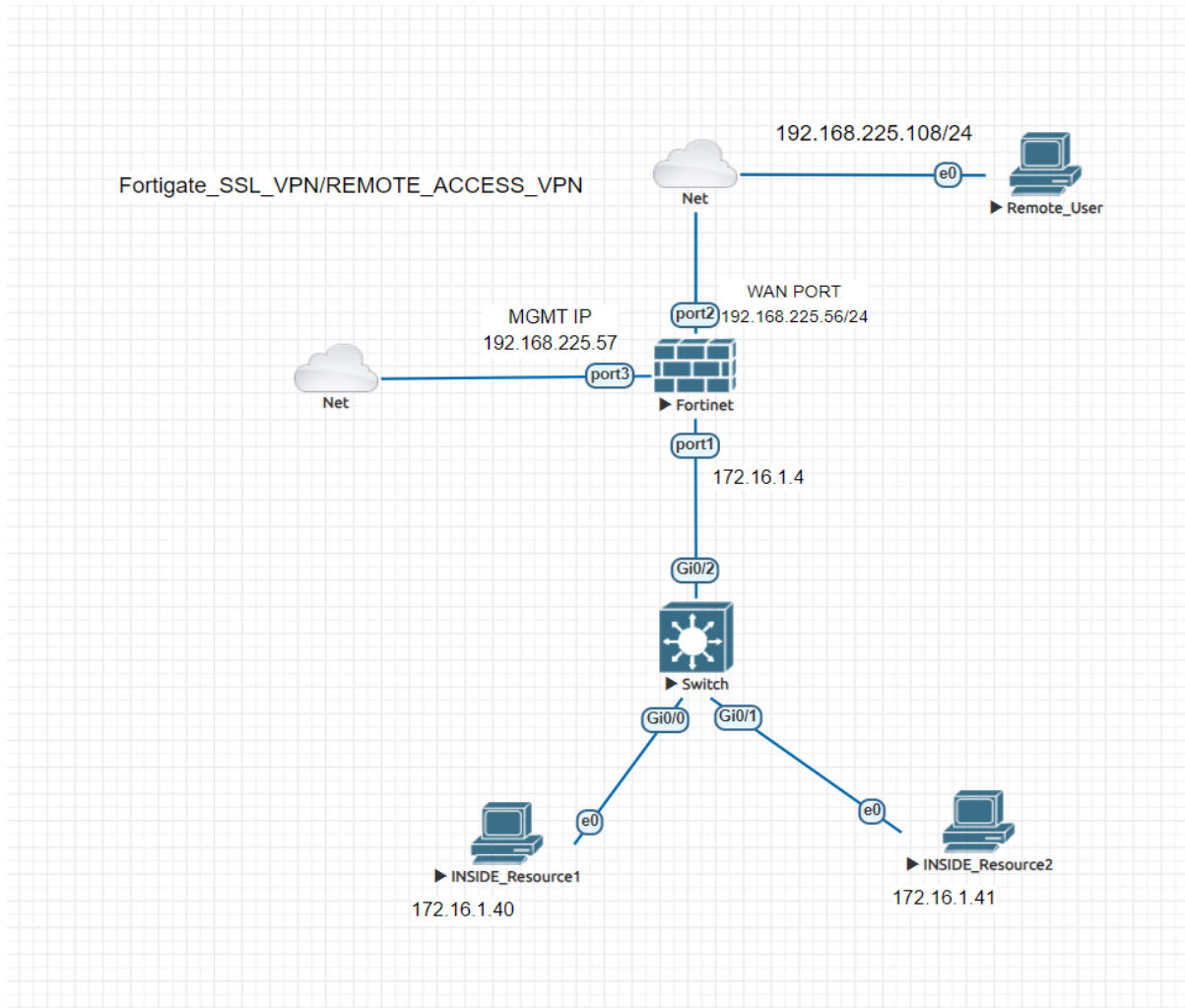


# Fortigate\_SSL\_VPN/REMOTE\_ACCESS\_VPN

1. Consider a below topology for SSL\_VPN\_LAB.

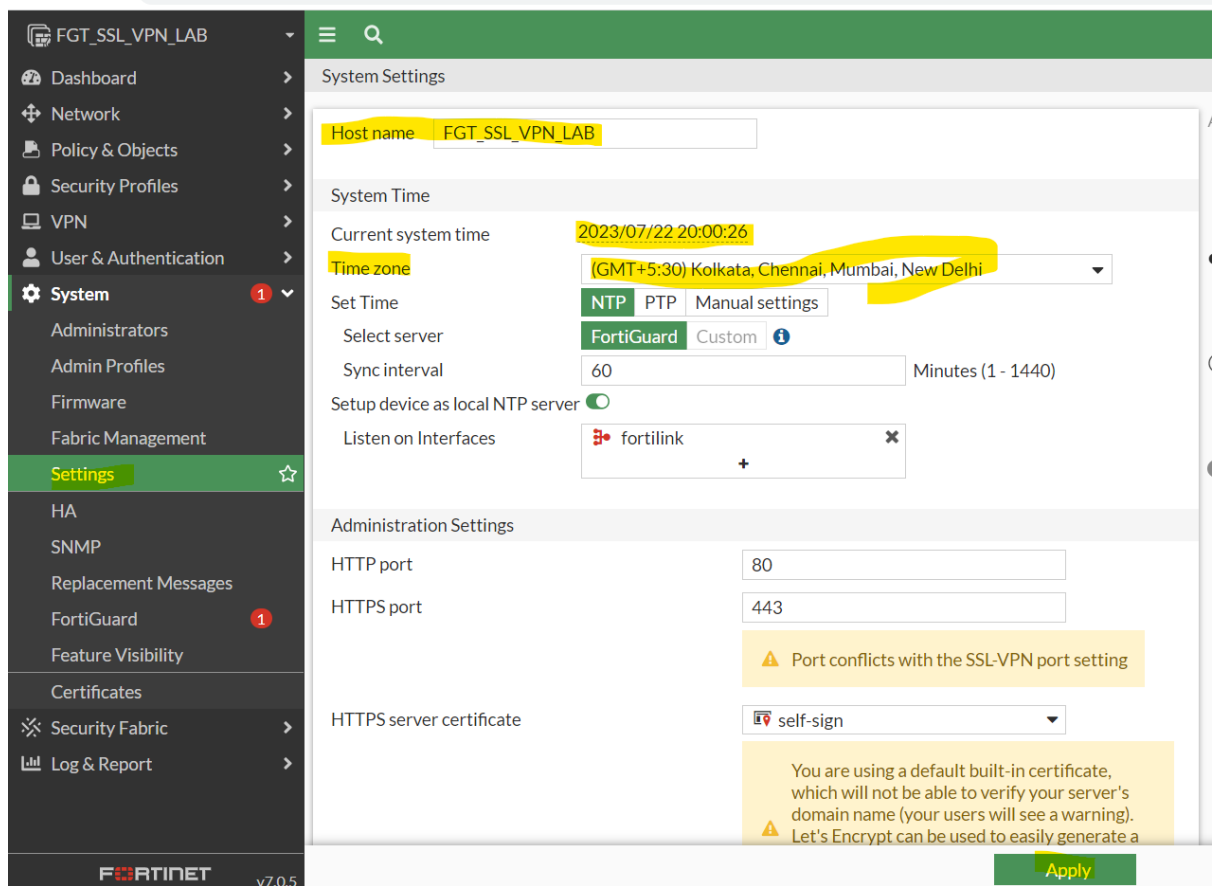


2. Now let us first take GUI access of FortiGate firewall.  
Management IP – 192.168.225.57 – so enter <http://192.168.225.57> in the browser

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

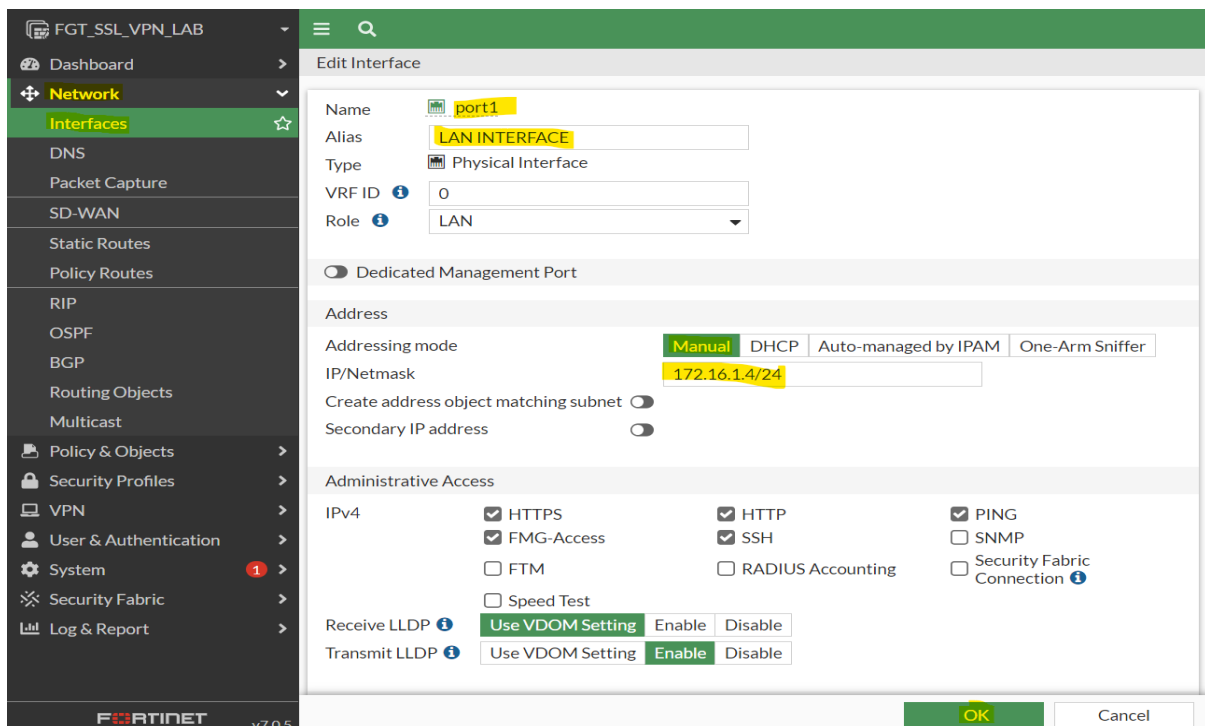
FortiGate-VM64-KVM # get system interface
== [ port1 ]
name: port1 mode: dhcp ip: 0.0.0.0 0.0.0.0 status: up netbios-forward:
disable type: physical ring-rx: 0 ring-tx: 0 netflow-sampler: disable
sflow-sampler: disable src-check: enable explicit-web-proxy: disable
explicit-ftp-proxy: disable proxy-captive-portal: 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-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
== [ 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
```

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



The screenshot shows the Fortinet FortiGate GUI with the 'System Settings' page. The left sidebar contains a menu with 'System' highlighted. The main content area is divided into sections: 'System Settings', 'System Time', and 'Administration Settings'. In the 'System Settings' section, the 'Host name' is set to 'FGT\_SSL\_VPN\_LAB'. In the 'System Time' section, the 'Current system time' is '2023/07/22 20:00:26', the 'Time zone' is '(GMT+5:30) Kolkata, Chennai, Mumbai, New Delhi', and the 'Set Time' method is 'NTP'. In the 'Administration Settings' section, the 'HTTP port' is '80' and the 'HTTPS port' is '443'. A warning message states: 'Port conflicts with the SSL-VPN port setting'. The 'HTTPS server certificate' is set to 'self-sign'. A yellow box contains a warning: 'You are using a default built-in certificate, which will not be able to verify your server's domain name (your users will see a warning). Let's Encrypt can be used to easily generate a'. The 'Apply' button is at the bottom right.

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



The screenshot shows the Fortinet FortiGate GUI with the 'Edit Interface' page. The left sidebar contains a menu with 'Network' highlighted. The main content area is divided into sections: 'Edit Interface', 'Address', and 'Administrative Access'. In the 'Edit Interface' section, the 'Name' is 'port1', the 'Alias' is 'LAN INTERFACE', the 'Type' is 'Physical Interface', the 'VRF ID' is '0', and the 'Role' is 'LAN'. In the 'Address' section, the 'Addressing mode' is 'Manual', the 'IP/Netmask' is '172.16.1.4/24', and the 'Secondary IP address' is disabled. In the 'Administrative Access' section, the 'IPv4' section has checkboxes for 'HTTPS', 'FMG-Access', 'FTM', 'Speed Test', 'HTTP', 'SSH', 'RADIUS Accounting', and 'PING'. The 'Receive LLDP' and 'Transmit LLDP' sections have 'Use VDOM Setting' and 'Enable' buttons. The 'OK' button is at the bottom right.

Go to Network > Interface > Edit Port2

**FGT\_SSL\_VPN\_LAB** v7.0.5

**Edit Interface**

Name: WAN INTERFACE (port2)  
Alias: WAN INTERFACE  
Type: Physical Interface  
VRF ID: 0  
Role: WAN  
Estimated bandwidth: 0 kbps Upstream, 0 kbps Downstream

**Address**

Addressing mode: Manual **DHCP**  
Status: ☒ Connected  
Obtained IP/Netmask: 192.168.225.56/255.255.0.0   
Expiry Date: 2023/07/23 10:14:36  
Acquired DNS: 192.168.225.1  
Default gateway: 192.168.225.1  
Retrieve default gateway from server: ☐  
Distance: 5  
Override internal DNS: ☐

**Administrative Access**

IPv4 ☐ HTTPS ☐ PING ☐ FMG-Access  
☐ SSH ☐ SNMP ☐ FTM

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

**FGT\_SSL\_VPN\_LAB** v7.0.5

**Users/Groups Creation Wizard**

1 **User Type** > 2 Login Credentials > 3 Contact Info > 4 Extra Info

**Local User**  
Remote RADIUS User  
Remote TACACS+ User  
Remote LDAP User  
FSSO  
FortiNAC User

FGT\_SSL\_VPN\_LAB

Dashboard

Network

Policy & Objects

Security Profiles

VPN

User & Authentication

User Definition

User Groups

Guest Management

LDAP Servers

RADIUS Servers

Users/Groups Creation Wizard

1 User Type 2 Login Credentials 3 Contact Info 4 Extra Info

Username test1

Password .....

Click On Next and Submit

Now create another user.

FGT\_SSL\_VPN\_LAB

Dashboard

Network

Policy & Objects

Security Profiles

VPN

User & Authentication

User Definition

User Groups

Guest Management

LDAP Servers

RADIUS Servers

Single Sign-On

Authentication Settings

FortiTokens

+ Create New Edit Clone Delete Search

Name	Type	Two-factor Authentication	Groups	Status	Ref.
guest	LOCAL		Guest-group	Enabled	1
test1	LOCAL			Enabled	0
test2	LOCAL			Enabled	0

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

FGT\_SSL\_VPN\_LAB

Dashboard

Network

Policy & Objects

Security Profiles

VPN

User & Authentication

User Definition

User Groups

Guest Management

LDAP Servers

RADIUS Servers

Single Sign-On

Authentication Settings

FortiTokens

System

Security Fabric

Log & Report

New User Group

Name SSL\_VPN\_LAB

Type Firewall

Fortinet Single Sign-On (FSSO)

RADIUS Single Sign-On (RSSO)

Guest

Members test1 test2

OK Cancel

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

FGT\_SSL\_VPN\_LAB

Dashboard

Network

Policy & Objects

Firewall Policy

IPv4 DoS Policy

Addresses

Internet Service Database

Services

Schedules

Virtual IPs

IP Pools

Protocol Options

Traffic Shaping

Security Profiles

VPN

User & Authentication

System

Security Fabric

Log & Report

Edit Address

Name: Remote\_VPN- 192.168.225.0

Color: Change

Type: Subnet

IP/Netmask: 192.168.225.0 255.255.255.0

Interface: any

Static route configuration: ☐

Comments: Write a comment... 0/255

OK Cancel

Now we need to create another object as LAN segment

Dashboard

Network

Policy & Objects

Firewall Policy

IPv4 DoS Policy

Addresses

Internet Service Database

Services

Schedules

Virtual IPs

IP Pools

Protocol Options

Traffic Shaping

Security Profiles

VPN

User & Authentication

System

Security Fabric

New Address

Name: LAN-SEG-172.16.1.0

Color: Change

Type: Subnet

IP/Netmask: 172.16.1.0/24

Interface: any

Static route configuration: ☐

Comments: Write a comment... 0/255

OK Cancel

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.

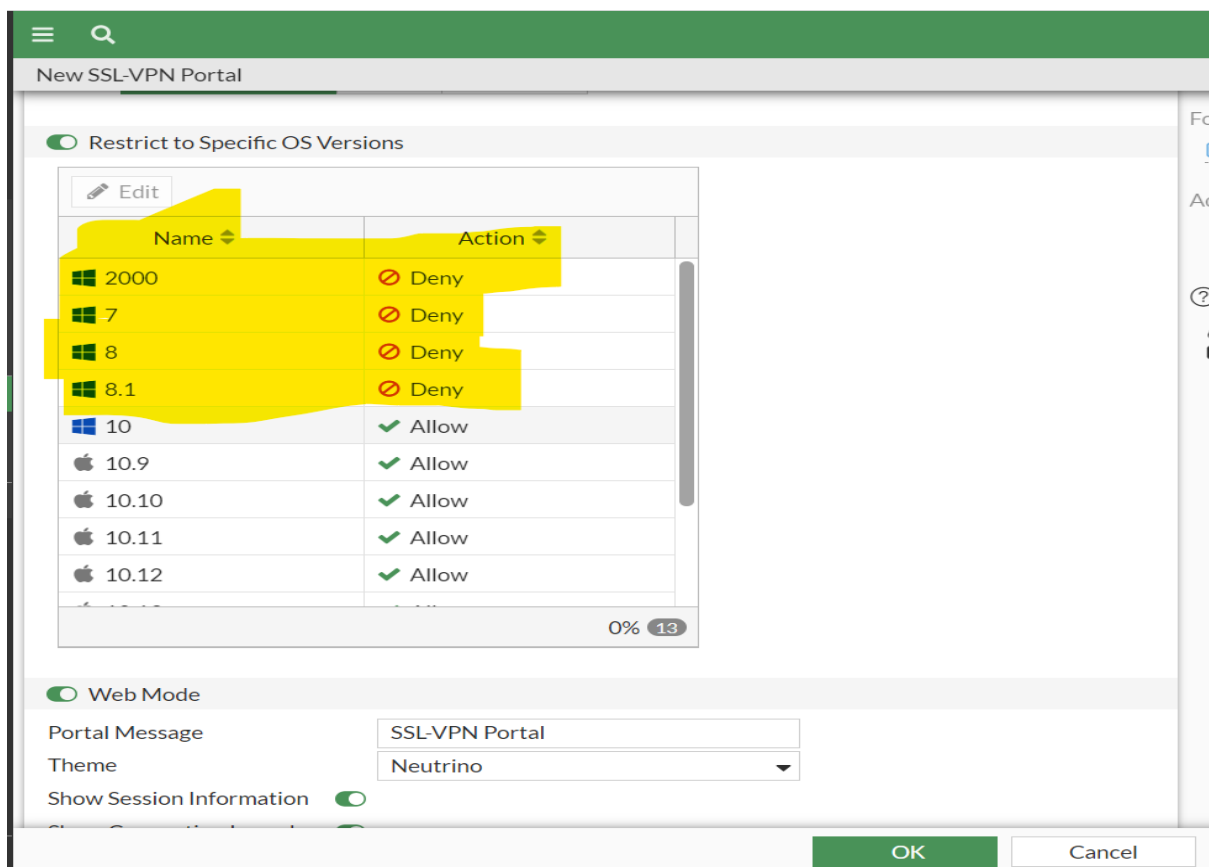
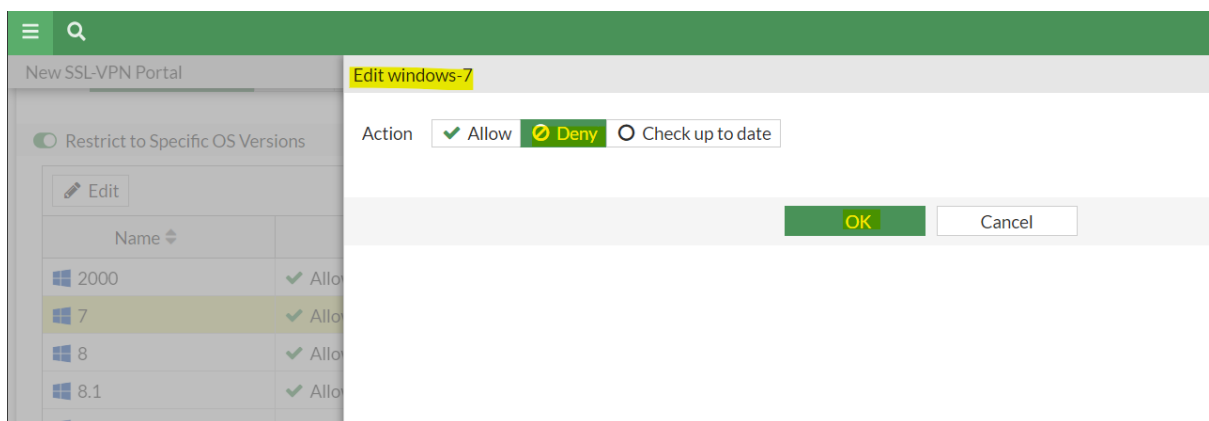
- I. Name – here we have to define the name – SSL\_VPN\_LAB\_PORTAL
- II. We have the option to limit the one connection at a time – Disabled it currently
- III. Tunnel Mode – There are two options Tunnel and Split.

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 Windows 7,8 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

The screenshot shows the 'New Bookmark' dialog box in the Fortinet SSL-VPN configuration interface. The dialog box is open, and the 'Web Mode' checkbox is checked. The 'Name' field is set to 'RDP - 172.16.1.40/24', the 'Type' is 'RDP', the 'Host' is '172.16.1.40', the 'Port' is '3389', the 'Description' is 'RDP-PC', the 'Single Sign-On' is 'Disable', the 'Username' is 'user', the 'Password' is masked with dots, the 'Color depth' is '16 Bit', the 'Screen width' is '1024', the 'Screen height' is '768', the 'Keyboard layout' is 'English, United States.', and the 'Security' is 'Standard RDP encryption.'. The 'Restricted admin mode' checkbox is unchecked. The 'OK' button is highlighted with a yellow box.

- X. Click on Ok.
9. Now let us configure the SSL\_VPN\_Settings
- Enable SSL VPN
  - Listen on interface – select the WAN interface
  - Listen on port – any port we can define – let us keep it as 50443
  - Server Certificate – Create and select that certificate

The screenshot shows the 'Create Certificate' wizard in the Fortinet SSL-VPN configuration interface. The wizard is at step 2, 'Certificate Details'. The 'Certificate authority' is 'Fortinet\_CA\_SSL'. The 'Certificate name' is 'SSLC2cert'. The 'Common name' is '192.168.225.56'. A note indicates that the common name should match the FQDN or IP of the primary SSL-VPN interface. The 'Subject alternative name' field is empty. The 'Create' button is highlighted with a green box.

- 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

← → ↻ ⚠ Not secure | 192.168.225.57/ng/vpn/ssl/settings

FGT\_SSL\_VPN\_LAB

Dashboard

Network

Policy & Objects

Security Profiles

**VPN**

Overlay Controller VPN

IPsec Tunnels

IPsec Wizard

IPsec Tunnel Template

SSL-VPN Portals

**SSL-VPN Settings**

SSL-VPN Clients

VPN Location Map

User & Authentication

System 1

Security Fabric

Log & Report

SSL-VPN Settings

Connection Settings ⓘ

Enable SSL-VPN ☒

Listen on Interface(s) WAN INTERFACE (port2) +

Listen on Port 50443

Web mode access will be listening at <https://192.168.225.56:50443>

Server Certificate SSL2CERT

Redirect HTTP to SSL-VPN ☐

Restrict Access **Allow access from any host** Limit access to specific hosts

Idle Logout ☒

Inactive For 300 Seconds

Require Client Certificate ☐

Tunnel Mode Client Settings ⓘ

Address Range Automatically assign addresses Specify custom IP ranges

IP Ranges Remote\_VPN- 192.168.225.0 +

DNS Server Same as client system DNS Specify

DNS Server #1 4.2.2.2

DNS Server #2 8.8.8.8

Apply

FORTINET

v7.0.5



DNS Server

DNS Server #1

DNS Server #2

Specify WINS Servers ☐

Authentication/Portal Mapping ?

Users/Groups	Portal
SSL_VPN_LAB	SSL_VPN_LAB_PORTAL
All Other Users/Groups	Not Set
2	

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

FGT\_SSL\_VPN\_LAB

- Dashboard
- Network
- Policy & Objects**
  - Firewall Policy**
  - IPv4 DoS Policy
  - Addresses
  - Internet Service Database
  - Services
  - Schedules
  - Virtual IPs
  - IP Pools
  - Protocol Options
  - Traffic Shaping
  - Security Profiles
  - VPN
  - User & Authentication
  - System
  - Security Fabric
  - Log & Report

Edit Policy

Name

SSL\_VPN\_POLICY

Incoming Interface

SSL-VPN tunnel interface (ssl.root)

Outgoing Interface

LAN INTERFACE (port1)

Source

Remote\_VPN- 192.168.225.0

SSL\_VPN\_LAB

Destination

LAN-SEG-172.16.1.0

Schedule

always

Service

ALL

Action

☒ ACCEPT ☐ DENY

Inspection Mode

Flow-based Proxy-based

Firewall / Network Options

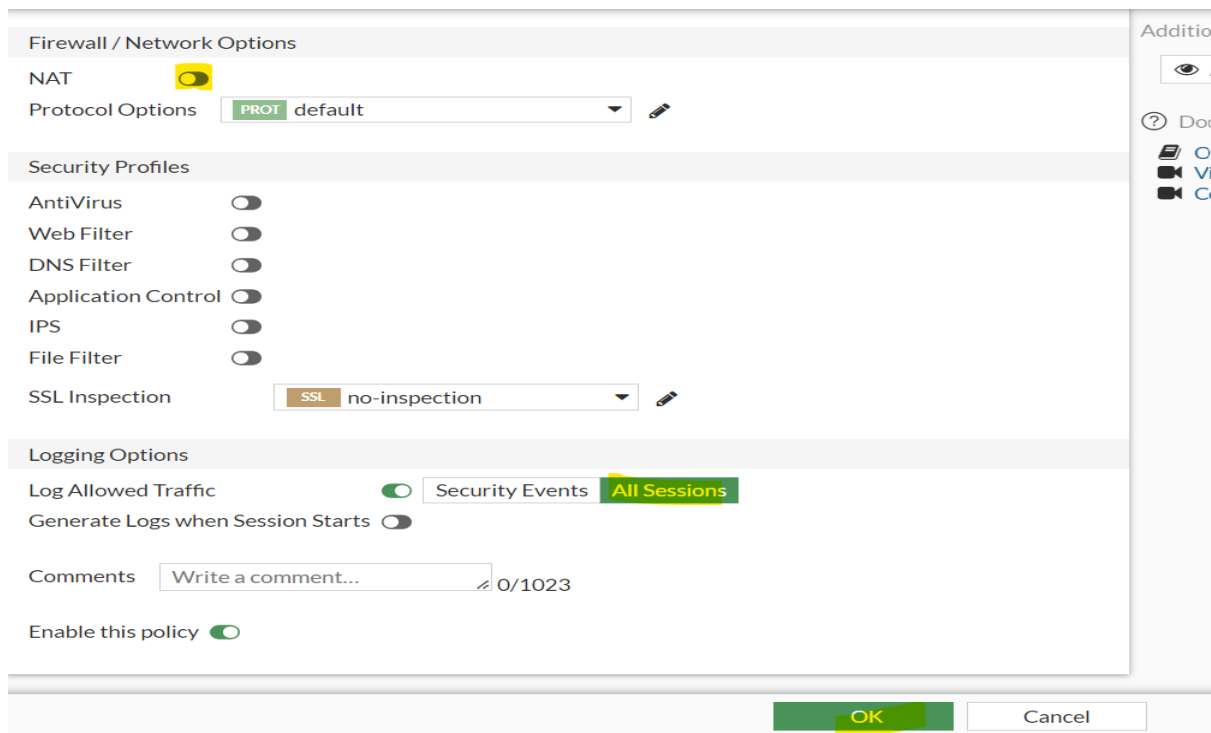
NAT ☐

Protocol Options PROT default

Security Profiles

AntiVirus ☐

Web Filter ☐



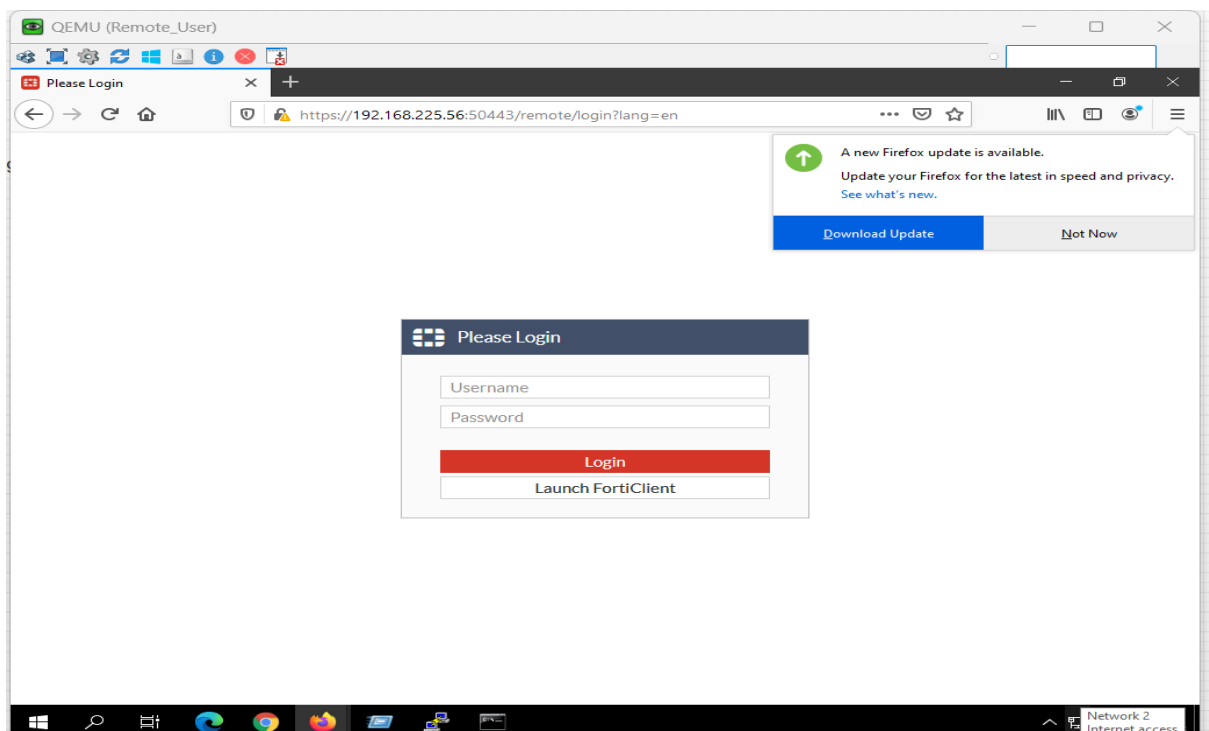
11. Now let us check first the Web based access i.e clientless access.

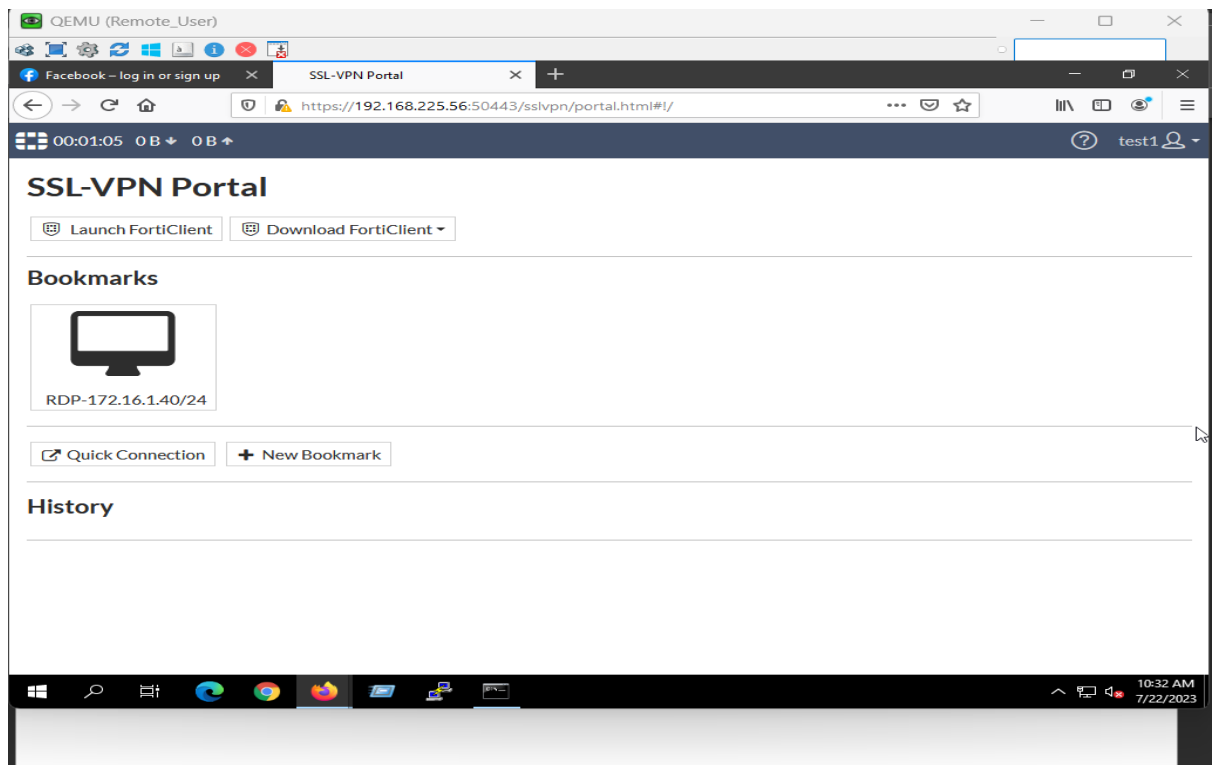
So go to remote user and hit the IP – 192.168.225.56:50443 in the browser.

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**