Cisco ENCS Single WAN IP Deployment Scenarios

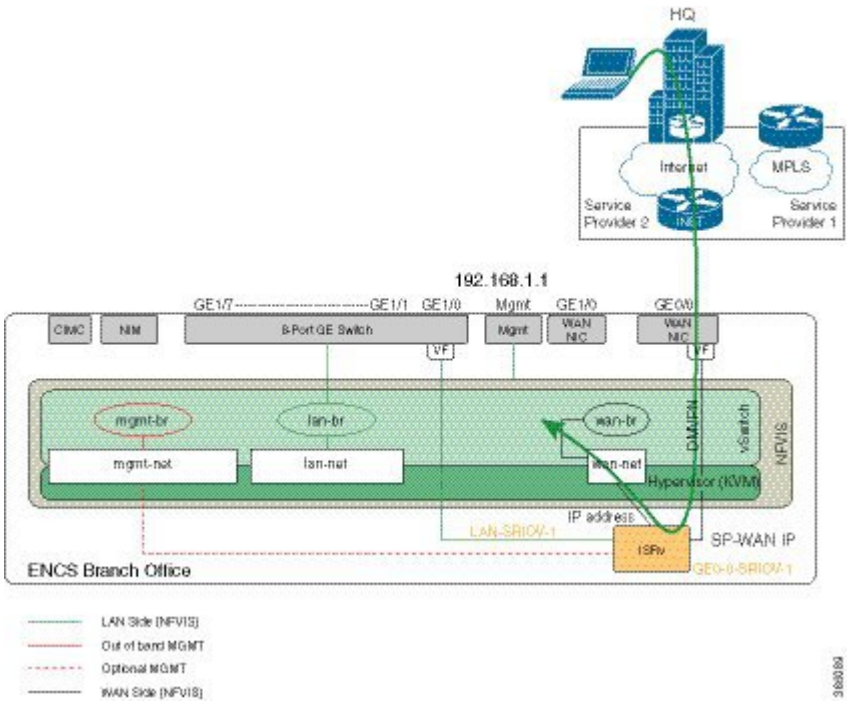
Single WAN IP Deployment

A single WAN IP deployment can be considered when the Cisco ENCS is preconfigured at the corporate main office with the service provider's WAN IP address, and shipped to the branch office for quick deployment. At the branch office, you do not have to perform any installation or configuration task. You just have to boot the system with the preconfigured setup. The single WAN IP deployment scenario could vary as per customer requirements. The following are two sample single WAN IP deployment scenarios with the Cisco ISRv:

Note Ensure that you preconfigure the Cisco ENCS at the main office before shippping the device to the branch office. You cannot connect to the remote branch office from your main office in a single WAN IP deployment scenario.

- Single WAN IP Deployment with Gigabit Ethernet Interface
- Single WAN IP Deployment with the 4G Interface

Figure 1: Single WAN IP Deployment Topology



Preconfiguring the Cisco ENCS for a Single WAN IP Deployment

To preconfigure the Cisco ENCS:

1. Install Cisco Enterprise NFVIS on the Cisco ENCS via CIMC. For details, see Installing Cisco Enterprise NFVIS on a Cisco ENCS 5100 and 5400.
2. Connect your local system (laptop) to the local management interface of the host server.
3. Open the Cisco Enterprise NFVIS portal via https://192.168.1.1.
4. Upload the Cisco ISRv image using the portal, and register the VM.
5. From the portal, remove the default Gigabit Ethernet 0/0 or GE0-0 WAN interface.
6. Deploy Cisco ISRv with Gigabit Ethernet 2 for SRIOV-1 and Gigabit Ethernet 3 for the wan-net.
7. Open the Cisco ISRv VNC.
8. From the VNC console, configure ISRv Gigabit Ethernet 2 and Gigabit Ethernet 3 interfaces with appropriate IP addresses. Then, perform a "no shut" of the interfaces.
9. Set the WAN static IP address to be on the same subnet as ISRv Gigabit Ethernet 2 IP address, and use ISRv Gigabit Ethernet 2 interface IP address as the default gateway.
10. Ping with the Cisco ISRv IP address to ensure connectivity.
11. Configure Dynamic Multipoint VPN on the Cisco ISRv, and ensure the main server can access the portal.

For details, see the Dynamic Multipoint VPN Configuration Guide https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_dmvpn/configuration/xe-16/sec-conn-dmvpn-xe-16-book.html .

Single WAN IP Deployment with Gigabit Ethernet Interface 0/0

In this scenario, two Gigabit Ethernet interfaces are configured on the Cisco ISRv: Gigabit Ethernet2 as the outbound interface and Gigabit Ethernet3 as the internal interface. The outbound interface IP address is provided by the service provider. The internal interface is the WAN interface that serves as the default gateway for Cisco Enterprise NFVIS.

```
crypto isakmp policy 5
 authentication pre-share
 group 2
crypto isakmp key dmvpnkey address 0.0.0.0

crypto ipsec transform-set dmvpnset esp-3des esp-sha-hmac
 mode tunnel

crypto ipsec profile dmvpnprof
 set security-association lifetime seconds 1200
 set transform-set dmvpnset

! DMVPN tunnel configuration
interface Tunnel100
 ip address 192.0.2.3 255.255.255.0
 no ip redirects
 ip mtu 1440
 ip nhrp authentication dmvpnkey
 ip nhrp map 192.0.2.1 198.51.100.1
 ip nhrp network-id 90
 ip nhrp nhs 192.0.2.2
 tunnel source GigabitEthernet2
 tunnel mode gre multipoint
 tunnel key 100000
 tunnel protection ipsec profile dmvpnprof
!
interface GigabitEthernet2
 description this is the outbound interface
 ip address 198.51.100.2 255.255.0.0

interface GigabitEthernet3
 description this is the inside interface
 ip address 192.0.2.10 255.255.255.0
!

router eigrp 90
 network 10.4.76.0 0.0.0.255
 network 192.0.2.1
 eigrp stub connected
 no auto-summary
!
ip route 20.1.0.0 255.255.0.0 198.51.100.1
!
Smart license configuration

ip name-server 198.51.100.9
ip domain lookup
service internal
do test license smart dev-cert Enable
```

```
service call-home
call-home
 contact-email-addr callhome@cisco.com
 mail-server 192.0.2.8 priority 1
 alert-group-config snapshot
  add-command "show license tech su"
 profile "CiscoTAC-1"
  active
  no destination transport-method email
  destination transport-method http
  no destination address http https://tools.cisco.com/its/service/oddce/services/DDCEService

  destination address http http://10.22.183.117:8080/ddce/services/DDCEService
!
clock timezone PST -7
ntp server 192.0.2.9
do license smart register idtoken NDM1NjE1MDAtNDViZC00ZTQ5LTg4MGEtNmRj
Njg2Mjg5ZDVlLTE0OTg5NDk2%0ANjEzNzd8elk5SEtoL2pMTGtuNSs3Q3Jxd
GVoSUVpTmFnY2l0alVqR3B5MzFj%0AVWVrST0%3D%0A
```

Single WAN IP Deployment with the 4G Interface

In this scenario, a 4G interface (NIM card) is configured as the outbound interface and Gigabit Ethernet3 as the internal interface. The outbound interface IP address is provided by the service provider. The internal interface is the WAN interface that serves as the default gateway for Cisco Enterprise NFVIS.

```
License Level: ax
License Type: N/A(Smart License Enabled)
Next reload license Level: ax

service timestamps debug datetime msec
service timestamps log datetime msec
service internal
service call-home
no platform punt-keepalive disable-kernel-core
platform console virtual
platform hardware throughput level MB 1000
!
hostname ISRv
!
boot-start-marker
boot system bootflash:isrv-universalk9.16.03.02.SPA.bin
boot-end-marker

clock timezone PST -7 0
call-home
 contact-email-addr callhome@cisco.com
 mail-server 192.0.2.8 priority 1
 alert-group-config snapshot
  add-command "show license tech su"
 profile "CiscoTAC-1"
  active
  destination transport-method http
  no destination transport-method email
  destination address http
http://198.51.100.4/Transportgateway/services/DeviceRequestHandler
  no destination address http
https://tools.cisco.com/its/service/oddce/services/DDCEService
!
ip name-server 198.51.100.2
```

```
ip domain name cisco.com

! IPsec configuration

crypto isakmp policy 5
 authentication pre-share
 group 2
crypto isakmp key dmvpnkey address 0.0.0.0
!
!
crypto ipsec transform-set dmvpnset esp-3des esp-sha-hmac
 mode tunnel
!
!
crypto ipsec profile dmvpnprof
 set security-association lifetime seconds 1200
 set transform-set dmvpnset
!
!4G interface
controller Cellular 0/2/0
 lte modem link-recovery rssi onset-threshold -110
 lte modem link-recovery monitor-timer 20
 lte modem link-recovery wait-timer 10
 lte modem link-recovery debounce-count 6
!
!
!
no ip ftp passive
ip ftp username admin
ip ftp password admin
!DMVPN tunnel configuration

interface Tunnel100
 ip address 198.51.100.3 255.255.255.0
 no ip redirects
 ip mtu 1440
 ip nhrp authentication dmvpnkey
 ip nhrp map 198.51.100.5 192.0.2.7
 ip nhrp network-id 90
 ip nhrp nhs 198.51.100.5
 tunnel source Cellular0/2/0
 tunnel mode gre multipoint
 tunnel key 100000
 tunnel protection ipsec profile dmvpnprof
!
!
interface GigabitEthernet2
 ip address 198.51.100.6 255.255.255.0
 ip nat inside
 negotiation auto
!
interface GigabitEthernet3
 ip address 198.51.100.11 255.255.255.0
 negotiation auto
!
interface Cellular0/2/0
 ip address negotiated
 load-interval 30
 dialer in-band
 dialer idle-timeout 0
 dialer-group 1
 ipv6 address autoconfig
 pulse-time 1
```

```
!
interface Cellular0/2/1
 no ip address
!
!
router eigrp 90
 network 198.51.100.0 0.0.0.255
 network 198.52.100.0 0.0.0.255
 network 99.0.0.0
 eigrp stub connected
!
!
virtual-service csr_mgmt
 ip shared host-interface GigabitEthernet1
 activate
!
ip forward-protocol nd
ip http server
ip http authentication local
ip http secure-server
!
ip route 0.0.0.0 0.0.0.0 Cellular0/2/0
ip route 192.0.2.12 255.255.255.0 198.51.100.5
ip route 192.0.2.13 255.255.255.255 198.51.100.5
ip route 192.0.2.14 255.255.255.255 198.51.100.5
ip route 192.0.2.15 255.255.255.255 198.51.100.5
ip route vrf Mgmt-intf 0.0.0.0 0.0.0.0 198.51.100.20
ip ssh authentication-retries 5
ip ssh rsa keypair-name ssh-key
ip ssh version 2
ip scp server enable
!
dialer-list 1 protocol ip permit
!
!
line con 0
 stopbits 1
line vty 0 4
 password cisco123
 login local
 transport input telnet ssh
!
ntp server 198.51.100.17
```