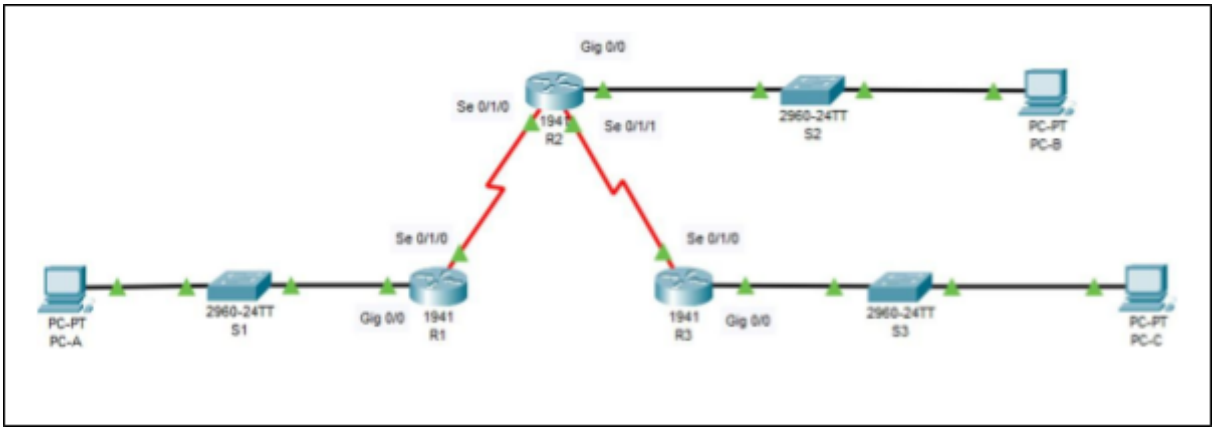
Name :Harsh Kadu Roll No : 33

Practical 9

Configure and Verify a Site-to-Site IPsec VPN using CLI

Topology:



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
Router1 (R1)	GigabitEthernet0/0	192.168.1.1	255.255.255.0	
	Serial 0/1/0	10.1.1.2	255.255.255.252	
Router2 (R2)	GigabitEthernet0/0	192.168.2.1	255.255.255.0	
	Serial 0/1/0	10.1.1.1	255.255.255.252	
	Serial 0/1/1	10.2.2.1	255.255.255.252	
Router3 (R3)	GigabitEthernet0/0	192.168.3.1	255.255.255.0	
	Serial 0/1/0	10.2.2.2	255.255.255.252	
PC-A	FastEthernet0	192.168.1.3	255.255.255.0	192.168.1.1
PC-B	FastEthernet0	192.168.2.3	255.255.255.0	192.168.2.1
PC-C	FastEthernet0	192.168.3.3	255.255.255.0	192.168.3.1

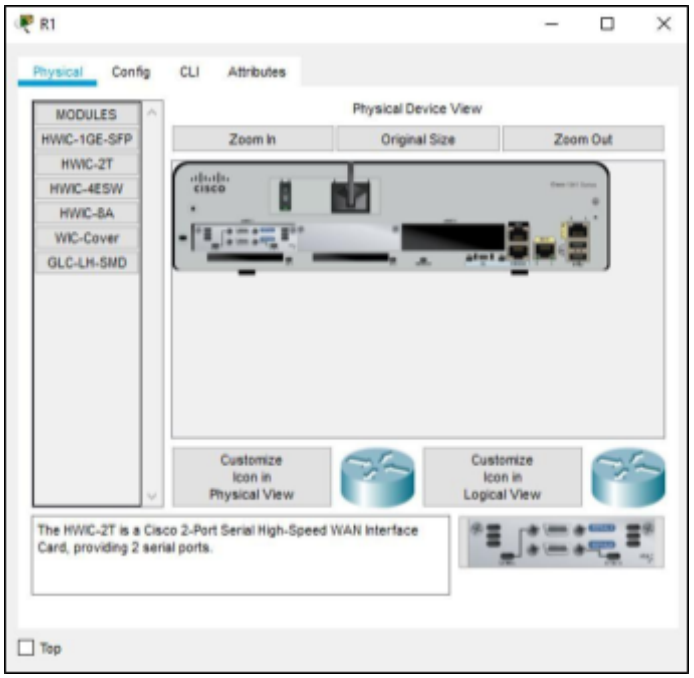
Name :Harsh Kadu Roll No : 33

Procedure:

Step 1: Add Serial Interface to each Router before connecting component:

i) Click on Router1 (R1) ➜ Physical Tab ➜ Switch off the switch first ➜ Select H2WIC-2T ➜ Drag it and place it on Interface ➜ Make Switch On.

Repeat the same procedure on Router2 (R2) and Router3



(R3).

Step 2: Configuration Commands on all 3 Routers:

i) Click on Router1 (R1) ➜ CLI Tab ➜ Type the following Commands:

```
R1>enable
R1#config t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#enable secret enpa55
R1(config)#line console 0
R1(config-line)#password conpa55
R1(config-line)#login
R1(config-line)#exit
R1(config)#
R1(config)#ip domain-name ccnasecurity.com
R1(config)#username admin secret adminpa55
R1(config)#line vty 0 4
R1(config-line)#login local
R1(config-line)#exit
R1(config)#crypto key generate rsa
The name for the keys will be: R1.ccnasecurity.com
Choose the size of the key modulus in the range of 360 to 2048 for
your
  General Purpose Keys. Choosing a key modulus greater than 512 may
take
  a few minutes.

How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
```

ii) Click on Router2 (R2) ➜ CLI Tab ➜ Type the following Commands:

```
R2>enable
R2#config t
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#enable secret enpa55
R2(config)#line console 0
R2(config-line)#password conpa55
R2(config-line)#login
R2(config-line)#exit
R2(config)#
R2(config)#ip domain-name ccnasecurity.com
R2(config)#username admin secret adminpa55
R2(config)#line vty 0 4
R2(config-line)#login local
R2(config-line)#exit
R2(config)#crypto key generate rsa
The name for the keys will be: R2.ccnasecurity.com
Choose the size of the key modulus in the range of 360 to 2048 for
your
  General Purpose Keys. Choosing a key modulus greater than 512 may
take
  a few minutes.

How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
```

iii) Click on Router3 (R3) ➜ CLI Tab ➜ Type the following Commands:

```
R3>enable
R3#config t
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)#enable secret enpa55
R3(config)#line console 0
R3(config-line)#password conpa55
R3(config-line)#login
R3(config-line)#exit
R3(config)#
R3(config)#ip domain-name ccnasecurity.com
R3(config)#username admin secret adminpa55
R3(config)#line vty 0 4
R3(config-line)#login local
R3(config-line)#exit
R3(config)#crypto key generate rsa
The name for the keys will be: R3.ccnasecurity.com
Choose the size of the key modulus in the range of 360 to 2048 for
your
  General Purpose Keys. Choosing a key modulus greater than 512 may
take
  a few minutes.

How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
```

Step 3: Assign OSPF and Network to all Routers:

i) Click on Router1 (R1) ➜ CLI Tab ➜ Type the following Commands:

```
User Access Verification

Password:

R1>enable
Password:
R1#config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#router ospf 1
R1(config-router)#network 192.168.1.0 0.0.0.255 area 0
R1(config-router)#network 10.1.1.0 0.0.0.3 area 0
R1(config-router)#exit
R1(config)#exit
R1#
%SYS-5-CONFIG_I: Configured from console by console
```

ii) Click on Router2 (R2) ➜ CLI Tab ➜ Type the following Commands:

```
R2>enable
Password:
R2#config t
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#router ospf 1
R2(config-router)#network 192.168.2.0 0.0.0.255 area 0
R2(config-router)#network 10.1.1.0 0.0.0.3 area 0
R2(config-router)#network 10.1.1.0 0.0.0.3 area 0
00:40:58: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.1.1 on Serial0/1/0
from
R2(config-router)#network 10.2.2.0 0.0.0.3 area 0
R2(config-router)#exit
R2(config)#
```

iii) Click on Router3 (R3) ➜ CLI Tab ➜ Type the following Commands:

```
User Access Verification

Password:
R3>enable
Password:
Password:
R3#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)#interface GigabitEthernet0/0
R3(config-if)#exit
R3(config)#router ospf 1
R3(config-router)#network 192.168.3.0 0.0.0.255 area 0
R3(config-router)#network 10.2.2.0 0.0.0.3 area 0
R3(config-router)#exit
R3(config)#
00:43:56: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.2.1 on Serial0/1/0
from LOADING to FULL, Loading Done
```

Step 4: Verify Connectivity from PC-A to PC-B & PC-C:

i) Click on PC-A ➜ Desktop ➜ Command Prompt ➜ Type the following Command:

```
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=2ms TTL=125
Reply from 192.168.3.3: bytes=32 time=2ms TTL=125
Reply from 192.168.3.3: bytes=32 time=3ms 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 = 2ms, Maximum = 3ms, Average = 2ms
```

```
C:\>ping 192.168.2.3

Pinging 192.168.2.3 with 32 bytes of data:

Request timed out.
Reply from 192.168.2.3: bytes=32 time=1ms TTL=126
Reply from 192.168.2.3: bytes=32 time=1ms TTL=126
Reply from 192.168.2.3: bytes=32 time=10ms TTL=126

Ping statistics for 192.168.2.3:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 10ms, Average = 4ms
```

Step 5: Configure IPsec Parameters on R1:

i) Click on Router1 (R1) ➜ CLI Tab ➜ Type the following Commands:

```
R1>enable
Password:
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 54 seconds
```

```
License Info:

License UDI:

-------------------------------------------------
Device#    PID                 SN
-------------------------------------------------
*0         CISCO1941/K9        FTX1524F90S-


Technology Package License Information for Module:'c1900'

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

Configuration register is 0x2102
```

Name :Harsh Kadu Roll No : 33

```
R1#config 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.
```

```
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]: yes
% 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#copy run start
Destination filename [startup-config]?
Building configuration...
[OK]
R1#reload
Proceed with reload? [confirm]
System Bootstrap, Version 15.1(4)M4, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 2010 by cisco Systems, Inc.
Total memory size = 512 MB - On-board = 512 MB, DIMM0 = 0 MB
CISCO1941/K9 platform with 524288 Kbytes of main memory
Main memory is configured to 64/-1(On-board/DIMM0) bit mode with ECC
disabled

Readonly ROMMON initialized

program load complete, entry point: 0x80803000, size: 0x1b340
program load complete, entry point: 0x80803000, size: 0x1b340

IOS Image Load Test
___________________
Digitally Signed Release Software
program load complete, entry point: 0x81000000, size: 0x2bb1c58
Self decompressing the image :
########################
```

```
R1>enable
Password:
R1#config t
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 vpnpa address 10.2.2.2
R1(config)#crypto ipsec transform-set VPN-SET
% Incomplete command.
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)#int se 0/1/0
R1(config-if)#crypto map VPN-MAP
*Jan  3 07:16:26.785: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
R1(config-if)#exit
R1(config)#
```

ii) Click on Router3 (R3) ➜ CLI Tab ➜ Type the following Commands:

```
R3>enable
Password:
R3#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
```

```
License Info:

License UDI:

-------------------------------------------------
Device#   PID                   SN
-------------------------------------------------
*0        CISCO1941/K9          FTX15244BPI-


Technology Package License Information for Module:'c1900'

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

Configuration register is 0x2102
```

Name :Harsh Kadu Roll No : 33

```
R3#config t
Enter configuration commands, one per line.  End with CNTL/Z.
R3(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.
```

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


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

R3(config)#: %IOS_LICENSE_IMAGE_APPLICATION-6-LICENSE_LEVEL: Module name = C1900
Next reboot level = securityk9 and License = securityk9

R3(config)#exit
R3#
%SYS-5-CONFIG_I: Configured from console by console
```

```
R3#copy run start
Destination filename [startup-config]?
Building configuration...
[OK]
R3#reload
Proceed with reload? [confirm]
System Bootstrap, Version 15.1(4)M4, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 2010 by cisco Systems, Inc.
Total memory size = 512 MB - On-board = 512 MB, DIMM0 = 0 MB
CISCO1941/K9 platform with 524288 Kbytes of main memory
Main memory is configured to 64/-1(On-board/DIMM0) bit mode with ECC disabled

Readonly ROMMON initialized

program load complete, entry point: 0x80803000, size: 0x1b340
program load complete, entry point: 0x80803000, size: 0x1b340

IOS Image Load Test
___________________
Digitally Signed Release Software
program load complete, entry point: 0x81000000, size: 0x2bb1c50
Self decompressing the image :
##########################
```

```
R3#config t
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)#access-list 110 permit ip 192.168.1.0 0.0.0.255 192.168.3.0 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 vpnpa address 10.1.1.2
R3(config)#crypto ipsec transform-set VPN-SET
% Incomplete command.
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)#int se 0/1/0
R3(config-if)#crypto map VPN-MAP
*Jan  3 07:16:26.785: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
R3(config-if)#exit
R3(config)#
```

Name :Harsh Kadu Roll No : 33

Step 6: Verify the IPsec VPN:

i) Click on Router1 (R1) ➜ CLI Tab ➜ Type the following Commands:

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

interface: Serial0/1/0
    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: 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 Serial0/1/0
     current outbound spi: 0x0(0)

     inbound esp sas:

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:
```

ii) Click on PC-C ➜ Desktop ➜ Command Prompt ➜ Type the following Command:

```
Packet Tracer PC Command Line 1.0
C:\>ping 192.168.1.3

Pinging 192.168.1.3 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.1.3:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

iii) Click on Router1 (R1) ➜ CLI Tab ➜ Type the following Commands:

```
R1#show crypto ipsec sa

interface: Serial0/1/0
    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: 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 Serial0/1/0
     current outbound spi: 0x0(0)

     inbound esp sas:

     inbound ah sas:

     inbound pcp sas:
```

iv) Click on PC-B ➜ Desktop ➜ Command Prompt ➜ Type the following Command:

```
Packet Tracer PC Command Line 1.0
C:\>ping 192.168.1.3

Pinging 192.168.1.3 with 32 bytes of data:

Request timed out.
Reply from 192.168.1.3: bytes=32 time=10ms TTL=126
Reply from 192.168.1.3: bytes=32 time=12ms TTL=126
Reply from 192.168.1.3: bytes=32 time=11ms TTL=126

Ping statistics for 192.168.1.3:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 10ms, Maximum = 12ms, Average = 11ms
```

v) Click on Router1 (R1) ➜ CLI Tab ➜ Type the following Command:

```
R1#
R1#ping 192.168.3.3

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.3.3, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 2/6/20 ms
```

vi) Click on Router3 (R3) ➜ CLI Tab ➜ Type the following Command:

```
R3#ping 192.168.1.3

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.3, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/9/20 ms
```