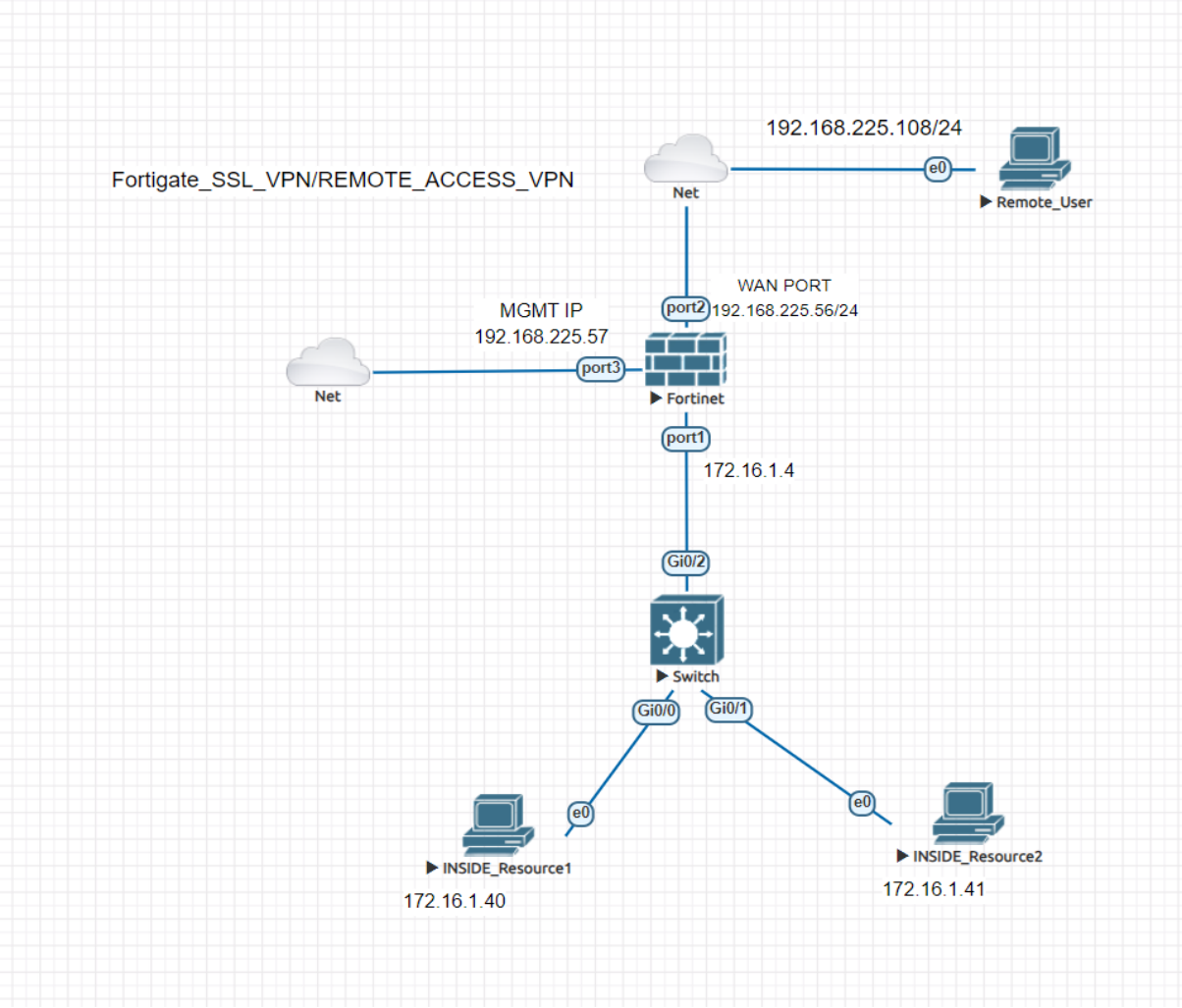
Fortigate_SSL_VPN/REMOTE_ACCESS_VPN

1. Consider a below topology for SSL_VPN_LAB.

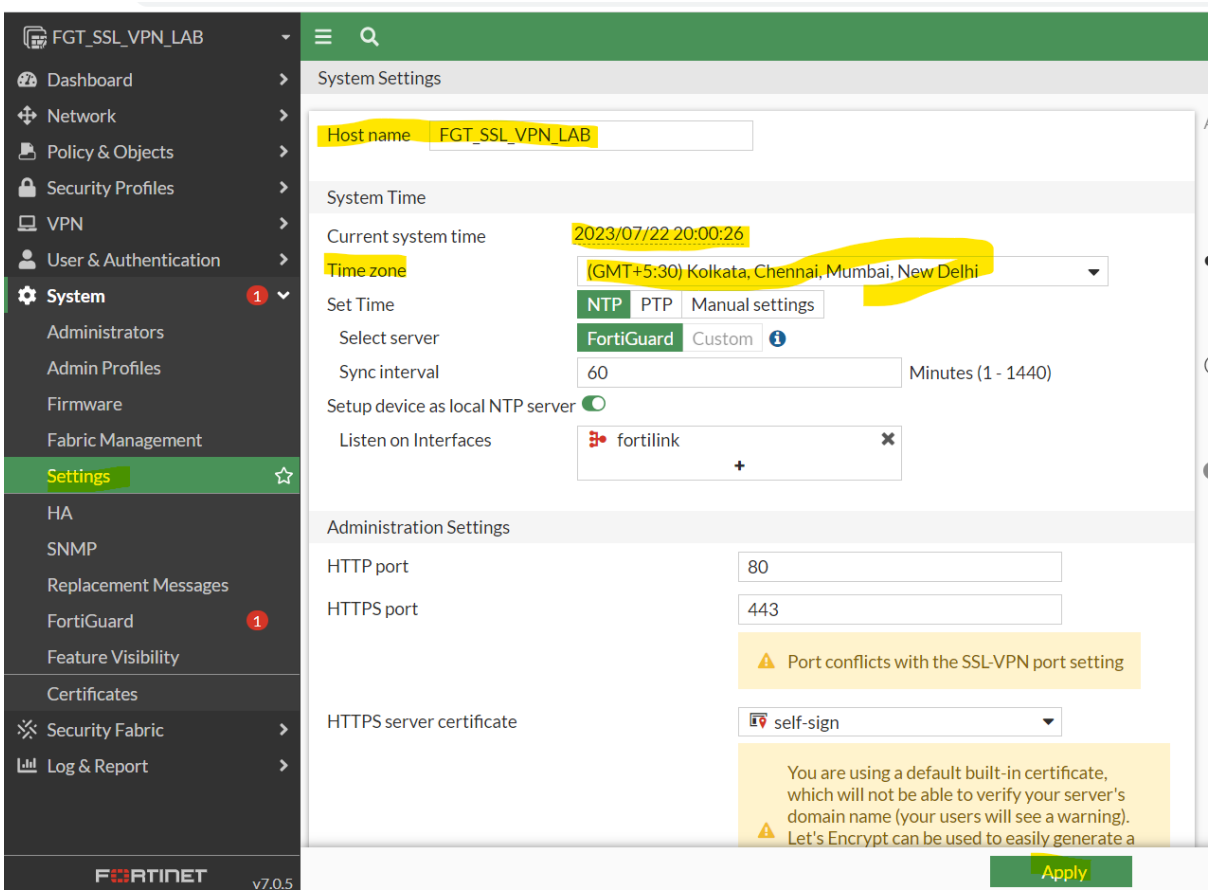


2. Now let us first take GUI access of FortiGate firewall.
   Management IP – 192.168.225.57 – so enter http://192.168.225.57 in the browser

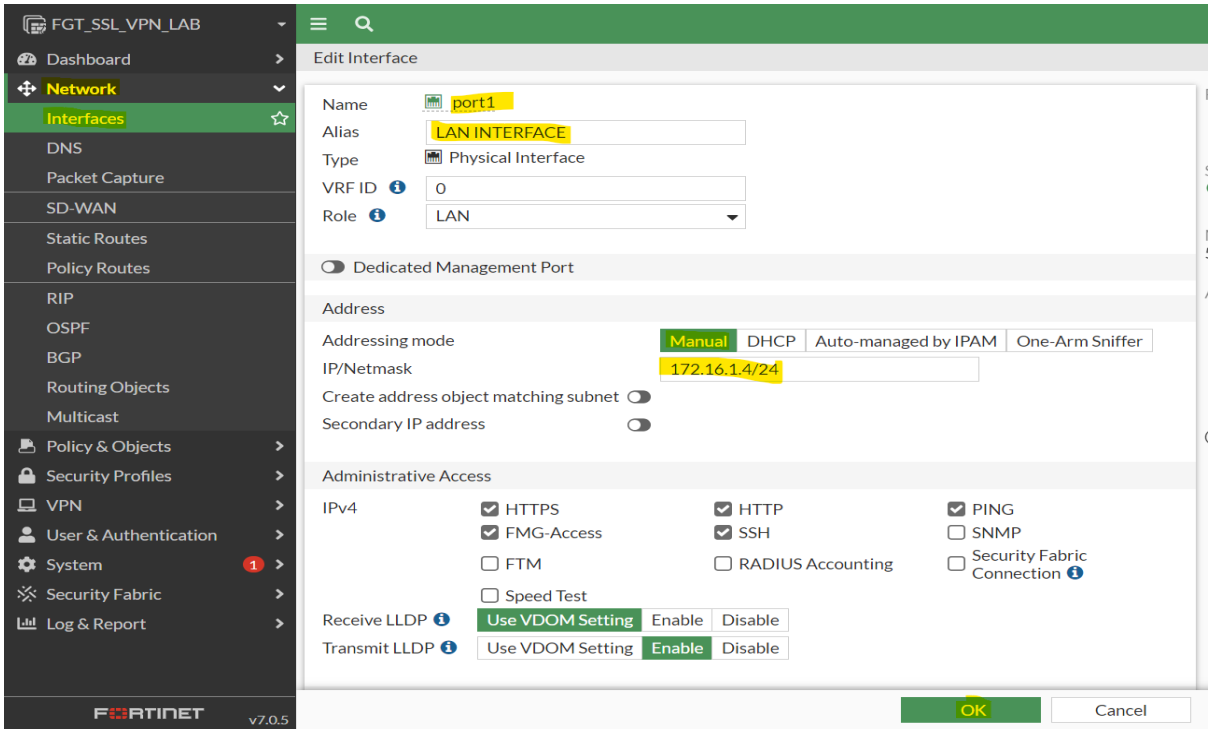
```
FortiGate-VM64-KVM login: admin
Password:
Welcome!

FortiGate-VM64-KVM # get system interface
== [ port1 ]
name: port1   mode: dhcp    ip: 0.0.0.0 0.0.0.0   status: up    netbios-forward:
 disable    type: physical   ring-rx: 0   ring-tx: 0   netflow-sampler: disable
   sflow-sampler: disable    src-check: enable    explicit-web-proxy: disable
 explicit-ftp-proxy: disable    proxy-captive-portal: disable    mtu-override: d
isable    wccp: disable    drop-overlapped-fragment: disable    drop-fragment: d
isable
== [ port2 ]
name: port2   mode: static    ip: 0.0.0.0 0.0.0.0   status: up    netbios-forwar
d: disable    type: physical   ring-rx: 0   ring-tx: 0   netflow-sampler: disabl
e    sflow-sampler: disable    src-check: enable    explicit-web-proxy: disable
   explicit-ftp-proxy: disable    proxy-captive-portal: disable    mtu-override:
 disable    wccp: disable    drop-overlapped-fragment: disable    drop-fragment:
 disable
== [ port3 ]
name: port3   mode: dhcp    ip: 192.168.225.57 255.255.0.0   status: up    netbi
os-forward: disable    type: physical   ring-rx: 0   ring-tx: 0   netflow-sample
r: disable    sflow-sampler: disable    src-check: enable    explicit-web-proxy:
 disable    explicit-ftp-proxy: disable    proxy-captive-portal: disable    mtu-
override: disable    wccp: disable    drop-overlapped-fragment: disable    drop-
fragment: disable
```

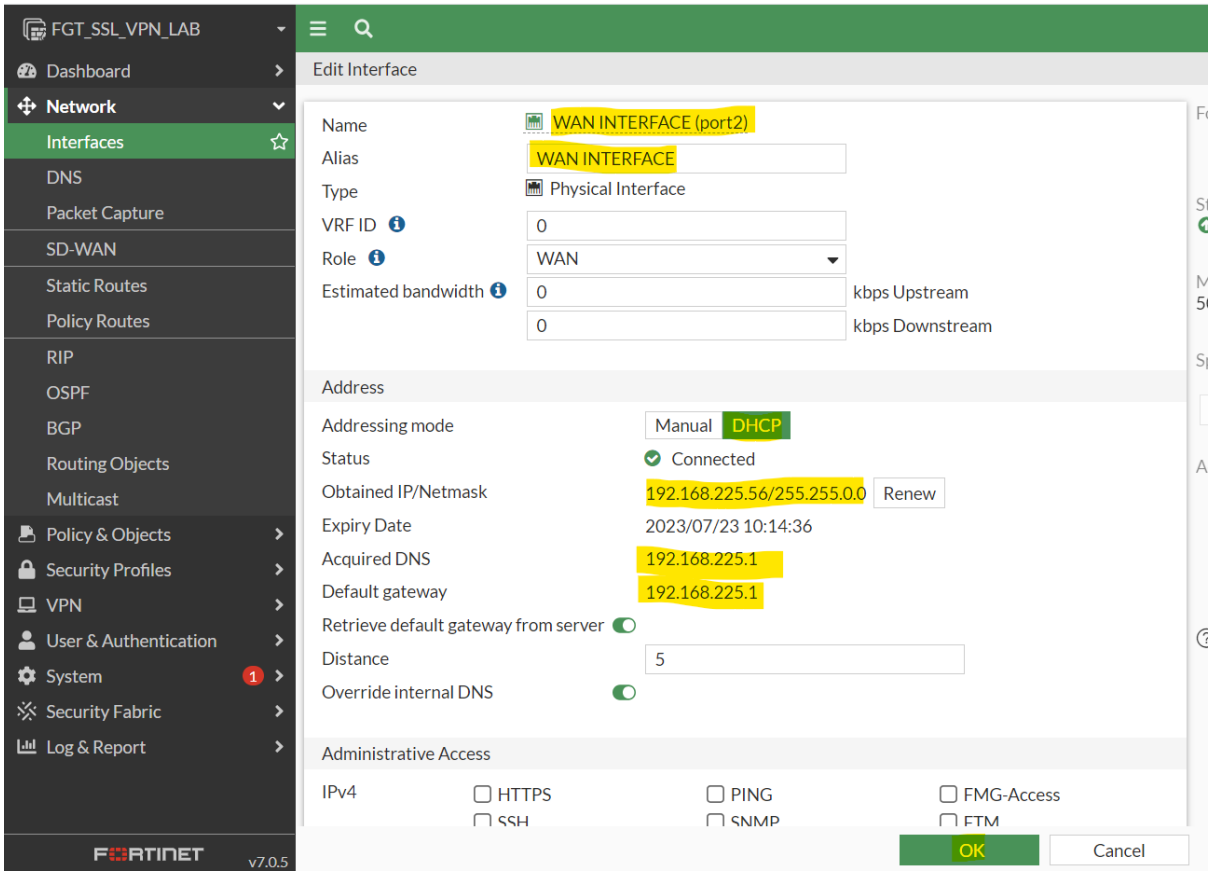
3. Once we get the GUI access, then do the basic configuration such as setting hostname, time zone, etc.



4. Let us first configure the interface.
   Go to Network > Interface > Edit Port1

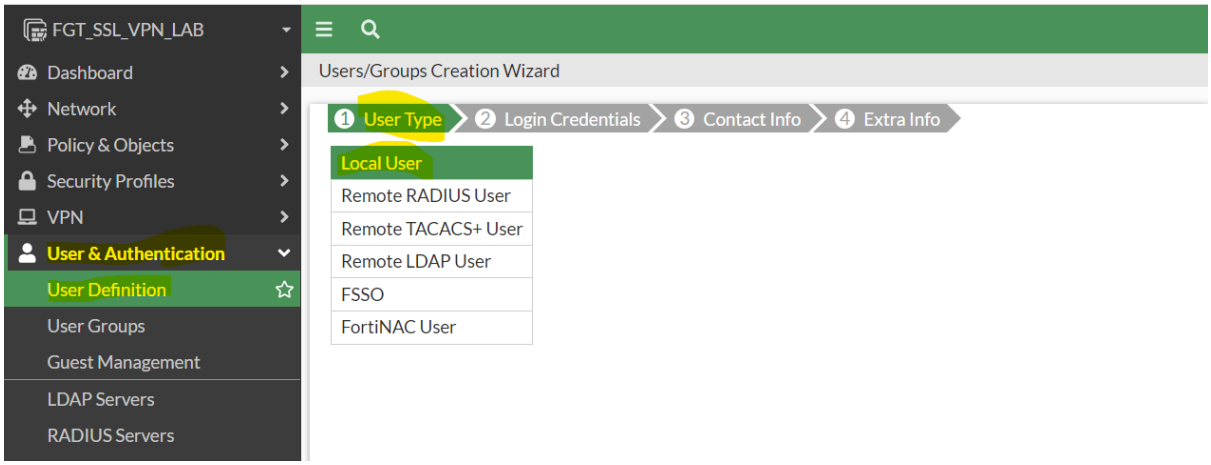


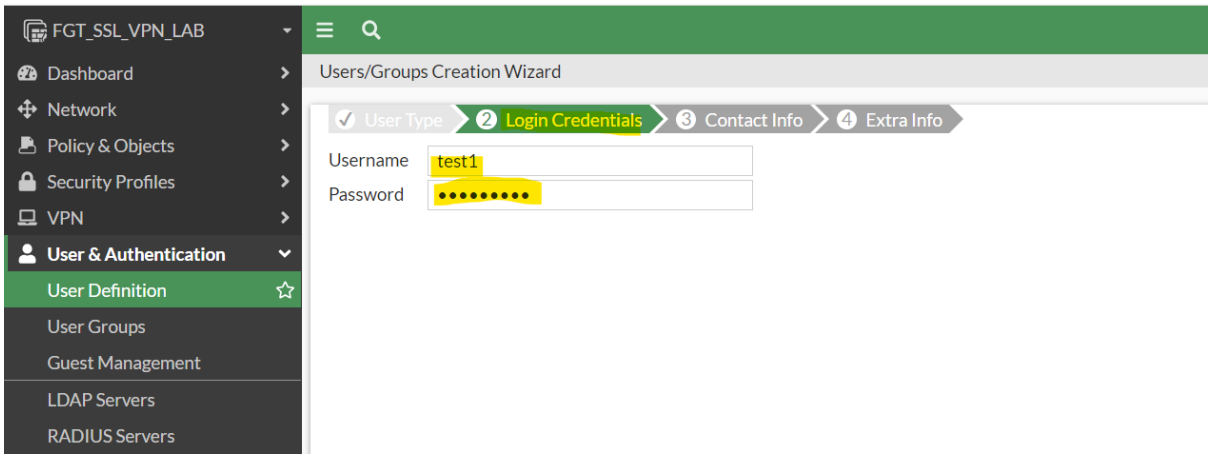
Go to Network > Interface > Edit Port2



5. Now we have to define the users in the database. There are two methods that we can use. First is that we can create users if firewall database or we can integrate firewall with the Active Directory.
   We will define the users by the first method.

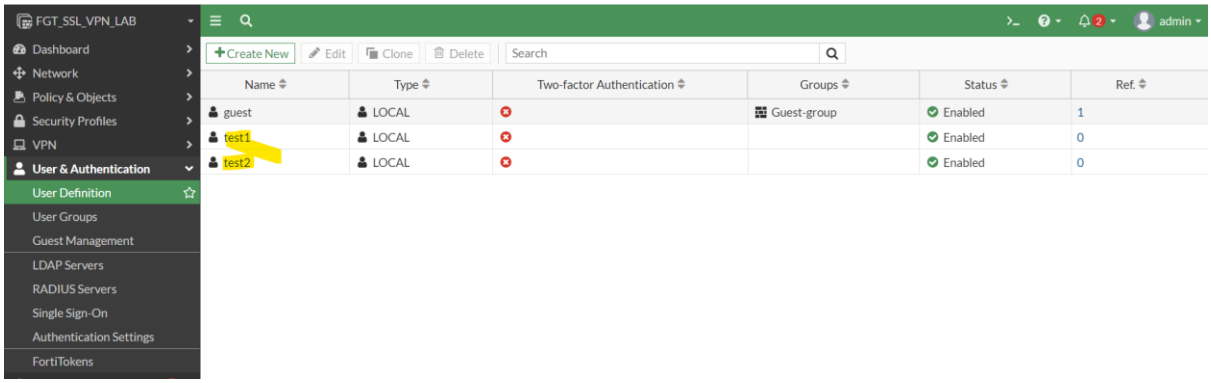
   Go to Users and Authentication > user definition > Create New
   In User Type – Select Local User > click on Next
   Add Username and Password > Click on Next



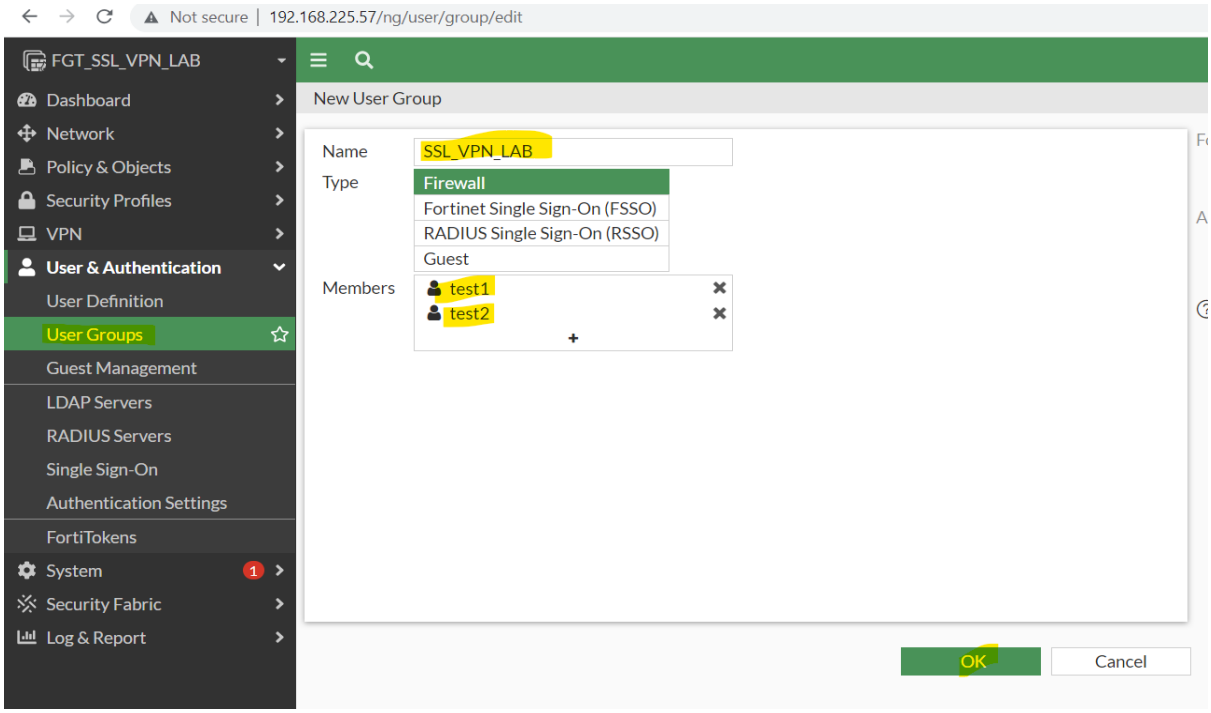


Click On Next and Submit

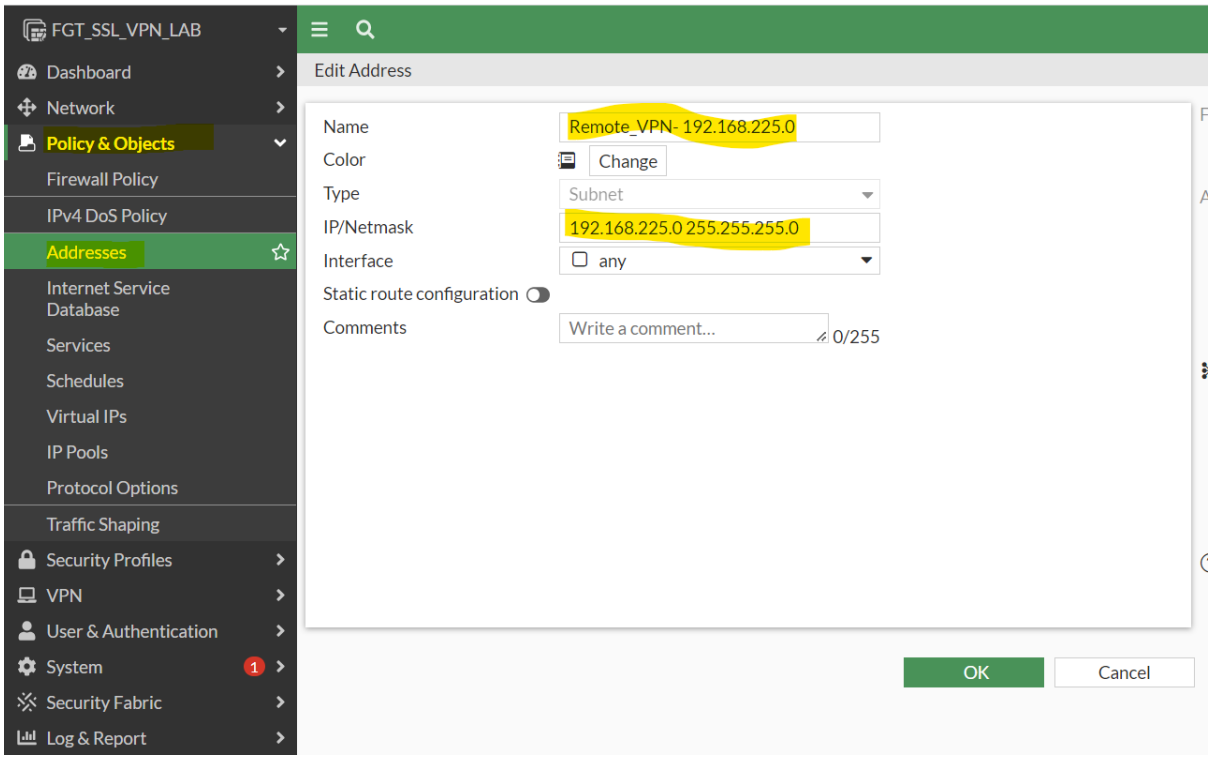
Now create another user.



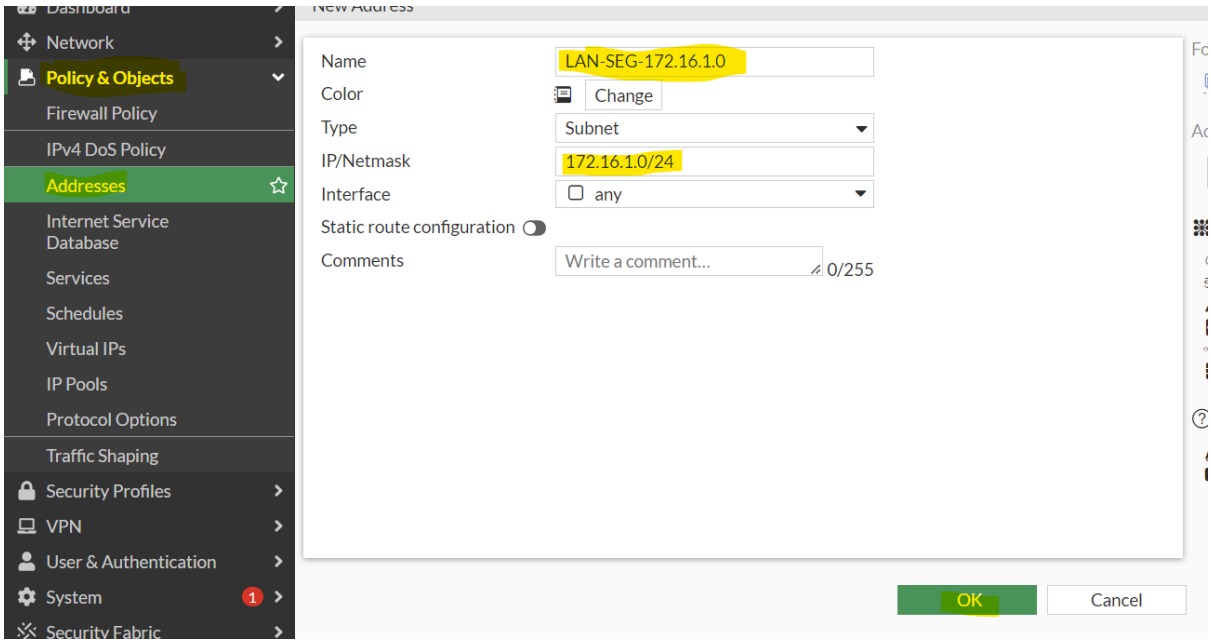
6. Now we have to create a User Group and assign the users that we created in it.
   Go to User Groups > Create new



7. Now we have to create an object so that the remote users which are trying to access then they should get the IP from the subnet that we define in the object.
   Go to Policy and objects > Create New



Now we need to create another object as LAN segment



8. Now let us move to the configuration of SSL_VPN
   Go to VPN > VPN Portals.
   VPN Portal allow us to perform VPN tunnel configurations and specific settings.
   I. Name – here we have to define the name – SSL_VPN_LAB_PORTAL
   II. We have the option to limit the one connection at a time – Disabled it currently
   III. Tunnel Mode – There are two options Tunnel and Split.

In Split Tunnel – traffic intended for the LAN side will only route through firewall whereas the traffic which is not intended for LAN will route through its internet.
In Tunnel – All the traffic will route through firewall.

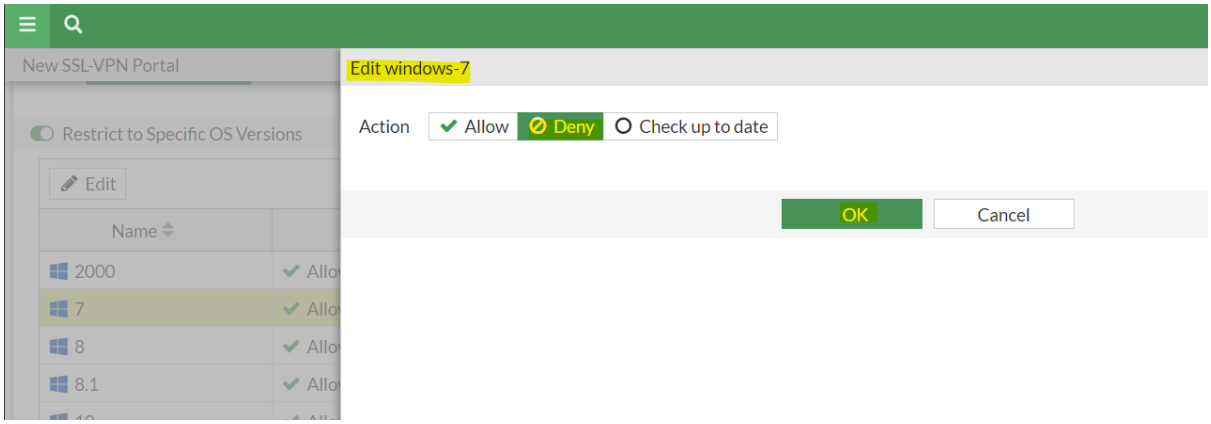
IV. Routing address override – Here we have to define that which subnet in the LAN we have to allow for the remote users to access – 172.16.1.0/24

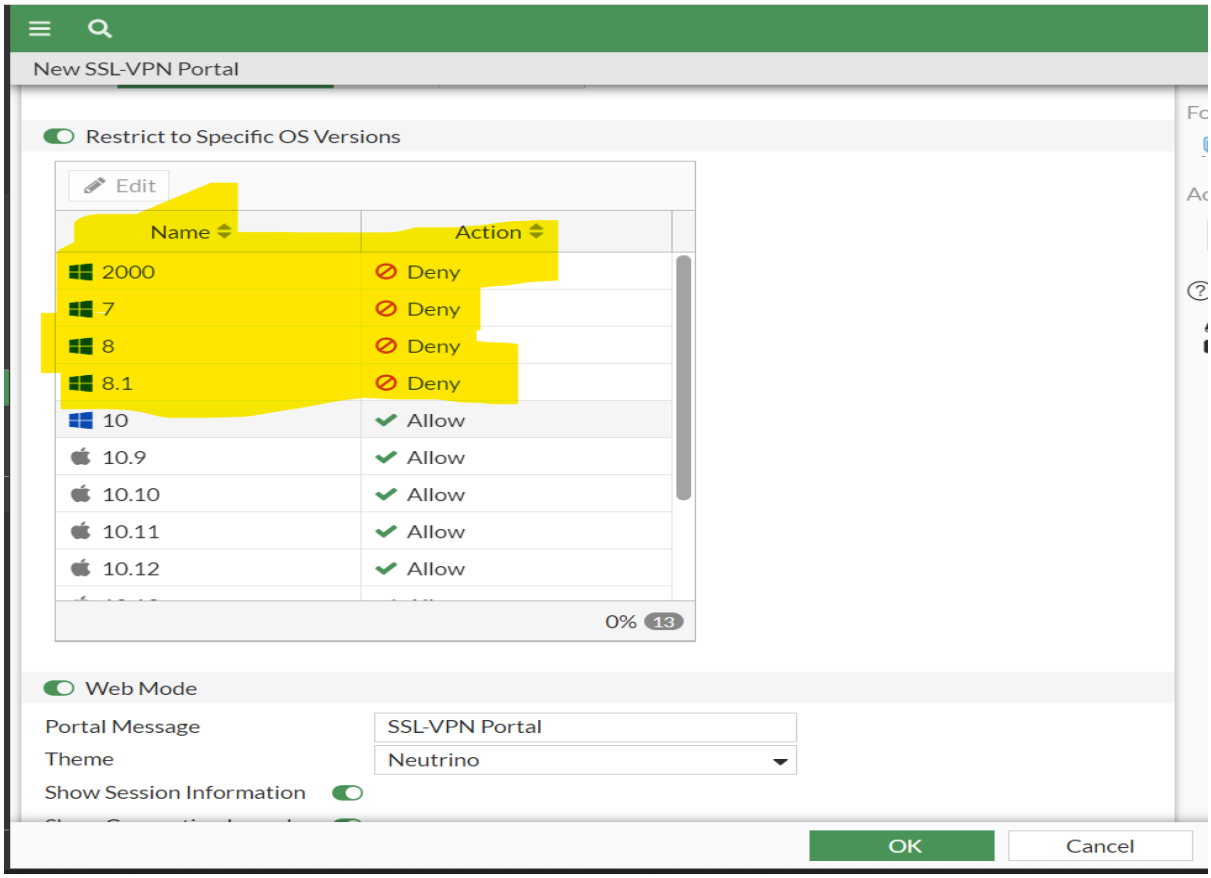
V. Source IP pools – Here we have to define that which IP address the remote user will carry – 192.168.199.0/24

VI. Tunnel Mode Client Options – Here we can allow or disallow client to save password, client to connect automatically, client to keep connections alive, DNS split tunnelling.

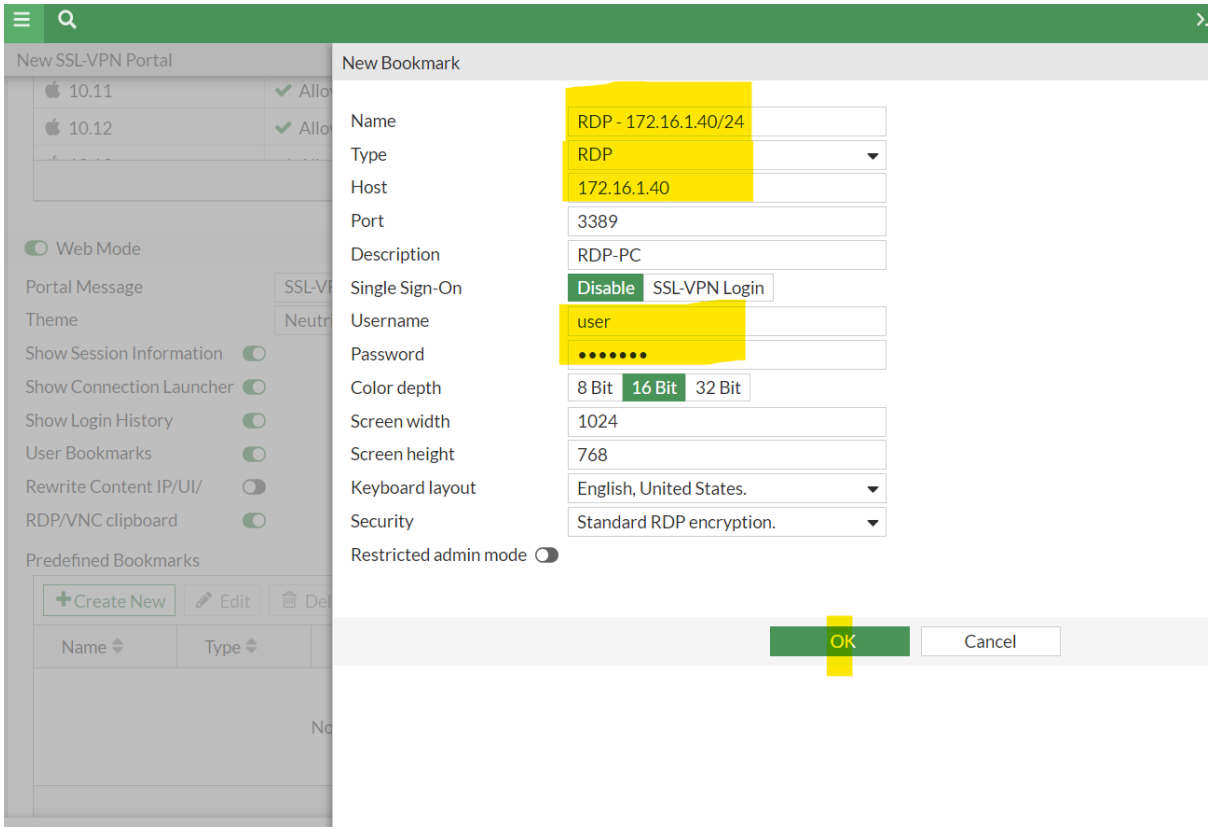
VII. Host Check – if enabled we can select that what checks should be done, whether to do antivirus check on host or firewall checks or both.

VIII. Restrict to specific OS versions – Here we can define which OS can be allowed to access the resource and which OS should not be allowed.
So, in our case the remote PC that we are using is of windows 10 OS version. So let us disable the access for Windows7,8 machines.





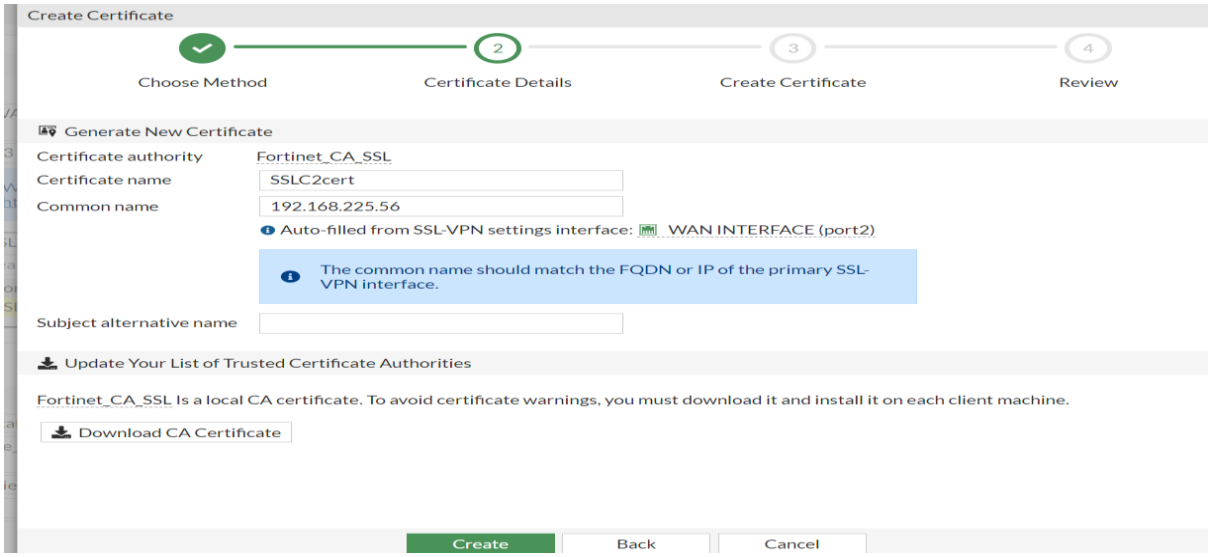
IX. Web Mode – It is clientless VPN which allow users to access the resource without agent installed on their machine.
So here let us enable the web mode for one of the resources in our internal network.
Click on Bookmarks > create new



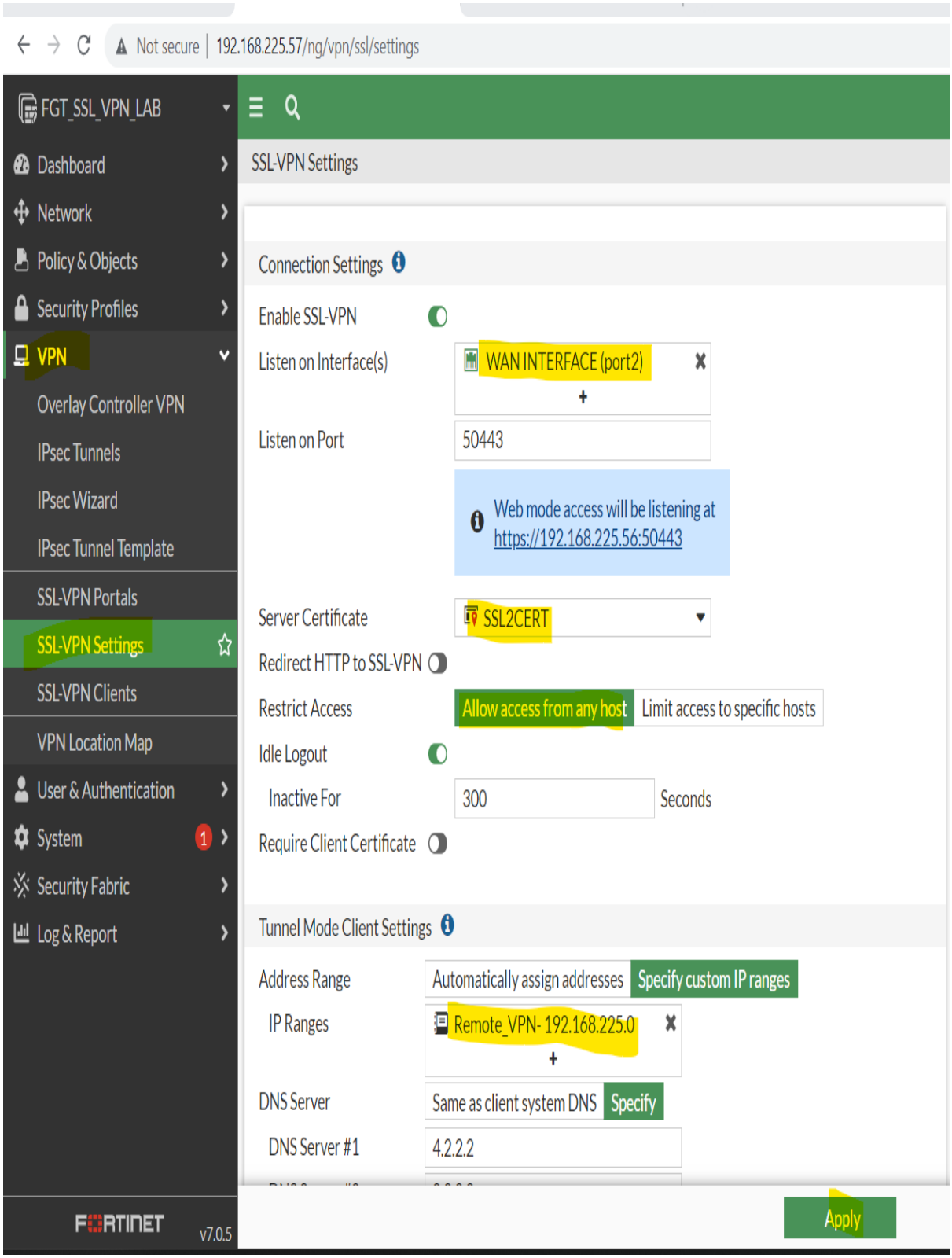
X. Click on Ok.

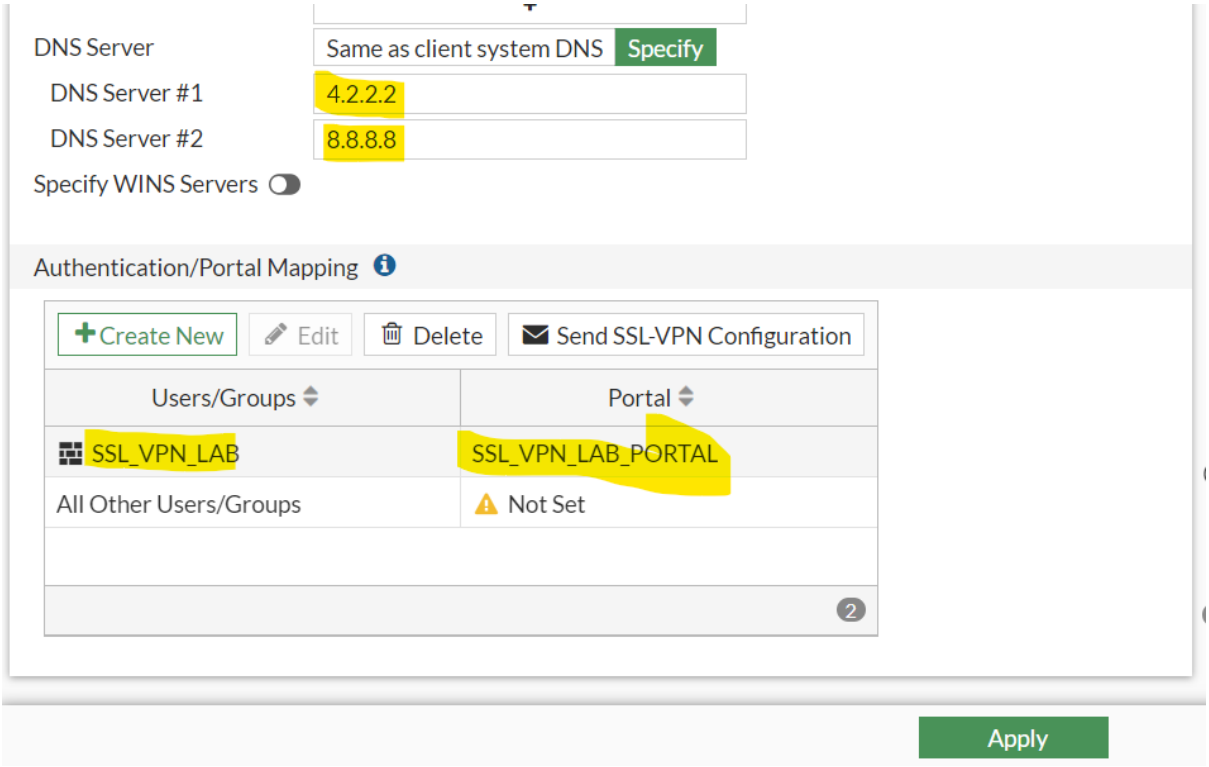
9. Now let us configure the SSL_VPN_Settings

i. Enable SSL VPN
ii. Listen on interface – select the WAN interface
iii. Listen on port – any port we can define – let us keep it as 50443
iv. Server Certificate – Create and select that certificate

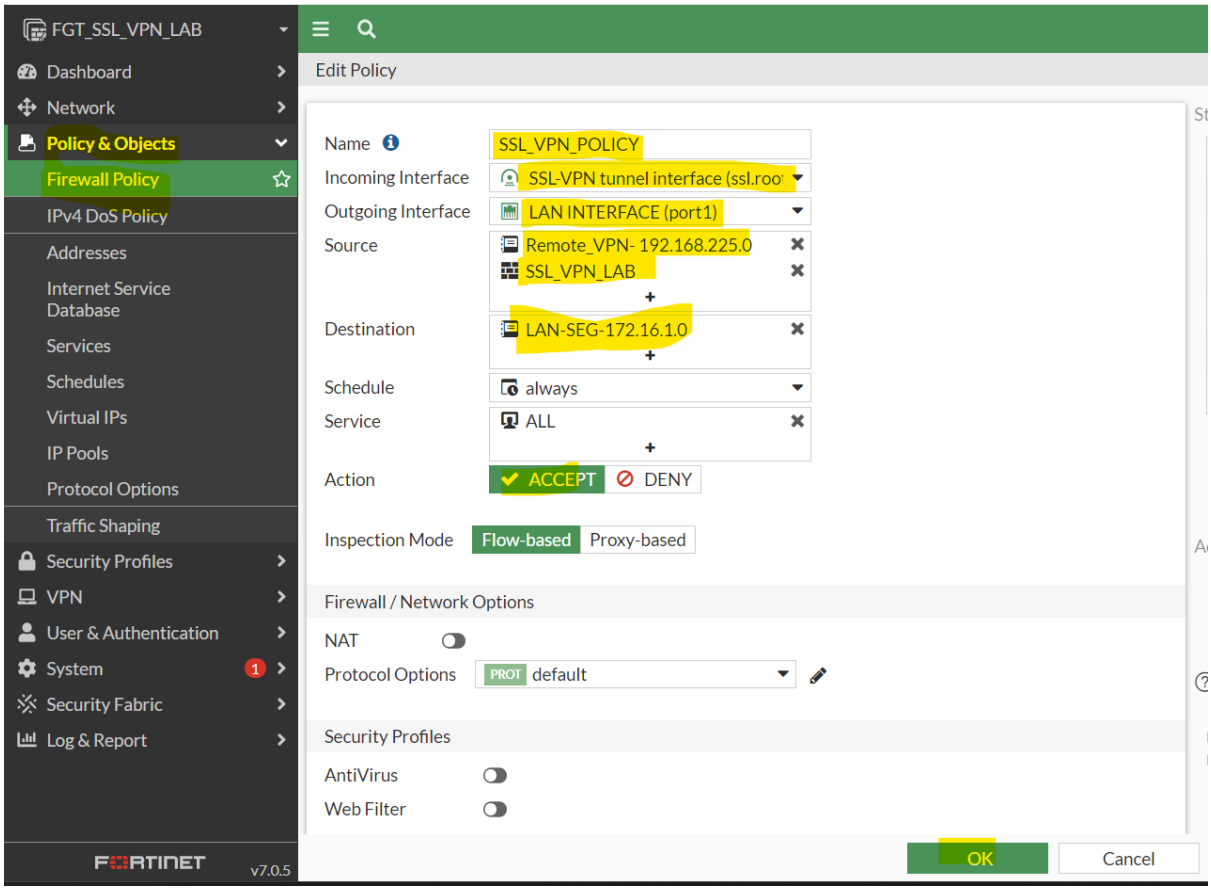


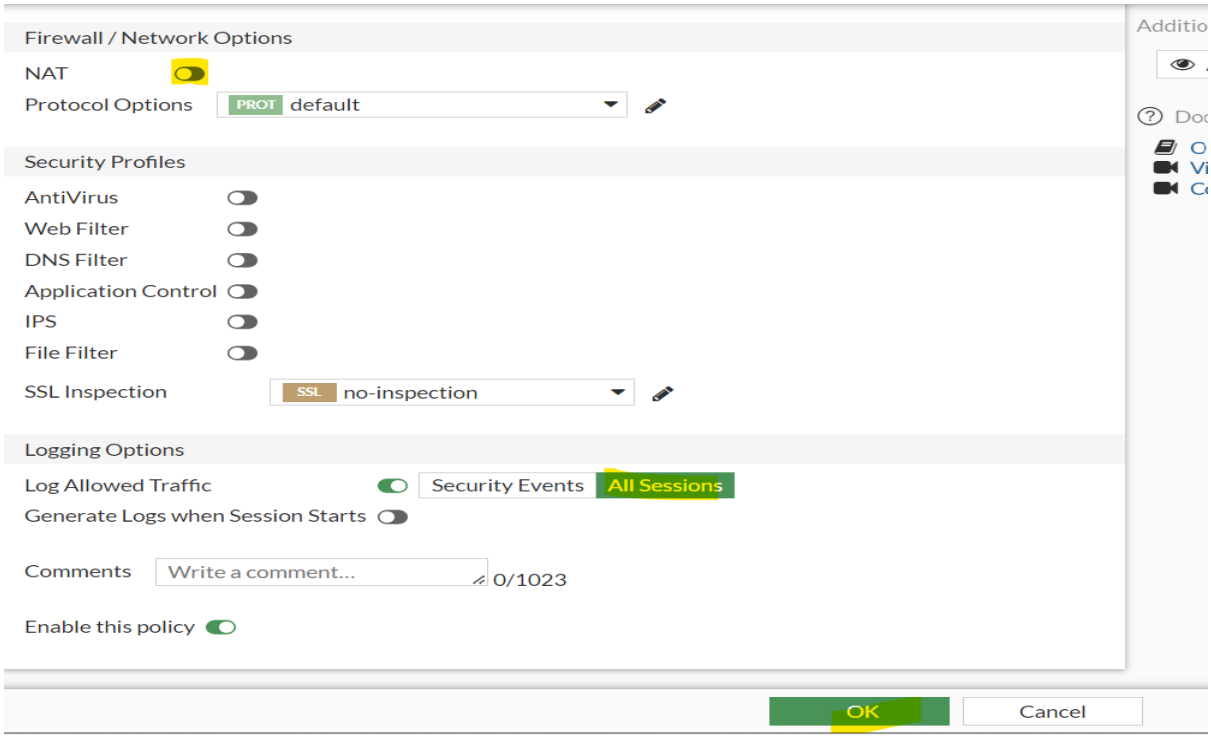
i. IP – select the custom IP ranges and select our remote define IP range
ii. DNS Servers – 4.2.2.2 and 8.8.8.8
iii. Portal Mapping – select the user group and portal that we created in earlier step



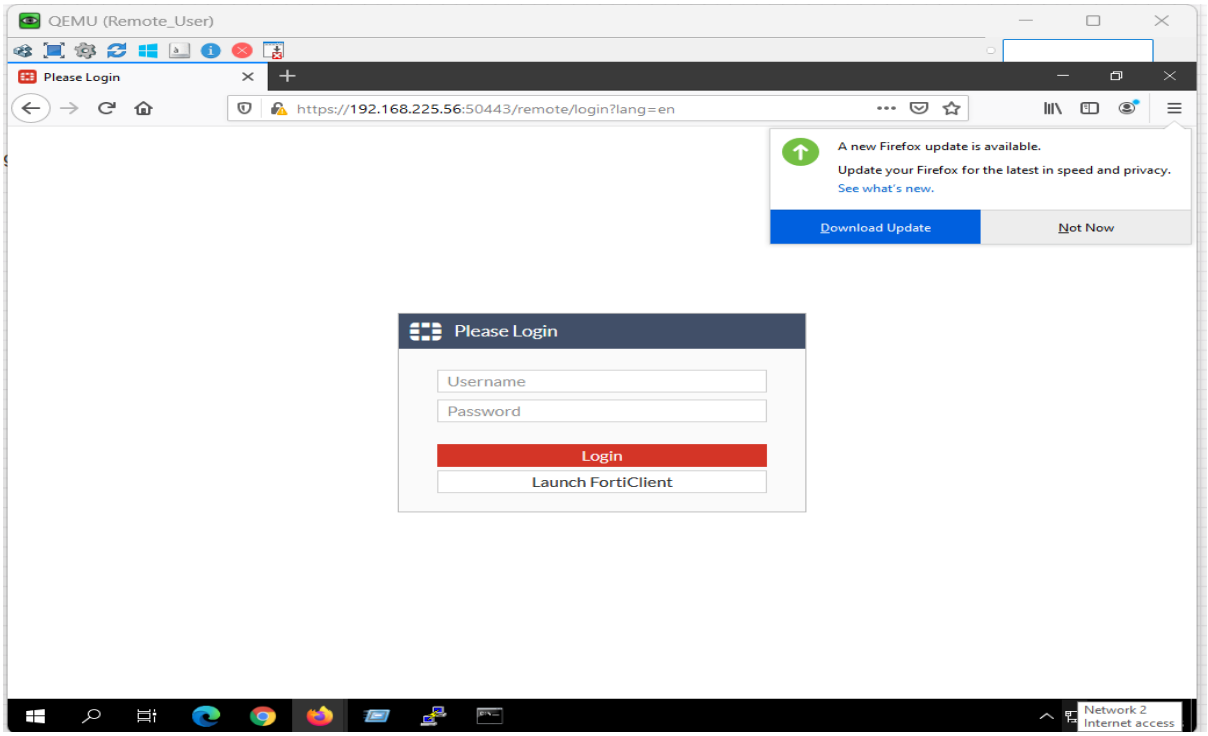


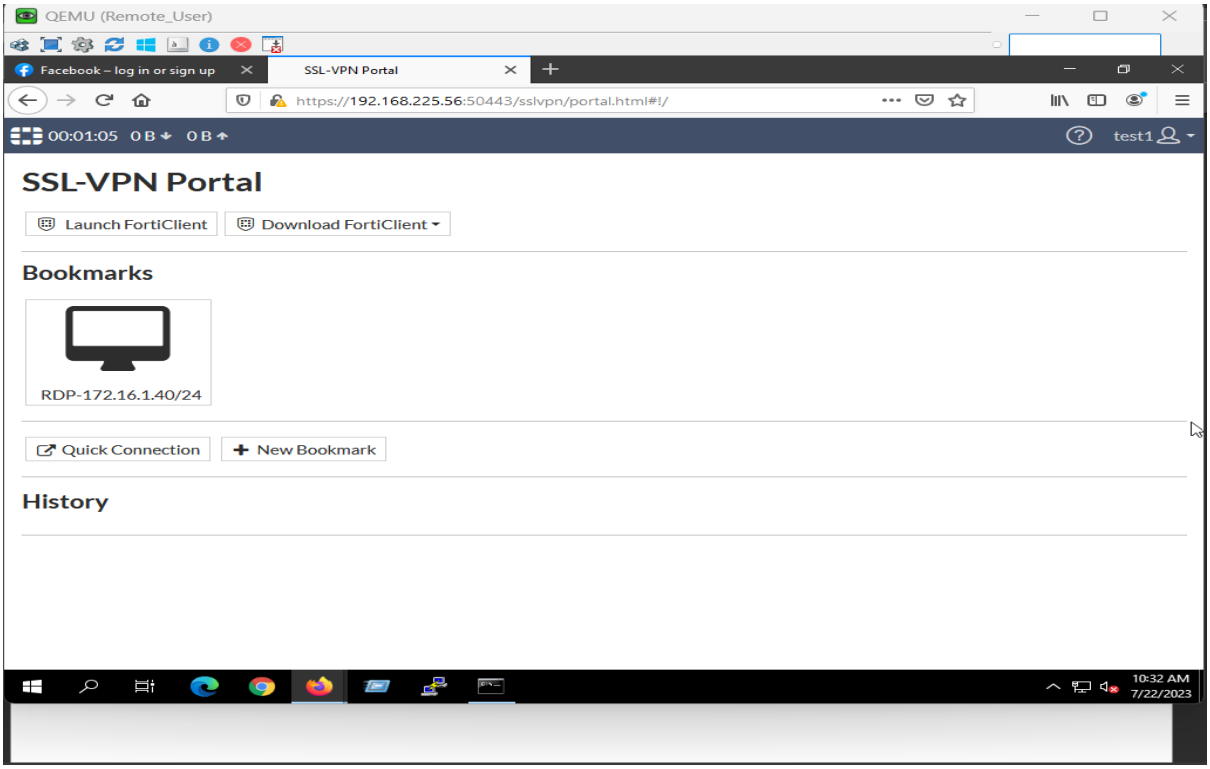
10. Now we need to create a firewall policy for SSL Tunnel to Inside
    Go to Policy and Objects > firewall Policy





11. Now let us check first the Web based access i.e clientless access.
    So go to remote user and hit the IP – 192.168.225.56:50443 in the browser.
    Then we will see the page of Forti web Client for login.
    Here we have to enter the credentials that we have defined for users then we get the page as below.
    So over here we can take RDP of our internal resource by clicking on RDP icon.





12. Now we can also check by using the FortiClient, let us download it from the page shown above with option Download FortiClient and connect using the credentials.

Thankyou