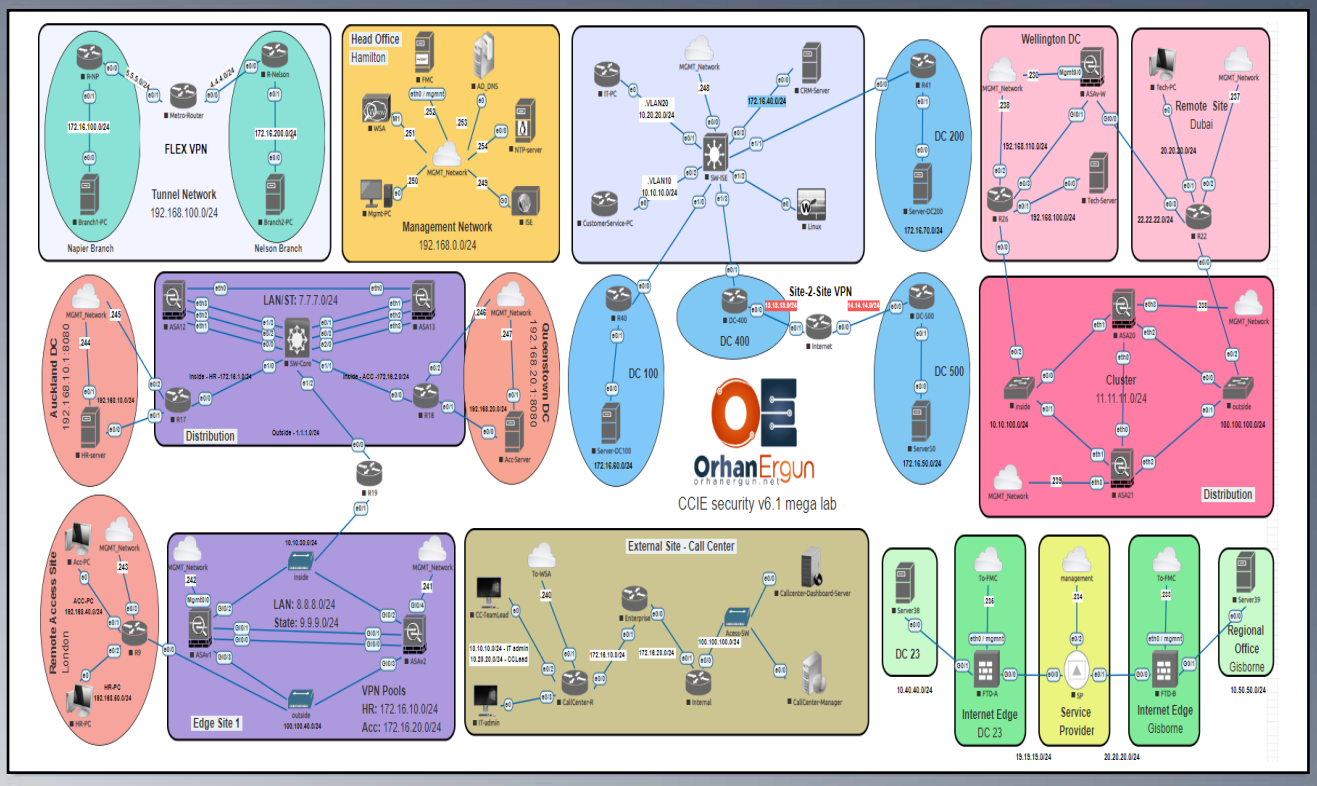
2024

CCIE Security V6.1 Mega LAB WorkBook

Orhan Ergun LLC



OrhanErgun
orhanergun.net

Lab 1: Configure Active/Passive relationship between ASAv1 and ASAv2

Lab 2: Configure Active/Active relationship between ASA12 and ASA13

Lab 3: Configure Clustering relationship between ASA20 and ASA21

Lab 4: Configure AnyConnect VPN on London Site with requirements as below

Lab 5: Configure Clientless SSL VPN for Dubai Remote-Site on ASAv-W

Lab 6: Configure Site-2-Site IKEv1 VPN between DC23 and Gisborne edges.

Lab 7: Configure Flex VPN between Napier & Nelson branch

Lab 8: Configure Site-2-Site VPN between DC400 & DC500 branch

Lab 9: Configure Dot1x and Mab for Customer service-PC & IT-PC

Lab 10: Configure NTP server on your NTP router

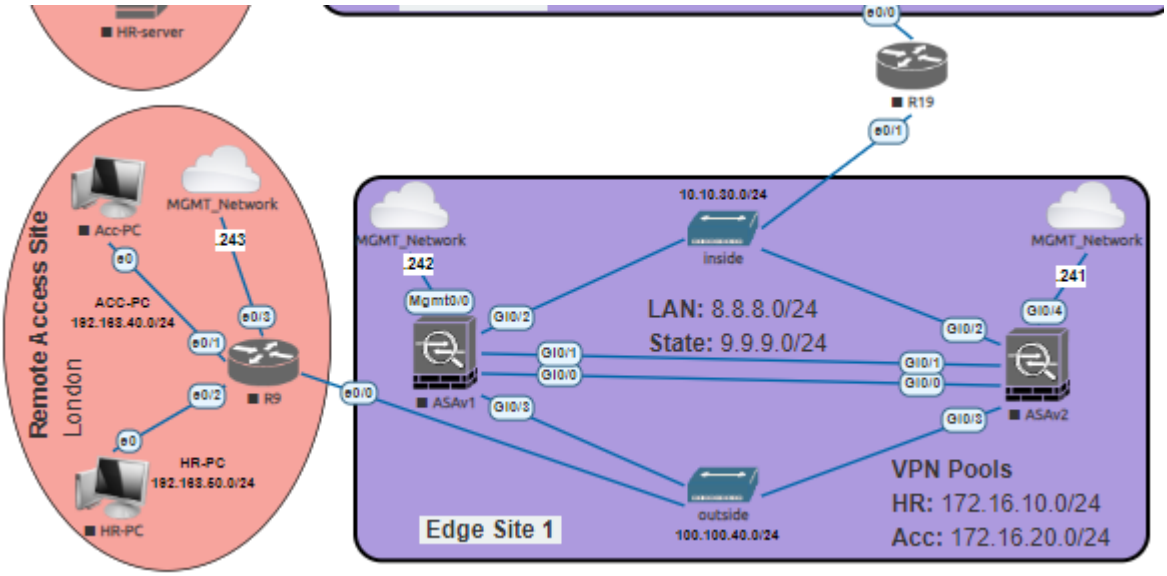
Lab 11: Configure SYSLOG on R9

Lab 12: Configure WSA redirection on Call center router

Lab 13: Optimization/Troubleshooting

Lab 1: Configure Active/Passive relationship between ASAv1 and ASAv2

- must be named “inside”, “outside”, and “mgmt”.
- Follow the IP addressing as per the diagram
- Ensure Fail and state interfaces are names as LAN and state
- Use .1 (first IP of octet) to assign addresses to the FWs



We will start with Configuring R9 & R19 First

R9:

```
interface Ethernet0/0
 no shutdown
 ip address 100.100.40.254 255.255.255.0
 duplex auto
!
interface Ethernet0/1
 no shutdown
 ip address 192.168.40.254 255.255.255.0
 duplex auto
!
interface Ethernet0/2
 no shutdown
 ip address 192.168.50.254 255.255.255.0
 duplex auto
!
interface Ethernet0/3
 no shutdown
 ip address 192.168.0.243 255.255.255.0
 duplex auto
ip route 0.0.0.0 0.0.0.0 100.100.40.1
```

R19:

```
interface Ethernet0/0
 no shutdown
 ip address 1.1.1.254 255.255.255.0
 duplex auto
!
interface Ethernet0/1
 no shutdown
 ip address 10.10.30.254 255.255.255.0
 duplex auto
!
no ip http server
no ip http secure-server
ip route 0.0.0.0 0.0.0.0 10.10.30.1
ip route 172.16.1.0 255.255.255.0 1.1.1.1
ip route 172.16.2.0 255.255.255.0 1.1.1.3
ip route 192.168.10.0 255.255.255.0 1.1.1.1
ip route 192.168.20.0 255.255.255.0 1.1.1.3
```

For Failover

ASAv1

```
int gi0/1
no shutdown
failover lan interface LAN gi0/1
failover interface ip LAN 8.8.8.1 255.255.255.0 standby 8.8.8.2
failover lan unit primary
failover key mohsin123
failover

int gi0/0
no shutdown
failover link state gi0/0
failover interface ip state 9.9.9.1 255.255.255.0 standby 9.9.9.2
```

ASAv2

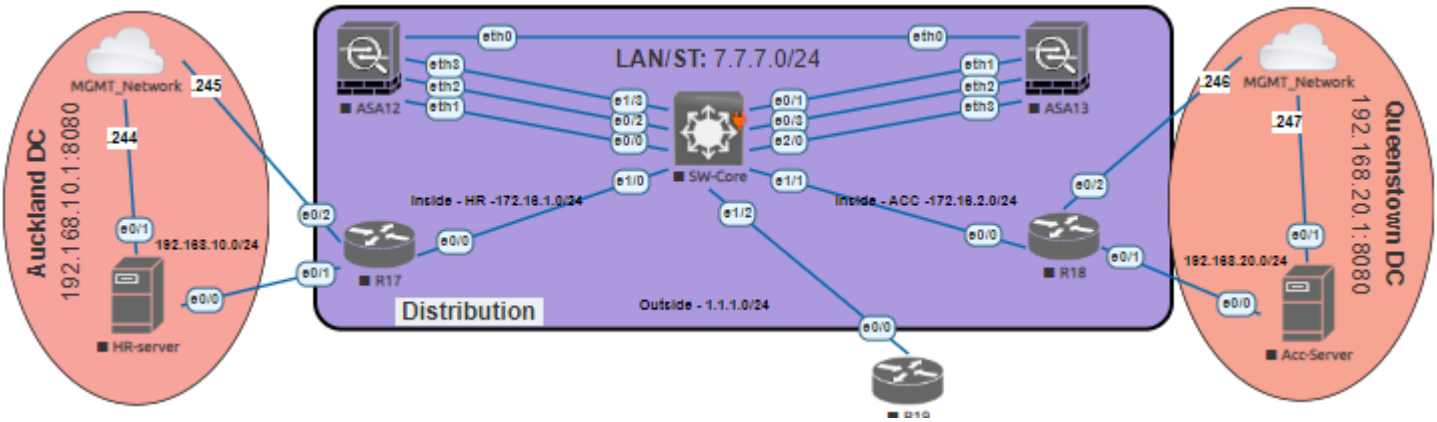
```
int gi0/1
no shutdown
failover lan interface LAN gi0/1
failover interface ip LAN 8.8.8.1 255.255.255.0 standby 8.8.8.2
failover lan unit secondary
failover key mohsin123
failover
```

ASAv1

```
interface GigabitEthernet0/2
 nameif inside
 security-level 100
 ip address 10.10.30.1 255.255.255.0 standby 10.10.30.2
!
interface GigabitEthernet0/3
 nameif outside
 security-level 0
 ip address 100.100.40.1 255.255.255.0 standby 100.100.40.2
!
interface Management0/0
 nameif mgmt
 security-level 0
ip address 192.168.0.242 255.255.255.0 standby 192.168.0.241
route outside 0.0.0.0 0.0.0.0 100.100.40.254 1
route inside 192.168.10.0 255.255.255.0 10.10.30.254 1
route inside 192.168.20.0 255.255.255.0 10.10.30.254 1
access-list outside extended permit icmp any any echo
access-list outside extended permit icmp any any echo-reply
```

Lab 2 :Configure Active/Active relationship between ASA12 and ASA13

- must be named “inside”, “outside”, and “mgmt”.
- context HR and context ACC is to be created and assign Ips as per the diagram
- Follow the IP addressing as per the diagram
- Ensure Fail and state interfaces are names as LAN/ST
- Use .1 (first IP of octet) to assign addresses to the FWs



We will start this lab by configuring respective routers first

R17

```
interface Ethernet0/0
 no shutdown
 ip address 172.16.1.254 255.255.255.0
 duplex auto
!
interface Ethernet0/1
 no shutdown
 ip address 192.168.10.254 255.255.255.0
 duplex auto
!
interface Ethernet0/2
 no shutdown
 ip address 192.168.0.245 255.255.255.0
 shutdown
 duplex auto
ip route 0.0.0.0 0.0.0.0 172.16.1.1
```

R18

```
interface Ethernet0/0
 no shutdown
 ip address 172.16.2.254 255.255.255.0
 duplex auto
!
interface Ethernet0/1
 no shutdown
 ip address 192.168.20.254 255.255.255.0
 duplex auto
!
interface Ethernet0/2
 no shutdown
 ip address 192.168.0.246 255.255.255.0
 shutdown
 duplex auto
ip route 0.0.0.0 0.0.0.0 172.16.2.1
```

HR Server

```
interface Ethernet0/0
 no shutdown
 ip address 192.168.10.1 255.255.255.0
 duplex auto
ip http server
ip http port 8080
ip http authentication local
no ip http secure-server
ip route 0.0.0.0 0.0.0.0 192.168.10.254
username mohsin privilege 15 password 0 mohsin
```

ACC Server

```
interface Ethernet0/0
 no shutdown
 ip address 192.168.20.1 255.255.255.0
 duplex auto
ip http server
ip http port 8080
ip http authentication local
no ip http secure-server
ip route 0.0.0.0 0.0.0.0 192.168.20.254
username mohsin privilege 15 password 0 mohsin
```

ASA12

```
Context HR
 allocate-interface E3 outside
 allocate-interface E2 inside
 config-url flash:HR.cfg

Context ACC
 allocate-interface E3 outside
 allocate-interface E1 inside
 config-url flash:ACC.cfg

changeto Context HR
 interface inside
 nameif inside
 no shutdown
 ip add 172.16.1.1 255.255.255.0 standby 172.16.1.2
 interface outside
 nameif outside
 no shutdown
 ip add 1.1.1.1 255.255.255.0 standby 1.1.1.2

 changeto Context ACC
 interface inside
 nameif inside
 no shutdown
 ip add 172.16.2.1 255.255.255.0 standby 172.16.2.2
 interface outside
 nameif outside
 no shutdown
 ip add 1.1.1.3 255.255.255.0 standby 1.1.1.4

int e0
no shutdown
failover lan interface LAN E0
failover interface ip LAN 7.7.7.1 255.255.255.0 standby 7.7.7.2
failover lan unit primary
failover key mohsin123
failover link ST E0
```

ASA13

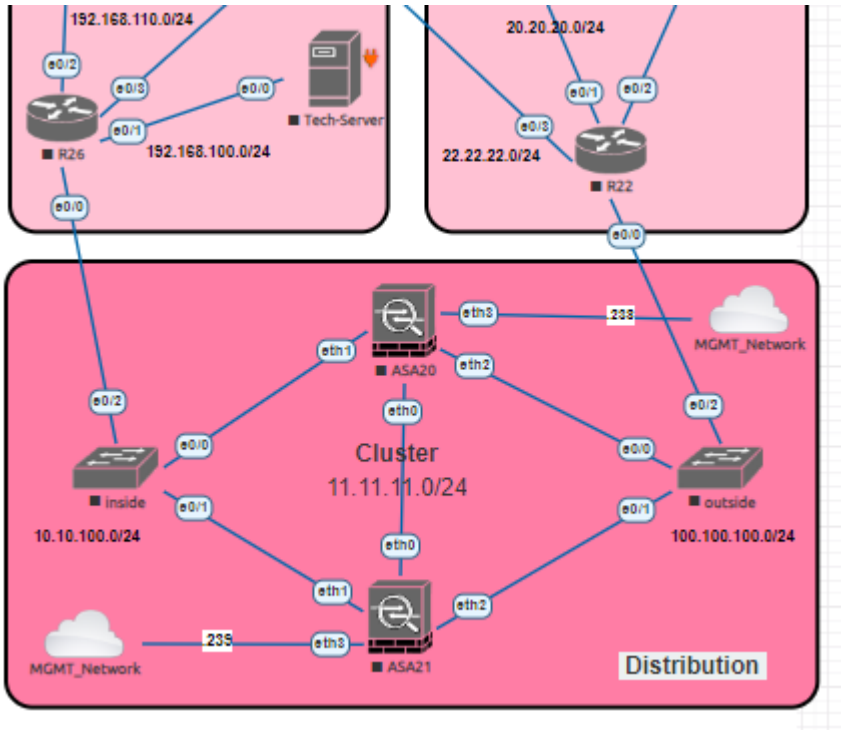
```
ASA13
int e0
no shutdown
failover lan interface LAN E0
failover interface ip LAN 7.7.7.1 255.255.255.0 standby 7.7.7.2
failover lan unit secondary
failover key mohsin123
failover link ST E0
```

ASA12

```
failover group 1
 primary
 preempt

failover group 2
 secondary
 preempt

context HR
 join-failover-group 1

context ACC
 join-failover-group 2
```

Lab 3 : Configure Clustering relationship between ASA20 and ASA21

- must be named “inside”, “outside”, and “mgmt”.
- Cluster group name should be Cisco
- Follow the IP addressing as per the diagram
- Key should be C1sC0123!
- Inside network should be part of VLAN 100 & outside network should be part of VLAN 200
- Use .1 (first IP of octet) to assign addresses to the FWs



Tech-Server

```
interface Ethernet0/0
 no shutdown
 ip address 192.168.100.1 255.255.255.0
 duplex auto

ip route 0.0.0.0 0.0.0.0 192.168.100.254

ip http server
ip http authentication local
no ip http secure-server
ip route 0.0.0.0 0.0.0.0 192.168.20.254
username mohsin privilege 15 password 0 mohsin
```

R26

```
interface Ethernet0/0
 no shutdown
 ip address 10.10.100.254 255.255.255.0
 duplex auto
!
interface Ethernet0/1
 no shutdown
 ip address 192.168.100.254 255.255.255.0
 duplex auto
!
interface Ethernet0/2
 no shutdown
 ip address 192.168.0.238 255.255.255.0
 shutdown
 duplex auto
!
interface Ethernet0/3
 no shutdown
 ip address 192.168.110.254 255.255.255.0
 duplex auto
ip route 0.0.0.0 0.0.0.0 10.10.100.1
```

R22

```
interface Ethernet0/0
 no shutdown
 ip address 100.100.100.254 255.255.255.0
 duplex auto
!
interface Ethernet0/1
 no shutdown
 ip address 20.20.20.254 255.255.255.0
 duplex auto

interface Ethernet0/3
 no shutdown
 ip address 22.22.22.254 255.255.255.0
 duplex auto

ip route 0.0.0.0 0.0.0.0 100.100.100.1
```

ASA20

```
cluster interface-mode spanned

int e0
no shutdown

cluster group Cisco
 local-unit ASA-A
 cluster-interface E0 ip 11.11.11.1 255.255.255.0
 key C1sC0123!
 priority 5
 enable
```

ASA21

```
cluster interface-mode spanned

int e0
no shutdown

cluster group Cisco
 local-unit ASA-b
 cluster-interface E0 ip 11.11.11.2 255.255.255.0
 key C1sC0123!
 priority 10
 enable
```

Inside-SW

```
interface Port-channel1
 no shutdown
 switchport access vlan 100

interface Ethernet0/0
 no shutdown
 switchport access vlan 100
 channel-group 1 mode active
!
interface Ethernet0/1
 no shutdown
 switchport access vlan 100
 channel-group 1 mode active
!
interface Ethernet0/2
 no shutdown
 switchport access vlan 100
 switchport mode access
```

Outside-SW

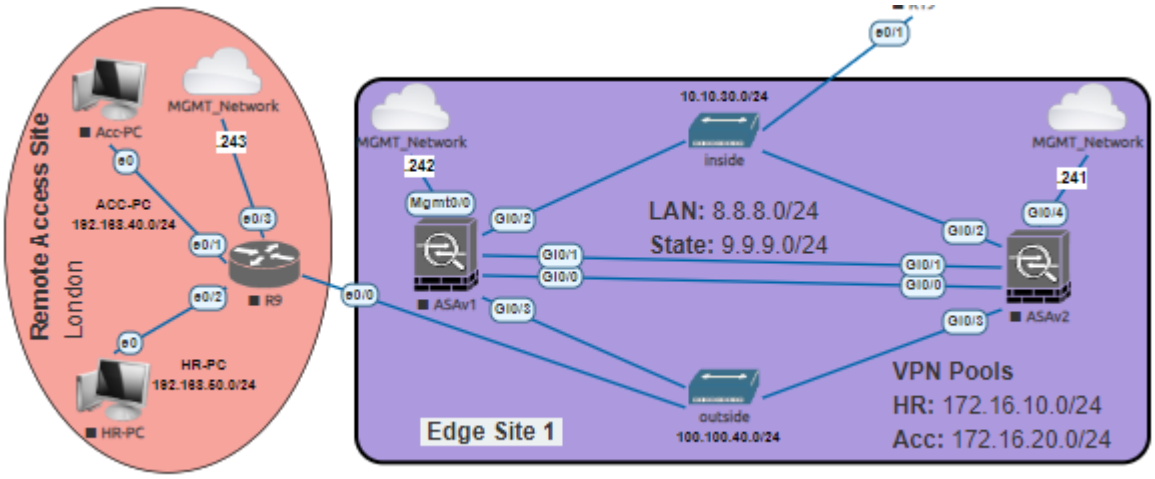
```
interface Port-channel2
 no shutdown
 switchport access vlan 200
 switchport mode access
!
interface Ethernet0/0
 no shutdown
 switchport access vlan 200
 switchport mode access
 channel-group 2 mode active
!
interface Ethernet0/1
 no shutdown
 switchport access vlan 200
 switchport mode access
 channel-group 2 mode active
!
interface Ethernet0/2
 no shutdown
 switchport access vlan 200
```

ASA20

```
ip local pool MGMT 192.168.0.239-192.168.0.240
interface Ethernet1
 channel-group 1 mode active
 no nameif
 no security-level
 no ip address
!
interface Ethernet2
 channel-group 2 mode active
 no nameif
 no security-level
 no ip address
!
interface Ethernet3
 management-only
 nameif mgmt
 security-level 0
 ip address 192.168.0.241 255.255.255.0 cluster-pool MGMT
!
interface Port-channel1
 port-channel span-cluster
 mac-address aaaa.bbbb.1111
 nameif inside
 security-level 100
 ip address 10.10.100.1 255.255.255.0
!
interface Port-channel2
 port-channel span-cluster
 mac-address aaaa.bbbb.2222
 nameif outside
 security-level 0
 ip address 100.100.100.1 255.255.255.0
!
ftp mode passive
access-list outside extended permit icmp any any echo
access-list outside extended permit icmp any any echo-reply

access-group outside in interface outside
route outside 0.0.0.0 0.0.0.0 100.100.100.254 1
route inside 192.168.100.0 255.255.255.0 10.10.100.254 1
http 0.0.0.0 0.0.0.0 mgmt
```

Lab 4 : Configure AnyConnect VPN on London Site with requirements as below

- HR department should have a dedicated profile named as HR-Profile and pool 172.16.10.0/24
- ACC department should have a dedicated profile named as SALES-Profile and pool 172.16.20.0/24
- Ensure you enable split tunneling
- IPSec IKEV2 tunnel with an idle timeout of 2 Days.
- Create local users on ASA DB for HR it should be hr/cisco123
- Create local users on ASA DB for ACC it should be acc/cisco123

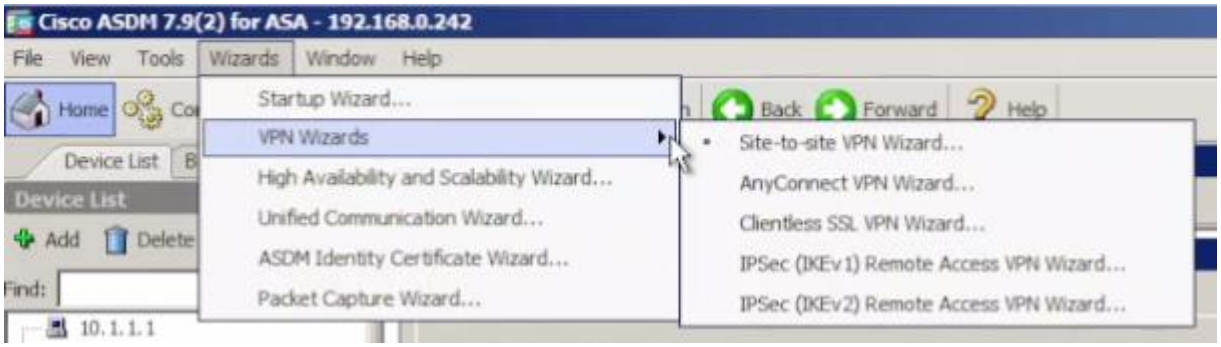


Assign your PCs address as below

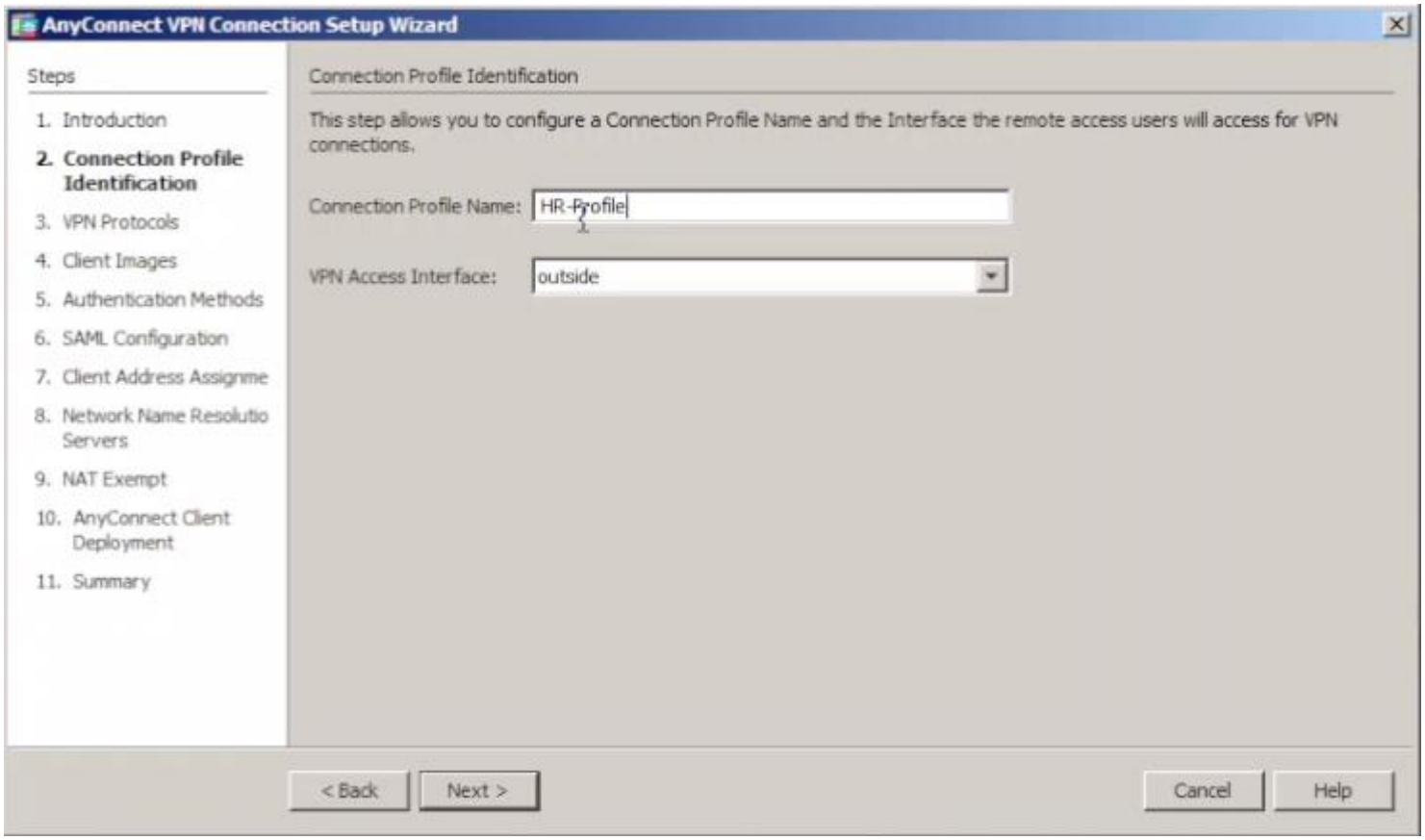
HR-PC	192.168.60.2
ACC-PC	192.168.40.2

1) Login to ASAV1 using ASDM

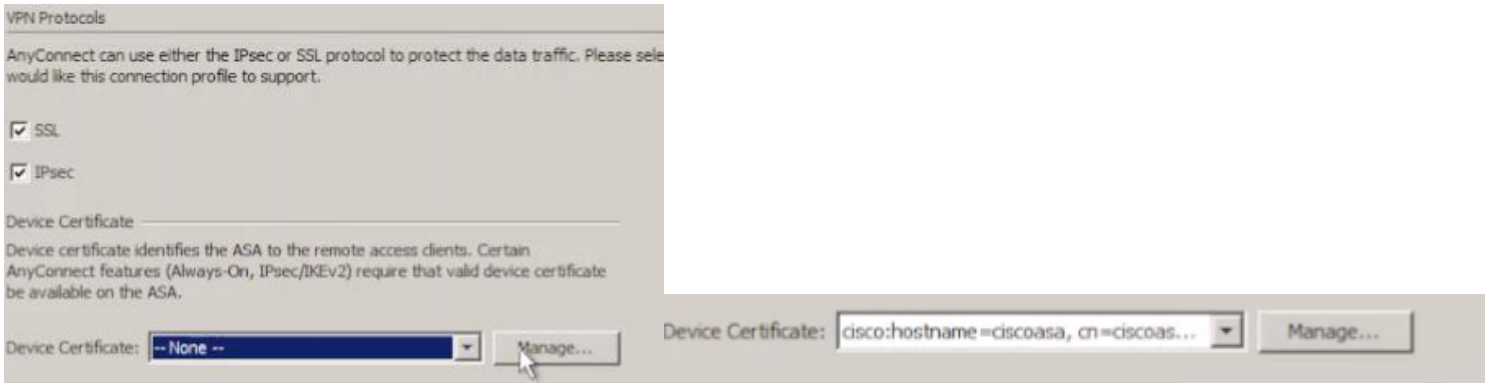
2) VPN Wizards -> Anyconnect VPN



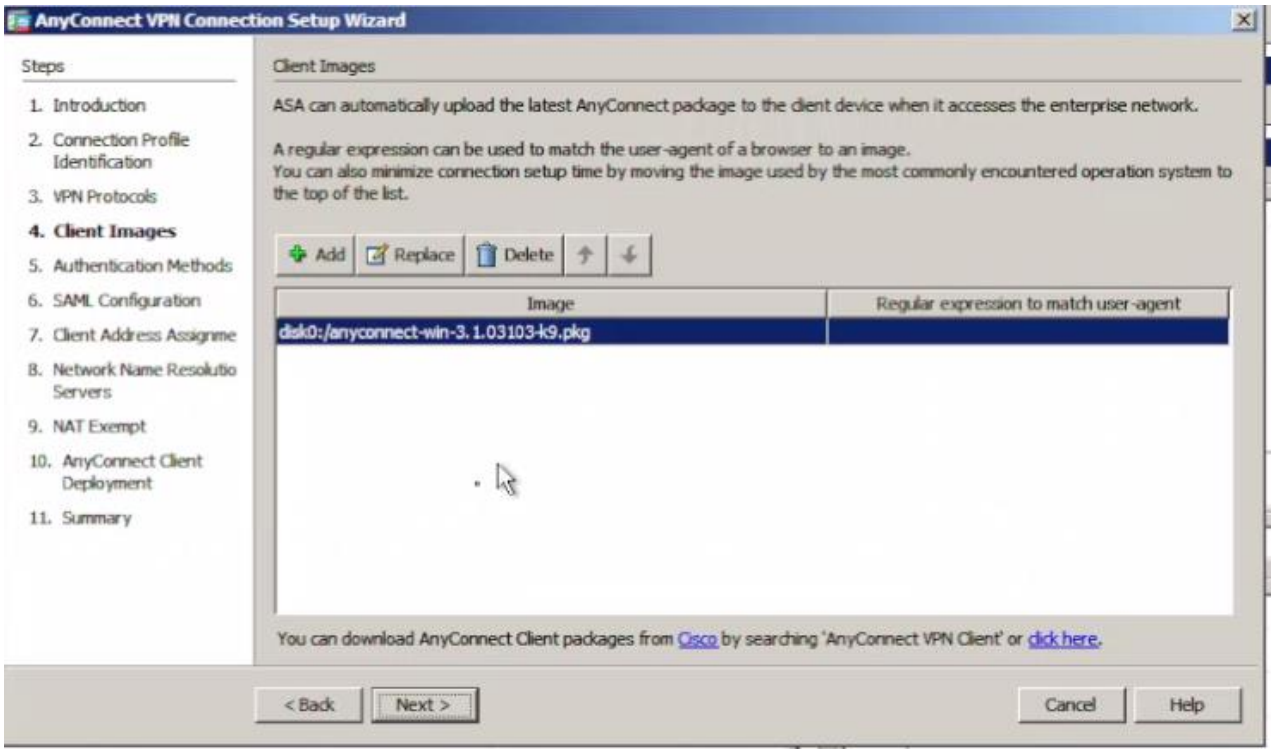
3) Add connection profile name and interface outside



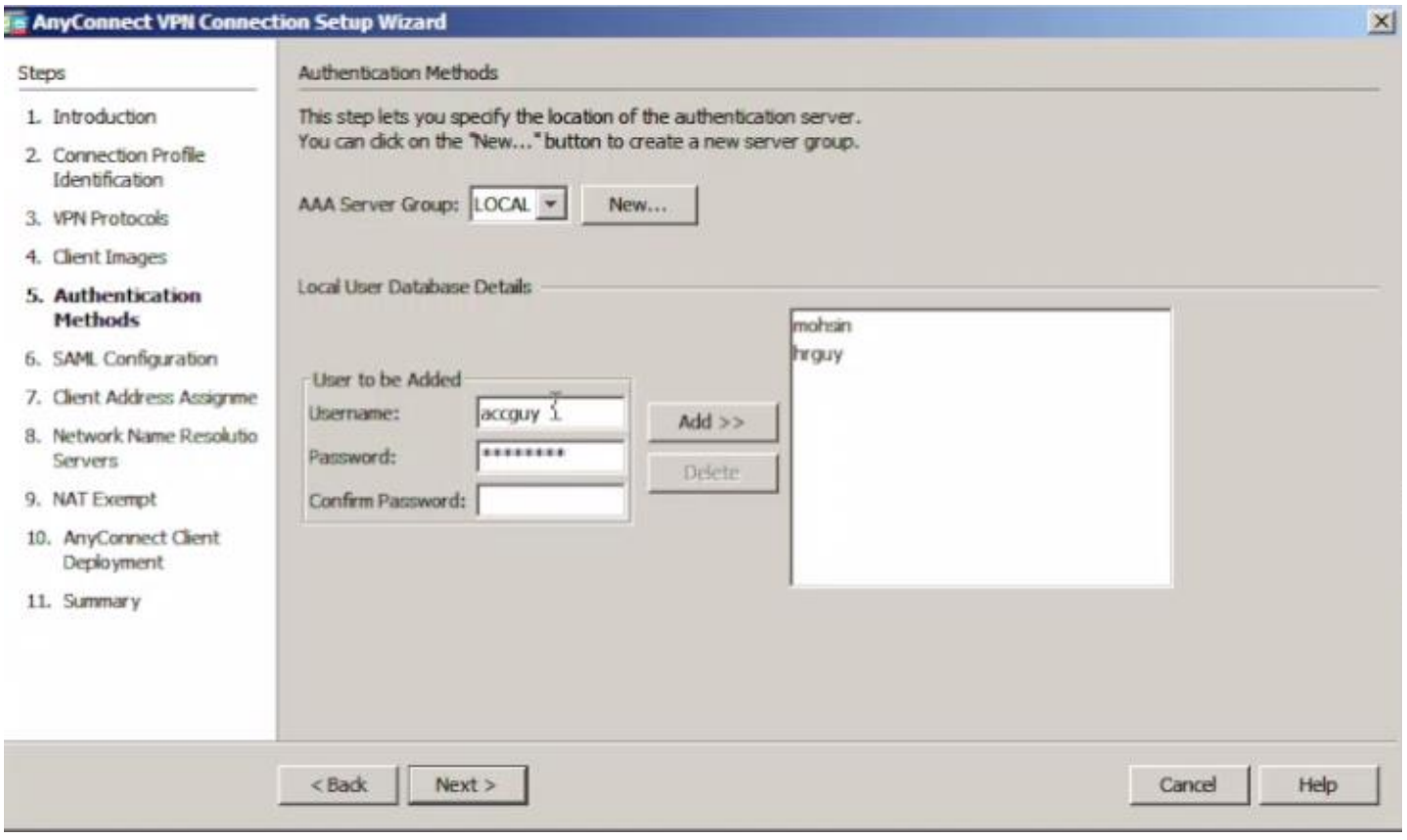
4) Ensure SSL and IPsec are checked and then click on manage to add Certificate



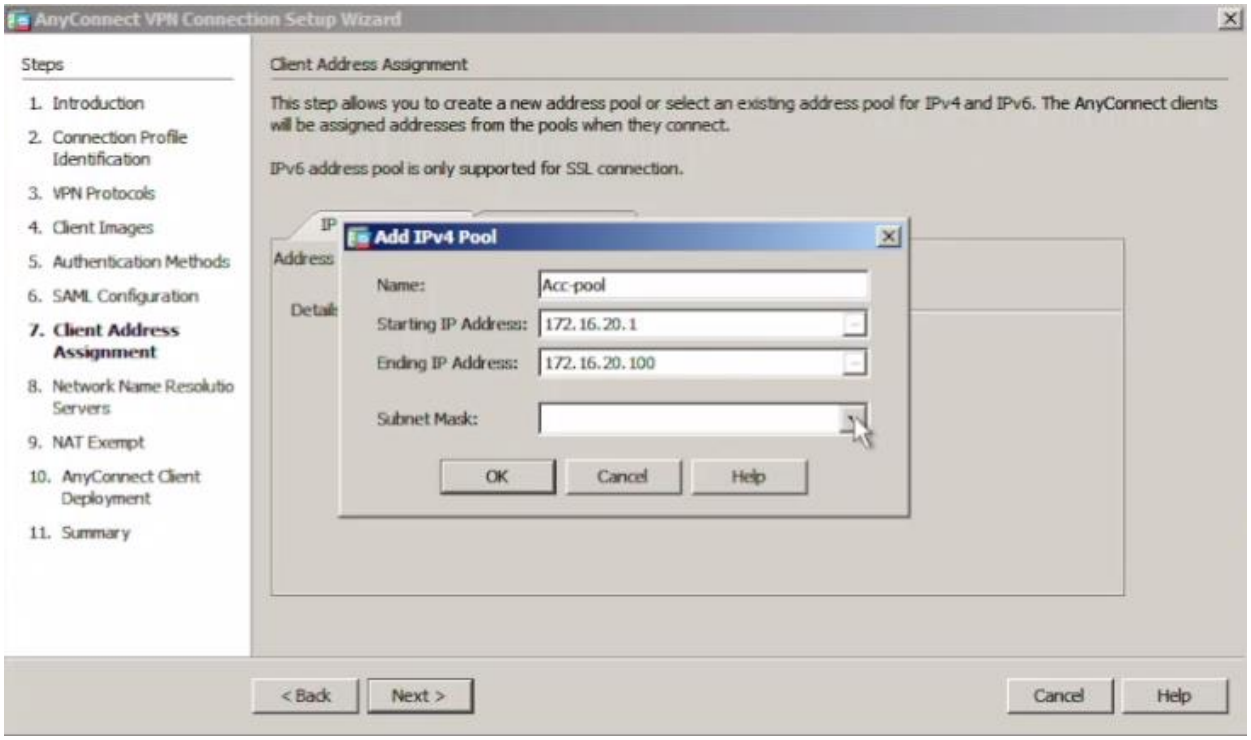
5) Select Anyconnect package file



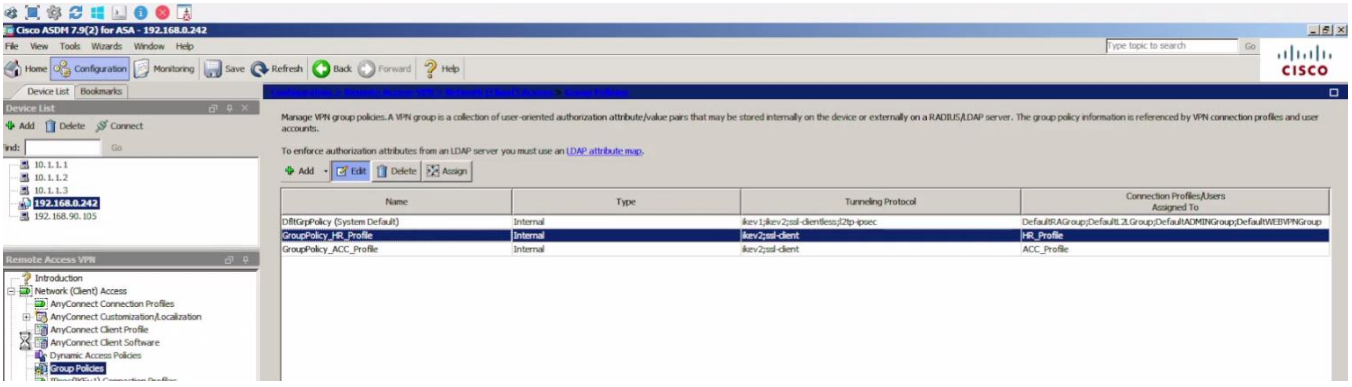
6) Create user accounts



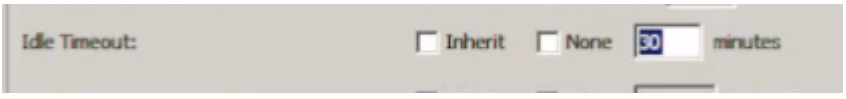
7) Create Pools for Acc/HR



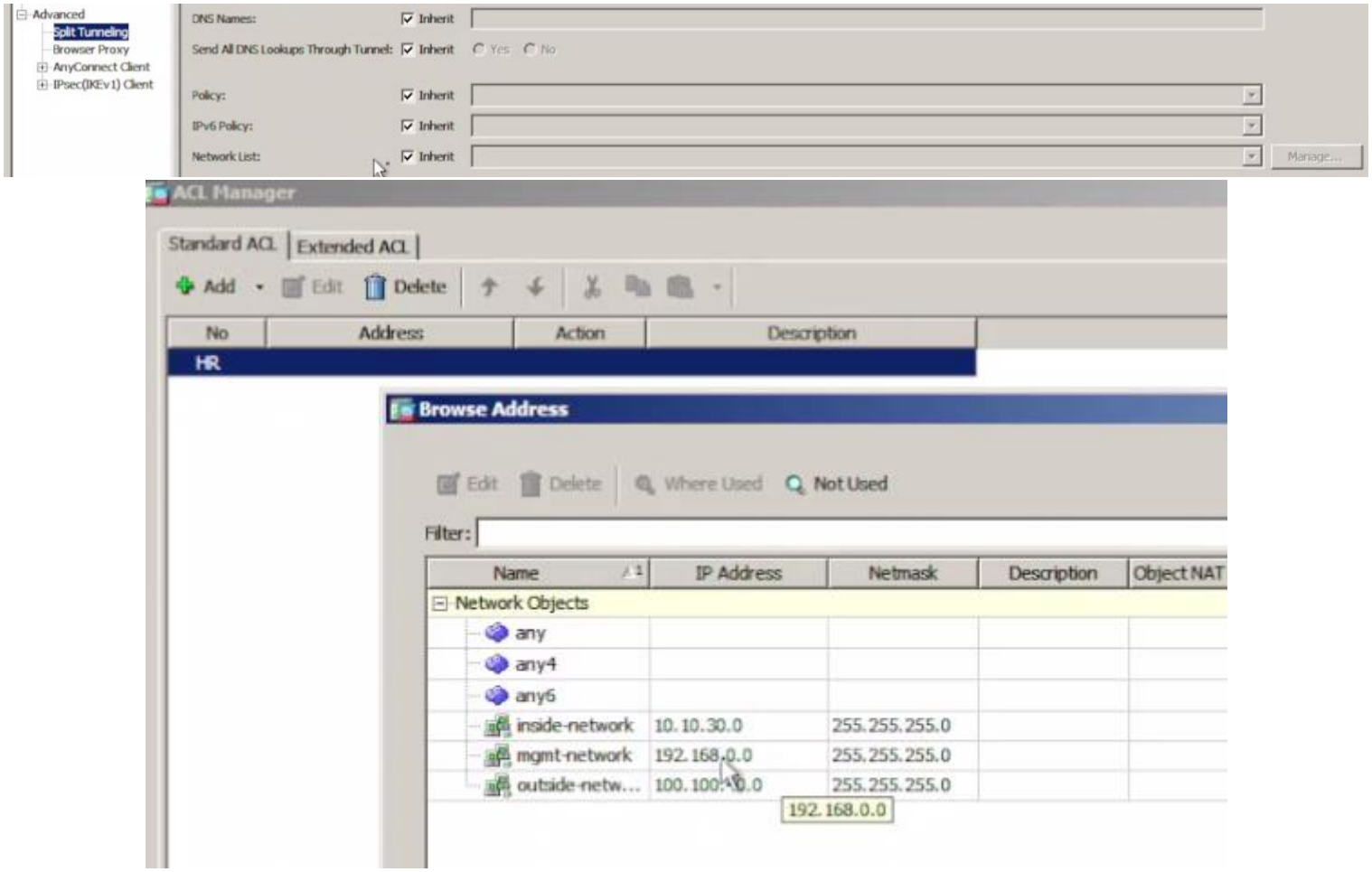
8) Under Group policies, Click on the relevant profile either HR or ACC, edit



9) Under General, Make sure you set the idle time as per requirements



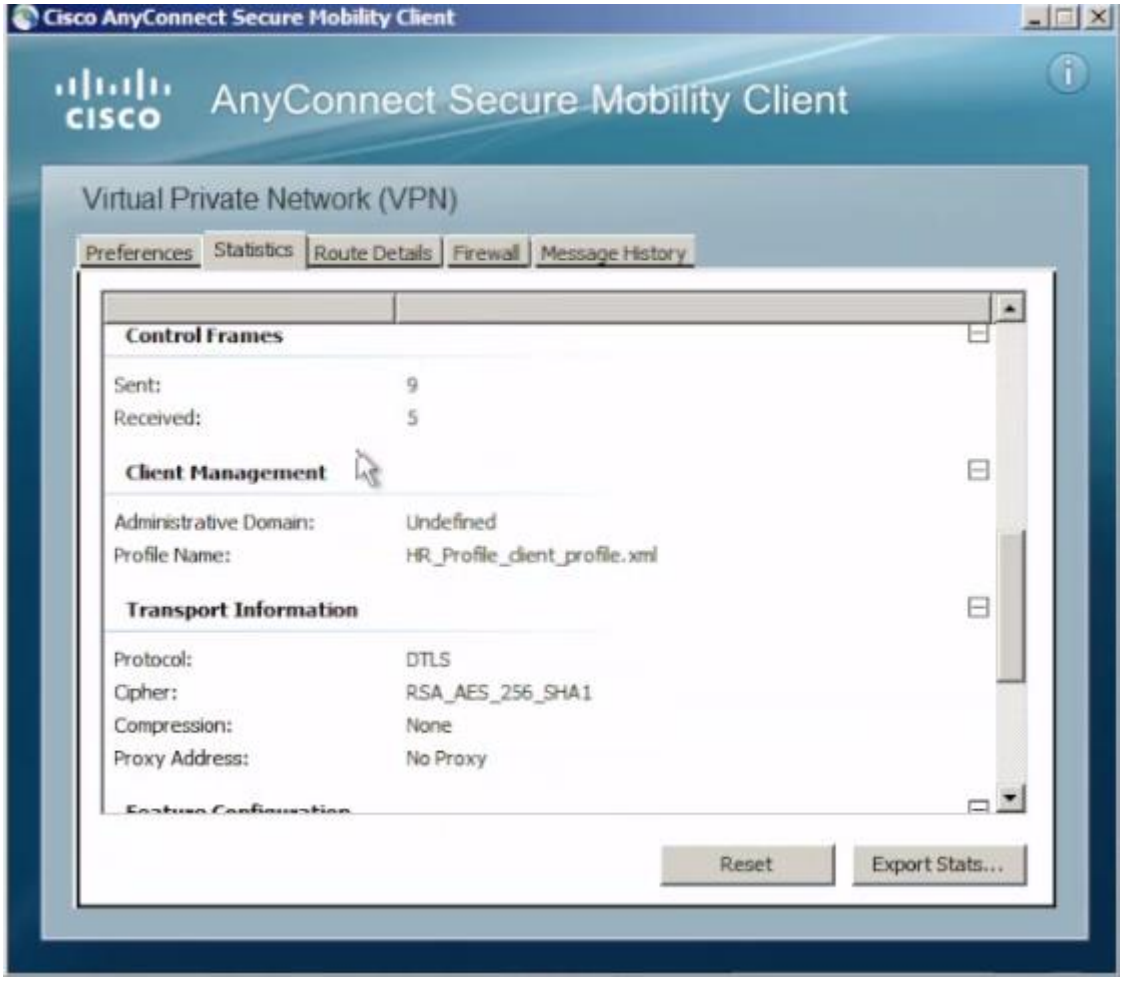
10) In advanced -> Split tunneling
   a. Policy -> Tunnel networks list below
   b. Network list > manage and create the network list you want to allow in tunnel



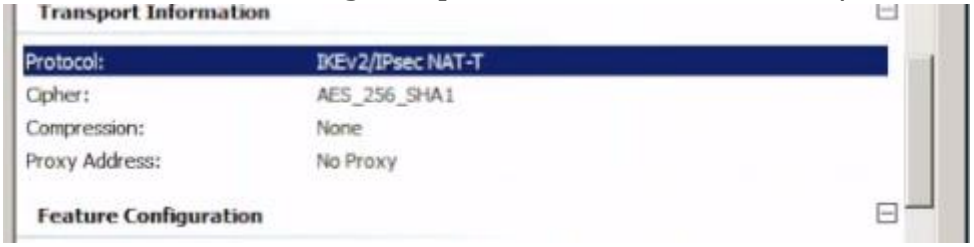
11) On remote PC -> download your Client and put outside interface IP to connect

12) On remote PC -> download your Client and put outside interface IP to connect

13) Under statistics for the first time you will see Protocol DTLS -> AES_256_SHA1

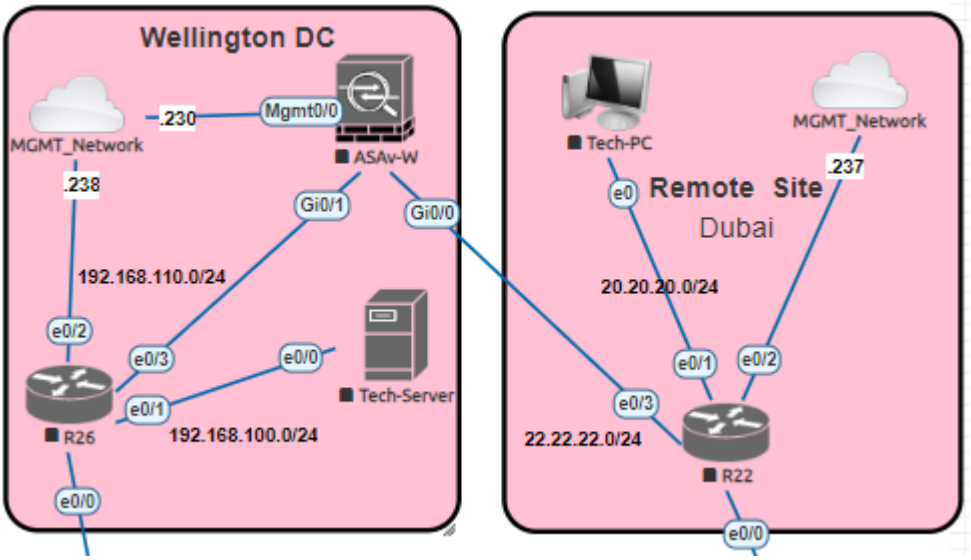


15) Disconnect the VPN and reconnect again –protocol should be IKEv2/IPSECNAT-T



Lab 5 : Configure Clientless SSL VPN for Dubai Remote-Site on ASAv-W

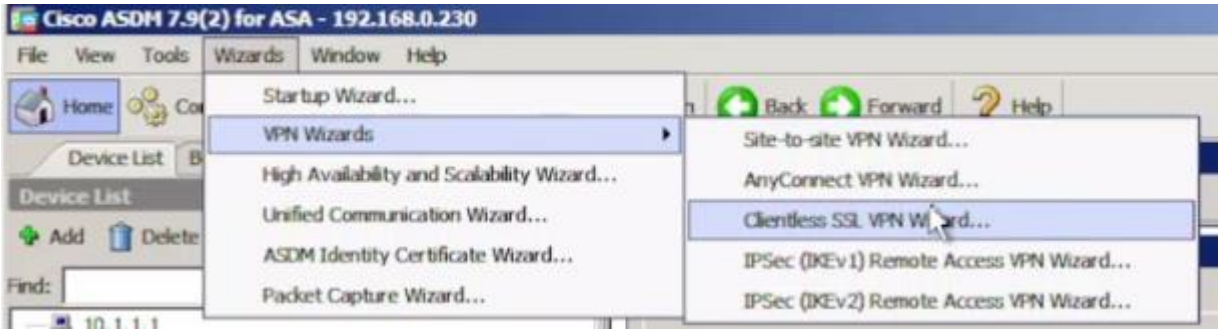
- Tech department should have a dedicated profile named as Tech-profile
- Username should be tech and password cisco123
- Use a web-acl and add it the group policy so that user tech can access tech-server only.



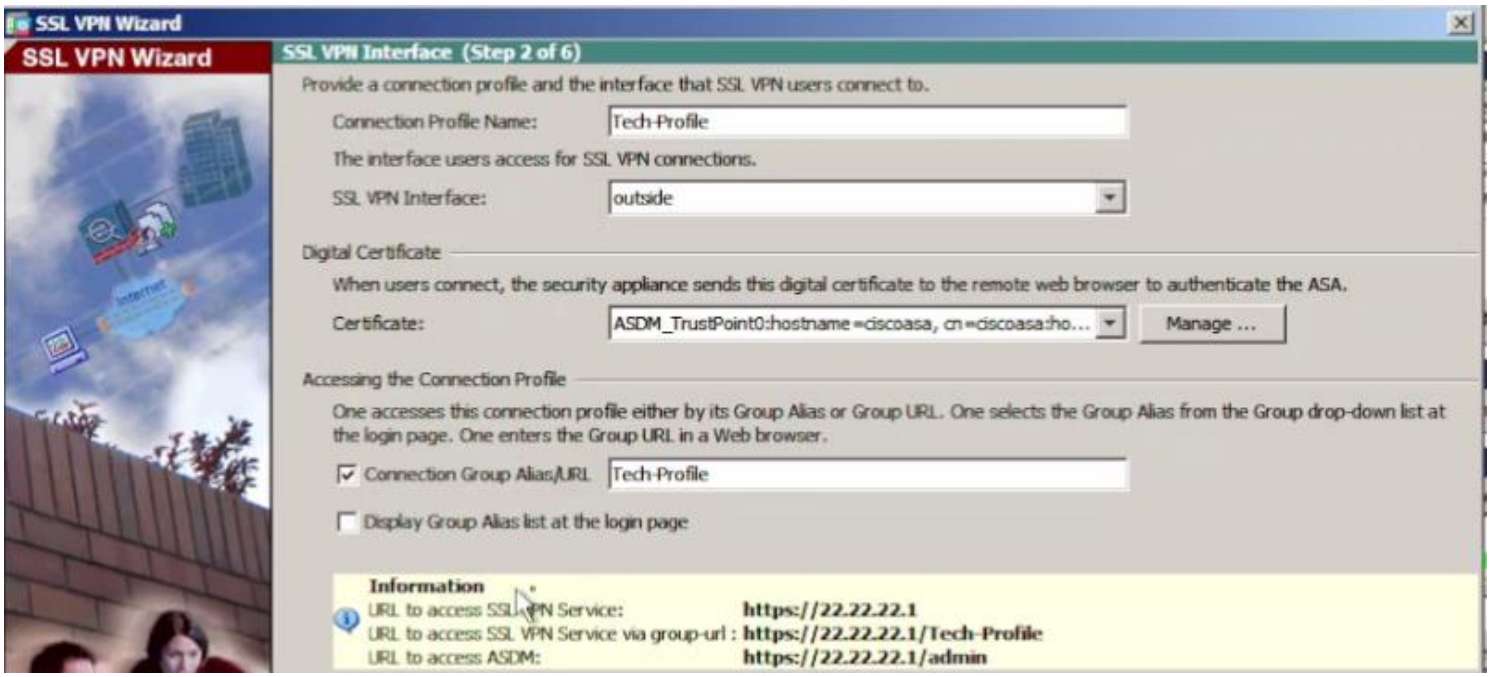
ASAVw

```
interface GigabitEthernet0/0
 nameif outside
 security-level 0
 ip address 22.22.22.1 255.255.255.0
!
interface GigabitEthernet0/1
 nameif inside
 security-level 100
 ip address 192.168.110.1 255.255.255.0
interface Management0/0
 nameif mgmt
 security-level 0
 ip address 192.168.0.230 255.255.255.0
route outside 0.0.0.0 0.0.0.0 22.22.22.254 1
route inside 192.168.100.0 255.255.255.0 192.168.110.254 1
http server enable
http 0.0.0.0 0.0.0.0 mgmt
```

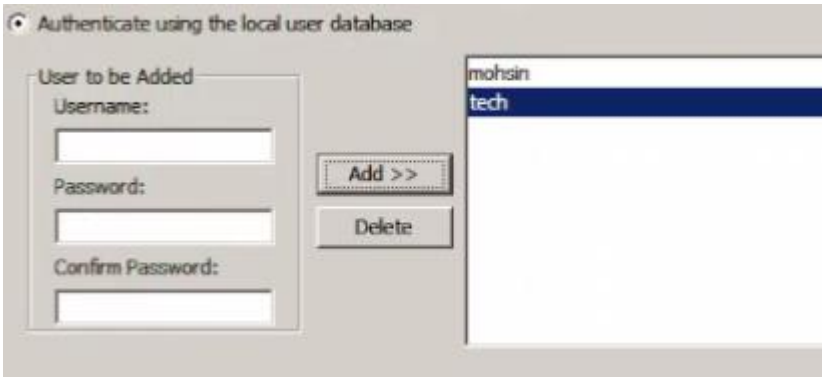
1) Login to ASA using ASDM
2) Wizards -> VPN Wizards -> Clientless SSL VPN



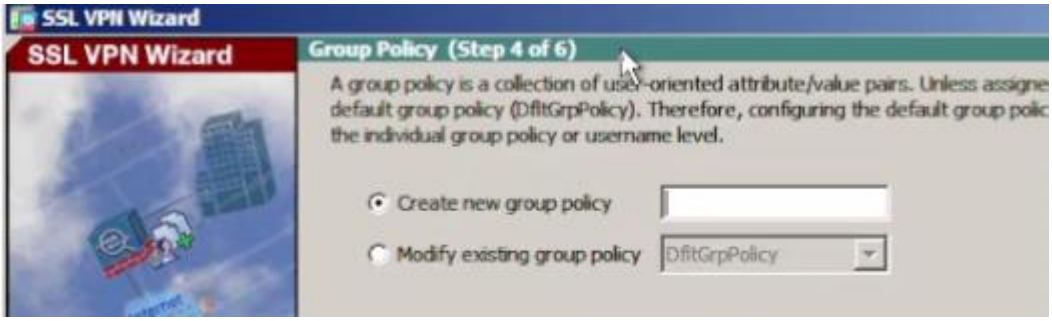
3) Ensure you type correct Connection profile name, select interface outside, Create certificate as per requirements and connection group URL



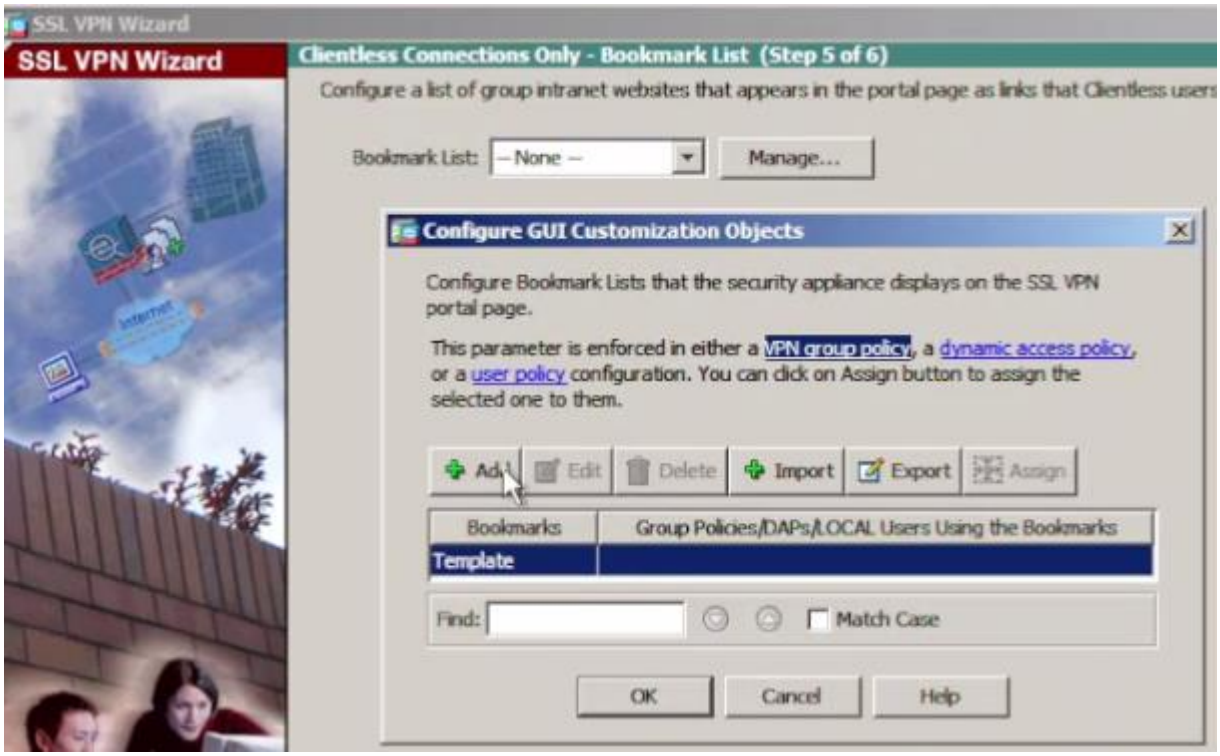
4) Add the user/password as per requirements



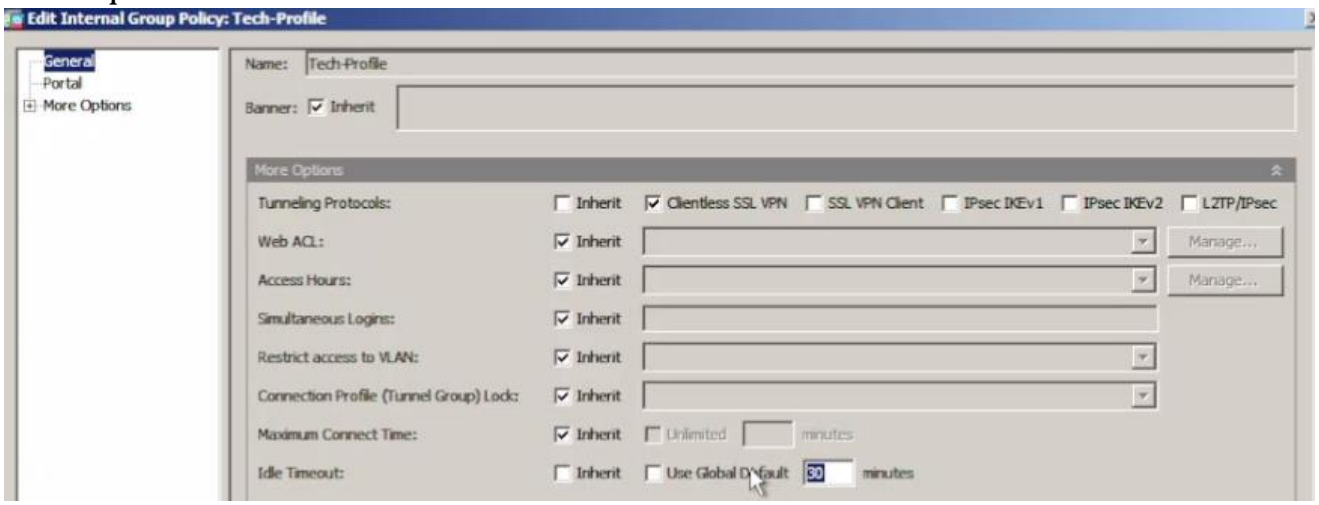
5) Create group Policy, click on create new group policy (Tech-Profile)



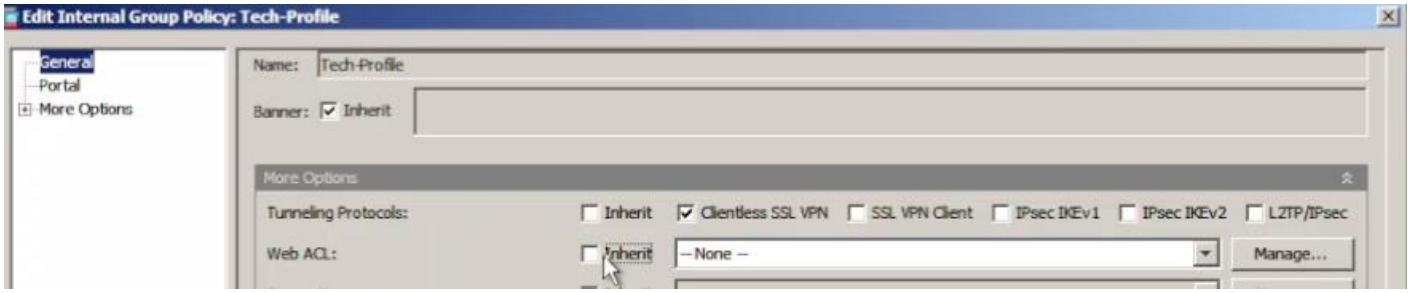
6) Click on bookmarks and create bookmarks as per the requirements.



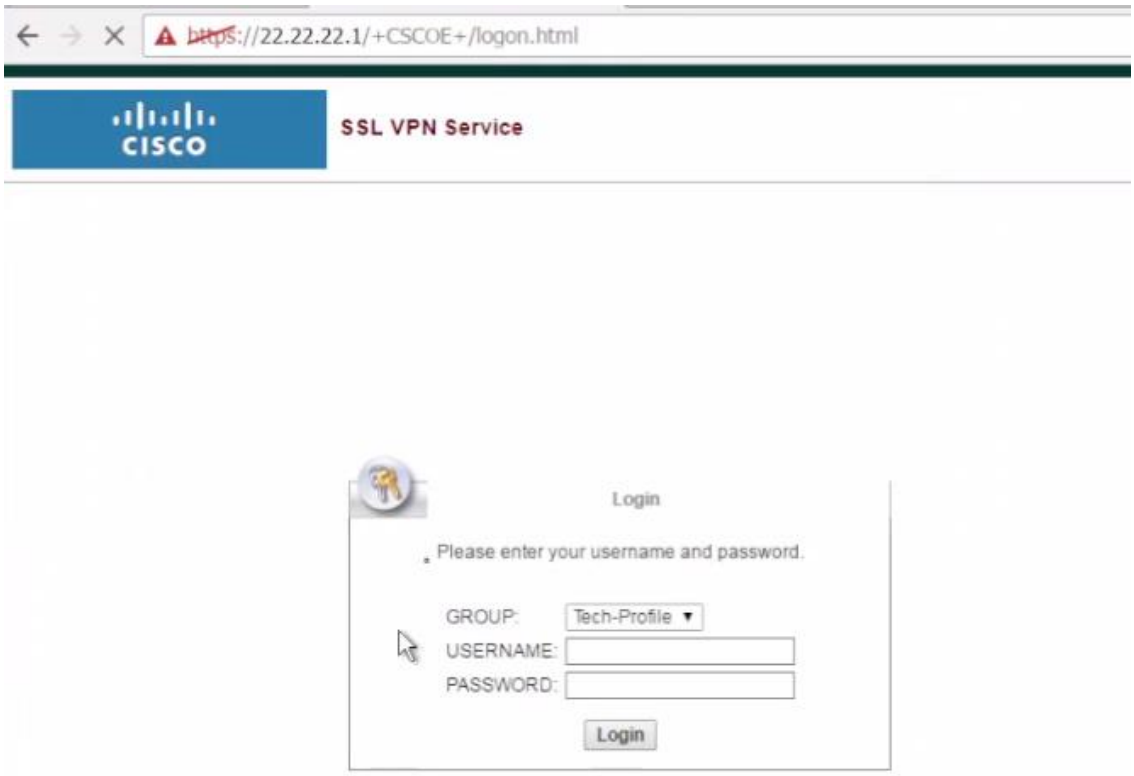
7) Click on Group policy settings, and then click on idle timeout to edit and ensure It is as per the requirements



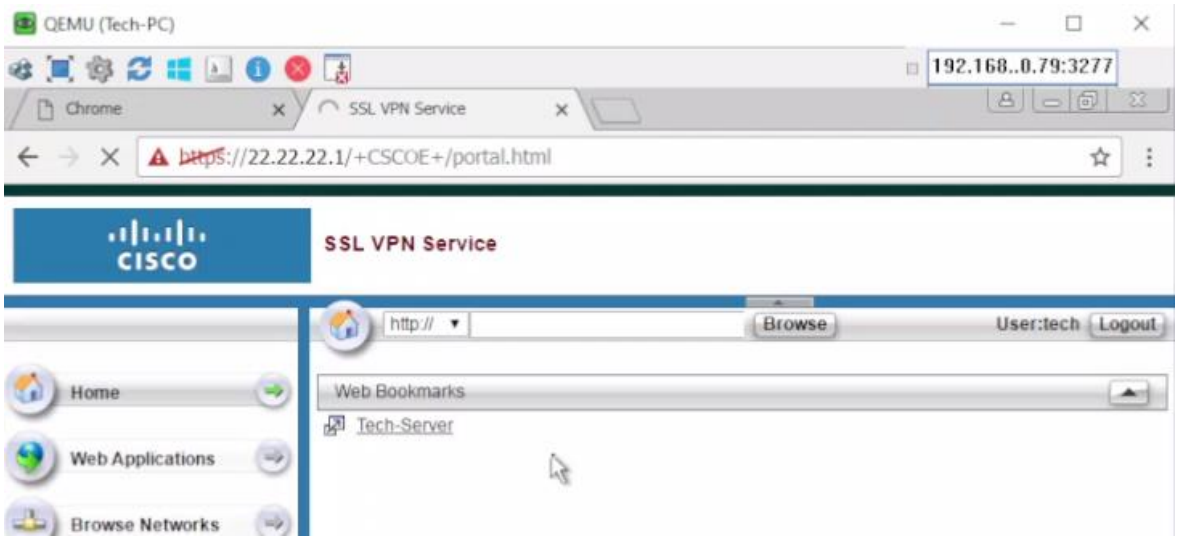
8) Under webacl, create a proper ACL to match your destination server



9) On Tech-PC, Remote site Dubai open browser, and login with credentials.



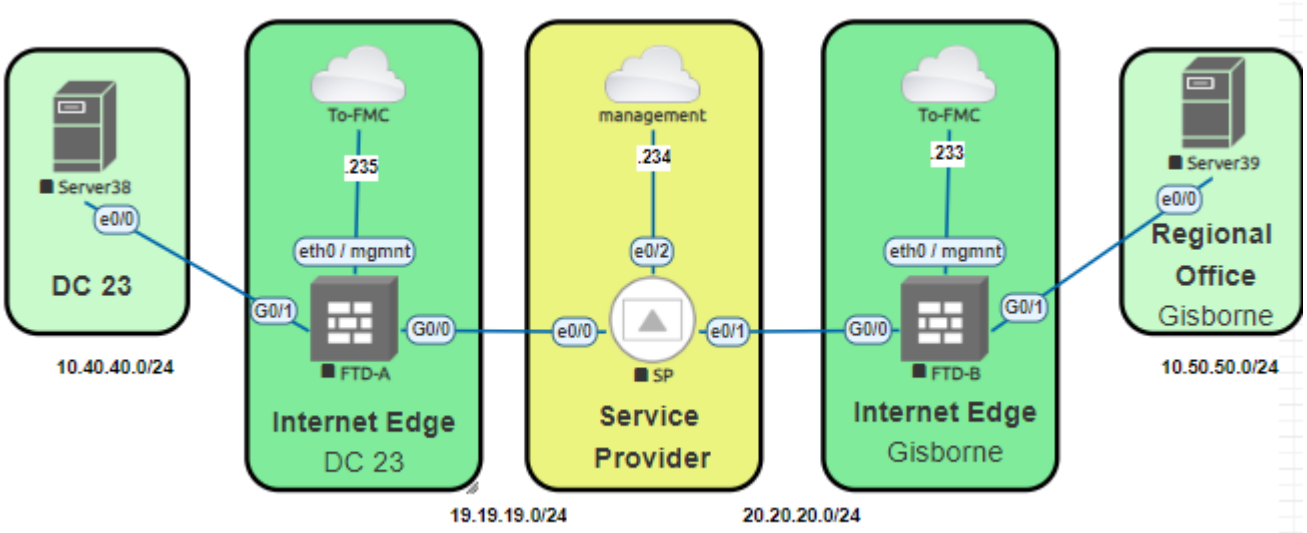
10) On Tech-PC, Remote site Dubai open browser, and login with credentials.

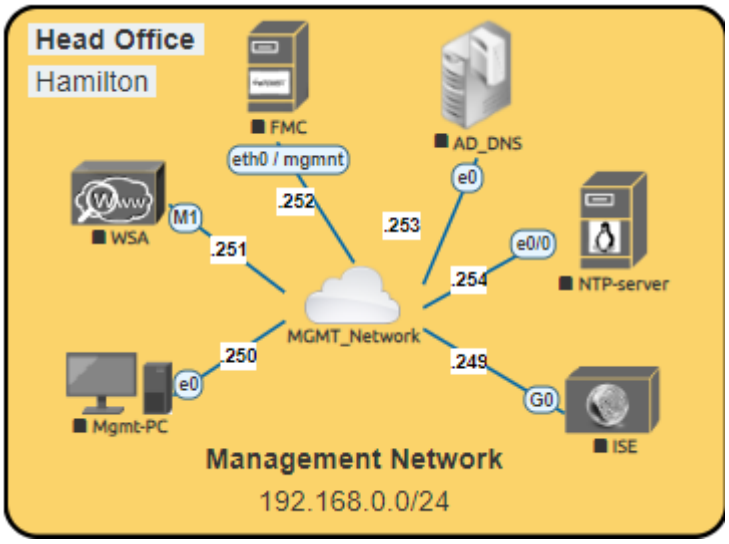


11) You should be able to access Tech-server

Lab 6 : Configure Site-2-Site IKEv1 VPN between DC23 and Gisborne edges.

- Ensure your VPN profile name is DC23-GS
- Pre-shared key should be Cisco123
- Ensure your DC23 FTD should be added as FTD-DC23
- Ensure your GISBORNE FTD should be added as FTD-GISBORNE



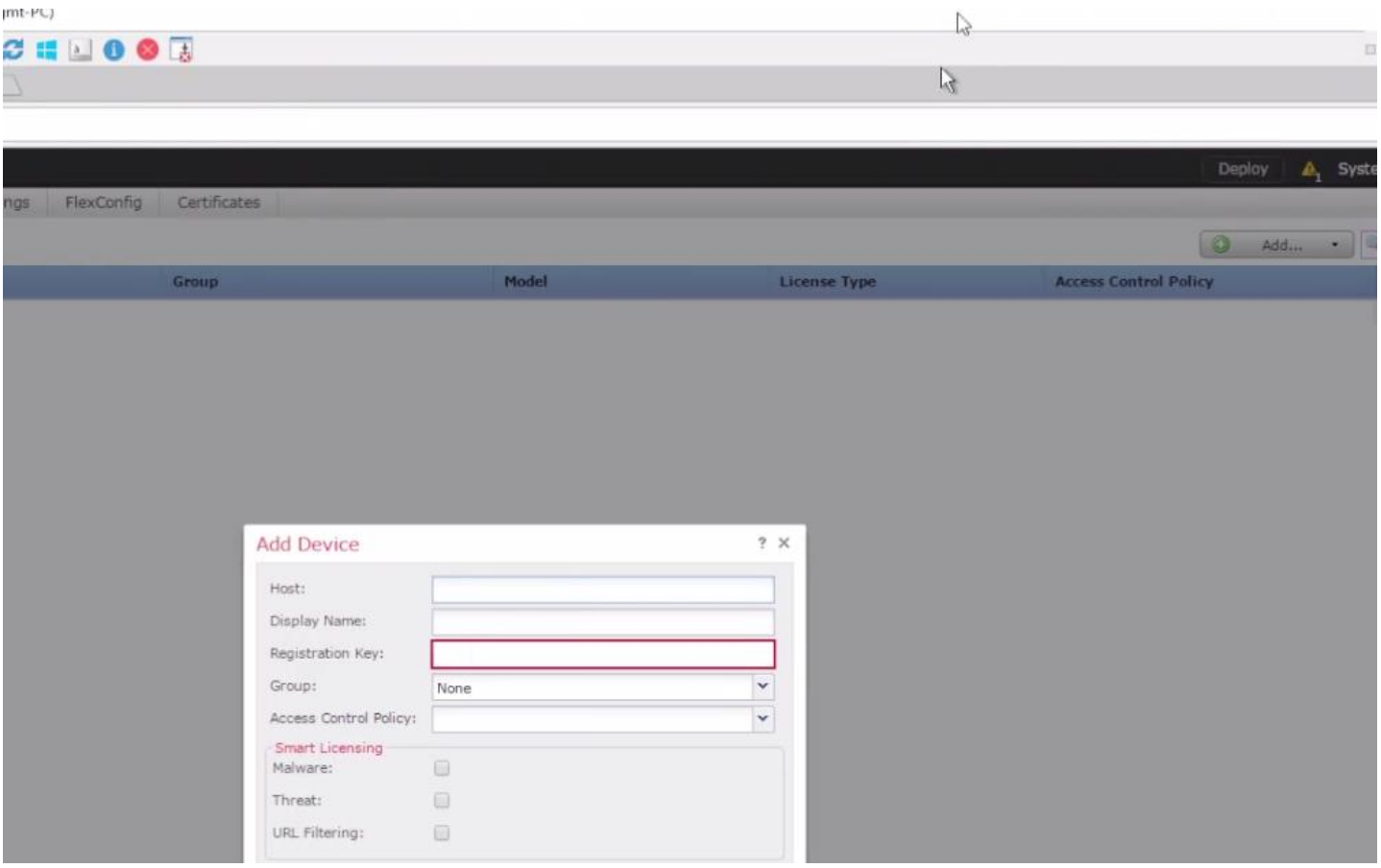


On FTD1 –
configure network ipv4 manual 192.168.0.235 255.255.255.0 192.168.0.254
configure manager add 192.168.0.252 Cisco123
On FTD2 –
configure network ipv4 manual 192.168.0.235 255.255.255.0 192.168.0.254
configure manager add 192.168.0.252 Cisco123
FMC -
to change existing ip if required
sudo /usr/local/sf/bin/configure-network

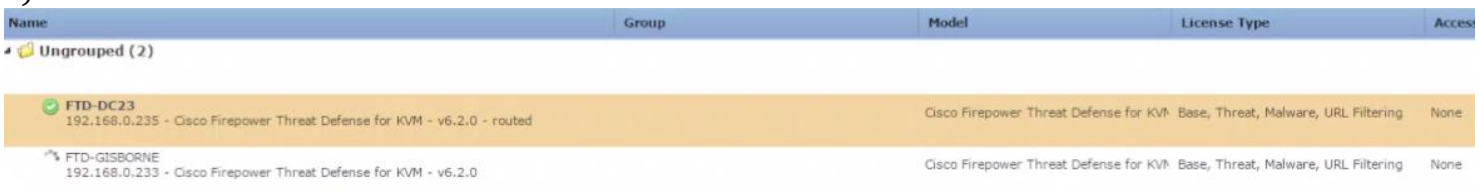
SP

```
interface Ethernet0/0
 no shutdown
 ip address 19.19.19.254 255.255.255.0
 duplex auto
!
interface Ethernet0/1
 no shutdown
 ip address 20.20.20.254 255.255.255.0
 duplex auto
```

1) ON FMC, login to GUI -> Devices -> Click on Add devices
   a. 192.168.0.235
   b. Host **FTD-DC23**
   c. Cisco123
   d. Access control policy -> Block policy (if not created in exam, create one)
   e. Smart licensing -> malware, threat, URL filtering (select all of them)
2) ON FMC, login to GUI -> Devices -> Click on Add devices
   a. 192.168.0.233
   b. Host **FTD-DC23**
   c. Cisco123
   d. Access control policy -> Block policy (if not created in exam, create one)
   e. Smart licensing -> malware, threat, URL filtering (select all of them)



3) You should see both FTD-DC23 & FTD-GISBORNE

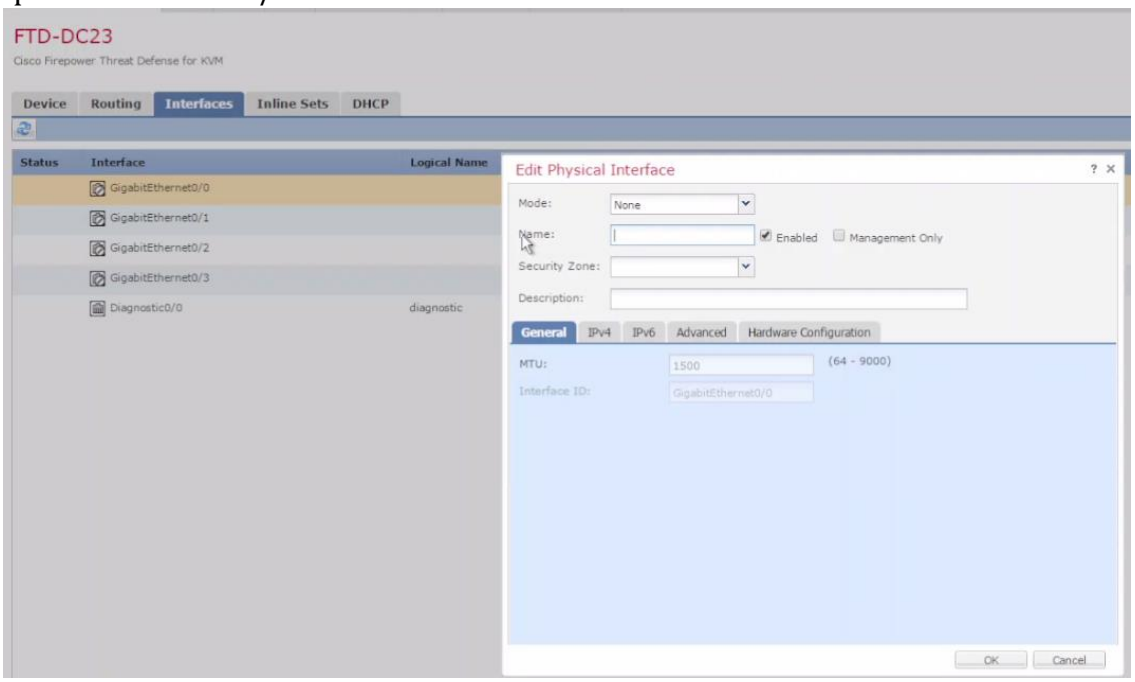


4) Configure your FTD- Devices accordingly

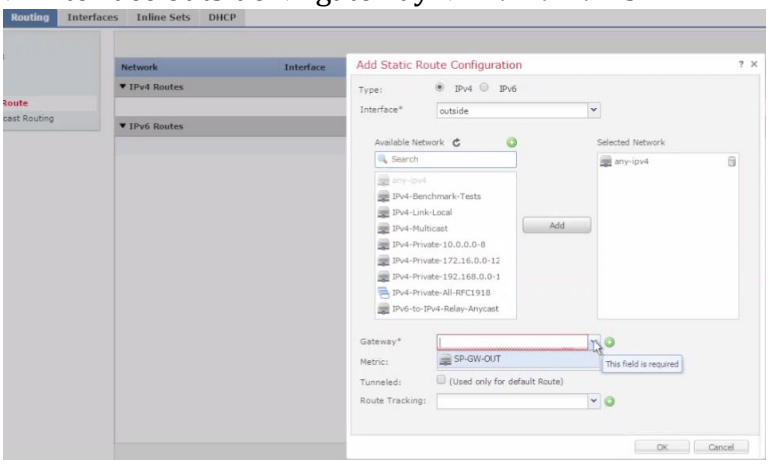
FTD-DC23

a. Gigabitethernet0/0
   i. Name: outside
   ii. Security zone: outside (create one if not there)
   iii. Ipv4: 19.19.19.1/24

b. Gigabitethernet0/1
   i. Name: inside
   ii. Security zone: inside (create one if not there)
   iii. Ipv4: 10.40.40.254/24

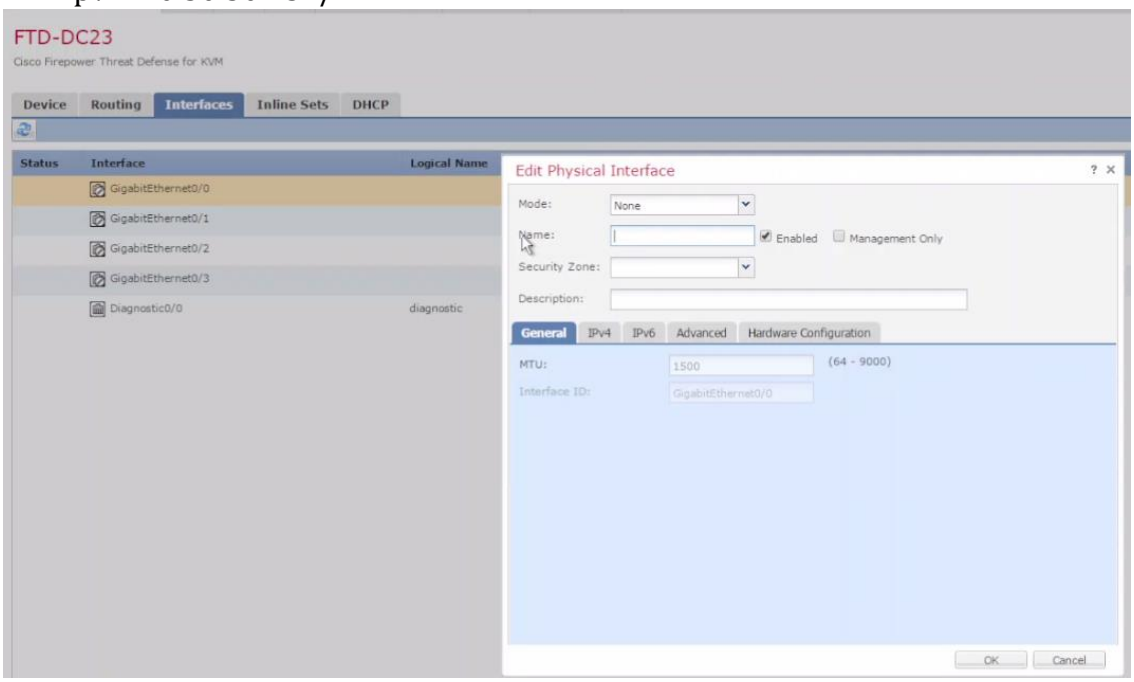


c. Click on static routes and point a default route for outside to SP
   i. Routing -> interface outside -> gateway -> 19.19.19.254

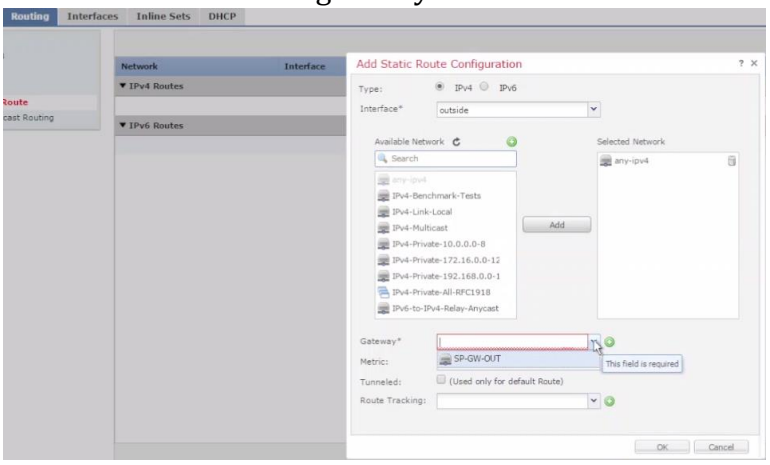


FTD-DC23

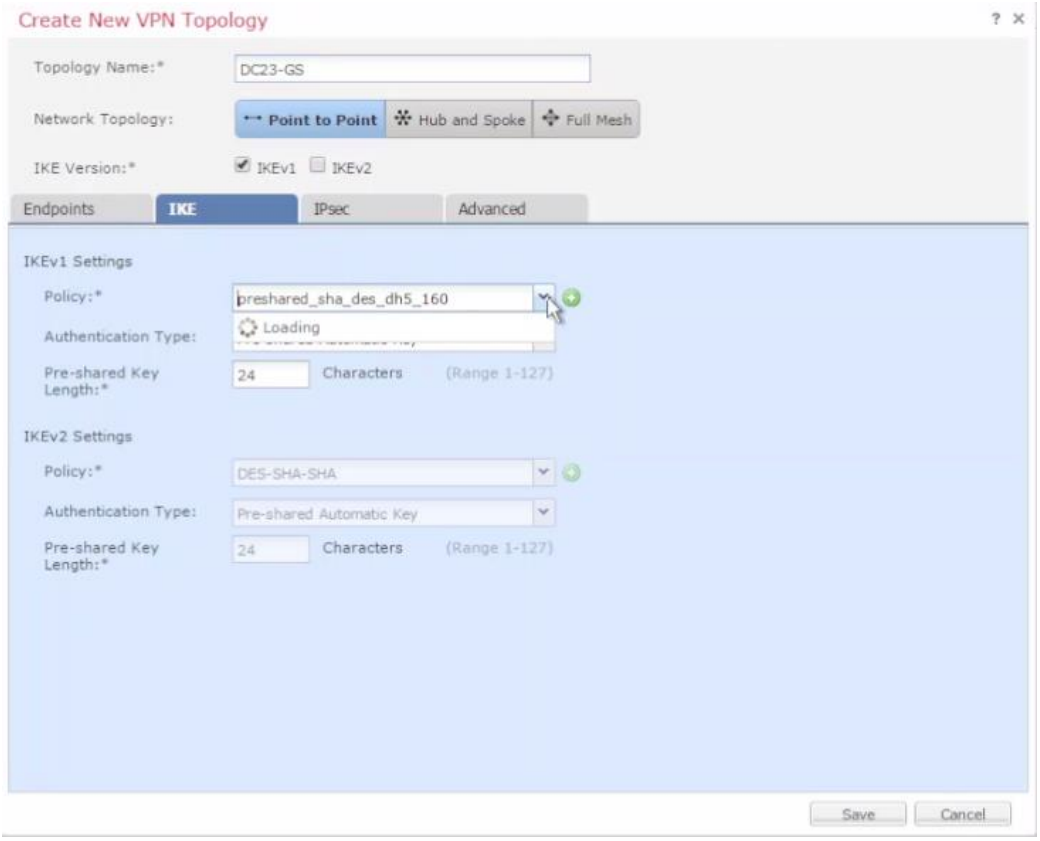
d. Gigabitethernet0/0
   i. Name: outside
   ii. Security zone: outside (create one if not there)
   iii. Ipv4: 20.20.20.1/24
e. Gigabitethernet0/1
   i. Name: inside
   ii. Security zone: inside (create one if not there)
   iii. Ipv4: 10.50.50.254/24



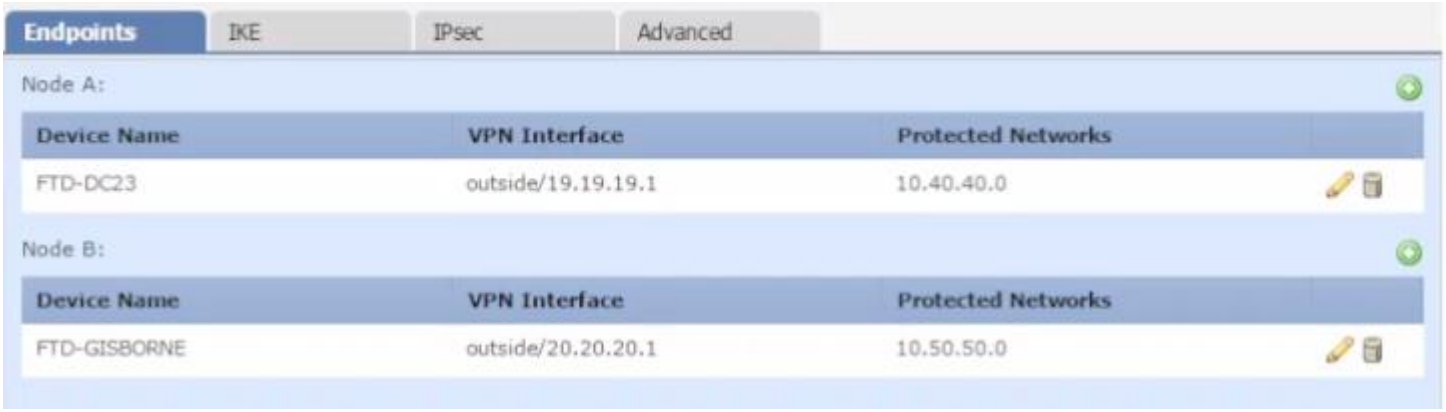
c. Click on static routes and point a default route for outside to SP
   i. Routing -> interface outside -> gateway -> 20.20.20..254



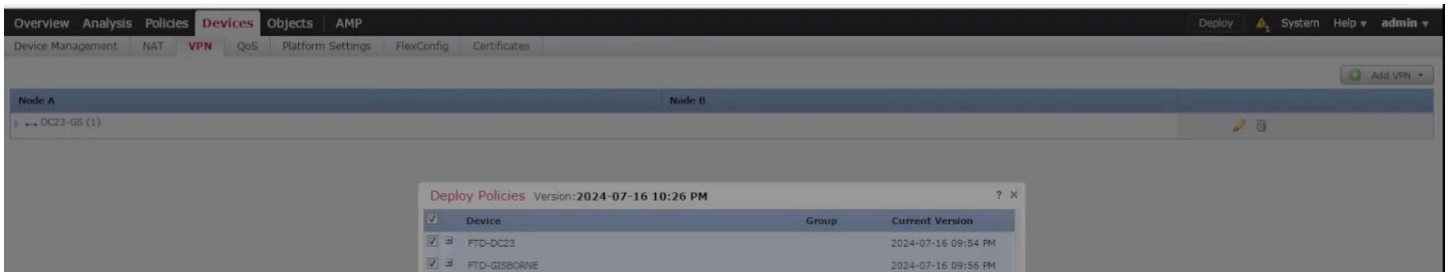
5) Configure VPN -> Device -> VPN -> ensure you do proper IKEV1 and IPSEC settings for what asked



6) Ensure you select Correct end points and protected networks



7) Once all the configs are done, Click on deploy – Make sure to select both FTD's



DC23 – Server 38

```
interface Ethernet0/0
 no shutdown
 ip address 10.40.40.1 255.255.255.0
ip route 0.0.0.0 0.0.0.0 10.40.40.254
```

Regional Office – Server 39

```
interface Ethernet0/0
 no shutdown
 ip address 10.50.50.1 255.255.255.0
ip route 0.0.0.0 0.0.0.0 10.40.40.254
```

8)Test traffic from Server 38 to Server 39, you should be able to ping.

Lab 7 : Configure Flex VPN between Napier & Nelson branch

- Tunnel network to be used is 192.168.100.0/24
- Pre-shared key to be used is Cisco123
- Tunnel should be native ipsec
- Ensure you exchange internal routes using EIGRP and AS to be used is 100

R-NP

```
!
interface Ethernet0/0
 no shutdown
 ip address 5.5.5.1 255.255.255.0
 duplex auto
!
interface Ethernet0/1
 no shutdown
 ip address 172.16.100.254 255.255.255.0
 duplex auto
!
ip route 0.0.0.0 0.0.0.0 5.5.5.254
```

R-NP

```
!
interface Ethernet0/0
 no shutdown
 ip address 4.4.4.1 255.255.255.0
 duplex auto
!
interface Ethernet0/1
 no shutdown
 ip address 172.16.200.254 255.255.255.0
 duplex auto!
!
ip route 0.0.0.0 0.0.0.0 4.4.4.254
```

Metro-Router

```
interface Ethernet0/0
 no shutdown
 ip address 4.4.4.254 255.255.255.0
 duplex auto
!
interface Ethernet0/1
 no shutdown
 ip address 5.5.5.254 255.255.255.0
 duplex auto
```

Branch1-PC

```
interface Ethernet0/0
 no shutdown
 ip address 172.16.100.1 255.255.255.0
 duplex auto
ip route 0.0.0.0 0.0.0.0 172.16.100.254
```

Branch2-PC

```
interface Ethernet0/0
 no shutdown
 ip address 172.16.200.1 255.255.255.0
 duplex auto
ip route 0.0.0.0 0.0.0.0 172.16.200.254
```

R-NP

```
crypto ikev2 proposal PROPOSAL
 encryption aes-cbc-128 3des
 integrity sha1 md5
 group 2 5
!
crypto ikev2 policy POLICY
 proposal PROPOSAL
!
crypto ikev2 keyring NAPIER
 peer NELSON
  address 4.4.4.1
  pre-shared-key Cisco123
 !
!
!
crypto ikev2 profile IKEV2-PROF
 match identity remote address 4.4.4.1 255.255.255.255
 authentication remote pre-share
 authentication local pre-share
 keyring local NAPIER
!
!
crypto ipsec transform-set TS esp-3des esp-sha-hmac
 mode tunnel
!
crypto ipsec profile IPSECPROF
 set transform-set TS
 set ikev2-profile IKEV2-PROF
interface Tunnel1
 no shutdown
 ip address 192.168.100.1 255.255.255.0
 tunnel source 5.5.5.1
 tunnel mode ipsec ipv4
 tunnel destination 4.4.4.1
 tunnel protection ipsec profile IPSECPROF

router eigrp 100
 network 172.16.100.0 0.0.0.255
 network 192.168.100.0
```

R-NP

```
crypto ikev2 proposal PROPOSAL
 encryption aes-cbc-128 3des
 integrity sha1 md5
 group 2 5
!
crypto ikev2 policy POLICY
 proposal PROPOSAL
!
crypto ikev2 keyring NAPIER
 peer NELSON
  address 4.4.4.1
  pre-shared-key Cisco123
 !
!
!
crypto ikev2 profile IKEV2-PROF
 match identity remote address 4.4.4.1 255.255.255.255
 authentication remote pre-share
 authentication local pre-share
 keyring local NAPIER
!
!
crypto ipsec transform-set TS esp-3des esp-sha-hmac
 mode tunnel
!
crypto ipsec profile IPSECPROF
 set transform-set TS
 set ikev2-profile IKEV2-PROF
interface Tunnel1
 no shutdown
 ip address 192.168.100.1 255.255.255.0
 tunnel source 5.5.5.1
 tunnel mode ipsec ipv4
 tunnel destination 4.4.4.1
 tunnel protection ipsec profile IPSECPROF

router eigrp 100
 network 172.16.100.0 0.0.0.255
 network 192.168.100.0
```

R-NELSON

```
crypto ikev2 proposal PROPOSAL
 encryption aes-cbc-128 3des
 integrity sha1 md5
 group 2 5
!
crypto ikev2 policy POLICY
 proposal PROPOSAL
!
crypto ikev2 keyring NAPIER
 peer NAPIER
  address 5.5.5.1
  pre-shared-key Cisco123
 !
crypto ikev2 profile IKEV2-PROF
 match identity remote address 5.5.5.1 255.255.255.255
 authentication remote pre-share
 authentication local pre-share
 keyring local NAPIER
!
crypto ipsec transform-set TS esp-3des esp-sha-hmac
 mode tunnel
!
crypto ipsec profile IPSECPROF
 set transform-set TS
 set ikev2-profile IKEV2-PROF
!
interface Tunnel1
 no shutdown
 ip address 192.168.100.2 255.255.255.0
 tunnel source 4.4.4.1
 tunnel mode ipsec ipv4
 tunnel destination 5.5.5.1
 tunnel protection ipsec profile IPSECPROF
!
!
router eigrp 100
 network 172.16.200.0 0.0.0.255
 network 192.168.100.0
```

Lab 8 : Configure Site-2-Site VPN between DC400 & DC500 branch

Pre-shared key to be used is Cisco123

Make sure CRM server can talk to server 50 and back and forth

INTERNET

```
interface Ethernet0/0
 no shutdown
 ip address 14.14.14.254 255.255.255.0
 duplex auto
!
interface Ethernet0/1
 no shutdown
 ip address 13.13.13.254 255.255.255.0
 duplex auto
```

DC-400

```
crypto isakmp policy 10
 encr 3des
 hash md5
 authentication pre-share
 group 2
crypto isakmp key Cisco123 address 14.14.14.1

crypto ipsec transform-set TS esp-3des esp-sha-hmac
 mode tunnel
!
access-list 102 permit ip 172.16.40.0 0.0.0.255 172.16.50.0 0.0.0.255

crypto map CMAP 10 ipsec-isakmp
 set peer 14.14.14.1
 set transform-set TS
 match address 102
interface Ethernet0/0
 no shutdown
 ip address 13.13.13.1 255.255.255.0
 duplex auto
 crypto map CMAP
!
interface Ethernet0/1
 no shutdown
 ip address 172.16.40.254 255.255.255.0
 duplex auto
ip route 0.0.0.0 0.0.0.0 13.13.13.254
```

DC-500

```
crypto isakmp policy 10
 encr 3des
 hash md5
 authentication pre-share
 group 2
crypto isakmp key Cisco123 address 13.13.13.1

crypto ipsec transform-set TS esp-3des esp-sha-hmac
 mode tunnel
access-list 102 permit ip 172.16.50.0 0.0.0.255 172.16.40.0 0.0.0.255
access-list 102 permit ip 172.16.50.0 0.0.0.255 172.16.40.0 0.0.0.255

crypto map CMAP 10 ipsec-isakmp
 set peer 13.13.13.1
 set transform-set TS
 match address 102

interface Ethernet0/0
 no shutdown
 ip address 14.14.14.1 255.255.255.0
 duplex auto
 crypto map CMAP

interface Ethernet0/1
 no shutdown
 ip address 172.16.50.254 255.255.255.0
 duplex auto
ip route 0.0.0.0 0.0.0.0 14.14.14.254
```

Server-50

```
interface Ethernet0/0
 no shutdown
 ip address 172.16.50.1 255.255.255.0
 duplex auto

ip route 0.0.0.0 0.0.0.0 172.16.50.254
```

Server-50

```
interface Ethernet0/0
 no shutdown
 ip address 172.16.40.1 255.255.255.0
 duplex auto

ip route 0.0.0.0 0.0.0.0 172.16.50.254
```

Lab 9 : Configure Dot1x and Mab for Customer service-PC & IT-PC

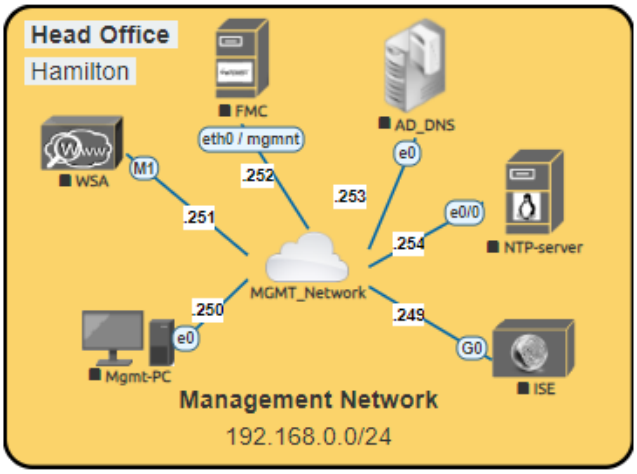
DHCP pool for IT-PC should be 10.10.10.0/24 VLAN 10

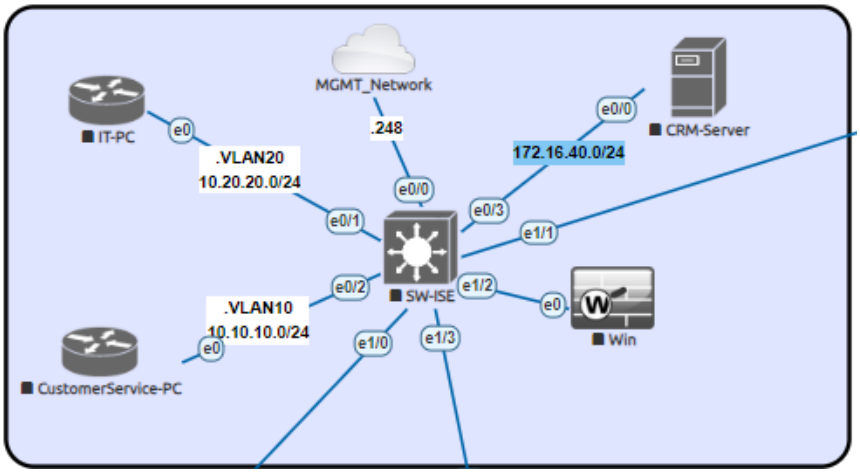
DHCP pool for Customer service should be 10.20.20.0/24 VLAN 20

Push DACL to IT-PC so that it can telnet CRMSERVER

Push DACL to Customer service so that it can browse the CRMSERVER

Ensure Customer service user is authenticated using ISE Local DB and username should be cspc/Cisco123





- ON IT PC, make sure you're able to get an IP from DHCP
- ON CustomerService-PC, make sure you're able to get an IP from DHCP

SW-ISE

```
ip dhcp excluded-address 10.10.10.1
ip dhcp excluded-address 10.20.20.1
ip dhcp pool CS
 network 10.10.10.0 255.255.255.0
 default-router 10.10.10.1
!
ip dhcp pool IT
 network 10.20.20.0 255.255.255.0
 default-router 10.20.20.1
dot1x system-auth-control

interface Ethernet0/1
 no shutdown
 switchport access vlan 20

interface Ethernet0/2
 no shutdown
 switchport access vlan 10

interface Ethernet0/0
 no shutdown
 switchport access vlan 100
 switchport mode access
 duplex auto

interface Vlan10
 no shutdown
 ip address 10.10.10.1 255.255.255.0
!
interface Vlan20
 no shutdown
 ip address 10.20.20.1 255.255.255.0
!
interface Vlan100
 no shutdown
 ip address 192.168.0.248 255.255.255.0

aaa new-model

aaa group server radius ISE-SVRS
 server name ISE1
!
aaa authentication dot1x default group ISE-SVRS
aaa authorization network default group ISE-SVRS
dot1x system-auth-control

radius server ISE1
 address ipv4 192.168.0.249 auth-port 1812 acct-port 1813
 key Cisco123
```

SW-ISE

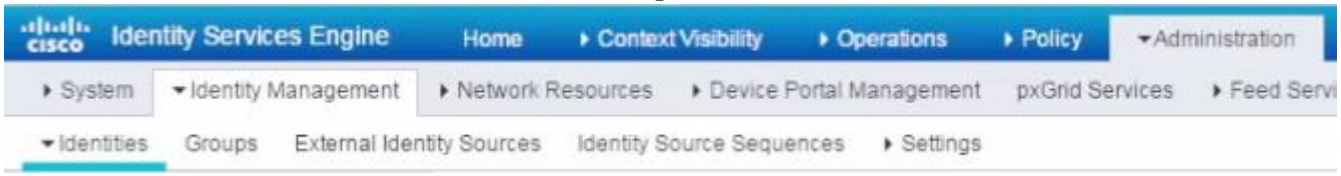
```
ip route 0.0.0.0 0.0.0.0 192.168.0.254

!
interface Ethernet0/1
 no shutdown
 switchport access vlan 20
 switchport mode access
 duplex auto
 authentication order mab dot1x
 authentication priority mab dot1x
 authentication port-control auto
 mab
 dot1x pae authenticator
!
interface Ethernet0/2
 no shutdown
 switchport access vlan 10
 switchport mode access
 duplex auto
 authentication order dot1x mab
 authentication priority dot1x mab
 authentication port-control auto
 mab
 dot1x pae authenticator
!
```

For DOT1X PC

1. Login to ISE
    a. Administration -> Network Device Groups
    b. Add Group -> Name : SWITHCES -> Parent group -> All Devicetypes

2. Add your Switch in Network Devices
    a. Administration -> Network Devices
    b. Name : SW
    c. IP address : 192.168.0.248
    d. Device Type : SWITCHES
    e. Protocol: RADIUS
    f. Shared Secret Password: cisco123

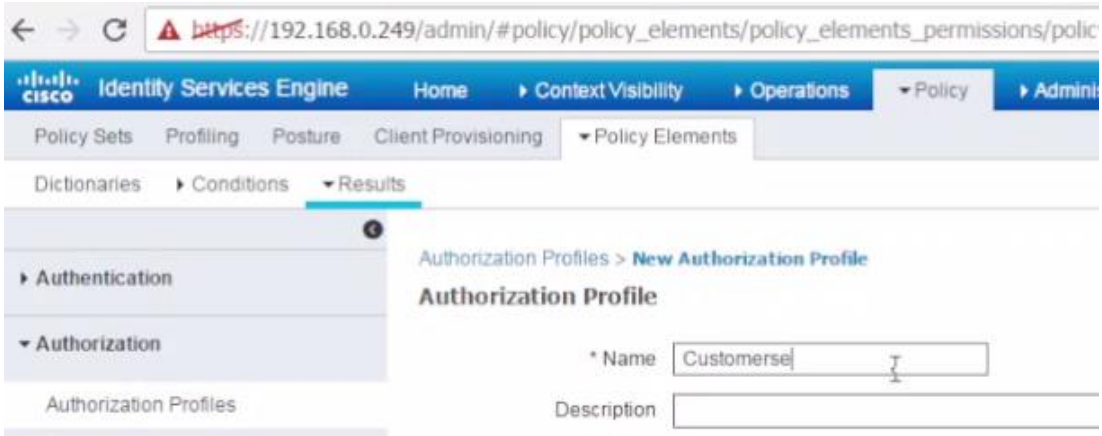
3. Configure the Local Authentication Database (Groups)
   a. Administration -> Identity Management -> Groups -> User Identity Groups
      i. Name: CustomerserviceGroup



4. Configure the Local Authentication Database (Users)
   a. Administration -> Identity Management -> Identities

      i. **Username: ccuser**
      ii. **Password: Cisco123**
      iii. **Group: CustomerserviceGroup**

5. Create Authorization Profiles to define characteristics that need to pushed to the Network Device



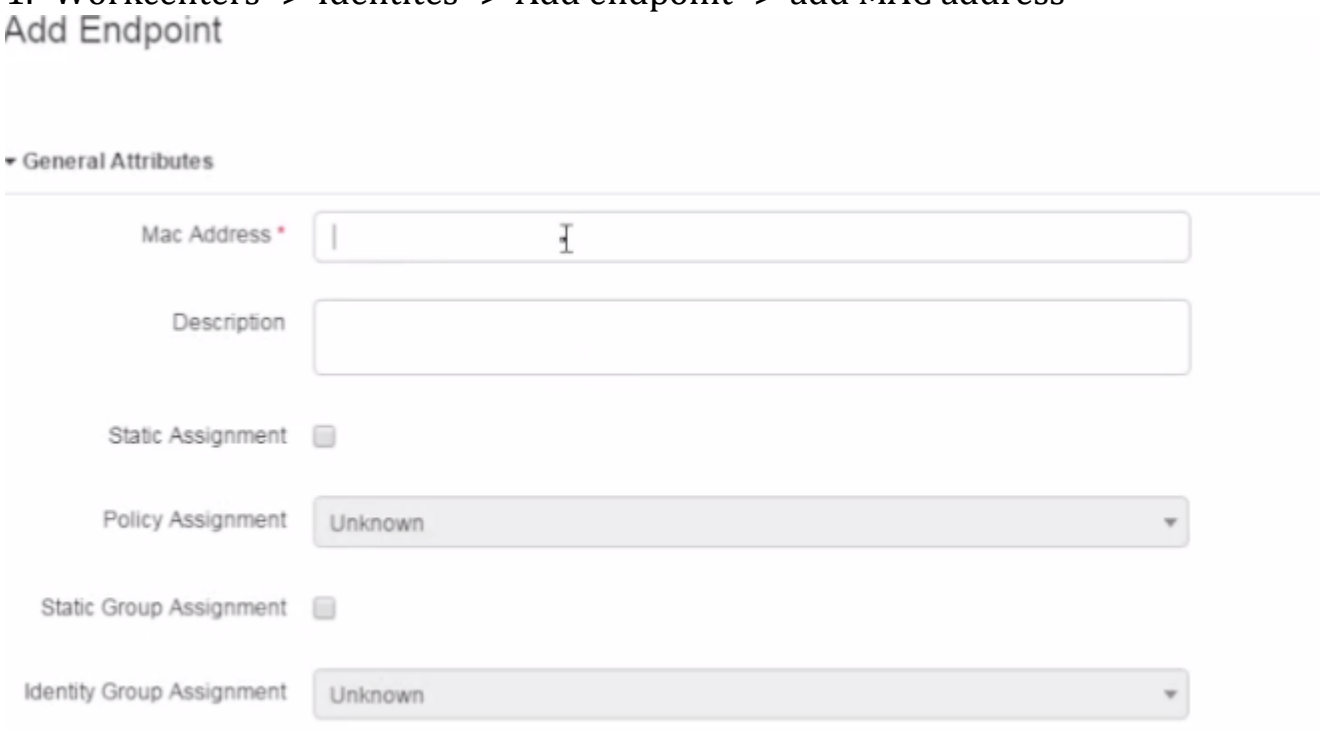
   a. Policy -> Policy Elements -> Results -> Authorization -> Authorization Profiles -> Add
      i. Name: IT-AUTH-PROF
      ii. VLAN ID: 20
      iii. Name: CC-AUTH-PROF
      iv. VLAN ID: 10

6. Authorization Policy to link the Groups to the appropriate Authorization Profile
   a. Policy -> Default -> Authorization Policy -> Insert at the Top
   Name: **CC-AUTH-POLICY**
      a. GROUP: CustomerserviceGroup
      b. Authentication Type: Wired_802.1x
      c. Network Device: SWITCHES
      i. SALES- CC-AUTH-PROF

7. On dot1x PC, start wired LAN service, and in your LAN settings, ensure your turn this settings off. Your PC will authenticate using dot1x

For MAB PC

1. Workcenters -> Identites -> Add endpoint -> add MAC address



2. Create Authorisation policy with below parameters and save, your MAB PC will be authenticated.

Lab 10: Configure NTP server on your NTP router

NTP should use authentication

Key should be 100

Password cisco123

Configure NTP client config on R17 & R18

Make sure you have proper clock time zones set on your routers i.e Clock time zone MEL 8

NTP-Server router

```
clock timezone GST 4
interface Ethernet0/0
 no shutdown
 ip address 192.168.0.254 255.255.255.0
ntp authentication-key 100 md5 cisco
ntp authenticate
ntp trusted-key 100
ntp master 2
```

R17

```
clock timezone IST 5 30
interface Ethernet0/0
 no shutdown
 ip address 192.168.0.245 255.255.255.0

ntp authentication-key 100 md5 cisco
ntp authenticate
ntp trusted-key 100
```

R18

```
clock timezone IST 5 30
interface Ethernet0/0
 no shutdown
 ip address 192.168.0.246 255.255.255.0

ntp authentication-key 100 md5 cisco
ntp authenticate
ntp trusted-key 100
```

Lab 11: Configure SYSLOG on R9

Ensure logs are sent to log server located in management PC

R9

```
logging host 192.168.0.252
!
service timestamps log datetime
```

Lab 12: Configure WSA redirection on Call center router

CC-team lead should be able to access Call center Dashboard

IT-admin should be able to access Call center manager

CallCenter-R

```
ip host www.dashboard.com 100.100.100.100
ip host www.manager.com 100.100.100.200
ip name-server 192.168.0.240

access-list 1 permit 192.168.0.251
access-list 101 permit tcp any any eq www

ip wccp 20 redirect-list 101 group-list 1 password 0 cisco

nterface Ethernet0/0
 no shutdown
 ip address 172.16.10.254 255.255.255.0
!
interface Ethernet0/1
 no shutdown
 ip address 192.168.0.240 255.255.255.0
!
interface Ethernet0/2
 no shutdown
 ip address 10.20.20.254 255.255.255.0
 ip wccp 20 redirect in
!
interface Ethernet0/3
 no shutdown
 ip address 10.10.10.254 255.255.255.0
 ip wccp 20 redirect in

router eigrp 100
 network 10.10.10.0 0.0.0.255
 network 10.20.20.0 0.0.0.255
```

Enterprise

```
interface Ethernet0/0
 no shutdown
 ip address 172.16.20.1 255.255.255.0
!
interface Ethernet0/1
 no shutdown
 ip address 172.16.10.1 255.255.255.0 network 172.16.10.0 0.0.0.255
 network 192.168.0.0
router eigrp 100
 network 172.16.10.0 0.0.0.255
 network 172.16.20.0 0.0.0.255
```

Enterprise

```
interface Ethernet0/0
 no shutdown
 ip address 100.100.100.254 255.255.255.0
!
interface Ethernet0/1
 no shutdown
 ip address 172.16.20.254 255.255.255.0
router eigrp 100
 network 100.100.100.0 0.0.0.255
 network 172.16.20.0 0.0.0.255
!
```

CallCenter-Manager Server

```
interface Ethernet0/0
 no shutdown
 ip address 100.100.100.200 255.255.255.0

ip http server
ip http authentication local

ip route 0.0.0.0 0.0.0.0 100.100.100.254
```

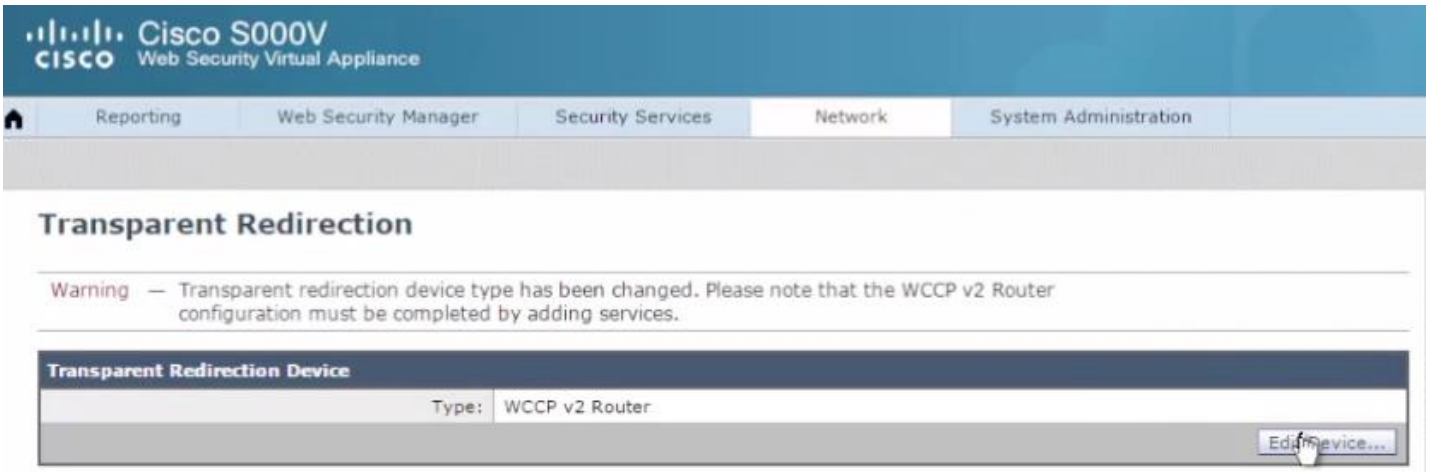
CallCenter-Dashboard-Server

```
interface Ethernet0/0
 no shutdown
 ip address 100.100.100.100 255.255.255.0
ip http server
ip http authentication local

ip route 0.0.0.0 0.0.0.0 100.100.100.254
```

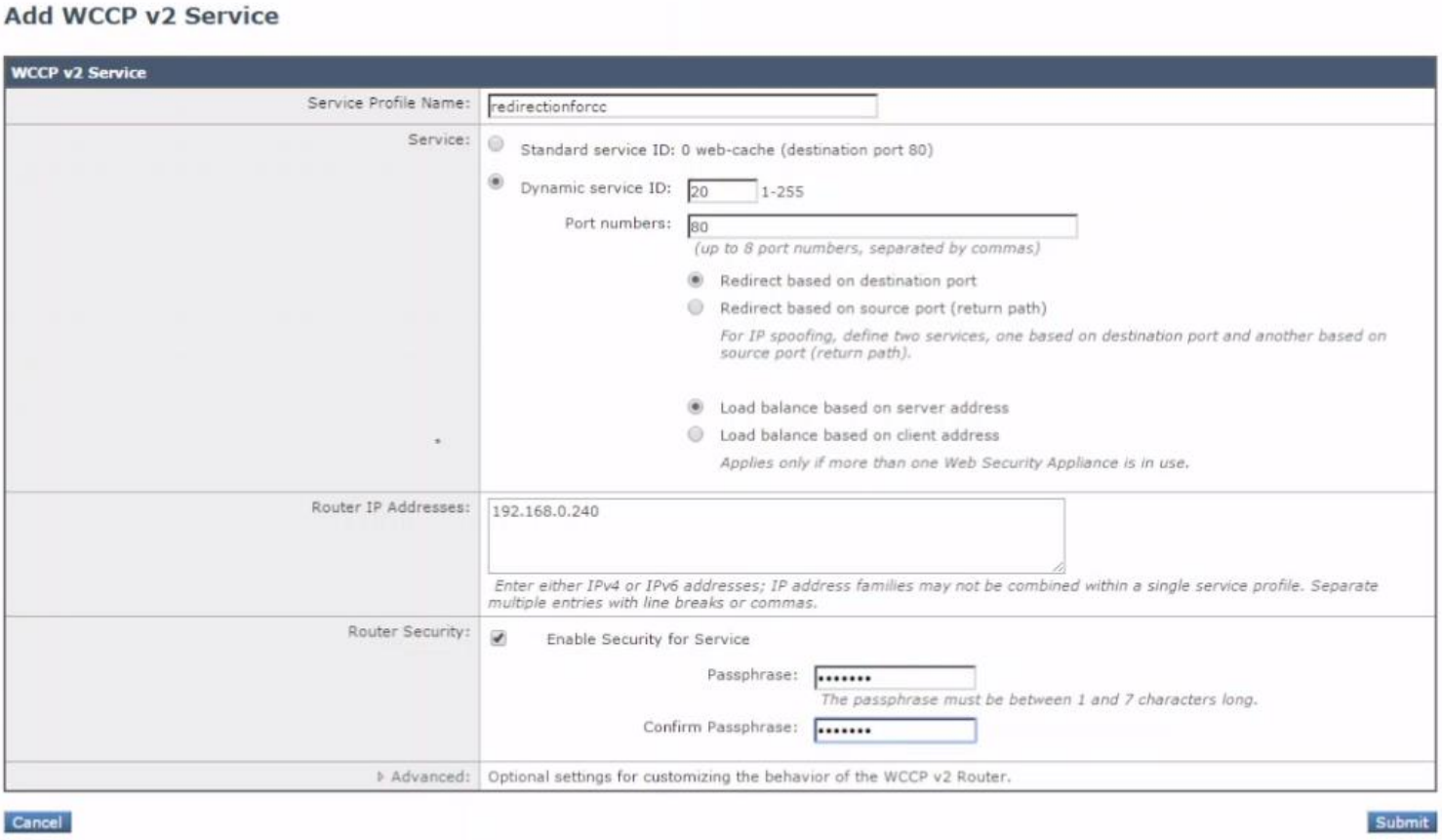
On WSA

1) Create WCCP interface
   a. Network -> Type -> Wccp V2 Router -> Submit

2) Edit Device



3) Add all relevant details as below



4) Add reverse static routes

5) Create Identification profile

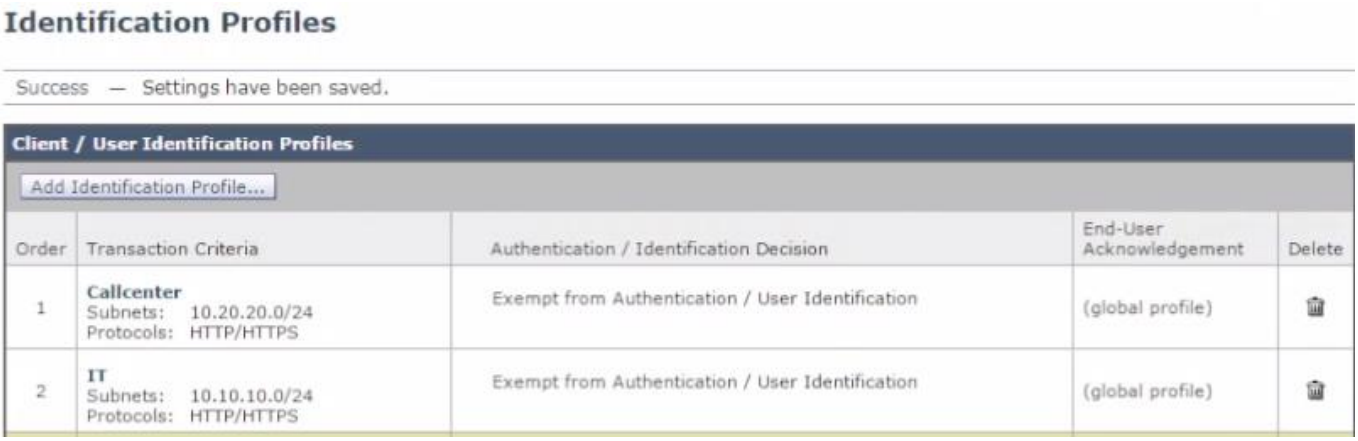
Web Security manager -> Identification profile -> Add profile

Name: IT

Define members by subnet: 10.10.10.0/24

Name: CallCenter

Define members by subnet: 10.20.20.0/24



6) Create Custom URL Categories

Web Security manager -> Custome and External URL Categories -> Add Category

Name: ITURL

Sites: www.manager.com

Name: CCURL

Sites: www.dashboard.com

7) Create Access-policy

Web Security manager -> Access-policy -> Add Group

Name: ITpolicy

Select Identification profile: IT

URL Category : ITURL (Allow)

Name: CallCenterpolicy

Define members by subnet: CallCenter

URL Category : CCURL (Allow)

Lab 13: Optimization/Troubleshooting

- You have been asked to optimize zone-based FW for DC100, so that only ICMP traffic from outside to inside should be inspected.
- Users on win machine are not able to connect to DC200 server on port 8080, troubleshoot and fix the issue.

ServerDC-100

```
interface Ethernet0/0
 no shutdown
 ip address 172.16.60.1 255.255.255.0
ip route 0.0.0.0 0.0.0.0 172.16.60.254
```

ServerDC-200

```
interface Ethernet0/0
 no shutdown
 ip address 172.16.70.1 255.255.255.0
ip route 0.0.0.0 0.0.0.0 172.16.70.254
```

R40

```
class-map type inspect match-any outside-to-inside
 match protocol icmp
!
policy-map type inspect policy-outside-to-inside
 class type inspect outside-to-inside
  inspect
 class class-default
  drop
!
zone security OUTSIDE
zone security INSIDE
zone-pair security outside-inside source OUTSIDE destination INSIDE
 service-policy type inspect policy-outside-to-inside
interface Ethernet0/0
 no shutdown
 ip address 192.168.0.44 255.255.255.0
 zone-member security OUTSIDE
!
interface Ethernet0/1
 no shutdown
 ip address 172.16.60.254 255.255.255.0
 zone-member security INSIDE
```

R4

```
interface Ethernet0/0
 no shutdown
 ip address 192.168.0.5 255.255.255.0
!
interface Ethernet0/1
 no shutdown
 ip address 172.16.70.254 255.255.255.0
```

ServerDC-200

```
ip http server
ip http port 8080
ip http authentication local
no ip http secure-server
```

SW-ISE

```
interface Ethernet1/1
 no shutdown
 switchport access vlan 100
 switchport mode access
 duplex auto
interface Ethernet1/2
 no shutdown
 switchport access vlan 100
 switchport mode access
 duplex auto
```