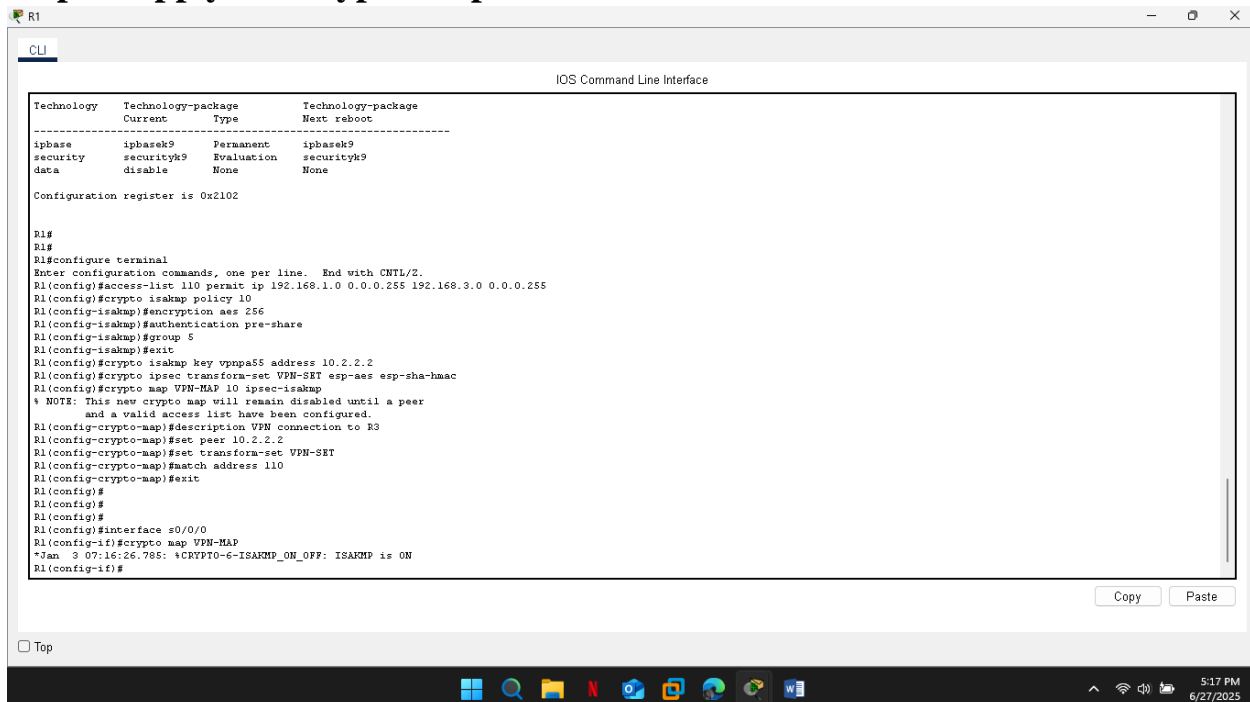
```
Technology Package License Information for Module:'c1900'
-----
Technology      Technology-package      Technology-package
Current         Type                   Next reboot
-----
ipbase          ipbasek9               Permanent          ipbasek9
security        securityk9              Evaluation         securityk9
data            disable                 None               None

Configuration register is 0x2102

R1#
R1#
R1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#access-list 110 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 vpnpsk5 address 10.2.2.2
R1(config)#crypto ipsec transform-set VPN-SET esp-aes esp-sha-hmac
R1(config)#crypto map VPN-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)#description VPN connection to R3
R1(config-crypto-map)#set peer 10.2.2.2
R1(config-crypto-map)#set transform-set VPN-SET
R1(config-crypto-map)#match address 110
R1(config-crypto-map)#exit
R1(config)#
R1(config)#
R1(config)#
R1(config)#
```

Buttons: Copy, Paste

Step 6: Apply the Crypto Map to the Interface



The screenshot shows the R1 CLI interface with the following commands and output:

```
Technology Package License Information for Module:'c1900'
-----
Technology      Technology-package      Technology-package
Current         Type                   Next reboot
-----
ipbase          ipbasek9               Permanent          ipbasek9
security        securityk9              Evaluation         securityk9
data            disable                 None               None

Configuration register is 0x2102

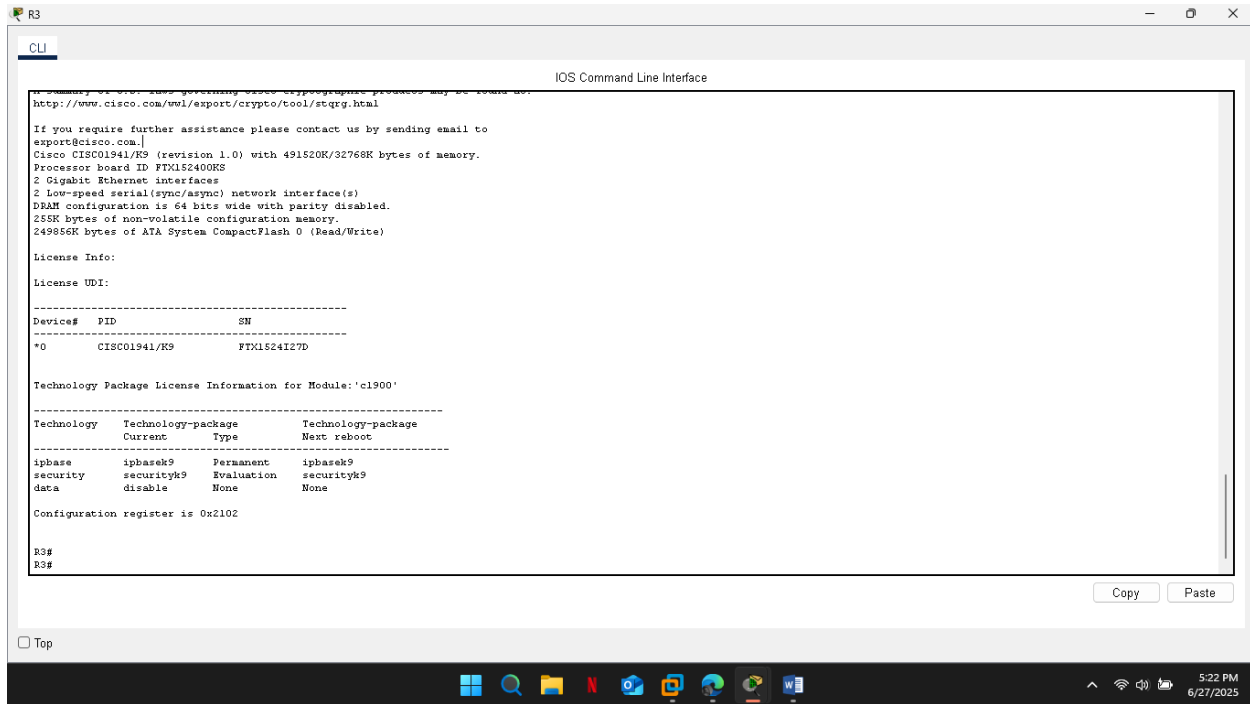
R1#
R1#
R1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#access-list 110 permit ip 192.168.1.0 0.0.0.255 192.168.3.0 0.0.0.255
R1(config)#crypto isakmp policy 10
R1(config-isakmp)#encryption aes 256
R1(config-isakmp)#authentication pre-share
R1(config-isakmp)#group 5
R1(config-isakmp)#exit
R1(config)#crypto isakmp key vpnpsk5 address 10.2.2.2
R1(config)#crypto ipsec transform-set VPN-SET esp-aes esp-sha-hmac
R1(config)#crypto map VPN-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)#description VPN connection to R3
R1(config-crypto-map)#set peer 10.2.2.2
R1(config-crypto-map)#set transform-set VPN-SET
R1(config-crypto-map)#match address 110
R1(config-crypto-map)#exit
R1(config)#
R1(config)#
R1(config)#
R1(config)#interface s0/0/0
R1(config-if)#crypto map VPN-MAP
*Jan  9 07:16:26.785: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
R1(config-if)#
```

Buttons: Copy, Paste

Part 2: Configure IPsec on R3

Step 1: Enable the Security Technology package.

it's enabled and fully operational for your site-to-site IPsec VPN



The screenshot shows the R3 CLI interface with the following output:

```
http://www.cisco.com/wol/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending email to
export@cisco.com.
Cisco CISC01941/R9 (revision 1.0) with 491520K/32768K bytes of memory.
Processor board ID FTX1S24I27D
2 Gigabit Ethernet interfaces
2 Low-speed serial(sync/async) network interface(s)
DRAM configuration is 64 bits wide with parity disabled.
255K bytes of non-volatile configuration memory.
249856K bytes of ATA System CompactFlash 0 (Read/Write)

License Info:
License UDI:
-----
Device# PID SN
-----
*0 CISC01941/R9 FTX1S24I27D

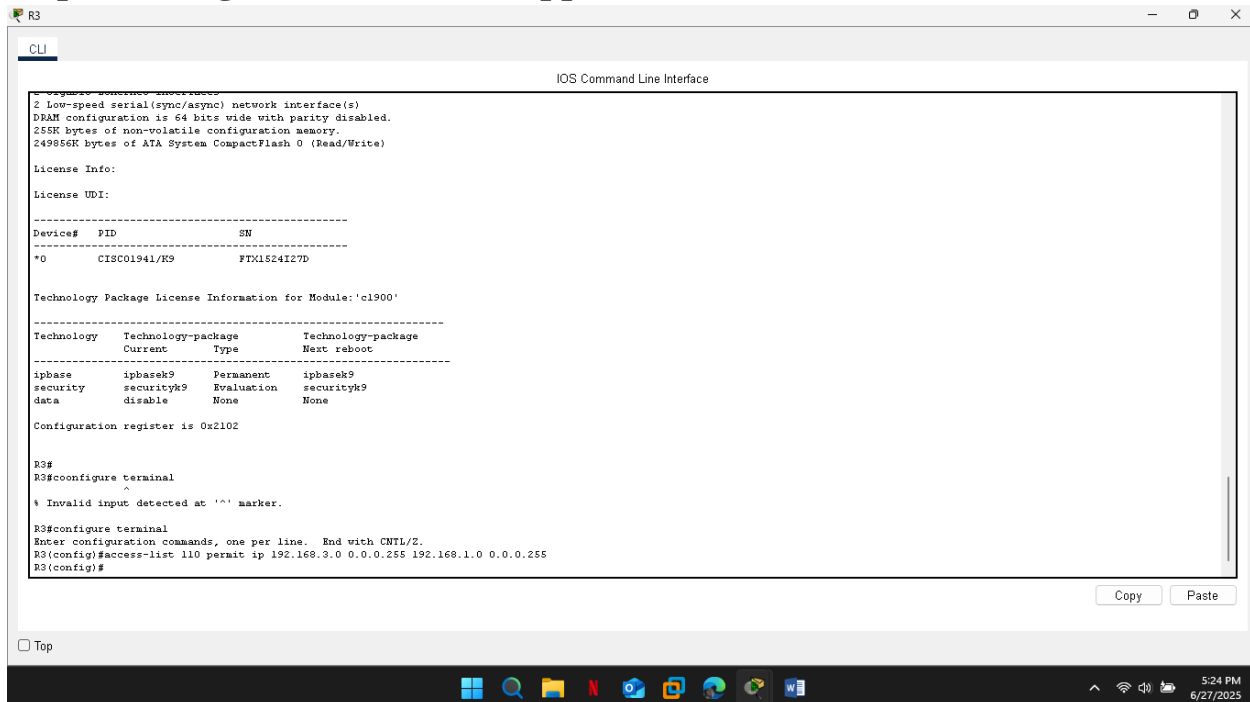
Technology Package License Information for Module:'c1900'
-----
Technology Technology-package Technology-package
Current Type Next reboot
-----
ipbase ipbasek9 Permanent ipbasek9
security securityk9 Evaluation securityk9
data disable None None

Configuration register is 0x2102

R3#
R3#
```

At the bottom of the CLI window, there are 'Copy' and 'Paste' buttons. Below the CLI window, there is a 'Top' button and a taskbar with various application icons and a system clock showing 5:22 PM on 6/27/2025.

Step 2: Configure router R3 to support a site-to-site VPN with R1.



The screenshot shows the R3 CLI interface with the following output:

```
2 Low-speed serial(sync/async) network interface(s)
DRAM configuration is 64 bits wide with parity disabled.
255K bytes of non-volatile configuration memory.
249856K bytes of ATA System CompactFlash 0 (Read/Write)

License Info:
License UDI:
-----
Device# PID SN
-----
*0 CISC01941/R9 FTX1S24I27D

Technology Package License Information for Module:'c1900'
-----
Technology Technology-package Technology-package
Current Type Next reboot
-----
ipbase ipbasek9 Permanent ipbasek9
security securityk9 Evaluation securityk9
data disable None None

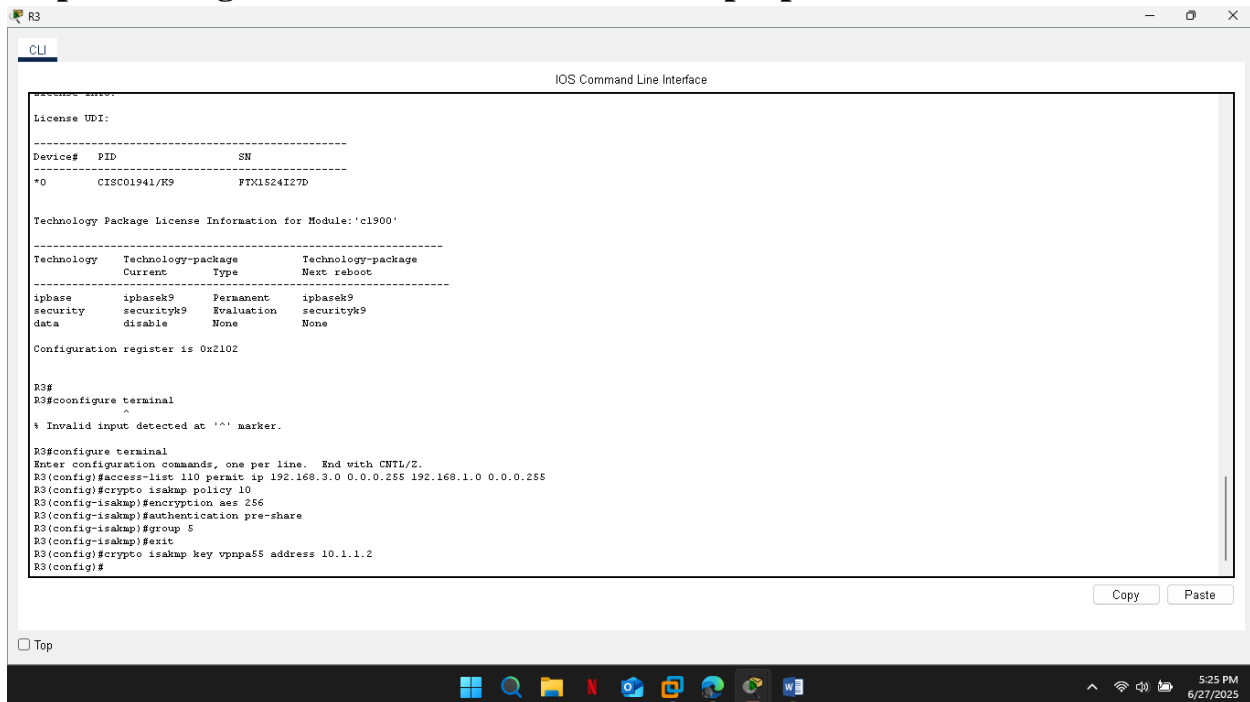
Configuration register is 0x2102

R3#
R3#configure terminal
R3(config)#
^
Invalid input detected at '^' marker.

R3#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#access-list 110 permit ip 192.168.3.0 0.0.0.255 192.168.1.0 0.0.0.255
R3(config)#
```

At the bottom of the CLI window, there are 'Copy' and 'Paste' buttons. Below the CLI window, there is a 'Top' button and a taskbar with various application icons and a system clock showing 5:24 PM on 6/27/2025.

Step 3: Configure the IKE Phase 1 ISAKMP properties on R3.



The screenshot shows the R3 CLI interface with the following commands and output:

```
R3#
R3#configure terminal
^
% Invalid input detected at '^' marker.
R3#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#access-list 110 permit ip 192.168.3.0 0.0.0.255 192.168.1.0 0.0.0.255
R3(config)#crypto isakmp policy 10
R3(config-isakmp)#encryption aes 256
R3(config-isakmp)#authentication pre-share
R3(config-isakmp)#group 5
R3(config-isakmp)#exit
R3(config)#crypto isakmp key vpnpa55 address 10.1.1.2
R3(config)#
```

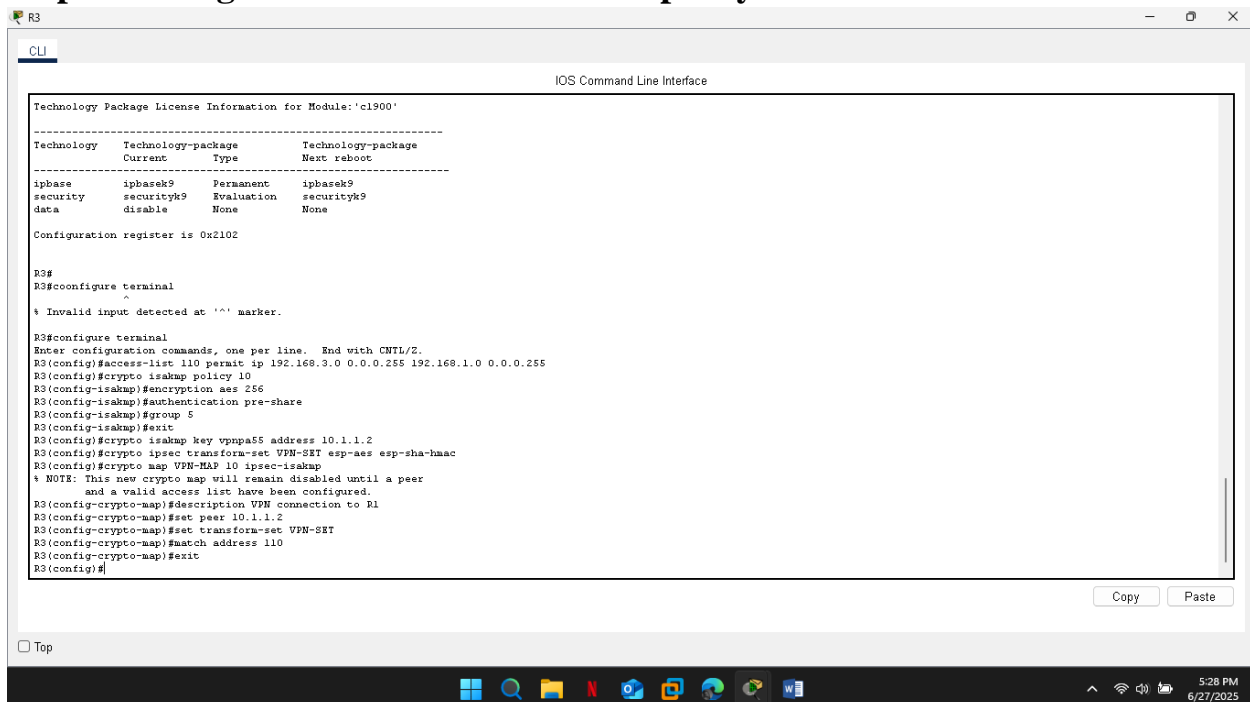
Technology Package License Information for Module: 'c1900'

| Technology | Technology-package | Technology-package | Technology-package |
|------------|--------------------|--------------------|--------------------|
| | Current | Type | Next reboot |
| ipbase | ipbasek9 | Permanent | ipbasek9 |
| security | securityk9 | Evaluation | securityk9 |
| data | disable | None | None |

Configuration register is 0x2102

Top

Step 4: Configure the IKE Phase 2 IPsec policy on R3.



The screenshot shows the R3 CLI interface with the following commands and output:

```
R3#
R3#configure terminal
^
% Invalid input detected at '^' marker.
R3#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#access-list 110 permit ip 192.168.3.0 0.0.0.255 192.168.1.0 0.0.0.255
R3(config)#crypto isakmp policy 10
R3(config-isakmp)#encryption aes 256
R3(config-isakmp)#authentication pre-share
R3(config-isakmp)#group 5
R3(config-isakmp)#exit
R3(config)#crypto isakmp key vpnpa55 address 10.1.1.2
R3(config)#crypto ipsec transform-set VPN-SET esp-aes esp-sha-hmac
R3(config)#crypto map VPN-MAP 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
and a valid access list have been configured.
R3(config-crypto-map)#description VPN connection to R1
R3(config-crypto-map)#set peer 10.1.1.2
R3(config-crypto-map)#set transform-set VPN-SET
R3(config-crypto-map)#match address 110
R3(config-crypto-map)#exit
R3(config)#
```

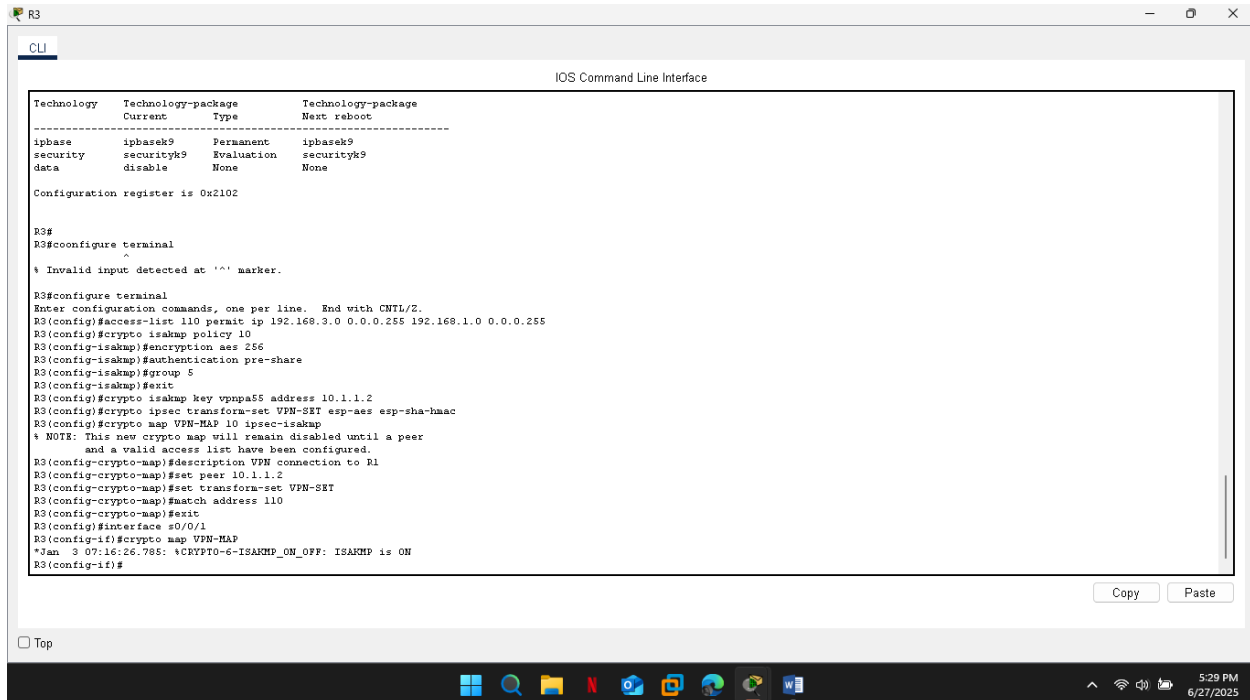
Technology Package License Information for Module: 'c1900'

| Technology | Technology-package | Technology-package | Technology-package |
|------------|--------------------|--------------------|--------------------|
| | Current | Type | Next reboot |
| ipbase | ipbasek9 | Permanent | ipbasek9 |
| security | securityk9 | Evaluation | securityk9 |
| data | disable | None | None |

Configuration register is 0x2102

Top

Step 5: Configure the crypto map on the outgoing interface.



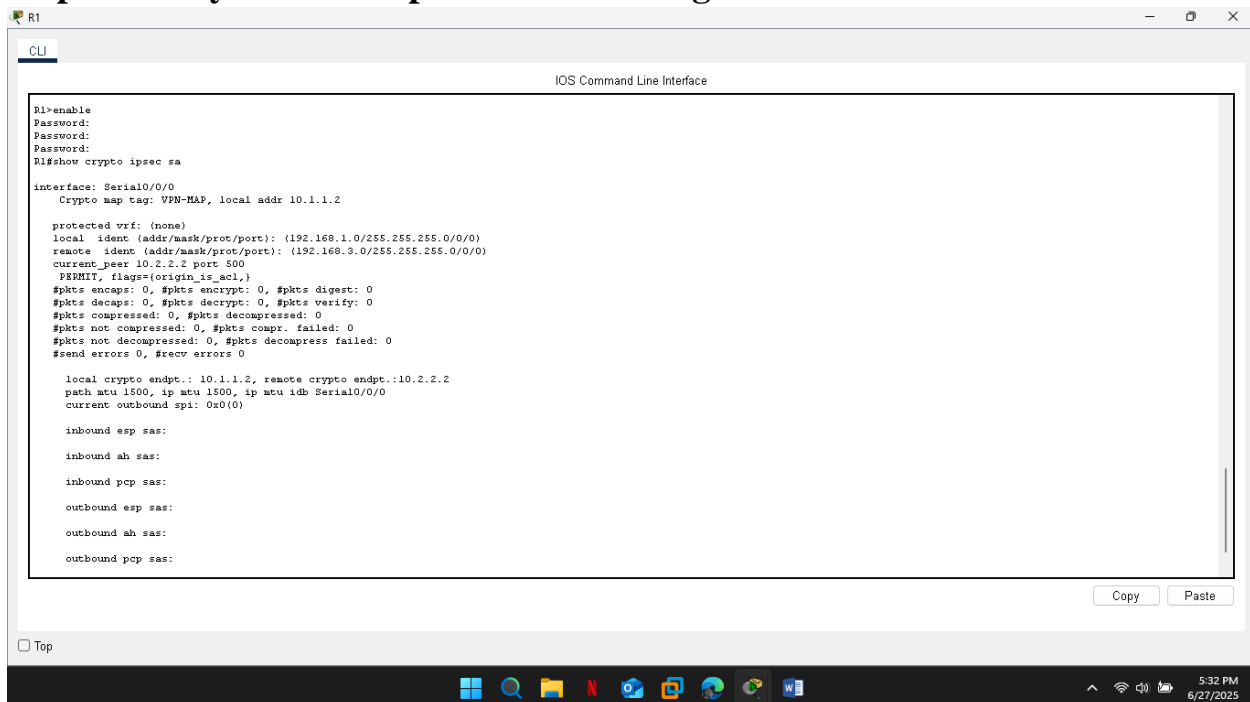
The screenshot shows the CLI of router R3. At the top, there is a table comparing current and next reboot technology packages. Below the table, the configuration register is set to 0x2102. The user enters 'configure terminal' and then 'access-list 110 permit ip 192.168.3.0 0.0.0.255 192.168.1.0 0.0.0.255'. Next, they configure an ISAKMP policy with encryption aes 256, authentication pre-share, and group 5. Then, they configure an IPsec transform set named 'VPN-SET' with esp-aes esp-sha-hmac and a crypto map named 'VPN-MAP' with transform set 'VPN-SET' and match address 110. Finally, they apply the crypto map to the Serial0/0/1 interface.

| Technology | Technology-package Current | Type | Technology-package Next reboot |
|------------|-------------------------------|------------|-----------------------------------|
| ipbase | ipbasek9 | Permanent | ipbasek9 |
| security | securityk9 | Evaluation | securityk9 |
| data | disable | None | None |

```
R3#
R3#configure terminal
R3(config)#access-list 110 permit ip 192.168.3.0 0.0.0.255 192.168.1.0 0.0.0.255
R3(config)#crypto isakmp policy 10
R3(config-isakmp)#encryption aes 256
R3(config-isakmp)#authentication pre-share
R3(config-isakmp)#group 5
R3(config-isakmp)#exit
R3(config)#crypto isakmp key vpnpa55 address 10.1.1.2
R3(config)#crypto ipsec transform-set VPN-SET esp-aes esp-sha-hmac
R3(config)#crypto map VPN-MAP 10 ipsec-isakmp
R3(config-crypto-map)#set transform-set VPN-SET
R3(config-crypto-map)#match address 110
R3(config-crypto-map)#exit
R3(config)#interface s0/0/1
R3(config-if)#crypto map VPN-MAP
*Jan  3 07:16:26.785: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
R3(config-if)#
```

Part 3: Verify the IPsec VPN

Step 1: Verify the tunnel prior to interesting traffic.



The screenshot shows the CLI of router R1. The user enters 'enable' and then 'show crypto ipsec sa'. The output displays the status of the IPsec security association (SA) for the VPN-MAP. It shows the local and remote identities, the current peer, the protected vrf, the path mtu, and the inbound and outbound sas.

```
R1>enable
R1#show crypto ipsec sa

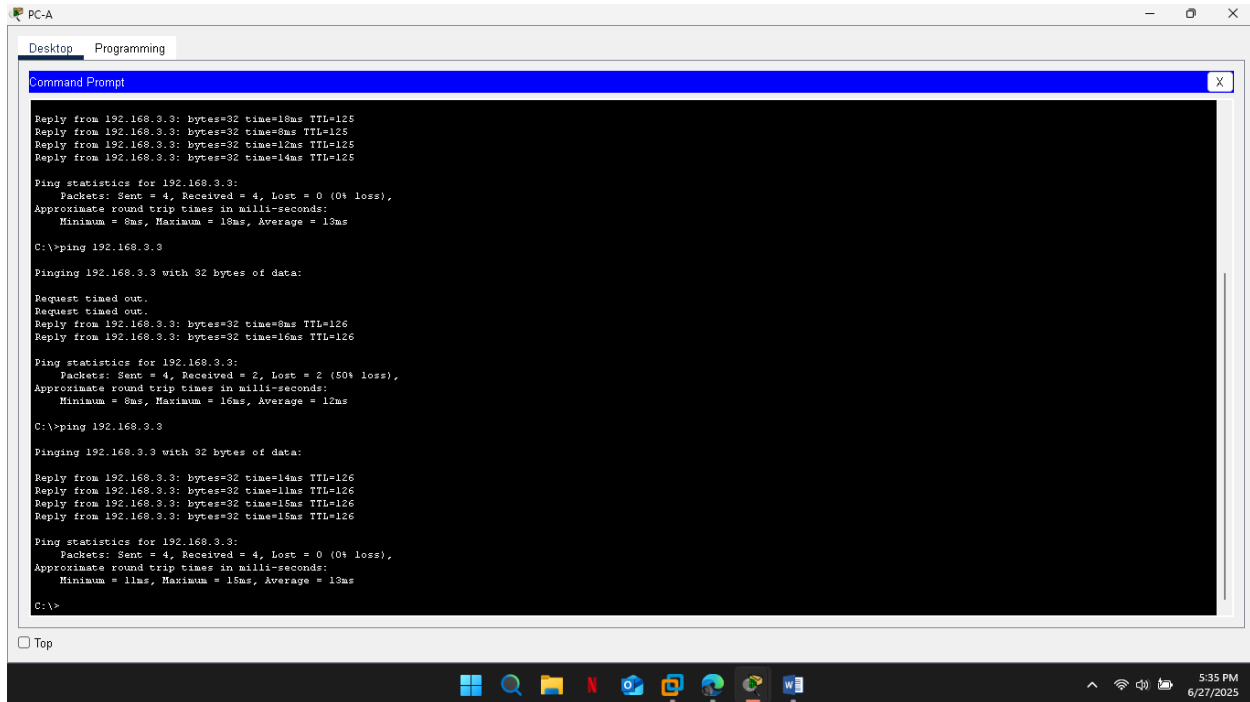
interface: Serial0/0/0
  Crypto map tag: VPN-MAP, local addr 10.1.1.2

  protected vrf: (none)
  local ident (addr/mask/prot/port): (192.168.1.0/255.255.255.0/0/0)
  remote ident (addr/mask/prot/port): (192.168.3.0/255.255.255.0/0/0)
  current_peer 10.2.2.2 port 800
    PERMIT, flags={origin_is_acl,}
    #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
    #pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0

  local crypto endpt.: 10.1.1.2, remote crypto endpt.: 10.2.2.2
  path mtu 1500, ip mtu 1500, ip mtu idb Serial0/0/0
  current outbound spi: 0x0(0)

  inbound esp sas:
  inbound ah sas:
  inbound pcp sas:
  outbound esp sas:
  outbound ah sas:
  outbound pcp sas:
```

Step 2: Create interesting traffic.



The screenshot shows a Windows desktop environment. A Command Prompt window is open, displaying the results of several ping and pathping commands. The first set of pings to 192.168.3.3 shows successful results with 0% loss. The second set shows a 50% loss. The third set shows successful results again. The pathping command shows a path of 1500 hops.

```
Reply from 192.168.3.3: bytes=32 time=10ms TTL=125
Reply from 192.168.3.3: bytes=32 time=8ms TTL=125
Reply from 192.168.3.3: bytes=32 time=12ms TTL=125
Reply from 192.168.3.3: bytes=32 time=14ms TTL=125

Ping statistics for 192.168.3.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 8ms, Maximum = 14ms, Average = 13ms

C:\>ping 192.168.3.3

Pinging 192.168.3.3 with 32 bytes of data:

Request timed out.
Request timed out.
Reply from 192.168.3.3: bytes=32 time=8ms TTL=126
Reply from 192.168.3.3: bytes=32 time=16ms TTL=126

Ping statistics for 192.168.3.3:
    Packets: Sent = 4, Received = 2, Lost = 2 (50% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 8ms, Maximum = 16ms, Average = 12ms

C:\>ping 192.168.3.3

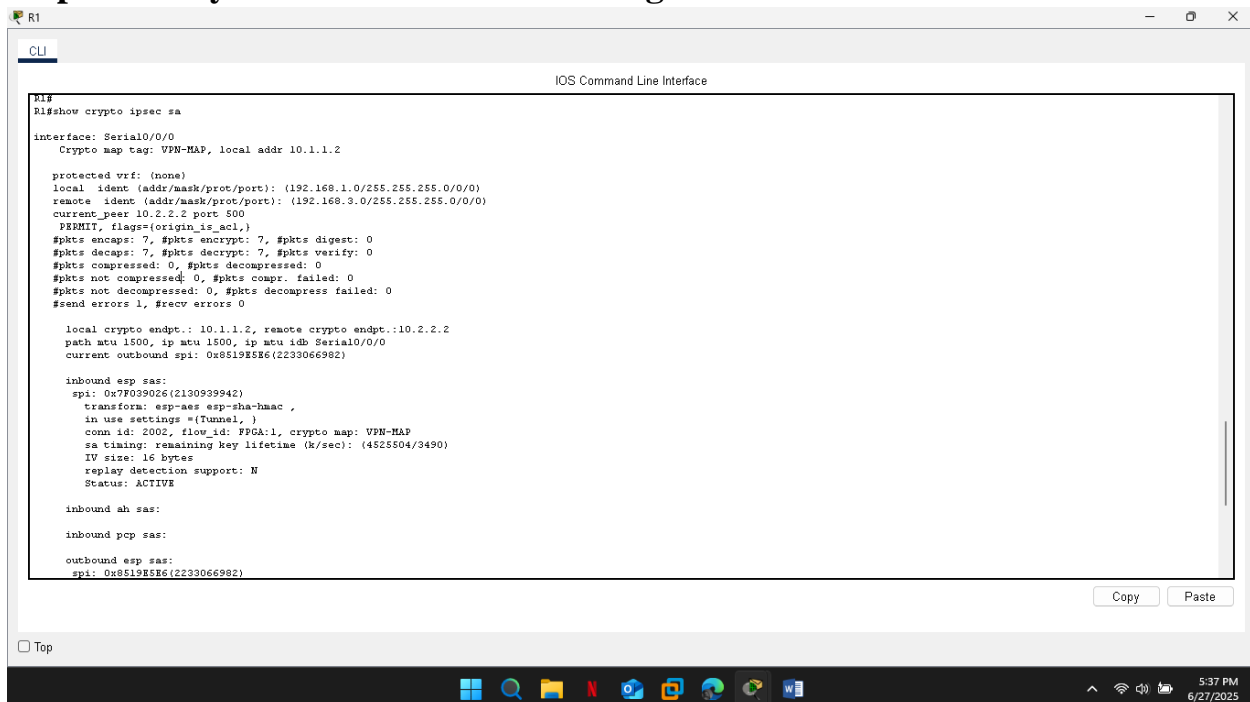
Pinging 192.168.3.3 with 32 bytes of data:

Reply from 192.168.3.3: bytes=32 time=14ms TTL=126
Reply from 192.168.3.3: bytes=32 time=11ms TTL=126
Reply from 192.168.3.3: bytes=32 time=13ms TTL=126
Reply from 192.168.3.3: bytes=32 time=15ms TTL=126

Ping statistics for 192.168.3.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 11ms, Maximum = 15ms, Average = 13ms

C:\>
```

Step 3: Verify the tunnel after interesting traffic.



The screenshot shows a Windows desktop environment. A CLI window is open, displaying the output of the 'show crypto ipsec sa' command. The output shows the configuration and status of the IPsec tunnel, including the local and remote endpoints, the crypto map, the protected vrf, the local and remote identities, the current peer, the PERMIT flags, the number of packets sent and received, the local and remote crypto endpoints, the path, the inbound and outbound ESP and AH SAs, and the status of the tunnel.

```
CLI
IOS Command Line Interface

R1#
R1#show crypto ipsec sa

interface: Serial0/0/0
Crypto map tag: VPN-MAP, local addr 10.1.1.2

protected vrf: (none)
local ident (addr/mask/prot/port): (192.168.1.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port): (192.168.3.0/255.255.255.0/0/0)
current_peer 10.2.2.2 port 500
PERMIT, flags={origin_is_acl,}
#pkts encaps: 7, #pkts encrypt: 7, #pkts digest: 0
#pkts decaps: 7, #pkts decrypt: 7, #pkts verify: 0
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 1, #recv errors 0

local crypto endpt.: 10.1.1.2, remote crypto endpt.: 10.2.2.2
path mtu 1500, ip mtu 1500, ip mtu idb Serial0/0/0
current outbound spi: 0x8519E5E6(2233066982)

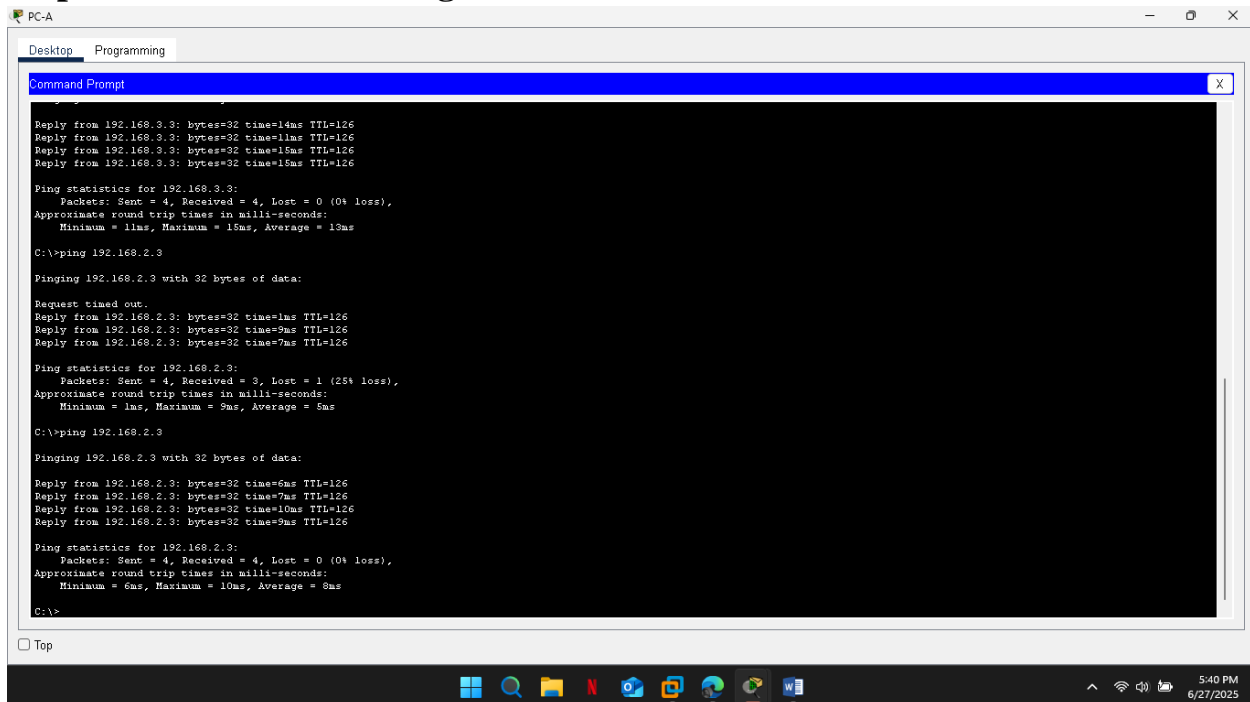
inbound esp sas:
spi: 0x7F039026(2130939942)
transform: esp-aes esp-sha-hmac ,
in use settings ={Tunnel,}
conn id: 2002, flow_id: FPGA:1, crypto map: VPN-MAP
sa timing: remaining key lifetime (k/sec): (4525504/3490)
IV size: 16 bytes
replay detection support: N
Status: ACTIVE

inbound ah sas:

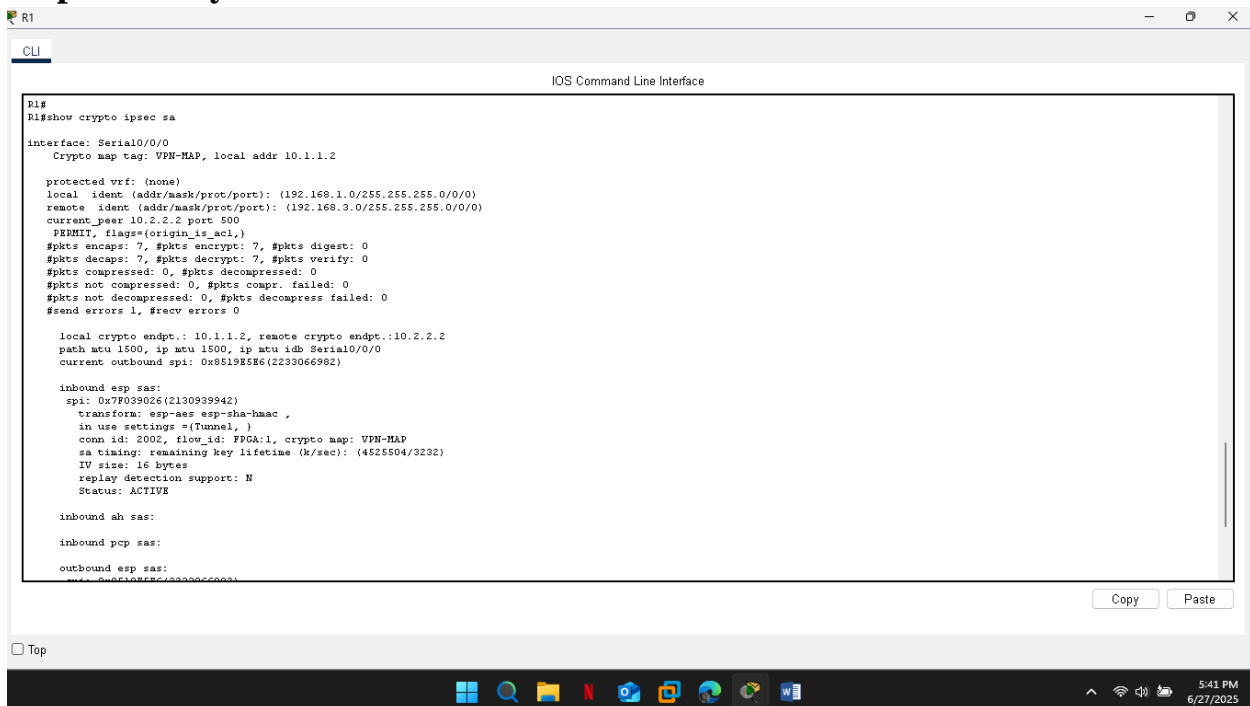
inbound pcp sas:

outbound esp sas:
spi: 0x8519E5E6(2233066982)
```

Step 4: Create uninteresting traffic.



Step 5: Verify the tunnel.



Step 6: Check results.

Cisco Packet Tracer - C:\Users\user\Downloads\Configuring Site-to-Site VPNs (Optional).pkt - Guest - 2025-06-27 15:44:56

File Edit Options View Tools Extensions Window Help

Activity Results Time Elapsed: 01:57:10

Congratulations Guest! You completed the activity.

Overall Feedback Assessment Items Connectivity Tests

Congratulations on completing this activity!

Close

5:42 PM
6/27/2025

CONCLUSION

Upon completion of this activity, the IPsec VPN tunnel between R1 and R3 was successfully established and verified. Encrypted communication was confirmed by observing increased encapsulation and encryption counters following a successful ping from PC-A (192.168.1.3) to PC-C (192.168.3.3), which matched the defined interesting traffic. Uninteresting traffic, such as pings to PC-B, bypassed the VPN as expected.

This activity reinforced the foundational steps of creating a secure site-to-site VPN using Cisco IOS CLI, including license activation, access-list definition, ISAKMP and IPsec configuration, and crypto map application. By simulating a secure inter-branch communication scenario, it highlighted the importance of IPsec in protecting sensitive data over insecure networks and deepened understanding of VPN tunnel negotiation and maintenance in a routed network environment.