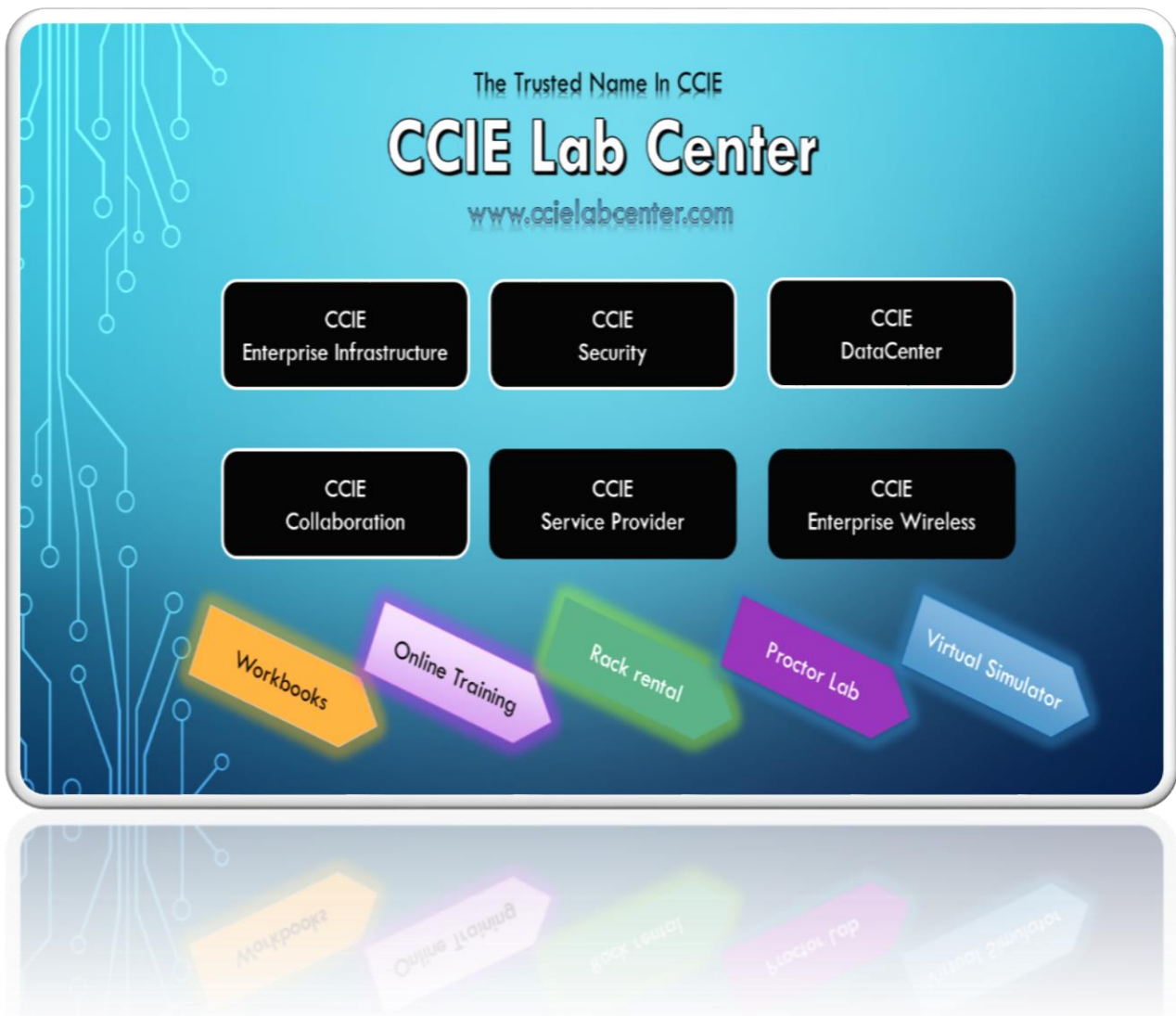


CCIE Lab Center

CLC

CCIE Security v6: Practice Lab v1.2



CCIE Lab Center

Workbook Description

Author: CCIE Lab Center (CLC)

Focus: Practice

Level: Expert (CCIE)

Stream: CCIE Security v6: NAT & VPN Technology

Lab: Practice Lab v1.2

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

Format: PDF

Protection: DRM Protected

Price/Cost: \$150 USD

CCIE Lab Center

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 accessible from New Jersey ,Virginia & New York using MPLS Link	31
2.6 telnet-ssh should 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
3.5 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

CCIE Lab Center

1: LAB Details

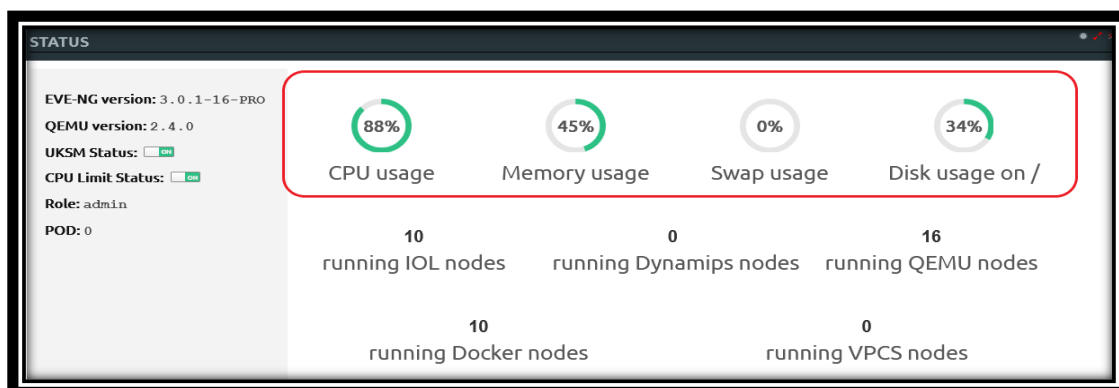
1.1: LAB Summary

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 core
RAM 32 GB
HDD 500 GB

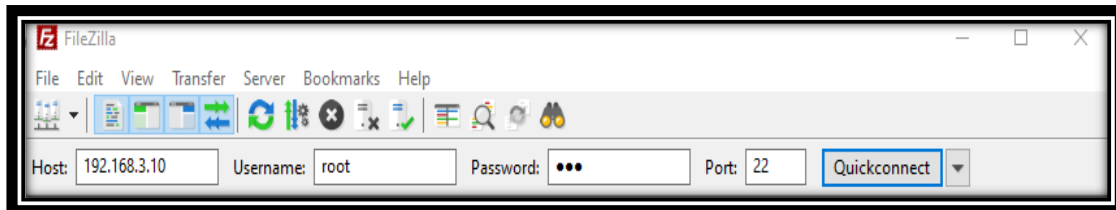
Note: After starting all nodes wait for 10 minutes for CPU utilization getting back to normal.



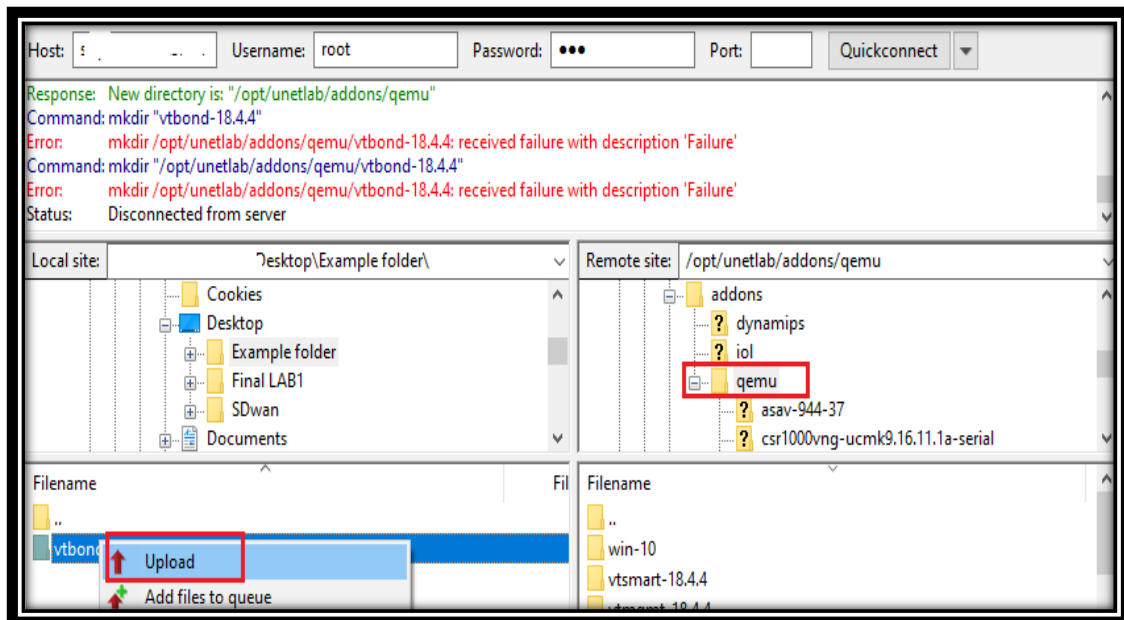
CCIE Lab Center

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

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



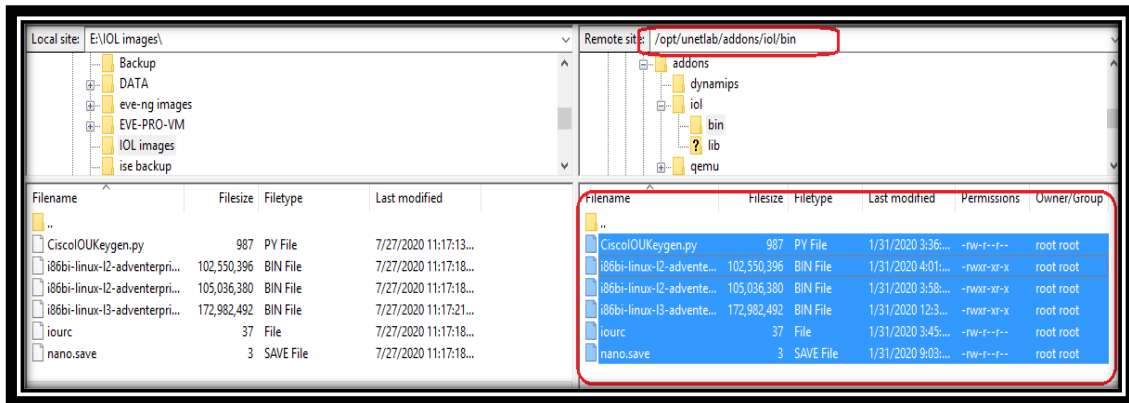
Step3: Login to your eve-ng server/hypervisor/vmware/etc. with username root & password eve

Step4: Run below command using cli

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

CCIE Lab Center

Step5: Uploading IOL images as shown below



Step6: Run below command using cli

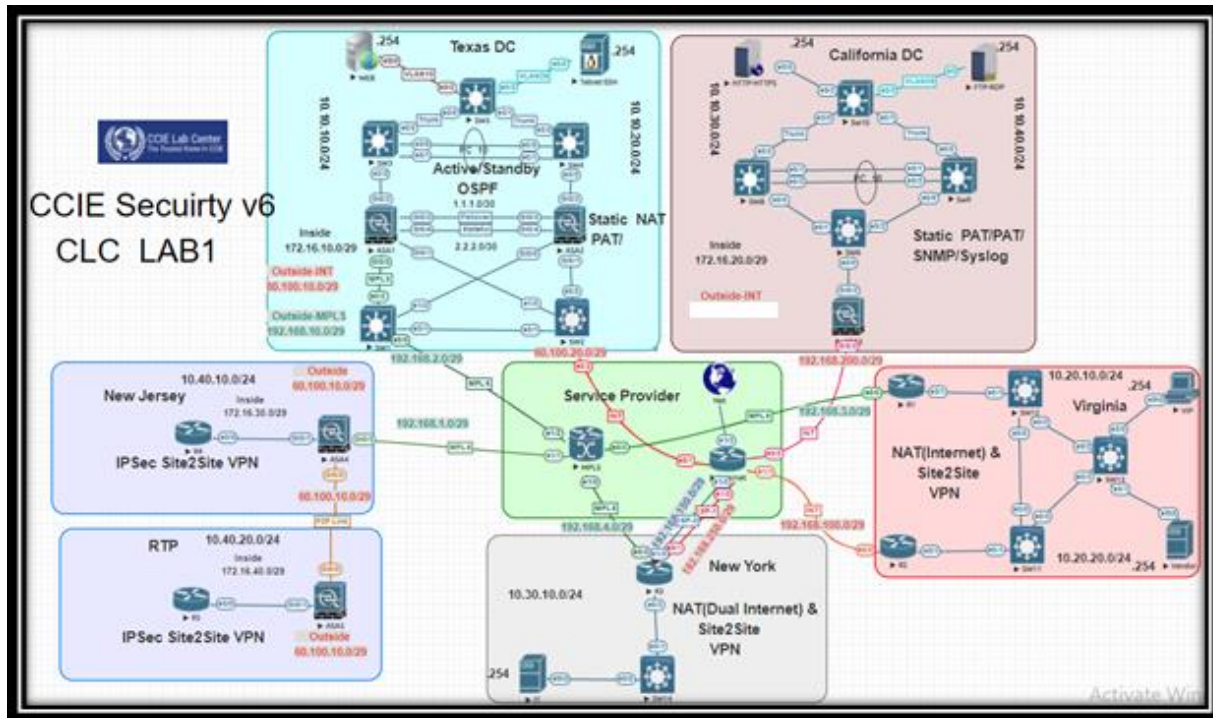
`/opt/unetlab/wrappers/unl_wrapper -a fixpermissions`

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/>

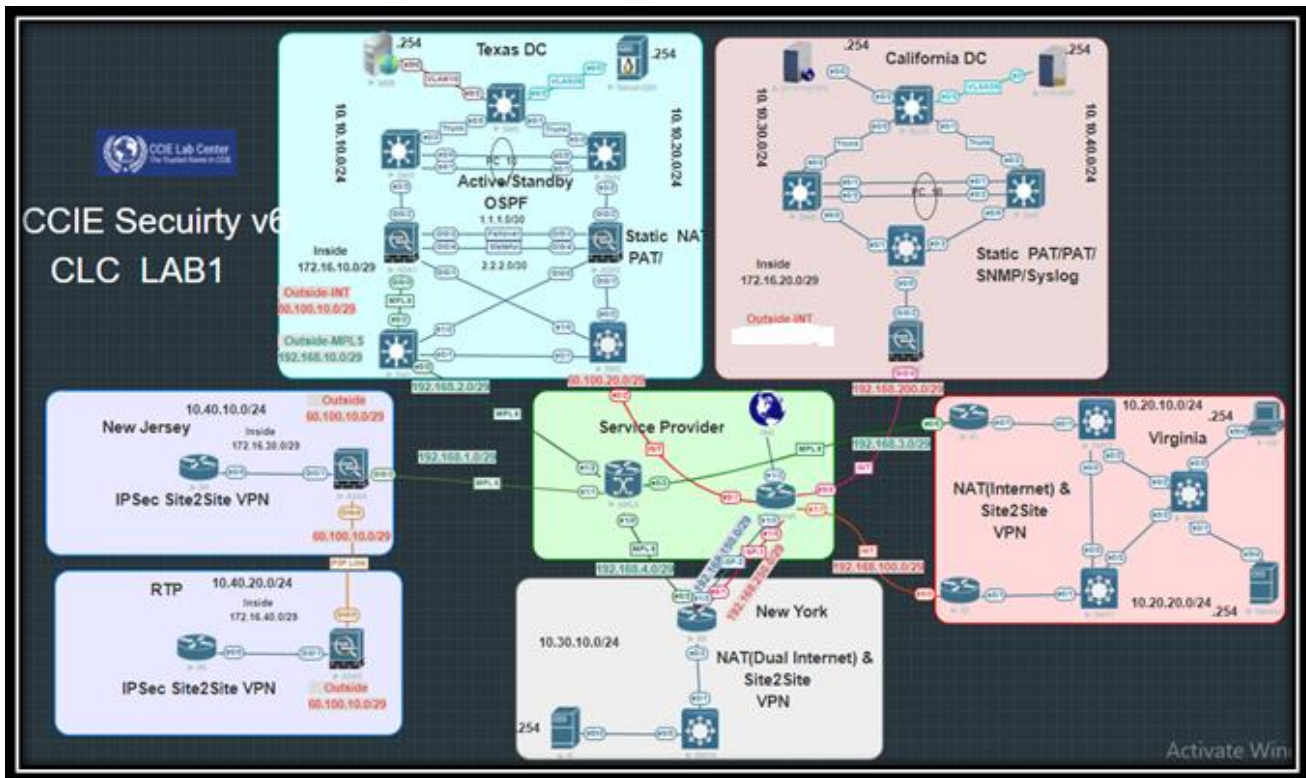
CCIE Lab Center

1.1. c: Lab Topology in Light Mode



CCIE Lab Center

1.1. d: Lab Topology in Dark Mode



CCIE Lab Center

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	192.168.200.2/29	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 v:ASA 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: EVE Docker GUI-Server
- Windows10: FTP/RDP
- Virtual PC:Testing

CCIE Lab Center

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 ccielabcenter.com
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
```

CCIE Lab Center

```

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	
<input type="text" value="MPLS"/>	
Icon	
 <input type="text" value="MPLS.png"/>	
NVRAM (KB)	RAM (MB)
<input type="text" value="1024"/>	<input type="text" value="2048"/>
Ethernet portgroups (4 int each)	Serial portgroups (4 int each)
<input type="text" value="2"/>	<input type="text" value="0"/>

hostname MPLS

ip domain name ccielabcenter.com

```

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

```

CCIE Lab Center

```

!
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 ccielabcenter.com

```

```

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
!

```

CCIE Lab Center

```
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 ccielabcenter.com
```

```
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 clc
vtp version 2
vtp mode server
ip domain name ccielabcenter.com
```

```
vlan 10
name web
```

CCIE Lab Center

```

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 clc
vtp version 2
vtp mode client
ip domain name ccielabcenter.com
interface Port-channel10
description *** Created for SW3 ***

```

CCIE Lab Center

```

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 Backup ***
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 10.10.10.3 255.255.255.0
vrrp 10 ip 10.10.10.1
!
interface Vlan20
description *** Ftp ***
ip address 10.10.20.3 255.255.255.0
vrrp 20 ip 10.10.20.1
!
interface Vlan200
description *** Inside ***
ip address 172.16.10.5 255.255.255.0
vrrp 200 ip 172.16.10.2

ip route 0.0.0.0 0.0.0.0 172.16.10.1

```

VII. SW5

```

hostname SW5
vtp domain clc
vtp version 2
vtp mode client

ip domain name ccielabcenter.com

interface Ethernet0/0
description *** Connected to SW3 ***
switchport trunk encapsulation dot1q
switchport mode trunk
!
interface Ethernet0/1
description *** Connected to SW4 ***

```

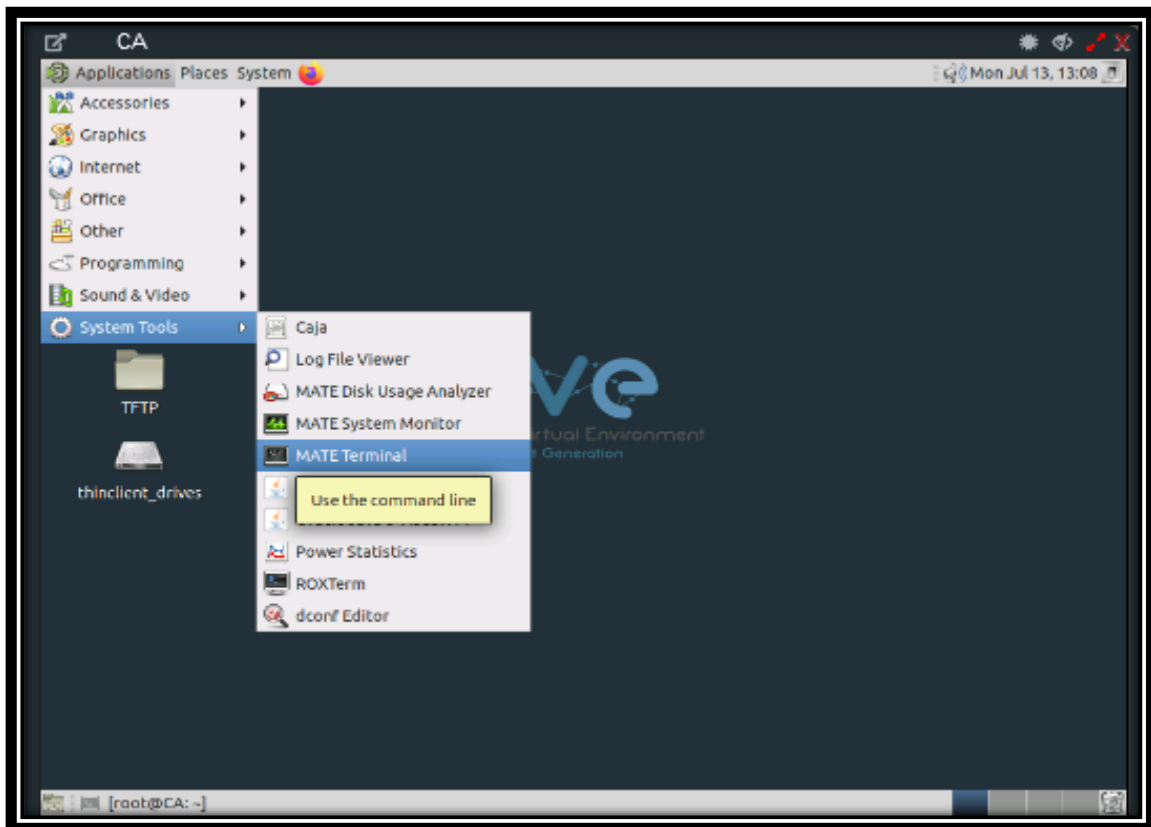
CCIE Lab Center

```

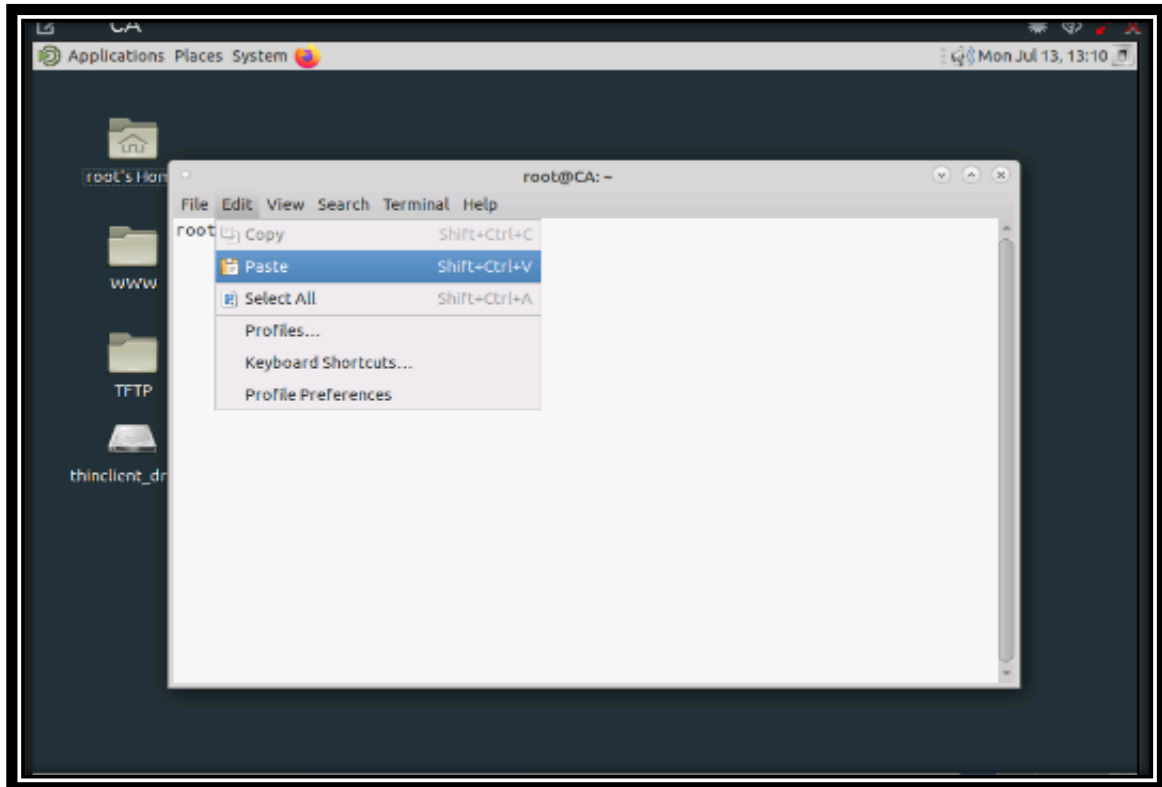
switchport trunk encapsulation dot1q
switchport mode trunk
!
interface Ethernet0/2
description *** Connected to WEB ***
switchport access vlan 10
switchport mode access
!
interface Ethernet0/3
description *** Connected to TELNET-SSH ***
switchport access vlan 20
switchport mode access

```

VIII. WEB (for Pro version)



CCIE Lab Center



```
ifconfig eth0 10.10.10.254 netmask 255.255.255.0
route add default gw 10.10.10.1 eth0
```

IX. Web (for Community version)

```
hostname web
```

```
username clc privilege 15 password 0 clc
interface Ethernet0/0
ip address 10.10.10.254 255.255.255.0
no shut
```

```
ip http server
ip http authentication local
ip http secure-server
ip route 0.0.0.0 0.0.0.0 10.10.10.1
```

X. Telnet-SSH

```
hostname SW7
```

```
ip domain name ccielabcenter.com
crypto key generate rsa
1024
username clc privilege 15 password clc
```

```
interface Ethernet0/0
ip address 10.10.20.254 255.255.255.0
```

CCIE Lab Center

```
ip default-gateway 10.10.20.1
```

```
line vt 0 4
transport input ssh telnet
login local
```

on SW6

```
vtp domain clc
vtp version 2
vtp mode server
```

```
hostname SW6
vlan 10
name HTTP-HTTPS
vlan 20
name FTP-RDP
ip domain name ccielabcenter.com
```

```
interface Ethernet0/0
description *** Connected to ASA3 Inside ***
no switchport
ip address 172.16.20.2 255.255.255.248
duplex auto
!
interface Ethernet0/1
description *** Connected to SW8 ***
switchport trunk encapsulation dot1q
switchport mode trunk
!
interface Ethernet0/2
description *** Connected to SW9 ***
switchport trunk encapsulation dot1q
switchport mode trunk
!
interface Vlan10
description *** Created for HTTP-HTTPS ***
ip address 10.10.30.1 255.255.255.0
!
interface Vlan20
description *** Created for FTP-RDP ***
ip address 10.10.40.1 255.255.255.0
!
!
ip route 0.0.0.0 0.0.0.0 172.16.20.1
```

on SW8

```
hostname SW8
vtp domain clc
vtp version 2
vtp mode client
ip domain name ccielabcenter.com
```

CCIE Lab Center

```

interface Port-channel10
switchport trunk encapsulation dot1q
switchport mode trunk
!
interface Ethernet0/0
description *** Connected to SW6 ***
switchport trunk encapsulation dot1q
switchport mode trunk
!
interface Ethernet0/1
description ** COnnected to to SW9 ***
switchport trunk encapsulation dot1q
switchport mode trunk
channel-group 10 mode active
!
interface Ethernet0/2
description ** COnnected to to SW9 ***
switchport trunk encapsulation dot1q
switchport mode trunk
channel-group 10 mode active
!
interface Ethernet0/3
description *** Connected to SW10 ***
switchport trunk encapsulation dot1q
switchport mode trunk

```

on SW9

```

hostname SW9
vtp domain clc
vtp version 2
vtp mode client
ip domain name ccielabcenter.com

```

```

interface Port-channel10
switchport trunk encapsulation dot1q
switchport mode trunk
!
interface Ethernet0/0
description *** Connected to SW6
switchport trunk encapsulation dot1q
switchport mode trunk
!
interface Ethernet0/1
description *** Connected to SW8 ***
switchport trunk encapsulation dot1q
switchport mode trunk
channel-group 10 mode active
!
interface Ethernet0/2
description *** Connected to SW8 ***
switchport trunk encapsulation dot1q
switchport mode trunk
channel-group 10 mode active
!

```

CCIE Lab Center

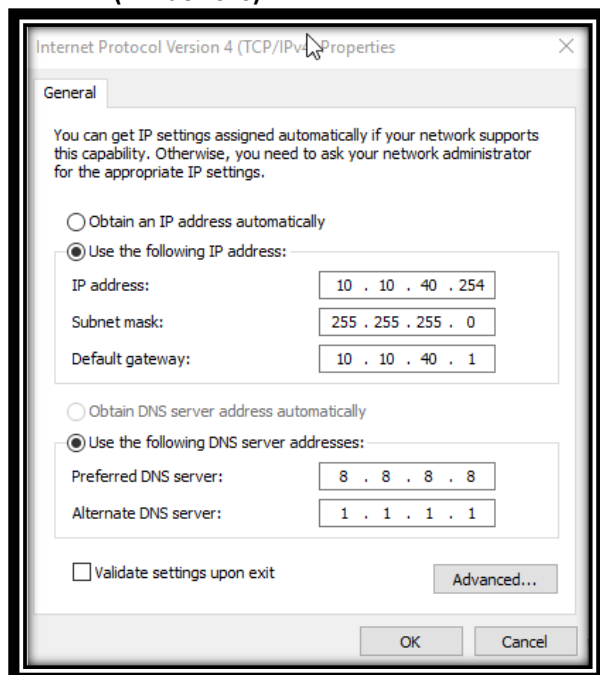
```
interface Ethernet0/3
description *** Connected to SW10 ***
switchport trunk encapsulation dot1q
switchport mode trunk
```

on SW10

```
vtp domain clc
vtp version 2
vtp mode client
ip domain name ccielabcenter.com
```

```
hostname SW10
interface Ethernet0/0
description *** Connected to SW8 ***
switchport trunk encapsulation dot1q
switchport mode trunk
!
interface Ethernet0/1
description *** Connected to SW9 ***
switchport trunk encapsulation dot1q
switchport mode trunk
!
interface Ethernet0/2
description *** Connected to HTTP-HTTPS ***
switchport access vlan 10
switchport mode access
!
interface Ethernet0/3
description *** Connected to FTP-RDP ***
switchport access vlan 20
switchport mode access
```

XI. FTP-RDP(Windows10)



CCIE Lab Center

XII. R1

```
ip domain name ccielabcenter.com
Hostname R1
    interface Ethernet0/0
description *** Connected to MPLS ***
ip address 192.168.3.2 255.255.255.248
duplex auto
!
interface Ethernet0/1
description *** Connected to SW12 ***
ip address 10.20.10.1 255.255.255.0
!
!
router ospf 10
 redistribute connected subnets
 network 192.168.3.0 0.0.0.7 area 0
```

XIII. R2

```
ip domain name ccielabcenter.com
Hostname R2
interface Ethernet0/0
description *** Connected to Internet ***
ip address 192.168.200.2 255.255.255.248
!
interface Ethernet0/1
description *** Connected to SW11 ***
ip address 10.20.20.1 255.255.255.0

ip route 0.0.0.0 0.0.0.0 192.168.200.1
!
```

XIV. SW11,SW12,SW13

```
Hostname SW11
Hostname SW12
Hostname SW13
ip domain name ccielabcenter.com
```

XV. VIP

```
hostname vip

interface Ethernet0/0

ip address 10.20.10.254 255.255.255.0

no shut

ip route 0.0.0.0 0.0.0.0 10.20.10.1
```

XVI. Vendor (for Pro version)

Go to Application > system tools >MATE Terminal
 ifconfig eth0 10.20.20.254 netmask 255.255.255.0

CCIE Lab Center

```
route add default gw 10.20.20.1 eth0
```

```
vim /etc/resolv.conf
```

```
nameserver 1.1.1.1
```

```
nameserver 8.8.8.8
```

```
esc>:wq
```

Vendor (for Community version)

```
hostname vendor
```

```
interface Ethernet0/0
```

```
ip address 10.20.20.254 255.255.255.0
```

```
no shut
```

```
ip route 0.0.0.0 0.0.0.0 10.20.20.1
```

XVII. R3

```
Hostname R3
```

```
interface Ethernet0/2
```

```
description *** Connected to SW14 ***
```

```
ip domain name ccielabcenter.com
```

```
ip address 10.30.10.1 255.255.255.0
```

```
interface Ethernet0/3
```

```
description *** Connected to MPLS ***
```

```
ip address 192.168.4.2 255.255.255.248
```

```
duplex auto
```

```
!
```

```
interface Ethernet1/0
```

```
description *** Connected to ISP1 ***
```

```
ip address 192.168.150.2 255.255.255.248
```

```
router ospf 10
```

```
redistribute connected subnets
```

```
network 192.168.4.0 0.0.0.7 area 0
```

```
ip route 0.0.0.0 0.0.0.0 192.168.150.1
```

XVIII. SW14

```
Hostname SW14
```

```
ip domain name ccielabcenter.com
```

XIX. IT (for Pro version)

Go to Application > system tools >MATE Terminal

```
ifconfig eth0 10.30.10.254 netmask 255.255.255.0
```

```
route add default gw 10.30.10.1 eth0
```

CCIE Lab Center

```
vim /etc/resolv.conf
```

```
nameserver 1.1.1.1
nameserver 8.8.8.8
```

```
esc>:wq
```

for Community version

```
hostname IT
```

```
username clc privilege 15 password 0 clc
interface Ethernet0/0
 ip address 10.30.10.254 255.255.255.0
no shut
```

```
ip http server
ip http authentication local
ip http secure-server
ip route 0.0.0.0 0.0.0.0 10.30.10.1
```

XX. R4

```
Hostname R4
ip domain name ccielabcenter.com
```

```
interface Loopback10
 ip address 10.40.10.1 255.255.255.0
!
interface Ethernet0/0
 description *** Connected to ASA4 Inside ***
 ip address 172.16.30.2 255.255.255.248
 duplex auto
```

```
ip route 0.0.0.0 0.0.0.0 172.16.30.1
```

XXI. R5

```
Hostname R4
ip domain name ccielabcenter.com
```

```
interface Loopback10
 ip address 10.40.20.1 255.255.255.0
!
interface Ethernet0/0
 description *** Connected to ASA5 Inside ***
 ip address 172.16.40.2 255.255.255.248
 duplex auto
```

```
ip route 0.0.0.0 0.0.0.0 172.16.40.1
```

CCIE Lab Center

2: Texas DC site Deployment

2.1: CONFIGURE ASA1 & 2 FOR ACTIVE/STANDBY

- Configure hostname as ASAv1 and ASAv2
- Configure ASAv2 device to back up ASAv1 in the event of failure
- Configure gi0/3 as the failover link
- Configure gi0/4 as the Stateful link
- Authenticate the failover control messages using a key "clc"
- Monitor all interfaces

ASA1 & ASA2 IP information					
hostname	nterface	SEC Level	Nameif	PRI IP	SEC IP
ASA1	Gi0/1	0	internet	80.100.10.2/29	80.100.10.3/29
	Gi0/0	0	mpls	192.168.2.2/29	192.168.2.3/29
	Gi0/2	100	inside	172.16.10.1/29	172.16.10.3/29
	Gi0/3	NA	fo	1.1.1.1/30	1.1.1.2/30
	Gi0/4	NA	stateful	2.2.2.1/30	2.2.2.2/30

Solution

On ASA1

```
hostname ASA1
```

```
interface g 0/0
no shut
nameif mpls
ip address 192.168.10.2 255.255.255.248 standby 192.168.10.3
interface g0/1
no shut
nameif internet
ip address 80.100.10.2 255.255.255.248 standby 80.100.10.3
```

```
interface g0/2
no shut
nameif inside
ip address 172.16.10.1 255.255.255.248 standby 172.16.10.3
```

CCIE Lab Center

```

interface g 0/3
no shut
description failover link
interface g0/4
no shut
description statefull link

failover lan unit primary
failover lan interface FO GigabitEthernet0/3
failover key clc
failover link STATE GigabitEthernet0/4
failover interface ip FO 1.1.1.1 255.255.255.252 standby 1.1.1.2
failover interface ip STATE 2.2.2.1 255.255.255.252 standby 2.2.2.2

```

On ASA2

```

interface g 0/3
no shut

interface g0/4
no shut

failover lan unit secondary
failover lan interface FO GigabitEthernet0/3
failover key clc
failover link STATE GigabitEthernet0/4
failover interface ip FO 1.1.1.1 255.255.255.252 standby 1.1.1.2
failover interface ip STATE 2.2.2.1 255.255.255.252 standby 2.2.2.2

```

Output on Primary

```

ASA1(config)# monitor-interface ins
ASA1(config)# monitor-interface inside
ASA1(config)# monitor-interface inter
ASA1(config)# monitor-interface internet
ASA1(config)# monitor-interface ou
ASA1(config)# monitor-interface outs
ASA1(config)# monitor-interface out
ASA1(config)# monitor-interface mpls
ASA1(config)# sh mon
ASA1(config)# sh monitor-interface
    This host: Primary - Active
        Interface internet (80.100.10.2): Normal (Monitored)
        Interface inside (172.16.10.1): Normal (Monitored)
        Interface mpls (192.168.10.2): Normal (Monitored)
    Other host: Secondary - Standby Ready
        Interface internet (80.100.10.3): Normal (Monitored)
        Interface inside (172.16.10.3): Normal (Monitored)
        Interface mpls (192.168.10.3): Normal (Monitored)
ASA1(config)#

```

CCIE Lab Center

```
MAC Address Move Notification Interval not set
ASA1(config-if)# fa
ASA1(config)# .

No Active mate detected
Beginning configuration replication: Sending to mate.
End Configuration Replication to mate
```

```
ASA1(config)# sh fa
Failover On
Failover unit Primary
Failover LAN Interface: FO GigabitEthernet0/3 (up)
Reconnect timeout 0:00:00
Unit Poll frequency 1 seconds, holdtime 15 seconds
Interface Poll frequency 5 seconds, holdtime 25 seconds
Interface Policy 1
Monitored Interfaces 3 of 61 maximum
MAC Address Move Notification Interval not set
Version: Ours 9.4(4)37, Mate 9.4(4)37
Last Failover at: 06:14:01 UTC Sep 23 2020
This host: Primary - Active
Active time: 112 (sec)
slot 0: empty
Interface internet (80.100.10.2): Normal (Monitored)
Interface inside (172.16.10.1): Normal (Monitored)
Interface mpls (192.168.10.2): Normal (Monitored)
Other host: Secondary - Standby Ready
Active time: 0 (sec)
Interface internet (80.100.10.3): Normal (Monitored)
Interface inside (172.16.10.3): Normal (Monitored)
Interface mpls (192.168.10.3): Normal (Monitored)

Stateful Failover Logical Update Statistics
Link : STATE GigabitEthernet0/4 (up)
Stateful Obj  xmit      xerr      rcv        rerr
General       27          0         13          0
sys cmd       13          0         13          0
up time        0          0          0          0
RPC services   0          0          0          0
TCP conn       0          0          0          0
UDP conn       0          0          0          0
ARP tbl       5          0          0          0
Xlate Timeout  0          0          0          0
IPv6 ND tbl    0          0          0          0
VPN IKEv1 SA   0          0          0          0
VPN IKEv1 P2   0          0          0          0
```

Output on Secondary

```
ciscoasa(config)# fa
ciscoasa(config)# ..

Detected an Active mate
Beginning configuration replication from mate.
WARNING: Local user database is empty and there are still 'aaa' commands for 'LOCAL'.
Creating trustpoint "_SmartCallHome_ServerCA" and installing certificate...

Trustpoint CA certificate accepted.

WARNING: Trustpoint _SmartCallHome_ServerCA is already authenticated.
End configuration replication from mate.
```

CCIE Lab Center

```

ASA1(config)# sh fa
Failover On
Failover unit Secondary
Failover LAN Interface: FO GigabitEthernet0/3 (up)
Reconnect timeout 0:00:00
Unit Poll frequency 1 seconds, holdtime 15 seconds
Interface Poll frequency 5 seconds, holdtime 25 seconds
Interface Policy 1
Monitored Interfaces 3 of 61 maximum
MAC Address Move Notification Interval not set
Version: Ours 9.4(4)37, Mate 9.4(4)37
Last Failover at: 07:06:36 UTC Sep 21 2020
  This host: Secondary - Standby Ready
    Active time: 0 (sec)
      slot 0: empty
        Interface mpls (192.168.10.3): Normal (Monitored)
        Interface internet (80.100.10.3): Normal (Monitored)
        Interface inside (172.16.10.3): Normal (Monitored)
  Other host: Primary - Active
    Active time: 223 (sec)
      Interface mpls (192.168.10.2): Normal (Monitored)
      Interface internet (80.100.10.2): Normal (Monitored)
      Interface inside (172.16.10.1): Normal (Monitored)

```

CCIE Lab Center

2.2: Configure Static routing on ASA1

10.10.10.0/24 & 10.10.20.0/24 Next hop IP is 172.16.10.2

Solution

```
route inside 10.10.10.0 255.255.255.0 172.16.10.2
```

```
route inside 10.10.20.0 255.255.255.0 172.16.10.2
```

```
ASA1(config)# ping 10.10.10.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.10.10.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/6/10 ms
ASA1(config)# ping 10.10.20.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.10.20.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/4/10 ms
ASA1(config)#
```

CCIE Lab Center

2.3: Configure telnet & SSH access on ASA1 from inside

Solution

```
passwd cisco
domain-name ccielabcenter.com
crypto key generate rsa modulus 1024
username admin password cisco privilege 15
aaa authentication ssh console LOCAL
ssh 0.0.0.0 0.0.0.0 inside
telnet 0.0.0.0 0.0.0.0 inside
```

```
% No user specified nor available for SSH client
SW3#telnet 172.16.10.1
Trying 172.16.10.1 ... Open

User Access Verification

Username: clc
Password: ***
Type help or '?' for a list of available commands.
ASA1>
```

SSH access from telnet-ssh system

```
telnet-SSH#ssh -l clc 172.16.10.1

*Sep 25 09:24:16.784: %SYS-5-CONFIG_I: Configured from console by console
Password:
Type help or '?' for a list of available commands.
ASA1>
ASA1> en
Password: ***
```

CCIE Lab Center

2.4: Configure OSPF on ASA1 for MPLS link

On ASA1

```
router ospf 10
network 192.168.10.0 255.255.255.248 area 0
redistribute static subnets
```

output

```
ASA1(config)# sh ospf neighbor

Neighbor ID      Pri   State           Dead Time   Address      Interface
192.168.10.1      1    FULL/DR         0:00:34    192.168.10.1 mpls
ASA1(config)#
```

CCIE Lab Center

2.5: Web server 10.10.10.254 should be accessible from New Jersey, Virginia & New York using MPLS Link

Solution

object network web-server

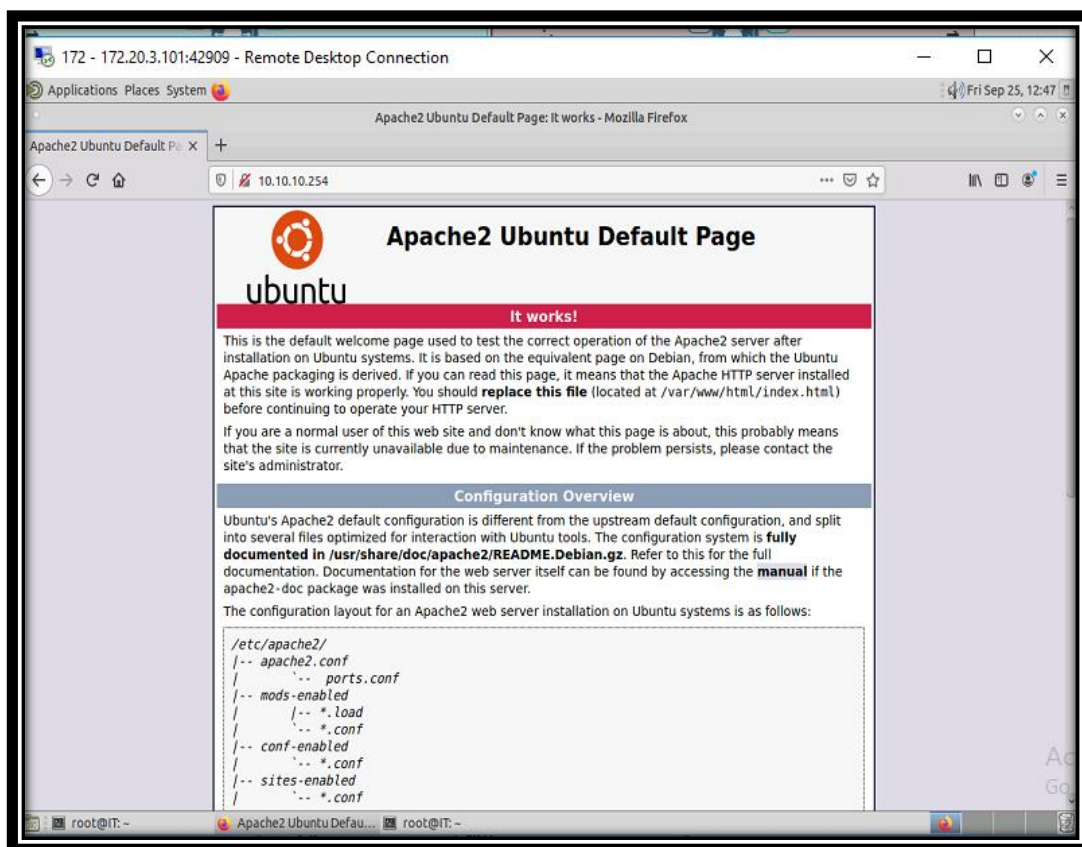
host 10.10.10.254

access-list mpls permit tcp any object web-server eq 80

access-group mpls in interface mpls

Output

on New York (IT System)



CCIE Lab Center

On Virginia R1 router

```
R1#telnet 10.10.10.254 80
Trying 10.10.10.254, 80 ... Open

^C
HTTP/1.1 400 Bad Request
Date: Fri, 25 Sep 2020 12:50:11 GMT
Server: Apache/2.4.29 (Ubuntu)
Content-Length: 301
Connection: close
Content-Type: text/html; charset=iso-8859-1

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
    <html><head>
        <title>400 Bad Request</title>
    </head><body>
        <h1>Bad Request</h1>
        <p>Your browser sent a request that
this server could not understand.<br />
        </p>
        <hr>
        <address>Apache/2.4.29 (Ubuntu)
Server at 127.0.0.1 Port 80</address>
    </body></html>

[Connection to 10.10.10.254 closed by foreign host]
R1#
```

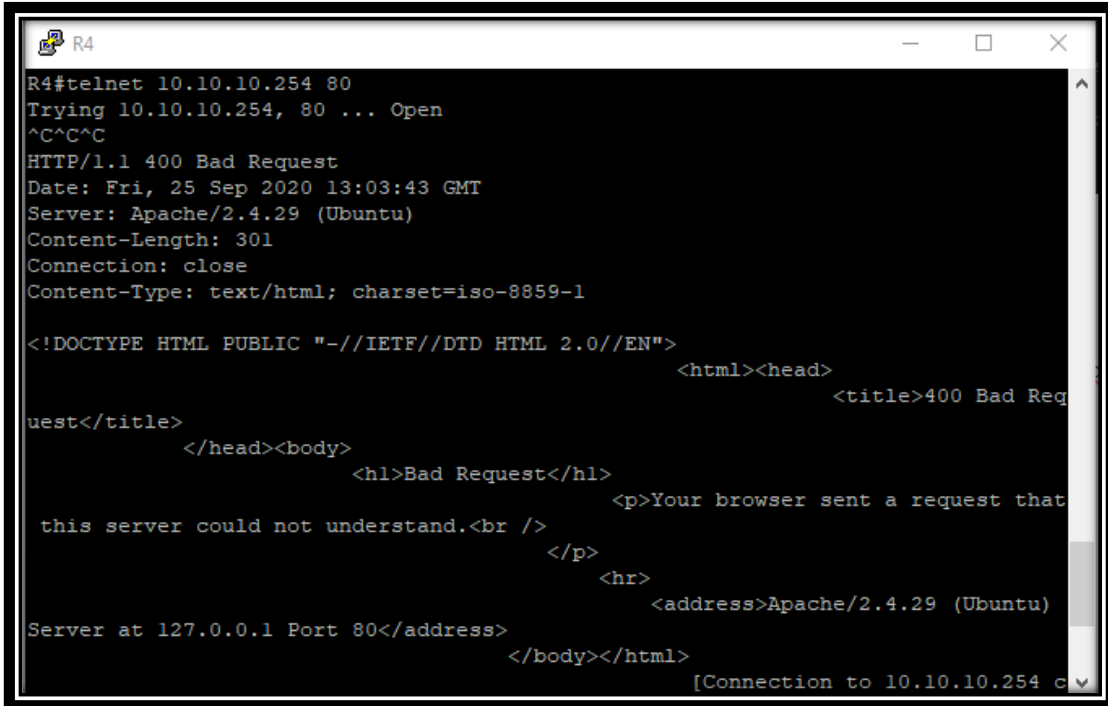
On New Jersey R4 can be try once after configuring ASA4

On ASA4

```
router ospf 10
network 192.168.1.0 255.255.255.248 area 0
redistribute connected subnets
```

```
access-list in extended permit tcp any host 10.10.10.254 eq www
access-group in in interface inside
```

CCIE Lab Center



```
R4#telnet 10.10.10.254 80
Trying 10.10.10.254, 80 ... Open
^C^C^C
HTTP/1.1 400 Bad Request
Date: Fri, 25 Sep 2020 13:03:43 GMT
Server: Apache/2.4.29 (Ubuntu)
Content-Length: 301
Connection: close
Content-Type: text/html; charset=iso-8859-1

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
    <html><head>
        <title>400 Bad Request</title>
    </head><body>
        <h1>Bad Request</h1>
        <p>Your browser sent a request that
this server could not understand.<br />
        </p>
        <hr>
        <address>Apache/2.4.29 (Ubuntu)
Server at 127.0.0.1 Port 80</address>
    </body></html>
[Connection to 10.10.10.254 closed]
```

CCIE Lab Center

2.6: telnet-ssh should accessible from Virginia & New York using MPLS Link

```
R1#  
R1#tel  
R1#telnet 10.10.20.254  
Trying 10.10.20.254 ... open  
  
User Access Verification  
  
Username: c1c  
Password:  
telnet-SSH#  
telnet-SSH#  
telnet-SSH#exit  
  
[Connection to 10.10.20.254 closed by foreign host]  
R1#  
R1#ssh -l c1c 10.10.20.254  
Password:  
telnet-SSH#
```

CCIE Lab Center

3: Deployment of California

3.1 Configuring ASA3 interfaces with below configuration

ASA3 IP information				
hostname	Interface	SEC Level	Nameif	IP
ASA3	Gi0/0	0	outside	192.168.200.2/29
	Gi0/2	100	inside	172.16.20.1/29

Solution

```
interface GigabitEthernet0/0
nameif outside
security-level 0
ip address 192.168.200.2 255.255.255.248
```

```
interface GigabitEthernet0/2
nameif inside
security-level 100
ip address 172.16.20.1 255.255.255.248
```

CCIE Lab Center

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

Task2 Configuring ASA3 with Static routes

10.10.30.0/24 & 10.10.40.0/24—Next hop is 172.16.20.2

Solution

```
route outside 0.0.0.0 0.0.0.0 192.168.200.1 1
route inside 10.10.30.0 255.255.255.0 172.16.20.2 1
route inside 10.10.40.0 255.255.255.0 172.16.20.2 1
```

```
ASA3(config)# ping 10.10.30.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.10.30.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/6/20 ms
ASA3(config)# ping 10.10.40.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.10.40.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/4/10 ms
ASA3(config)#
```

CCIE Lab Center

3.3: Configuring ASA3 for SNMP with inside host 10.10.40.254

solution

```
snmp-server community clc
snmp-server enable traps
snmp-server host inside 10.10.40.254
snmp-server location california
snmp-server contact clcadmin
```

3.4: Configuring ASA3 for logging with inside host 10.10.40.254

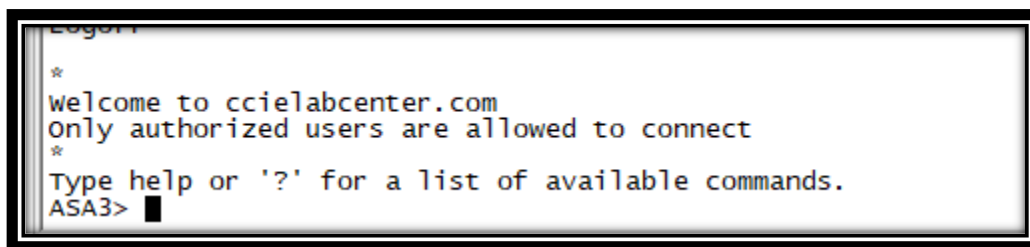
Solution

```
logging enable
logging buffer-size 4096
logging host inside 10.10.40.254
logging facility 16
```

CCIE Lab Center

3.5: Configuring Banner for ASA3 with below message

```
banner motd *  
banner motd Welcome to ccielabcenter.com  
banner motd Only authorized users are allowed to connect  
banner motd *
```



3.6: Configuring Static NAT for Web(HTTP,HTTPS) & FTP-RDP.

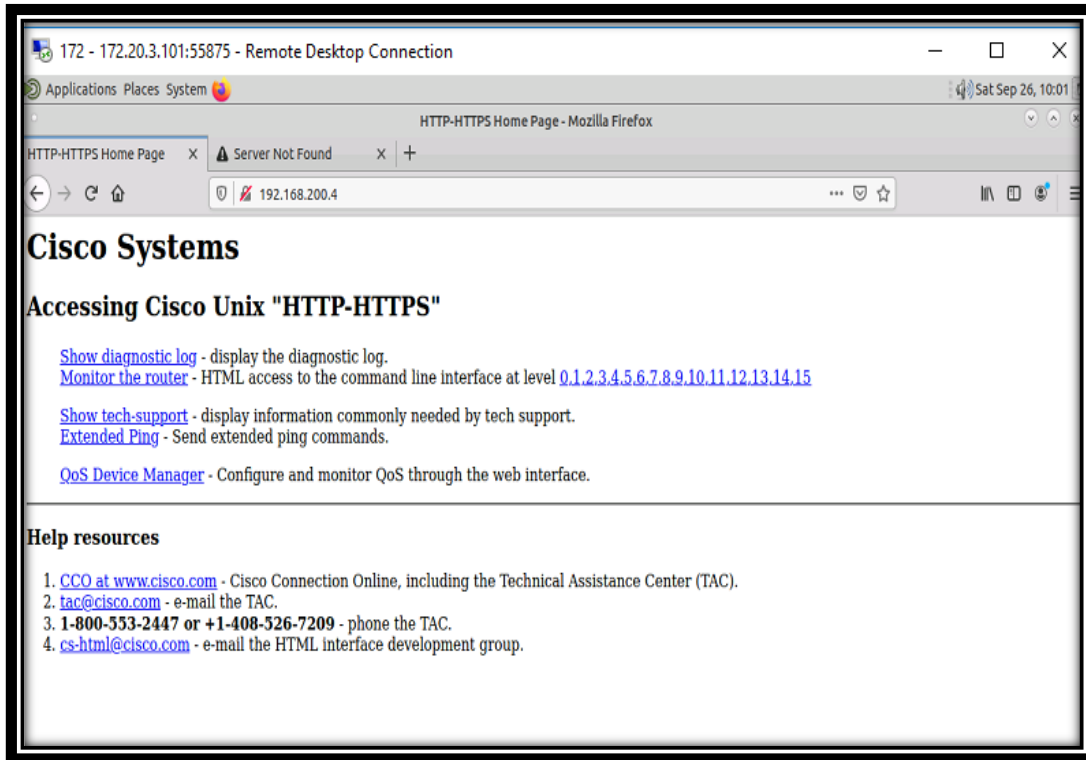
PartA

```
object network web-server  
host 10.10.30.254  
nat (inside,outside) static 192.168.200.4  
access-list out permit tcp any object web-server eq 80  
access-list out permit tcp any object web-server eq 443  
access-group out in interface outside
```

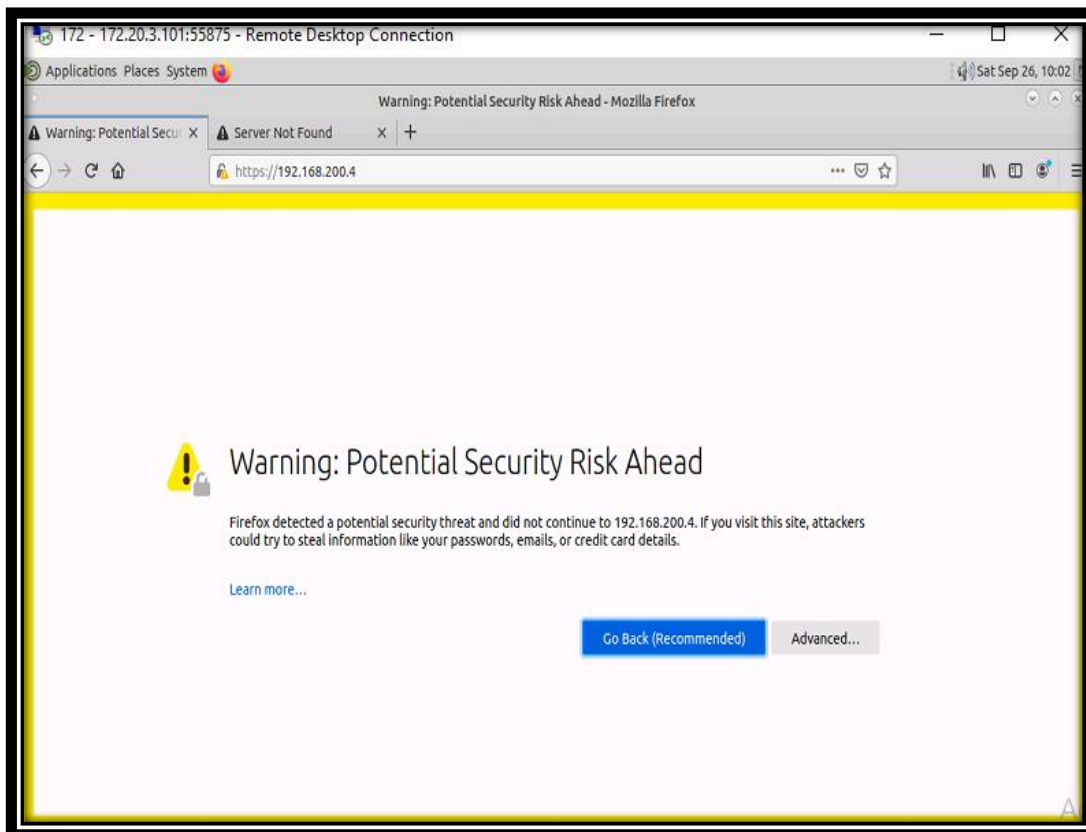
Verification from IT PC (New York)

For HTTP

CCIE Lab Center



For HTTPs



CCIE Lab Center

```
ASA3(config)# sh xlate
1 in use, 1 most used
Flags: D - DNS, e - extended, I - identity, i - dynamic, r - portmap,
      s - static, T - twice, N - net-to-net
NAT from inside:10.10.30.254 to outside:192.168.200.4
      flags s idle 0:01:27 timeout 0:00:00
ASA3(config)#
```

PartB 10.10.40.254

Configuration of ASA3

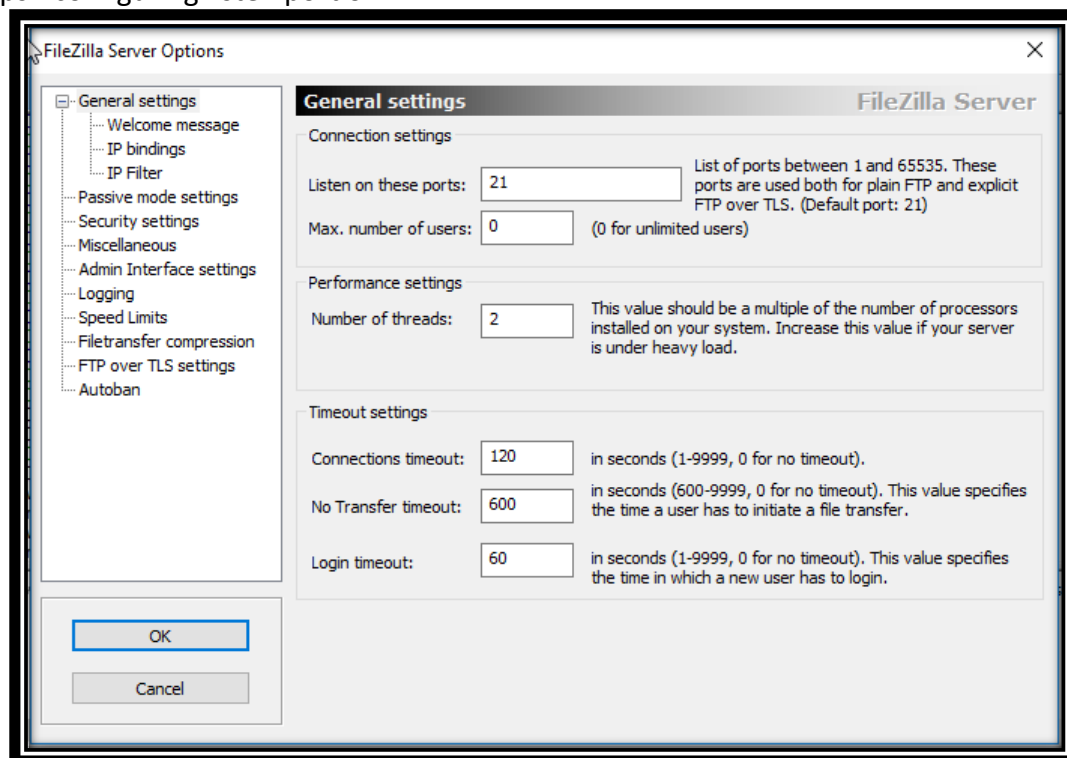
object network RDP
host 10.10.40.254

object network RDP
nat (inside,outside) static 192.168.200.5
access-list out extended permit tcp any object RDP eq 3389
access-list out extended permit tcp any object RDP range 20 21

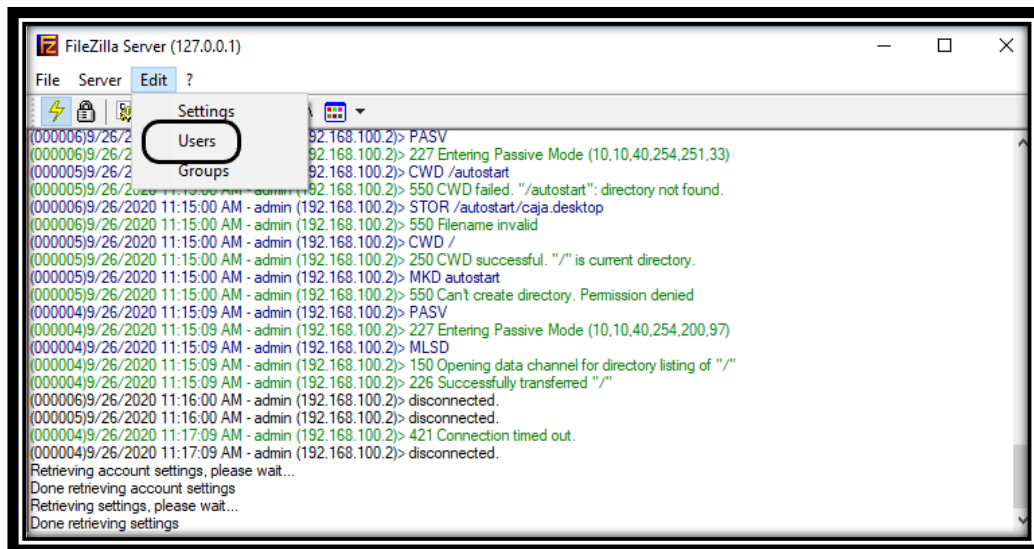
Configuration of RDP server

Steps1: Download filezilla server for windwos
<https://filezilla-project.org/download.php?type=server>

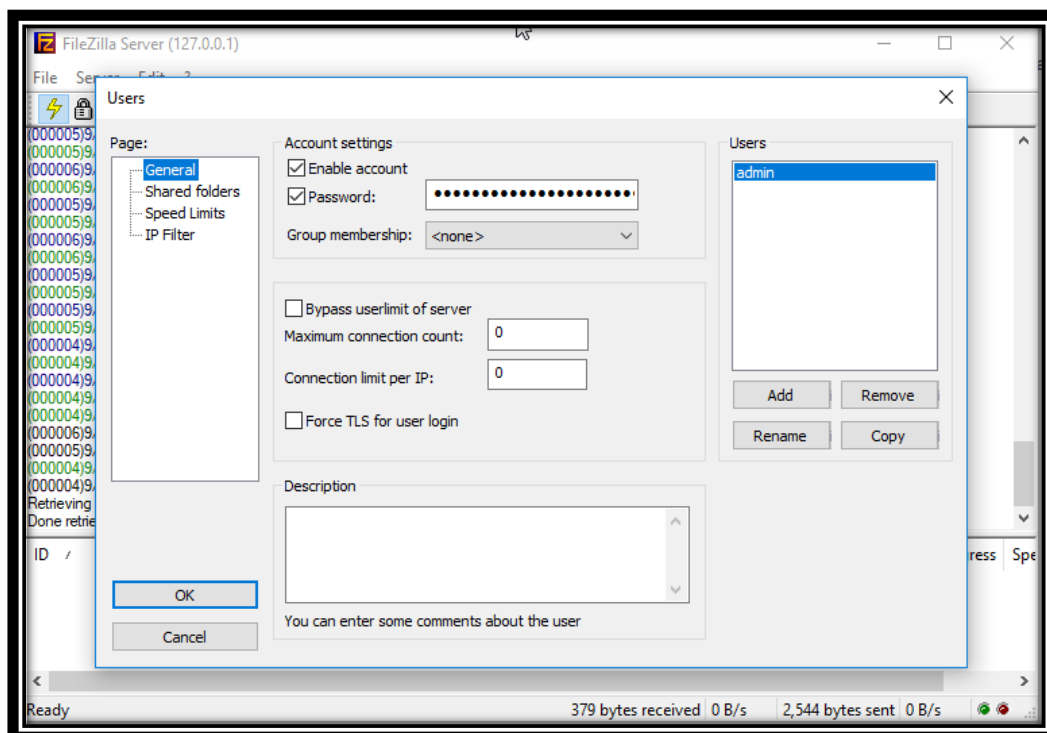
steps2:configuring listen port on 21



CCIE Lab Center

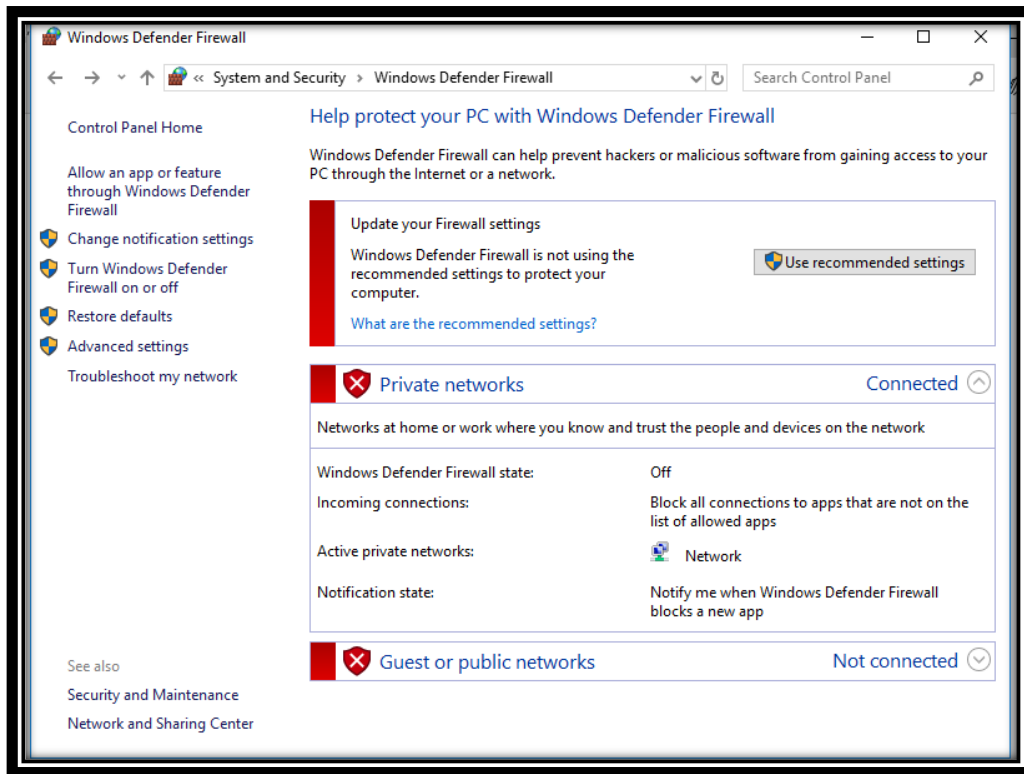


Steps: create user admin & password clc



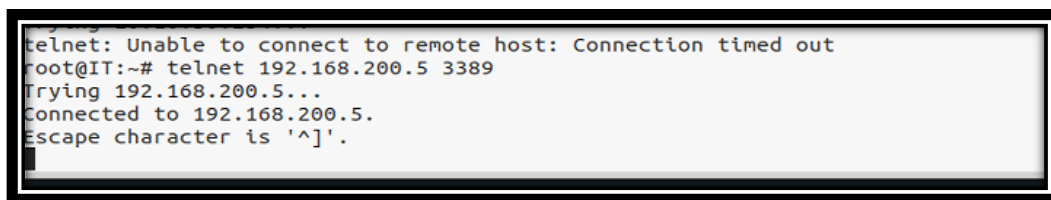
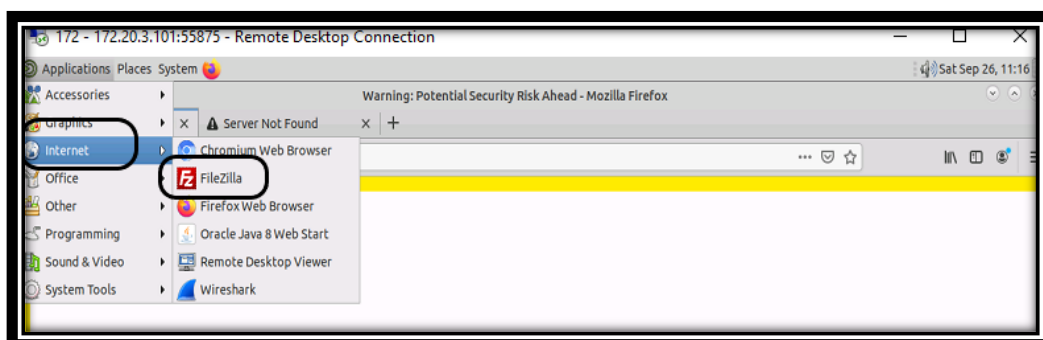
CCIE Lab Center

Steps 4:disable windows firewall

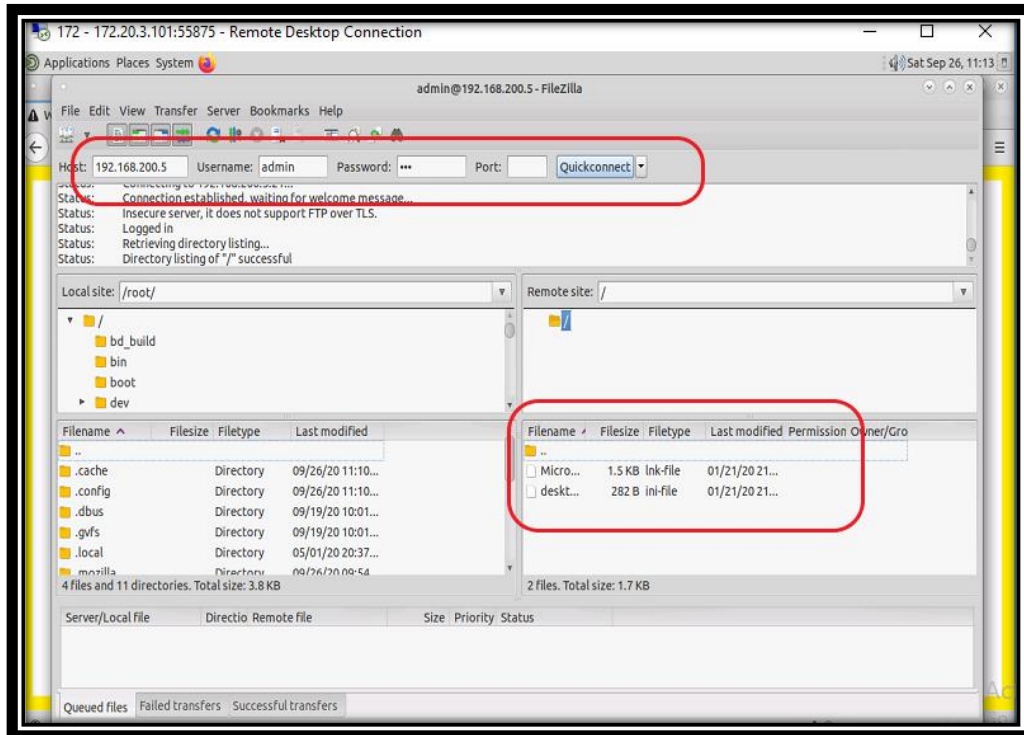
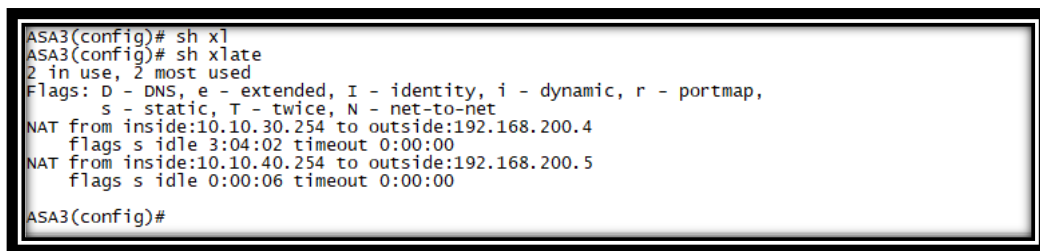


Verification

On IT system (New York)



CCIE Lab Center



CCIE Lab Center

3.7 :Configuring Internet access on 10.10.30.0/24 & 10.10.40.0/24 Network

Solution

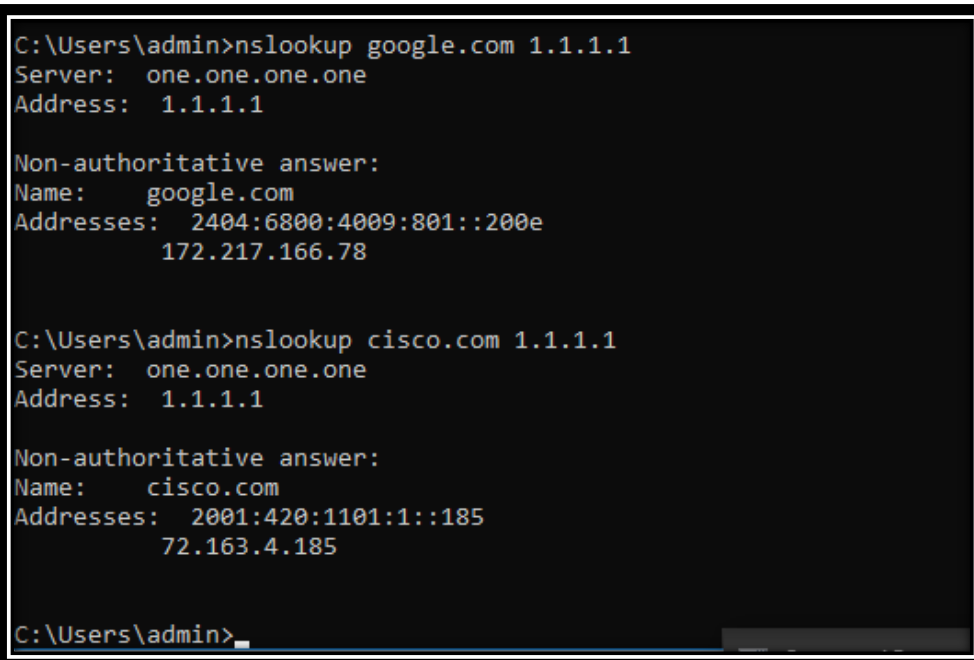
On ASA3

```
object network web
 subnet 10.10.30.0 255.255.255.0
 nat (inside,outside) dynamic interface
```

```
object network ftp
 subnet 10.10.40.0 255.255.255.0
 nat (inside,outside) dynamic interface
```

```
access-list out permit ip any object web
access-list out permit ip any object ftp
```

on Windows PC



```
C:\Users\admin>nslookup google.com 1.1.1.1
Server:  one.one.one.one
Address:  1.1.1.1

Non-authoritative answer:
Name:     google.com
Addresses: 2404:6800:4009:801::200e
          172.217.166.78

C:\Users\admin>nslookup cisco.com 1.1.1.1
Server:  one.one.one.one
Address:  1.1.1.1

Non-authoritative answer:
Name:     cisco.com
Addresses: 2001:420:1101:1::185
          72.163.4.185

C:\Users\admin>
```

CCIE Lab Center

4: Deployment of Virginia & New York

4.1 Configuring Internet access for 10.20.20.0/24 on R2 router

Solution

```

interface Ethernet0/0
description *** Connected to Internet ***
ip address 192.168.100.2 255.255.255.248
ip nat outside
ip virtual-reassembly in
!
interface Ethernet0/1
description *** Connected to SW11 ***
ip address 10.20.20.1 255.255.255.0
ip nat inside
ip virtual-reassembly in

ip nat inside source list NAT interface Ethernet0/0 overload
ip route 0.0.0.0 0.0.0.0 192.168.100.1
!
ip access-list extended NAT
permit ip 10.20.20.0 0.0.0.255 any

```

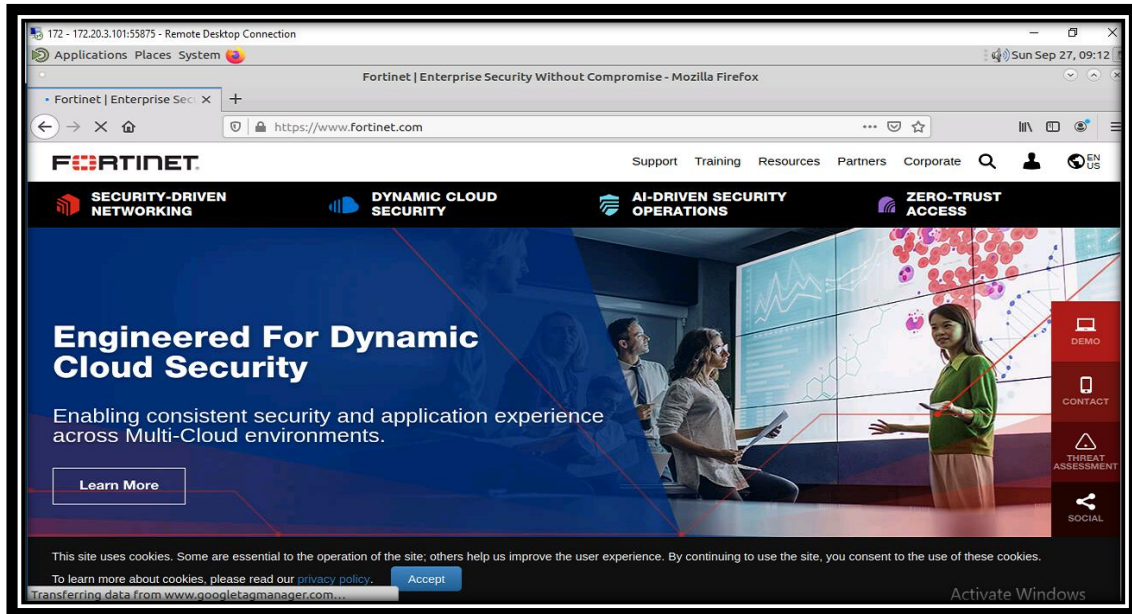
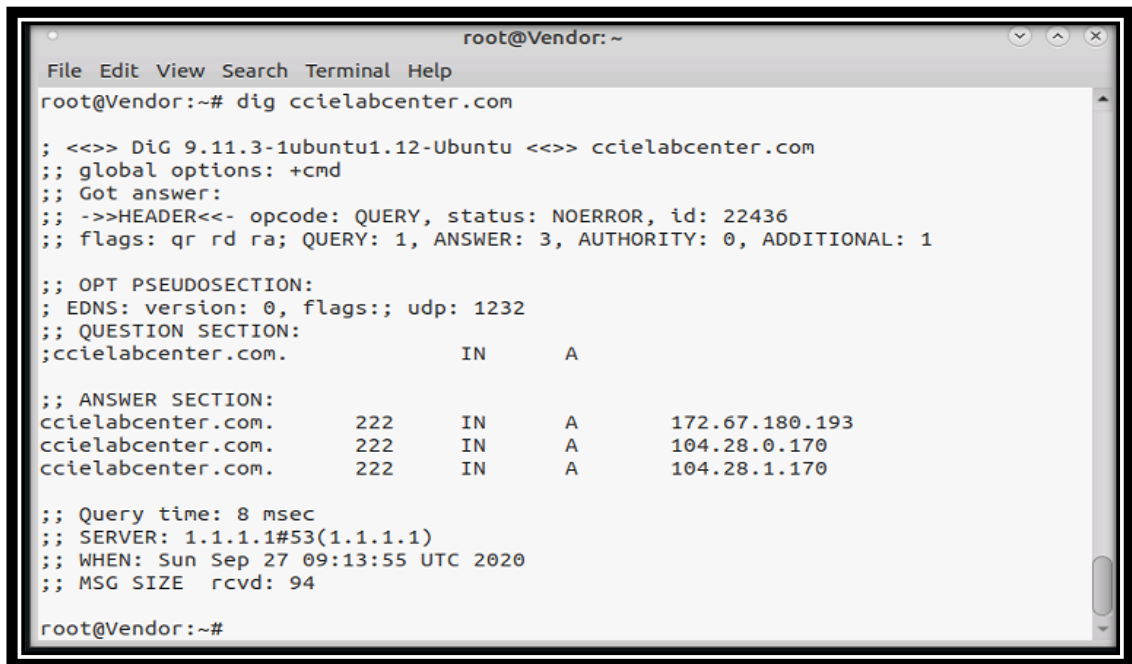
Output

```

R2#ping 1.1.1.1 source ethernet 0/1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 1.1.1.1, timeout is 2 seconds:
Packet sent with a source address of 10.20.20.1
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 3/3/4 ms
R2#ping 1.1.1.1 source ethernet 0/1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 1.1.1.1, timeout is 2 seconds:
Packet sent with a source address of 10.20.20.1
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 3/3/4 ms
R2#

```

CCIE Lab Center



CCIE Lab Center

4.2 : Configuring Internet access for 10.30.10.0/24 on R3 router

On R3

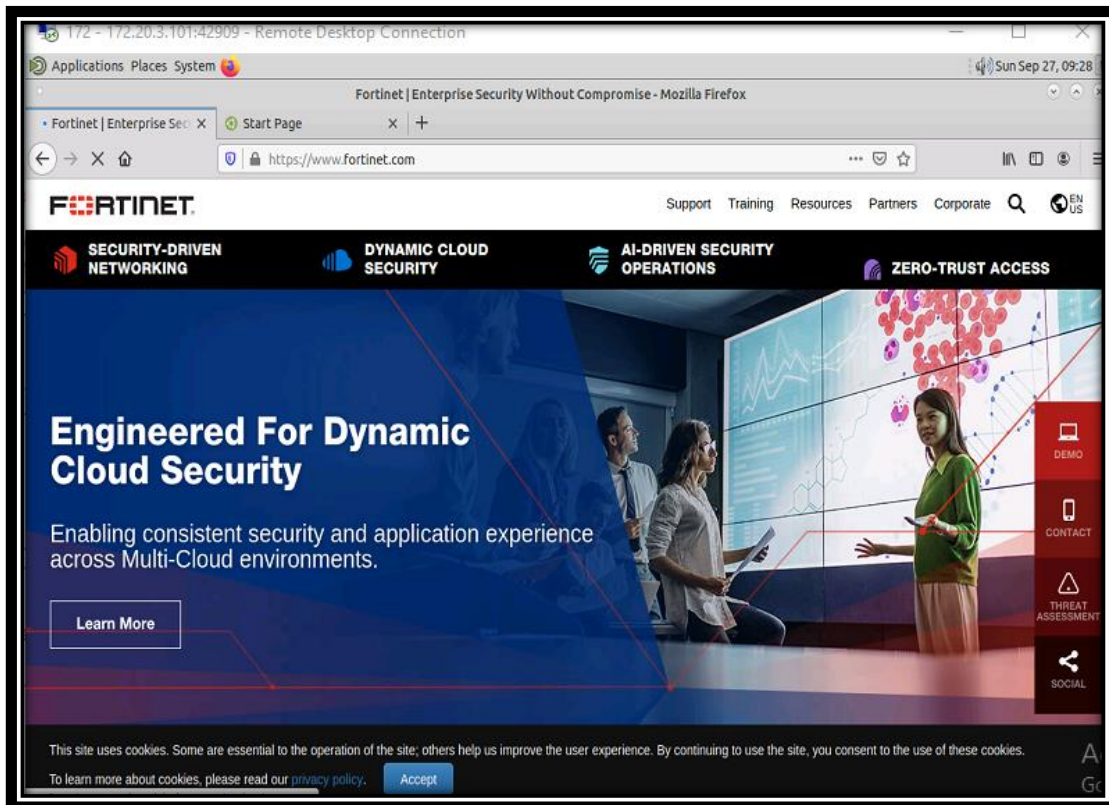
```
interface Ethernet0/1
description *** Connected to ISP2 ***
ip address 192.168.250.2 255.255.255.248
ip nat outside
ip virtual-reassembly in
duplex auto
!
interface Ethernet0/2
description *** Connected to SW14 ***
ip address 10.30.10.1 255.255.255.0
ip nat inside
ip virtual-reassembly in

ip nat inside source list NAT interface Ethernet0/1 overload

ip route 0.0.0.0 0.0.0.0 192.168.250.1
!
ip access-list extended NAT
permit ip 10.30.10.0 0.0.0.255 any
```

```
Success rate is 100 percent (5/5)
R3#ping 1.1.1.1 source ethernet 0/1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 1.1.1.1, timeout is 2 seconds:
Packet sent with a source address of 192.168.250.2
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 3/3/4 ms
R3#ping 1.1.1.1 source ethernet 0/1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 1.1.1.1, timeout is 2 seconds:
Packet sent with a source address of 192.168.250.2
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 3/3/4 ms
R3#
```

CCIE Lab Center



```

root@IT: ~
File Edit View Search Terminal Help
root@IT:~# dig ccielabcenter.com

; <<>> DiG 9.11.3-1ubuntu1.12-Ubuntu <<>> ccielabcenter.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 43004
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
;; QUESTION SECTION:
;ccielabcenter.com.                IN      A

;; ANSWER SECTION:
ccielabcenter.com.        300     IN      A      172.67.180.193
ccielabcenter.com.        300     IN      A      104.28.0.170
ccielabcenter.com.        300     IN      A      104.28.1.170

;; Query time: 9 msec
;; SERVER: 1.1.1.1#53(1.1.1.1)
;; WHEN: Sun Sep 27 09:29:33 UTC 2020
;; MSG SIZE rcvd: 94

root@IT:~#

```

CCIE Lab Center

4.3 : Configuring single Gateway IPSec VPN between R2 & R3 with internet access.

VPN Configuration on R2

```

crypto isakmp policy 5
  encr 3des
  hash md5
  authentication pre-share
  group 2
crypto isakmp key cisco123 address 192.168.250.2
!
!
crypto ipsec transform-set CLC esp-3des esp-md5-hmac
  mode tunnel
!
!
!
crypto map SITE 10 ipsec-isakmp
  set peer 192.168.250.2
  set transform-set CLC
  match address 101

interface Ethernet0/0
  description *** Connected to Internet ***
  ip address 192.168.100.2 255.255.255.248
  ip nat outside
  ip virtual-reassembly in
  crypto map SITE

ip nat inside source list NAT interface Ethernet0/0 overload
ip route 0.0.0.0 0.0.0.0 192.168.100.1
!
ip access-list extended NAT
  deny ip 10.20.20.0 0.0.0.255 10.30.10.0 0.0.0.255
  permit ip 10.20.20.0 0.0.0.255 any
!
!
!
access-list 101 permit ip 10.20.20.0 0.0.0.255 10.30.10.0 0.0.0.255

```

CCIE Lab Center

VPN Configuration on R3

```
crypto isakmp policy 5
  encr 3des
  hash md5
  authentication pre-share
  group 2
crypto isakmp key cisco123 address 192.168.100.2
!
!
crypto ipsec transform-set CLC esp-3des esp-md5-hmac
  mode tunnel
!
!
!
crypto map SITE 10 ipsec-isakmp
  set peer 192.168.100.2
  set transform-set CLC
  match address 101

interface Ethernet0/1
  description *** Connected to ISP2 ***
  ip address 192.168.250.2 255.255.255.248
  ip nat outside
  ip virtual-reassembly in
  duplex auto
  crypto map SITE

ip nat inside source list NAT interface Ethernet0/1 overload
ip route 0.0.0.0 0.0.0.0 192.168.250.1

ip access-list extended NAT
  deny ip 10.30.10.0 0.0.0.255 10.20.20.0 0.0.0.255
  permit ip 10.30.10.0 0.0.0.255 any

access-list 101 permit ip 10.30.10.0 0.0.0.255 10.20.20.0 0.0.0.255
```

CCIE Lab Center

Output on R3

```

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.20.20.1, timeout is 2 seconds:
Packet sent with a source address of 10.30.10.1
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 7/7/8 ms
R3#ping 10.20.20.1 source ethernet 0/2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.20.20.1, timeout is 2 seconds:
Packet sent with a source address of 10.30.10.1
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 6/6/7 ms
R3#ping 10.20.20.1 source ethernet 0/2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.20.20.1, timeout is 2 seconds:
Packet sent with a source address of 10.30.10.1
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 3/5/7 ms
R3#sh cr

```

```

R3#sh crypto ipsec sa
interface: Ethernet0/1
  Crypto map tag: SITE, local addr 192.168.250.2

protected vrf: (none)
local ident (addr/mask/prot/port): (10.30.10.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port): (10.20.20.0/255.255.255.0/0/0)
current peer 192.168.100.2 port 500
  PERMIT, flags={origin_is_acl,}
  #pkts encaps: 19, #pkts encrypt: 19, #pkts digest: 19
  #pkts decaps: 19, #pkts decrypt: 19, #pkts verify: 19
  #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.: 192.168.250.2, remote crypto endpt.: 192.168.100.2
  plaintext mtu 1446, path mtu 1500, ip mtu 1500, ip mtu idb Ethernet0/1
  current outbound spi: 0x6B85E186(1803936134)
  PFS (Y/N): N, DH group: none

inbound esp sas:
  spi: 0xD5BE1391(3586003857)
    transform: esp-3des esp-md5-hmac ,
    in use settings ={Tunnel,}
    conn id: 59, flow_id: SW:59, sibling_flags 80004040, crypto map: SITE
    sa timing: remaining key lifetime (k/sec): (4229742/3554)
    IV size: 8 bytes
    replay detection support: Y
    Status: ACTIVE(ACTIVE)

```

```

R3#ping 10.20.20.1 source ethernet 0/2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.20.20.1, timeout is 2 seconds:
Packet sent with a source address of 10.30.10.1
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 6/6/7 ms
R3#sh crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst          src          state          conn-id status
192.168.100.2 192.168.250.2 QM_IDLE        1005 ACTIVE

IPv6 Crypto ISAKMP SA
R3#

```

CCIE Lab Center

```
R3#ping 10.20.20.1 source ethernet 0/2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.20.20.1, timeout is 2 seconds:
Packet sent with a source address of 10.30.10.1
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 6/6/8 ms
R3#sh crypto session
Crypto session current status

Interface: Ethernet1/0
Session status: DOWN
Peer: 192.168.100.2 port 500
IPSEC FLOW: permit ip 10.30.10.0/255.255.255.0 10.20.20.0/255.255.255.0
Active SAs: 0, origin: crypto map

Interface: Ethernet0/1
Session status: UP-ACTIVE
Peer: 192.168.100.2 port 500
Session ID: 0
IKEv1 SA: local 192.168.250.2/500 remote 192.168.100.2/500 Active
IPSEC FLOW: permit ip 10.30.10.0/255.255.255.0 10.20.20.0/255.255.255.0
Active SAs: 2, origin: crypto map

R3#
```

From IT system

```
root@IT:~# ping 10.20.20.254
PING 10.20.20.254 (10.20.20.254) 56(84) bytes of data:
64 bytes from 10.20.20.254: icmp_seq=1 ttl=62 time=5.02 ms
64 bytes from 10.20.20.254: icmp_seq=2 ttl=62 time=6.11 ms
64 bytes from 10.20.20.254: icmp_seq=3 ttl=62 time=21.0 ms
64 bytes from 10.20.20.254: icmp_seq=4 ttl=62 time=6.17 ms
64 bytes from 10.20.20.254: icmp_seq=5 ttl=62 time=5.10 ms
^C
--- 10.20.20.254 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4004ms
rtt min/avg/max/mdev = 5.027/8.700/21.087/6.212 ms
root@IT:~# traceroute 10.20.20.254
traceroute to 10.20.20.254 (10.20.20.254), 30 hops max, 60 byte packets
 1 10.30.10.1 (10.30.10.1) 1.660 ms 1.558 ms 8.180 ms
 2 * * *
 3 10.20.20.254 (10.20.20.254) 8.369 ms 8.373 ms 8.499 ms
root@IT:~#
```

CCIE Lab Center

```

root@IT:~# ping 1.1.1.1
PING 1.1.1.1 (1.1.1.1) 56(84) bytes of data.
64 bytes from 1.1.1.1: icmp_seq=1 ttl=56 time=4.54 ms
64 bytes from 1.1.1.1: icmp_seq=2 ttl=56 time=4.99 ms
64 bytes from 1.1.1.1: icmp_seq=3 ttl=56 time=4.57 ms
64 bytes from 1.1.1.1: icmp_seq=4 ttl=56 time=4.45 ms
64 bytes from 1.1.1.1: icmp_seq=5 ttl=56 time=5.03 ms
64 bytes from 1.1.1.1: icmp_seq=6 ttl=56 time=5.30 ms
^C
--- 1.1.1.1 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5005ms
rtt min/avg/max/mdev = 4.454/4.817/5.305/0.318 ms
root@IT:~# dig ccielabcenter.com

; <<>> DiG 9.11.3-1ubuntu1.12-Ubuntu <<>> ccielabcenter.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 674
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
;; QUESTION SECTION:
;ccielabcenter.com.                IN      A

;; ANSWER SECTION:
ccielabcenter.com.      300     IN      A      104.28.0.170
ccielabcenter.com.      300     IN      A      104.28.1.170
ccielabcenter.com.      300     IN      A      172.67.180.193

```

CCIE Lab Center

4.4 : Configuring Dual Gateway IPsec VPN between R2 & R3 with internet access.

On R2

```

crypto isakmp policy 5
  encr 3des
  hash md5
  authentication pre-share
  group 2
crypto isakmp key cisco123 address 192.168.250.2
crypto isakmp key cisco123 address 192.168.150.2
!
!
crypto ipsec transform-set CLC esp-3des esp-md5-hmac
  mode tunnel
!
!
!
crypto map SITE 10 ipsec-isakmp
  set peer 192.168.250.2
  set peer 192.168.150.2
  set transform-set CLC
  match address 101

interface Ethernet0/0
  description *** Connected to Internet ***
  ip address 192.168.100.2 255.255.255.248
  ip nat outside
  ip virtual-reassembly in
  crypto map SITE

ip nat inside source list NAT interface Ethernet0/0 overload
ip route 0.0.0.0 0.0.0.0 192.168.100.1
!
ip access-list extended NAT
  deny ip 10.20.20.0 0.0.0.255 10.30.10.0 0.0.0.255
  permit ip 10.20.20.0 0.0.0.255 any
!
!
access-list 101 permit ip 10.20.20.0 0.0.0.255 10.30.10.0 0.0.0.255

```

CCIE Lab Center

On R3

Configuring Dual Internet connection

```

interface Ethernet0/1
description *** Connected to ISP1 ***
ip address 192.168.250.2 255.255.255.248
ip nat outside
ip virtual-reassembly in
duplex auto
crypto map SITE
!
interface Ethernet0/2
description *** Connected to SW14 ***
ip address 10.30.10.1 255.255.255.0
ip nat inside
ip virtual-reassembly in
ip policy route-map PBR
duplex auto

track 10 ip sla 1 reachability
delay down 2 up 2
!
track 20 ip sla 2 reachability
delay down 2 up 2
!
interface Ethernet1/3
ip address 192.168.150.2 255.255.255.248
description *** Connected to ISP2 ***
ip nat outside
ip virtual-reassembly in
duplex auto

ip nat inside source route-map ISP1 interface Ethernet0/1 overload
ip nat inside source route-map ISP2 interface Ethernet1/3 overload
ip route 0.0.0.0 0.0.0.0 192.168.250.1 name ISP1 track 10
ip route 0.0.0.0 0.0.0.0 192.168.150.1 name ISP2 track 20
!
ip access-list extended NAT
deny ip 10.30.10.0 0.0.0.255 10.20.20.0 0.0.0.255

```

CCIE Lab Center

```

permit ip 10.30.10.0 0.0.0.255 any
!
ip sla 1
icmp-echo 192.168.250.1
frequency 5
ip sla schedule 1 life forever start-time now
ip sla 2
icmp-echo 192.168.150.1
frequency 5
ip sla schedule 2 life forever start-time now
ipv6 ioam timestamp
!
route-map PBR permit 10
match ip address 130
set ip next-hop verify-availability 192.168.250.1 1 track 10
set ip next-hop verify-availability 192.168.150.1 2 track 20
!
route-map ISP2 permit 10
match ip address NAT
match interface Ethernet1/3
!
route-map ISP1 permit 10
match ip address NAT
match interface Ethernet0/1
!
!
access-list 130 permit ip any any

```

for Dual VPN gateway

```

interface Ethernet1/3
ip address 192.168.150.2 255.255.255.248
description *** Connected to ISP2 ***
crypto map SITE
ip nat outside
ip virtual-reassembly in
duplex auto

```

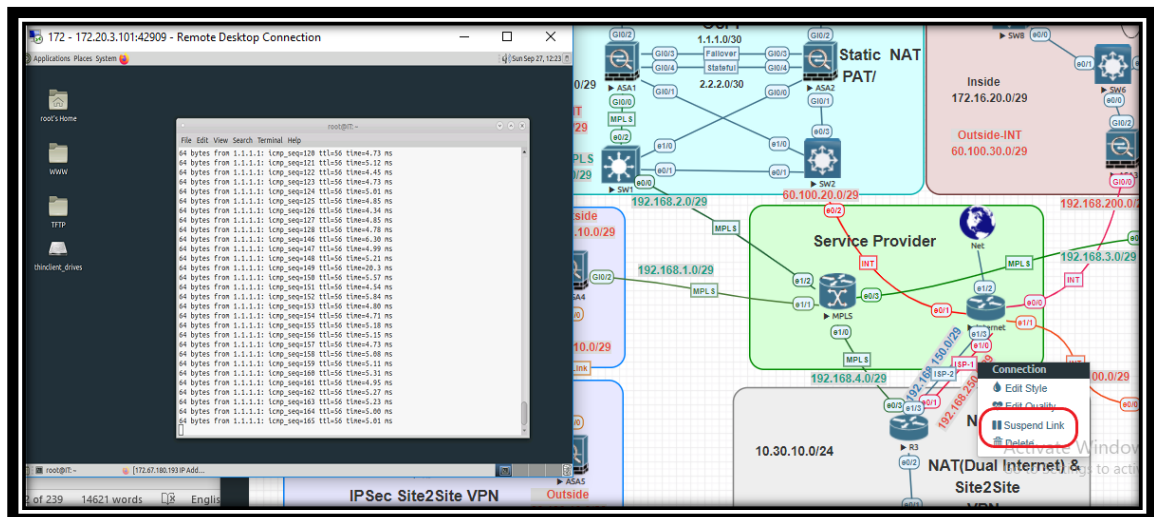
CCIE Lab Center

Internet verification

```
R3#ping 1.1.1.1 source ethernet 0/1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 1.1.1.1, timeout is 2 seconds:
Packet sent with a source address of 192.168.250.2
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 3/3/4 ms
R3#ping 1.1.1.1 source ethernet 1/3
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 1.1.1.1, timeout is 2 seconds:
Packet sent with a source address of 192.168.150.2
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 3/3/4 ms
R3#
```

Case1

Shutdown PRI ISP

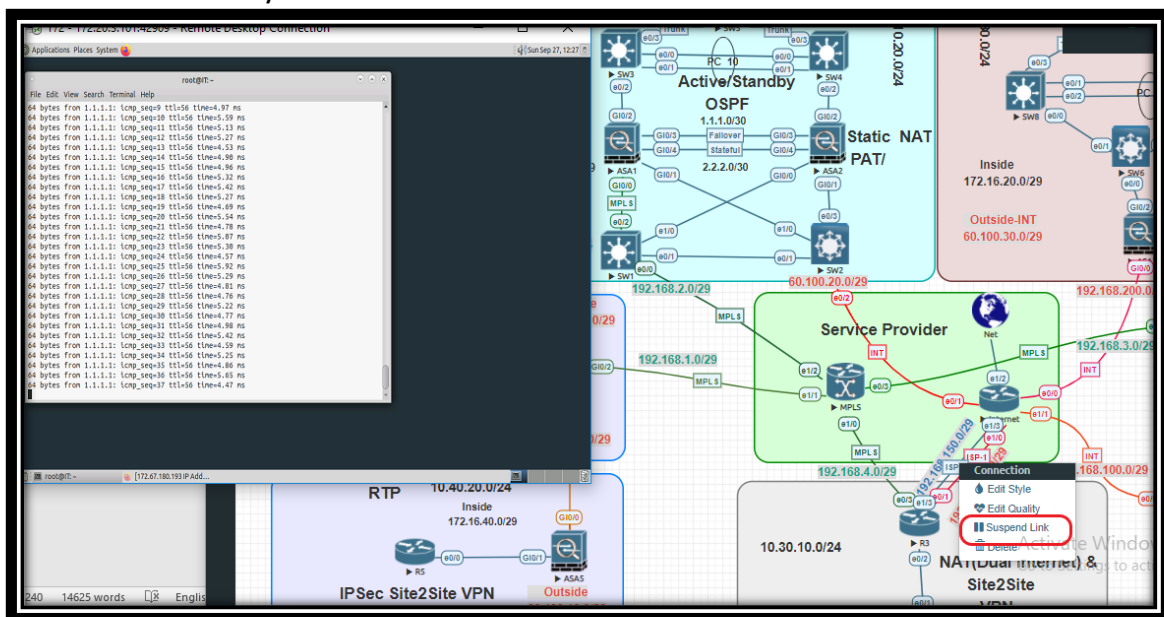


Going from Secondary ISP

```
root@IT:~# traceroute 1.1.1.1
traceroute to 1.1.1.1 (1.1.1.1), 30 hops max, 60 byte packets
 1 10.30.10.1 (10.30.10.1) 3.210 ms 3.224 ms 3.476 ms
 2 192.168.150.1 (192.168.150.1) 2.530 ms 2.870 ms 2.929 ms
 3 172.29.129.234 (172.29.129.234) 3.550 ms 3.655 ms 4.483 ms
 4 172.20.2.1 (172.20.2.1) 4.884 ms 5.613 ms 5.614 ms
```

Case 2

Shutdown Secondary Link



Study Group: <https://t.me/cciestudygroup>

CCIE Lab Center

```

R3#sh ip sla su
R3#sh ip sla summary
IPSLAS Latest Operation Summary
Codes: * active, ^ inactive, ~ pending

ID      Type      Destination      Stats      Return      Last
-----  ---      -
*1      icmp-echo  192.168.250.1    RTT=2      OK          1 second ago

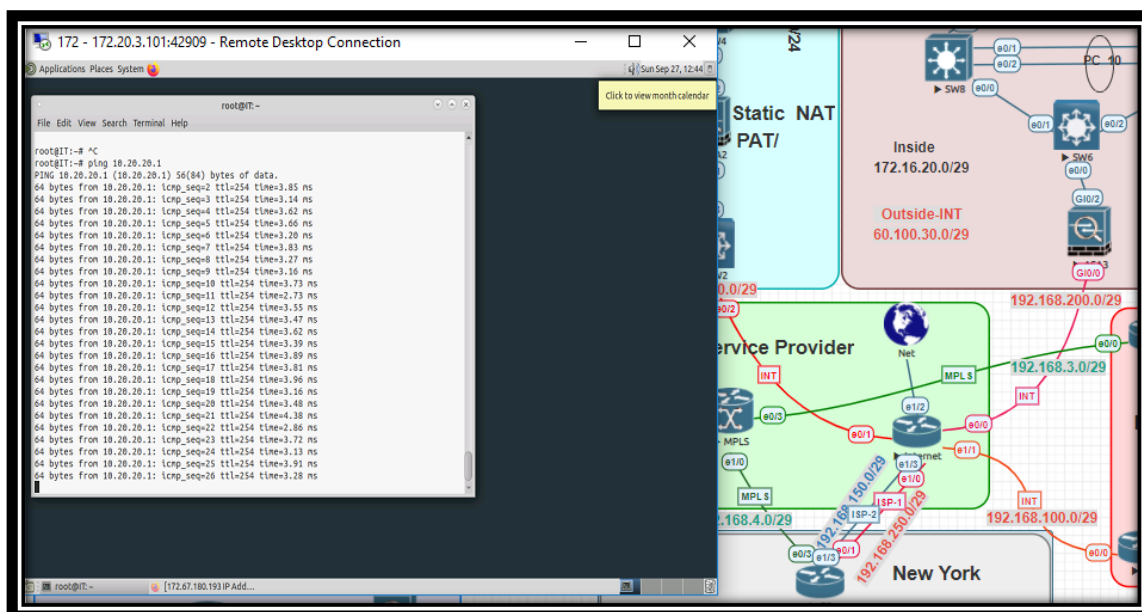
*2      icmp-echo  192.168.150.1    -          Timeout     6 seconds ago

R3#sh ip route
R3#sh ip route 0.0.0.0
Routing entry for 0.0.0.0/0, supernet
Known via "static", distance 0, candidate default path
Routing Descriptor Blocks:
* 192.168.250.1
  Route metric is 0, traffic share count is 1
R3#sh ro
R3#sh route-m
R3#sh route-map PBR
route-map PBR, permit, sequence 10
Match clauses:
  ip address (access-lists): 130
Set clauses:
  ip next-hop verify-availability 192.168.250.1 1 track 10 [up]
  ip next-hop verify-availability 192.168.150.1 2 track 20 [down]
Policy routing matches: 1859 packets, 184229 bytes
R3#

```

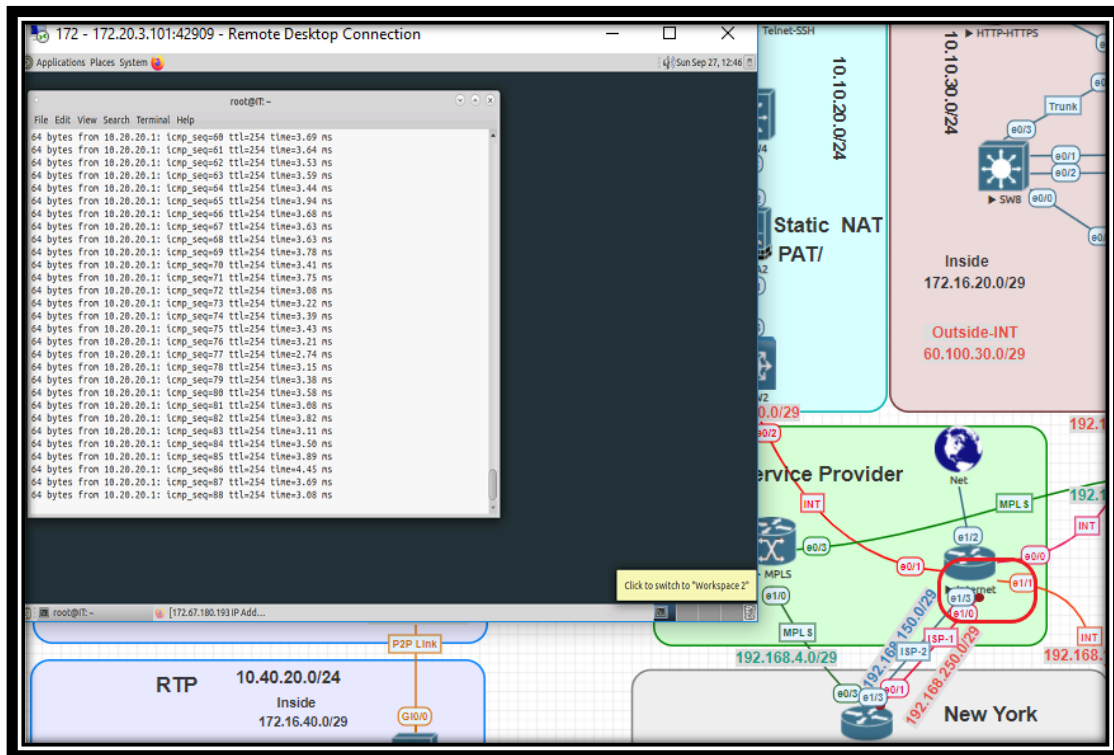
Dual IPsec Verification,

Case1 when both ISP's are up



Case2 when both ISP1 is down

CCIE Lab Center



R3#clear crypto session

Start ping from IT system 10.20.20.1

```

R3#sh crypto session
Crypto session current status

Interface: Ethernet0/1
Session status: DOWN-NEGOTIATING
Peer: 192.168.100.2 port 500
  Session ID: 0
  IKEv1 SA: local 192.168.250.2/500 remote 192.168.100.2/500 Inactive
  IPSEC FLOW: permit ip 10.30.10.0/255.255.255.0 10.20.20.0/255.255.255.0
  Active SAs: 0, origin: crypto map

Interface: Ethernet1/3
Session status: UP-ACTIVE
Peer: 192.168.100.2 port 500
  Session ID: 0
  IKEv1 SA: local 192.168.150.2/500 remote 192.168.100.2/500 Active
  Session ID: 0
  IKEv1 SA: local 192.168.150.2/500 remote 192.168.100.2/500 Inactive
  IPSEC FLOW: permit ip 10.30.10.0/255.255.255.0 10.20.20.0/255.255.255.0
  Active SAs: 2, origin: crypto map

R3#

```

CCIE Lab Center

```

R3#sh crypto ipsec sa
interface: Ethernet0/1
  Crypto map tag: SITE, local addr 192.168.250.2

protected vrf: (none)
local ident (addr/mask/prot/port): (10.30.10.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port): (10.20.20.0/255.255.255.0/0/0)
current_peer 192.168.100.2 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

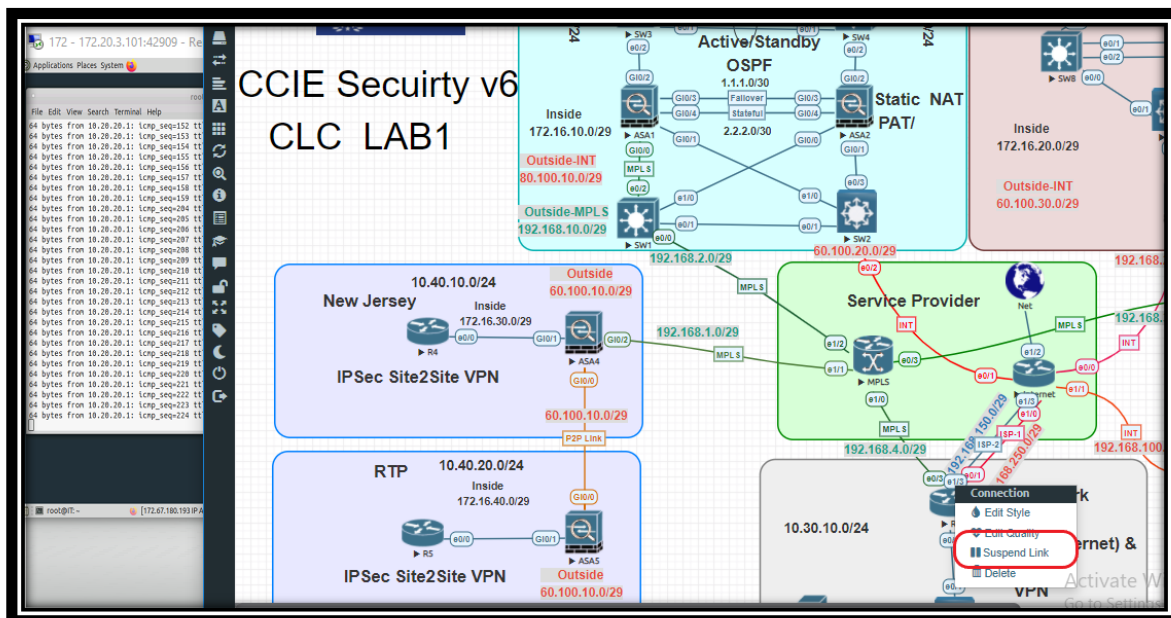
local crypto endpt.: 192.168.250.2, remote crypto endpt.: 192.168.100.2
plaintext mtu 1446, path mtu 1500, ip mtu 1500, ip mtu idb Ethernet0/1
current outbound spi: 0x0(0)
PFS (Y/N): N, DH group: none

inbound esp sas:
inbound ah sas:
inbound pcp sas:
outbound esp sas:
outbound ah sas:
outbound pcp sas:

interface: Ethernet1/3
  Crypto map tag: SITE, local addr 192.168.150.2

protected vrf: (none)
local ident (addr/mask/prot/port): (10.30.10.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port): (10.20.20.0/255.255.255.0/0/0)
current_peer 192.168.100.2 port 500
  PERMIT, flags={origin_is_acl,}
    #pkts encaps: 79, #pkts encrypt: 79, #pkts digest: 79
    #pkts decaps: 79, #pkts decrypt: 79, #pkts verify: 79
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
  
```

Case3 when both ISP2 is down



R3#clear crypto session

Start ping from IT system 10.20.20.1

CCIE Lab Center

```
R3#sh crypto session
Crypto session current status

Interface: Ethernet0/1
Session status: UP-ACTIVE
Peer: 192.168.100.2 port 500
Session ID: 0
IKEv1 SA: local 192.168.250.2/500 remote 192.168.100.2/500 Active
IPSEC FLOW: permit ip 10.30.10.0/255.255.255.0 10.20.20.0/255.255.255.0
Active SAS: 2, origin: crypto map

Interface: Ethernet1/3
Session status: UP-IDLE
Peer: 192.168.100.2 port 500
Session ID: 0
IKEv1 SA: local 192.168.150.2/500 remote 192.168.100.2/500 Active
IPSEC FLOW: permit ip 10.30.10.0/255.255.255.0 10.20.20.0/255.255.255.0
Active SAS: 0, origin: crypto map
```

```
R3#sh crypto ipsec sa
R3#sh crypto ipsec sa

interface: Ethernet0/1
Crypto map tag: SITE, local addr 192.168.250.2

protected vrf: (none)
local ident (addr/mask/prot/port): (10.30.10.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port): (10.20.20.0/255.255.255.0/0/0)
current peer 192.168.100.2 port 500
PERMIT, flags={origin_is_acl,}
#pkts encaps: 121, #pkts encrypt: 121, #pkts digest: 121
#pkts decaps: 121, #pkts decrypt: 121, #pkts verify: 121
#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.: 192.168.250.2, remote crypto endpt.: 192.168.100.2
plaintext mtu 1446, path mtu 1500, ip mtu 1500, ip mtu idb Ethernet0/1
current outbound spi: 0xF532AF45(4113739589)
PFS (Y/N): N, DH group: none

inbound esp sas:
spi: 0x50EFD2F(1357896751)
transform: esp-3des esp-md5-hmac ,
in use settings ={Tunnel,}
conn id: 7, flow_id: Sw:7, sibling_flags 80004040, crypto map: SITE
```

CCIE Lab Center

5: Deployment of Virginia & New york

5.1 Configuring IPSec VPN between ASA4 & 5

On ASA4

```
interface GigabitEthernet0/0
 nameif outside
 security-level 0
 ip address 60.100.10.2 255.255.255.248
!
interface GigabitEthernet0/1
 nameif inside
 security-level 100
 ip address 172.16.30.1 255.255.255.248
!
interface GigabitEthernet0/2
 nameif mpls
 security-level 0
 ip address 192.168.1.2 255.255.255.248

router ospf 10
 network 192.168.1.0 255.255.255.248 area 0
 log-adj-changes
 redistribute connected subnets
 route outside 0.0.0.0 0.0.0.0 60.100.10.1 1
 route inside 10.40.10.0 255.255.255.0 172.16.30.2 1
```

VPN Configuration

```
crypto ikev1 enable outside
crypto ikev1 policy 2
 authentication pre-share
 encryption 3des
 hash sha
 group 2
 lifetime 86400
```

```
access-list 1 extended permit ip 10.40.10.0 255.255.255.0 10.40.20.0 255.255.255.0
```

CCIE Lab Center

```
crypto ipsec ikev1 transform-set ipsec-vpn esp-aes esp-sha-hmac
crypto map site-a 10 match address 1
crypto map site-a 10 set pfs
crypto map site-a 10 set peer 60.100.10.1
crypto map site-a 10 set ikev1 transform-set ipsec-vpn
crypto map site-a interface outside
```

```
tunnel-group 60.100.10.1 type ipsec-l2l
tunnel-group 60.100.10.1 ipsec-attributes
ikev1 pre-shared-key cisco123
```

on ASA5

```
interface GigabitEthernet0/0
 nameif outside
 security-level 0
 ip address 60.100.10.1 255.255.255.248
 no shutdown
!
interface GigabitEthernet0/1
 nameif inside
 security-level 100
 ip address 172.16.40.1 255.255.255.248
 no shutdown
```

```
route outside 0.0.0.0 0.0.0.0 60.100.10.2 1
route inside 10.40.20.0 255.255.255.0 172.16.40.2 1
```

VPN configuration

```
access-list 1 extended permit ip 10.40.20.0 255.255.255.0 10.40.10.0 255.255.255.0
```

```
crypto ikev1 enable outside
crypto ikev1 policy 2
 authentication pre-share
 encryption 3des
 hash sha
 group 2
 lifetime 86400
```

CCIE Lab Center

```
crypto ipsec ikev1 transform-set ipsec-vpn esp-aes esp-sha-hmac
crypto map site-b 10 match address 1
crypto map site-b 10 set pfs
crypto map site-b 10 set peer 60.100.10.2
crypto map site-b 10 set ikev1 transform-set ipsec-vpn
crypto map site-b interface outside
```

```
tunnel-group 60.100.10.2 type ipsec-l2l
tunnel-group 60.100.10.2 ipsec-attributes
ikev1 pre-shared-key cisco123
```

Verification on R4

```
Loopback10 10.40.10.1 YES manual up
R4#ping 10.40.20.1 so
R4#ping 10.40.20.1 source loo
R4#ping 10.40.20.1 source loopback 10
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.40.20.1, timeout is 2 seconds:
Packet sent with a source address of 10.40.10.1
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 9/13/22 ms
R4#ping 10.40.20.1 source loopback 10
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.40.20.1, timeout is 2 seconds:
Packet sent with a source address of 10.40.10.1
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 7/9/12 ms
R4#
```

Verification on ASA4

CCIE Lab Center

```

ASA4(config)# sh crypto ipsec sa
ASA4(config)# sh crypto ipsec sa
interface: outside
Crypto map tag: site-a, seq num: 10, local addr: 60.100.10.2

access-list 1 extended permit ip 10.40.10.0 255.255.255.0 10.40.20.0 255.255.255.0
local ident (addr/mask/prot/port): (10.40.10.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port): (10.40.20.0/255.255.255.0/0/0)
current_peer: 60.100.10.1

#pkts encaps: 1106, #pkts encrypt: 1106, #pkts digest: 1106
#pkts decaps: 1103, #pkts decrypt: 1103, #pkts verify: 1103
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 1106, #pkts comp failed: 0, #pkts decomp failed: 0
#pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
#PMTUS sent: 0, #PMTUS rcvd: 0, #decapsulated frgs needing reassembly: 0
#TFC rcvd: 0, #TFC sent: 0
#Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0
#send errors: 0, #recv errors: 0

local crypto endpt.: 60.100.10.2/0, remote crypto endpt.: 60.100.10.1/0
path mtu 1500, ipsec overhead 74(44), media mtu 1500
PMTU time remaining (sec): 0, DF policy: copy-df
ICMP error validation: disabled, TFC packets: disabled
current outbound spi: C8FE9D56
current inbound spi : 8EC033E3

```

```

stats          show ikev1 statistics
ASA4(config)# sh crypto ikev1 sa

IKEV1 SAs:

  Active SA: 1
  Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey)
Total IKE SA: 1

1  IKE Peer: 60.100.10.1
   Type    : L2L           Role    : initiator
   Rekey   : no           State   : MM_ACTIVE
ASA4(config)# sh cr
ASA4(config)# sh cry
ASA4(config)# sh crypto ?

```

CCIE Lab Center

100% Real | 100% Pass
Visit ccielabcenter.com