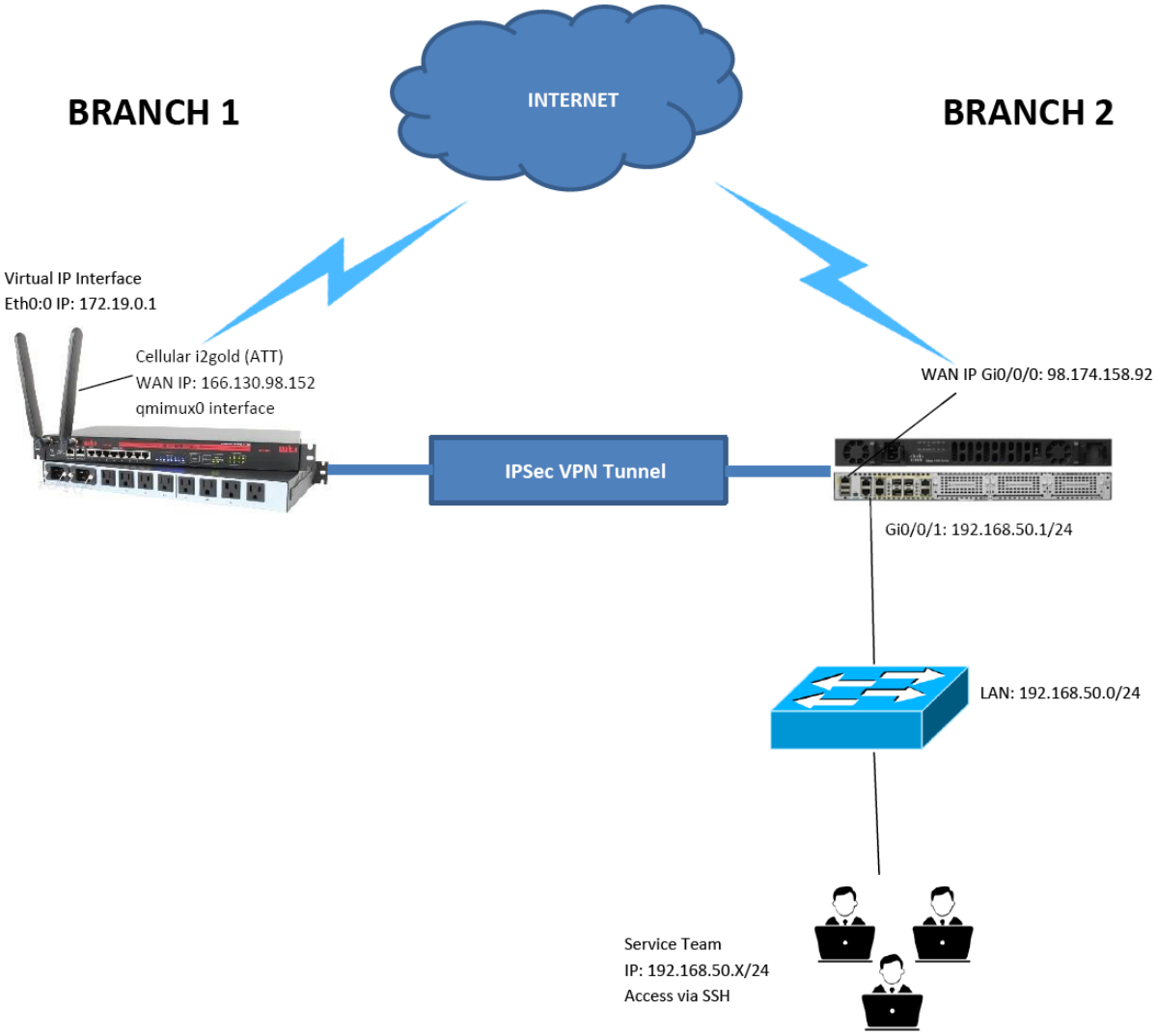
Cisco ISR IPSec VPN with WTI Virtual IP Address



In this scenario, the service team needs to access the attached devices from Branch 1. They can get access using the “IPSec VPN” feature with Virtual IP Interface define in WTI unit. The cell interface can be accessed securely because of an IPSec VPN Tunnel that has been established between the WTI and Cisco ISR’s IPSEC router.

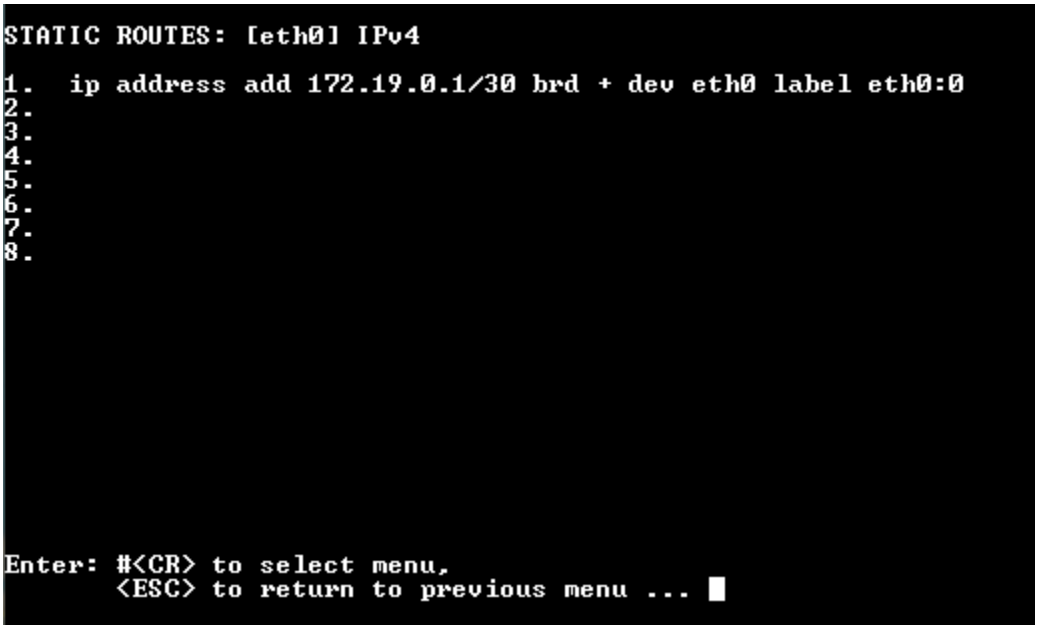
Setup configuration requirements:

WTI Network	
qmimux0 – Cell (i2gold)	166.130.98.152
Eth0:0 – Virtual Interface	172.19.0.1/30
Remote Network (Peer)	192.168.50.0/24
Tunnel Interface name	CiscoISR-WTI
Cisco ISR Router Network	
Gi0/0/0 – Outside (WAN)	98.174.158.92
Gi0/0/1 – Inside (LAN)	192.168.50.1
Local Network (LAN)	192.168.50.0/24
Remote Network (Peer Virtual IP Address)	172.19.0.0/30

Create Eth0:0 Virtual IP Interface

To create an Eth0:0 virtual IP Interface from WTI CLI, type /N and hit enter then select 6 for Static Route and enter the command mentioned below to create a virtual IP interface and assign an IP Address to it. In this example, we use IP Address 172.19.0.1 as our Virtual IP Address for eth0:0 interface.

ip address add 172.19.0.1/30 brd + dev eth0 label eth0:0



Create a NAT in IP TABLES

type /N and hit enter then select 5 for IP Tables enter the command mentioned below to allow remote peer (LAN) to access.

iptables -t nat -A POSTROUTING -d 192.168.50.0/24 -j SNAT --to-source 172.19.0.1

```
IPTABLES commands

1. These commands take standard Linux/Unix iptables syntax.
2. The Prefix for all entries must be "iptables".
3. Each line can be up to 256 characters.




Enter: <SPACE><CR> to clear,
       <iptables entry><CR> to change,
       <ESC> to return to previous menu.

(undefined)
--------------------------------------------------------------------------------
iptables -t nat -A POSTROUTING -d 192.168.50.0/24 -j SNAT --to-source 172.19.0.1
```

Configure WTI IPSEC VPN

To configure or setup IPSec VPN from WTI CLI, type /vpn and hit enter. Select 1 IPsec (Site-To-Site) to create a tunnel connection.

1. Enable:	**On**	
2. Tunnel Name:	**CiscoISR-WTI**	
3. Security:	**Pre-shared Secret (Static Key File)**	
4. Authentication Type:	**ESP**	
5. Left Address:	**166.130.98.152**	#WTI (Cell i2Gold) IP Address
6. Left ID:	**166.130.98.152**	#WTI (Cell i2Gold) IP Address
7. Left Subnet:	**172.19.0.1/30**	#Virtual IP LAN Subnet
8. Right Address:	**98.174.158.92**	#Cisco ISR WAN IP Address
9. Right ID:	**98.174.158.92**	#Cisco ISR WAN IP Address
10. Right Subnet:	**192.168.50.0/24**	#Cisco ISR LAN Subnet
11. Force Encaps:	**Off**	
12. Pre-shared Key:	**(Defined)**	#(Enter your pre-share key)
13. Tunnel Option	**(Defined)**	

1. **keyexchange**
   Parameter: **keyexchange**
   Value: **ikev2**

```
1.    Parameter:              keyexchange
2.    Value:                  ikev2
```

2. **Ike**

   Parameter: **ike**

   Value: **aes128-sha1-modp1536**

```
1.    Parameter:            ike
2.    Value:                aes128-sha1-modp1536
```

3. **esp**

   Parameter: **esp**

   Value: **aes128-sha1**

```
1.    Parameter:            esp
2.    Value:                aes128-sha1
```

4. **auto** #auto start VPN session

   Parameter: **auto**

   Value: **start**

```
1.    Parameter:            auto
2.    Value:                start
```

14 and 15 leave as default setting. Below is the overview of IPSec configuration.

```
IPSEC CLIENT VPN ASSOCIATED DETAILS: [CiscoISR-WTI] IPv4/IPv6

1.    Enable:               On
2.    Tunnel Name:          CiscoISR-WTI
3.    Security:             Pre-shared Secret (Static Key File)
4.    Authentication Type:  ESP
5.    Left Address:         166.130.98.152
6.    Left ID:              166.130.98.152
7.    Left Subnet :         172.19.0.1/30
8.    Right Address:        98.174.158.92
9.    Right ID:             98.174.158.92
10.   Right Subnet:         192.168.50.0/24
11.   Force Encaps:         Off
12.   Pre-Shared Key:       (defined)
13.   Tunnel Options:       (defined)
14.   Associated Menu:      (default)
15.   EAP User Menu:        (undefined)
16.   Runtime Status:
```

Cisco ISR 4300 Series Site to Site IKEv2 IPSec VPN Configuration

1. Define IKEv2 Keyring

```
CiscoISR#configure terminal
CiscoISR (config)#crypto ikev2 keyring keys
CiscoISR (config-ikev2-keyring)#peer WTI
CiscoISR (config-ikev2-keyring-peer)#address 166.130.98.152
CiscoISR (config-ikev2-keyring-peer)#pre-shared-key local test123
CiscoISR (config-ikev2-keyring-peer)#pre-shared-key remote test123
CiscoISR (config-ikev2-keyring-peer)#exit
CiscoISR (config-ikev2-keyring)#exit
CiscoISR (config)#exit
```

2. Define IKEv2 Proposal

```
CiscoISR#configure terminal
CiscoISR(config)#crypto ikev2 proposal ikev2proposal
CiscoISR(config-ikev2-proposal)#encryption aes-cbc-128
CiscoISR(config-ikev2-proposal)#integrity sha1
CiscoISR(config-ikev2-proposal)#group 5
CiscoISR(config-ikev2-proposal)#exit
CiscoISR(config)#exit
```

3. Define IKEv2 Policies

```
CiscoISR#configure terminal
CiscoISR(config)#crypto ikev2 policy ikev2policy
CiscoISR(config-ikev2-policy)#match fvrf any
CiscoISR(config-ikev2-policy)#proposal ikev2proposal
CiscoISR(config-ikev2-policy)#exit
CiscoISR(config)#exit
```

4. Define Crypto ACL to identify IPSec secured traffic

```
CiscoISR#configure terminal
CiscoISR(config)#ip access-list extended SITE1-SITE2-CACL
CiscoISR(config-ext-nacl)#permit ip 192.168.50.0 0.0.0.255 172.19.0.0 0.0.0.255
CiscoISR(config-ext-nacl)#exit
CiscoISR(config)#exit
```

5. Define Transform Sets

CiscoISR#configure terminal
CiscoISR(config)#crypto ipsec transform-set TS esp-aes esp-sha-hmac
CiscoISR(cfg-crypto-trans)#exit
CiscoISR(config)#exit

6. Define IKEv2 Profiles

CiscoISR#configure terminal
CiscoISR(config)#crypto ikev2 profile ikev2profile
CiscoISR(config-ikev2-profile)#match identity remote address 166.130.98.152 255.255.255.255
CiscoISR(config-ikev2-profile)#authentication local pre-share
CiscoISR(config-ikev2-profile)#authentication remote pre-share
CiscoISR(config-ikev2-profile)#keyring local keys
CiscoISR(config-ikev2-profile)#exit
CiscoISR(config)#exit

7. Define Crypto Maps

CiscoISR#configure terminal
CiscoISR(config)#crypto map cmap 10 ipsec-isakmp
CiscoISR(config-crypto-map)#set peer 166.130.98.152
CiscoISR(config-crypto-map)#set security-association lifetime seconds 86400
CiscoISR(config-crypto-map)#set transform-set TS
CiscoISR(config-crypto-map)#set ikev2-profile ikev2profile
CiscoISR(config-crypto-map)#match address SITE1-SITE2-CACL
CiscoISR(config-crypto-map)#exit
CiscoISR(config)#exit

8. Activate Crypto Maps by applying the Crypto Map to Router's wan Interface

CiscoISR#configure terminal
CiscoISR(config)#interface gi0/0/0
CiscoISR(config-if)#crypto map cmap
CiscoISR(config-if)#exit
CiscoISR(config)#exit

To check the vpn connection from WTI CLI

/bash ipsec status

```
CPM> /bash ipsec status
Security Associations (1 up, 0 connecting):
CiscoISR-WTI[1]: ESTABLISHED 46 seconds ago, 166.130.98.152[166.130.98.152]...98.174.158.92[98.174.158.92]
CiscoISR-WTI{1}:  INSTALLED, TUNNEL, reqid 1, ESP SPIs: cdf96ea5_i c8f0ecb2_o
CiscoISR-WTI{1}:   172.19.0.0/30 === 192.168.50.0/24
CiscoISR-WTI{2}:  INSTALLED, TUNNEL, reqid 1, ESP SPIs: cb33d3c4_i 3470d272_o
CiscoISR-WTI{2}:   172.19.0.0/30 === 192.168.50.0/24
```

/bash ipsec statusall

```
CPM> /bash ipsec statusall
Status of IKE charon daemon (strongSwan 5.9.3, Linux 5.4.0, armv7l):
  uptime: 10 seconds, since Aug 12 15:46:51 2022
  malloc: sbrk 540672, mmap 0, used 203744, free 336928
  worker threads: 11 of 16 idle, 5/0/0/0 working, job queue: 0/0/0/0, scheduled: 4
  loaded plugins: charon tpm aes des rc2 sha2 sha1 md5 mgf1 random nonce x509 revocation constraints pubkey pkcs1 pkcs7 pkcs8 pkcs1
cket-default stroke vici updown eap-identity eap-mschapv2 xauth-generic counters
Listening IP addresses:
  172.19.0.1
  166.130.98.152
Connections:
CiscoISR-WTI:  166.130.98.152...98.174.158.92  IKEv2, dpddelay=30s
CiscoISR-WTI:   local:  [166.130.98.152] uses pre-shared key authentication
CiscoISR-WTI:   remote: [98.174.158.92] uses pre-shared key authentication
CiscoISR-WTI:   child:  172.19.0.0/30 === 192.168.50.0/24 TUNNEL, dpdaction=restart
Security Associations (1 up, 0 connecting):
CiscoISR-WTI[1]: ESTABLISHED 9 seconds ago, 166.130.98.152[166.130.98.152]...98.174.158.92[98.174.158.92]
CiscoISR-WTI[1]: IKEv2 SPIs: b5f750475c577026_i* e6167ac5429666ed_r, pre-shared key reauthentication in 54 minutes
CiscoISR-WTI[1]: IKE proposal: AES_CBC_128/HMAC_SHA1_96/PRF_HMAC_SHA1/MODP_1536
CiscoISR-WTI{1}:  INSTALLED, TUNNEL, reqid 1, ESP SPIs: cdf96ea5_i c8f0ecb2_o
CiscoISR-WTI{1}:  AES_CBC_128/HMAC_SHA1_96, 1296 bytes_i (18 pkts, 0s ago), 1296 bytes_o (18 pkts, 0s ago), rekeying in 14 minutes
CiscoISR-WTI{1}:   172.19.0.0/30 === 192.168.50.0/24
```