

Dynamips.Store

Workbook Description

Author: Dynamips.store

Focus: Practice

Level: Expert (CCIE)

Stream: CCIE Security v6: NAT & VPN Technology

Content: Topology, Questions, Initial Configuration, Solutions, Verifications.

Format: PDF

Table of Contents	Page No
1. Lab Details	4
1.1 Lab Summary	4
1.2 Initial Configuration	10
2. Texas DC Site Deployment	24
2.1 CONFIGURE ASA1 & 2 FOR ACTIVE/STANDBY	24
2.2 Configure Static routing on ASA1	28
2.3 Configure telnet & SSH access on ASA1 from inside	29
2.4 Configure OSPF on ASA1 for MPLS link	30
2.5 Web server 10.10.10.254 should be accessible from New Jersey, Virginia & New York using MPLS Link	31
2.6 telnet-ssh should be accessible from Virginia & New York using MPLS Link	34
3. Deployment of California	35
3.1 Configuring ASA3 interfaces with below configuration	35
3.2 Configuring ASA3 with Static routes 10.10.30.0/24 & 10.10.40.0/24—Next hop is 172.16.20.2 Default routes—Next hop is 192.168.200.1	36
3.3 Configuring ASA3 for SNMP with inside host 10.10.40.254	37
3.4 Configuring ASA3 for logging with inside host 10.10.40.254	37
3.6 Configuring Banner for ASA3 with below message	38
3.6 Configuring Static NAT for Web(HTTP,HTTPS) & FTP-RDP.	38
3.7 Configuring Internet access on 10.10.30.0/24 & 10.10.40.0/24 Network	44
4. Deployment of Virginia & New	45
4.1 Configuring Internet access for 10.20.20.0/24 on R2	45
4.2 Configuring Internet access for 10.30.10.0/24 on R3 router	47
4.3 Configuring single Gateway IPSec VPN between R2 & R3 with internet access	49
4.4 Configuring Dual Gateway IPSec VPN between R2 & R3 with internet access	54
5. Deployment of Virginia & New York	63
5.1 Configuring IPSec VPN between ASA4 & 5	63

1: LAB Details

1.1: LAB Summary

1.1. a: Hardware details

- 1) Active/Standby Failover
- 2) Local Internet Access
- 3) Static & Dynamic NAT
- 4) Policy NAT
- 5) IPsec VPN
- 6) Dual IPSEC VPN+NAT (PAT) on Router
- 7) Dynamic Routing in ASA

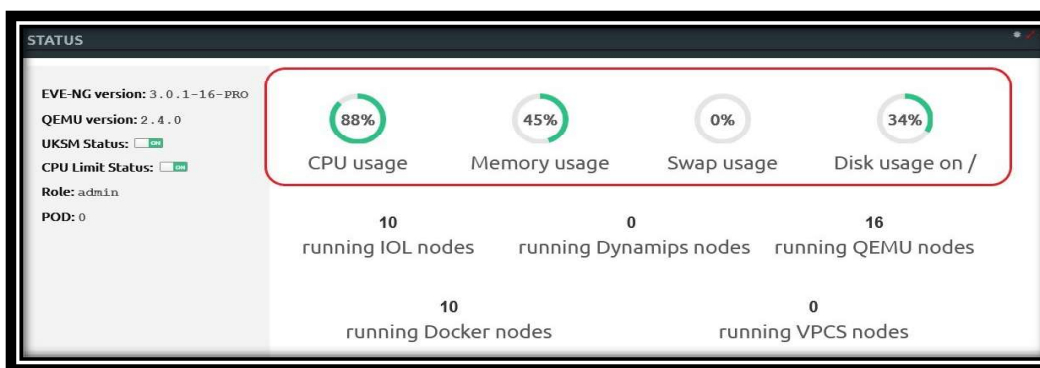
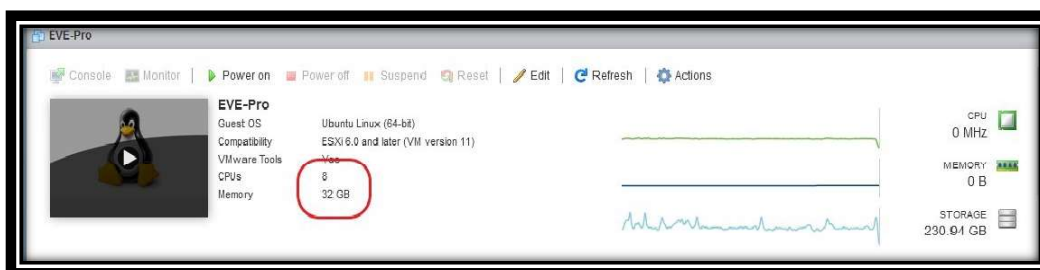
CPU 8/14 cores
RAM 32/64 GB
HDD 500 GB

NOTE: Recommended EVE-NG hosted server (if you do NOT have a strong PC or a Server)

- Link: <https://dynamips.store/product/eve-ng-lab/>

Dedicated IP, Server for practice CCIE Security and more.
Included All in one (IOS and Workbooks) to start your journey.

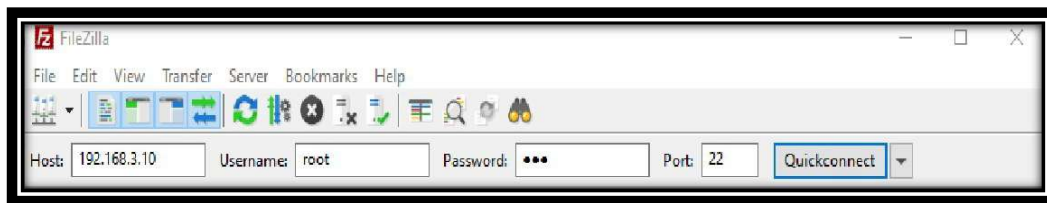
Note: After starting all nodes wait for 10 minutes for CPU utilization getting back to normal.



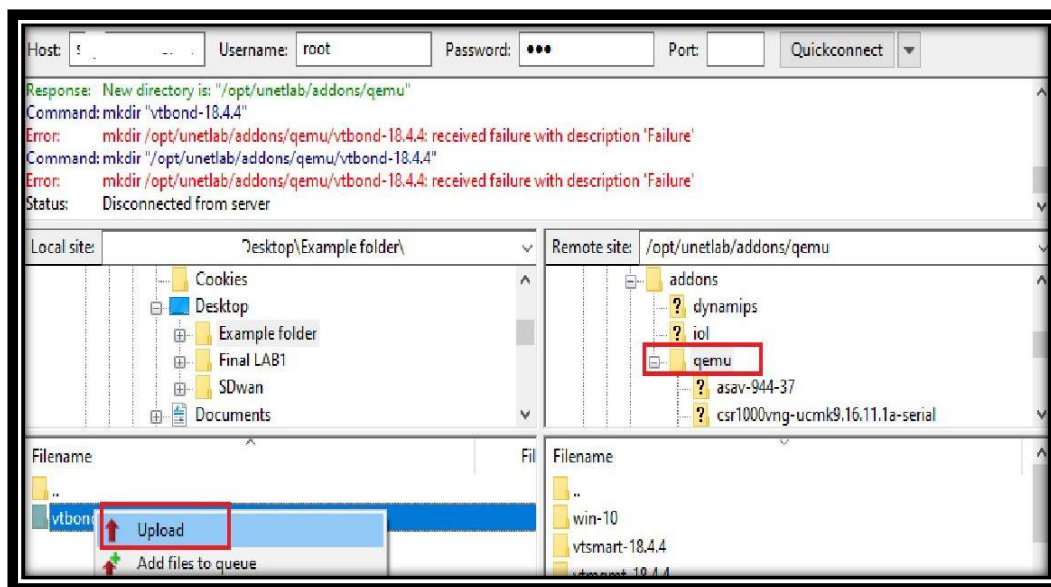
1.1. b: How to upload images into EVE-NG

NOTE: (escape the section below if you have purchased eve-ng full pack or eve-ng hosted server)

Step1: After starting eve-ng instance Login with FileZilla (with your displayed ip address using username & password as root & eve respectively)



Step2: Upload qemu images as shown below

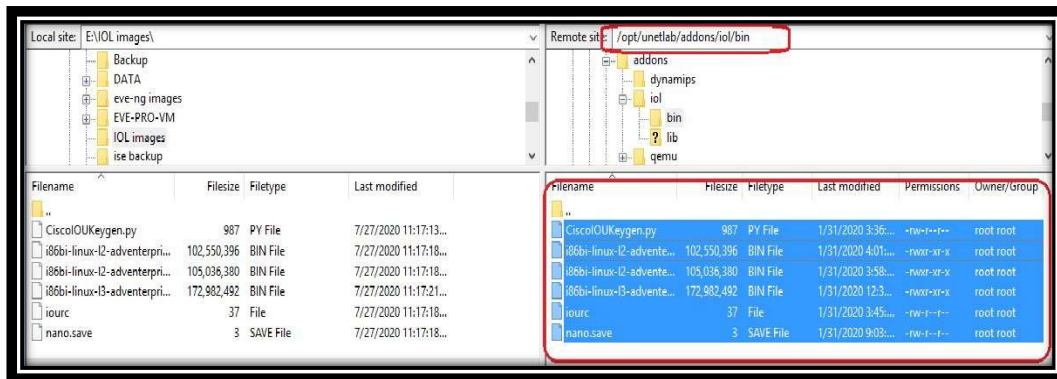


Step3: Login to your eve-ng server/hypervisor/vmware/etc. with username root & password eve

Step4: Run below command using cli

`/opt/unetlab/wrappers/unl_wrapper -a fixpermissions`

Step5: Uploading IOL images as shown below



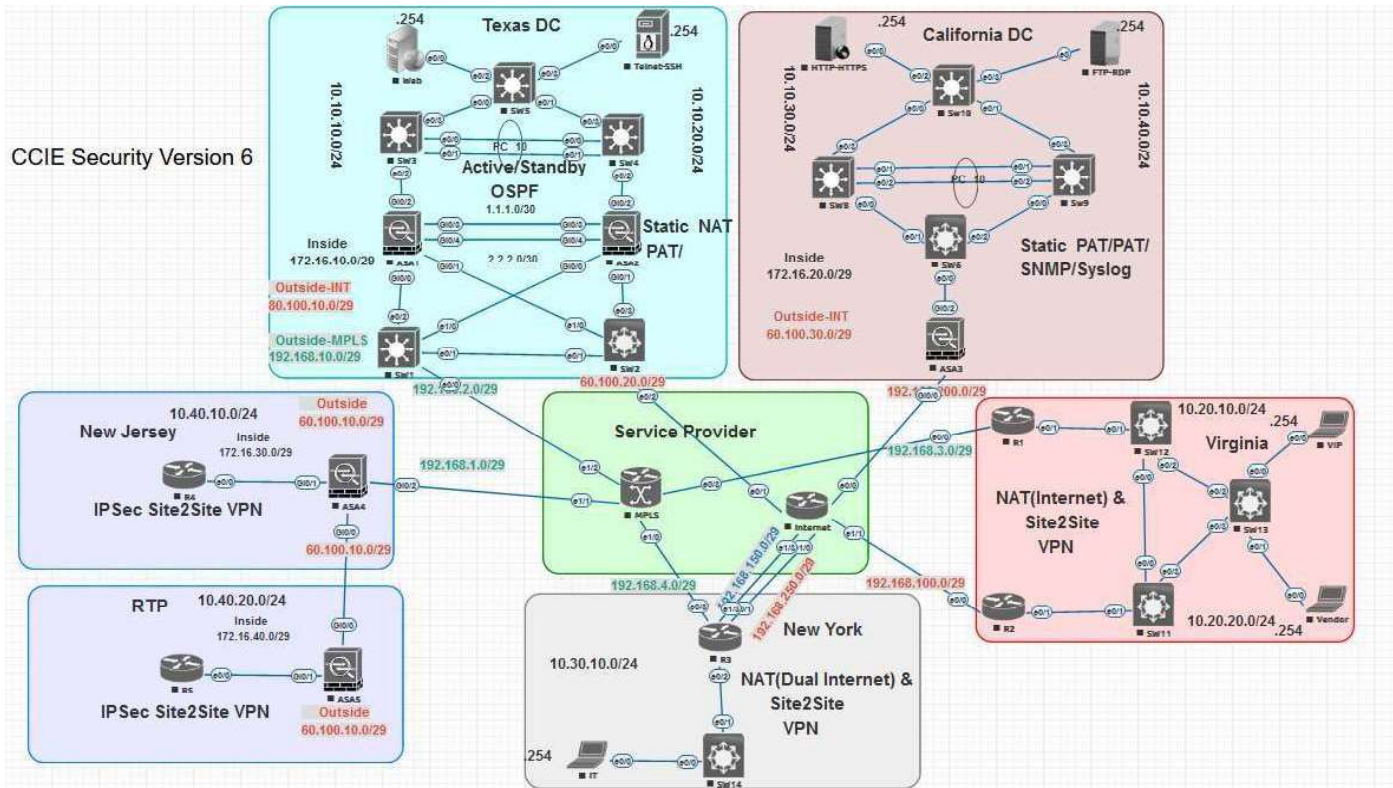
Step6: Run below command using cli

`/opt/unetlab/wrappers/unl_wrapper -a fixpermissions`

For more details on uploading images you can visit the below link.

<https://www.eve-ng.net/index.php/documentation/howtos/howto-add-cisco-iol-ios-on-linux/>

1.1. c: Lab Topology in Light Mode



1.1. e: IP Details

S/N	Host name	Location	IP's		
			Outside	Inside	
1	ASA1	Texas	192.168.2.2/29	80.100.10.2/29	172.16.10.1/29
2	ASA3	California	NA	60.100.30.2/29	172.16.20.1/29
3	ASA4	New Jersey	60.100.10.2/29	NA	172.16.30.1/29
4	ASA5	RTP	60.100.10.1/29	NA	172.16.40.1/29

1.1. f: Lab Nodes Used

Image versions used in Lab.

- Cisco ASAv Cisco Adaptive Security Appliance Software Version 9.4(4)37
- MPLS Router: i86bi_LinuxL3-AdvEnterpriseK9-M2_15.bin
- Internet Router: i86bi_LinuxL3-AdvEnterpriseK9-M2_15.bin
- L2 Switch: i86bi_linux_l2-adventerprisek9-15.2b.bin
- Host system: iol router or windows desktop
- Windows10: FTP/RDP
- Virtual PC: Testing

1.2 : Initial Configuration

For ISP Router, Switches, Hosts and Servers configurations are given below.

Startup Configuration

i86bi_LinuxL3-AdvEnterpriseK9-M2_157_3_May_2018.bin

Name/prefix
Internet

Icon
Router.png

NVRAM (KB)
1024

RAM (MB)
2048

Ethernet portgroups (4 int each)
2

Serial portgroups (4 int each)
0

I. Internet Router

```
hostname internet
ip name-server 8.8.8.8
ip name-server 1.1.1.1
```

```
ip domain-name dynamips.store
interface Ethernet0/0
description *** Connected to ASA3 ***
ip address 192.168.200.1 255.255.255.248
ip nat inside
ip virtual-reassembly in
duplex auto
!
interface Ethernet0/1
description *** Connected to SW2 ***
ip address 60.100.20.1 255.255.255.248
ip nat inside
ip virtual-reassembly in
duplex auto
!
!
interface Ethernet0/3
description *** Connected to R3 ISP1 ***
no ip address
ip nat inside
ip virtual-reassembly in
duplex auto
!
interface Ethernet1/0
description *** Connected to R3 ISP2 ***
ip address 192.168.250.1 255.255.255.248
ip nat inside
```

```

ip virtual-reassembly in
duplex auto
!
interface Ethernet1/1
description *** Connected to R2 ***
ip address 192.168.100.1 255.255.255.248
ip nat inside
ip virtual-reassembly in
duplex auto
!
interface Ethernet1/2
description *** Connected to internet ***
ip address dhcp
ip nat outside
ip virtual-reassembly in
duplex auto
!
interface Ethernet1/3
ip address 192.168.150.1 255.255.255.248
ip nat inside
ip virtual-reassembly in
duplex auto
!
ip nat inside source list NAT interface Ethernet1/2 overload
ip route 80.100.10.0 255.255.255.248 60.100.20.2
!
ip access-list standard NAT
permit 60.100.20.0 0.0.0.7
permit 80.100.10.0 0.0.0.7
permit 192.168.200.0 0.0.0.7
permit 192.168.100.0 0.0.0.7
permit 192.168.150.0 0.0.0.7
permit 192.168.250.0 0.0.0.7
!

```

II. MPLS

Name/prefix
MPLS

Icon
MPLS.png

NVRAM (KB)
1024

RAM (MB)
2048

Ethernet portgroups (4 int each)
2

Serial portgroups (4 int each)
0

hostname MPLS

```
ip domain name dynamips.store
```

```

interface Ethernet0/3
description *** Connected to R1 ***
ip address 192.168.3.1 255.255.255.248
duplex auto

```

```

!
interface Ethernet1/0
description *** Connected to R3 ***
ip address 192.168.4.1 255.255.255.248
duplex auto
!
interface Ethernet1/1
description *** Connected to ASA4 ***
ip address 192.168.1.1 255.255.255.248
duplex auto
!
interface Ethernet1/2
description *** Connected to SW1 ***
ip address 192.168.2.1 255.255.255.248
duplex auto
!
router ospf 10
redistribute connected subnets
network 192.168.1.0 0.0.0.7 area 0
network 192.168.2.0 0.0.0.7 area 0
network 192.168.3.0 0.0.0.7 area 0
network 192.168.4.0 0.0.0.7 area 0

```

III. SW1

```

hostname SW1

vlan 100
name MPLS
ip domain name dynamips.store

interface Ethernet0/0
description *** Connected to MPLS ***
no switchport
ip address 192.168.2.2 255.255.255.248
duplex auto
!
interface Ethernet0/1
description *** Connected to SW2 ***
switchport trunk encapsulation dot1q
switchport mode trunk
duplex auto
!
interface Ethernet0/2
description *** Connected to ASA1 Gi0/0 Active ***
switchport access vlan 100
switchport mode access
duplex auto
!
!
interface Ethernet1/0
description *** Connected to ASA2 Gi0/0 SEC ***
switchport access vlan 100
switchport mode access
!

```

```

interface Vlan100
description *** COnnected to MPLS ***
ip address 192.168.10.1 255.255.255.248
!
router ospf 10
 redistribute connected subnets
 network 192.168.2.0 0.0.0.7 area 0
 network 192.168.10.0 0.0.0.7 area 0

```

IV. SW2

```

hostname SW2
vlan 200
name INT
ip domain name dynamips.store

```

```

interface Ethernet0/1
description *** Connected to SW1 ***
switchport trunk encapsulation dot1q
switchport mode trunk
!
interface Ethernet0/2
no switchport
ip address 60.100.20.2 255.255.255.248
duplex auto
!
interface Ethernet0/3
description *** Connected to ASA2 Gi0/1 SEC ***
switchport access vlan 200
switchport mode access
!
interface Ethernet1/0
description *** Connected to ASA1 Gi0/1 Active ***
switchport access vlan 200
switchport mode access
duplex auto
!!
interface Vlan200
description *** INT Link ***
ip address 80.100.10.1 255.255.255.248
!

```

```

ip route 0.0.0.0 0.0.0.0 60.100.20.1

```

V. SW3

```

hostname SW3

vtp domain ds
vtp version 2
vtp mode server
ip domain name dynamips.store

```

```

vlan 10
name web

```

```

vlan 20
name telnet-ssh

interface Port-channel10
description *** Created for SW4 ***
switchport trunk encapsulation dot1q
switchport mode trunk
!
interface Ethernet0/0
switchport trunk encapsulation dot1q
switchport mode trunk
channel-group 10 mode active
!
interface Ethernet0/1
switchport trunk encapsulation dot1q
switchport mode trunk
channel-group 10 mode active
!
interface Ethernet0/2
description *** Connected to ASA1 Gi0/2 Active ***
switchport access vlan 200
switchport mode access
!
interface Ethernet0/3
description *** Connected to Sw5 ***
switchport trunk encapsulation dot1q
switchport mode trunk
!
interface Vlan10
description *** Web ***
ip address 10.10.10.2 255.255.255.0
vrrp 10 ip 10.10.10.1
vrrp 10 priority 200
!
interface Vlan20
description *** FTP ***
ip address 10.10.20.2 255.255.255.0
vrrp 20 ip 10.10.20.1
vrrp 20 priority 200
!
interface Vlan200
description *** Inside ***
ip address 172.16.10.4 255.255.255.248
vrrp 200 ip 172.16.10.2
vrrp 200 priority 200

ip route 0.0.0.0 0.0.0.0 172.16.10.1

```

VI. SW4

```

hostname SW4
vtp domain ds
vtp version 2
vtp mode client
ip domain name dynamips.store
interface Port-channel10
description *** Created for SW3 ***

```