SSL VPN

Mohamed Saad Abdelwahab Essa

DEPI_1_ONL1_ISS8_S1E FORTINET CYBERSECURITY ENGINEER

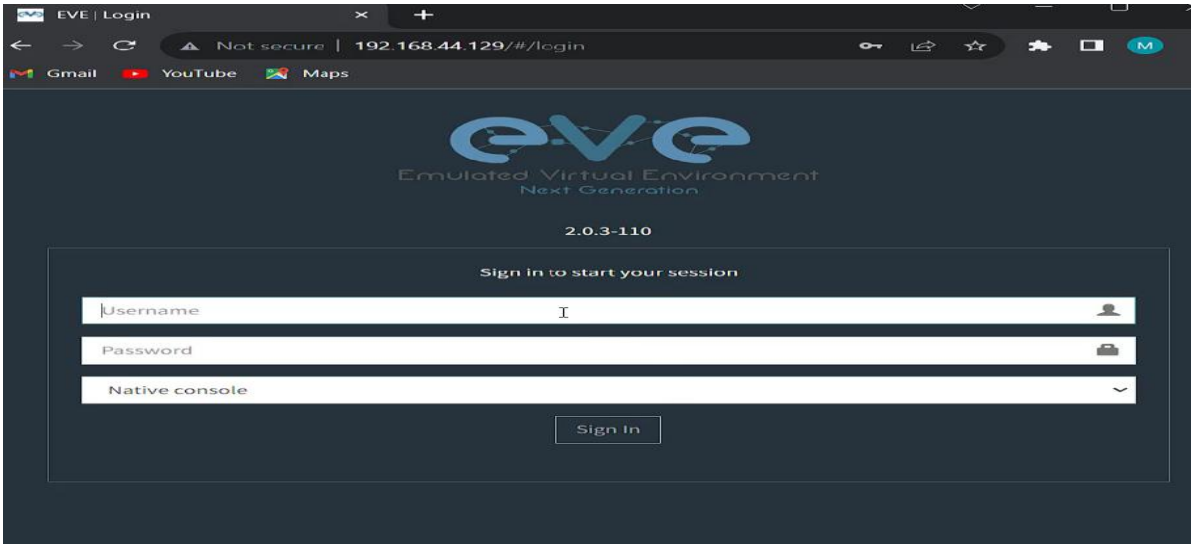
SSL VPN lab

Objective of the Lab

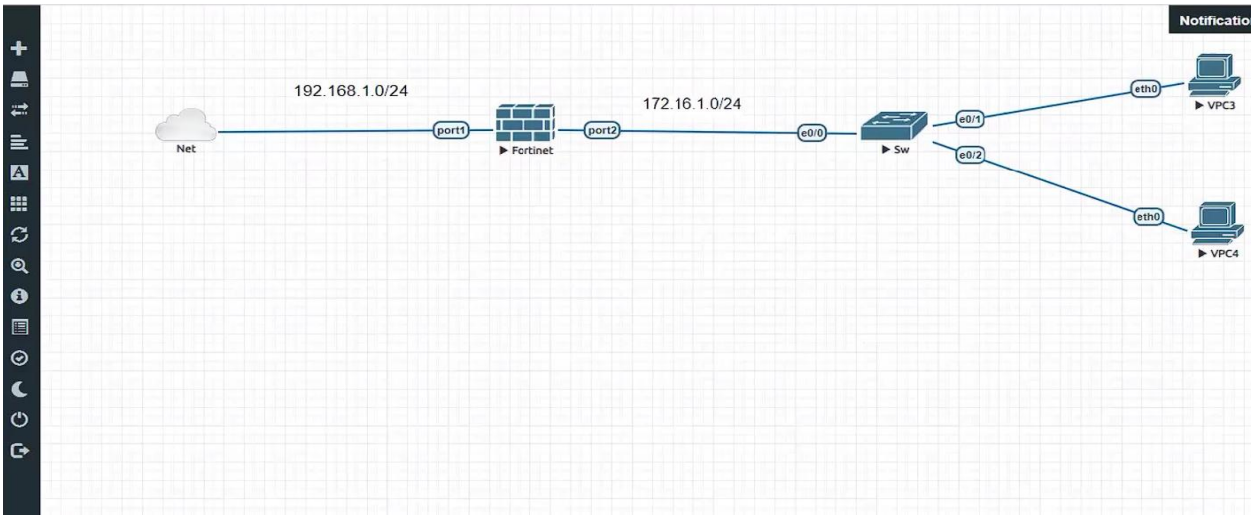
The objective of this lab is to configure and test **SSL VPN (Secure Socket Layer Virtual Private Network)**, allowing remote users to securely connect to a private network using encrypted communication. The lab focuses on setting up an SSL VPN connection, configuring devices, and verifying the secure access to internal resources.

Credentials:

- Username: admin
- Password: EVE



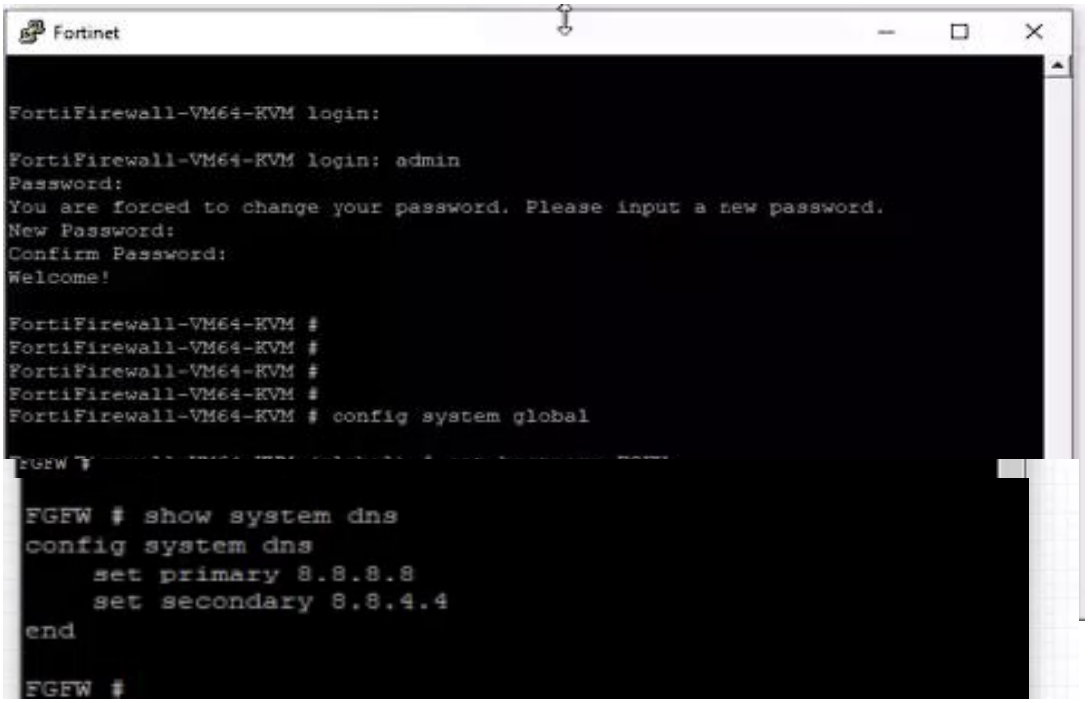
Topology

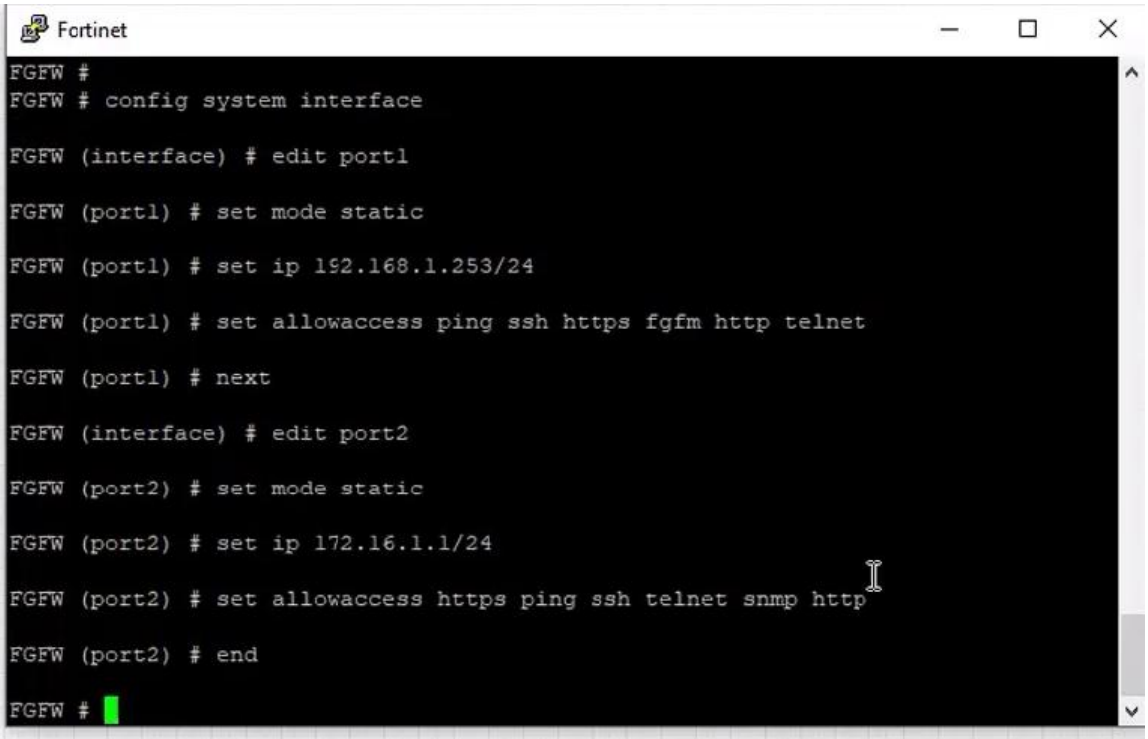


Components used

- Fortinet firewall
- Switch
- Internet
- 2 pcs

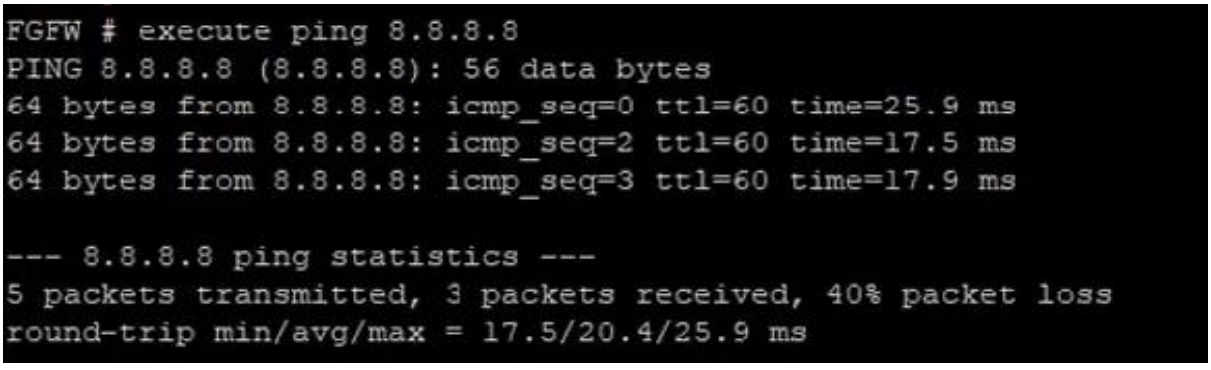
configuration done on the devices

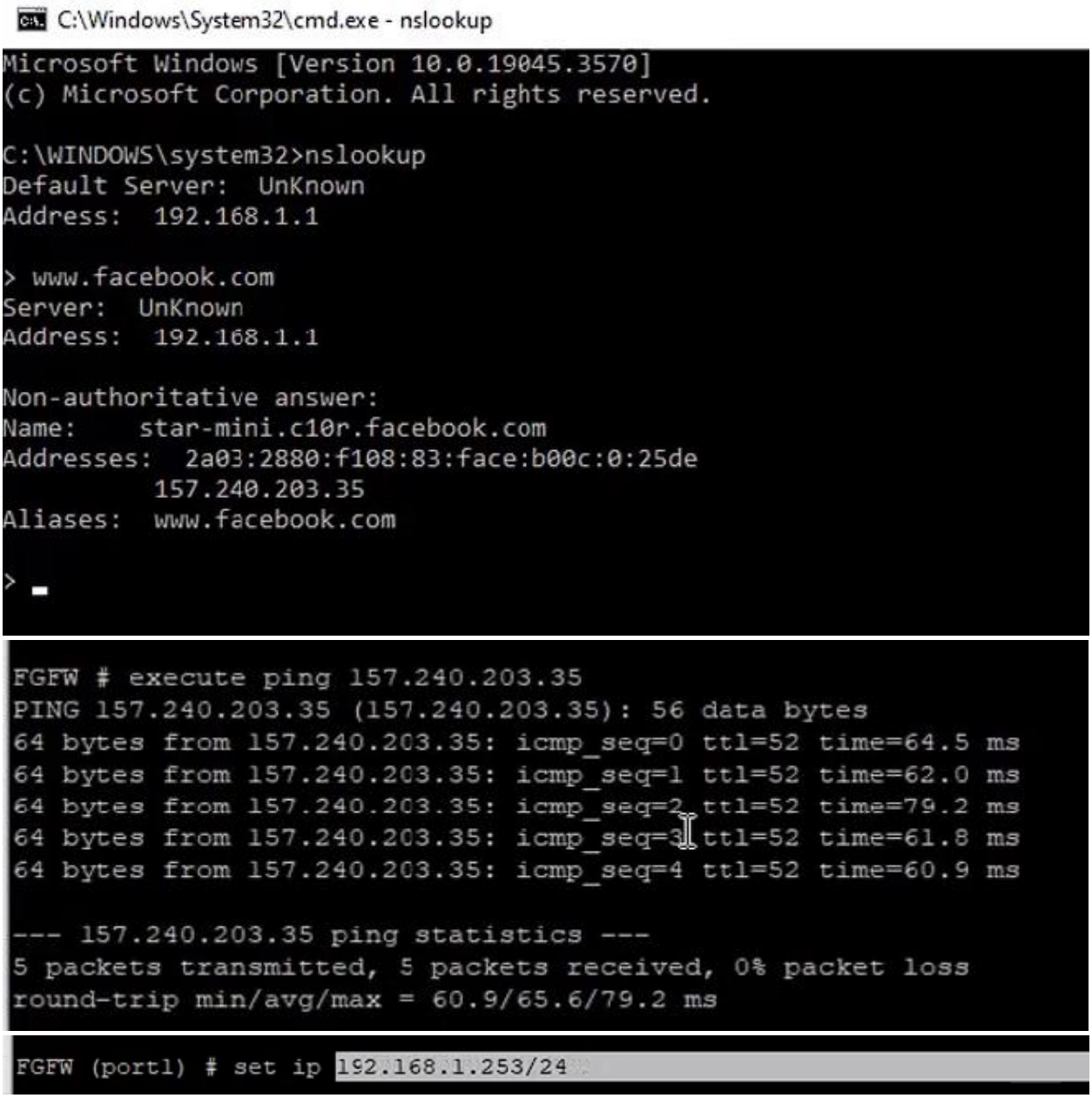



Fortinet
FGFW #
FGFW # config system interface
FGFW (interface) # edit port1
FGFW (port1) # set mode static
FGFW (port1) # set ip 192.168.1.253/24
FGFW (port1) # set allowaccess ping ssh https fgfm http telnet
FGFW (port1) # next
FGFW (interface) # edit port2
FGFW (port2) # set mode static
FGFW (port2) # set ip 172.16.1.1/24
FGFW (port2) # set allowaccess https ping ssh telnet snmp http
FGFW (port2) # end
FGFW #


FGFW # ping 8.8.8.8
Unknown action 0
FGFW # execute ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8): 56 data bytes
sendto failed
sendto failed
sendto failed
sendto failed
sendto failed
--- 8.8.8.8 ping statistics ---
5 packets transmitted, 0 packets received, 100% packet loss

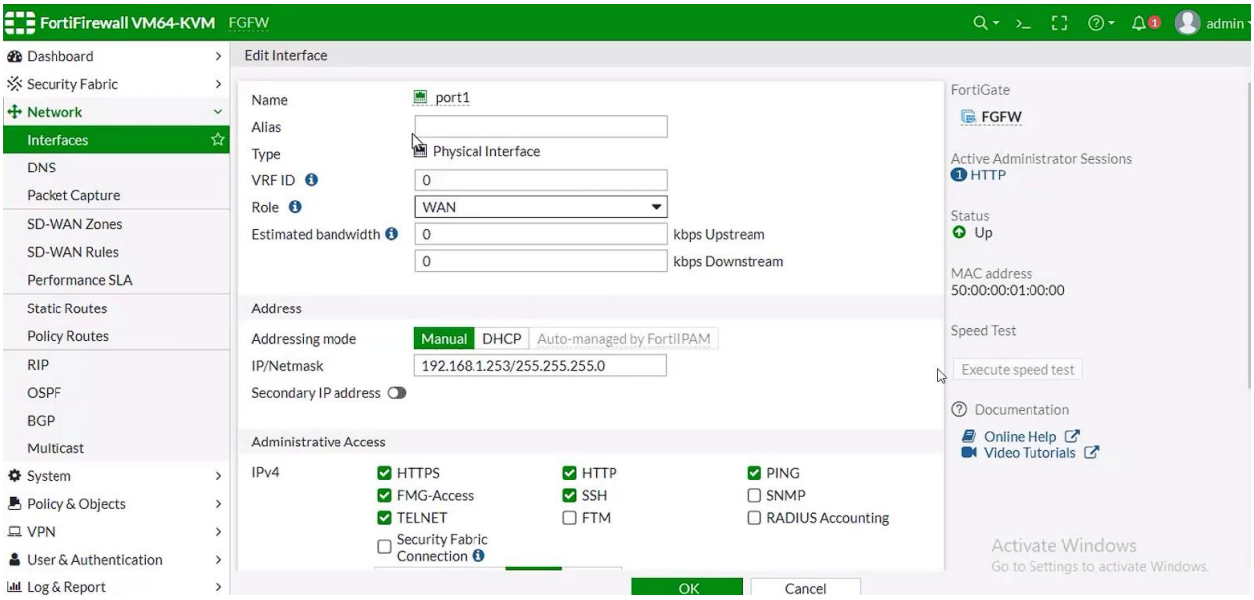
FGFW (static) # edit 1
new entry '1' added
FGFW (1) # set gateway 192.168.1.1
FGFW (1) # set device port1
FGFW (1) # next
FGFW (static) # end

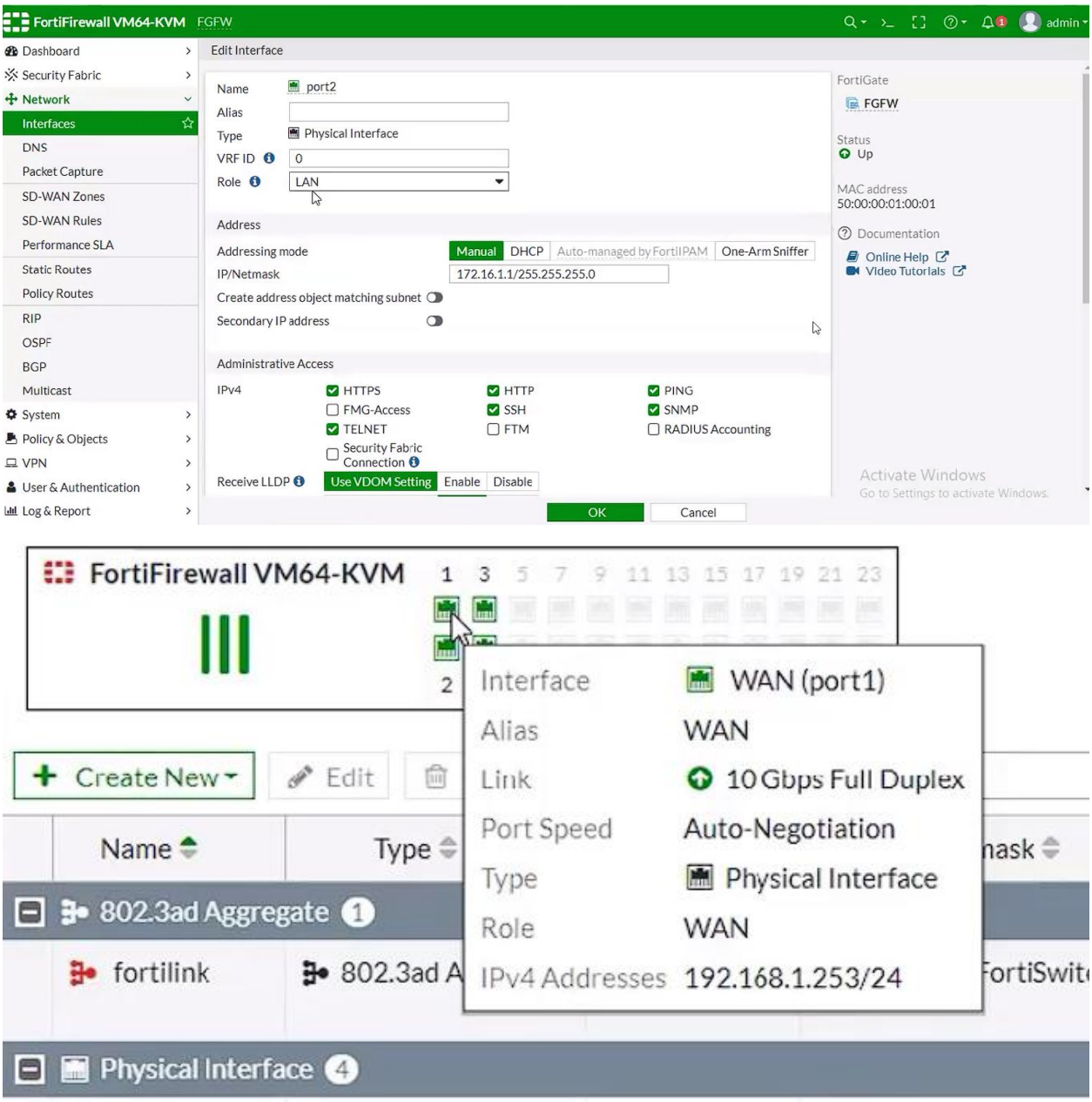

FGFW # execute ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8): 56 data bytes
64 bytes from 8.8.8.8: icmp_seq=0 ttl=60 time=25.9 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=60 time=17.5 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=60 time=17.9 ms
--- 8.8.8.8 ping statistics ---
5 packets transmitted, 3 packets received, 40% packet loss
round-trip min/avg/max = 17.5/20.4/25.9 ms


C:\Windows\System32\cmd.exe - nslookup
Microsoft Windows [Version 10.0.19045.3570]
(c) Microsoft Corporation. All rights reserved.
C:\WINDOWS\system32>nslookup
Default Server: UnKnown
Address: 192.168.1.1
> www.facebook.com
Server: UnKnown
Address: 192.168.1.1
Non-authoritative answer:
Name: star-mini.c10r.facebook.com
Addresses: 2a03:2880:f108:83:face:b00c:0:25de
157.240.203.35
Aliases: www.facebook.com
>
FGFW # execute ping 157.240.203.35
PING 157.240.203.35 (157.240.203.35): 56 data bytes
64 bytes from 157.240.203.35: icmp_seq=0 ttl=52 time=64.5 ms
64 bytes from 157.240.203.35: icmp_seq=1 ttl=52 time=62.0 ms
64 bytes from 157.240.203.35: icmp_seq=2 ttl=52 time=79.2 ms
64 bytes from 157.240.203.35: icmp_seq=3 ttl=52 time=61.8 ms
64 bytes from 157.240.203.35: icmp_seq=4 ttl=52 time=60.9 ms
--- 157.240.203.35 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 60.9/65.6/79.2 ms
FGFW (port1) # set ip 192.168.1.253/24

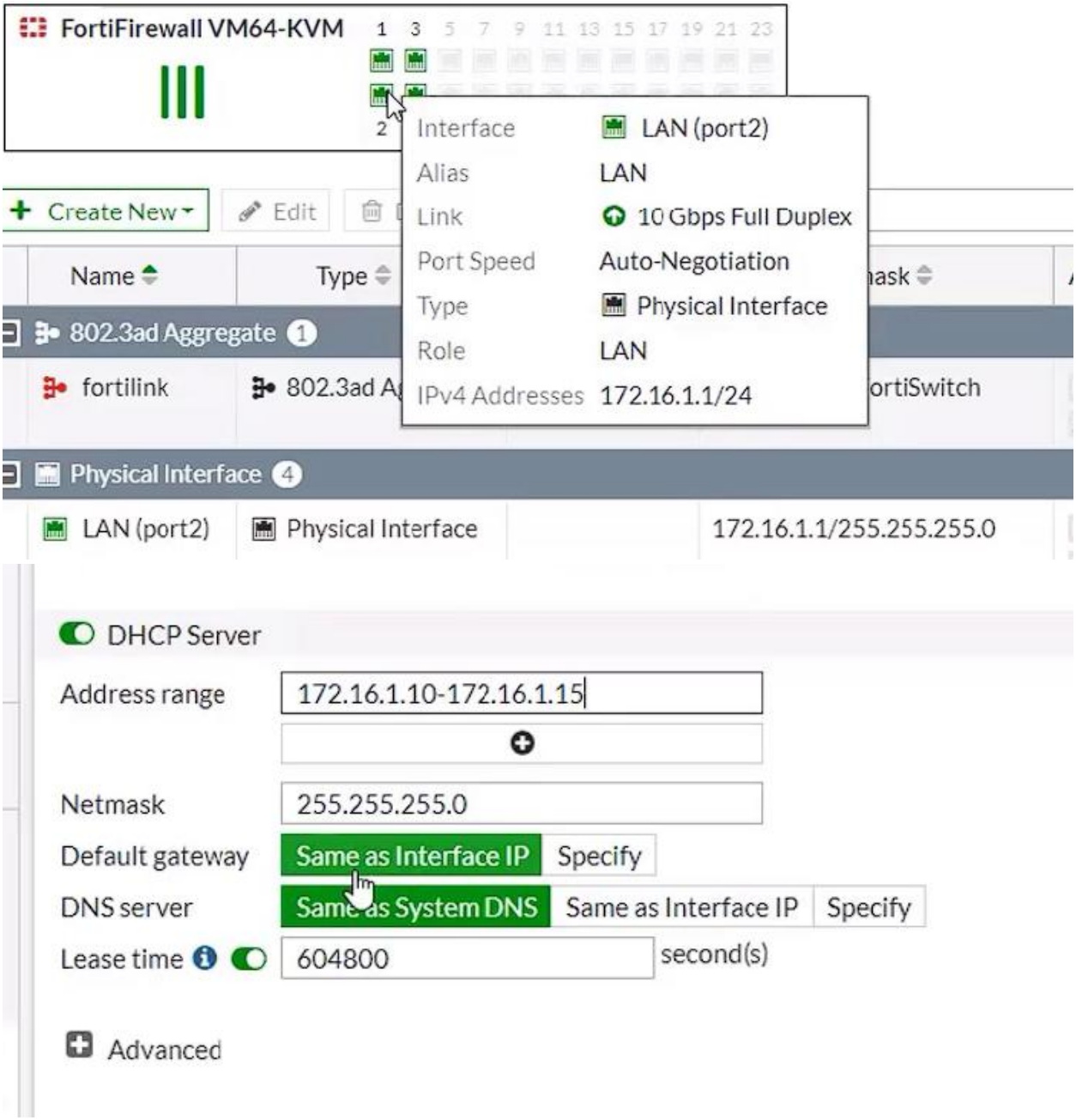
Steps of the lab

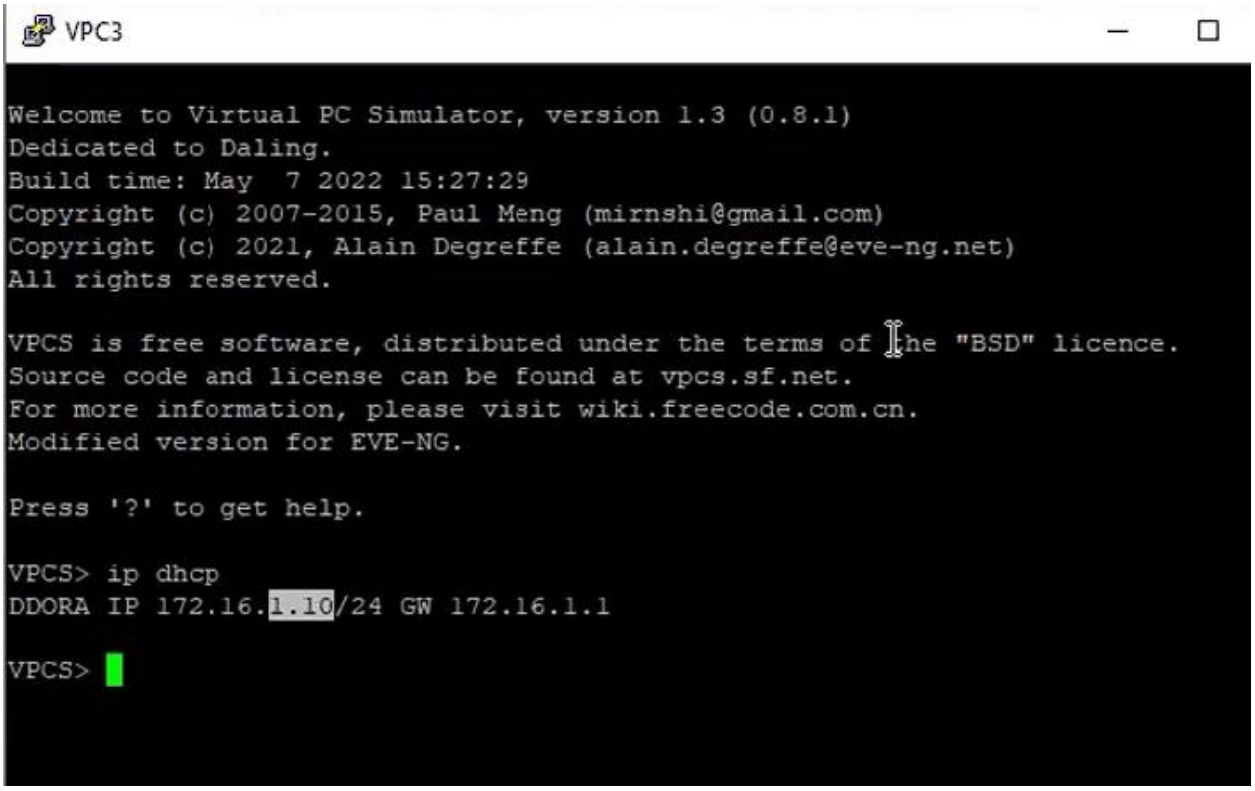
CLI Configuration

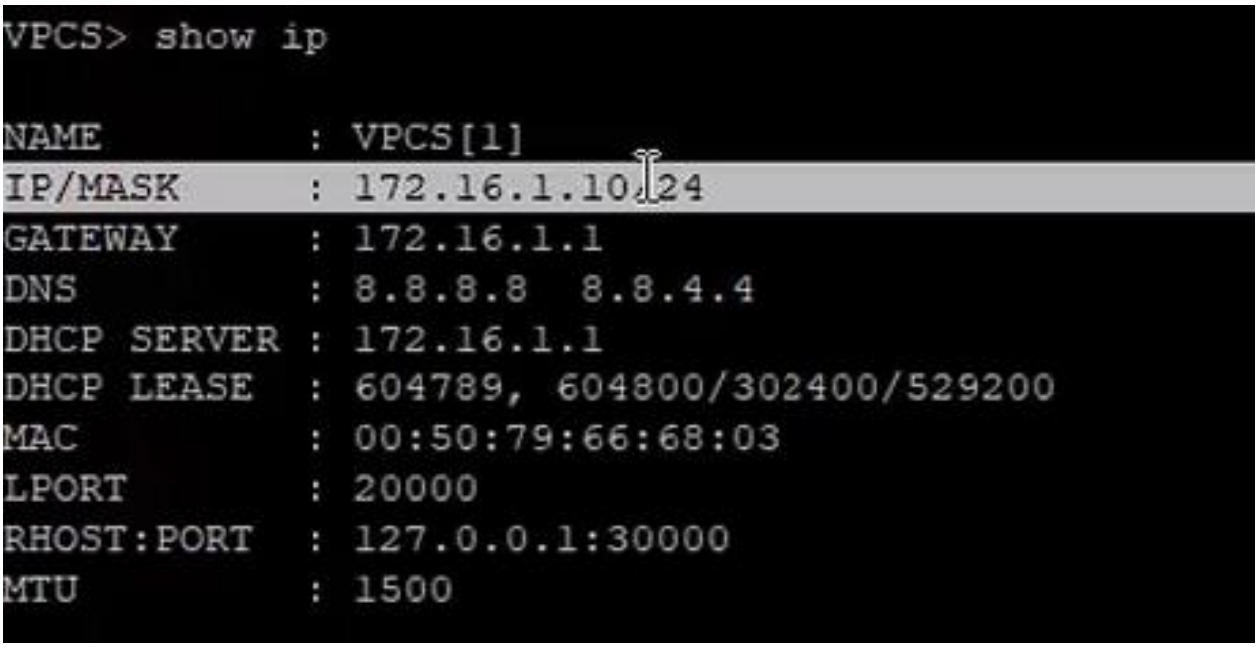



FortiFirewall VM64-KVM
FGFW
admin
Dashboard
Security Fabric
Network
Interfaces
DNS
Packet Capture
SD-WAN Zones
SD-WAN Rules
Performance SLA
Static Routes
Policy Routes
RIP
OSPF
BGP
Multicast
System
Policy & Objects
VPN
User & Authentication
Log & Report
Edit Interface
Name
port2
Alias
Type
Physical Interface
VRF ID
0
Role
LAN
Address
Addressing mode
Manual
DHCP
Auto-managed by FortiIPAM
One-Arm Sniffer
IP/Netmask
172.16.1.1/255.255.255.0
Create address object matching subnet
Secondary IP address
Administrative Access
IPv4
HTTPS
HTTP
PING
FMG-Access
SSH
SNMP
TELNET
FTM
RADIUS Accounting
Security Fabric Connection
Receive LLDP
Use VDOM Setting
Enable
Disable
OK
Cancel
FortiGate
FGFW
Status
Up
MAC address
50:00:00:01:00:01
Documentation
Online Help
Video Tutorials
Activate Windows
Go to Settings to activate Windows.

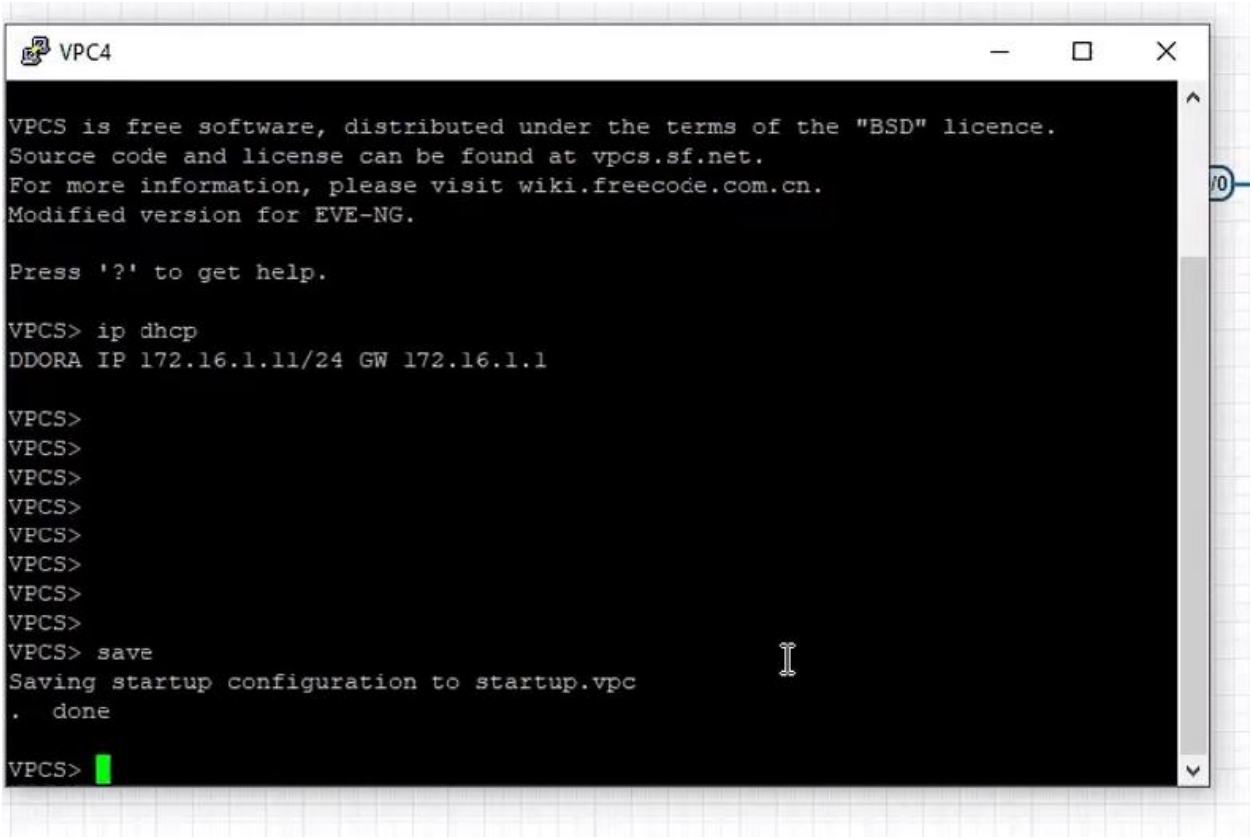
FortiFirewall VM64-KVM
1 3 5 7 9 11 13 15 17 19 21 23
2
Interface
WAN (port1)
Alias
WAN
Link
10 Gbps Full Duplex
Port Speed
Auto-Negotiation
Type
Physical Interface
Role
WAN
IPv4 Addresses
192.168.1.253/24
Create New
Edit
Name
Type
802.3ad Aggregate 1
fortilink
802.3ad A
Physical Interface 4


FortiFirewall VM64-KVM
1 3 5 7 9 11 13 15 17 19 21 23
2
Interface LAN (port2)
Alias LAN
Link 10 Gbps Full Duplex
Port Speed Auto-Negotiation
Type Physical Interface
Role LAN
IPv4 Addresses 172.16.1.1/24
Create New
Edit
Name
Type
802.3ad Aggregate 1
fortilink
802.3ad Ag
ortiSwitch
Physical Interface 4
LAN (port2)
Physical Interface
172.16.1.1/255.255.255.0
DHCP Server
Address range
172.16.1.10-172.16.1.15
Netmask
255.255.255.0
Default gateway
Same as Interface IP
Specify
DNS server
Same as System DNS
Same as Interface IP
Specify
Lease time
604800
second(s)
Advanced


VPC3
Welcome to Virtual PC Simulator, version 1.3 (0.8.1)
Dedicated to Daling.
Build time: May 7 2022 15:27:29
Copyright (c) 2007-2015, Paul Meng (mirnshi@gmail.com)
Copyright (c) 2021, Alain Degreffe (alain.degreffe@eve-ng.net)
All rights reserved.
VPCS is free software, distributed under the terms of the "BSD" licence.
Source code and license can be found at vpcs.sf.net.
For more information, please visit wiki.freecode.com.cn.
Modified version for EVE-NG.
Press '?' to get help.
VPCS> ip dhcp
DDORA IP 172.16.1.10/24 GW 172.16.1.1
VPCS>


VPCS> show ip
NAME : VPCS[1]
IP/MASK : 172.16.1.10/24
GATEWAY : 172.16.1.1
DNS : 8.8.8.8 8.8.4.4
DHCP SERVER : 172.16.1.1
DHCP LEASE : 604789, 604800/302400/529200
MAC : 00:50:79:66:68:03
LPORT : 20000
RHOST:PORT : 127.0.0.1:30000
MTU : 1500

```
VPCS> save
Saving startup configuration to startup.vpc
.  done
```



Configuration SSL VPN

To configure SSL VPN using the GUI:

1. Configure the interface and firewall address. The port1 interface connects to the internal network.

a. Go to Network > Interfaces and edit the wan1 interface.

b. Set IP/Network Mask to 172.20. 120.123/255.255.255.0.

c. Edit port 1 interface and set IP/Network Mask to 192.168.1.99/255.255.255.0.

d. Click OK.

e. Go to Policy & Objects > Address and create an address for internal subnet 192.168.1.0.

2. Configure user and user group.

a. Go to User & Device > User Definition to create a local user sslvpnuser1.

b. Go to User & Device > User Groups to create a group ss/vpngroup with the member sslvpnusert.

3. Configure SSL VPN web portal.

a. Go to VPN > SSL-VPN Portals to create a tunnel mode only portal my-split-tunnel-portal.

b. Enable Split Tunneling.

c. Select Routing Address to define the destination network that will be routed through the tunnel. Leav undefined to use the destination in the respective firewall policies.

4. Configure SSL VPN settings.

a. Go to VPN > SSL-VPN Settings.

b. For Listen on Interface(s), select wan1.

c. Set Listen on Port to 10443.

d. Optionally, set Restrict Access to Limit access to specific hosts, and specify the addresses of the host are allowed to connect to this VPN.

e. Choose a certificate for Server Certificate. The default is Fortinet_Factory.

f. In Authentication/Portal Mapping All Other Users/Groups, set the Portal to tunnel-access.

g. Create new Authentication/Portal Mapping for group sslvpngroup mapping portal my-split-tu

5. Configure SSL VPN firewall policy.

a. Go to Policy & Objects > IPv4 Policy.

b. Fill in the firewall policy name. In this example, sslvpn split tunnel access.

c. Incoming interface must be SSL-VPN tunnel interface(ssl.root).

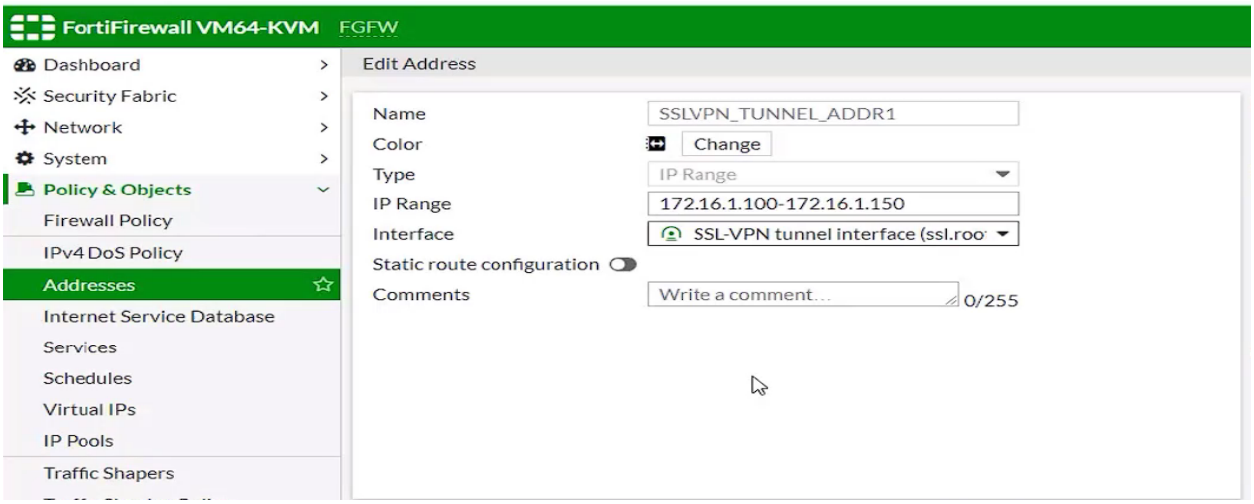
d. Choose an Outgoing Interface. In this example, port1.

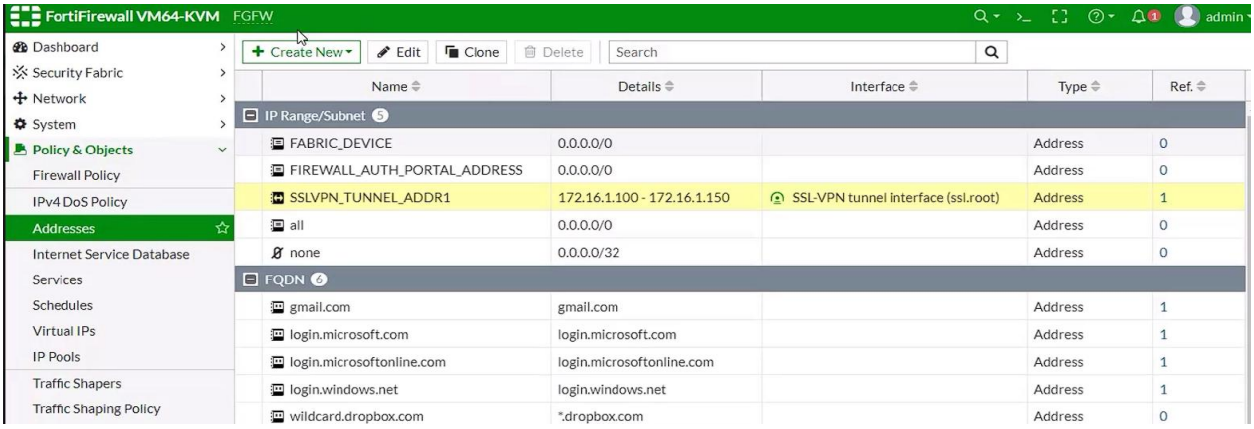
e. Set the Source to SSLVPN_TUNNEL_ADDR1 and group to ss/vpngroup. The source address the tunnel IP addresses that the remote clients are using.

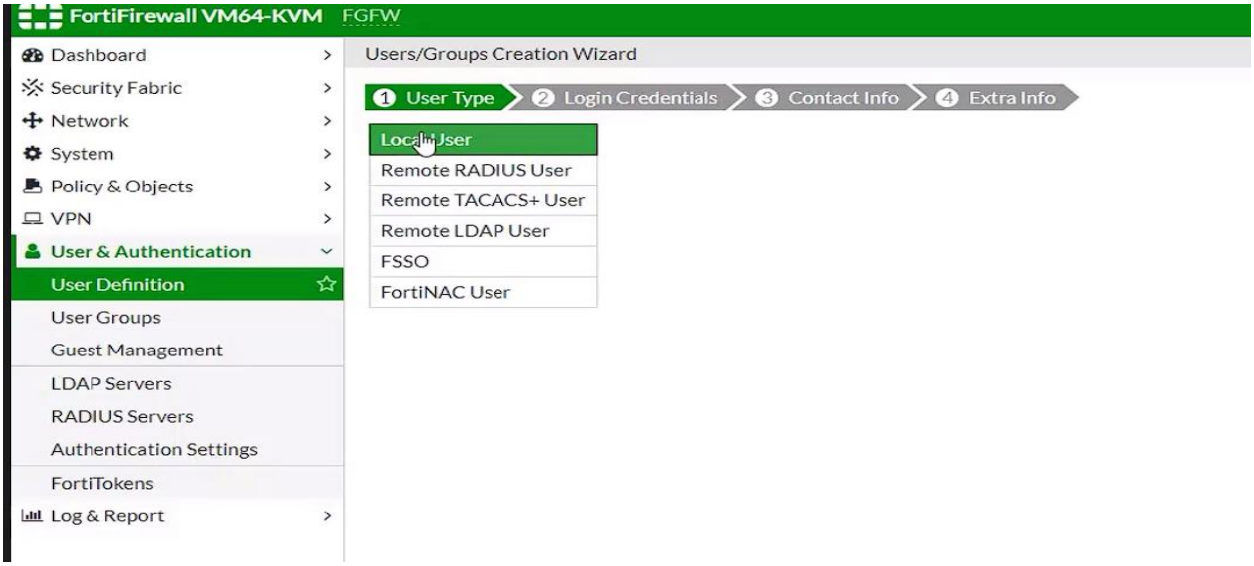
f. In this example, the Destination is 192.168.1.0.

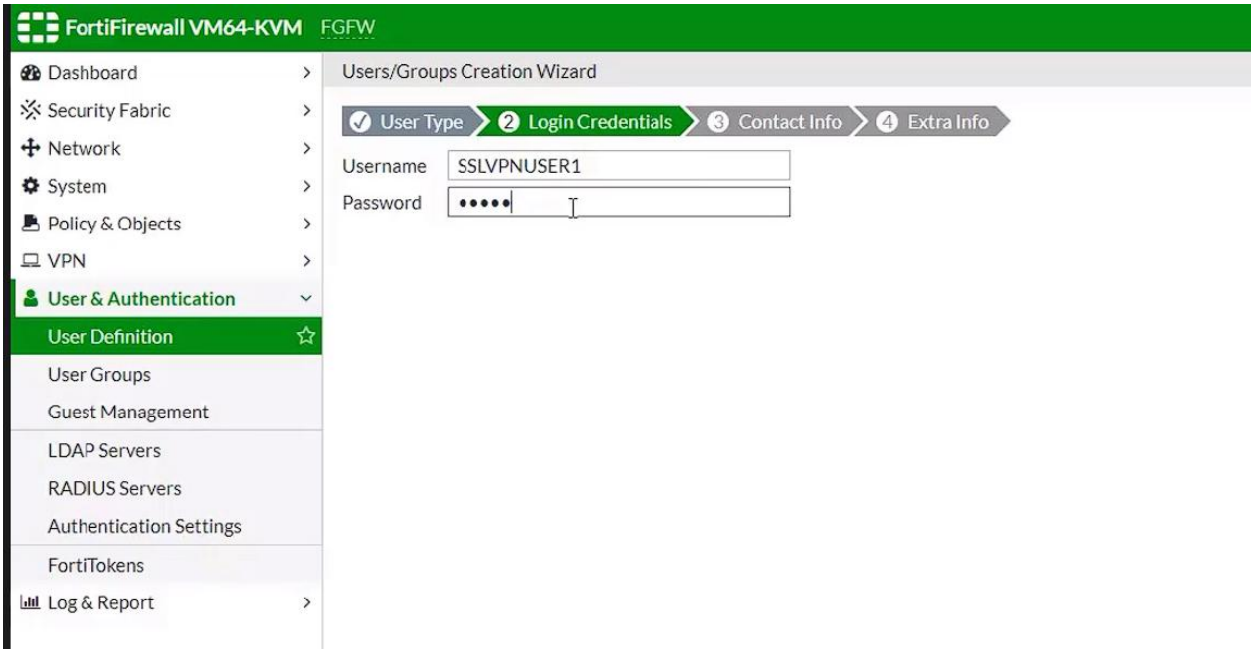
g. Set Schedule to always, Service to ALL, and Action to Accept.

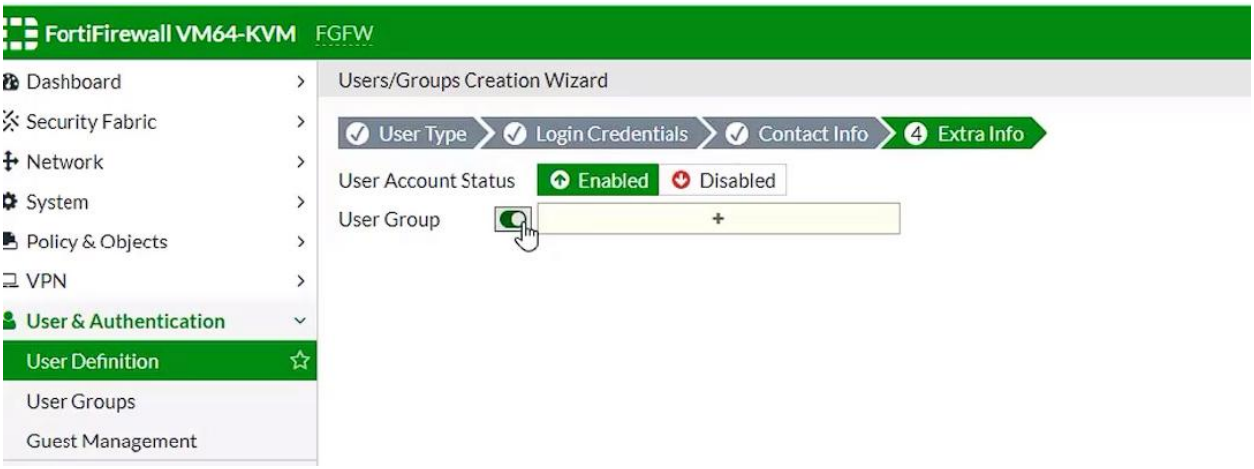
h. Click OK.

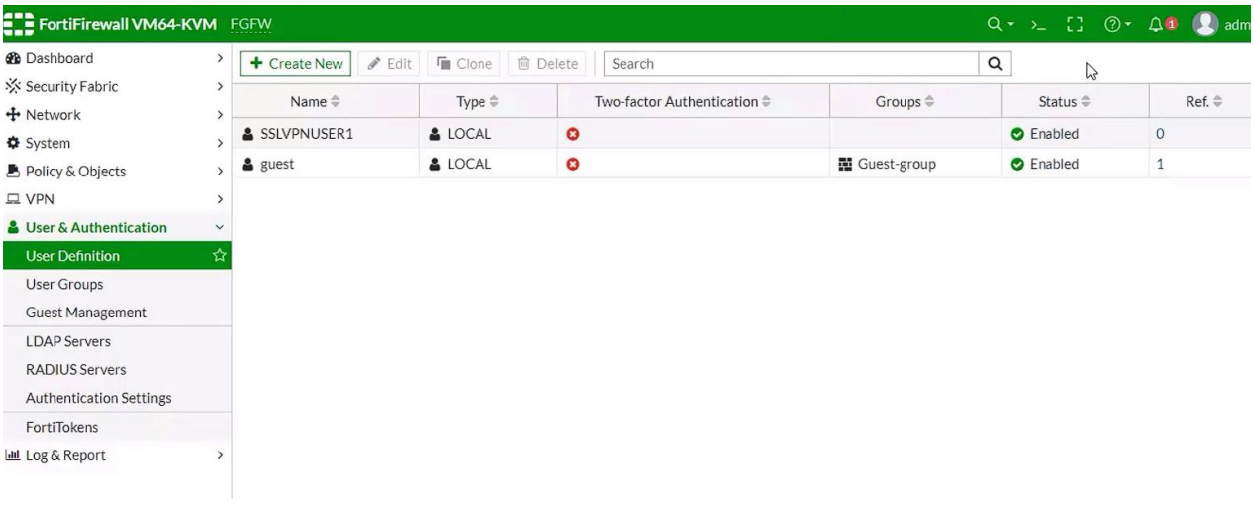

FortiFirewall VM64-KVM
FGFW
Dashboard
Security Fabric
Network
System
Policy & Objects
Firewall Policy
IPv4 DoS Policy
Addresses
Internet Service Database
Services
Schedules
Virtual IPs
IP Pools
Traffic Shapers
Edit Address
Name
SSLVPN_TUNNEL_ADDR1
Color
Change
Type
IP Range
IP Range
172.16.1.100-172.16.1.150
Interface
SSL-VPN tunnel interface (ssl.roo
Static route configuration
Comments
Write a comment...
0/255

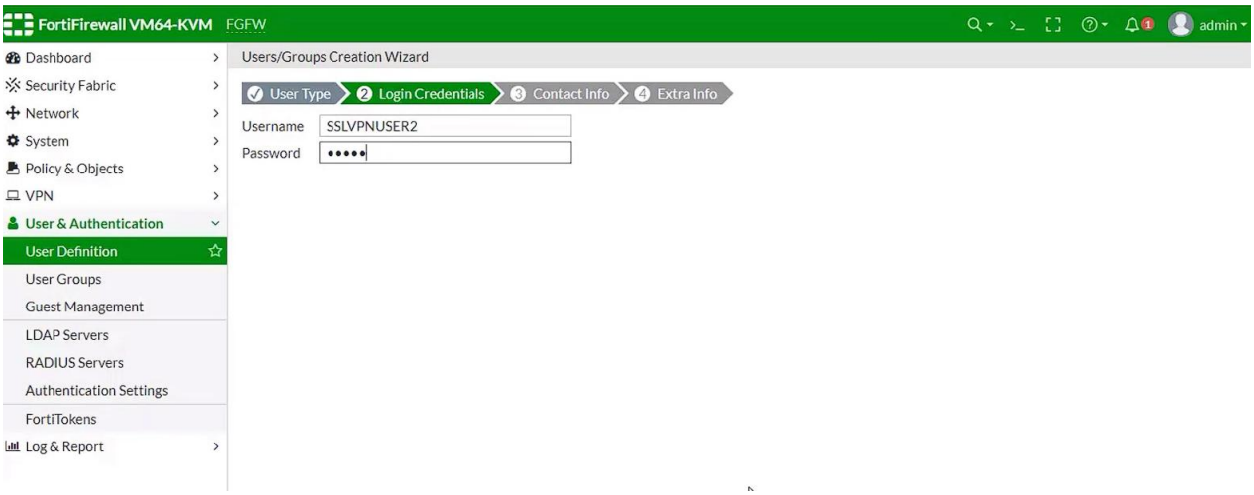

FortiFirewall VM64-KVM
FGFW
admin
Create New
Edit
Clone
Delete
Search
Name
Details
Interface
Type
Ref.
IP Range/Subnet 5
FABRIC_DEVICE
0.0.0.0/0
Address
0
FIREWALL_AUTH_PORTAL_ADDRESS
0.0.0.0/0
Address
0
SSLVPN_TUNNEL_ADDR1
172.16.1.100 - 172.16.1.150
SSL-VPN tunnel interface (ssl.root)
Address
1
all
0.0.0.0/0
Address
0
none
0.0.0.0/32
Address
0
FQDN 6
gmail.com
gmail.com
Address
1
login.microsoft.com
login.microsoft.com
Address
1
login.microsoftonline.com
login.microsoftonline.com
Address
1
login.windows.net
login.windows.net
Address
1
wildcard.dropbox.com
*.dropbox.com
Address
0

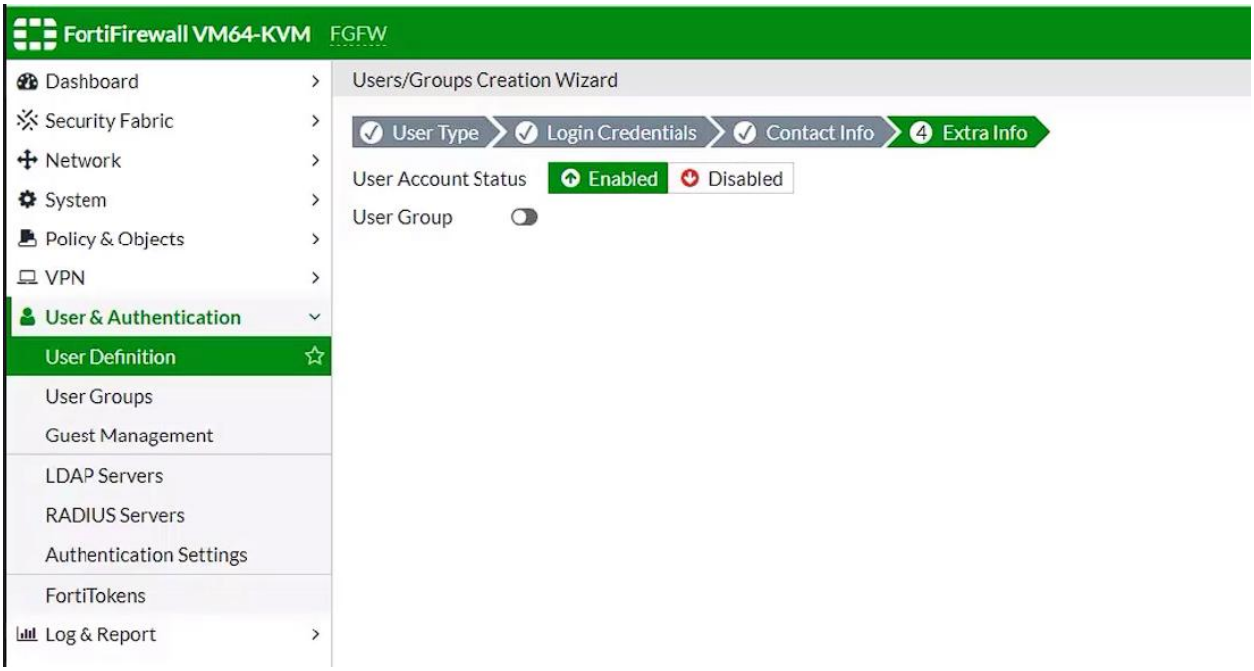

FortiFirewall VM64-KVM
FGFW
Dashboard
Security Fabric
Network
System
Policy & Objects
VPN
User & Authentication
User Definition
User Groups
Guest Management
LDAP Servers
RADIUS Servers
Authentication Settings
FortiTokens
Log & Report
Users/Groups Creation Wizard
1 User Type
2 Login Credentials
3 Contact Info
4 Extra Info
Local User
Remote RADIUS User
Remote TACACS+ User
Remote LDAP User
FSSO
FortiNAC User

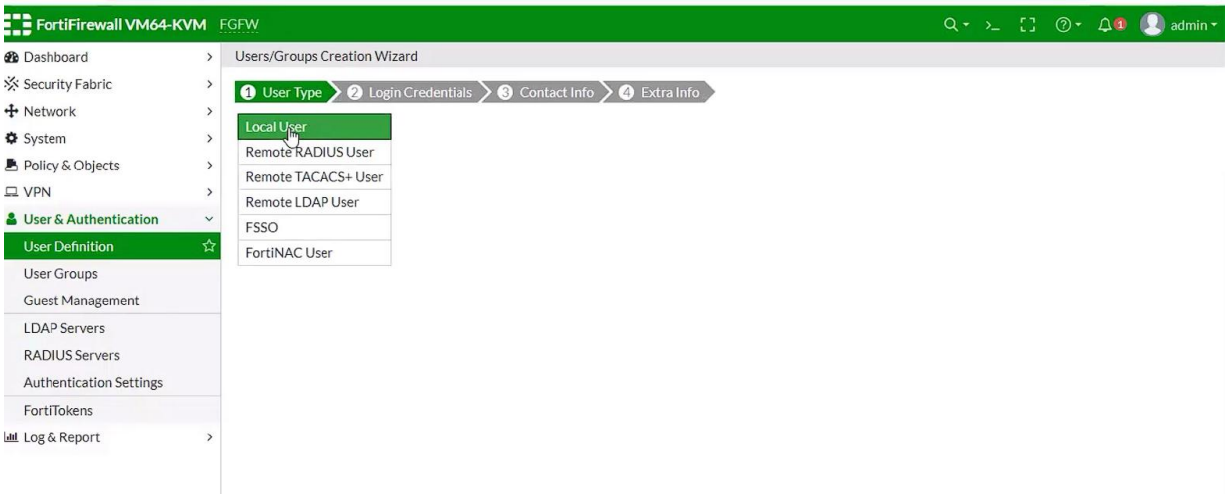

FortiFirewall VM64-KVM
FGFW
Dashboard
Security Fabric
Network
System
Policy & Objects
VPN
User & Authentication
User Definition
User Groups
Guest Management
LDAP Servers
RADIUS Servers
Authentication Settings
FortiTokens
Log & Report
Users/Groups Creation Wizard
User Type
2 Login Credentials
3 Contact Info
4 Extra Info
Username
SSLVPNUSER1
Password

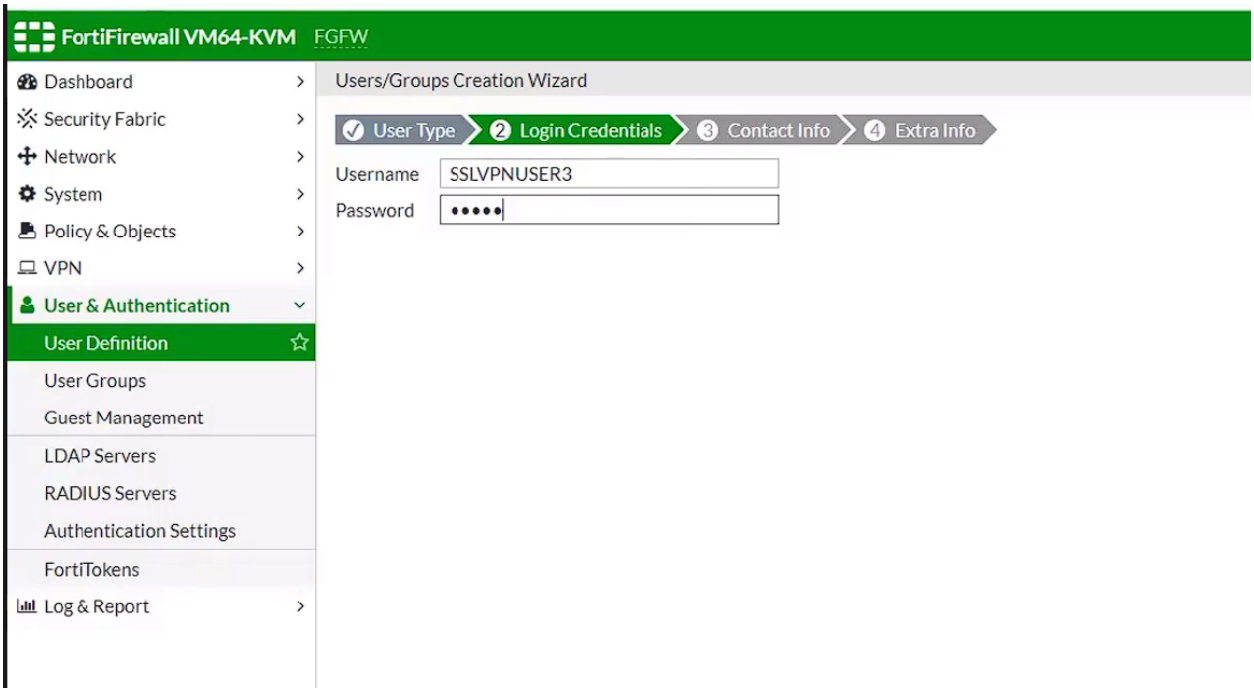

FortiFirewall VM64-KVM
FGFW
Dashboard
Security Fabric
Network
System
Policy & Objects
VPN
User & Authentication
User Definition
User Groups
Guest Management
Users/Groups Creation Wizard
User Type
Login Credentials
Contact Info
4 Extra Info
User Account Status
Enabled
Disabled
User Group

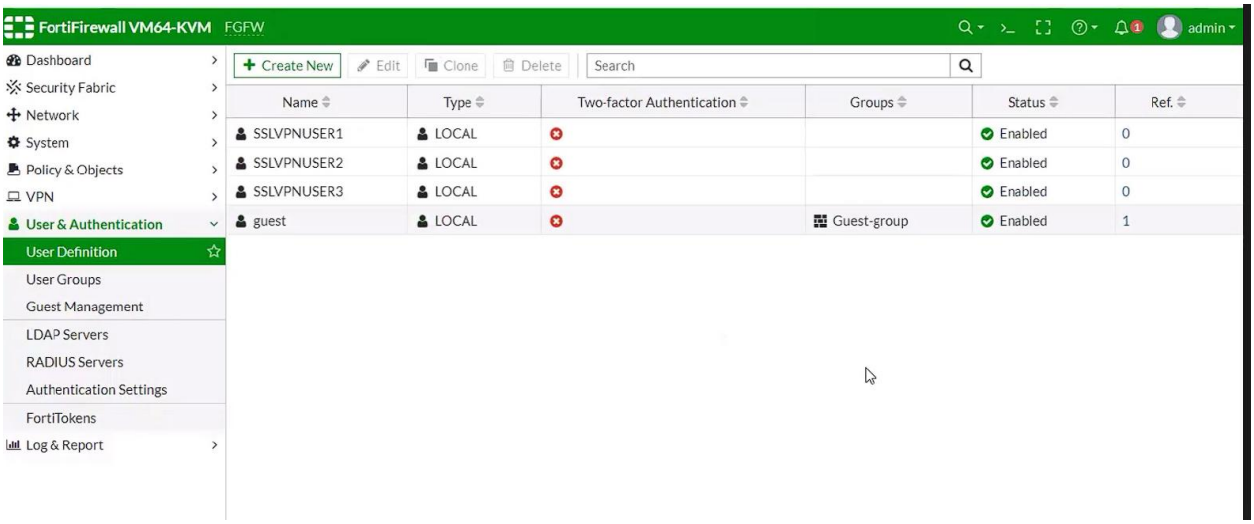

FortiFirewall VM64-KVM
FGFW
Create New
Edit
Clone
Delete
Search
Name
Type
Two-factor Authentication
Groups
Status
Ref.
SSLVPNUSER1
LOCAL
Enabled
0
guest
LOCAL
Guest-group
Enabled
1
Dashboard
Security Fabric
Network
System
Policy & Objects
VPN
User & Authentication
User Definition
User Groups
Guest Management
LDAP Servers
RADIUS Servers
Authentication Settings
FortiTokens
Log & Report

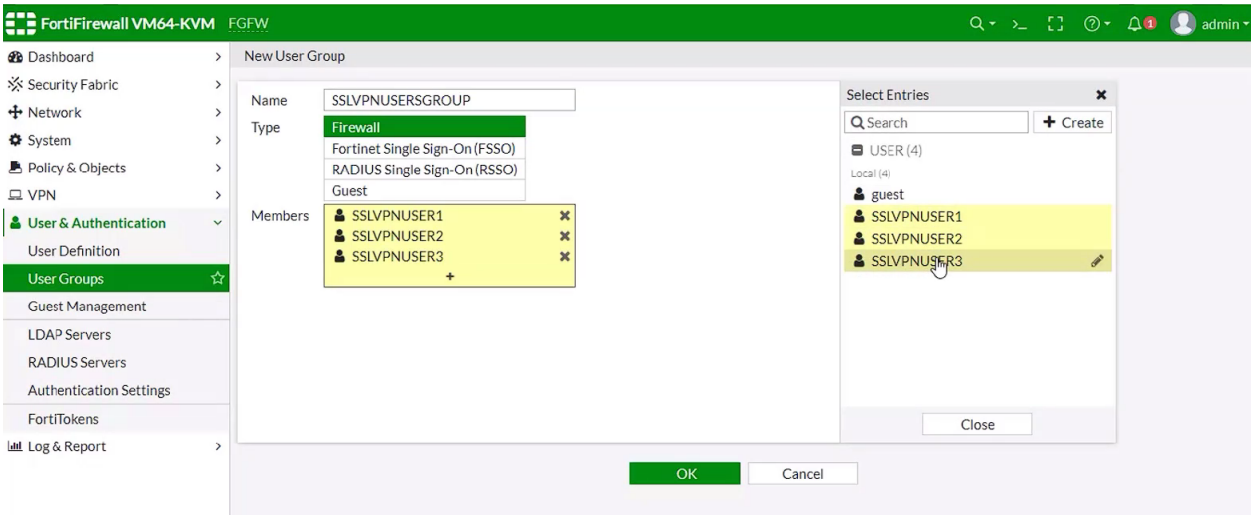

FortiFirewall VM64-KVM
FGFW
admin
Dashboard
Security Fabric
Network
System
Policy & Objects
VPN
User & Authentication
User Definition
User Groups
Guest Management
LDAP Servers
RADIUS Servers
Authentication Settings
FortiTokens
Log & Report
Users/Groups Creation Wizard
User Type
Login Credentials
Contact Info
Extra Info
Username
SSLVPNUSER2
Password

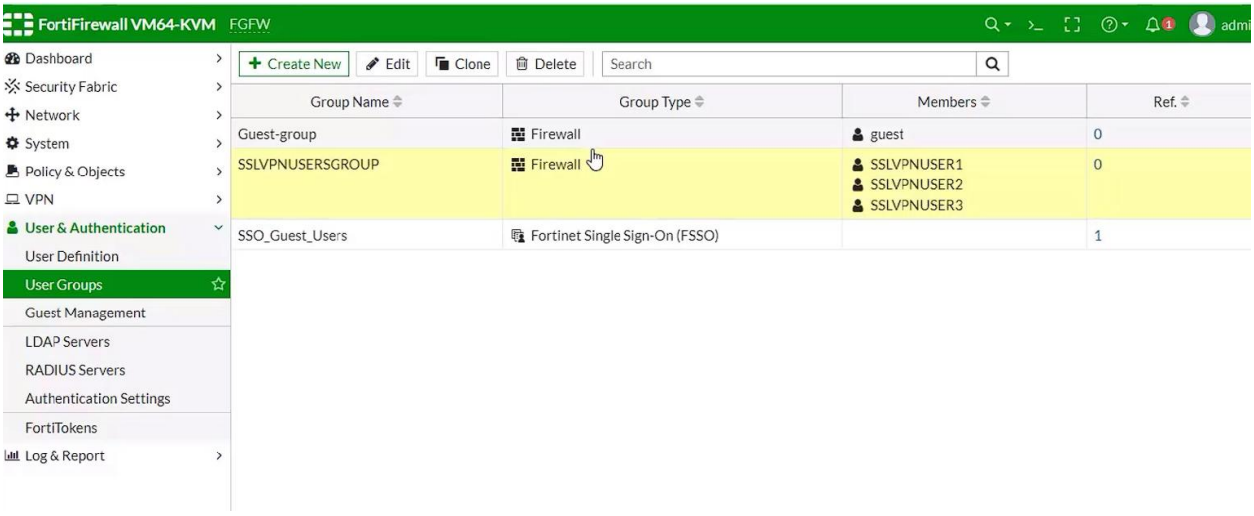

FortiFirewall VM64-KVM
FGFW
Dashboard
Security Fabric
Network
System
Policy & Objects
VPN
User & Authentication
User Definition
User Groups
Guest Management
LDAP Servers
RADIUS Servers
Authentication Settings
FortiTokens
Log & Report
Users/Groups Creation Wizard
User Type
Login Credentials
Contact Info
4 Extra Info
User Account Status
Enabled
Disabled
User Group

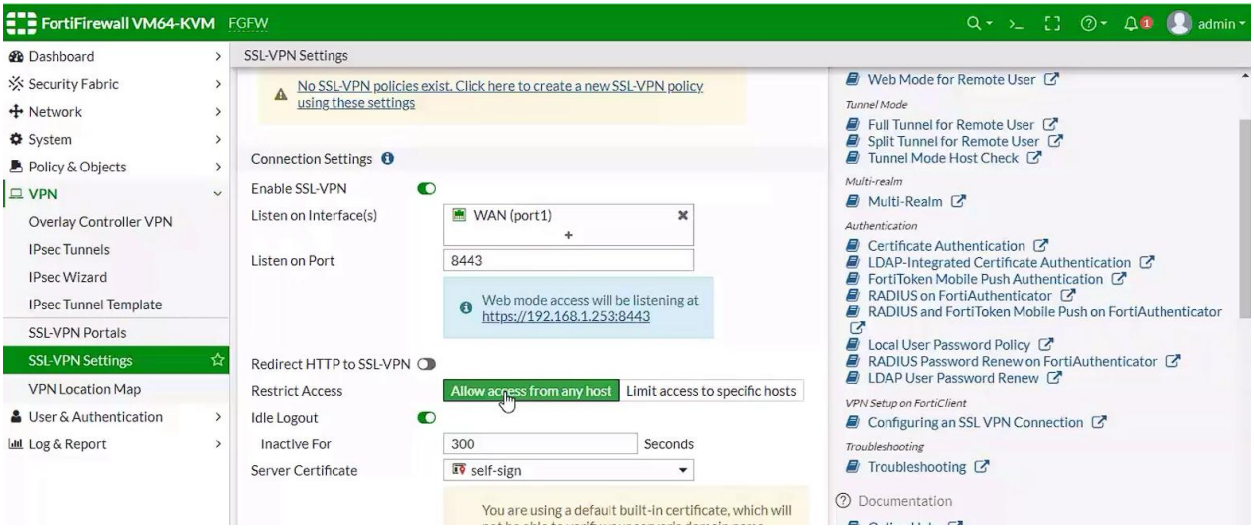

FortiFirewall VM64-KVM
FGFW
admin
Dashboard
Security Fabric
Network
System
Policy & Objects
VPN
User & Authentication
User Definition
User Groups
Guest Management
LDAP Servers
RADIUS Servers
Authentication Settings
FortiTokens
Log & Report
Users/Groups Creation Wizard
1 User Type
Login Credentials
Contact Info
Extra Info
Local User
Remote RADIUS User
Remote TACACS+ User
Remote LDAP User
FSSO
FortiNAC User

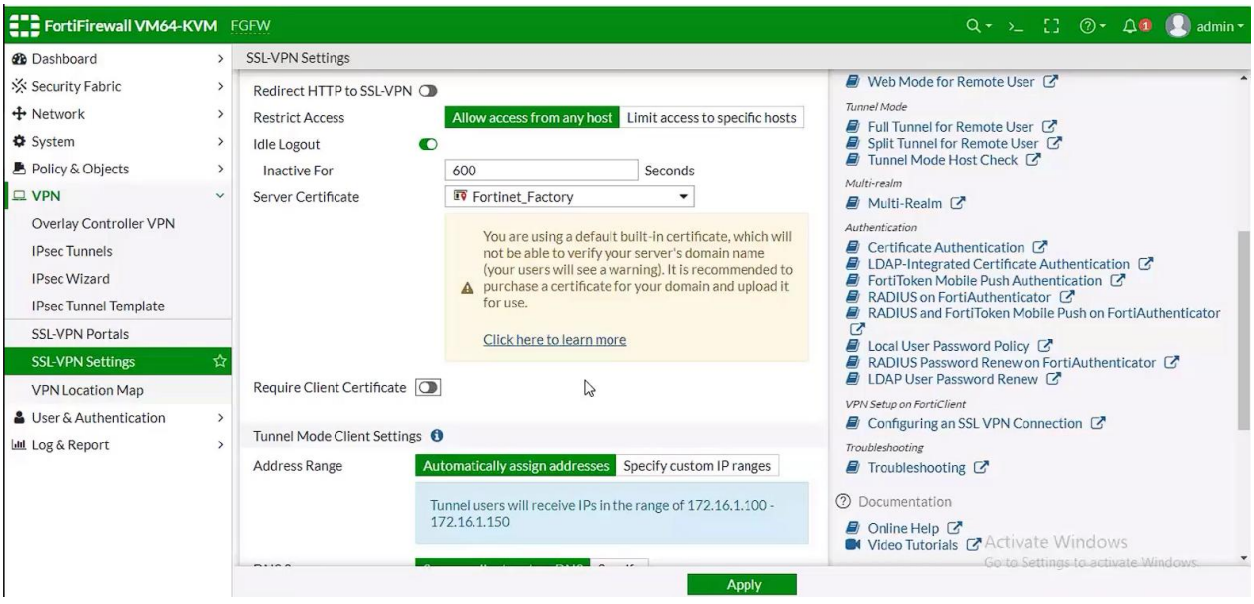

FortiFirewall VM64-KVM
FGFW
Dashboard
Security Fabric
Network
System
Policy & Objects
VPN
User & Authentication
User Definition
User Groups
Guest Management
LDAP Servers
RADIUS Servers
Authentication Settings
FortiTokens
Log & Report
Users/Groups Creation Wizard
User Type
2 Login Credentials
3 Contact Info
4 Extra Info
Username
SSLVPNUSER3
Password

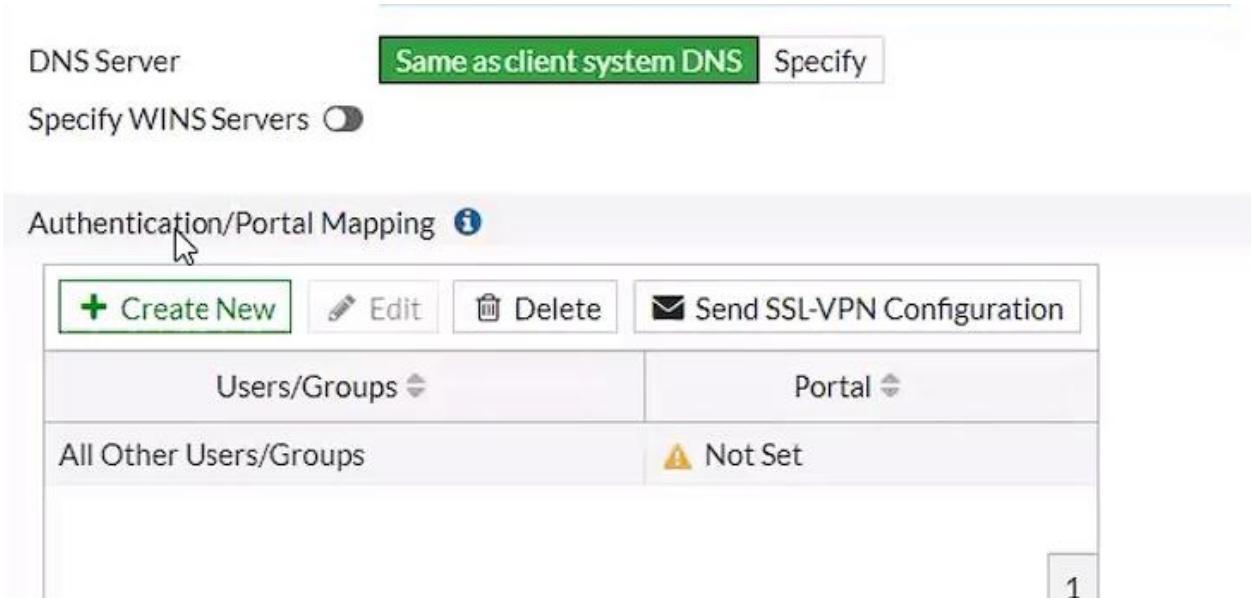

FortiFirewall VM64-KVM
FGFW
admin
Create New
Edit
Clone
Delete
Search
Name
Type
Two-factor Authentication
Groups
Status
Ref.
SSLVPNUSER1 LOCAL Enabled 0
SSLVPNUSER2 LOCAL Enabled 0
SSLVPNUSER3 LOCAL Enabled 0
guest LOCAL Guest-group Enabled 1

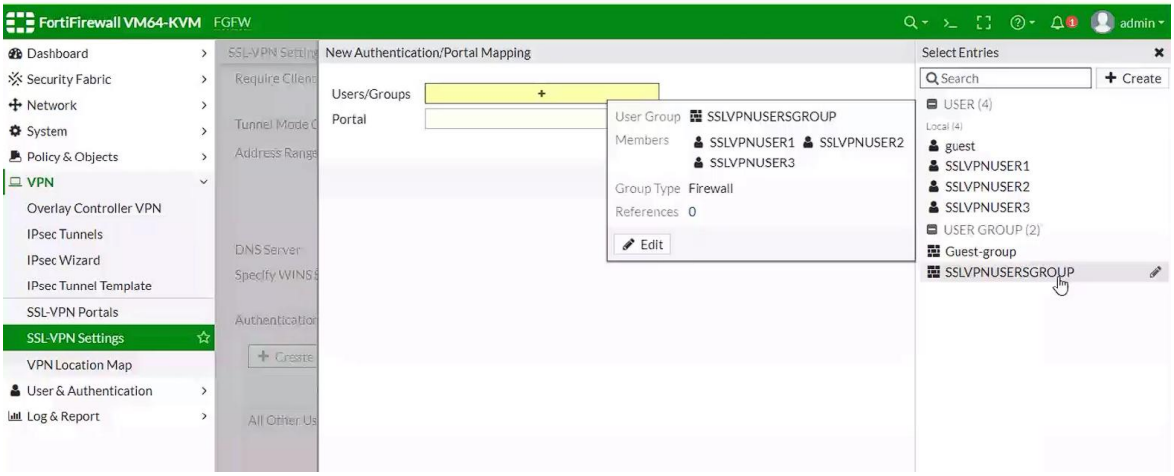

FortiFirewall VM64-KVM
FGFW
admin
New User Group
Name
SSLVPNUSERSGROUP
Type
Firewall
Fortinet Single Sign-On (FSSO)
RADIUS Single Sign-On (RSSO)
Guest
Members
SSLVPNUSER1
SSLVPNUSER2
SSLVPNUSER3
Select Entries
Search
Create
USER (4)
Local (4)
guest
SSLVPNUSER1
SSLVPNUSER2
SSLVPNUSER3
Close
OK
Cancel

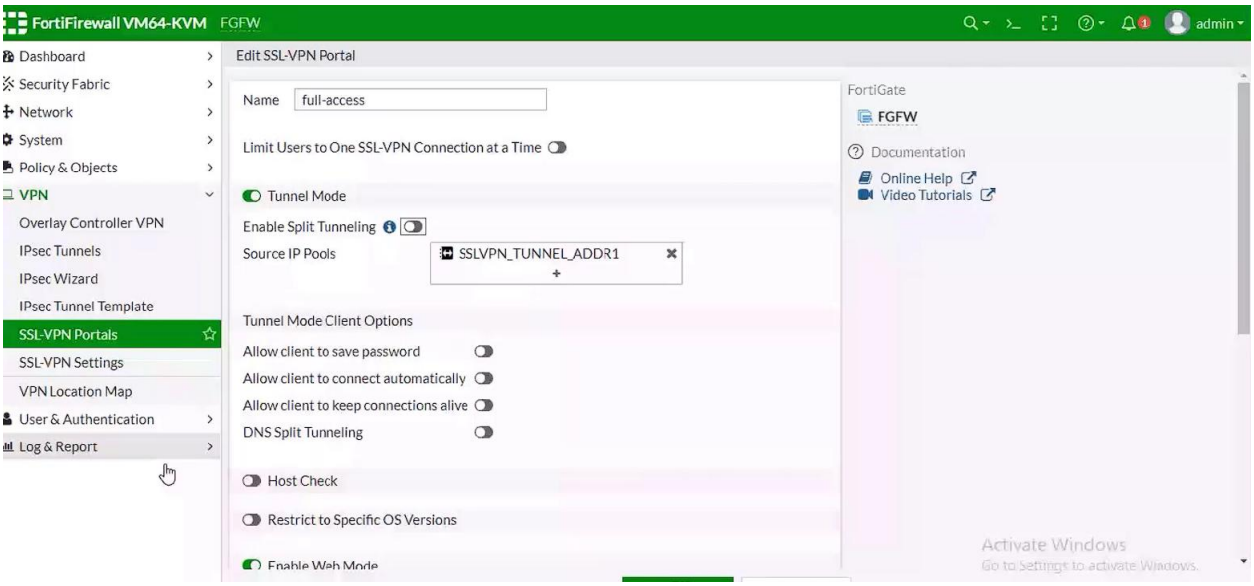

FortiFirewall VM64-KVM FGFW
Dashboard
Security Fabric
Network
System
Policy & Objects
VPN
User & Authentication
User Definition
User Groups
Guest Management
LDAP Servers
RADIUS Servers
Authentication Settings
FortiTokens
Log & Report
Create New
Edit
Clone
Delete
Search
Group Name
Group Type
Members
Ref.
Guest-group
Firewall
guest
0
SSLVPNUSERSGROUP
Firewall
SSLVPNUSER1
SSLVPNUSER2
SSLVPNUSER3
0
SSO_Guest_Users
Fortinet Single Sign-On (FSSO)
1


FortiFirewall VM64-KVM FGFW
admin
SSL-VPN Settings
No SSL-VPN policies exist. Click here to create a new SSL-VPN policy using these settings
Connection Settings
Enable SSL-VPN
Listen on Interface(s)
WAN (port1)
Listen on Port
8443
Web mode access will be listening at https://192.168.1.253:8443
Redirect HTTP to SSL-VPN
Restrict Access
Allow access from any host
Limit access to specific hosts
Idle Logout
Inactive For
300
Seconds
Server Certificate
self-sign
You are using a default built-in certificate, which will
Web Mode for Remote User
Tunnel Mode
Full Tunnel for Remote User
Split Tunnel for Remote User
Tunnel Mode Host Check
Multi-realm
Multi-Realm
Authentication
Certificate Authentication
LDAP-Integrated Certificate Authentication
FortiToken Mobile Push Authentication
RADIUS on FortiAuthenticator
RADIUS and FortiToken Mobile Push on FortiAuthenticator
Local User Password Policy
RADIUS Password Renewon FortiAuthenticator
LDAP User Password Renew
VPN Setup on FortiClient
Configuring an SSL VPN Connection
Troubleshooting
Troubleshooting
Documentation

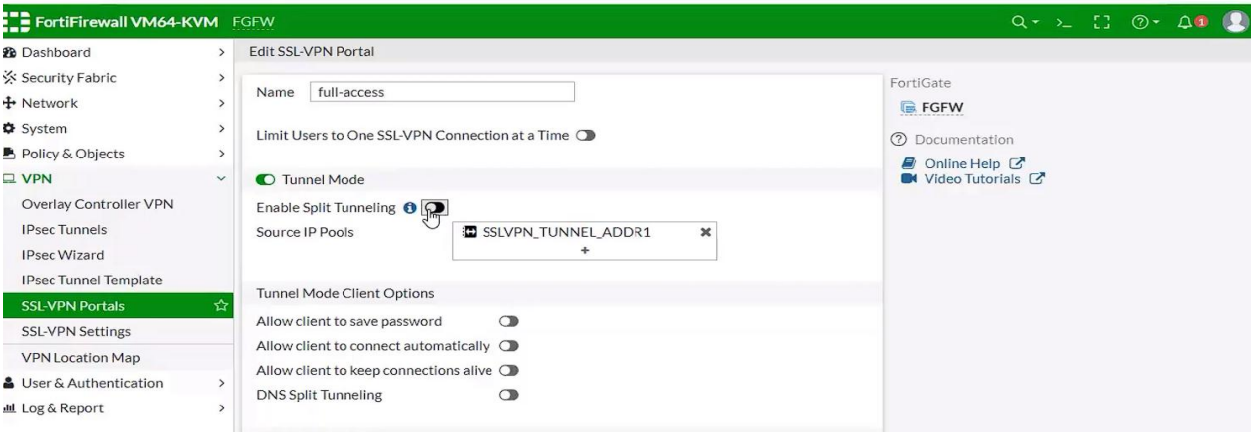

FortiFirewall VM64-KVM FGFW
admin
SSL-VPN Settings
Redirect HTTP to SSL-VPN
Restrict Access
Allow access from any host
Limit access to specific hosts
Idle Logout
Inactive For
600
Seconds
Server Certificate
Fortinet_Factory
You are using a default built-in certificate, which will not be able to verify your server's domain name (your users will see a warning). It is recommended to purchase a certificate for your domain and upload it for use.
Click here to learn more
Require Client Certificate
Tunnel Mode Client Settings
Address Range
Automatically assign addresses
Specify custom IP ranges
Tunnel users will receive IPs in the range of 172.16.1.100 - 172.16.1.150
Apply
Web Mode for Remote User
Tunnel Mode
Full Tunnel for Remote User
Split Tunnel for Remote User
Tunnel Mode Host Check
Multi-realm
Multi-Realm
Authentication
Certificate Authentication
LDAP-Integrated Certificate Authentication
FortiToken Mobile Push Authentication
RADIUS on FortiAuthenticator
RADIUS and FortiToken Mobile Push on FortiAuthenticator
Local User Password Policy
RADIUS Password Renewon FortiAuthenticator
LDAP User Password Renew
VPN Setup on FortiClient
Configuring an SSL VPN Connection
Troubleshooting
Troubleshooting
Documentation
Online Help
Video Tutorials
Activate Windows
Go to Settings to activate Windows.

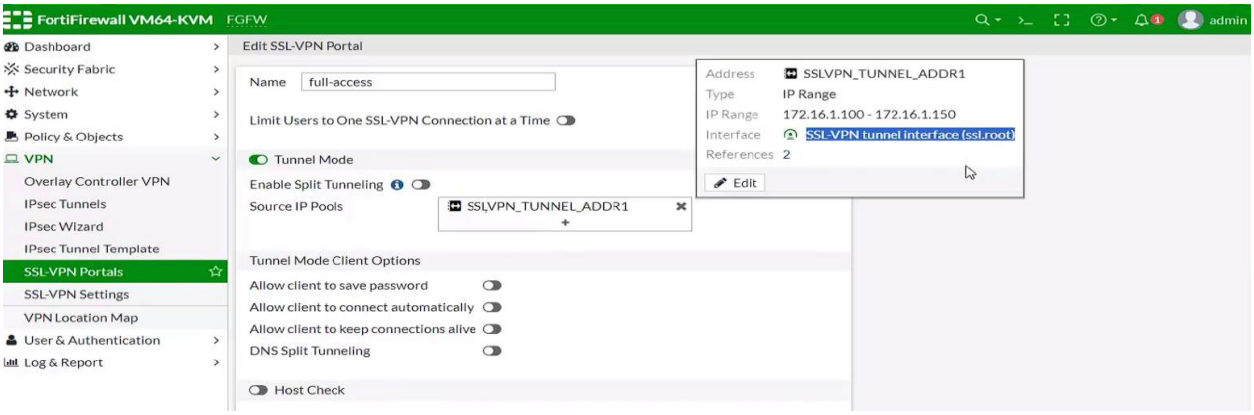

DNS Server
Same as client system DNS
Specify
Specify WINS Servers
Authentication/Portal Mapping
Create New
Edit
Delete
Send SSL-VPN Configuration
Users/Groups
Portal
All Other Users/Groups
Not Set
1

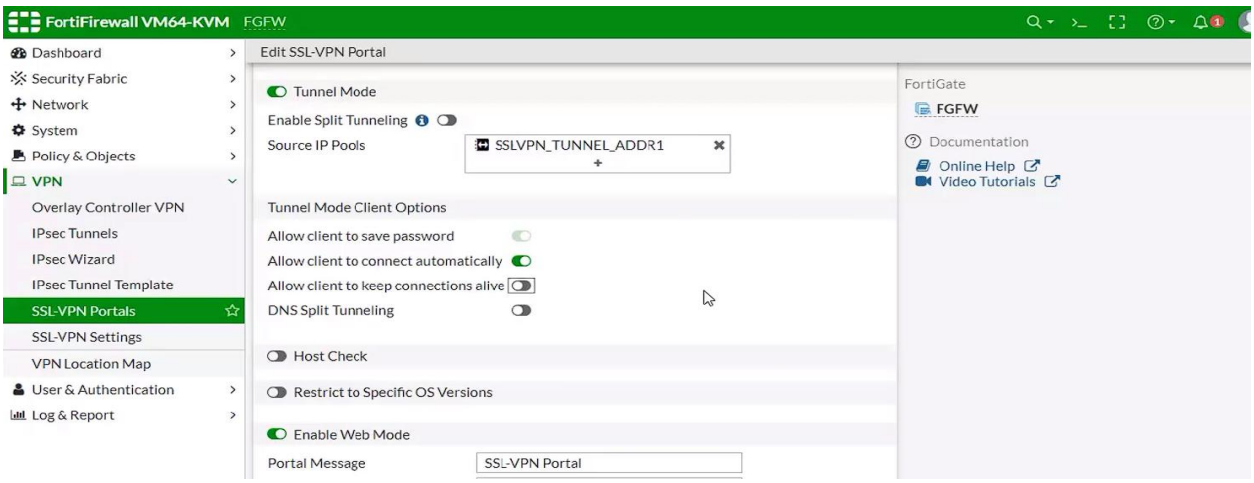

FortiFirewall VM64-KVM
FGFW
admin
Dashboard
Security Fabric
Network
System
Policy & Objects
VPN
Overlay Controller VPN
IPsec Tunnels
IPsec Wizard
IPsec Tunnel Template
SSL-VPN Portals
SSL-VPN Settings
VPN Location Map
User & Authentication
Log & Report
New Authentication/Portal Mapping
Users/Groups
Portal
User Group SSLVPNUSERSGROUP
Members SSLVPNUSER1 SSLVPNUSER2 SSLVPNUSER3
Group Type Firewall
References 0
Edit
Select Entries
Search
Create
USER (4)
guest
SSLVPNUSER1
SSLVPNUSER2
SSLVPNUSER3
USER GROUP (2)
Guest-group
SSLVPNUSERSGROUP

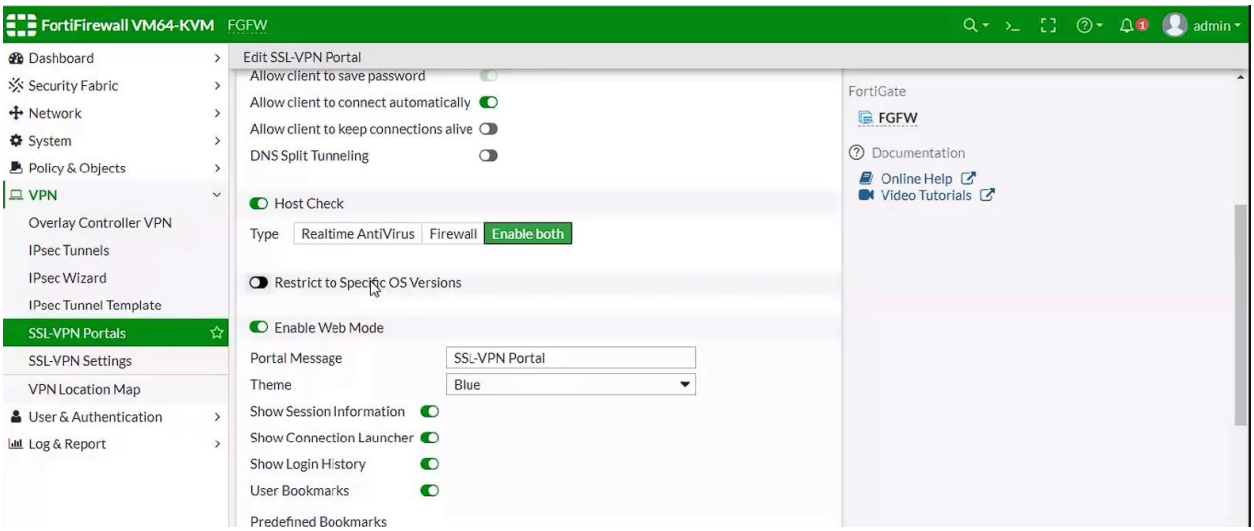

FortiFirewall VM64-KVM
FGFW
admin
Edit SSL-VPN Portal
Name full-access
Limit Users to One SSL-VPN Connection at a Time
Tunnel Mode
Enable Split Tunneling
Source IP Pools
SSLVPN_TUNNEL_ADDR1
Tunnel Mode Client Options
Allow client to save password
Allow client to connect automatically
Allow client to keep connections alive
DNS Split Tunneling
Host Check
Restrict to Specific OS Versions
Enable Web Mode
FortiGate
FGFW
Documentation
Online Help
Video Tutorials
Activate Windows

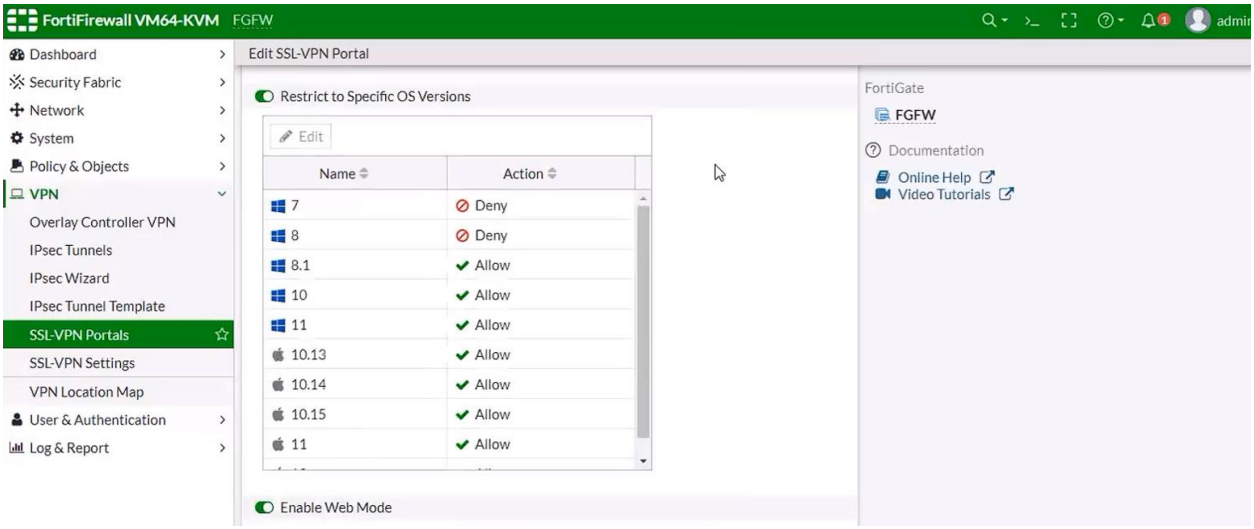

admin
Login

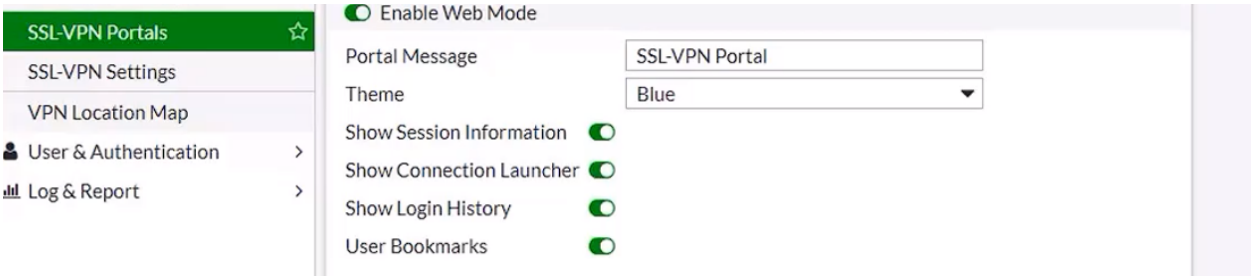

FortiFirewall VM64-KVM
FGFW
Dashboard
Security Fabric
Network
System
Policy & Objects
VPN
Overlay Controller VPN
IPsec Tunnels
IPsec Wizard
IPsec Tunnel Template
SSL-VPN Portals
SSL-VPN Settings
VPN Location Map
User & Authentication
Log & Report
Edit SSL-VPN Portal
Name
full-access
Limit Users to One SSL-VPN Connection at a Time
Tunnel Mode
Enable Split Tunneling
Source IP Pools
SSLVPN_TUNNEL_ADDR1
Tunnel Mode Client Options
Allow client to save password
Allow client to connect automatically
Allow client to keep connections alive
DNS Split Tunneling
FortiGate
FGFW
Documentation
Online Help
Video Tutorials

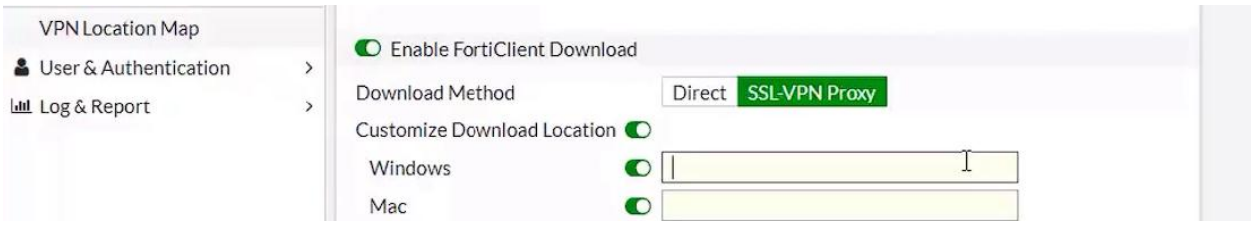

FortiFirewall VM64-KVM
FGFW
admin
Edit SSL-VPN Portal
Name
full-access
Limit Users to One SSL-VPN Connection at a Time
Tunnel Mode
Enable Split Tunneling
Source IP Pools
SSLVPN_TUNNEL_ADDR1
Tunnel Mode Client Options
Allow client to save password
Allow client to connect automatically
Allow client to keep connections alive
DNS Split Tunneling
Host Check
Address
SSLVPN_TUNNEL_ADDR1
Type
IP Range
IP Range
172.16.1.100 - 172.16.1.150
Interface
SSL-VPN tunnel interface (ssl.root)
References
2
Edit

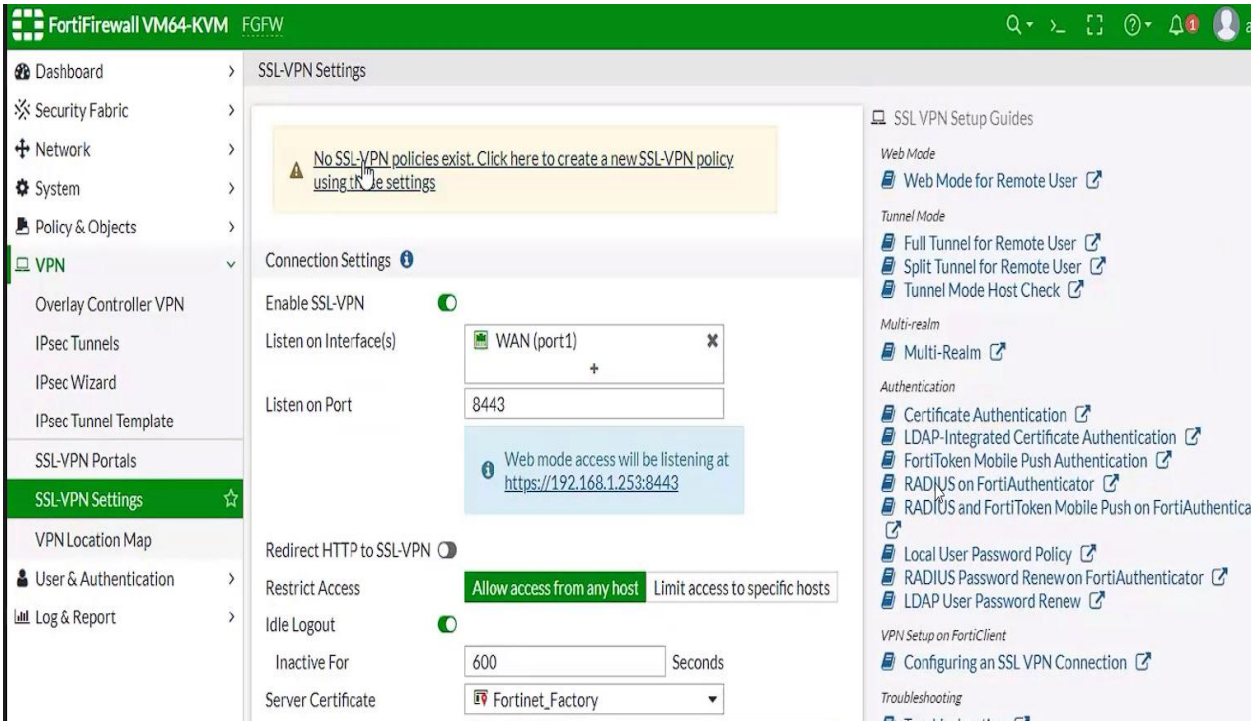

FortiFirewall VM64-KVM
FGFW
Edit SSL-VPN Portal
Tunnel Mode
Enable Split Tunneling
Source IP Pools
SSLVPN_TUNNEL_ADDR1
Tunnel Mode Client Options
Allow client to save password
Allow client to connect automatically
Allow client to keep connections alive
DNS Split Tunneling
Host Check
Restrict to Specific OS Versions
Enable Web Mode
Portal Message
SSL-VPN Portal
FortiGate
FGFW
Documentation
Online Help
Video Tutorials

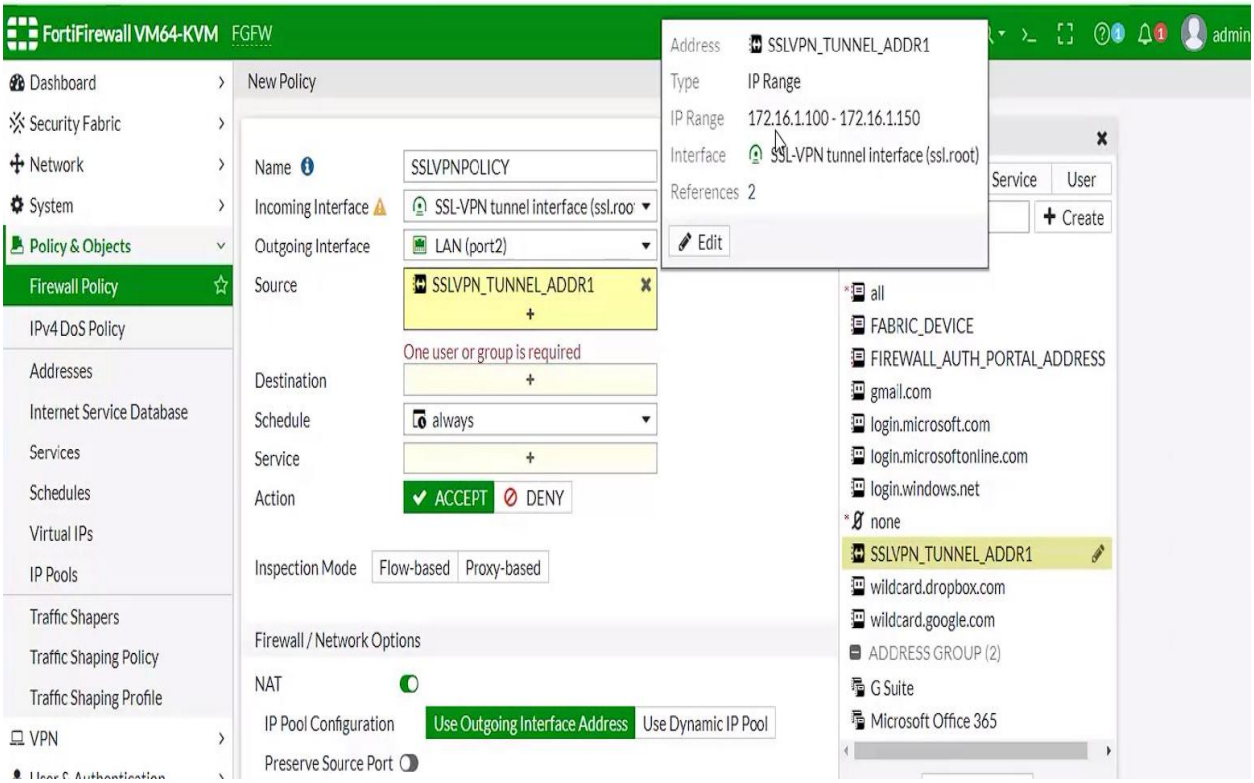

FortiFirewall VM64-KVM FGFW
admin
Dashboard
Security Fabric
Network
System
Policy & Objects
VPN
Overlay Controller VPN
IPsec Tunnels
IPsec Wizard
IPsec Tunnel Template
SSL-VPN Portals
SSL-VPN Settings
VPN Location Map
User & Authentication
Log & Report
Edit SSL-VPN Portal
Allow client to save password
Allow client to connect automatically
Allow client to keep connections alive
DNS Split Tunneling
Host Check
Type
Realtime AntiVirus
Firewall
Enable both
Restrict to Specific OS Versions
Enable Web Mode
Portal Message
SSL-VPN Portal
Theme
Blue
Show Session Information
Show Connection Launcher
Show Login History
User Bookmarks
Predefined Bookmarks
FortiGate
FGFW
Documentation
Online Help
Video Tutorials

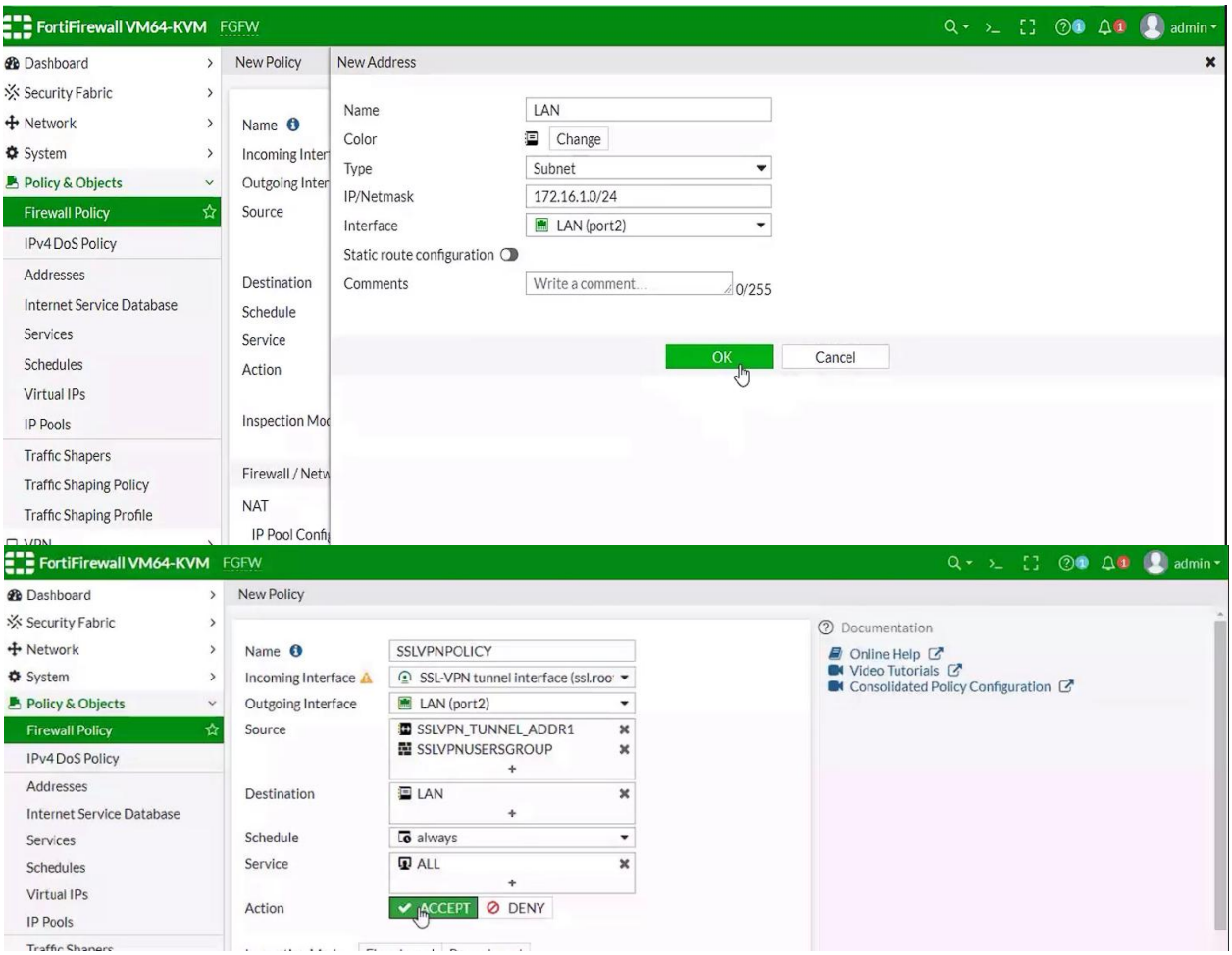

FortiFirewall VM64-KVM FGFW
admin
Dashboard
Security Fabric
Network
System
Policy & Objects
VPN
Overlay Controller VPN
IPsec Tunnels
IPsec Wizard
IPsec Tunnel Template
SSL-VPN Portals
SSL-VPN Settings
VPN Location Map
User & Authentication
Log & Report
Edit SSL-VPN Portal
Restrict to Specific OS Versions
Edit
Name
Action
7 Deny
8 Deny
8.1 Allow
10 Allow
11 Allow
10.13 Allow
10.14 Allow
10.15 Allow
11 Allow
Enable Web Mode
FortiGate
FGFW
Documentation
Online Help
Video Tutorials

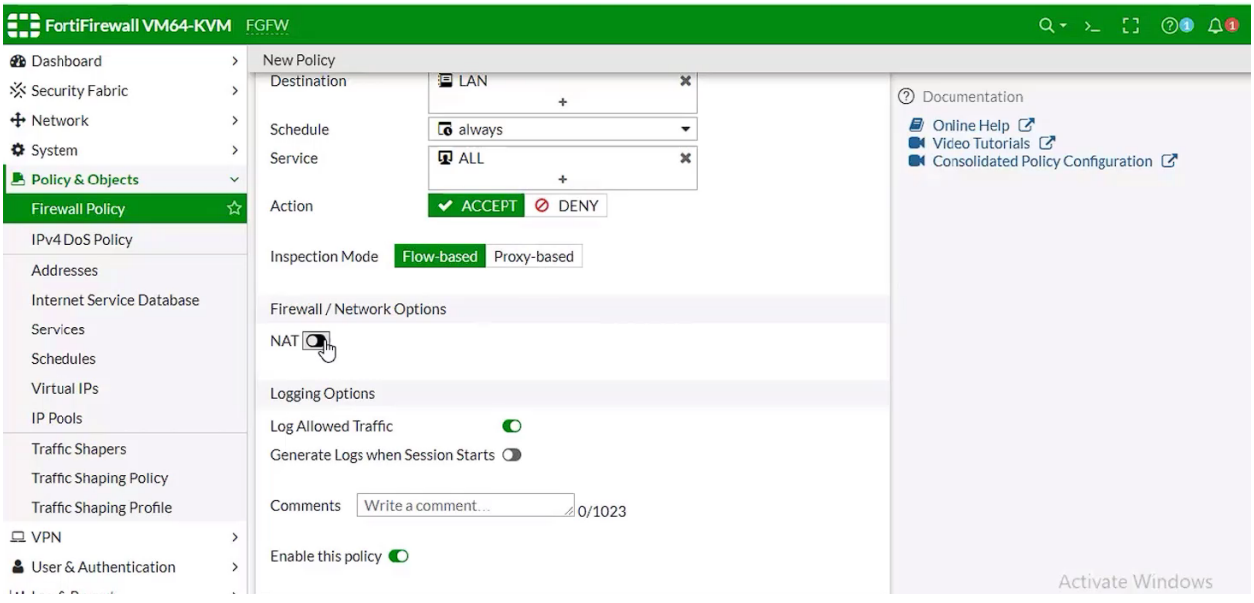

SSL-VPN Portals
SSL-VPN Settings
VPN Location Map
User & Authentication
Log & Report
Enable Web Mode
Portal Message
SSL-VPN Portal
Theme
Blue
Show Session Information
Show Connection Launcher
Show Login History
User Bookmarks

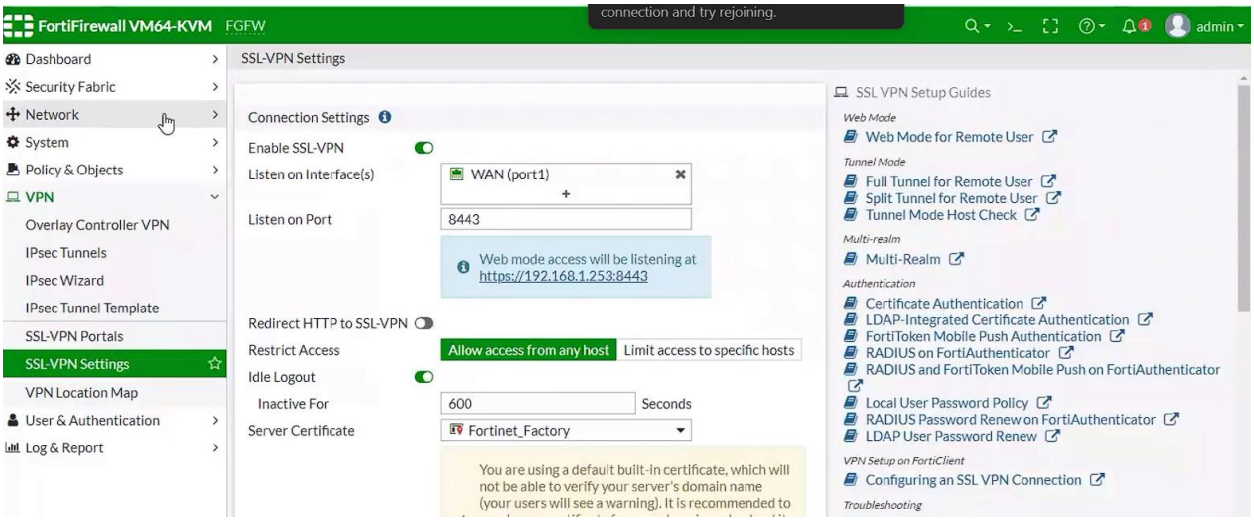

VPN Location Map
User & Authentication
Log & Report
Enable FortiClient Download
Download Method
Direct
SSL-VPN Proxy
Customize Download Location
Windows
Mac


FortiFirewall VM64-KVM
FGFW
Dashboard
Security Fabric
Network
System
Policy & Objects
VPN
Overlay Controller VPN
IPsec Tunnels
IPsec Wizard
IPsec Tunnel Template
SSL-VPN Portals
SSL-VPN Settings
VPN Location Map
User & Authentication
Log & Report
SSL-VPN Settings
No SSL-VPN policies exist. Click here to create a new SSL-VPN policy using the settings
Connection Settings
Enable SSL-VPN
Listen on Interface(s)
WAN (port1)
Listen on Port
8443
Web mode access will be listening at https://192.168.1.253:8443
Redirect HTTP to SSL-VPN
Restrict Access
Allow access from any host
Limit access to specific hosts
Idle Logout
Inactive For
600
Seconds
Server Certificate
Fortinet_Factory
SSL VPN Setup Guides
Web Mode
Web Mode for Remote User
Tunnel Mode
Full Tunnel for Remote User
Split Tunnel for Remote User
Tunnel Mode Host Check
Multi-realm
Multi-Realm
Authentication
Certificate Authentication
LDAP-Integrated Certificate Authentication
FortiToken Mobile Push Authentication
RADIUS on FortiAuthenticator
RADIUS and FortiToken Mobile Push on FortiAuthentica
Local User Password Policy
RADIUS Password Renew on FortiAuthenticator
LDAP User Password Renew
VPN Setup on FortiClient
Configuring an SSL VPN Connection
Troubleshooting


FortiFirewall VM64-KVM
FGFW
admin
Dashboard
Security Fabric
Network
System
Policy & Objects
Firewall Policy
IPv4 DoS Policy
Addresses
Internet Service Database
Services
Schedules
Virtual IPs
IP Pools
Traffic Shapers
Traffic Shaping Policy
Traffic Shaping Profile
VPN
New Policy
Name
SSLVPNPOLICY
Incoming Interface
SSL-VPN tunnel interface (ssl.roo
Outgoing Interface
LAN (port2)
Source
SSLVPN_TUNNEL_ADDR1
One user or group is required
Destination
Schedule
always
Service
Action
ACCEPT
DENY
Inspection Mode
Flow-based
Proxy-based
Firewall / Network Options
NAT
IP Pool Configuration
Use Outgoing Interface Address
Use Dynamic IP Pool
Preserve Source Port
Address
SSLVPN_TUNNEL_ADDR1
Type
IP Range
IP Range
172.16.1.100 - 172.16.1.150
Interface
SSL-VPN tunnel interface (ssl.root)
References
2
Edit
Service
User
Create
all
FABRIC_DEVICE
FIREWALL_AUTH_PORTAL_ADDRESS
gmail.com
login.microsoft.com
login.microsoftonline.com
login.windows.net
none
SSLVPN_TUNNEL_ADDR1
wildcard.dropbox.com
wildcard.google.com
ADDRESS GROUP (2)
G Suite
Microsoft Office 365


FortiFirewall VM64-KVM
FGFW
admin
Dashboard
Security Fabric
Network
System
Policy & Objects
Firewall Policy
IPv4 DoS Policy
Addresses
Internet Service Database
Services
Schedules
Virtual IPs
IP Pools
Traffic Shapers
Traffic Shaping Policy
Traffic Shaping Profile
New Policy
New Address
Name
Color
Change
Type
Subnet
IP/Netmask
172.16.1.0/24
Interface
LAN (port2)
Static route configuration
Comments
Write a comment...
0/255
OK
Cancel
Destination
Schedule
Service
Action
NAT
SSLVPNPOLICY
Incoming Interface
SSL-VPN tunnel interface (ssl.roo
Outgoing Interface
LAN (port2)
Source
SSLVPN_TUNNEL_ADDR1
SSLVPNUSERSGROUP
LAN
always
ALL
ACCEPT
DENY
Documentation
Online Help
Video Tutorials
Consolidated Policy Configuration


FortiFirewall VM64-KVM
FGFW
Dashboard
Security Fabric
Network
System
Policy & Objects
Firewall Policy
IPv4 DoS Policy
Addresses
Internet Service Database
Services
Schedules
Virtual IPs
IP Pools
Traffic Shapers
Traffic Shaping Policy
Traffic Shaping Profile
VPN
User & Authentication
New Policy
Destination
LAN
Schedule
always
Service
ALL
Action
ACCEPT
DENY
Inspection Mode
Flow-based
Proxy-based
Firewall / Network Options
NAT
Logging Options
Log Allowed Traffic
Generate Logs when Session Starts
Comments
Write a comment...
0/1023
Enable this policy
Documentation
Online Help
Video Tutorials
Consolidated Policy Configuration
Activate Windows



Testing the Lab

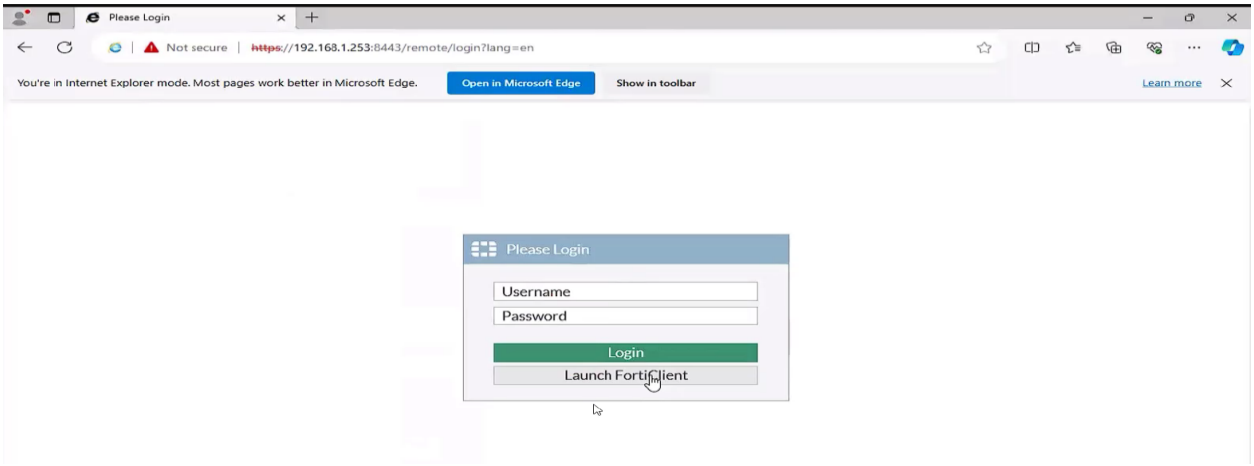
To test the SSL VPN configuration:

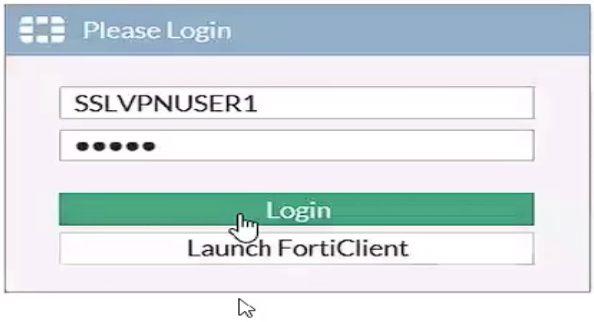
1. Open a browser on the client machine.
2. Enter the VPN portal address (e.g., https://<vpn-portal-ip>).
3. Log in with the configured credentials.
4. Check connectivity to internal resources:
    - Ping internal IP addresses.
    - Access services behind the VPN.

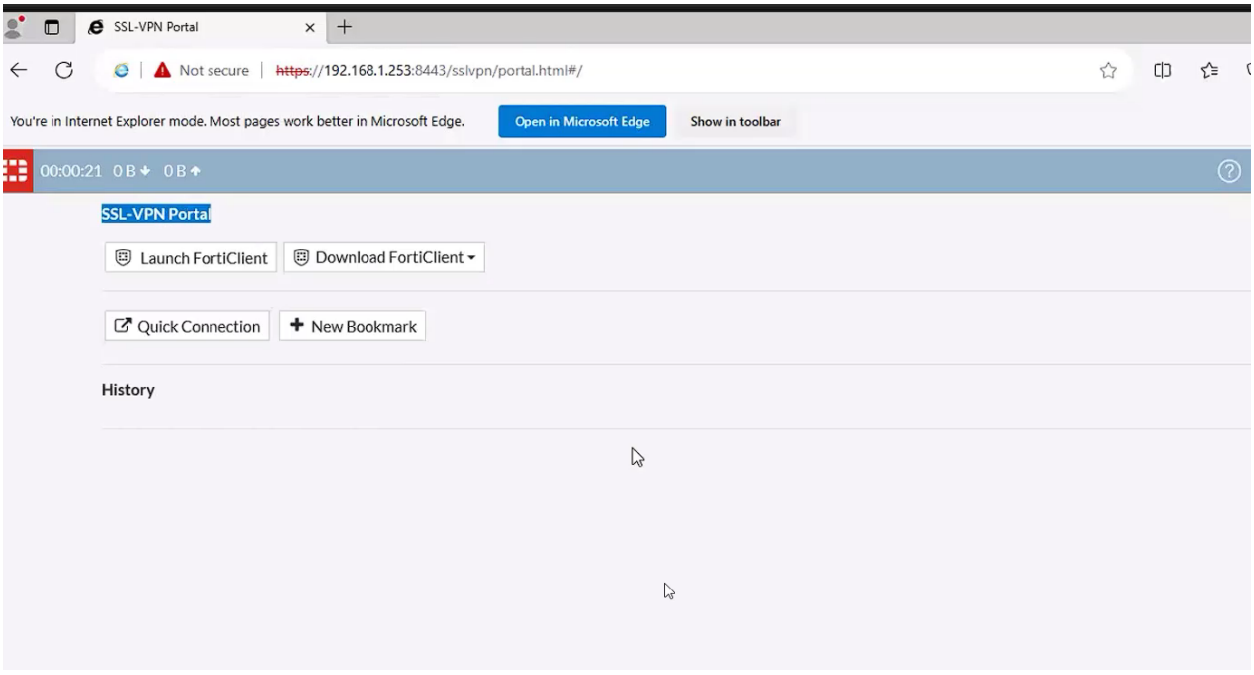
The Results

After completing the above steps:

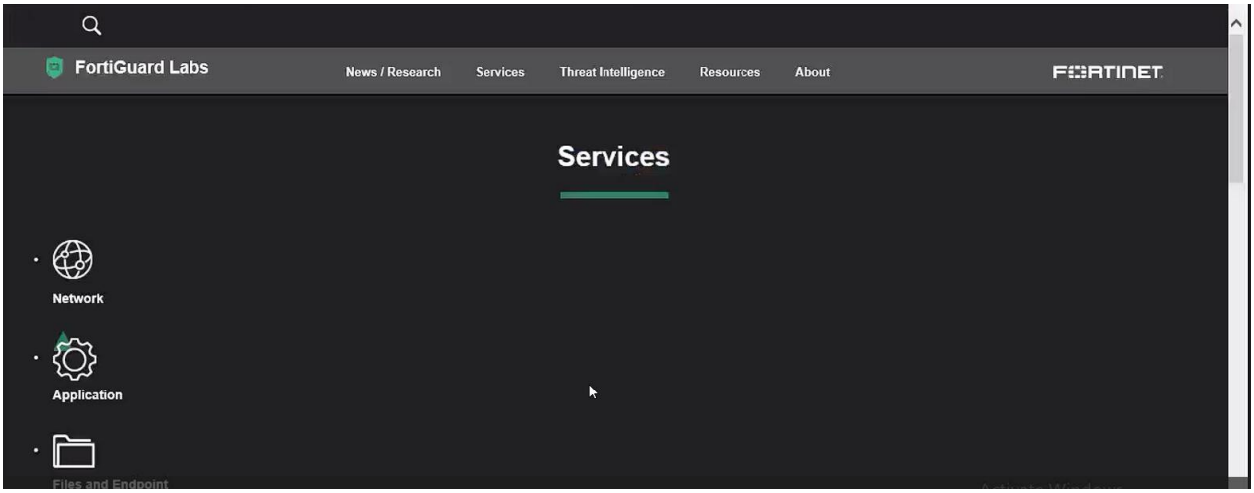
- SSL VPN was successfully configured on the network device.
- The client machine was able to:
    - Log in to the VPN portal.
    - Establish an encrypted SSL VPN connection.
    - Access internal network resources securely.


Please Login
Not secure | https://192.168.1.253:8443/remote/login?lang=en
You're in Internet Explorer mode. Most pages work better in Microsoft Edge.
Open in Microsoft Edge
Show in toolbar
Learn more
Please Login
Username
Password
Login
Launch FortiClient


Please Login
SSLVPNUSER1
Login
Launch FortiClient


SSL-VPN Portal
Not secure | https://192.168.1.253:8443/sslvpn/portal.html#/
You're in Internet Explorer mode. Most pages work better in Microsoft Edge.
Open in Microsoft Edge
Show in toolbar
00:00:21 0 B 0 B
SSL-VPN Portal
Launch FortiClient
Download FortiClient
Quick Connection
New Bookmark
History


00:00:47 0 B 0 B
SSL-VPN Portal
Launch FortiClient
Download FortiClient
iOS
Android
Windows
Mac
Quick Connection
History


FortiGuard Labs
News / Research
Services
Threat Intelligence
Resources
About
FORTINET
Services
Network
Application
Files and Endpoint