



Fortigate

Firewall Config & Rules

Original Author: *Vijay*



Table of Contents

Abstract.....	3
Firewall Lab Setup: FortiGate	4
Prerequisites.....	4
What is Firewall.....	4
Download FortiGate Virtual firewall.....	4
Configure Virtual network interfaces	8
Deployment of FortiGate VM image in VMWare	10
Configuring the Management Interface	15
Accessing FortiGate Firewall GUI.....	18
GUI Demonstration.....	21
Implementation of Firewall Policies: FortiGate	25
Connect Network Devices.....	26
Configure Network Interfaces	27
Add a Default Route	31
Create an IPV4 Firewall Policy.....	32
Create an IPv4 Dos Policy	35
Blocking Facebook with Web filter	39
Enable Web filter	40
Enable Default Web Filter Profile.....	41
Create Web Filter Security Policy	44
Enable web Filter	47
Edit Default Web Filter Profile	47
Site-to-Site IPsec VPN Tunnel with 2 FortiGates	51
Configure IPsec VPN on HQ	52
Configure IPsec VPN on a branch	57
Simplifying Policies with Zone	63
Create an Interface Zone	71
Create a Zone Firewall Policy	72
Conclusion	75
References	75



Abstract

In network security, there is no middle ground—you are either secure or vulnerable. Any computer connected to the Internet is at risk of online attacks, though some are more susceptible than others. Whether for personal use or large enterprises, security should always be the top priority.

A firewall acts as a barrier, protecting computers from harmful forces and preventing unauthorized access to a network. Among firewall options, NAT (Network Address Translation) firewalls are considered one of the safest choices.

This report focuses on the configuration and installation of the FortiGate virtual firewall. It also covers the process of creating FortiGate policies and explores different FortiGate firewall policy recipes.

Disclaimer: This report is provided for educational and informational purpose only (Penetration Testing). Penetration Testing refers to legal intrusion tests that aim to identify vulnerabilities and improve cybersecurity, rather than for malicious purposes.



Firewall Lab Setup: FortiGate

Prerequisites

To configure the virtual FortiGate Firewall on your system there are some prerequisites required for installation

- VMWare Workstation
- FortiGate Firewall VM Image
- 3 or more NIC (Network interface cards) E1000 compatible network cards
- Root privileges

What is Firewall

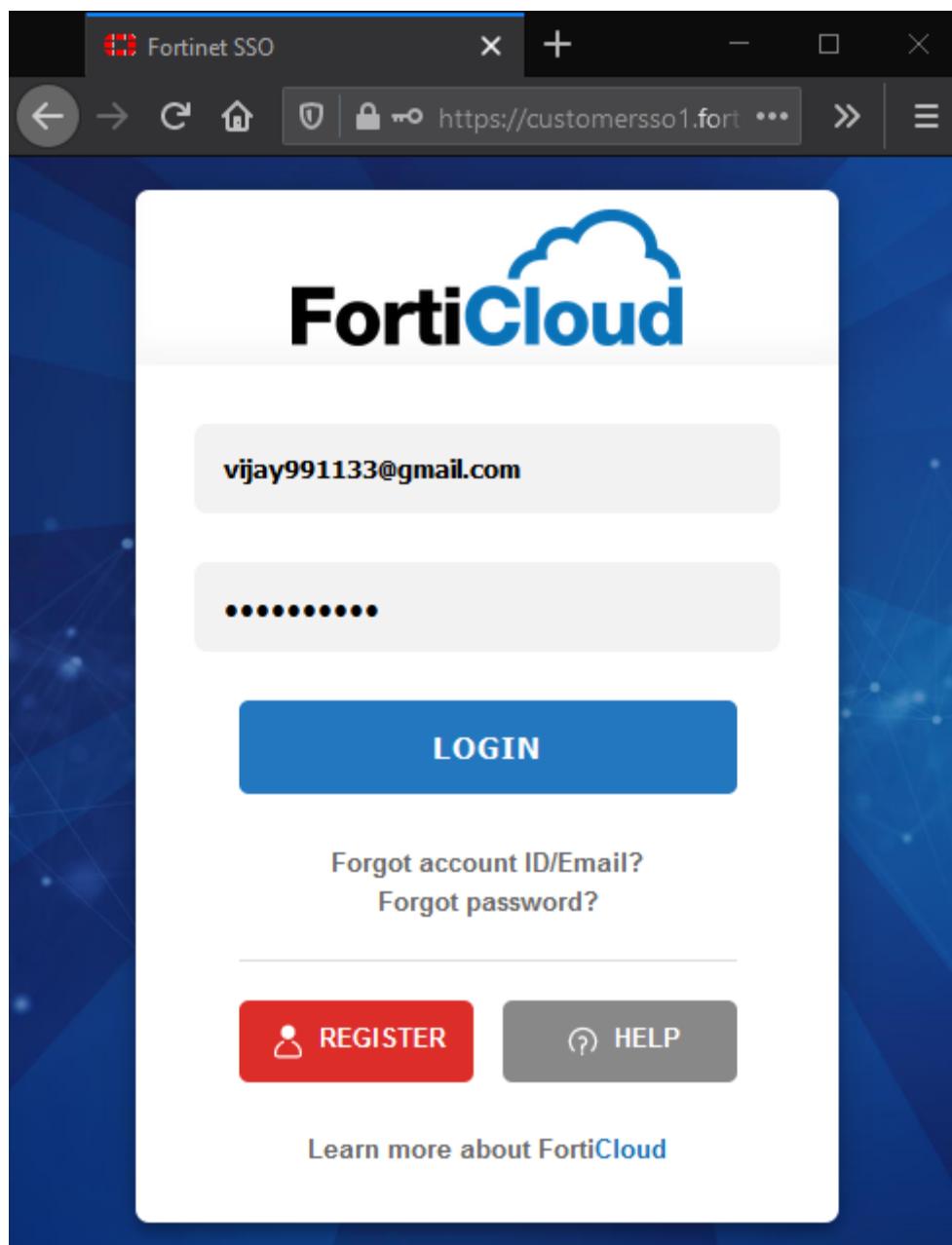
In the computing language, a firewall is a security software or hardware that can monitor and control network traffic, both incoming and outgoing. It establishes a kind of barrier between reliable internal and unknown external networks.

Therefore, a firewall, also known as a network firewall, is capable of preventing unauthorized access to/from private networks.

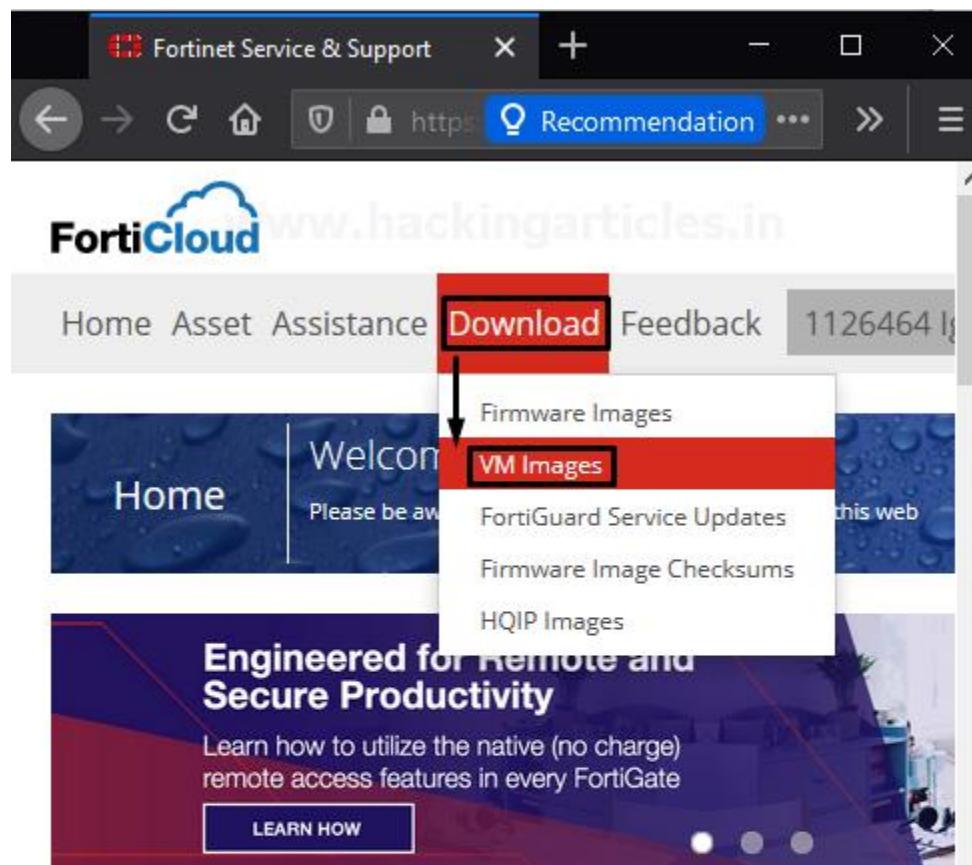
A network firewall is based on security rules to **accept**, **reject**, or **drop** specific traffic. The firewall aims to allow or deny the connection or request, depending on implemented rules.

Download FortiGate Virtual firewall

First, we need to download the virtual FortiGate Firewall from the official FortiGate portal.



By creating an account or log in to the account go to **Download > VM Images** as shown in the image below.



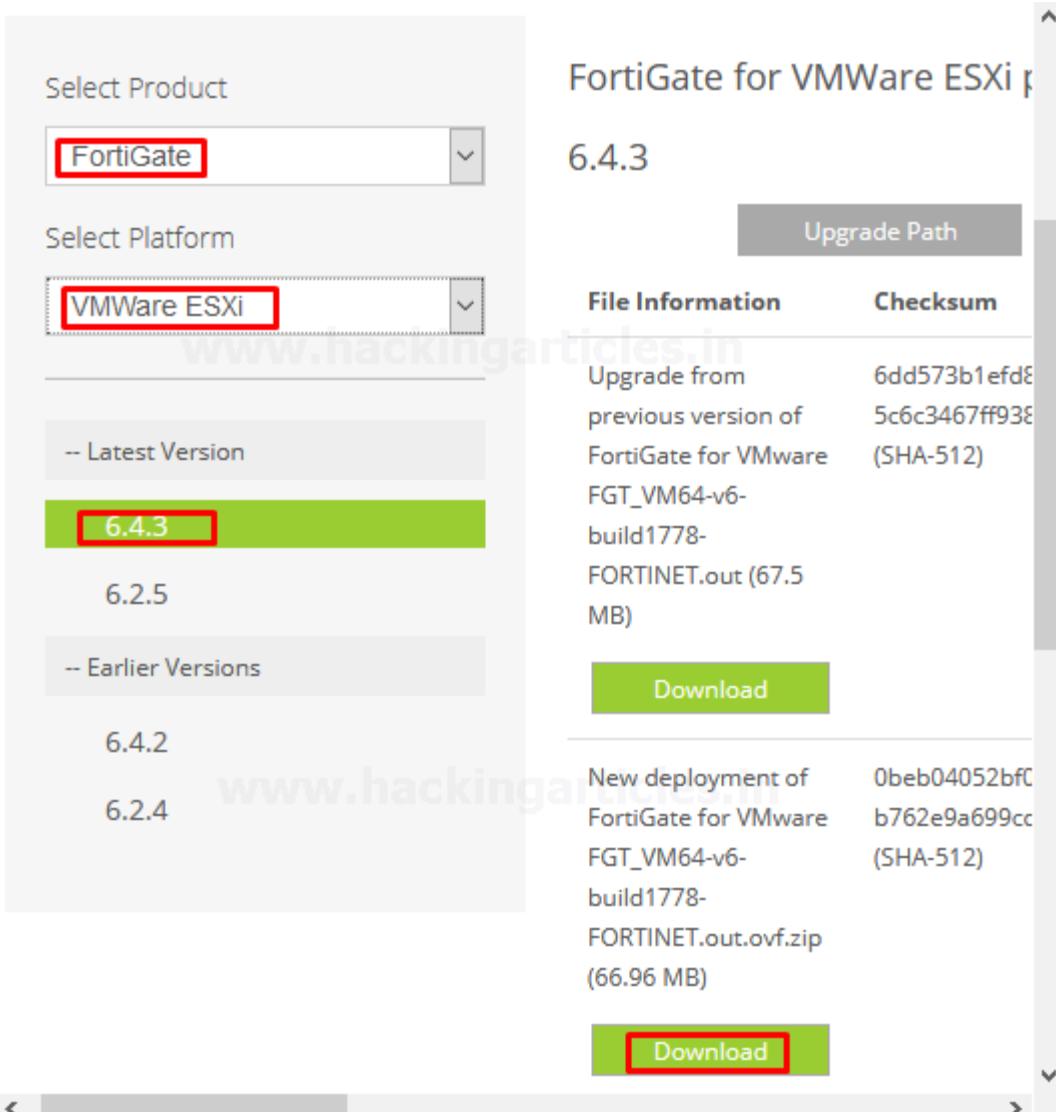
Asset



Register/Activate Contracts

Register HW/Virtual appliance or software; Activate your registered product.

Further then Select Product: **FortiGate** > Select Platform: **VMWare ESXi** as shown in the image below. By default, you don't have any license associated with your virtual image so, you can go with the trial version or you can buy the license as per your requirement.



The screenshot shows a software download interface for FortiGate. On the left, there's a sidebar with dropdown menus for 'Select Product' (set to 'FortiGate') and 'Select Platform' (set to 'VMWare ESXi'). Below these are sections for 'Latest Version' (highlighted in green) and 'Earlier Versions'. The 'Latest Version' section shows '6.4.3' in a green box, which is also highlighted with a red border. To the right, under the heading 'FortiGate for VMWare ESXi', is a table titled 'Upgrade Path' with two columns: 'File Information' and 'Checksum'. It lists two files: one for upgrading from previous versions and another for a new deployment. Both files are 'FGT_VM64-v6-build1778-FORTINET.out' files, with the first being 67.5 MB and the second being 66.96 MB. Each file has a green 'Download' button below it, with the top one also having a red border.

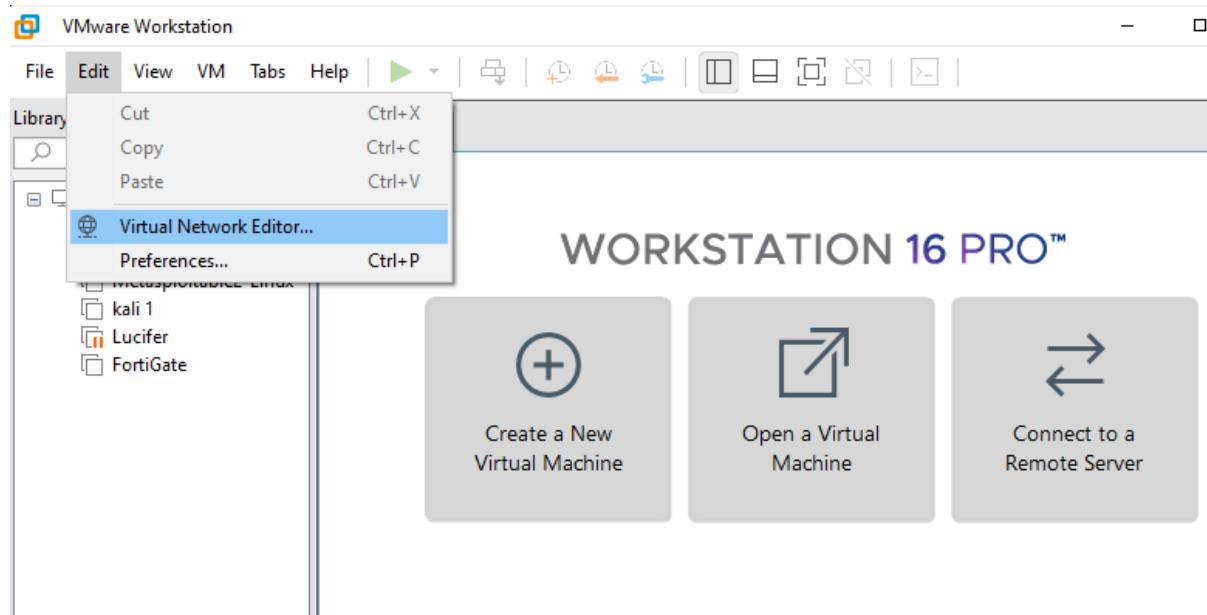
After downloading the compressed FortiGate VM file you need to extract the compressed Zip file by using your favourite extractor and the extracted Zip file similarly looks like the below image.

This PC > Downloads > FGT_VM64-v6-build1778-FORTINET.out.ovf				
	Name	Date modified	Type	Size
	datadrive	23-08-2010 23:02	VMDK File	70 KB
	FortiGate-VM64.hw07_vmxnet3	22-10-2020 02:32	Open Virtualizatio...	33 KB
	FortiGate-VM64.hw13	22-10-2020 02:32	Open Virtualizatio...	30 KB
	FortiGate-VM64.hw14	22-10-2020 02:32	Open Virtualizatio...	30 KB
	FortiGate-VM64.nsxt	22-10-2020 02:32	Open Virtualizatio...	14 KB
	FortiGate-VM64	22-10-2020 02:32	Open Virtualizatio...	27 KB
	FortiGate-VM64.vapp	22-10-2020 02:32	Open Virtualizatio...	44 KB
	fortios	22-10-2020 02:32	VMDK File	69,321 KB

Configure Virtual network interfaces

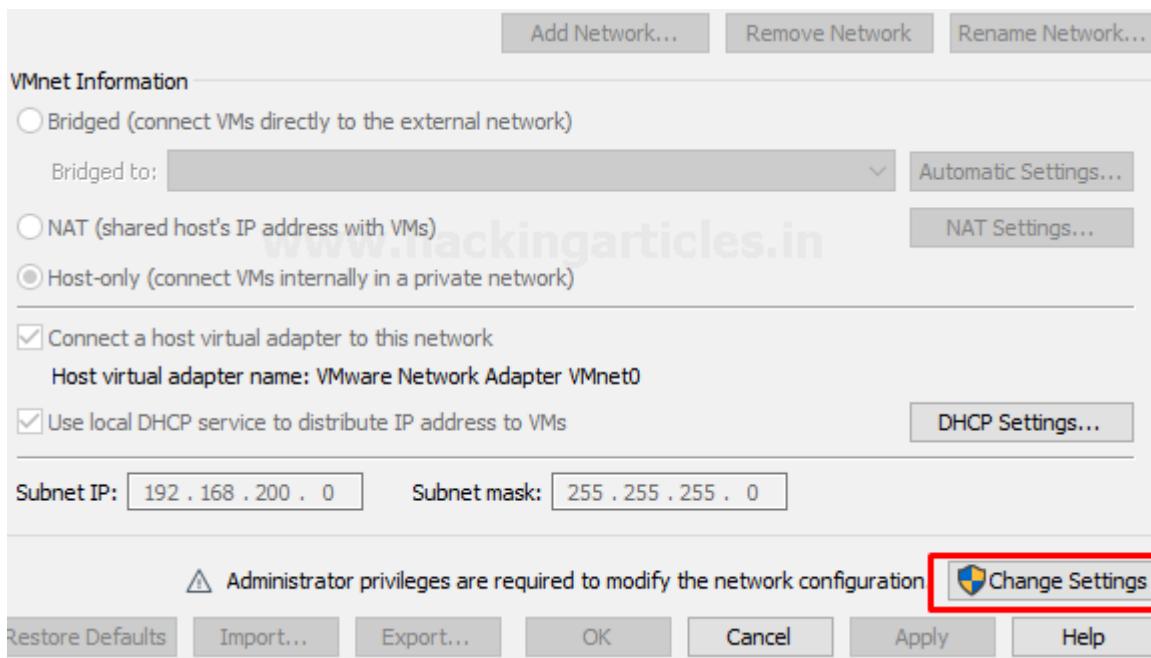
Let's configure Virtual Network Adapters as per your requirements.

To do this open VMware then go to Edit > Virtual Network Editor as shown in the image below



Further, then it will open another prompt that allows you to modify the network configuration.

To make changes in network configuration it needs the Administrator privileges to provide Admin privileges click on change settings as shown below



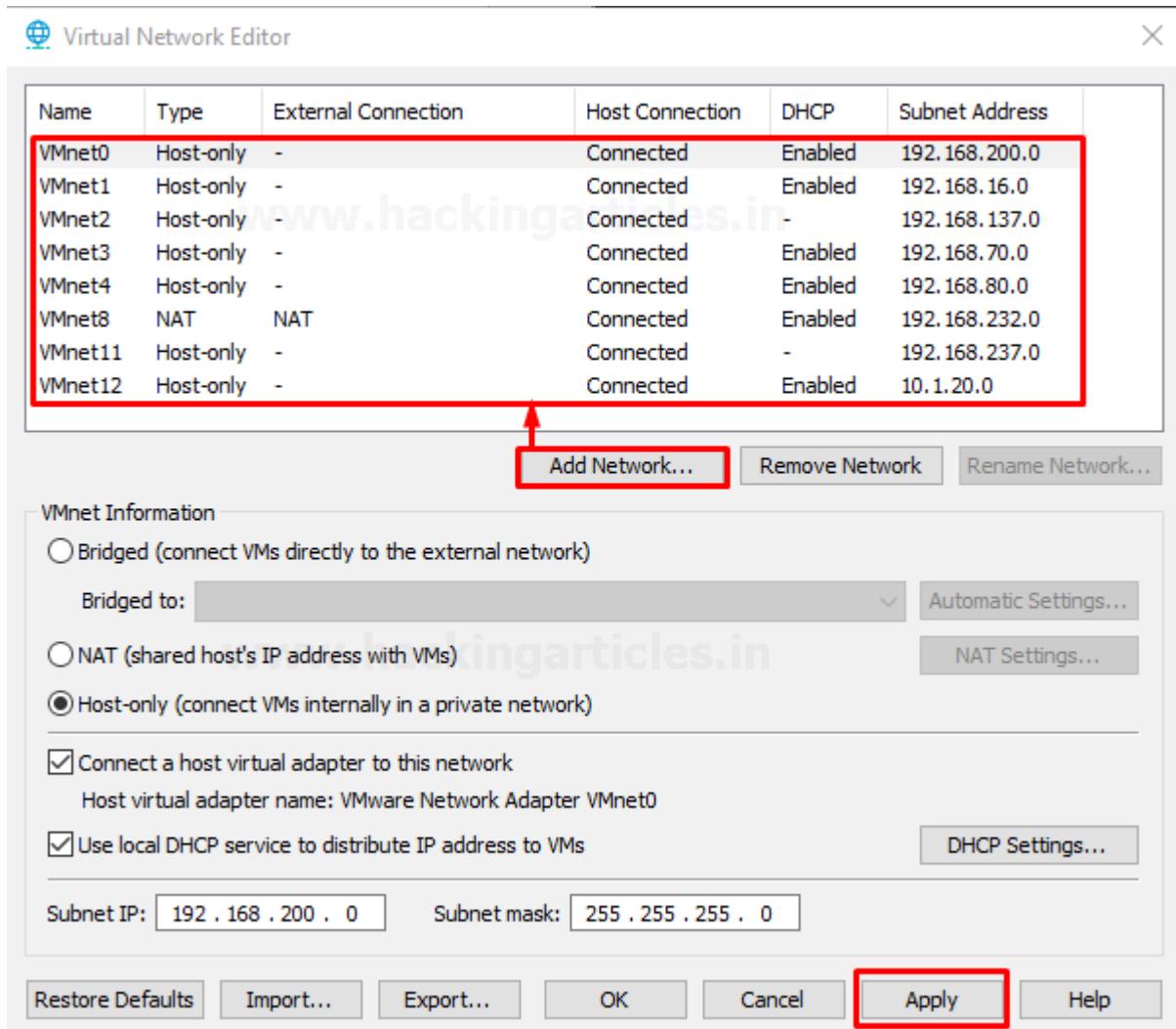
Or also you can directly access the Virtual network editor app by click on Windows Start Button and search for Virtual Network Editor. If you are using Linux (i.e. Ubuntu) you can type the below command to open Virtual Network Editor.

```
sudo vmware-netcfg
```

By default, there are only two virtual network interfaces, i.e., *VMNet1* and *VMNet8*. So, click on the Add Network and make your virtual interface host only. After that, you have to provide a unique IP address of network devices to each network interface.

For example, I am going to use 192.168.200.0/24 for the *vmnet0* interface and so on...

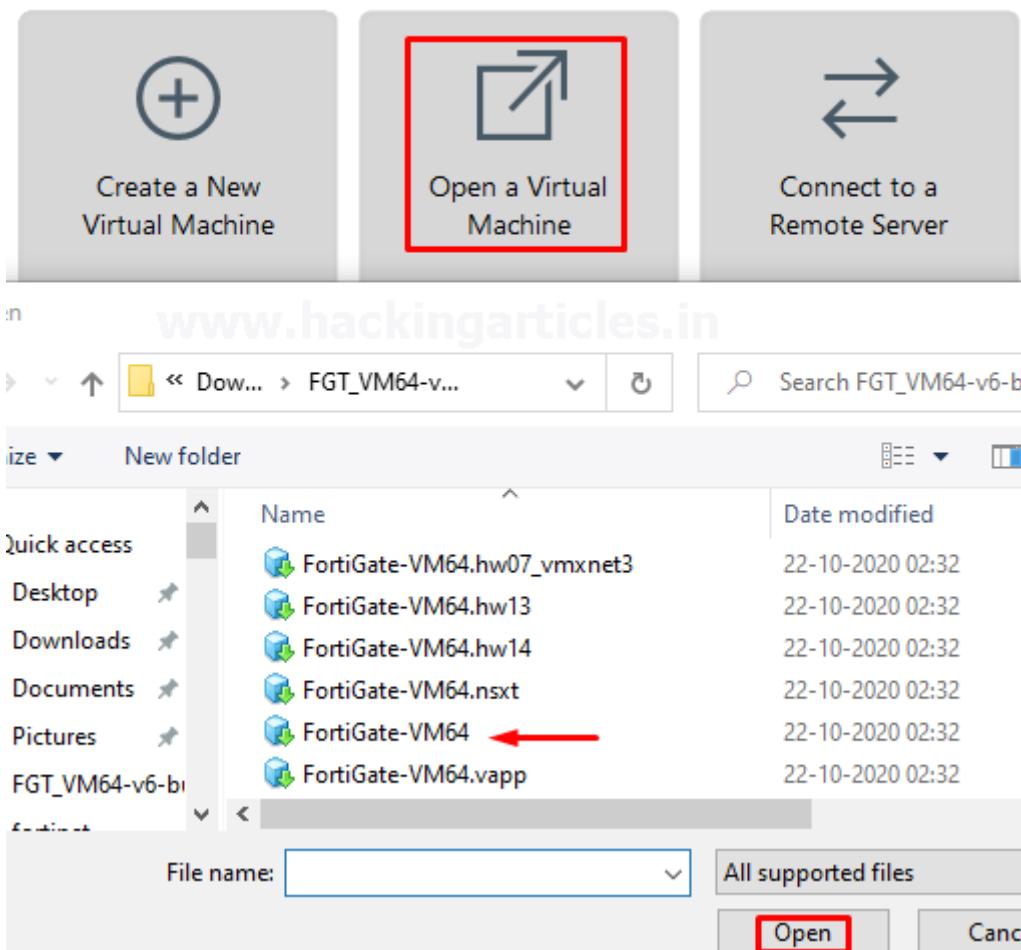
Use Ip of your network devices or whatever as per your requirement. Similarly, you can add as much as network interfaces as you want but remember one thing all network configuration should be configured to Host-only and you can enable or disable DHCP service as per your system requirement



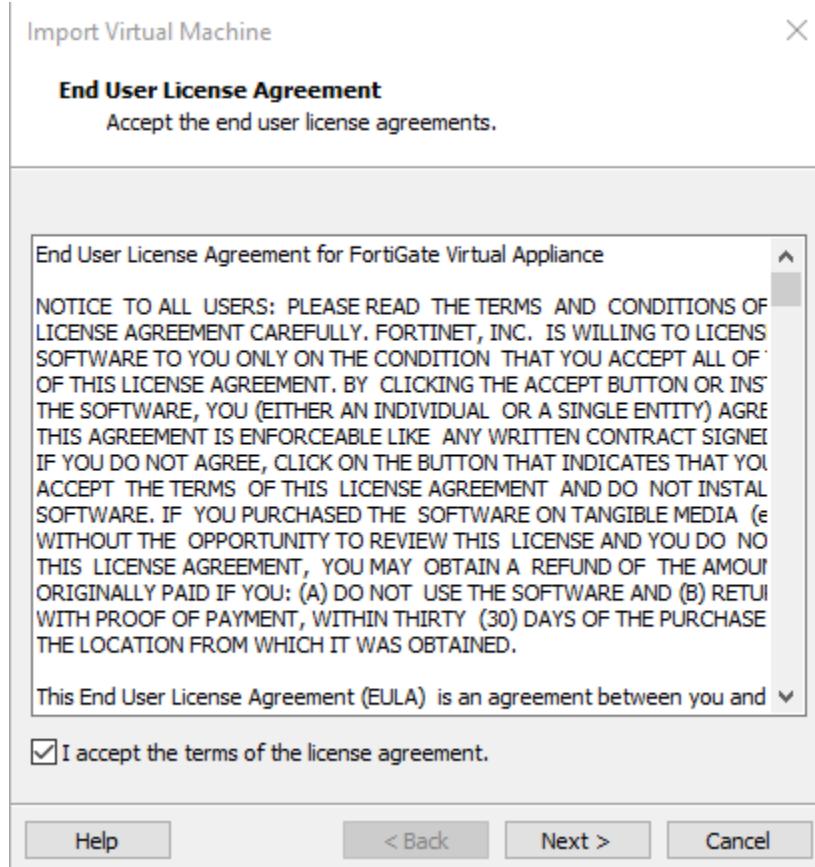
Deployment of FortiGate VM image in VMWare

Now it's time to deploy the FortiGate virtual firewall in VMWare Workstation. Just open the VMWare Workstation and go to **Files > Open** (Ctrl+O) or go to the Home tab and select open a virtual Machine. Select the FortiGate-VM64.ovf file that you have downloaded from the official Website of FortiGate as shown below

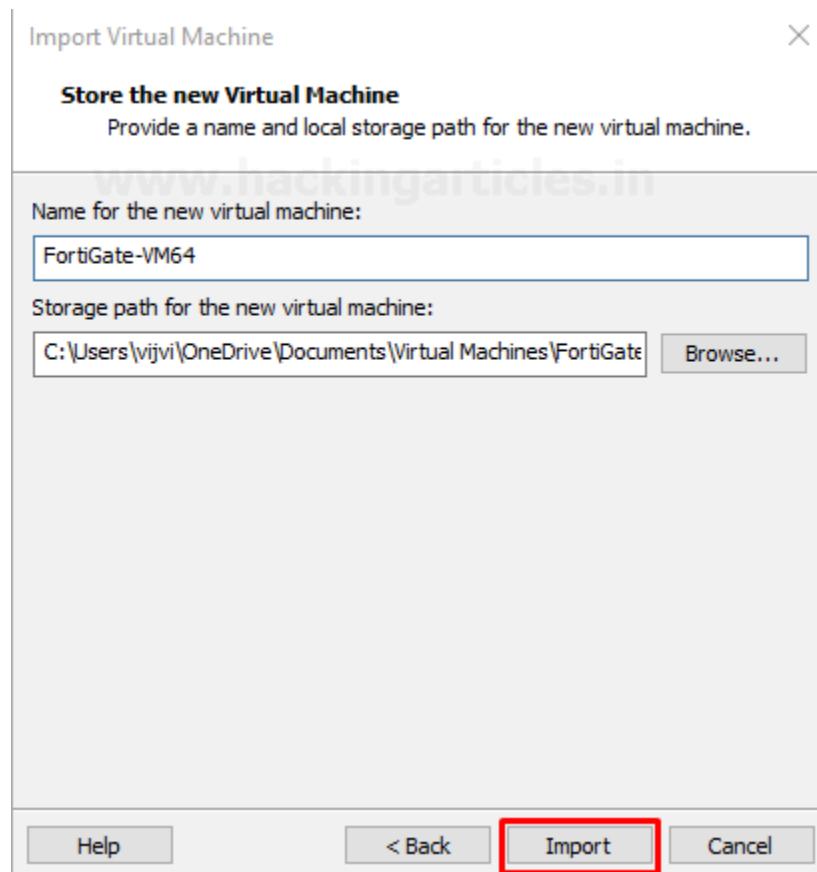
WORKSTATION 16 PRO™



Then after it will open another prompt of End User License Agreement accept it and move to next

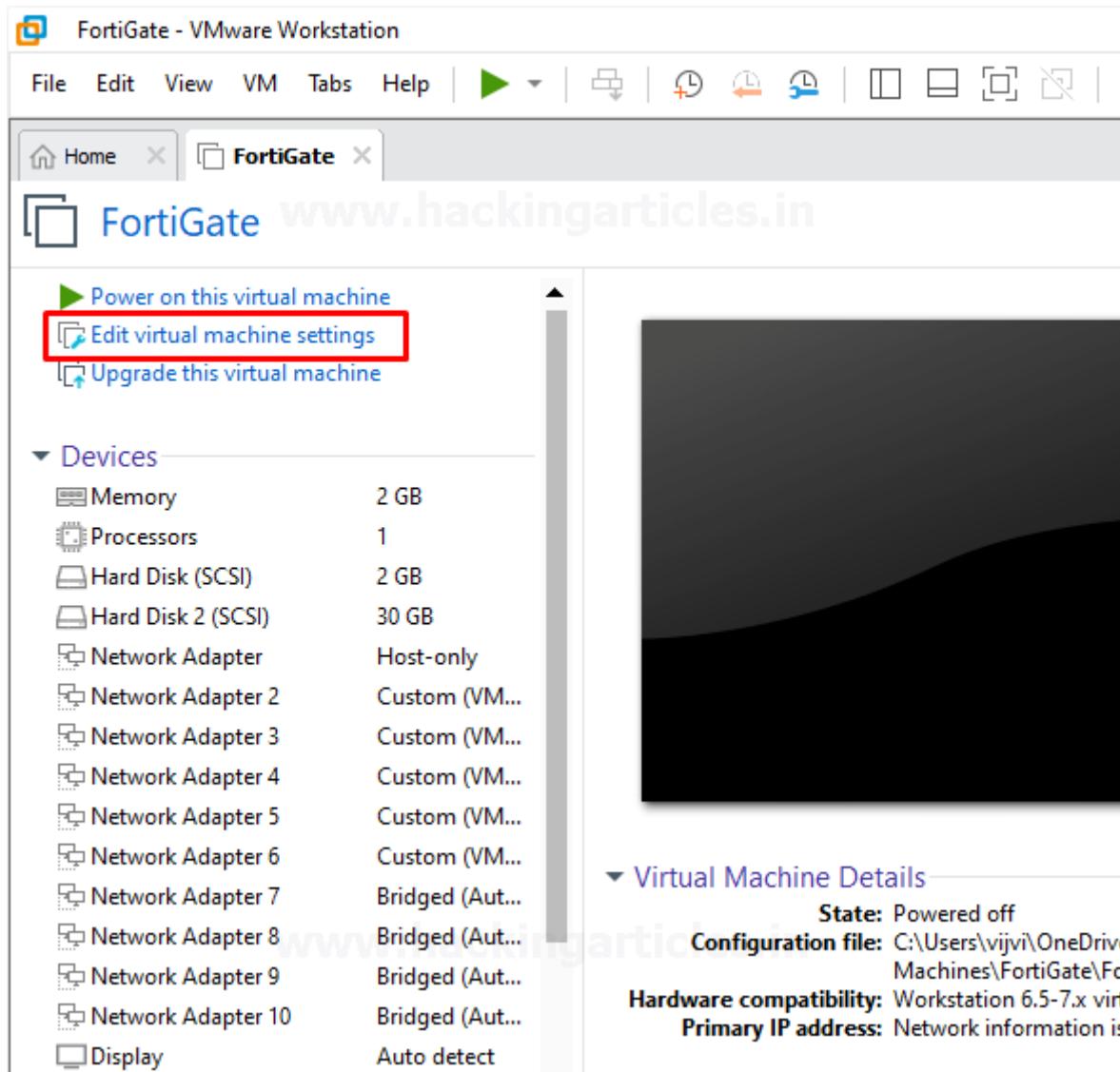


On the next prompt Assign a Name for the new Virtual machine and a Storage Path then after select import as shown below



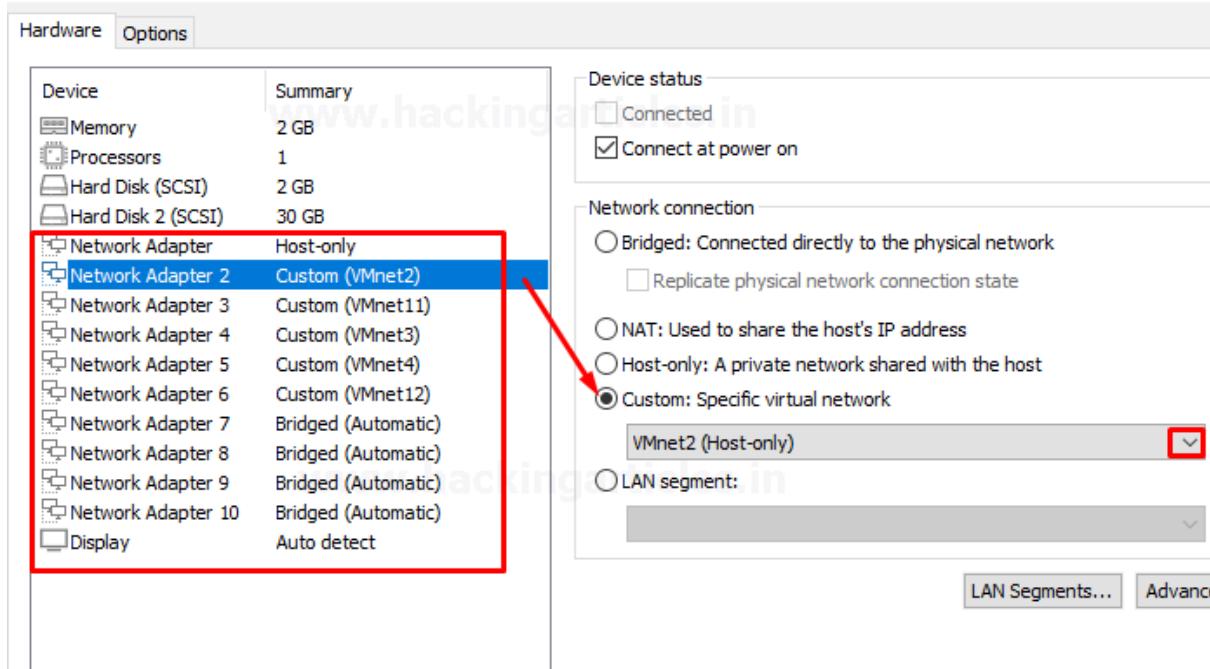
This process going to take some time, so have *patience*. After the successful completion of this process,

Now it's time to configure the Virtual Firewall resources by clicking on Edit virtual machine settings. just modify the assigned virtual network interfaces, memory, and processor by going to Edit virtual machine.



In my case, I'm giving 2GB RAM, 30 GB of Hard Disk, 1 Processor, and 6 different virtual network interfaces (VMNet2, VMNet3, VMNet4, VMNet11, VMnet11, VMnet12) to different network adaptors. Check the below image for reference.

Virtual Machine Settings



Configuring the Management Interface

We've just finished the deployment process of the FortiGate Firewall in the VMWare workstation.

Let's configure an IP Address to the management interface. In manner to assign an IP Address to management interface firstly, we need login to the system with default credentials

Login User: – Admin

Login Password: – In this circumstance, we don't know the default password, Hit enter and change the password as shown below



```

Loading flatkc... ok
Loading /rootfs.gz...ok

Decompressing Linux... Parsing ELF... done.
Booting the kernel.

System is starting...
Serial number is FGVMEV9T3UJPII0A

FortiGate-VM64 login: admin
Password:
You are forced to change your password. Please input a new password.
New Password:
Confirm Password:
Welcome!

FortiGate-VM64 #

```

Let's check the system interfaces by running the following command

show system interface

```

FortiGate-VM64 # show system interface ←
name      Name.
fortilink static  0.0.0.0 0.0.0.0  169.254.1.1 255.255.255.0 up    disable
aggregate enable
port1    dhcp   0.0.0.0 0.0.0.0  192.168.200.128 255.255.255.0 up    disable  ph
ysical enable
port2    static  0.0.0.0 0.0.0.0  0.0.0.0 0.0.0.0 up    disable  physical enab
le
port3    static  0.0.0.0 0.0.0.0  0.0.0.0 0.0.0.0 up    disable  physical enab
le
port4    static  0.0.0.0 0.0.0.0  0.0.0.0 0.0.0.0 up    disable  physical enab
le
port5    static  0.0.0.0 0.0.0.0  0.0.0.0 0.0.0.0 up    disable  physical enab
le
port6    static  0.0.0.0 0.0.0.0  0.0.0.0 0.0.0.0 up    disable  physical enab
le
port7    static  0.0.0.0 0.0.0.0  0.0.0.0 0.0.0.0 up    disable  physical enab
le
port8    static  0.0.0.0 0.0.0.0  0.0.0.0 0.0.0.0 up    disable  physical enab
le
port9    static  0.0.0.0 0.0.0.0  0.0.0.0 0.0.0.0 up    disable  physical enab
le
port10   static  0.0.0.0 0.0.0.0  0.0.0.0 0.0.0.0 up    disable  physical ena
ble
--More--

```

Port 1 will be for the management interface so, assign a unique IP address to the management port and set to mode static. In this example our IP Address will 192.168.200.128/24 so, the default gateway will be 192.168.200.1. To assign IP Address to management port run the following command as shown below



```
config system interface
edit port1
set mode static
set ip 192.168.200.128 255.255.255.0
set allowaccess http https telnet ssh ping
end
```

```
FortiGate-VM64 # config system interface ←
FortiGate-VM64 (interface) # edit port1 ←
FortiGate-VM64 (port1) # set mode static ←
FortiGate-VM64 (port1) # set ip 192.168.200.128 255.255.255.0 ←
FortiGate-VM64 (port1) # set allowaccess http https telnet ssh ping ←
FortiGate-VM64 (port1) # end ←
FortiGate-VM64 # _
```

Also, we can verify the make changes of system interfaces by running the following command

```
show system interface
```

```
FortiGate-VM64 # show system interface ←
config system interface
    edit "port1"
        set vdom "root"
        set ip 192.168.200.128 255.255.255.0
        set allowaccess ping https ssh http telnet
        set type physical
        set snmp-index 1
    next
    edit "port2"
        set vdom "root"
        set type physical
        set snmp-index 2
    next
    edit "port3"
        set vdom "root"
        set type physical
        set snmp-index 3
    next
    edit "port4"
        set vdom "root"
        set type physical
        set snmp-index 4
    next
--More-- _
```

Accessing FortiGate Firewall GUI

Let's check our firewall configuration by accessing the FortiGate Firewall GUI. Before accessing the GUI first, we will check the connectivity to our Firewall using the ping utility by running the following command

```
execute ping 192.268.200.128
```

```
FortiGate-UM64 # execute ping 192.168.200.128 ←
PING 192.168.200.128 (192.168.200.128): 56 data bytes
64 bytes from 192.168.200.128: icmp_seq=0 ttl=255 time=0.0 ms
64 bytes from 192.168.200.128: icmp_seq=1 ttl=255 time=0.0 ms
64 bytes from 192.168.200.128: icmp_seq=2 ttl=255 time=0.0 ms
64 bytes from 192.168.200.128: icmp_seq=3 ttl=255 time=0.0 ms
64 bytes from 192.168.200.128: icmp_seq=4 ttl=255 time=0.0 ms

--- 192.168.200.128 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms

FortiGate-UM64 #
```

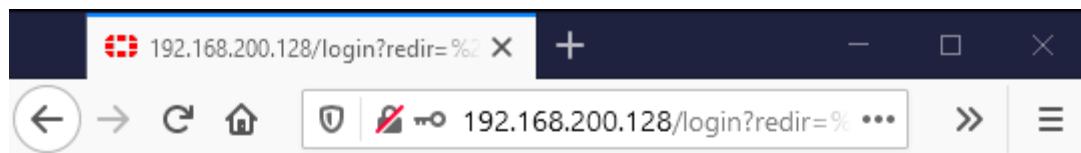
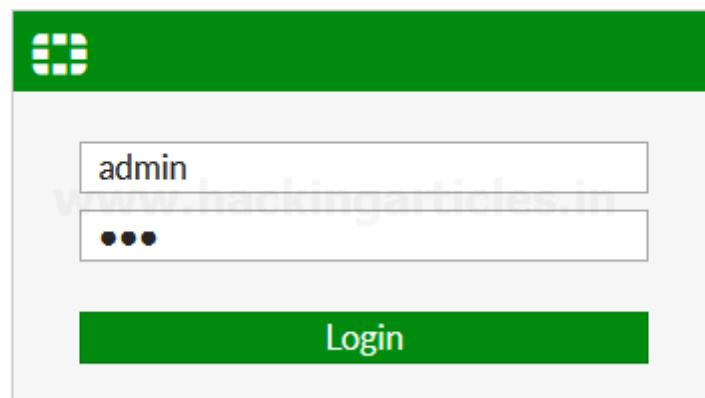
As we can see the IP Address is reachable which means it is working properly now, we will access the FortiGate Firewall GUI using its management interface IP address.

https://192.168.200.128

use the same login credential that we have set up on CLI

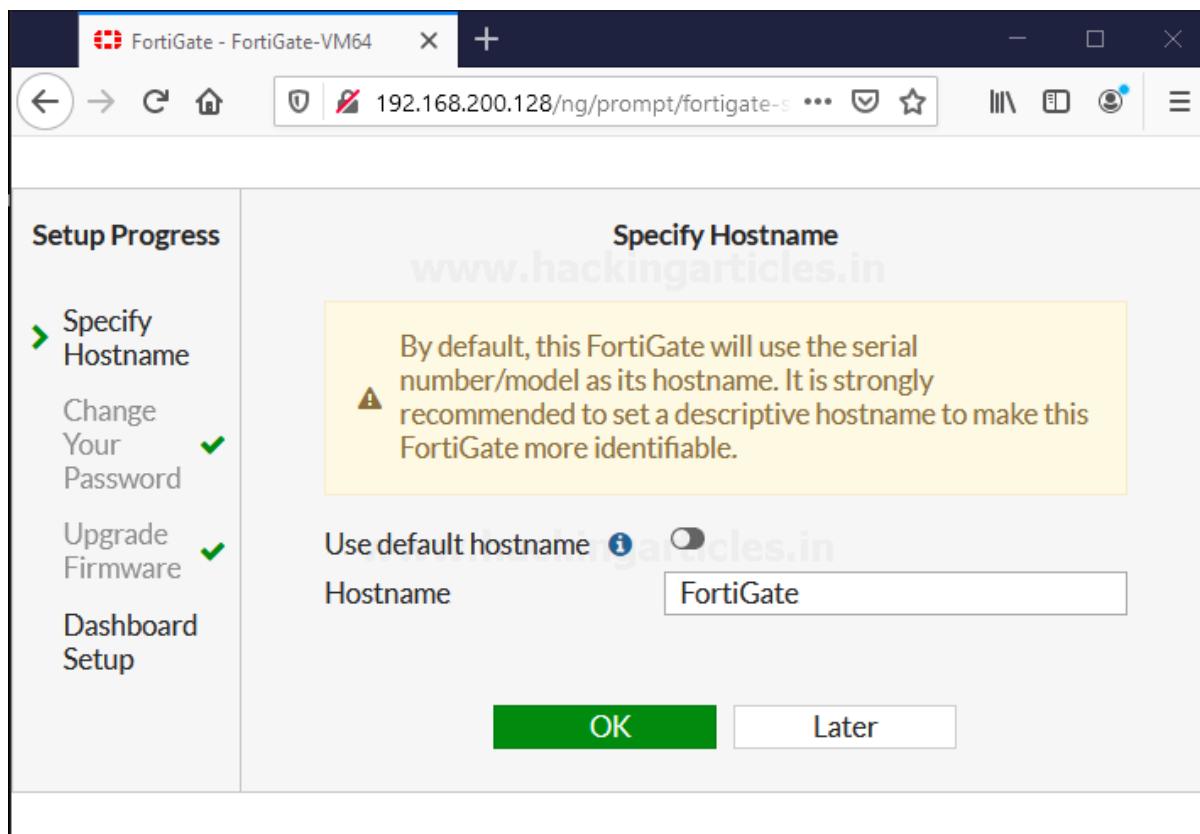
Username: – admin

Password: – 123

By logging in to the firewall it will open a setup Prompt where we need to specify the Hostname, change password upgrade firmware, and Dashboard setup

By default, this FortiGate will use the serial number/model as its hostname. To make it more identifiable set a descriptive hostname as shown below



Already we have changed the password in Firewall CLI and also, we have already downloaded the latest version of the firewall, so it automatically skips you to the last step to Dashboard setup. Select it to Optimal or Comprehensive as per your requirements



The screenshot shows a web-based setup interface for a FortiGate device. On the left, a vertical sidebar titled "Setup Progress" lists several steps: "Specify Hostname", "Change Your Password", "Upgrade Firmware", and "Dashboard Setup". The "Dashboard Setup" step is currently selected, indicated by a green arrow icon. The main content area is titled "Dashboard Setup" and contains the following text: "Select one of the following options to decide what dashboards will be available by default. You can always change your selection or manually customize your own dashboards later." Below this text are two radio button options: "Optimal" (selected, indicated by a green dot) and "Comprehensive". The "Optimal" option is described as "A set of popular default dashboards and FortiView monitors." The "Comprehensive" option is described as "A set of default dashboards as well as all monitors and FortiViews. This set will be familiar to users coming from previous FortiOS versions." At the bottom right of the content area is a large green "OK" button.

After selecting the type of Dashboard hit ok and finish the setup.

GUI Demonstration

The GUI contains the following main menus, which provide access to configuration options for most FortiOS features:



The screenshot shows the FortiGate VM64 dashboard interface. On the left, a sidebar lists navigation options: Dashboard, Status, Security, Network, Users & Devices, FortiView Sources, FortiView Destinations, FortiView Applications, FortiView Web Sites, FortiView Policies, FortiView Sessions, Security Fabric, Network, System, and Policy & Objects. The main area is divided into several sections: 'System Information' (Hostname: FortiGate, Serial Number: FGVMEVL1KCWJTV8, Firmware: v6.4.3 build1778 (GA), Mode: NAT, System Time: 2020/11/08 17:34:48, Uptime: 00:00:20:23, WAN IP: Unknown); 'Licenses' (FortiCare Support, Firmware & General Updates, IPS, AntiVirus, Web Filtering); 'FortiToken' (0/0, Unable to connect to FortiGuard servers); 'Security Fabric' (with icons for physical topology, logical topology, audit, and settings); 'Administrators' (1 HTTP, 0 FortiExplorer, admin, super_admin).

Dashboard: – The dashboard displays various widgets that display important system information and allow you to configure some system options.

Security Fabric: – Access the physical topology, logical topology, audit, and settings of the Fortinet Security Fabric.

FortiView: – A collection of dashboards and logs that give insight into network traffic, showing which users are creating the most traffic, what sort of traffic it is, when the traffic occurs, and what kind of threat the traffic may pose to the network.

Network: – Options for networking, including configuring system interfaces and routing options.

System: – Configure system settings, such as administrators, FortiGuard, and certificates.

Policy & Objects: – Configure firewall policies, protocol options, and supporting content for policies, including schedules, firewall addresses, and traffic shapers.

Security Profiles: – Configure your FortiGate's security features, including Antivirus, Web Filter, and Application Control.

VPN: – Configure options for IPsec and SSL virtual private networks (VPNs).

User & Device: – Configure user accounts, groups, and authentication methods, including external authentication and single sign-on (SSO).



WiFi & Switch Controller: – Configure the unit to act as a wireless network controller, managing the wireless Access Point (AP) functionality of FortiWiFi and FortiAP units. On certain FortiGate models, this menu has additional features allowing for FortiSwitch units to be managed by the FortiGate.

Log & Report: – Configure logging and alert email as well as reports.

Monitor: – View a variety of monitors, including the Routing Monitor, VPN monitors for both IPsec and SSL, monitors relating to wireless networking, and more.

Dashboard Demonstration

FortiGate dashboards can have a Network Operations Centre (NOC) or responsive layout.

- On a responsive dashboard, the number of columns is determined by the size of the screen. Widgets can only be resized horizontally, but the dashboard will fit on all screen sizes.
- On a NOC dashboard, the number of columns is explicitly set. Widgets can be resized both vertically and horizontally, but the dashboard will look best on the screen size that it is configured for.

Multiple dashboards of both types can be created, for both individual VDOMs and globally.

- Widgets are interactive; clicking or hovering over most widgets shows additional information or links to relevant pages.
- Widgets can be reorganized by clicking and dragging them around the screen.

Four dashboards are available by default: Status, Network, Security, and System Events

The Status dashboard includes the following widgets by default:

System Information: – The System Information widget lists information relevant to the FortiGate system, including hostname, serial number, and firmware. Clicking on the widget provides links to configure system settings and update the device firmware.

Licenses: – The License widget lists the status of various licenses, such as FortiCare Support and IPS. The number of used and available FortiTokens is also shown. Clicking on the widget provides a link to the FortiGuard settings page.

Virtual Machine: – The VM widget (shown by default in the dashboard of a FortiOS VM device) includes:

- License status and type
- vCPU allocation and usage
- RAM allocation and usage
- VMX license information (if the VM supports VMX)

Clicking on an item in the widget provides a link to the FortiGate VM License page, where license files can be uploaded.



FortiGate Cloud: – This widget displays the FortiGate Cloud and FortiSandbox Cloud status.

Security Fabric: – The Security Fabric widget displays a visual summary of the devices in the Fortinet Security Fabric.

Clicking on a product icon provides a link to a page relevancy to that product. For example, clicking the FortiAnalyzer shows a link to log settings.

Security Rating: – The Security Rating widget shows the security rating for your Security Fabric. It can show the current rating percentile, or historical security rating score or percentile charts.

Administrators: – This widget allows you to see logged-in administrators, connected administrators, and the protocols used by each. Clicking in the widget provides links to view active administrator sessions, and to open the FortiExplorer page on the App Store.

CPU: – This widget shows real-time CPU usage over the selected time frame. Hovering over any point on the graph displays the percentage of CPU power used at that specific time. It can be expanded to occupy the entire dashboard.

Memory: – This widget shows real-time memory usage over the selected time frame. Hovering over any point on the graph displays the percentage of the memory used at that specific time. It can be expanded to occupy the entire dashboard.

Sessions: – This widget shows the current number of sessions over the selected time frame. Hovering over any point on the graph displays the number of sessions at that specific time. It can be expanded to occupy the entire dashboard.

The Security dashboard includes the following widgets by default:

- **Top Compromised Hosts by Verdict:** – This widget lists the compromised hosts by verdict. A FortiAnalyzer is required. It can be expanded to occupy the entire dashboard.
- **Top Threats by Threat Level:** – This widget lists the top threats by threat level, from FortiView. It can be expanded to occupy the entire dashboard.
- **FortiClient Detected Vulnerabilities:** – This widget shows the number of vulnerabilities detected by FortiClient. FortiClient must be enabled. Clicking on the widget provides a link to view the information in FortiView.
- **Host Scan Summary:** – This widget lists the total number of hosts. Clicking on the widget provides links to view vulnerable devices in FortiView, FortiClient monitor, and the device inventory.
- **Top Vulnerable Endpoint Devices by Detected Vulnerabilities:** – This widget lists the top vulnerable endpoints by the detected vulnerabilities, from FortiView. It can be expanded to occupy the entire dashboard.

The System Events dashboard includes the following widgets by default:

- **Top System Events by Events:** – This widget lists the top system events, sorted by the number of events. It can be expanded to occupy the entire dashboard. Double click on an event to view the specific event log.



- **Top System Events by Level:** – This widget lists the top system events, sorted by the events' levels. It can be expanded to occupy the entire dashboard. Double click on an event to view the specific event log.

Implementation of Firewall Policies: FortiGate

Prerequisites

- Strong Knowledge of Networking
- Attacker Machine Kali Linux

How do firewall Works?

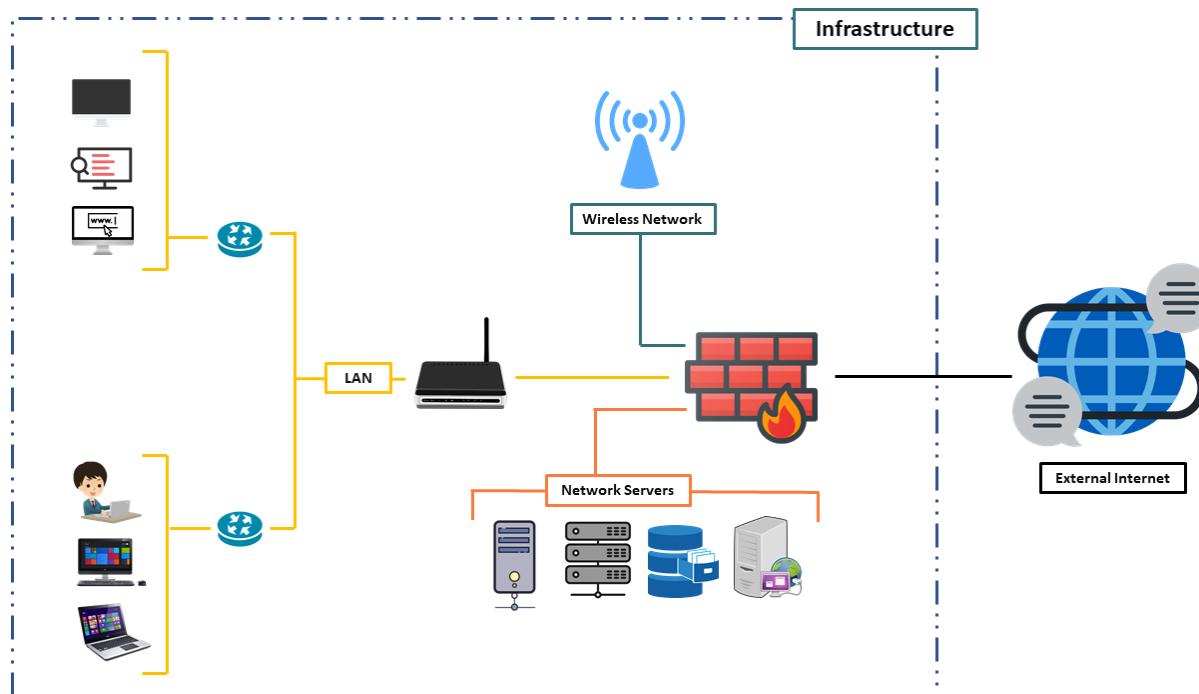
Basically, firewalls are divided into two parts

- Stateful: – Stateful firewalls are capable of monitoring whole network traffic, including their communication channels. These firewalls are also referred as dynamic packet filter as they filter traffic packets based on the context (it involves metadata of packets including ports and IP address belonging to that Endpoint) and state.
- Proxy: – Proxy Firewall can be Defined as, A firewall that can monitor and filter communication at the application level and protect the resources from unwanted dangerous traffic. A proxy firewall also is known as Application layer Firewall.

After some time in an inspection stateful firewall become more sophisticated and proxy Firewalls become too slow.

Today nearly all Firewalls are stateful and they are divided into two General Types.

- Host-based Firewalls
- Network Firewalls



In this article, you will learn how to connect and configure a new FortiGate unit in NAT route mode to securely connect a private network to the internet.

In NAT route mode a FortiGate unit is installed as a gateway or router between two networks. In most cases it is used between private networks and the internet, this allows the Firewall to hide the IP addresses of the private network using Network Address Translation (NAT) and the various firewall Policy of FortiGate firewall as a Firewall Recipe.

As you guys have one question here why we are calling it as Recipe... answer is quite simple without using the Recipe we can't cook a tasty food Wait for what... a tasty food... 🍽️ we can't even cook the food... 😊 similarly without proper firewall policy (recipe), we can't protect our network from dangerous network traffics.

Connect Network Devices

First, you need to connect a physical firewall or FortiGate into your network setup. On the place of a physical firewall, we are using a Virtual FortiGate Firewall to get hands-on.

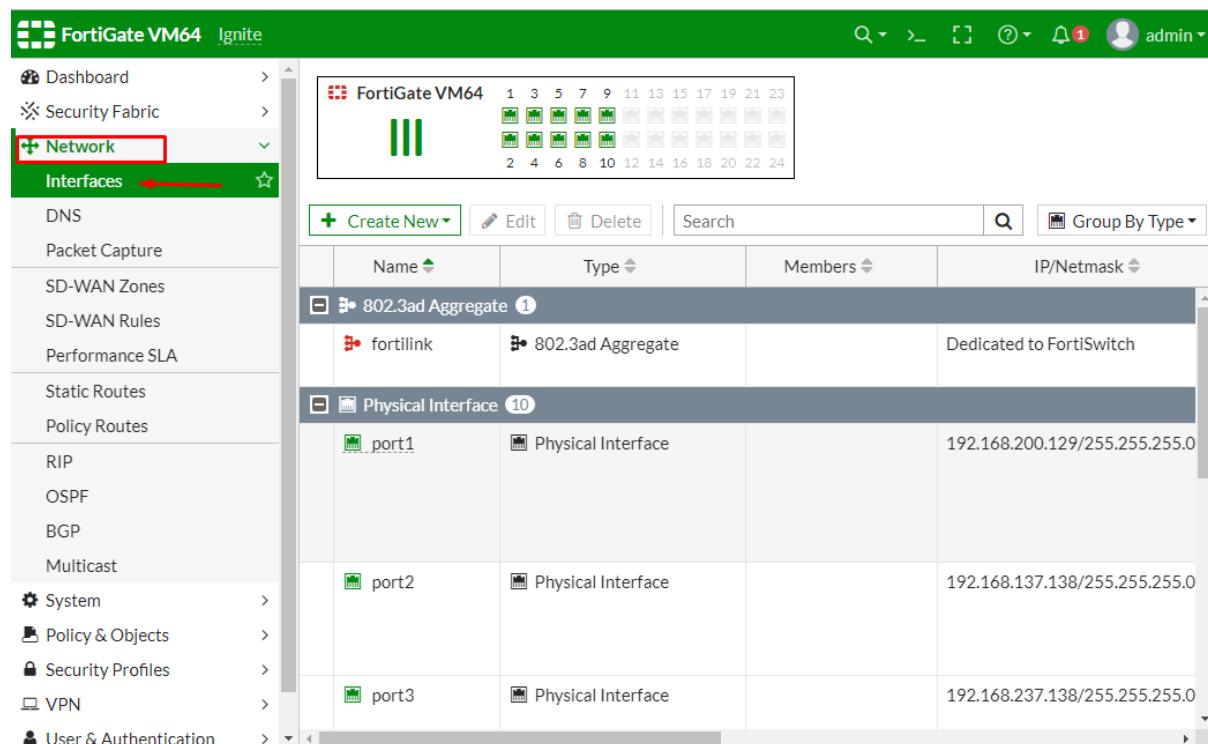
Connect the FortiGate internet facing interface usually WAN1 to your ISP supplied equipment and connect the PC to FortiGate using an internal port usually port 1 or as per your requirement.

Power on ISP equipment, firewall and the PC and they are now in the internal network.

Configure Network Interfaces

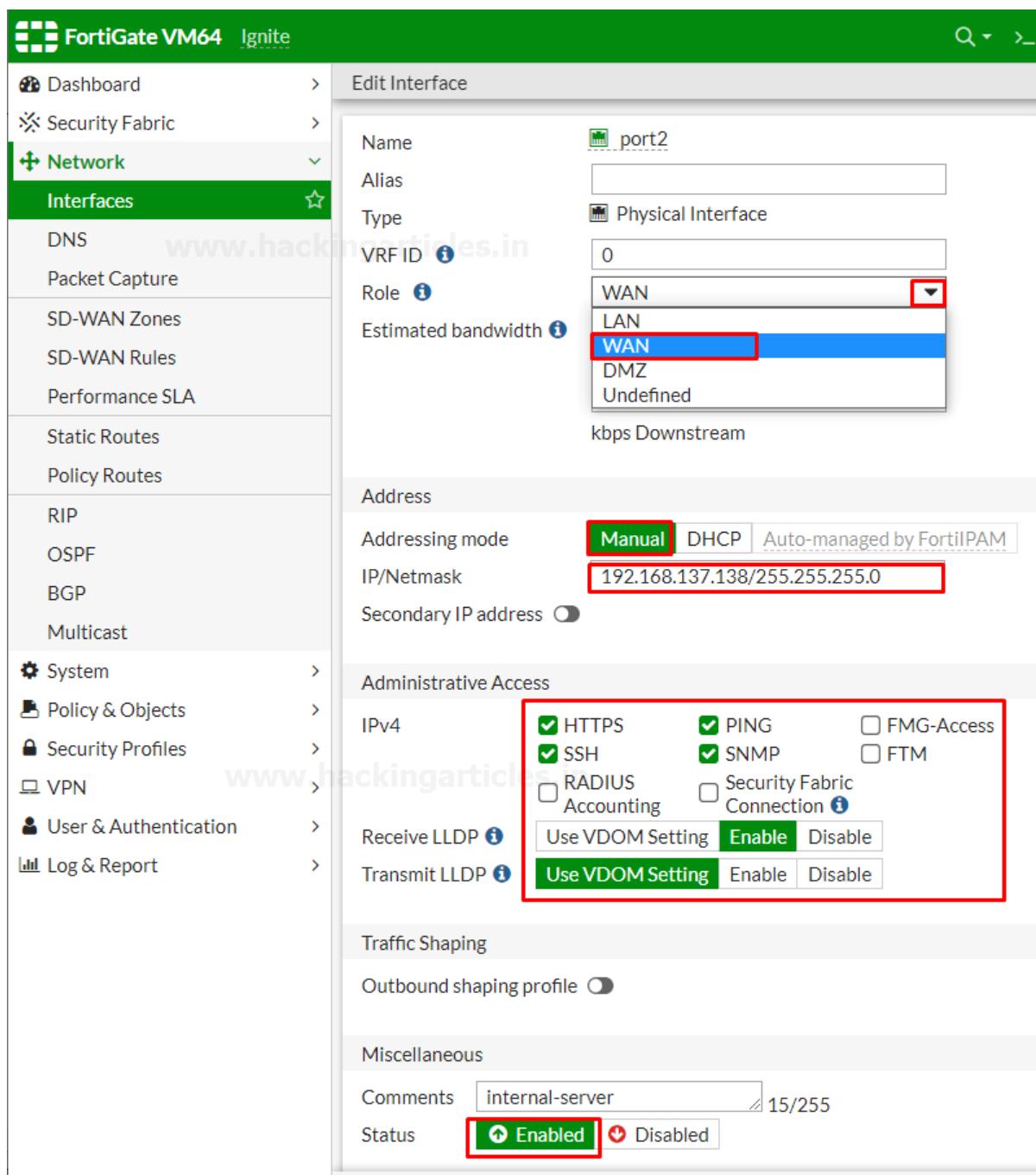
Now you need to configure the FortiGate's Network interfaces.

Go to network > Interfaces



Name	Type	Members	IP/Netmask
802.3ad Aggregate 1	802.3ad Aggregate		Dedicated to FortiSwitch
Physical Interface 10	Physical Interface		
port1	Physical Interface		192.168.200.129/255.255.255.0
port2	Physical Interface		192.168.137.138/255.255.255.0
port3	Physical Interface		192.168.237.138/255.255.255.0

and edit the internet-facing interface set the addressing mode to manual and the IP/Netmask to the public IP address provided by your ISP. Here in my case, I'm considering port2 as an internet-facing interface. Provide Administrative access as per your requirement to the network



FortiGate VM64 Ignite

Edit Interface

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

Address

Addressing mode: Manual (selected), DHCP, Auto-managed by FortiPAM
IP/Netmask: 192.168.137.138/255.255.255.0
Secondary IP address: Off

Administrative Access

IPv4: HTTPS, SSH, RADIUS Accounting, PING, SNMP, Security Fabric Connection, FMG-Access, FTM

Receive LLDP: Use VDOM Setting (selected), Enable, Disable
Transmit LLDP: Use VDOM Setting (selected), Enable, Disable

Traffic Shaping

Outbound shaping profile: Off

Miscellaneous

Comments: internal-server
Status: Enabled (selected), Disabled

Then save the configuration and then similarly edit the LAN interface which may be called internal network. Set the interfaces Role to the LAN or WAN and then set the addressing mode to manual and set the IP/Netmask to the private IP address that you want to assign to the FortiGate

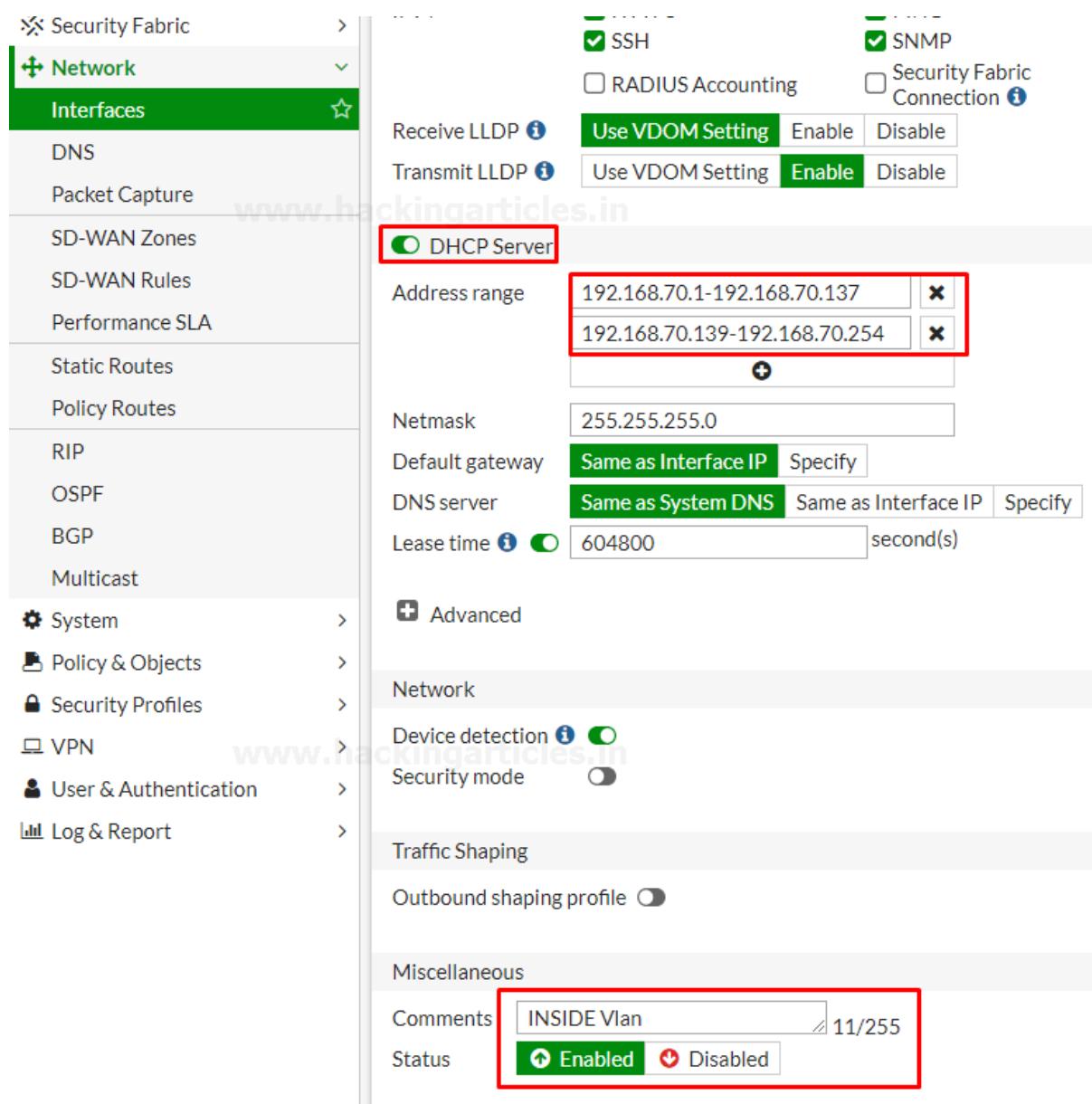
FortiGate VM64 1 3 5 7 9 11 13 15 17 19 21 23
 2 4 6 8 10 12 14 16 18 20 22 24

Create New ▾ **Edit** **Delete** **Search** **Group By Type ▾**

Administrative Access TELNET PING HTTPS SSH SNMP

Name	Type	Members	IP/Netmask	Administrative Access
port2	Physical Interface		192.168.137.138/255.255.255.0	PING HTTPS SSH SNMP
port3	Physical Interface		192.168.237.138/255.255.255.0	PING HTTPS SSH SNMP
port4	Physical Interface		192.168.70.138/255.255.255.0	PING HTTPS SSH SNMP
port5	Physical Interface		192.168.80.138/255.255.255.0	PING HTTPS SSH SNMP HTTP
port6	Physical Interface		10.1.20.138/255.255.255.0	PING HTTPS SSH SNMP HTTP
port7	Physical Interface		0.0.0.0/0.0.0.0	
port8	Physical Interface		0.0.0.0/0.0.0.0	
port9	Physical Interface		0.0.0.0/0.0.0.0	

If you need your FortiGate to provide IP addresses to devices connected to internal network enable the DHCP server and then save the configuration as shown below.



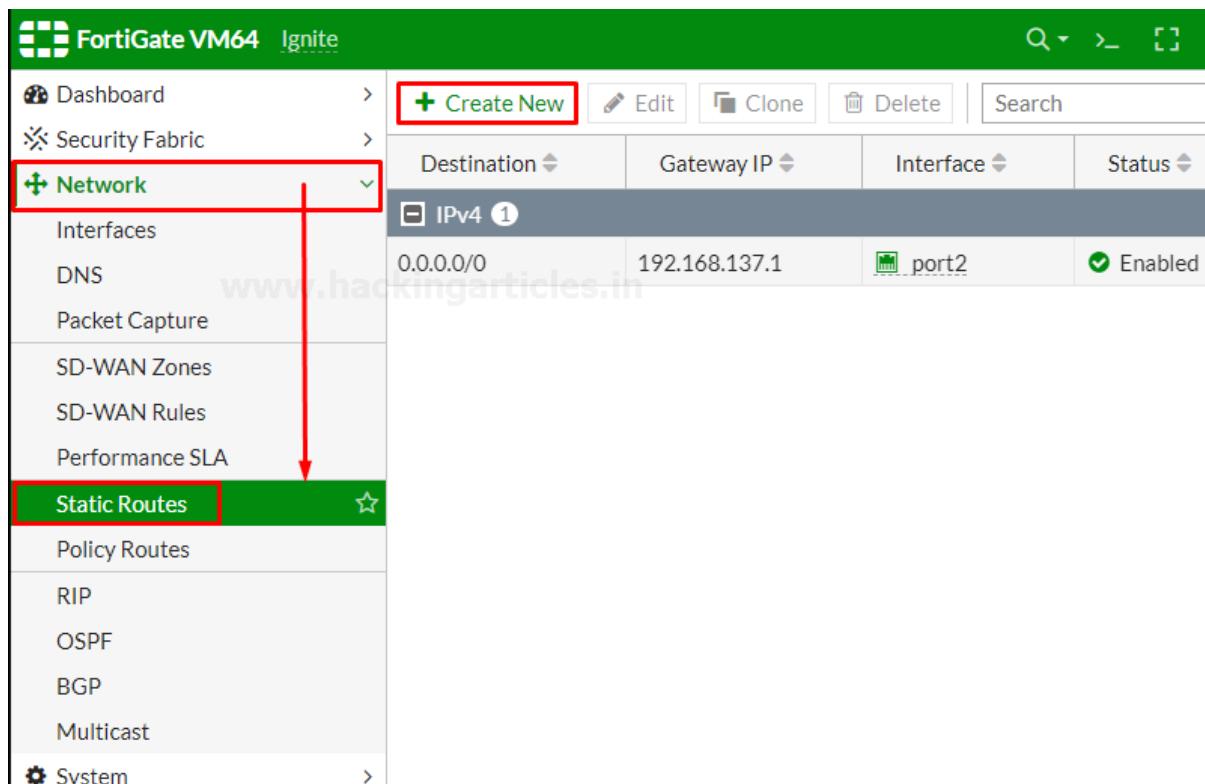
The screenshot shows the FortiGate interface configuration under the Network > Interfaces section. The left sidebar lists various network-related options like DNS, SD-WAN Zones, and System. The main configuration area is divided into several sections:

- SSH:** Enabled.
- RADIUS Accounting:** Disabled.
- SNMP:** Enabled.
- Security Fabric Connection:** Disabled.
- Receive LLDP:** Use VDOM Setting (Enabled).
- Transmit LLDP:** Use VDOM Setting (Enabled).
- DHCP Server:** Enabled. The address range is set to 192.168.70.1-192.168.70.137 and 192.168.70.139-192.168.70.254. A red box highlights this range.
- Netmask:** 255.255.255.0.
- Default gateway:** Same as Interface IP (Selected).
- DNS server:** Same as System DNS (Selected).
- Lease time:** 604800 second(s).
- Advanced:** Device detection (Enabled), Security mode (Disabled).
- Network:** Outbound shaping profile (Disabled).
- Traffic Shaping:** Outbound shaping profile (Disabled).
- Miscellaneous:** Comments: INSIDE Vlan, Status: Enabled (Selected). A red box highlights the status dropdown.

Changing the default IP of your interfaces is recommended for the security measures. But you are connected to the FortiGate through that interface the FortiGate will log you out and you must navigate to the new IP address assigned to the interface and login again.

Add a Default Route

Now Go to Network > Static Routes and create a new Route to allow your FortiGate to reach the internet



The screenshot shows the FortiGate VM64 Ignite web interface. The left sidebar is titled 'Network' and contains the following options: Dashboard, Security Fabric, Network (selected), Interfaces, DNS, Packet Capture, SD-WAN Zones, SD-WAN Rules, Performance SLA, Static Routes (highlighted with a red box), Policy Routes, RIP, OSPF, BGP, Multicast, and System. A red arrow points from the 'Static Routes' option in the sidebar to the 'Create New' button in the top right of the main content area. The main content area has a header with 'FortiGate VM64 Ignite' and buttons for Create New, Edit, Clone, Delete, and Search. Below the header is a table with columns: Destination, Gateway IP, Interface, and Status. A single row is shown under the 'IPv4' section, labeled '1'. The row details are: Destination 0.0.0.0/0, Gateway IP 192.168.137.1, Interface port2, and Status Enabled.

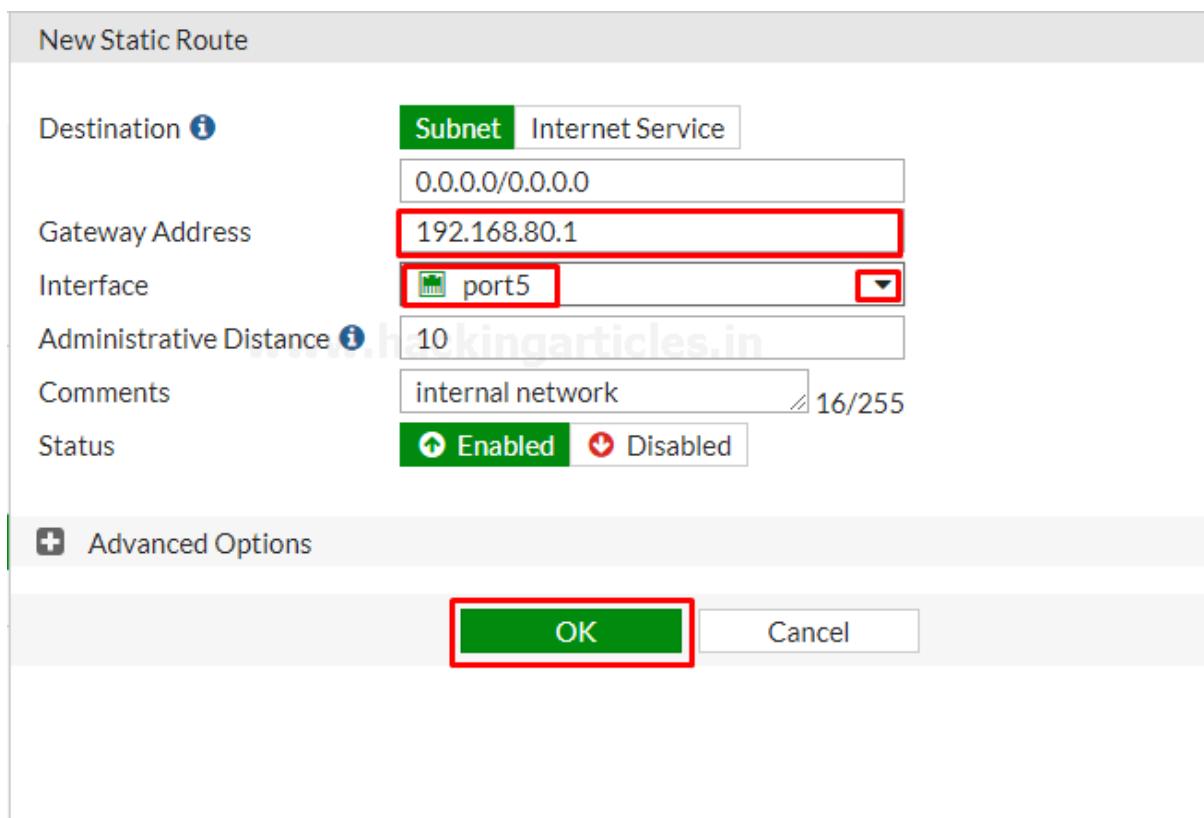
Set destination to subnet and enter IP/Netmask of Eight Zeros. Set the Gateway to the Gateway IP provided by your ISP and the interfaces to the internet-facing interface then save the Route.

New Static Route

Destination <small>i</small>	<input checked="" type="radio"/> Subnet <input type="radio"/> Internet Service
Gateway Address	0.0.0.0/0.0.0.0 192.168.80.1
Interface	<input checked="" type="radio"/> port5 <input type="radio"/>
Administrative Distance <small>i</small>	10
Comments	internal network / 16/255
Status	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled

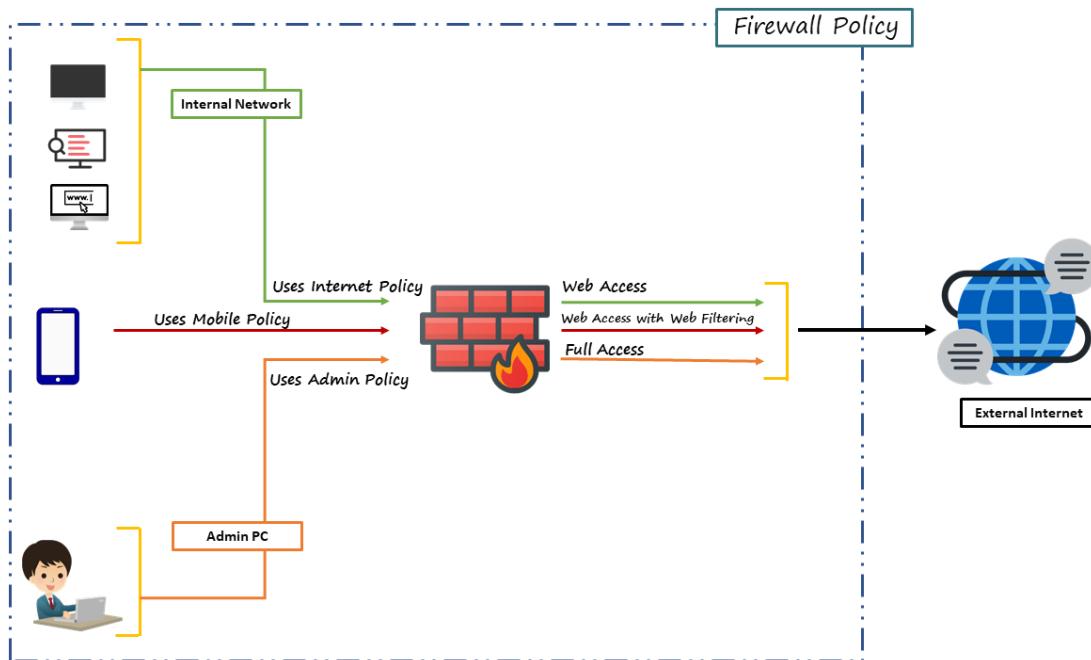
Advanced Options

OK **Cancel**

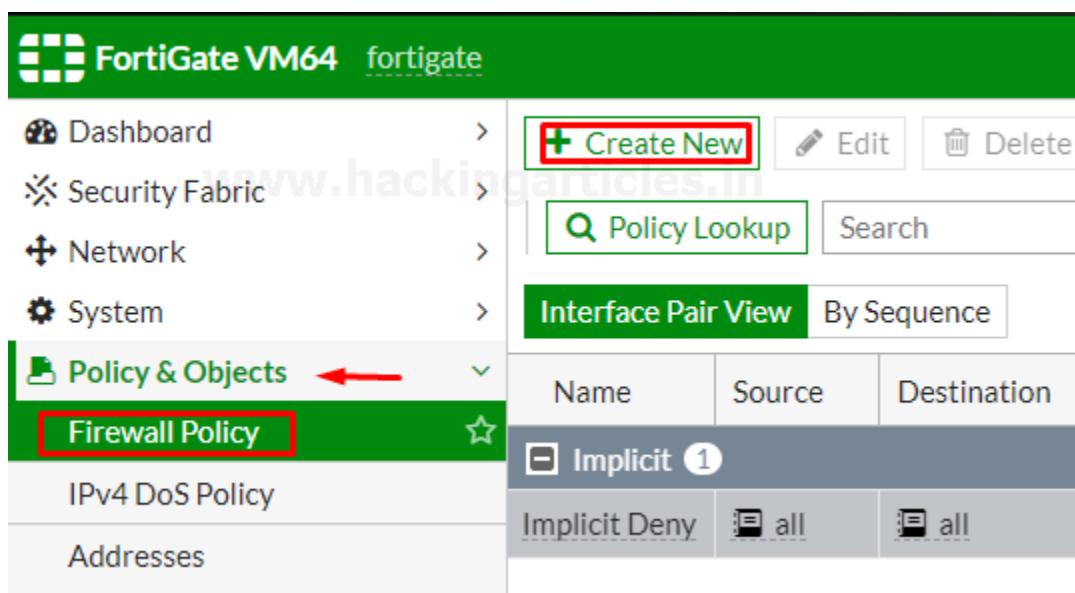


Create an IPV4 Firewall Policy

Firewall policy designed in a manner to examine Network Traffic using policy statements to block unauthorized access while permitting authorized communication.



Go to **Policy & Objects > Firewall Policy** and create a new policy which allow internet traffic through the FortiGate.



The screenshot shows the FortiGate VM64 web interface. The left sidebar menu is visible with the following items: Dashboard, Security Fabric, Network, System, Policy & Objects (highlighted with a red arrow), Firewall Policy (highlighted with a red box), IPv4 DoS Policy, and Addresses. The main content area shows a table for **Implicit** rules:

Name	Source	Destination
Implicit	Implicit Deny	all

Name the policy as “**Internet-Traffic**” or whatever you want. Set the incoming interface to the “**Internal interface**” and outgoing interface to the internet facing interface. Set the rest to allow “**ALL**” Traffic or you can select multiple rules by selecting **the + icon** and the action to “**Accept**” enable the “**NAT**” and make sure “**Use Outgoing Interface Address is enabled**”

New Policy

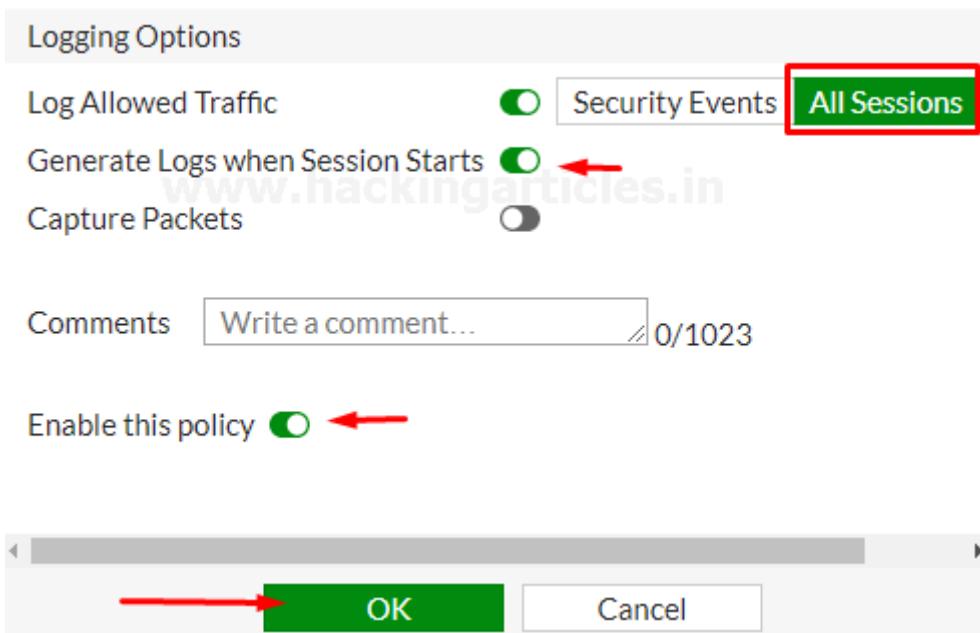
Name	internet access
Incoming Interface	port1
Outgoing Interface	port2
Source	all
Destination	all
Schedule	always
Service	<div style="border: 1px solid red; padding: 5px;"> DNS HTTP HTTPS </div>
Action	<input checked="" type="button"/> ACCEPT <input type="button"/> DENY
Inspection Mode	<input checked="" type="radio"/> Flow-based <input type="radio"/> Proxy-based
Firewall / Network Options	
NAT	<input checked="" type="checkbox"/>
IP Pool Configuration	<input type="radio"/> Use Outgoing Interface Address <input type="radio"/> Use Incoming Interface Address

Select Entries

Search

- SERVICE (61)
 - General (5)
 - * ALL
 - ALL_ICMP
 - ALL_ICMP6
 - ALL_TCP
 - ALL_UDP
- Web Access (2)
 - HTTP
 - HTTPS
- File Access (8)
 - AFS3
 - FTP
 - FTP_GET
 - FTP_PUT
 - NFS
 - SAMBA
 - SMB
 - TFTP
- Email (6)
 - IMAP
 - MAPI

Scroll down to view the logging options to Log and track internet traffic “enable Log Allowed Traffic and select All session”



After saving it you can check your saved policy is going back to a firewall policy

Policy List									Interface Pair View	By Sequence
Name	Source	Destination	Schedule	Action	NAT	Security Profiles	Log			
port1 → port2 ①	internet-traffic	all	always	ALL	ACCEPT	Enabled	SSL no-inspection	All		
Implicit ①	Implicit Deny	all	always	ALL	DENY	Enabled				

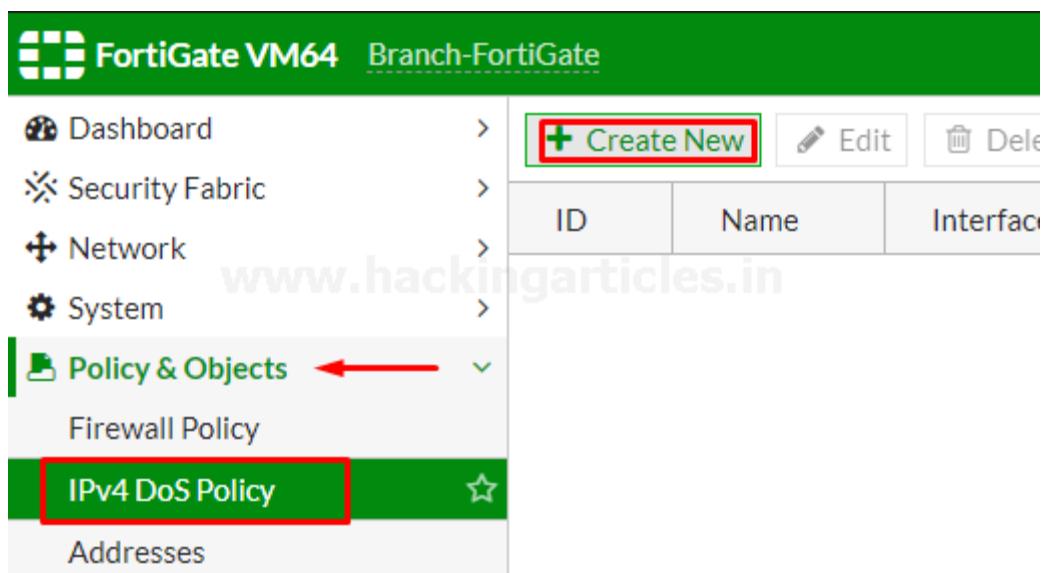
As you can see the policy successfully enabled.

Create an IPv4 Dos Policy

Dos policy is a traffic anomaly detection feature to identify network traffic that does not fit known or common traffic patterns. Dos policies are used to apply Dos anomaly checks to network traffic based on the FortiGate interface. A common example of anomalous traffic is the Dos (Denial of Service) Attack. A denial of service occurs when an attacking system starts an abnormally large number of sessions with the target system and resultant a large number of sessions slow down or disables the target system.

To configure IPV4 policy

- Go to Policy & Objects > IPv4 Dos Policy
- To create a new policy, select the Create New icon in the top left side of the right window.



The screenshot shows the FortiGate VM64 Branch-FortiGate interface. The left sidebar has a tree view with nodes: Dashboard, Security Fabric, Network, System, Policy & Objects (selected), Firewall Policy, IPv4 DoS Policy (selected with a red box around it), and Addresses. A red arrow points from the text 'IPv4 DoS Policy' in the main content area to the 'IPv4 DoS Policy' node in the sidebar. The main content area has a 'Create New' button with a green border and a red box around it. Below it is a table with columns ID, Name, and Interface.

Set the incoming interface parameter by using drop-down menu to select a single interface.

Set the Source Address, Destination Address, and Service to “ALL”. Single or multiple options can be selected as per your requirement.

Set the parameters for various type of Traffic Anomalies.

The breakup of traffic anomalies table is divided into 2 parts.

- L3 Anomalies
- L4 Anomalies

Here is the list of Anomaly profile that includes:

L3 Anomalies

- ip_src_session
- ip_dst_session

New Policy

Name	<input type="text" value="Dos-protection-policy"/>
Incoming Interface	<input type="text" value="port1"/>
Source Address	<input type="text" value="all"/>
Destination Address	<input type="text" value="all"/>
Service	<input type="text" value="ALL"/>

L3 Anomalies

Name	Logging	Action	Threshold
ip_src_session	<input checked="" type="checkbox"/>	<input type="button" value="Disable"/> <input checked="" type="button" value="Block"/> <input type="button" value="Monitor"/>	5000
ip_dst_session	<input checked="" type="checkbox"/>	<input type="button" value="Disable"/> <input checked="" type="button" value="Block"/> <input type="button" value="Monitor"/>	5000

L4 Anomalies

- tcp_syn_flood
- tcp_port_scan
- tcp_src_session
- tcp_dst_session
- udp_flood
- udp_scan
- udp_src_session
- udp_dst_session
- icmp_flood
- icmp_sweep
- icmp_src_session
- sctp_flood
- sctp_scan
- sctp_src_session
- sctp_dst_session

Name	Logging	Action	Threshold
		Disable Block Monitor	
tcp_syn_flood	<input checked="" type="checkbox"/>	Disable Block Monitor	2000
tcp_port_scan	<input checked="" type="checkbox"/>	Disable Block Monitor	1000
tcp_src_session	<input type="checkbox"/>	Disable Block Monitor	5000
tcp_dst_session	<input type="checkbox"/>	Disable Block Monitor	5000
udp_flood	<input checked="" type="checkbox"/>	Disable Block Monitor	2000
udp_scan	<input checked="" type="checkbox"/>	Disable Block Monitor	2000
udp_src_session	<input type="checkbox"/>	Disable Block Monitor	5000
udp_dst_session	<input type="checkbox"/>	Disable Block Monitor	5000
icmp_flood	<input checked="" type="checkbox"/>	Disable Block Monitor	250
icmp_sweep	<input type="checkbox"/>	Disable Block Monitor	100
icmp_src_session	<input type="checkbox"/>	Disable Block Monitor	300
icmp_dst_session	<input type="checkbox"/>	Disable Block Monitor	1000

OK Cancel

It all your choice whether or not to enable this policy and default is enabled. Here in our case, we have blocked some of the actions with the limited threshold values to check whether these policies working or not.

All Anomalies have the following parameters that can be set on Per Anomaly or Per Column Basis

- Status: – from this menu you can enable or disable the indicated profile.
- Logging: – Enable or Disable tracking and logging of the indicated profile being triggered.
- Action: – choices yours whether to pass or block traffic when it reaches the threshold limit.
- Threshold: – It is the number of anomalous packets detected before triggering the action.



And at last, select the ok button and save the policy.

Create New Edit Delete Search					
ID	Name	Interface	Source Address	Destination Address	Service
1	Dos-protection-policy	port1	all	all	All

As we can see Dos-protection-Policy is successfully deployed.

Let's check these policies are truly protect the network from Dos attacks or not.

Hmm, exited

Let's do it

Fire up the Attacker Machine kali Linux and run the following command

```
hping -c 15000 -d 120 -S -w 64 -p 80 -flood -rand-source 192.168.200.128
```

where 192.168.200.128 is the management IP of FortiGate

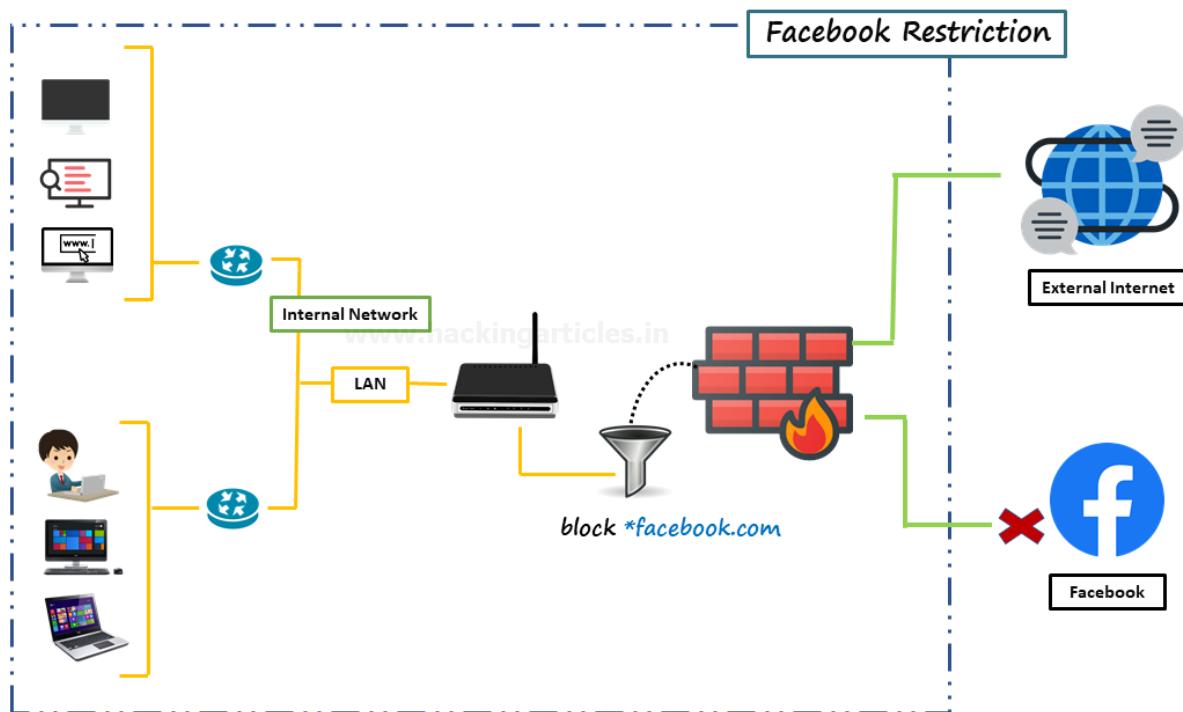
```
(root㉿kali)-[~/home/lucifer]
# hping3 -c 15000 -d 120 -S -w 64 -p 80 --flood --rand-source 192.168.200.128
HPING 192.168.200.128 (eth0 192.168.200.128): S set, 40 headers + 120 data bytes
hping in flood mode, no replies will be shown
^@^C
--- 192.168.200.128 hping statistic ---
10816342 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
(root㉿kali)-[~/home/lucifer]
#
```

As we can see it blocks whole traffic that means it works properly.

Blocking Facebook with Web filter

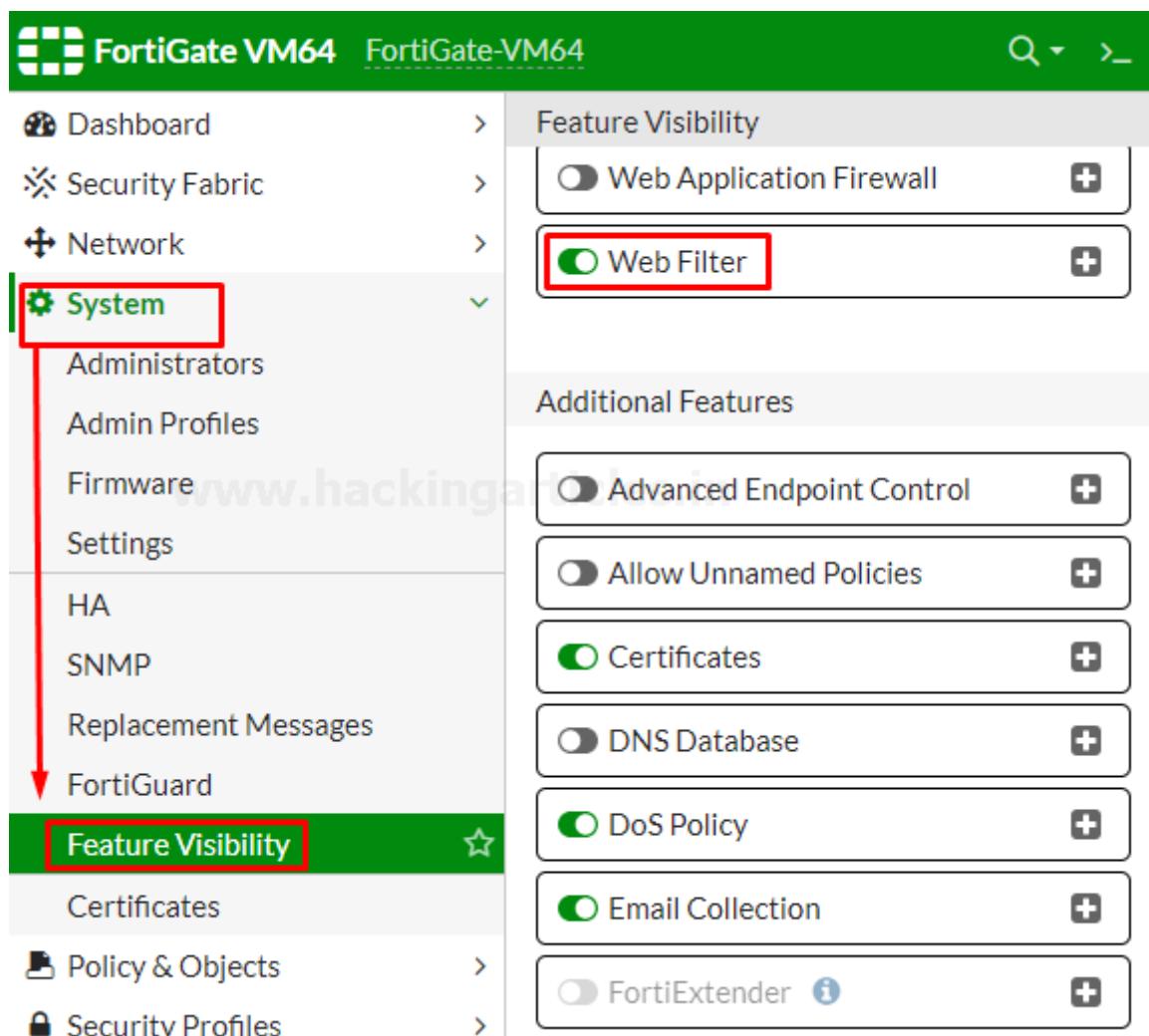
In this part, we are going to explain how to use a static URL filter to block access to Facebook and its subdomain in our network.

With the help of SSL inspection, you can also ensure that Facebook and its subdomains are also blocked whenever it will be accessed through HTTPS.



Enable Web filter

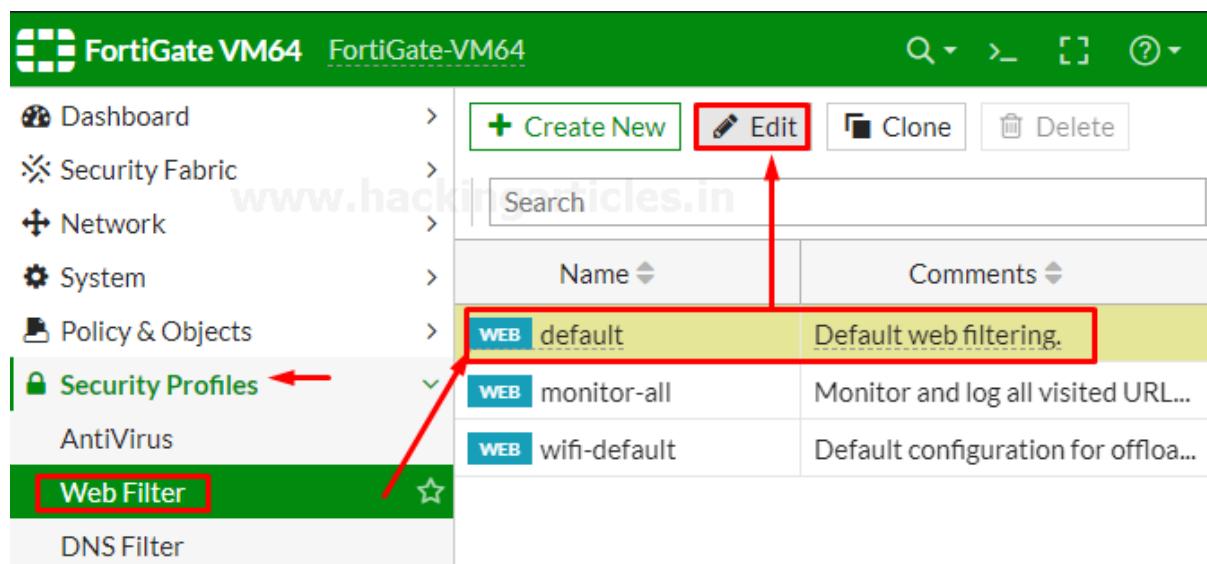
Go to **system > feature Visibility** and enable the Web Filter Feature



The screenshot shows the FortiGate VM64 web interface. The left sidebar has a 'System' section with 'Feature Visibility' highlighted. The main panel shows 'Feature Visibility' settings, where 'Web Filter' is turned on (green switch). Other features like 'Web Application Firewall' and 'Advanced Endpoint Control' are off (grey switches).

Enable Default Web Filter Profile

Go to **Security profiles > Web filter** and edit the default Web filter profile

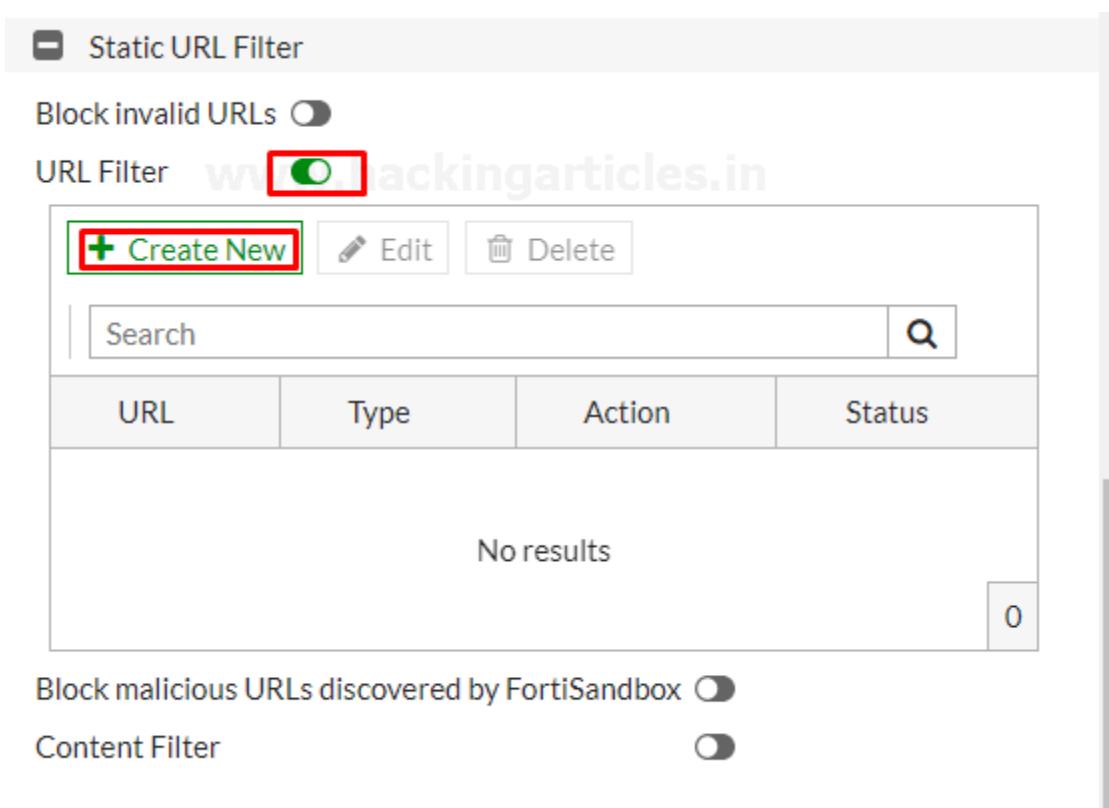


FortiGate VM64 FortiGate-VM64

- Dashboard
- Security Fabric
- Network
- System
- Policy & Objects
- Security Profiles** ←
- AntiVirus
- Web Filter**
- DNS Filter

Name	Comments
WEB default	Default web filtering.
WEB monitor-all	Monitor and log all visited URL...
WEB wifi-default	Default configuration for offloa...

Now go to Static URL filter, select the URL filter and then select “create”.



Static URL Filter

Block invalid URLs

URL Filter

URL	Type	Action	Status
No results 0			

Block malicious URLs discovered by FortiSandbox

Content Filter

Further then Set **URL** to “facebook.com”, set **Type** to “Wildcard”, set **Action** to “Block” and set **status** to “Enable”.

New URL Filter

URL	*facebook.com		
Type	Simple	Regular Expression	Wildcard
Action	Exempt	Block	Allow
Status	Enable	Disable	

OK Cancel

save it by selecting OK

URL Filter (On)

+ Create New	Edit	Delete	
Search 🔍			
URL	Type	Action	Status
*facebook.c...	Wildcard	Block	Enable

Block malicious URLs discovered by FortiSandbox (On)

Content Filter (Off)

Rating Options

Allow websites when a rating error occurs (On)

Rate URLs by domain and IP Address (On)

Proxy Options

HTTP POST Action Allow **Block**

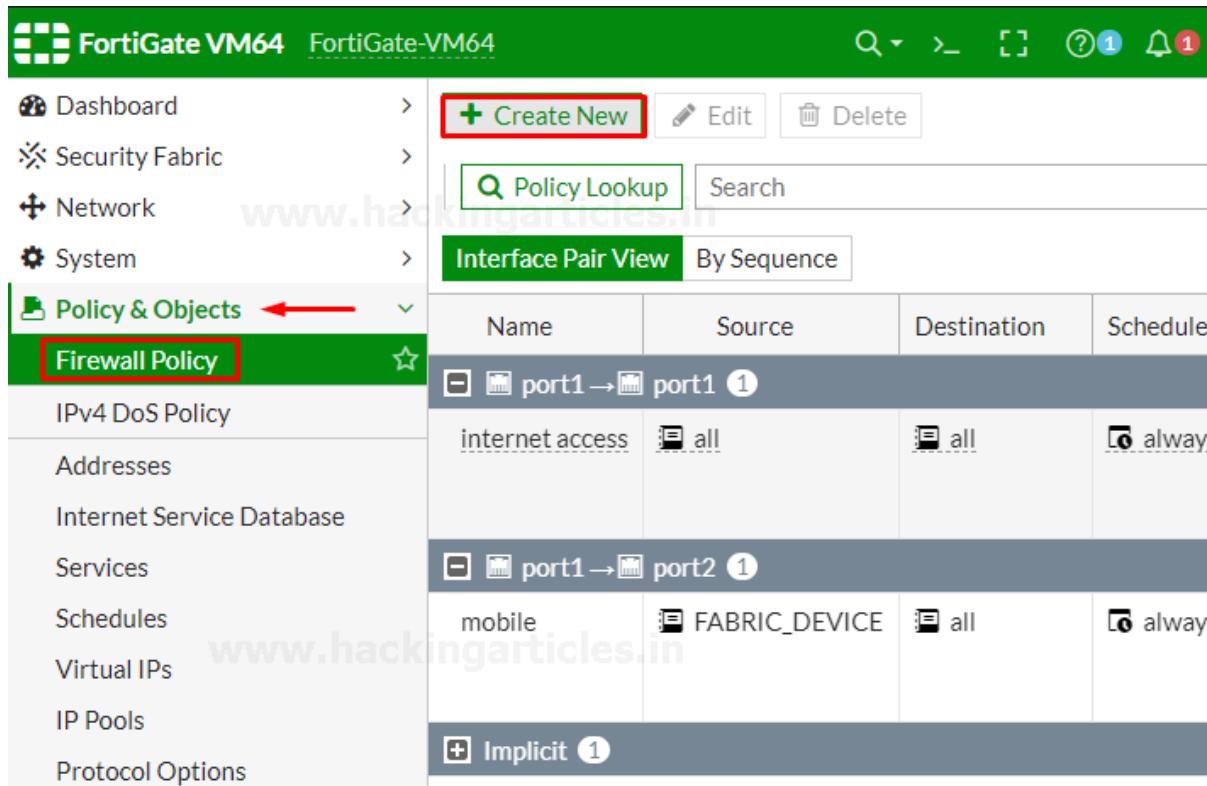
Remove Cookies (On)

OK Cancel

Now you have successfully enabled web filter to block Facebook.

Create Web Filter Security Policy

Go to Policy & Objects > Firewall Policy and Create a New policy.



The screenshot shows the FortiGate VM64 interface. The left sidebar has a red arrow pointing to the 'Policy & Objects' section, which is expanded to show 'Firewall Policy'. A red box highlights the 'Create New' button in the top right corner of the main content area. Below it, there's a search bar and tabs for 'Interface Pair View' and 'By Sequence'. The main table lists three firewall policies:

Name	Source	Destination	Schedule
port1 → port1 1	Internet access	all	always
port1 → port2 1	mobile	FABRIC_DEVICE	all
Implicit 1			

Give the name to the policy “No-Facebook-Internet-Access” to make it identifiable.

Set **Incoming Interface** to the internal network and set **Outgoing Interface** to the Internet-facing interface. Set the rest to allow “ALL” Traffic or you can select multiple rules by selecting the + icon and the action to “Accept” enable the “NAT” and make sure “Use Outgoing Interface Address is enabled”

Under **Security Profiles**, enable “**Web Filter**” and select the default web filter profile.

New Policy

Name	<input type="text" value="No-Facebook-internet-access"/>
Incoming Interface	<input type="button" value="port1"/>
Outgoing Interface	<input type="button" value="port2"/>
Source	<input type="button" value="all"/> + <input type="button" value="X"/>
Destination	<input type="button" value="all"/> + <input type="button" value="X"/>
Schedule	<input type="button" value="always"/>
Service	<input type="button" value="ALL"/> + <input type="button" value="X"/>
Action	<input checked="" type="button" value="ACCEPT"/> <input type="button" value="DENY"/> <input type="button" value="IPsec"/>

Inspection Mode

Firewall / Network Options

NAT	<input checked="" type="button"/>
IP Pool Configuration	<input type="button" value="Use Outgoing Interface Address"/> <input type="button" value="Use Dynamic IP Pool"/>
Preserve Source Port	<input type="button"/>
Protocol Options	<input type="button" value="PROT default"/> <input type="button"/>

Security Profiles

AntiVirus	<input type="button"/>
Web Filter	<input checked="" type="button"/> <input type="button" value="WEB default"/> <input type="button"/> <input type="button"/>

Now we have successfully deployed the policy that block the user to visit Facebook and its subdomains. But don't forget one important thing this policy won't work until it is on the top of list of deployed policies. Confirm this by viewing policies "**By Sequence**".



VM64

Create New Edit Delete Policy Lookup Search admin

Interface Pair View By Sequence

Name	From	To	Source	D...	Schedule	Service	Action	NAT	Securi
internet access	port1	port1	all	all	always	DNS HTTP HTTPS	✓ ACCEPT	✓ Enabled	SSL cert
mobile	port1	port2	FABR...	all	always	DNS HTTP HTTPS	✓ ACCEPT	✓ Enabled	WEB defa SSL cert
No-Facebook-i	port1	port2	all	all	always	ALL	✓ ACCEPT	✓ Enabled	WEB defa SSL cert
Implicit Deny	any	any	all	all	always	ALL	✗ DENY		

To move Policy up or down, select the policy and drag it up or down as per your requirement as shown below

VM64

Create New Edit Delete Policy Lookup Search admin

Interface Pair View By Sequence

⚙ Name	From	To	Source	D...	Schedule	Service	Action	NAT	Securi
No-Facebook-i	port1	port2	all	all	always	ALL	✓ ACCEPT	✓ Enabled	WEB defa SSL cert
internet access	port1	port1	all	all	always	DNS HTTP HTTPS	✓ ACCEPT	✓ Enabled	SSL cert
mobile	port1	port2	FABR...	all	always	DNS HTTP HTTPS	✓ ACCEPT	✓ Enabled	WEB defa SSL cert
Implicit Deny	any	any	all	all	always	ALL	✗ DENY		

Now this policy is in effect and successfully enabled.

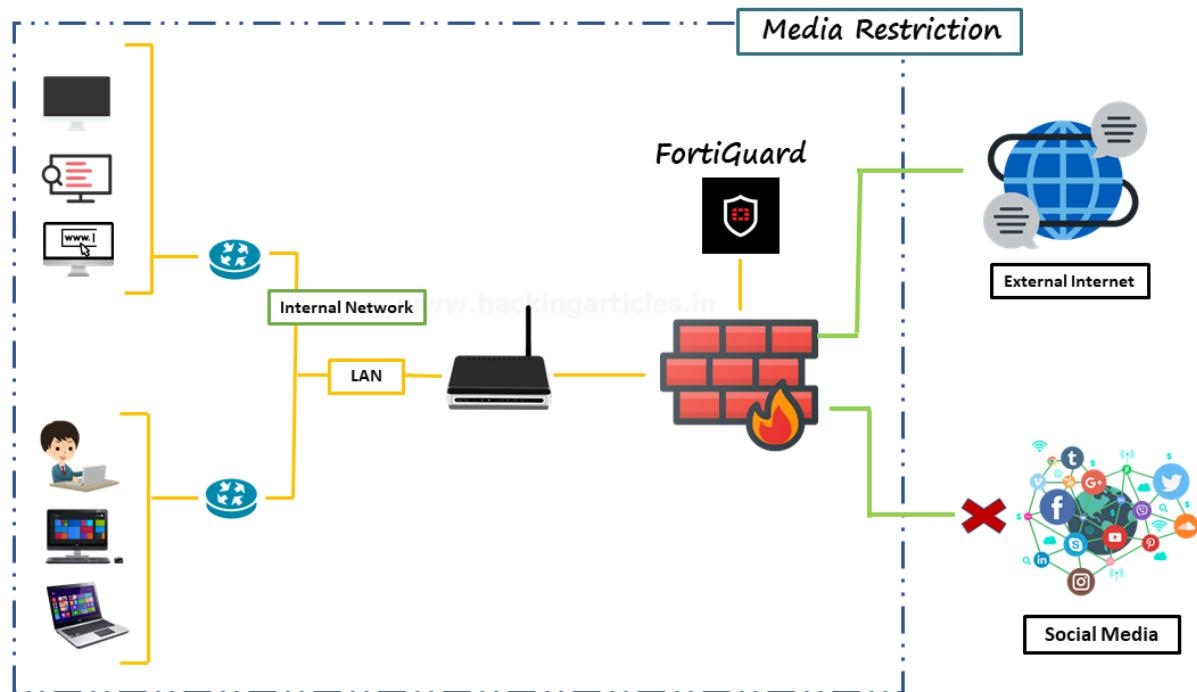
So, in this part, we have covered some basic policies that is much needed to save you network from unauthorized traffic.

Block Whole Social media using FortiGuard categories

In this part, we are going to explain how to block access to social media websites using FortiGuard categories.

Must remind one thing an active license of FortiGuard web filtering service is required for using this type of function.

Web filtration with FortiGuard categories enables you to take action against a group of websites on the other hand a static URL filter is intended to block or monitor specific URL.



Enable web Filter

Go to **system > feature Visibility** and enable the **Web Filter Feature**

Edit Default Web Filter Profile

Go to **Security Profiles > Web Filter** and edit the Default web filter profile and make sure that “**FortiGuard category-based**” filter service is enabled.

Right-click on **General interest** FortiGuard category. scroll down to **Social networking** subcategory and select action to “**Block**” as shown below.

FortiGuard category based filter

Warning: This device is not licensed for the FortiGuard web filtering service.



Traffic may be blocked if this option is enabled.

Allow Monitor Block Warning Authenticate

Name	Action
Education	<input checked="" type="checkbox"/> Allow
Health and Wellness	<input checked="" type="checkbox"/> Allow
Job Search	<input checked="" type="checkbox"/> Allow
Medicine	<input checked="" type="checkbox"/> Allow
News and Media	<input checked="" type="checkbox"/> Allow
Social Networking	<input type="checkbox"/> Block
Political Organizations	<input checked="" type="checkbox"/> Allow
Reference	<input checked="" type="checkbox"/> Allow
Global Religion	<input checked="" type="checkbox"/> Allow

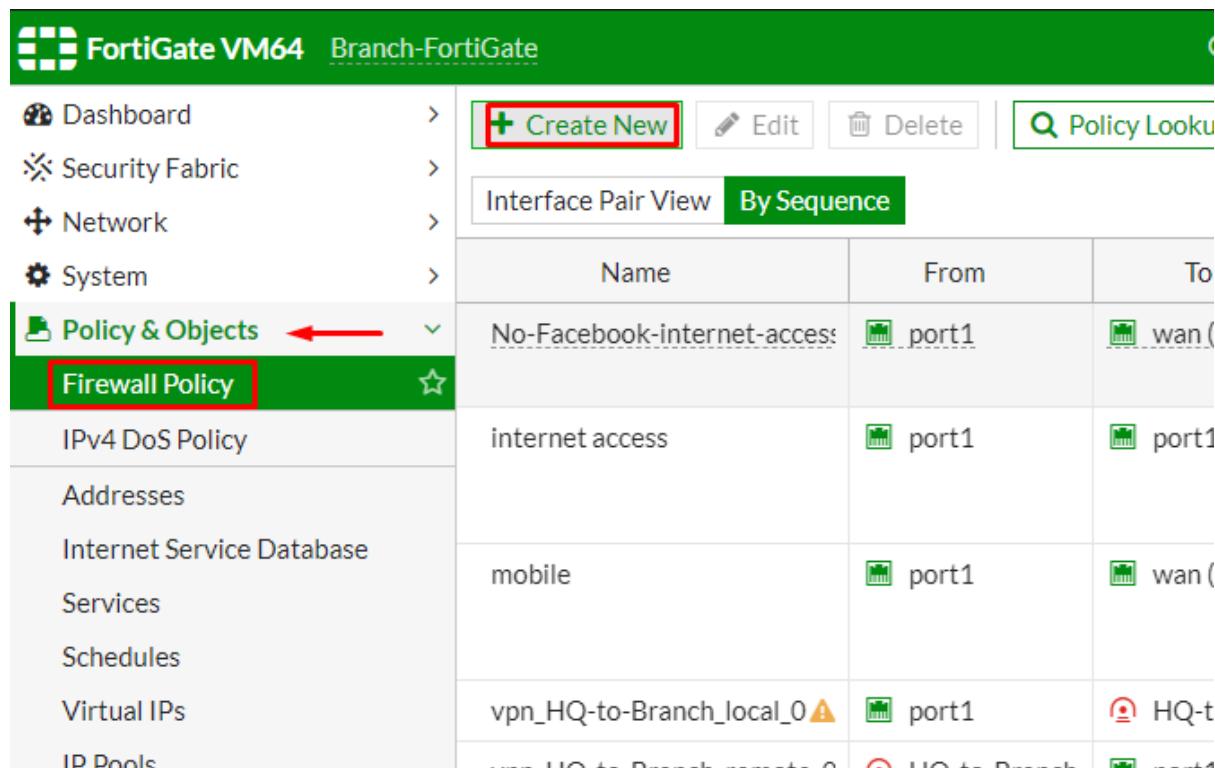
Allow
 Monitor
 Block
 Warning
 Authenticate

OK

Cancel

Add Web Filter Profile to Internet Access Policy

Go to Policy & objects > Firewall Policy and create a new policy



The screenshot shows the FortiGate VM64 interface under the 'Branch-FortiGate' tab. On the left, a sidebar lists various policy objects: Dashboard, Security Fabric, Network, System, Policy & Objects (with a red arrow pointing to it), Firewall Policy (highlighted with a red box), IPv4 DoS Policy, Addresses, Internet Service Database, Services, Schedules, Virtual IPs, and IP Pools. The main panel displays a table of Firewall Policies. The table has columns for Name, From, and To. The visible rows are:

Name	From	To
No-Facebook-internet-access	port1	wan (
internet access	port1	port1
mobile	port1	wan (
vpn_HQ-to-Branch_local_0	port1	HQ-t

At the top right of the main panel, there are buttons for Create New (highlighted with a red box), Edit, Delete, and Policy Lookup.

Give the name to the policy “Blocking-social-media” to make it identifiable. Set incoming interface to internal network and outgoing interface to internet facing interface. Set the rest to allow “ALL” Traffic or you can select multiple rules by selecting the + icon and the action to “Accept” enable the “NAT” and make sure “Use Outgoing Interface Address is enabled”.

Scroll down to **Security profiles** enable **Web Filter** and select **default web filter** profile and save the configuration.

New Policy

Name	Blocking-social-media
Incoming Interface	port1
Outgoing Interface	wan (port2)
Source	all
Destination	all
Schedule	always
Service	ALL
Action	<input checked="" type="checkbox"/> ACCEPT <input type="checkbox"/> DENY <input type="checkbox"/> IPsec

Inspection Mode Flow-based Proxy-based

Firewall / Network Options

NAT	<input checked="" type="radio"/>
IP Pool Configuration	<input checked="" type="radio"/> Use Outgoing Interface Address <input type="radio"/> Use Dynamic IP Poo
Preserve Source Port	<input checked="" type="radio"/>
Protocol Options	PROT default <input type="button" value=""/>

Security Profiles

AntiVirus	<input checked="" type="radio"/>
Web Filter	<input checked="" type="radio"/> WEB default <input type="button" value=""/>
DNS Filter	<input checked="" type="radio"/>

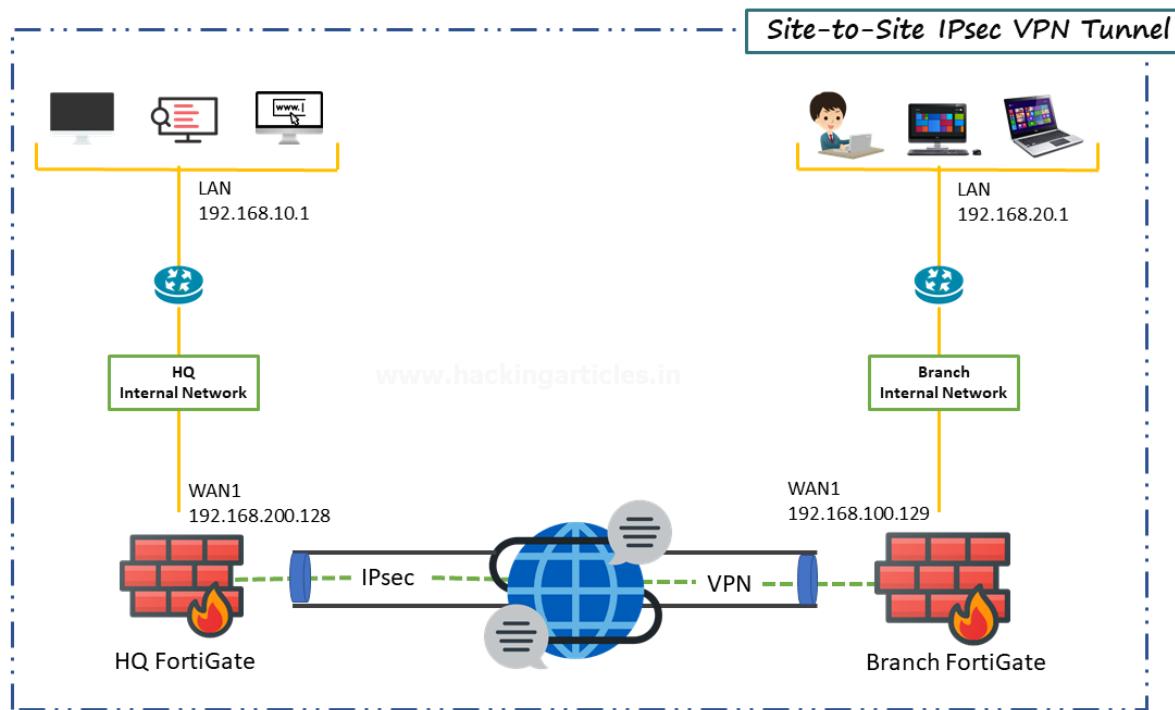
Now you have successfully enabled the social media blocking policy to move this policy to Top of the list to make it effective.

Create New	Edit	Delete	Policy Lookup	Search
Interface Pair View		By Sequence		
Name	From	To	Source	
Blocking-social-media	 port1	 wan (port2)		all
No-Facebook-internet-access	 port1	 wan (port2)		all
internet access	 port1	 port1		all
mobile	 port1	 wan (port2)		FABRIC_DEVICE
vpn_HQ-to-Branch_local_0	 port1	 HQ-to-Branch		HQ-to-Branch_local
vpn_HQ-to-Branch_remote_0	 HQ-to-Branch	 port1		HQ-to-Branch_remote
vpn_Branch-to-HQ_local_0	 wan (port2)	 Branch-to-HQ		Branch-to-HQ_local
vpn_Branch-to-HQ_remote_0	 Branch-to-HQ	 wan (port2)		Branch-to-HQ_remote
Implicit Deny	<input type="checkbox"/> any	<input type="checkbox"/> any		all

Site-to-Site IPsec VPN Tunnel with 2 FortiGates

In this part, we are going to configure a site-to-site IPsec VPN tunnel to allow communication between two networks that are situated behind different FortiGates.

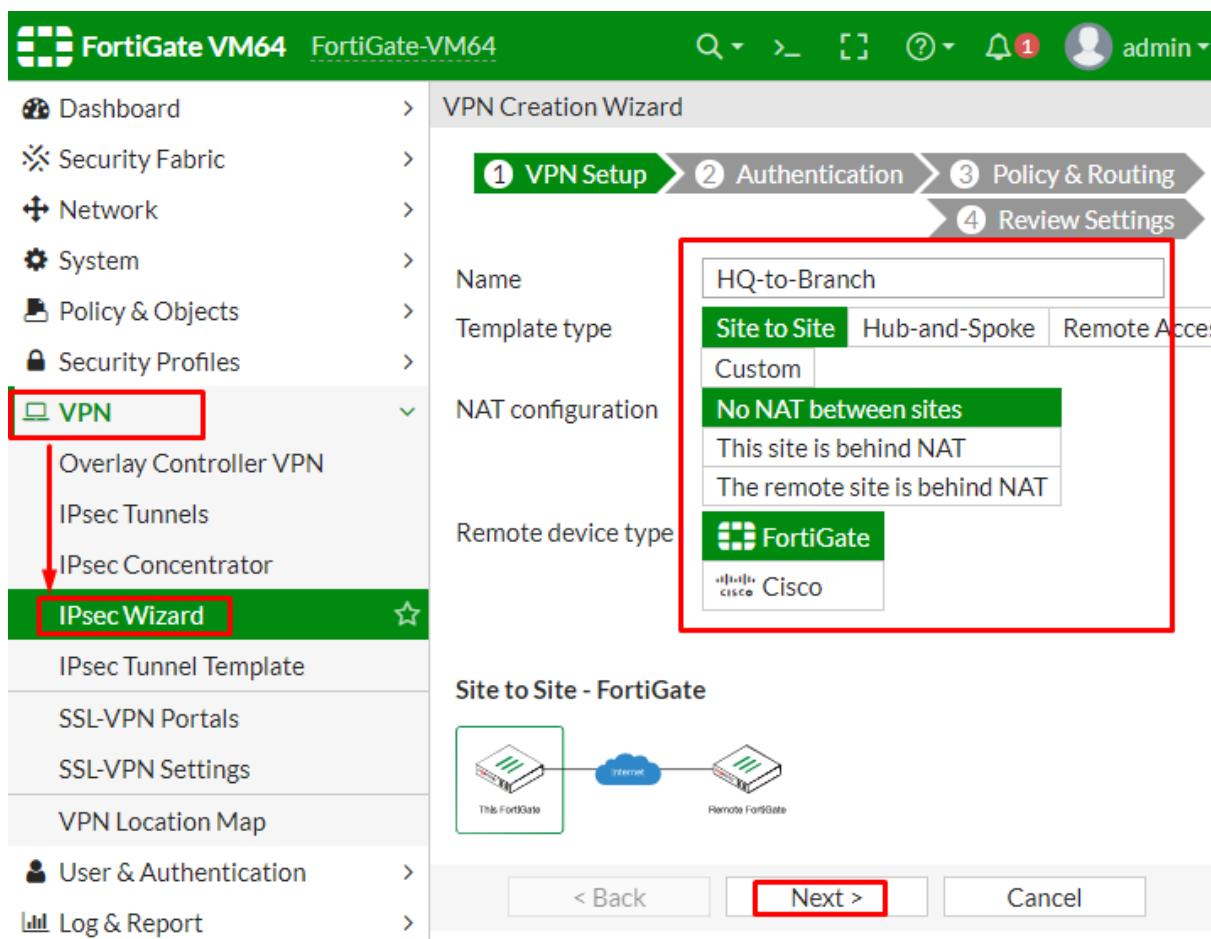
We are going to create an IPsec VPN tunnel between two FortiGates one is called HQ (Headquarter) another is called Branch.



Configure IPsec VPN on HQ

On HQ FortiGate, GO to VPN > IPsec wizard and create a new tunnel.

In the section, VPN setup describe a VPN name to make it identifiable, set Template type to Site-to-Site, set NAT configuration to NO NAT between sites and set Remote Device type to FortiGate.



The screenshot shows the FortiGate VM64 interface with the title "FortiGate VM64 FortiGate-VM64". The left sidebar has a red box around the "VPN" section, which is expanded to show "IPsec Wizard". The main content area shows the "VPN Creation Wizard" with four steps: 1. VPN Setup, 2. Authentication, 3. Policy & Routing, and 4. Review Settings. Step 1 is active. A red box highlights the "Name" field containing "HQ-to-Branch". Below it is a tab bar with "Site to Site" selected, followed by "Hub-and-Spoke" and "Remote Access". A sub-section titled "No NAT between sites" is shown, with "This site is behind NAT" and "The remote site is behind NAT" checked. The "Remote device type" dropdown shows "FortiGate" selected, with "Cisco" as an alternative. At the bottom, there's a diagram titled "Site to Site - FortiGate" showing two FortiGates connected via the Internet. The "Next >" button is highlighted with a red box.

In the Authentication Section, set IP address to Public IP address of the Branch FortiGate.

After entering the IP address an interface is assigned to the outgoing interface. You can change the interface by the drop-down menu as per your requirement.

Set a secure **Pre-shared** key that is used to connect and verification for both FortiGates.

VPN Creation Wizard

1 VPN Setup 2 Authentication 3 Policy & Routing
4 Review Settings

Remote device	IP Address	Dynamic DNS
Remote IP address	192.168.100.129	
Outgoing Interface	port2	
Authentication method	Pre-shared Key	Signature
Pre-shared key	••••••••••	

Site to Site - FortiGate



< Back Next > Cancel

The screenshot shows the second step of a 'VPN Creation Wizard'. The top navigation bar indicates '2 Authentication' is selected. The configuration section on the right is highlighted with a red box. It includes fields for 'IP Address' (192.168.100.129), 'Outgoing Interface' (port2), 'Authentication method' (Pre-shared Key), and a 'Pre-shared key' field containing several dots. Below this is a diagram titled 'Site to Site - FortiGate' showing two FortiGate units connected via the Internet. At the bottom are standard navigation buttons: '< Back', 'Next >' (which is highlighted with a red box), and 'Cancel'.

In the section of **Policy and Routing** set Local interface to “**LAN**” in my case “**Port1**” is dedicated to the LAN and local subnets will add automatically further then set “**Remote Subnets**” to the Branch network and set internet access to “**None**” as shown below

VPN Creation Wizard

1 VPN Setup > 2 Authentication > 3 Policy & Routing > 4 Review Settings

Local interface: port1

Local subnets: 192.168.200.0/24

Remote Subnets: 192.168.100.0/24

Internet Access: None Share Local Use Remote

Site to Site - FortiGate

This FortiGate --- Internet --- Remote FortiGate

< Back Next > Cancel

Review the configuration summary that you configured that shows the interfaces, firewall addresses, routes, and policies after verifying it select create an icon

VPN Creation Wizard

1 VPN Setup > 2 Authentication > 3 Policy & Routing > 4 Review Settings

i The following settings should be reviewed prior to creating the VPN.

Object Summary

Phase 1 interface	HQ-to-Branch
Local address group	HQ-to-Branch_local
Remote address group	HQ-to-Branch_remote
Phase 2 interface	HQ-to-Branch
Static route	static
Blackhole route	static
Local to remote policies	vpn_HQ-to-Branch_local
Remote to local policies	vpn_HQ-to-Branch_remote

< Back **Create** Cancel

After creating the VPN, you can verify the details as shown below.

VPN Creation Wizard

VPN Setup > Authentication > Policy & Routing > Review Settings

The VPN has been set up

Object Summary

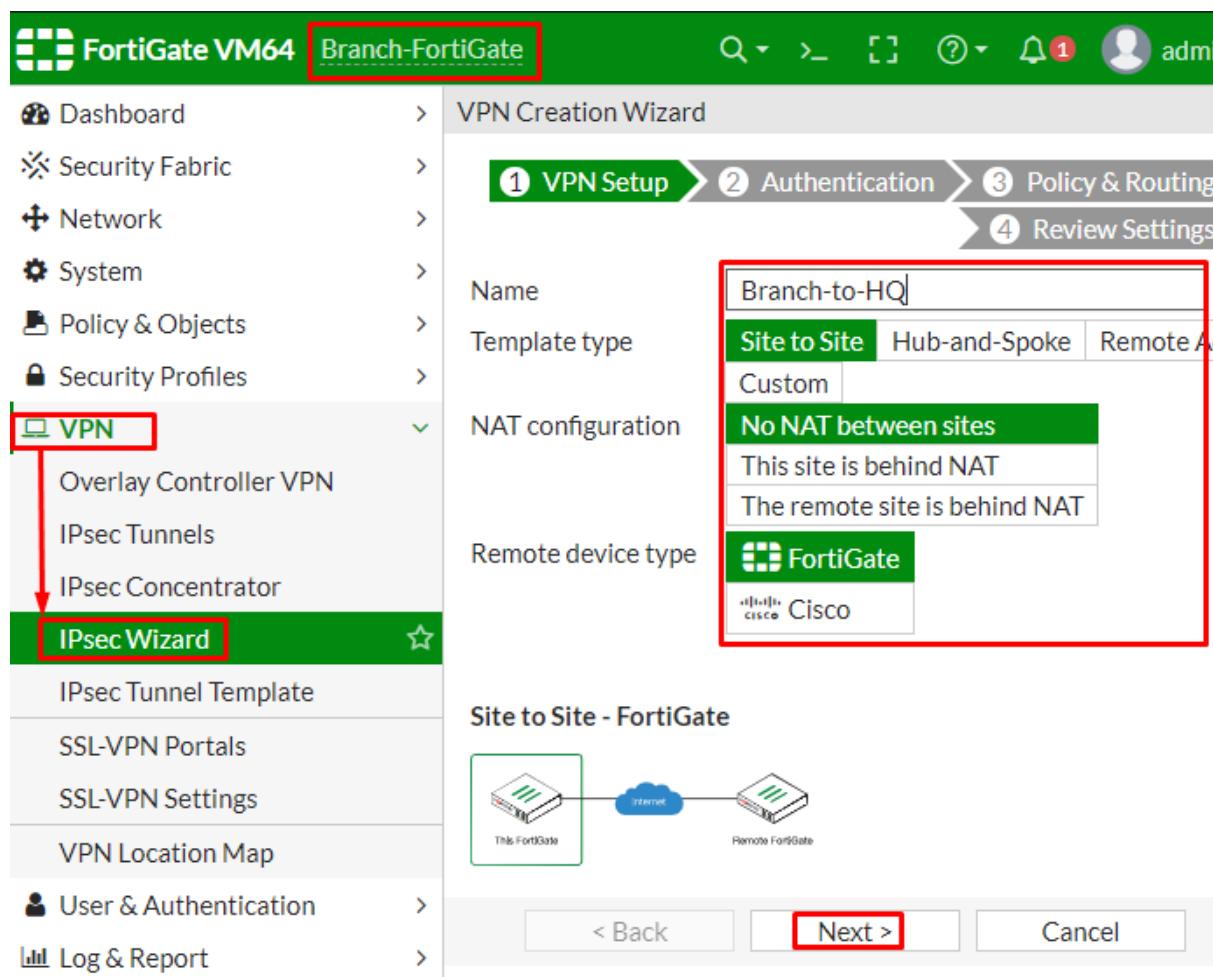
Phase 1 interface	  HQ-to-Branch
Local address group	  HQ-to-Branch_local Edit
Remote address group	  HQ-to-Branch_remote Edit
Phase 2 interface	 HQ-to-Branch
Static route	 1 Edit
Blackhole route	 2 Edit
Local to remote policies	 vpn_HQ-to-Branch_local_0 (4)
Remote to local policies	 vpn_HQ-to-Branch_remote_0 (5)

Add Another Show Tunnel List

Configure IPsec VPN on a branch

On Branch FortiGate, GO to VPN > IPsec wizard and create a new tunnel.

In the section, VPN setup describes a VPN name to make it identifiable, set Template type to Site-to-Site, set NAT configuration to “**NO NAT**” between sites and set Remote Device type to FortiGate.



The screenshot shows the FortiGate VM64 interface with the title bar "Branch-FortiGate". The left sidebar has a red box around "VPN" and a green box around "IPsec Wizard". The main content area shows the "VPN Creation Wizard" with four steps: 1. VPN Setup (selected), 2. Authentication, 3. Policy & Routing, 4. Review Settings. Step 1 has sub-fields: "Name" (Branch-to-HQ), "Template type" (Site to Site selected), "NAT configuration" (No NAT between sites selected), and "Remote device type" (FortiGate selected). A red box highlights the "Site to Site - FortiGate" diagram and the "Next >" button.

In the Authentication Section, set IP address to Public IP address of the Branch FortiGate.

After entering the IP address an interface is assigned to the outgoing interface. You can change the interface by the drop-down menu as per your requirement.

Set a secure **Pre-shared** key that was used on the VPN of HQ FortiGate.

VPN Creation Wizard

1 VPN Setup > 2 Authentication > 3 Policy & Routing > 4 Review Settings

Remote device	IP Address	Dynamic DNS
Remote IP address	192.168.200.128	
Outgoing Interface	port1	
Authentication method	Pre-shared Key	Signature
Pre-shared key	••••••••	

Site to Site - FortiGate



< Back **Next >** Cancel

In the section of **Policy and Routing** set Local interface to “**LAN**” in my case “**Port2**” is dedicated to the LAN and local subnets will add automatically further then set “**Remote Subnets**” to the HQ (Headquarter) network and set internet access to “**None**” as shown below

VPN Creation Wizard

1 VPN Setup > 2 Authentication > 3 Policy & Routing > 4 Review Settings

Local interface: port2

Local subnets: 192.168.100.0/24

Remote Subnets: 192.168.200.128/24

Internet Access: None

Site to Site - FortiGate

This FortiGate --- Internet --- Remote FortiGate

< Back | Next > | Cancel

The 'Local subnets' and 'Remote Subnets' sections are highlighted with a red box.

The 'Next >' button is highlighted with a red box.

Review the configuration summary that you configured that shows the interfaces, firewall addresses, routes, and policies after verifying it select create icon

VPN Creation Wizard

1 VPN Setup > 2 Authentication > 3 Policy & Routing > 4 Review Settings

i The following settings should be reviewed prior to creating the VPN.

Object Summary	
Phase 1 interface	Branch-to-HQ
Local address group	Branch-to-HQ_local
Remote address group	Branch-to-HQ_remote
Phase 2 interface	Branch-to-HQ
Static route	static
Blackhole route	static
Local to remote policies	vpn_Branch-to-HQ_local
Remote to local policies	vpn_Branch-to-HQ_remote

< Back Create Cancel

After creating the VPN, you can verify the details as shown below.

VPN Creation Wizard

VPN Setup > Authentication > Policy & Routing > Review Settings

The VPN has been set up

Object Summary

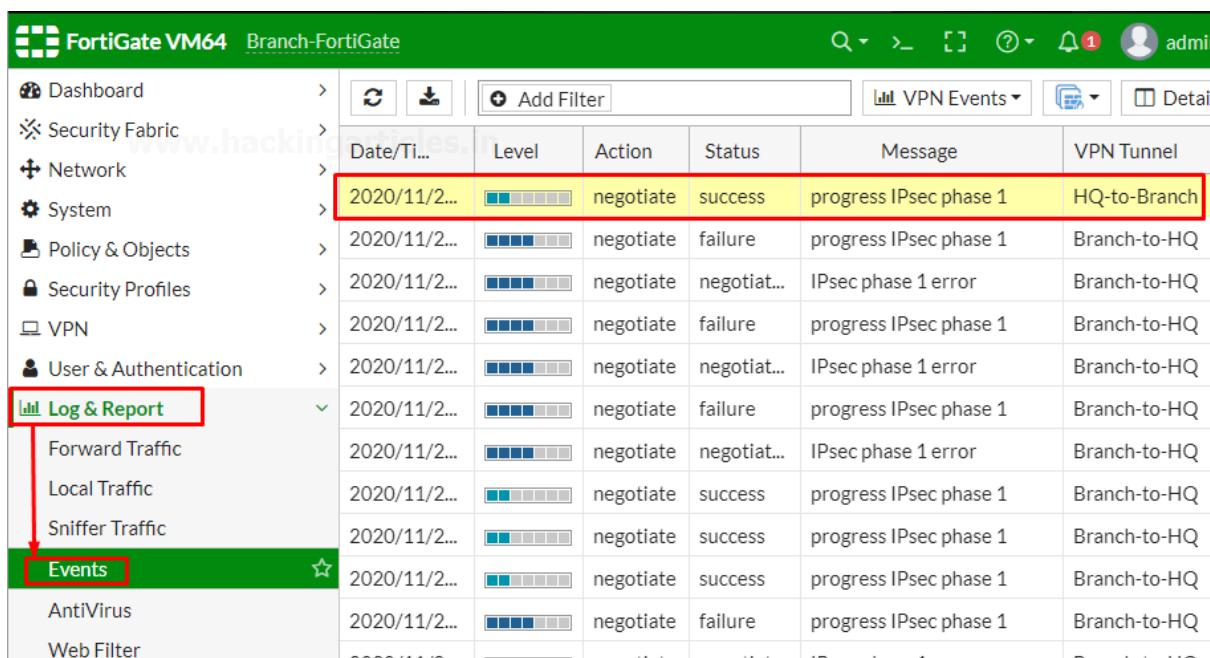
Phase 1 interface	<input checked="" type="checkbox"/> Branch-to-HQ
Local address group	<input checked="" type="checkbox"/> Branch-to-HQ_local Edit
Remote address group	<input checked="" type="checkbox"/> Branch-to-HQ_remote Edit
Phase 2 interface	<input checked="" type="checkbox"/> Branch-to-HQ
Static route	<input checked="" type="checkbox"/> 3 Edit
Blackhole route	<input checked="" type="checkbox"/> 4 Edit
Local to remote policies	<input checked="" type="checkbox"/> vpn_Branch-to-HQ_local_0 (6)
Remote to local policies	<input checked="" type="checkbox"/> vpn_Branch-to-HQ_remote_0 (7)

[Add Another](#) [Show Tunnel List](#)

You can also verify it by users of the Headquarter (HQ) can access resources on the Branch internal network and so on Vice Versa.

To test the connection, ping HQ LAN interface from the device Branch Internal network.

Or you Can also check the LOG events of VPN by going to Log & Report > Events > VPN Events and where you can see every Single logs of VPN.



The screenshot shows the FortiGate VM64 Branch-FortiGate interface. The left sidebar has several tabs: Dashboard, Security Fabric, Network, System, Policy & Objects, Security Profiles, VPN, User & Authentication, Log & Report, Forward Traffic, Local Traffic, Sniffer Traffic, and Events. The 'Events' tab is highlighted with a red box and a red arrow points to it from the left sidebar. The main area is a table with columns: Date/Ti..., Level, Action, Status, Message, and VPN Tunnel. The first row in the table is also highlighted with a red box.

Date/Ti...	Level	Action	Status	Message	VPN Tunnel
2020/11/2...	[progress bar]	negotiate	success	progress IPsec phase 1	HQ-to-Branch
2020/11/2...	[progress bar]	negotiate	failure	progress IPsec phase 1	Branch-to-HQ
2020/11/2...	[progress bar]	negotiate	negotiat...	IPsec phase 1 error	Branch-to-HQ
2020/11/2...	[progress bar]	negotiate	failure	progress IPsec phase 1	Branch-to-HQ
2020/11/2...	[progress bar]	negotiate	negotiat...	IPsec phase 1 error	Branch-to-HQ
2020/11/2...	[progress bar]	negotiate	failure	progress IPsec phase 1	Branch-to-HQ
2020/11/2...	[progress bar]	negotiate	negotiat...	IPsec phase 1 error	Branch-to-HQ
2020/11/2...	[progress bar]	negotiate	failure	progress IPsec phase 1	Branch-to-HQ
2020/11/2...	[progress bar]	negotiate	negotiat...	IPsec phase 1 error	Branch-to-HQ
2020/11/2...	[progress bar]	negotiate	success	progress IPsec phase 1	Branch-to-HQ
2020/11/2...	[progress bar]	negotiate	success	progress IPsec phase 1	Branch-to-HQ
2020/11/2...	[progress bar]	negotiate	success	progress IPsec phase 1	Branch-to-HQ
2020/11/2...	[progress bar]	negotiate	success	progress IPsec phase 1	Branch-to-HQ
2020/11/2...	[progress bar]	negotiate	failure	progress IPsec phase 1	Branch-to-HQ

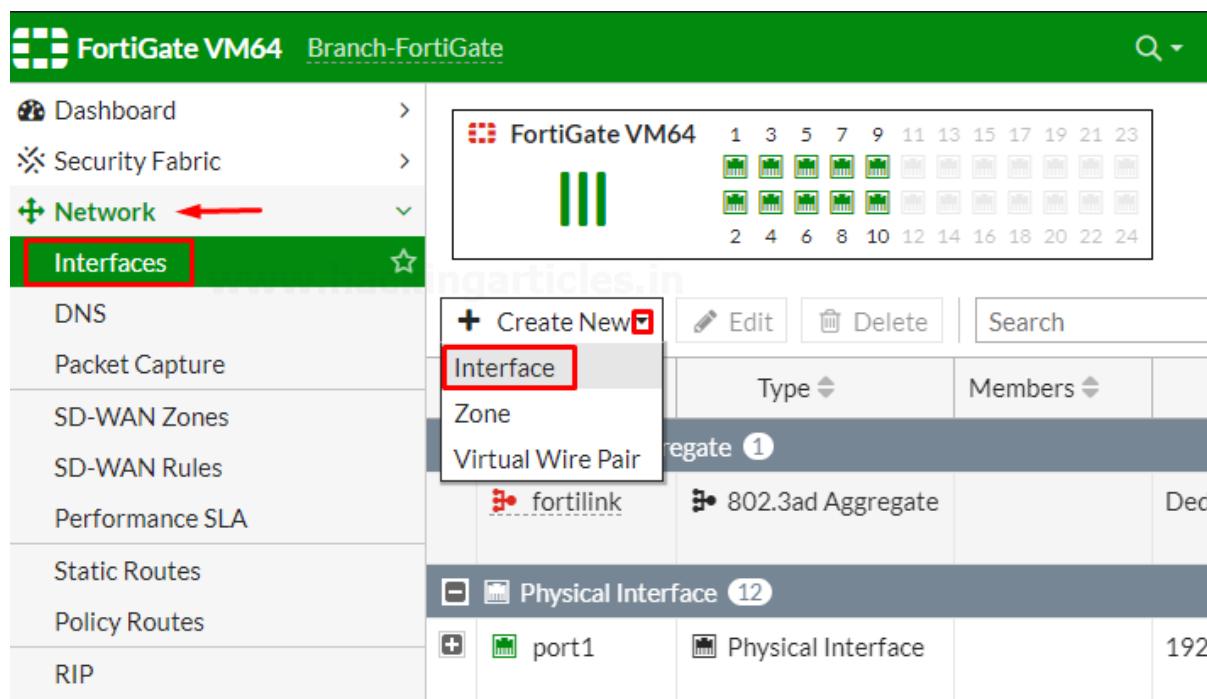
Simplifying Policies with Zone

In this Part, we're Going to Explain how to group multiple interfaces into Zone to simplify Firewall Policies.

By creating multiple VLANs we are going to add them into a zone, so that we can just use the single zone object as a source interface in our firewall policy, rather than having to reference each interface separately.

Create VLAN Interfaces

Go to Network > interfaces and create a new interface



The screenshot shows the FortiGate VM64 interface configuration screen. The left sidebar has a red arrow pointing to the 'Network' section, and the 'Interfaces' option is highlighted with a red box. The main panel displays a grid of 24 ports, with port 1 highlighted. A context menu is open over port 1, with 'Interface' selected. The menu also includes options for 'Zone' and 'Virtual Wire Pair'. Below the menu, there are buttons for 'Create New' (with a checked checkbox), 'Edit', 'Delete', and 'Search'. The table below shows one entry: 'Aggregate 1' (Type: 802.3ad Aggregate, Members: fortiflink). Another row for 'Physical Interface 12' is partially visible. At the bottom, there are buttons for '+', 'port1', and 'Physical Interface'.

Enter the name for the interface VLAN10 or whatever you want, select the type to VLAN, select Interface to LAN, enter the VLAN ID, enter the VRF Id. assign the Role to LAN, set the Addressing mode to manual, enter the IP/Netmask provided by your ISP and select the Administrative Access to HTTPS, PING

New Interface

Name	VLAN10
Alias	
Type	VLAN
Interface	LAN (port4)
VLAN ID	10
VRF ID	10
Role	LAN

Address

Addressing mode	Manual <input type="radio"/> DHCP <input type="radio"/> Auto-managed
IP/Netmask	192.168.10.2/24 
Create address object matching subnet	<input checked="" type="checkbox"/>
Name	<input type="text"/> VLAN10 address
Destination	192.168.10.2/24
Secondary IP address	<input type="checkbox"/>

Administrative Access

IPv4	<input checked="" type="checkbox"/> HTTPS	<input checked="" type="checkbox"/> PING	<input type="checkbox"/> FMG-Access
	<input type="checkbox"/> SSH	<input type="checkbox"/> SNMP	<input type="checkbox"/> FTM
	<input type="checkbox"/> RADIUS Accounting	<input type="checkbox"/> Security Fabric Connection 	

Enable the DHCP server and assign the address range further then save the configuration.



DHCP Server

Address range

Netmask

Default gateway

DNS server

Lease time second(s)

Advanced

Network

Device detection

Security mode

Traffic Shaping

Outbound shaping profile

Miscellaneous

Comments 0/255

Status

Next, create another by making the same selections...

Go to Network > interfaces and create a new interface.

Enter the name for the interface VLAN20 or whatever you want, select the type to VLAN, select Interface to LAN, enter the VLAN ID, enter the VRF Id. assign the Role to LAN, set the Addressing mode to manual, enter the IP/Netmask provided by your ISP and select the Administrative Access to HTTPS, PING

New Interface

Name	VLAN20
Alias	
Type	VLAN
Interface	LAN (port4)
VLAN ID	20
VRF ID	10
Role	LAN

Address

Addressing mode	Manual <input type="radio"/> DHCP <input type="radio"/> Auto-managed
IP/Netmask	<input type="text" value="192.168.20.1/24"/>
Create address object matching subnet	<input checked="" type="checkbox"/>
Name	<input type="text" value="VLAN20 address"/>
Destination	192.168.20.1/24
Secondary IP address	<input type="checkbox"/>

Administrative Access

IPv4	<input checked="" type="checkbox"/> HTTPS <input checked="" type="checkbox"/> PING <input type="checkbox"/> SSH <input type="checkbox"/> SNMP	<input type="checkbox"/> FMG-Access <input type="checkbox"/> FTM
------	--	---

Enable the DHCP server and assign the address range further then save the configuration.

DHCP Server

Address range	192.168.20.2-192.168.20.254
Netmask	255.255.255.0
Default gateway	Same as Interface IP <input type="button" value="Specify"/>
DNS server	Same as System DNS <input type="button" value="Specify"/> Same as Interface IP <input type="button" value="Specify"/>
Lease time <small>i</small> <input checked="" type="checkbox"/>	604800 second(s)

Advanced

Network

Device detection <small>i</small> <input checked="" type="checkbox"/>
Security mode <input type="checkbox"/>

Traffic Shaping

Outbound shaping profile <input type="checkbox"/>

Miscellaneous

Comments	0/255
Status	<input checked="" type="button" value="Enabled"/> <input type="button" value="Disabled"/>

OK **Cancel**

Finally, **create a 3rd VLAN** by making the same selection

Go to Network > interfaces and create a new interface.

Enter the name for the interface VLAN30 or whatever you want, select the type to VLAN, select Interface to LAN, enter the VLAN ID, enter the VRF Id. assign the Role to LAN, set the Addressing mode to manual, enter the IP/Netmask provided by your ISP and select the Administrative Access to HTTPS, PING

New Interface

Name	VLAN30
Alias	
Type	VLAN
Interface	LAN (port4)
VLAN ID	30
VRF ID	10
Role	LAN

Address

Addressing mode	Manual <input type="radio"/> DHCP <input type="radio"/> Auto-managed
IP/Netmask	192.168.30.1/24
Create address object matching subnet	<input checked="" type="checkbox"/>
Name	<input type="text"/> VLAN30 address
Destination	192.168.30.1/24
Secondary IP address	<input type="checkbox"/>

Administrative Access

IPv4	<input checked="" type="checkbox"/> HTTPS	<input checked="" type="checkbox"/> PING	<input type="checkbox"/> FMG-Access
	<input type="checkbox"/> SSH	<input type="checkbox"/> SNMP	<input type="checkbox"/> FTM

Enable the DHCP server and assign the address range further then save the configuration.

DHCP Server

Address range

Netmask

Default gateway Same as Interface IP Specify

DNS server Same as System DNS Same as Interface IP Specify

Lease time 604800 second(s)

Advanced

Network

Device detection

Security mode

Traffic Shaping

Outbound shaping profile

Miscellaneous

Comments 0/255

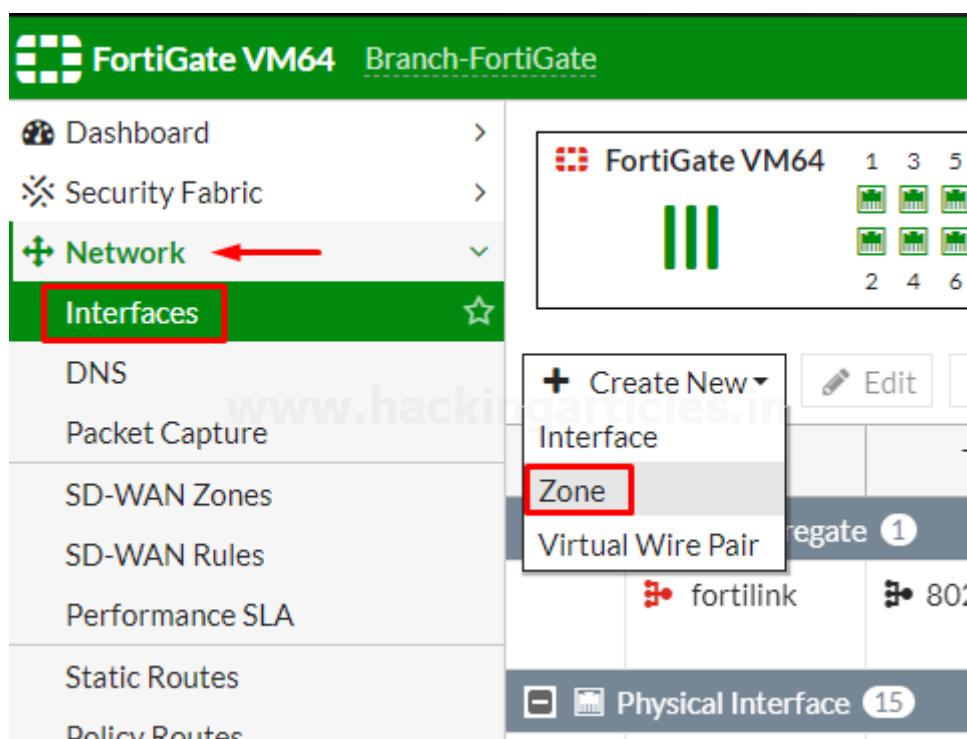
Status Enabled Disabled

Review the Interface list to see the VLAN's that you have created

802.3ad Aggregate 1				
	fortilink	802.3ad Aggregate	Dedicated to FortiSwitch	PING Security
Physical Interface 15				
	LAN (port4)	Physical Interface	192.168.255.100/255.2...	PING HTTPS SSH SNMP +3
•	VLAN10	VLAN	192.168.10.2/255.255.2...	PING HTTPS
•	VLAN20	VLAN	192.168.20.1/255.255.2...	PING HTTPS
•	VLAN30	VLAN	192.168.30.1/255.255.2...	PING HTTPS

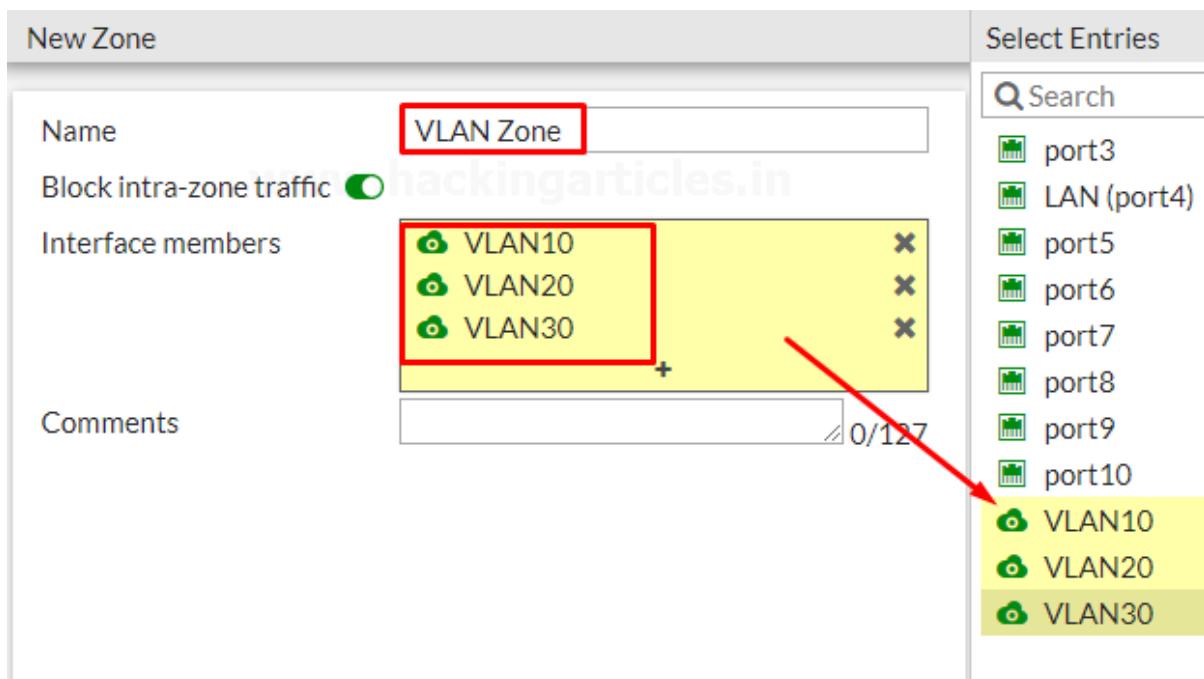
Create an Interface Zone

GO to the Network > Interfaces and select **create new Zone**



The screenshot shows the FortiGate VM64 interface. The main menu bar at the top has 'Branch-FortiGate'. Below it, the left sidebar menu includes 'Dashboard', 'Security Fabric', 'Network' (with a red arrow pointing to it), and 'Interfaces' (which is highlighted with a red box). The 'Interfaces' menu has sub-options: 'DNS', 'Packet Capture', 'SD-WAN Zones', 'SD-WAN Rules', 'Performance SLA', 'Static Routes', and 'Policy Routes'. To the right of the sidebar, there's a summary box for 'FortiGate VM64' showing ports 1, 3, 5, 2, 4, 6. Below this, a context menu is open over an interface entry, with options: '+ Create New', 'Edit', 'Interface' (highlighted with a red box), 'Zone' (also highlighted with a red box), and 'Virtual Wire Pair'. At the bottom of the interface list, there's a summary: 'Physical Interface 15'.

Name the zone to “**VLAN Zone**” to make it identifiable and add the newly created VLAN’s to it as shown below.



New Zone

Name	<input type="text" value="VLAN Zone"/>
Block intra-zone traffic	<input checked="" type="checkbox"/>
Interface members	<input checked="" type="checkbox"/> VLAN10 <input checked="" type="checkbox"/> VLAN20 <input checked="" type="checkbox"/> VLAN30
Comments	<input type="text" value="0/127"/>

Select Entries

- Search
- port3
- LAN (port4)
- port5
- port6
- port7
- port8
- port9
- port10
- VLAN10
- VLAN20
- VLAN30

Review the Zone list to see the VLAN’s that you have Added.

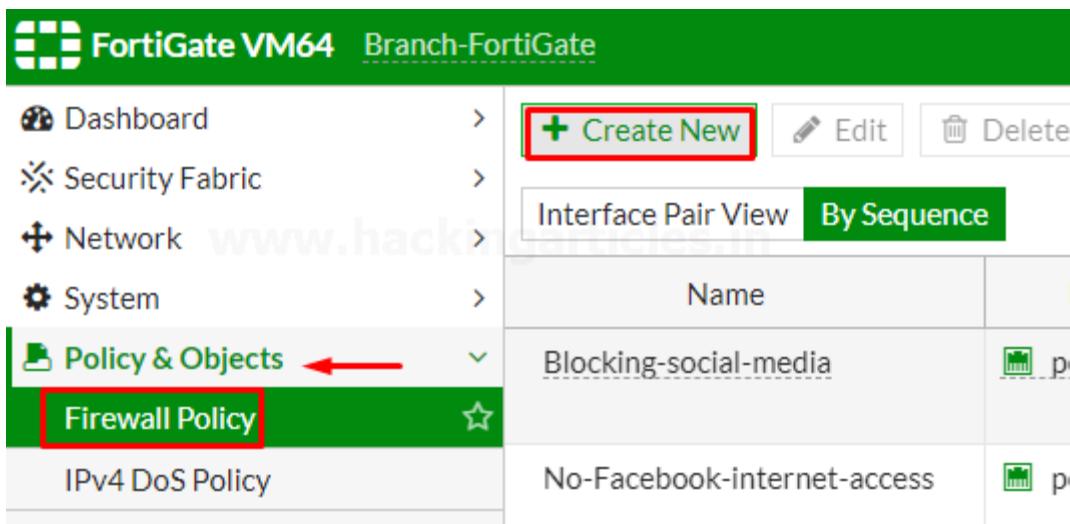


Zone 1

	<input type="checkbox"/> VLAN Zone	<input type="checkbox"/> Zone	Interface members	Address	Speed
			<input checked="" type="checkbox"/> VLAN10 <input checked="" type="checkbox"/> VLAN20 <input checked="" type="checkbox"/> VLAN30	0.0.0.0/0.0.0.0	100

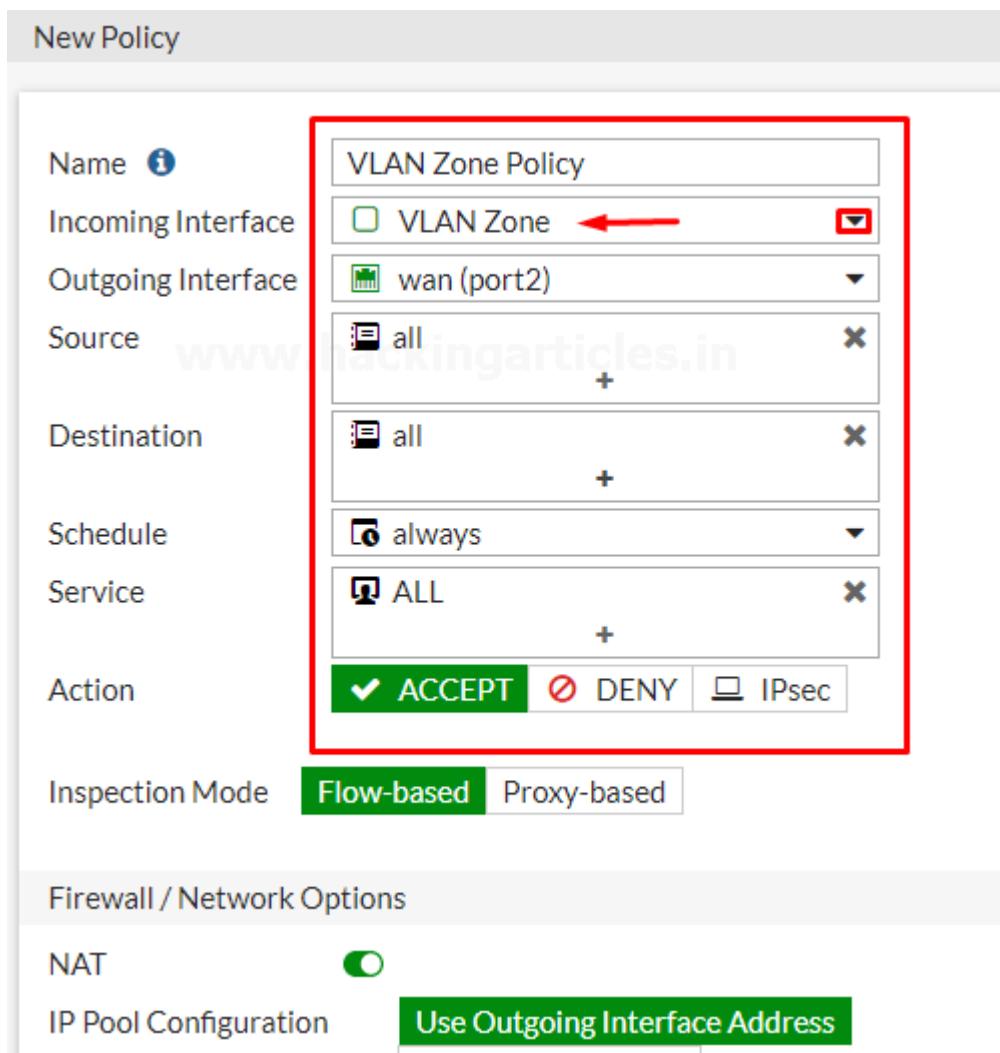
Create a Zone Firewall Policy

Go to Policy & Objects > Firewall Policy and create a new policy that will allow any VLAN in the Zone that we have created to access the internet.



The screenshot shows the FortiGate VM64 interface with the title "Branch-FortiGate". The left sidebar has a green header "Policy & Objects" with a red arrow pointing to it, and "Firewall Policy" is selected with a red box around it. The main area shows a table with two rows: "Blocking-social-media" and "No-Facebook-internet-access". At the top right, there are buttons for "Create New" (red box), "Edit", and "Delete". Below the table are tabs "Interface Pair View" and "By Sequence".

Assign a name to “VLAN Zone Policy” make it identifiable, set the **Incoming interface to your Zone** and the **outgoing interface to the internet-facing interface**. configure the rest as needed or as per your requirement.



The screenshot shows the "New Policy" configuration window. The "Name" field is set to "VLAN Zone Policy". The "Incoming Interface" dropdown is set to "wan (port2)". The "Source" section contains two "all" entries. The "Destination" section contains "always" and "ALL". The "Action" section has three buttons: "ACCEPT" (checked), "DENY", and "IPsec". The "Inspection Mode" is set to "Flow-based". Under "Firewall / Network Options", "NAT" is enabled and "IP Pool Configuration" is set to "Use Outgoing Interface Address". A red box highlights the "VLAN Zone Policy" name and the "wan (port2)" interface selection.

Select the Security Profiles as per your requirements and save the configuration by selecting OK.

Security Profiles

AntiVirus	<input checked="" type="checkbox"/> AV default	
Web Filter	<input checked="" type="checkbox"/> WEB default	
DNS Filter	<input type="checkbox"/>	
Application Control	<input type="checkbox"/>	
IPS	<input type="checkbox"/>	
File Filter	<input type="checkbox"/>	
SSL Inspection	SSL certificate-inspection	

Logging Options

Log Allowed Traffic	<input checked="" type="radio"/> Security Events	All Sessions
Generate Logs when Session Starts	<input type="radio"/>	
Capture Packets	<input type="radio"/>	

Comments 0/1023

Enable this policy

To make this Policy Effective move this Policy to the TOP of the List as per your environment which policy should be on Top.



Interface Pair View **By Sequence**

Name	From	To	Source	Dest
Blocking-social-media	port1	wan (port2)	all	all
No-Facebook-internet-access	port1	wan (port2)	all	all
internet access	port1	port1	all	all
mobile	port1	wan (port2)	FABRIC_DEVICE	all
VLAN Zone Policy	VLAN Zone	wan (port2)	all	all
vpn_HQ-to-Branch_local_0⚠	port1	HQ-to-Branch	HQ-to-Branch_local	HQ-to-Branch_local
vpn_HQ-to-Branch_remote_0⚠	HQ-to-Branch	port1	HQ-to-Branch_remote	HQ-to-Branch_remote
vpn_Branch-to-HQ_local_0⚠	wan (port2)	Branch-to-HQ	Branch-to-HQ_local	Branch-to-HQ_local
vpn_Branch-to-HQ_remote_0⚠	Branch-to-HQ	wan (port2)	Branch-to-HQ_remote	Branch-to-HQ_remote
Implicit Deny	any	any	all	all

Similarly, you can create as much policy as you want.

Conclusion

Hence, one can make use of these commands as a cybersecurity professional to assess vulnerabilities on systems and keep these systems away from threat.

References

- <https://www.hackingarticles.in/firewall-lab-setup-fortigate/>
- <https://www.hackingarticles.in/implementation-of-firewall-policies-fortigate-part-1/>
- <https://www.hackingarticles.in/implementation-of-firewall-policies-fortigate-part-2/>
- <https://support.fortinet.com/Download/VMImages.aspx>
- <http://docs.fortinet.com/document/fortigate/6.2.4/cookbook/856100/dashboard>
- <http://geekflare.com/firewall-introduction/>