# Module 8 – IPSec VPN Configuration Lab

**Objective: All the routers are pre-configured with basic interface, OSPF and BGP configuration according to the following topology diagram. Create IPSec VPN tunnel between CPE routers. After finishing the configuration please ensure that you can ping, telnet to your tunnel end point routers specifying loopback0 or fa0/0 as source and your packets are encrypted (Both IPv4 and IPv6). Your packets will be captured and analysed by a protocol analyser to verify the outcome.**

**Prerequisites: Knowledge of Cisco router CLI, Cryptography, IPSec, IPv6 etc.**

The following will be the common topology and IP address plan used for the labs.

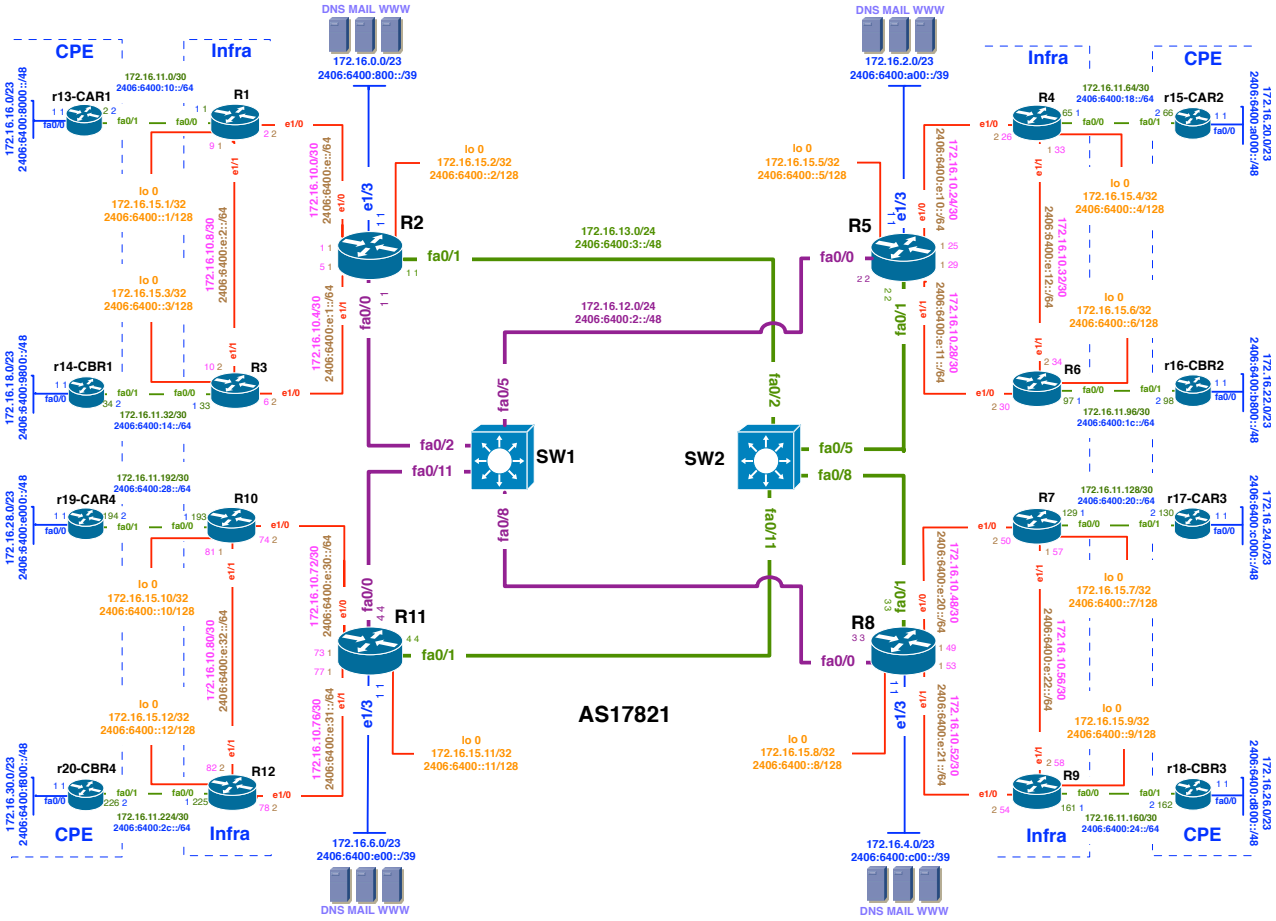


**Figure 1 – ISP Lab Basic Configuration**

## *Lab Notes*

IPSec point to point VPN tunnel will be created between CPE routers:

1. r13-CAR1 ⇔ r15-CAR2 [Interesting traffic R13 fa0/0 & R15 fa0/0, Tunnel end point R13 fa0/1 & R15 fa0/1, Capture R1 fa0/0 & R4 fa0/0]
2. r14-CBR1 ⇔ r16-CBR2 [Interesting traffic R14 fa0/0 & R16 fa0/0, Tunnel end point R14 fa0/1 & R16 fa0/1, Capture R3 fa0/0 & R6 fa0/0]
3. r19-CAR4 ⇔ r17-CAR3 [Interesting traffic R19 fa0/0 & R17 fa0/0, Tunnel end point R19 fa0/1 & R17 fa0/1, Capture R10 fa0/0 & R7 fa0/0]
4. r20-CBR4 ⇔ r18-CBR3 [Interesting traffic R20 fa0/0 & R18 fa0/0, Tunnel end point R20 fa0/1 & R18 fa0/1, Capture R12 fa0/0 & R9 fa0/0]

Please spend some time to be familiar with the network topology and addressing plan

## *Lab Exercise*

1. **Configure access-list:** To match the interesting traffic to encrypt first step is to define the access-list specifying the source and destination from both side on the tunnel.

   Here is an example access-list for CPE router R13 (Need for both IPv6 and IPv4):

   ```
   config t
   ipv6 access-list MATCH-IPV6
   permit 2406:6400:8000::/48 2406:6400:A000::/48
   exit
   ```

2. **Create ISAKMP Policy:** Second step to setup an IPSec tunnel is to configuration ISAKMP policy parameters. There are five policy parameters need to be defined to each policy entry. Here are those parameters and their default values:

   a. **IKE policy encryption:** Data Encryption Standard (DES) as the default,
   b. **IKE policy hash:** Secure Hash Standard-1 (SHA-1) as the default,
   c. **IKE key exchange:** Diffie-Hellman Group 1 (768-Bit) as the default,
   d. **IKE lifetime:** One-day (86,400 seconds) lifetime as the default,
   e. **IKE authentication:** RSA public key as the default.

   Example ISAKMP policy configuration for one of the CPE router:

   ```
   config t
   crypto isakmp policy 1
   encryption aes
   hash sha
   group 5
   authentication pre-share
   exit
   ```

3. **Create Pre Shared Key:** There are three methods can be used for peer authentication in IPSec VPN. I.e.:

   a. **Pre-shared keys:** A secret key configured into each peer manually by the administrator
   b. **RSA signature:** Digital certificate exchanged among the per to authenticate.
   c. **RSA encrypted nonces:** An encrypted random number generated by each IPSec peer then exchanged to authenticate. Two nonces are use during the authentication process.

   We will be using a symmetric key, which is pre-shared and need to be shared between IPSec peers out of band. Please note the key command below and address is your tunnel destination which is the WAN address of your peer (Between CPE router R13 and R15). You need to replace the address with your peer WAN address. Look at the diagram (Figure1) to find your peer WAN address.

   Example pre-shared key configuration on R13 (Need for both IPv6 and IPv4):

   ```
   config t
   crypto isakmp key Tr@ining123 address ipv6 2406:6400:18::2/128
   exit
   ```

4. **Configure IPSec transform set:** IPSec transform sets are exchange between peers during quick mode in phase 2. A transform set is a combination of algorithms and protocol that endorse a security policy for traffic.

   Example transform set configuration for one of the CPE router:

```
config t
crypto ipsec transform-set ESP-AES-SHA esp-aes esp-sha-hmac
exit
```

5. **Creating the crypto map:** Now need to create a crypto map to glue all those policy together. Please note the peer address which will be your IPSec tunnel destination. Normally WAN address of remote peer.

   Example crypto map configuration for one of the CPE router [R13] (Need for both IPv6 and IPv4):

```
config t
crypto map ipv6 IPV6-LAB-VPN 10 ipsec-isakmp
match address MATCH-IPV6
set transform-set ESP-AES-SHA
set peer 2406:6400:18::2
exit
```

6. **Apply crypto map to an interface:** Final step is to apply the crypto map to an outgoing interface.

   Example crypto map configuration for one of the CPE router [R13] (Need for both IPv6 and IPv4):

```
config t
int fa 0/1
ipv6 crypto map IPV6-LAB-VPN
exit
exit
wr
```

7. **Verify your IPSec configuration:**

   Command to show ISAKMP security associations (SAs) built between peers:

```
show crypto isakmp sa
```

   Command to shows IPsec SAs built between peers:

```
sh crypto ipsec sa
```

   Command to verify ISAKMP peer:

```
sh crypto isakmp peers
```

## 8. Generate interesting traffic and analyse IPSec tunnel between peers:

a. Lab instructor will start packet capture on R1 fa0/0, R3 fa0/0, R4 fa0/0, R6 fa0/0, R7 fa0/0, R9 fa0/0, R10 fa0/0, R12 fa0/0
b. Participants will telnet/ping to remote peer from their router without specifying any source Interface:
c. Lab instructor will stop packet capture on R1 fa0/0, R3 fa0/0, R4 fa0/0, R6 fa0/0, R7 fa0/0, R9 fa0/0, R10 fa0/0, R12 fa0/0
d. Open up the capture file and check the packet payload. Un-encrypted data and user name password are all visible.
e. Lab instructor will start second packet capture on R1 fa0/0, R3 fa0/0, R4 fa0/0, R6 fa0/0, R7 fa0/0, R9 fa0/0, R10 fa0/0, R12 fa0/0
f. Participants will telnet/ping to remote peer from their router with specifying any source Interface as fa0/0 or loopback 0:
g. Lab instructor will stop second packet capture on R1 fa0/0, R3 fa0/0, R4 fa0/0, R6 fa0/0, R7 fa0/0, R9 fa0/0, R10 fa0/0, R12 fa0/0
h. Open up the capture file and check the packet payload. Encrypted data and nothing is visible on the captured packet

## Workshop templates for reference purpose only:

### IPv4 VPN between R13 and R15

R13
config t
crypto isakmp policy 1
authentication pre-share
encryption aes
hash sha
group 5
exit
crypto isakmp key Tr@ining123 address 172.16.11.66
crypto ipsec transform-set ESP-AES-SHA esp-aes esp-sha-hmac
exit
access-list 101 permit ip 172.16.16.0 0.0.0.255 172.16.20.0 0.0.0.255
crypto map LAB-VPN 10 ipsec-isakmp
match address 101
set transform-set ESP-AES-SHA
set peer 172.16.11.66
exit
int fa 0/1
crypto map LAB-VPN
exit
exit
wr

Verification Command:

sh crypto ipsec sa
sh crypto isakmp peers
sh crypto isakmp sa

R15
config t
crypto isakmp policy 1
authentication pre-share
encryption aes
hash sha
group 5
exit
crypto isakmp key Tr@ining123 address 172.16.11.2
crypto ipsec transform-set ESP-AES-SHA esp-aes esp-sha-hmac
exit
access-list 101 permit ip 172.16.20.0 0.0.0.255 172.16.16.0 0.0.0.255
crypto map LAB-VPN 10 ipsec-isakmp
match address 101
set transform-set ESP-AES-SHA
set peer 172.16.11.2

exit
int fa0/1
crypto map LAB-VPN
exit
exit
wr

Verification Command:

sh crypto ipsec sa
sh crypto isakmp peers
sh crypto isakmp sa

## IPv6 VPN between R13 and R15

R13
config t
crypto isakmp policy 1
authentication pre-share
encryption aes
hash sha
group 5
exit
crypto isakmp key Tr@ining123 address ipv6 2406:6400:18::2/128
crypto ipsec transform-set ESP-AES-SHA esp-aes esp-sha-hmac
exit
ipv6 access-list MATCH-IPV6
permit 2406:6400:8000::/48 2406:6400:A000::/48
exit
crypto map ipv6 IPV6-LAB-VPN 10 ipsec-isakmp
match address MATCH-IPV6
set transform-set ESP-AES-SHA
set peer 2406:6400:18::2
exit
int fa 0/1
ipv6 crypto map IPV6-LAB-VPN
exit
exit
wr

Verification Command:

sh crypto ipsec sa
sh crypto isakmp peers
sh crypto isakmp sa

R15
config t
crypto isakmp policy 1
authentication pre-share

encryption aes
hash sha
group 5
exit
crypto isakmp key Tr@ining123 address ipv6 2406:6400:10::2/128
crypto ipsec transform-set ESP-AES-SHA esp-aes esp-sha-hmac
exit
ipv6 access-list MATCH-IPV6
permit 2406:6400:A000::/48 2406:6400:8000::/48
exit
crypto map ipv6 IPV6-LAB-VPN 10 ipsec-isakmp
match address MATCH-IPV6
set transform-set ESP-AES-SHA
set peer 2406:6400:10::2
exit
int fa0/1
ipv6 crypto map IPV6-LAB-VPN
exit
exit
wr

Verification Command:

sh crypto ipsec sa
sh crypto isakmp peers
sh crypto isakmp sa

## IPv4 VPN between R14 and R16

R14
config t
crypto isakmp policy 1
authentication pre-share
encryption aes
hash sha
group 5
exit
crypto isakmp key Tr@ining123 address 172.16.11.98
crypto ipsec transform-set ESP-AES-SHA esp-aes esp-sha-hmac
exit
access-list 101 permit ip 172.16.18.0 0.0.0.255 172.16.22.0 0.0.0.255
crypto map LAB-VPN 10 ipsec-isakmp
match address 101
set transform-set ESP-AES-SHA

```
set peer 172.16.11.98
exit
int fa 0/1
crypto map LAB-VPN
exit
exit
wr
```

Verification Command:

```
sh crypto ipsec sa
sh crypto isakmp peers
sh crypto isakmp sa
```

R16

```
config t
crypto isakmp policy 1
authentication pre-share
encryption aes
hash sha
group 5
exit
crypto isakmp key Tr@ining123 address 172.16.11.34
crypto ipsec transform-set ESP-AES-SHA esp-aes esp-sha-hmac
exit
access-list 101 permit ip 172.16.22.0 0.0.0.255 172.16.18.0 0.0.0.255
crypto map LAB-VPN 10 ipsec-isakmp
match address 101
set transform-set ESP-AES-SHA
set peer 172.16.11.34
exit
int fa0/1
crypto map LAB-VPN
exit
exit
wr
```

Verification Command:

```
sh crypto ipsec sa
sh crypto isakmp peers
sh crypto isakmp sa
```

## IPv6 VPN between R14 and R16

R14
config t
crypto isakmp policy 1
authentication pre-share
encryption aes
hash sha
group 5
exit
crypto isakmp key Tr@ining123 address ipv6 2406:6400:1c::2/128
crypto ipsec transform-set ESP-AES-SHA esp-aes esp-sha-hmac

exit
ipv6 access-list MATCH-IPV6
permit 2406:6400:9800::/48 2406:6400:b800::/48
exit
crypto map ipv6 IPV6-LAB-VPN 10 ipsec-isakmp
match address MATCH-IPV6
set transform-set ESP-AES-SHA
set peer 2406:6400:1c::2
exit
int fa 0/1
ipv6 crypto map IPV6-LAB-VPN
exit
exit
wr

Verification Command:

sh crypto ipsec sa
sh crypto isakmp peers
sh crypto isakmp sa

R16
config t
crypto isakmp policy 1
authentication pre-share
encryption aes
hash sha
group 5
exit
crypto isakmp key Tr@ining123 address ipv6 2406:6400:14::2/128
crypto ipsec transform-set ESP-AES-SHA esp-aes esp-sha-hmac
exit
ipv6 access-list MATCH-IPV6
permit 2406:6400:b800::/48 2406:6400:9800::/48
exit
crypto map ipv6 IPV6-LAB-VPN 10 ipsec-isakmp

match address MATCH-IPV6
set transform-set ESP-AES-SHA
set peer 2406:6400:14::2
exit
int fa0/1
ipv6 crypto map IPV6-LAB-VPN
exit
exit
wr

Verification Command:

sh crypto ipsec sa
sh crypto isakmp peers
sh crypto isakmp sa

**IPv4 VPN between R19 and R17**

R19
config t
crypto isakmp policy 1
authentication pre-share
encryption aes
hash sha
group 5
exit
crypto isakmp key Tr@ining123 address 172.16.11.130
crypto ipsec transform-set ESP-AES-SHA esp-aes esp-sha-hmac
exit
access-list 101 permit ip 172.16.28.0 0.0.0.255 172.16.24.0 0.0.0.255
crypto map LAB-VPN 10 ipsec-isakmp
match address 101
set transform-set ESP-AES-SHA
set peer 172.16.11.130
exit
int fa 0/1
crypto map LAB-VPN
exit
exit
wr

Verification Command:

sh crypto ipsec sa
sh crypto isakmp peers
sh crypto isakmp sa

R17
config t
crypto isakmp policy 1
authentication pre-share
encryption aes
hash sha
group 5
exit
crypto isakmp key Tr@ining123 address 172.16.11.194
crypto ipsec transform-set ESP-AES-SHA esp-aes esp-sha-hmac
exit
access-list 101 permit ip 172.16.24.0 0.0.0.255 172.16.28.0 0.0.0.255
crypto map LAB-VPN 10 ipsec-isakmp
match address 101
set transform-set ESP-AES-SHA
set peer 172.16.11.194

exit
int fa0/1
crypto map LAB-VPN
exit
exit
wr

Verification Command:

sh crypto ipsec sa
sh crypto isakmp peers
sh crypto isakmp sa

## IPv6 VPN between R19 and R17

R19
config t
crypto isakmp policy 1
authentication pre-share
encryption aes
hash sha
group 5
exit
crypto isakmp key Tr@ining123 address ipv6 2406:6400:20::2/128
crypto ipsec transform-set ESP-AES-SHA esp-aes esp-sha-hmac
exit
ipv6 access-list MATCH-IPV6
permit 2406:6400:e000::/48 2406:6400:c000::/48
exit
crypto map ipv6 IPV6-LAB-VPN 10 ipsec-isakmp
match address MATCH-IPV6
set transform-set ESP-AES-SHA

```
set peer 2406:6400:20::2
exit
int fa 0/1
ipv6 crypto map IPV6-LAB-VPN
exit
exit
wr
```

Verification Command:

```
sh crypto ipsec sa
sh crypto isakmp peers
sh crypto isakmp sa
```

R17

```
config t
crypto isakmp policy 1
authentication pre-share
encryption aes
hash sha
group 5
exit
crypto isakmp key Tr@ining123 address ipv6 2406:6400:28::2/128
crypto ipsec transform-set ESP-AES-SHA esp-aes esp-sha-hmac
exit
ipv6 access-list MATCH-IPV6
permit 2406:6400:c000::/48 2406:6400:e000::/48
exit
crypto map ipv6 IPV6-LAB-VPN 10 ipsec-isakmp
match address MATCH-IPV6
set transform-set ESP-AES-SHA
set peer 2406:6400:28::2
exit
int fa0/1
ipv6 crypto map IPV6-LAB-VPN
exit
exit
wr
```

Verification Command:

```
sh crypto ipsec sa
sh crypto isakmp peers
sh crypto isakmp sa
```

## IPv4 VPN between R20 and R18

R20
config t
crypto isakmp policy 1
authentication pre-share
encryption aes
hash sha
group 5
exit
crypto isakmp key Tr@ining123 address 172.16.11.162
crypto ipsec transform-set ESP-AES-SHA esp-aes esp-sha-hmac
exit
access-list 101 permit ip 172.16.30.0 0.0.0.255 172.16.26.0 0.0.0.255
crypto map LAB-VPN 10 ipsec-isakmp
match address 101
set transform-set ESP-AES-SHA
set peer 172.16.11.162
exit
int fa 0/1
crypto map LAB-VPN
exit

exit
wr

Verification Command:

sh crypto ipsec sa
sh crypto isakmp peers
sh crypto isakmp sa

R18
config t
crypto isakmp policy 1
authentication pre-share
encryption aes
hash sha
group 5
exit
crypto isakmp key Tr@ining123 address 172.16.11.226
crypto ipsec transform-set ESP-AES-SHA esp-aes esp-sha-hmac
exit
access-list 101 permit ip 172.16.26.0 0.0.0.255 172.16.30.0 0.0.0.255
crypto map LAB-VPN 10 ipsec-isakmp
match address 101
set transform-set ESP-AES-SHA
set peer 172.16.11.226
exit

int fa0/1
crypto map LAB-VPN
exit
exit
wr

Verification Command:

sh crypto ipsec sa
sh crypto isakmp peers
sh crypto isakmp sa

## IPv6 VPN between R20 and R18

R20
config t
crypto isakmp policy 1
authentication pre-share
encryption aes
hash sha
group 5
exit
crypto isakmp key Tr@ining123 address ipv6 2406:6400:24::2/128
crypto ipsec transform-set ESP-AES-SHA esp-aes esp-sha-hmac
exit
ipv6 access-list MATCH-IPV6
permit 2406:6400:f800::/48 2406:6400:d800::/48
exit
crypto map ipv6 IPV6-LAB-VPN 10 ipsec-isakmp
match address MATCH-IPV6
set transform-set ESP-AES-SHA
set peer 2406:6400:24::2
exit
int fa 0/1
ipv6 crypto map IPV6-LAB-VPN
exit
exit
wr

Verification Command:

sh crypto ipsec sa
sh crypto isakmp peers
sh crypto isakmp sa

R18
config t
crypto isakmp policy 1
authentication pre-share
encryption aes

```
hash sha
group 5
exit
crypto isakmp key Tr@ining123 address ipv6 2406:6400:2c::2/128
crypto ipsec transform-set ESP-AES-SHA esp-aes esp-sha-hmac
exit
ipv6 access-list MATCH-IPV6
permit 2406:6400:d800::/48 2406:6400:f800::/48
exit
crypto map ipv6 IPV6-LAB-VPN 10 ipsec-isakmp
match address MATCH-IPV6
set transform-set ESP-AES-SHA
set peer 2406:6400:2c::2
exit
int fa0/1
ipv6 crypto map IPV6-LAB-VPN
exit
exit
wr
```

Verification Command:

```
sh crypto ipsec sa
sh crypto isakmp peers
sh crypto isakmp sa
```