Fortigate

Firewall Config & Rules

Original Author: *Vijay*

Table of Contents

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

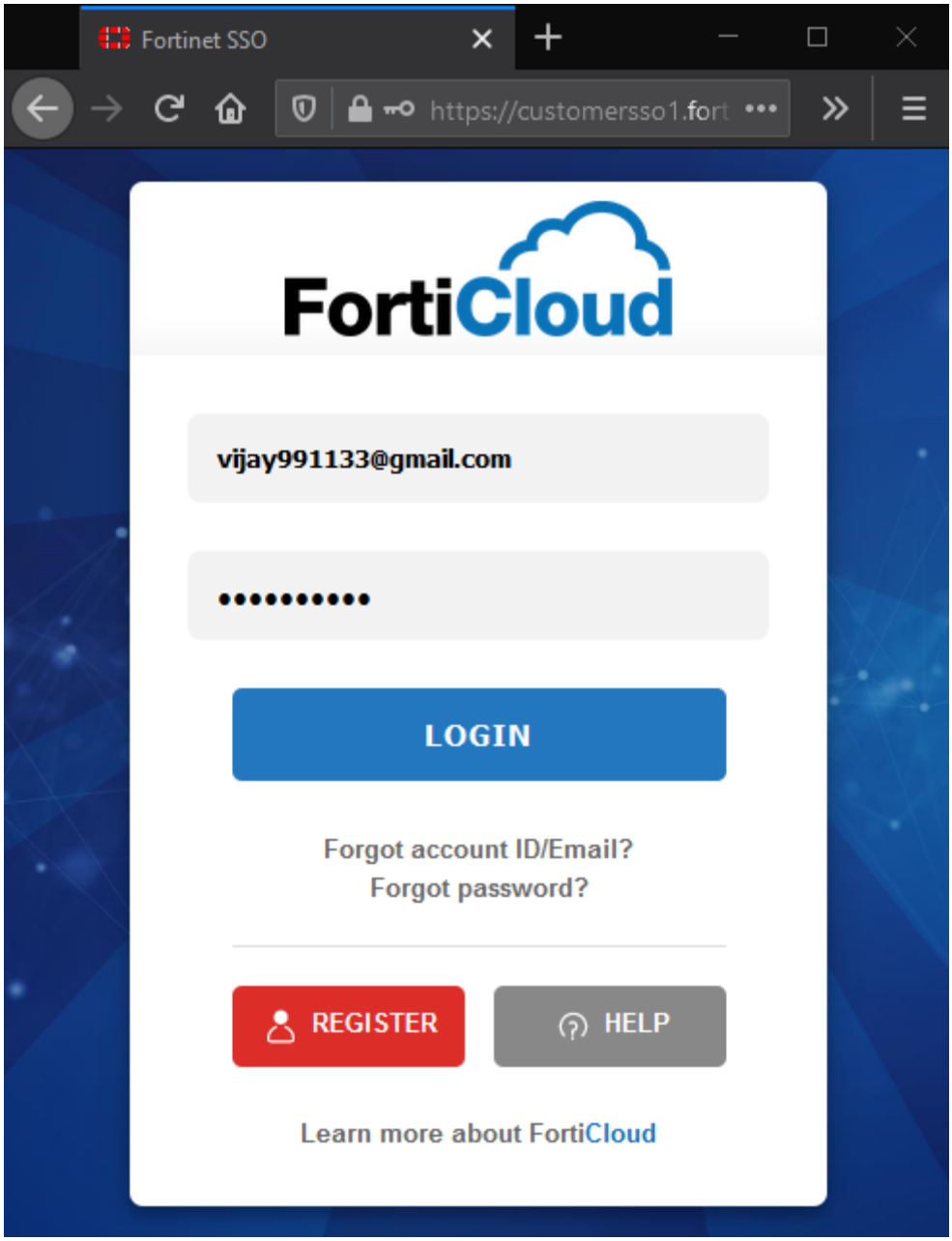
In the computing language, a firewall is a security software or hardware that can monitor and control network traffic, both incoming and outgoing. It establishes a kind of barrier between reliable internal and unknown external networks.

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

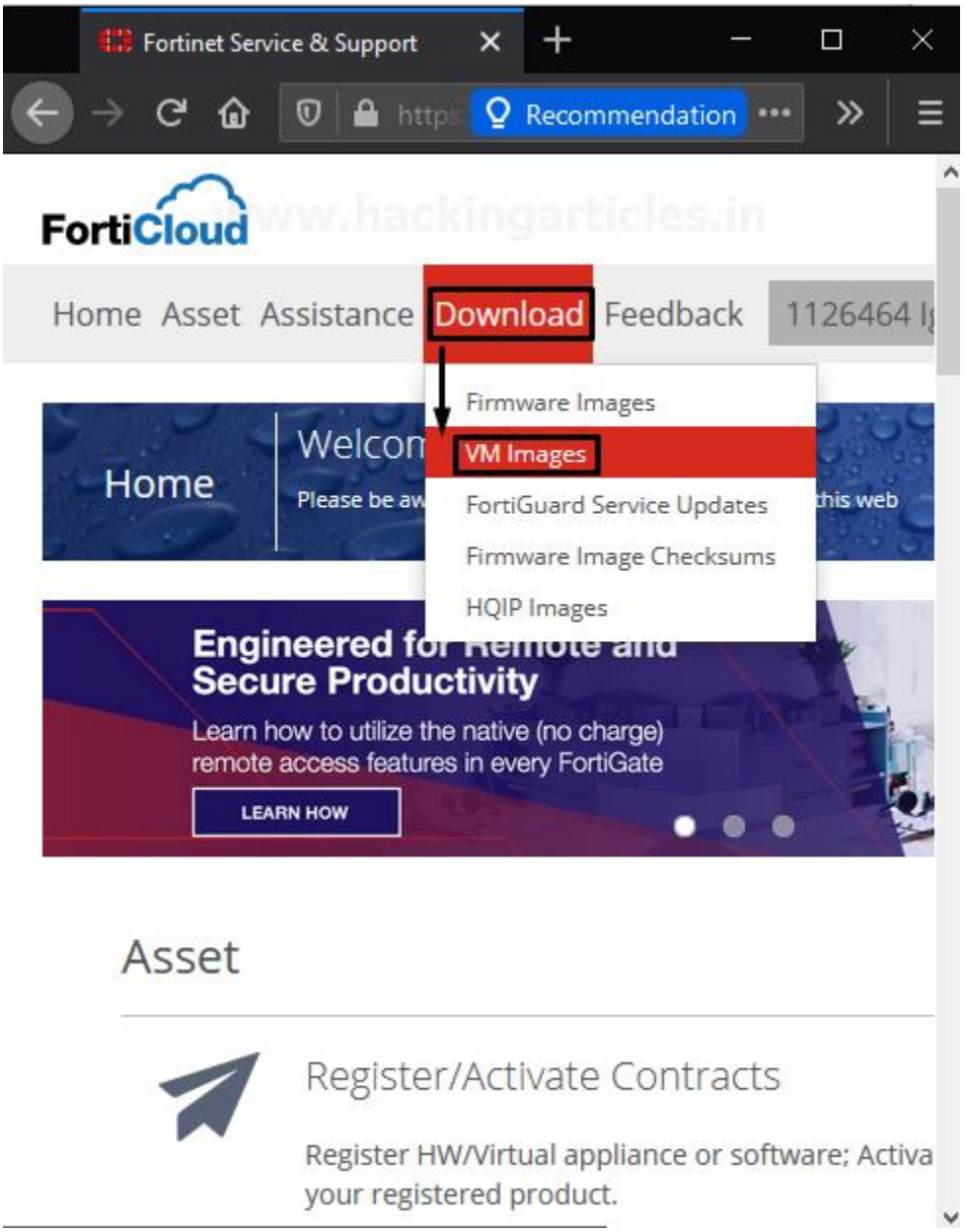
A network firewall is based on security rules to **accept**, **reject**, or **drop** specific traffic. The firewall aims to allow or deny the connection or request, depending on implemented rules.

Download FortiGate Virtual firewall

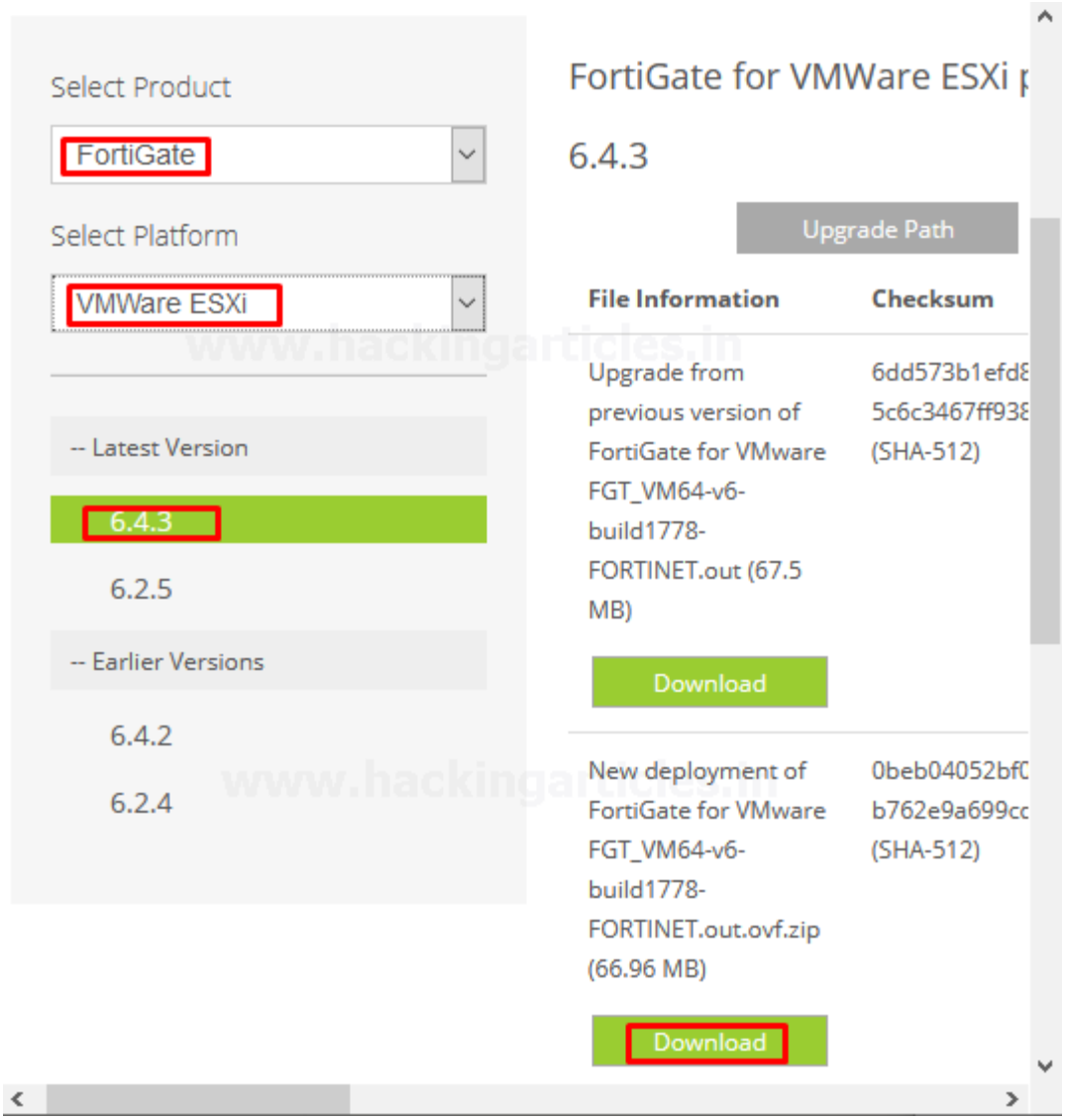
First, we need to download the virtual FortiGate Firewall from the official FortiGate portal.



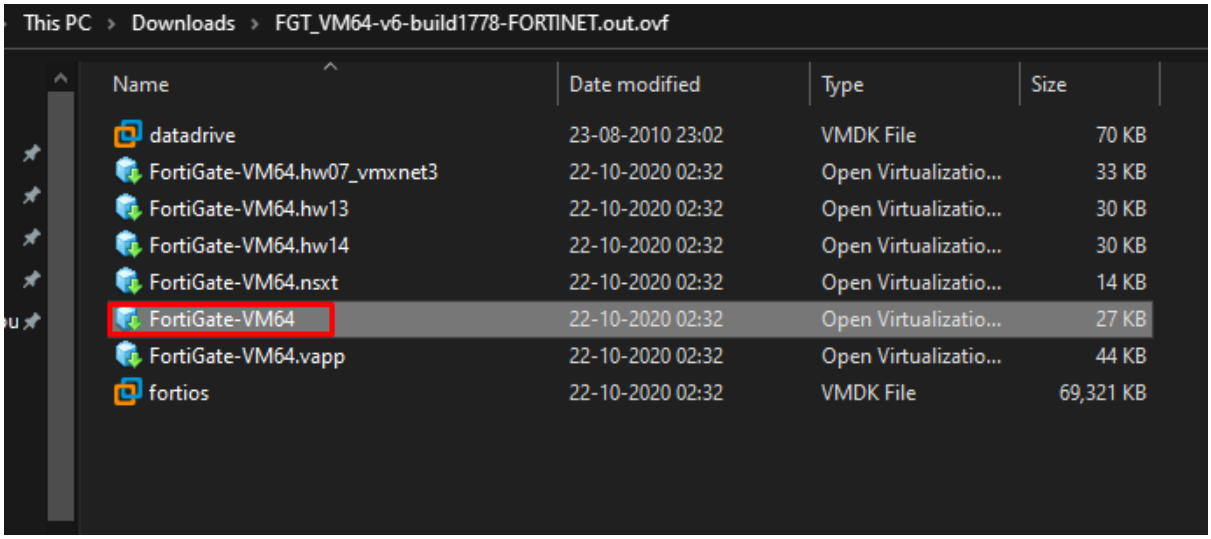
By creating an account or log in to the account go to **Download** > **VM Images** as shown in the image below.



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.



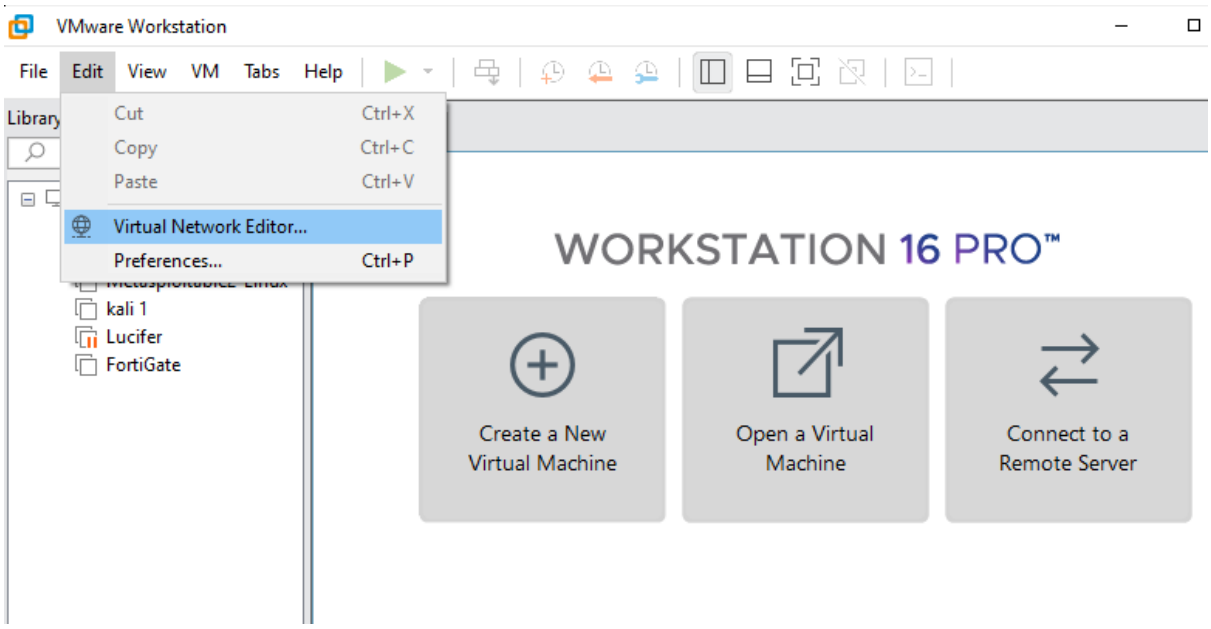
After downloading the compressed FortiGate VM file you need to extract the compressed Zip file by using your favourite extractor and the extracted Zip file similarly looks like the below image.



Configure Virtual network interfaces

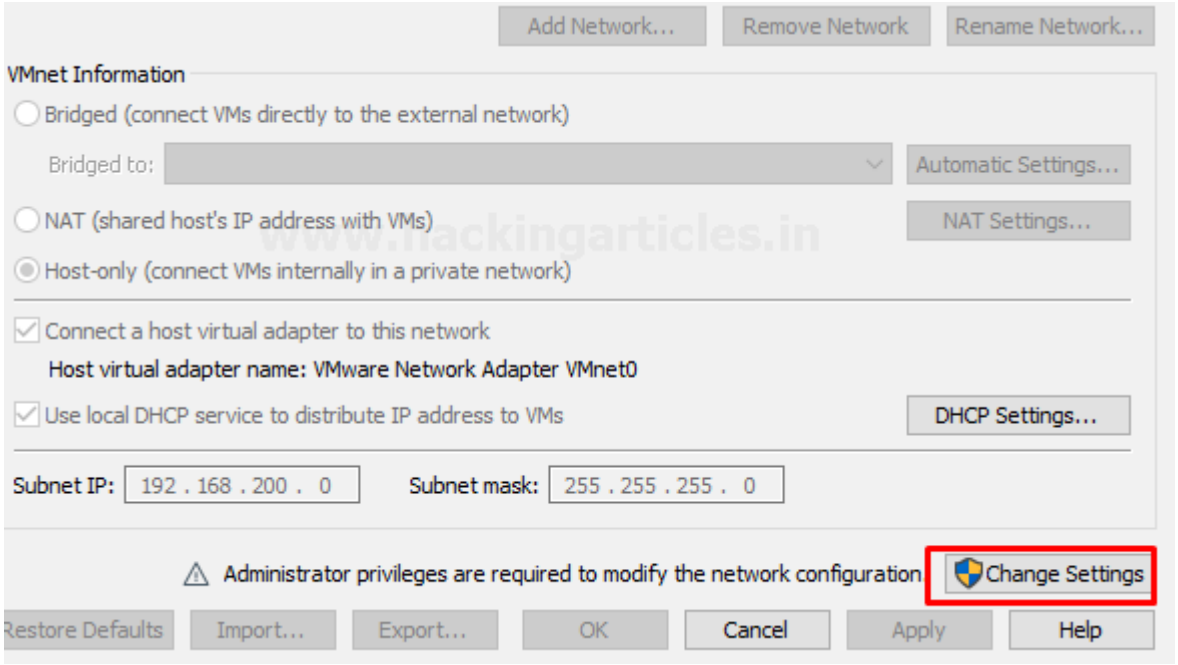
Let's configure Virtual Network Adaptors as per your requirements.

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



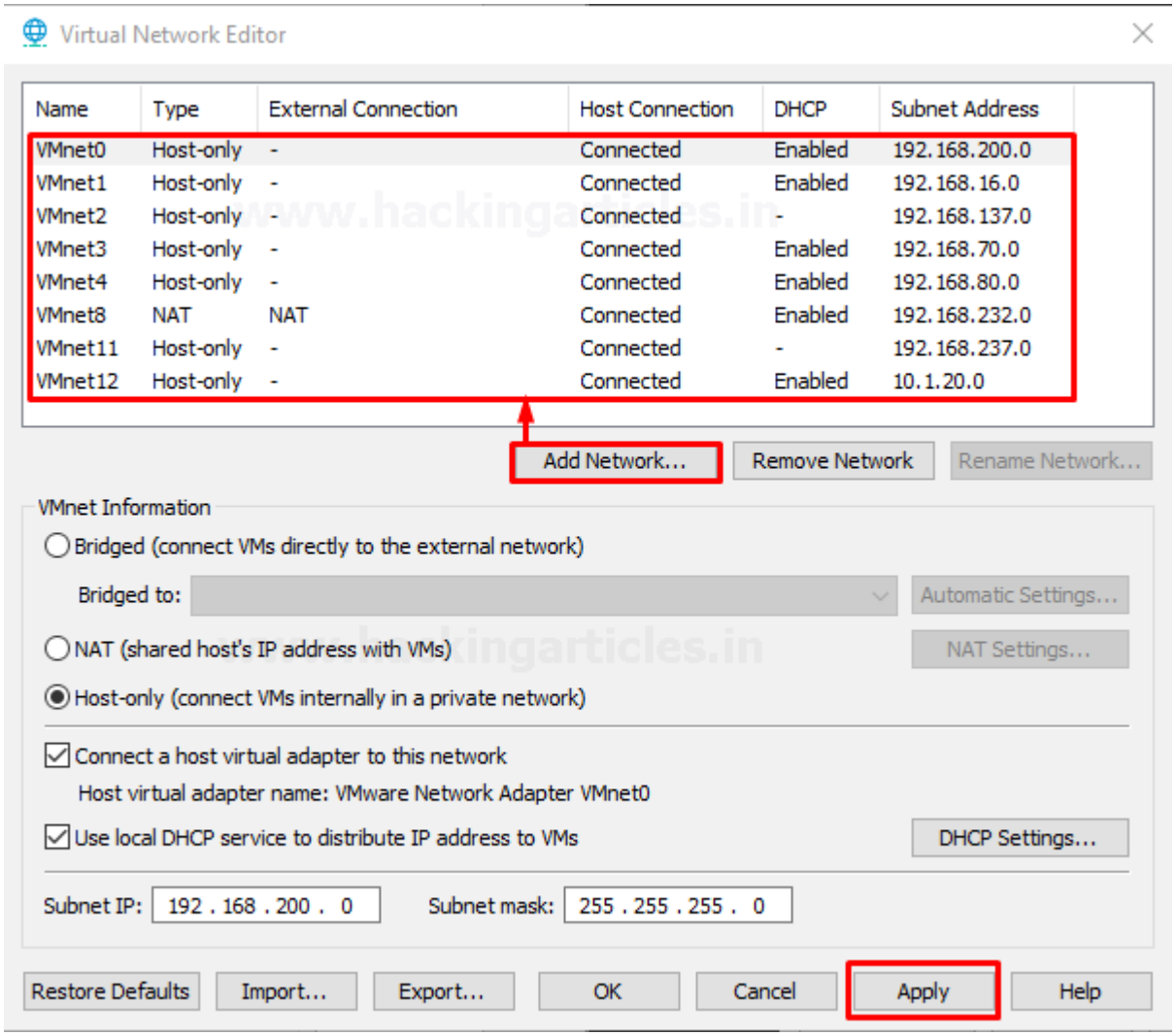
Or also you can directly access the Virtual network editor app by click on Windows Start Button and search for Virtual Network Editor. If you are using Linux (i.e. Ubuntu) you can type the below command to open Virtual Network Editor.

```
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.

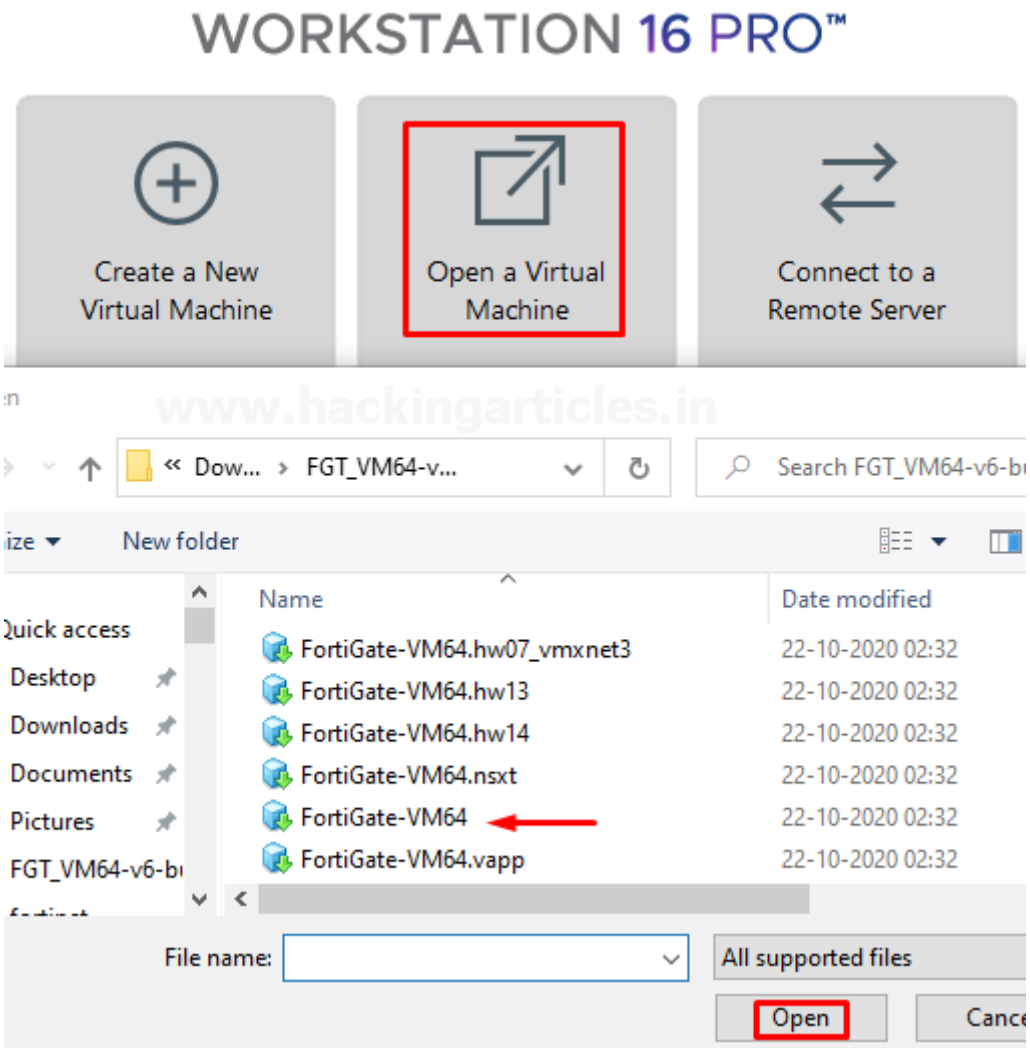
For example, I am going to use 192.168.200.0/24 for the vmnet0 interface and so on…

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 you system requirement

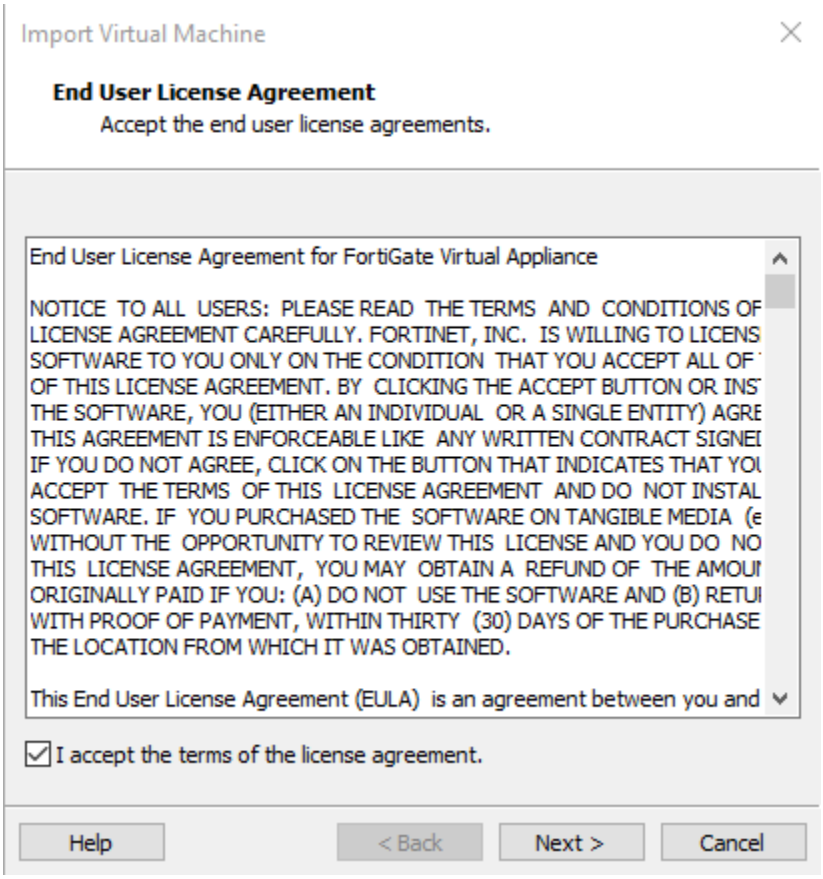


Deployment of FortiGate VM image in VMWare

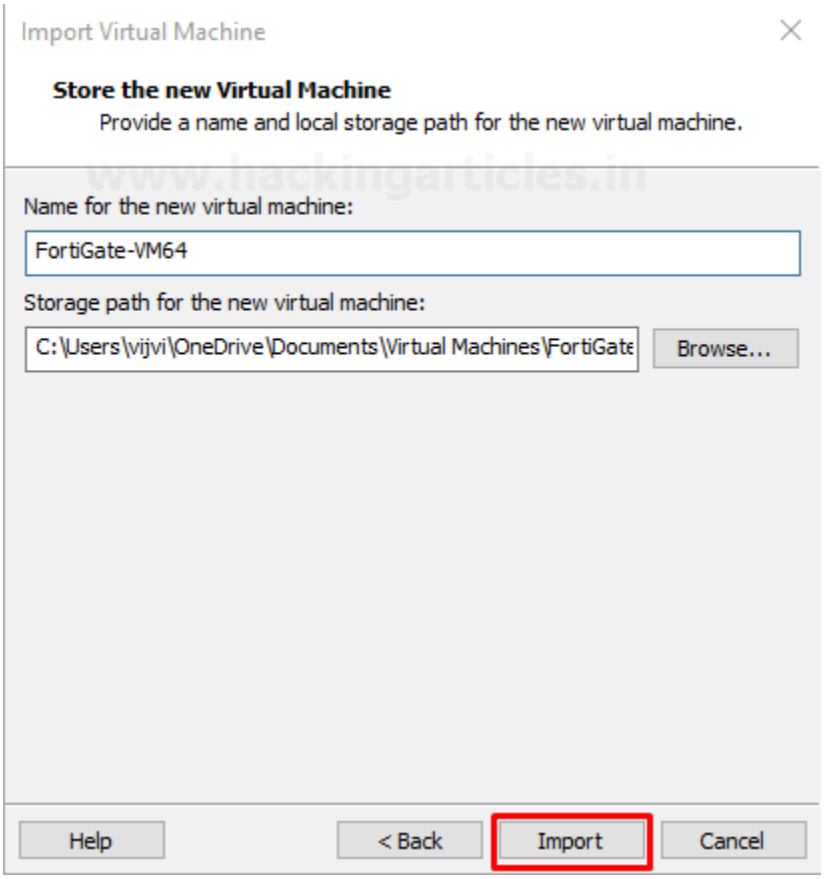
Now it's time to deploy the FortiGate virtual firewall in VMWare Workstation. Just open the VMWare Workstation and go to **Files** >> **Open** (Ctrl+O) or go to the Home tab and select open a virtual Machine. Select the FortiGate-VM64.ovf file that you have downloaded from the official Website of FortiGate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



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

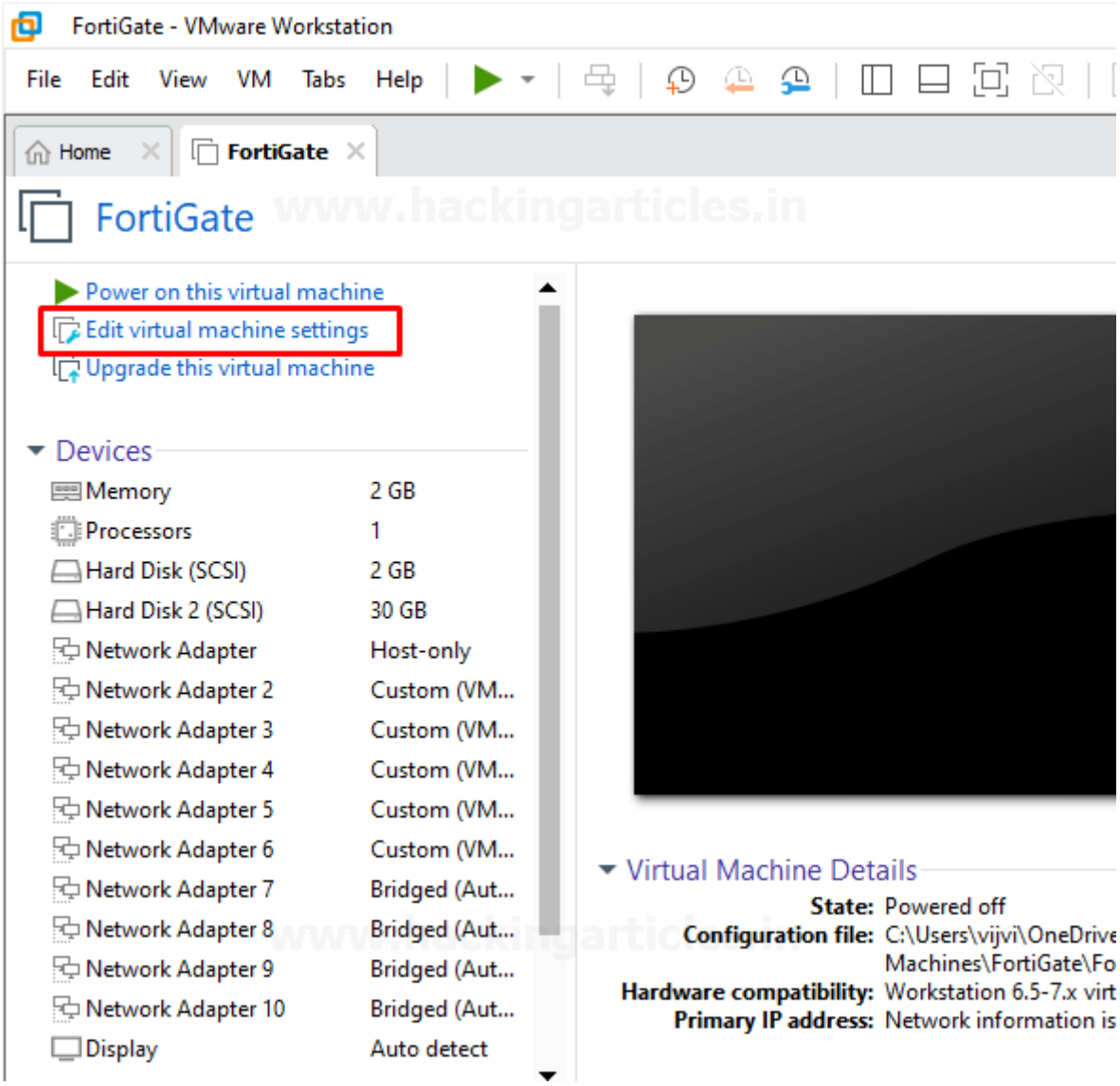


On the next prompt Assign a Name for the new Virtual machine and a Storage Path then after select import as shown below

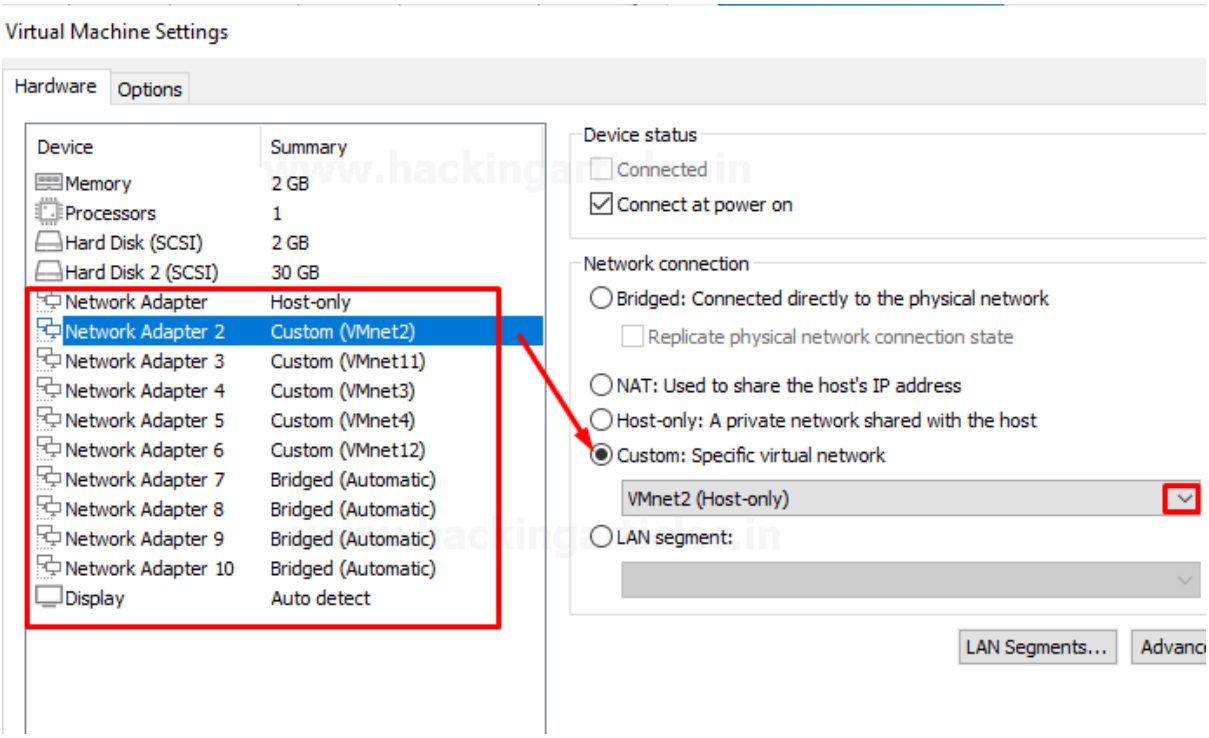


This process going to take some time, so have *patience*. After the successful completion of this process,

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.



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 FGVMEV9T3VJPII0A

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
```

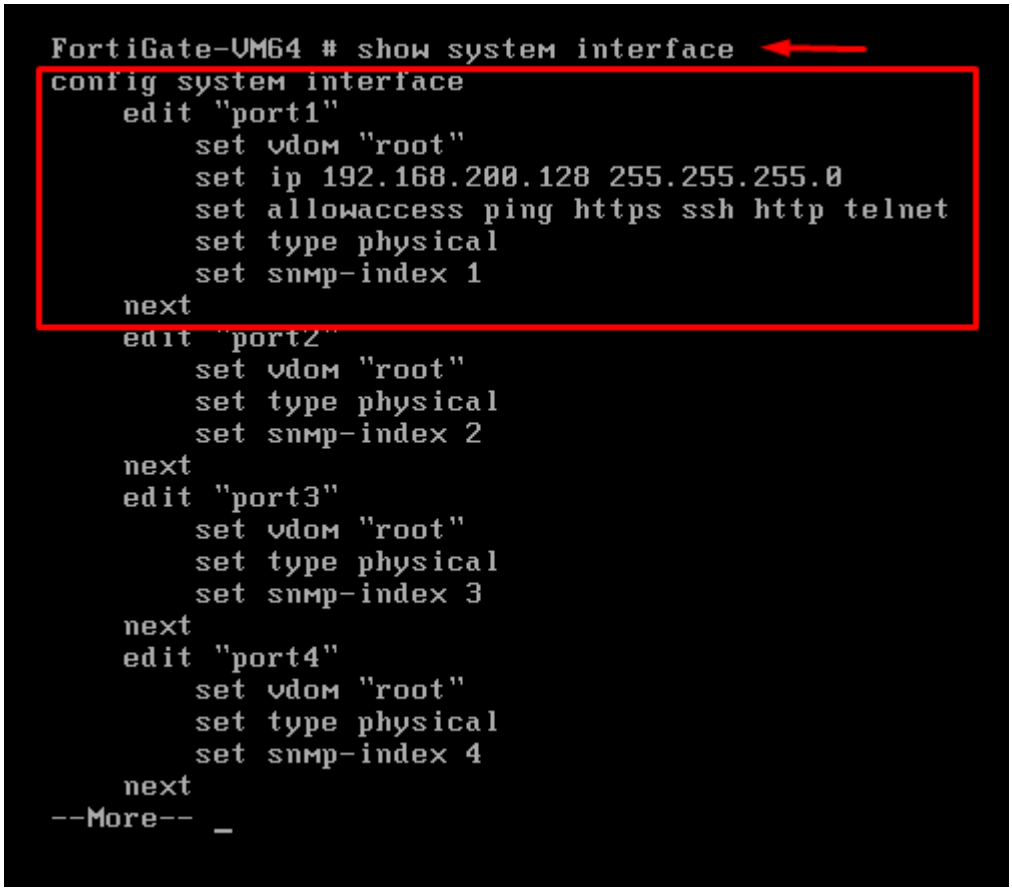
```
FortiGate-VM64 # show system interface
name    Name.
fortilink   static   0.0.0.0 0.0.0.0  169.254.1.1 255.255.255.0  up   disable
aggregate  enable
port1   dhcp   0.0.0.0 0.0.0.0  192.168.200.128 255.255.255.0  up   disable   ph
ysical  enable
port2   static   0.0.0.0 0.0.0.0  0.0.0.0 0.0.0.0  up   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
```

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

```
show system interface
```



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-VM64 # 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-VM64 #
```

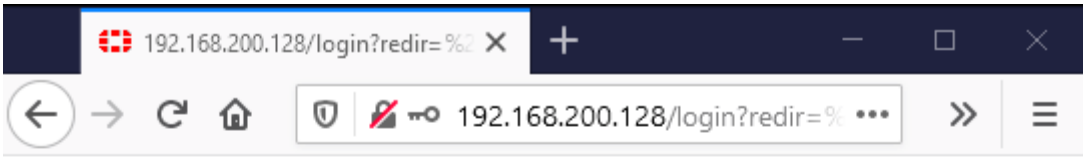
As we can see the IP Address is reachable which means it is working properly now, we will access the FortiGate Firewall GUI using its management interface IP address.

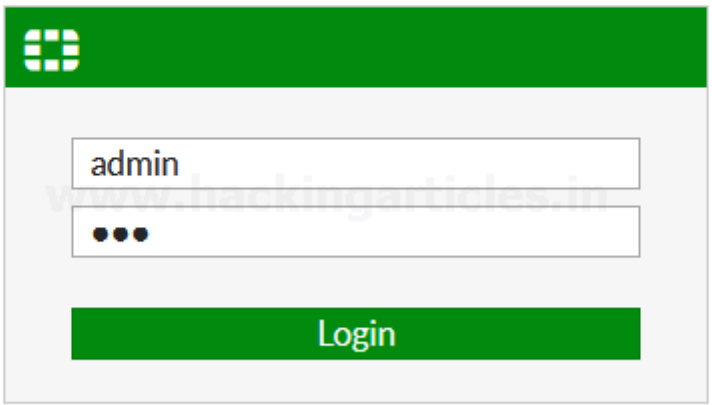
https://192.168.200.128

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

Username: – admin

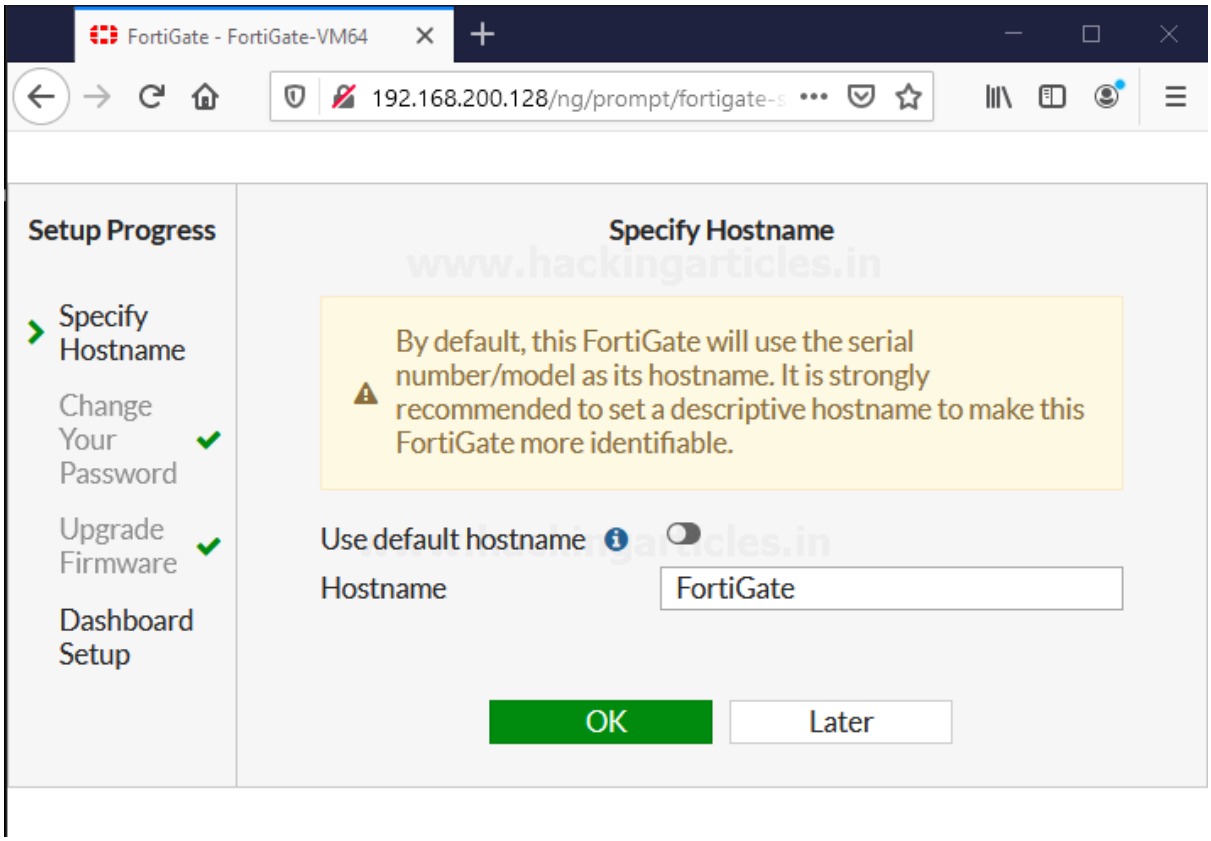
Password: – 123



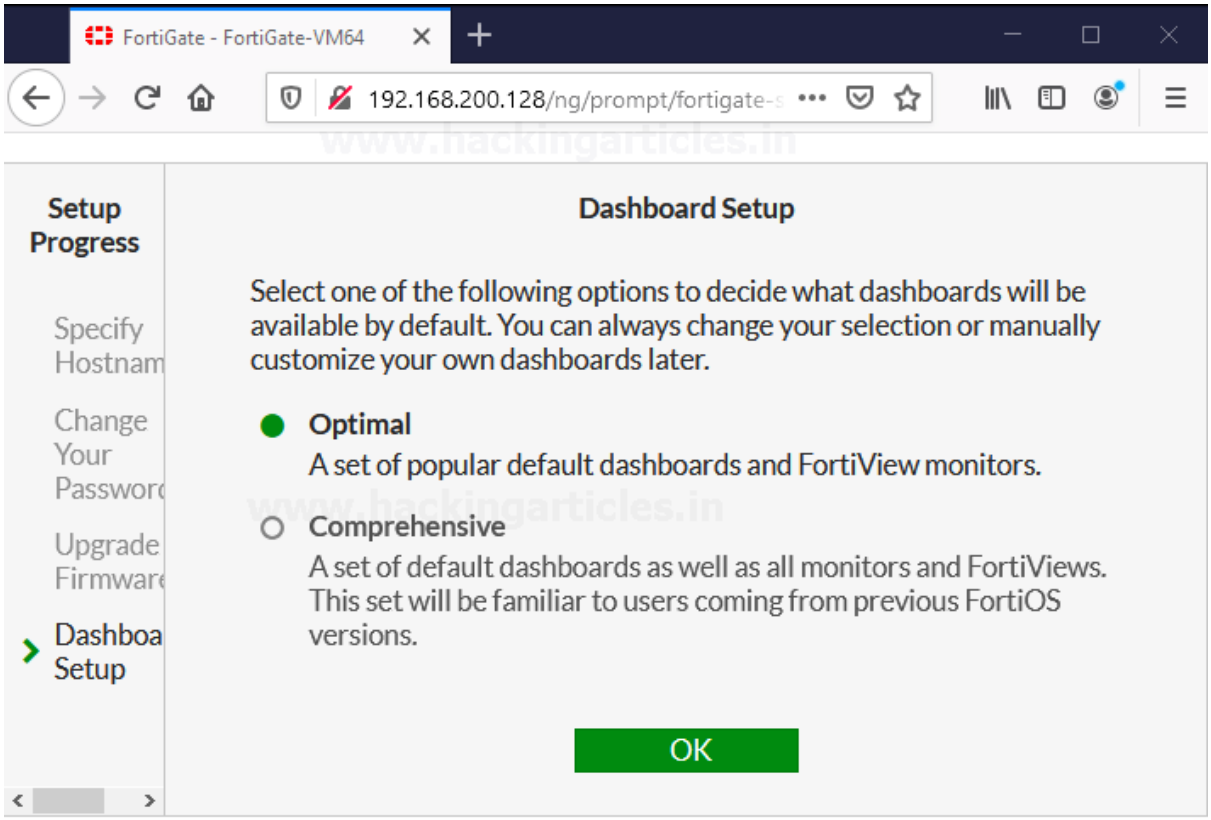


By logging in to the firewall it will open a setup Prompt where we need to specify the Hostname, change password upgrade firmware, and Dashboard setup

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



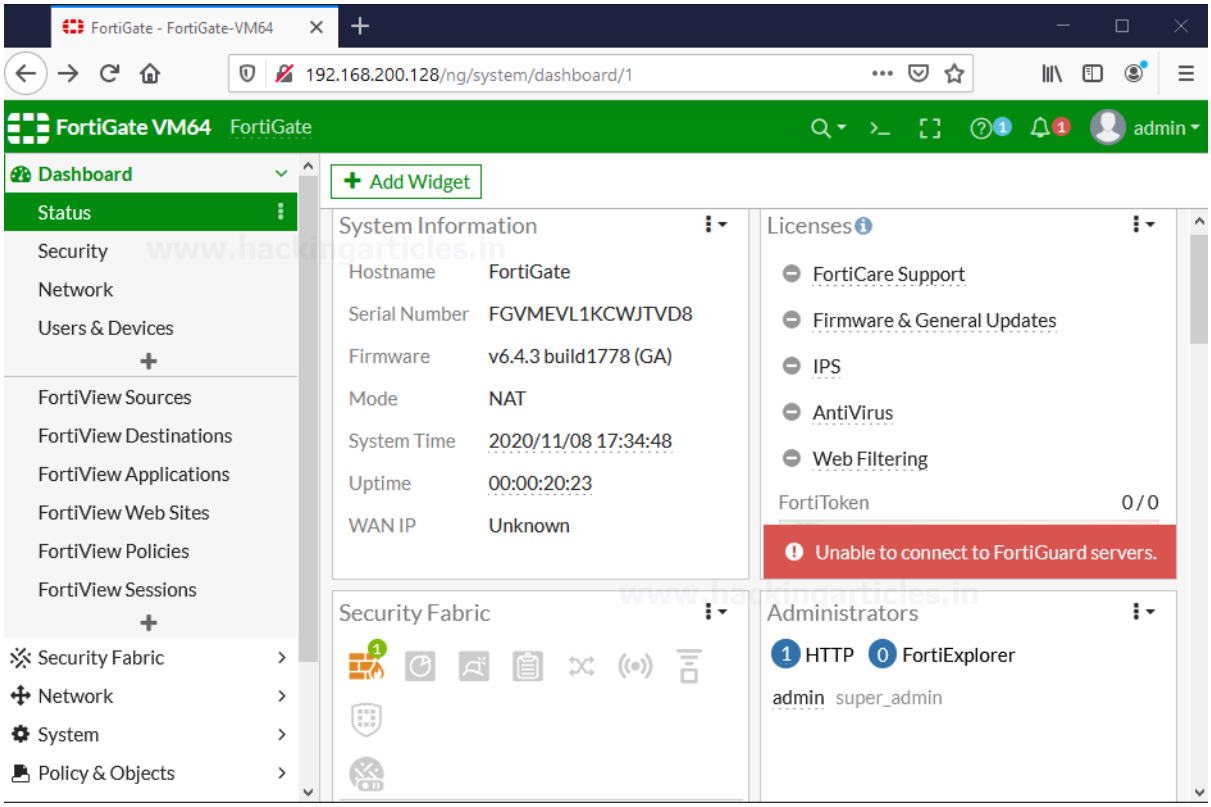
Already we have changed the password in Firewall CLI and also, we have already downloaded the latest version of the firewall, so it automatically skips you to the last step to Dashboard setup. Select it to Optimal or Comprehensive as per your requirements



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:



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,l 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?

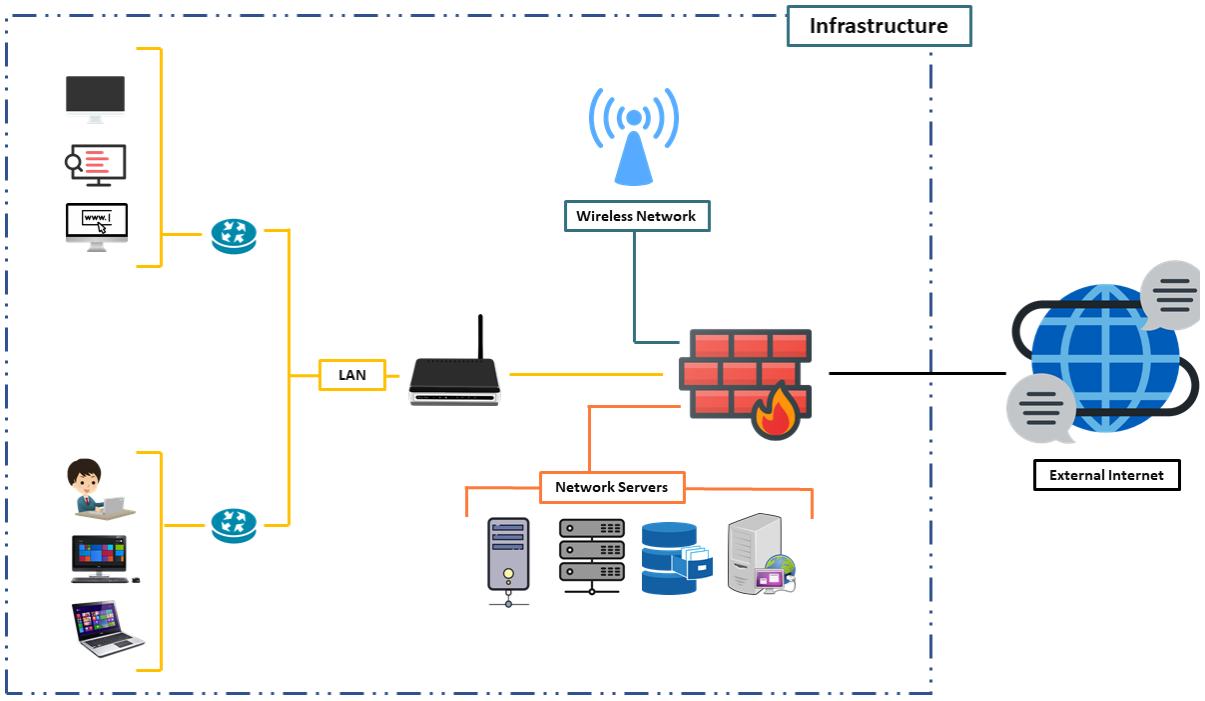
Basically, firewalls are divided into two parts

- 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.

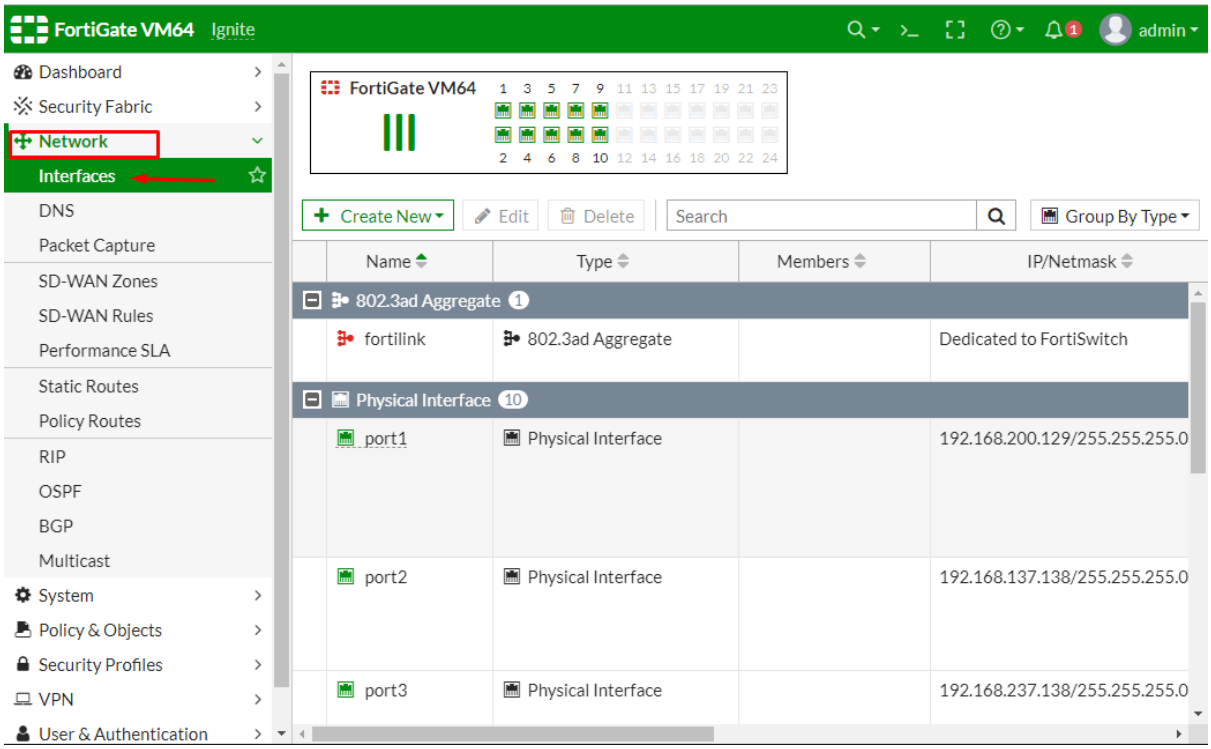
Connect the FortiGate internet facing interface usually WAN1 to your ISP supplied equipment and connect the PC to FortiGate using an internal port usually port 1 or as per your requirement.

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

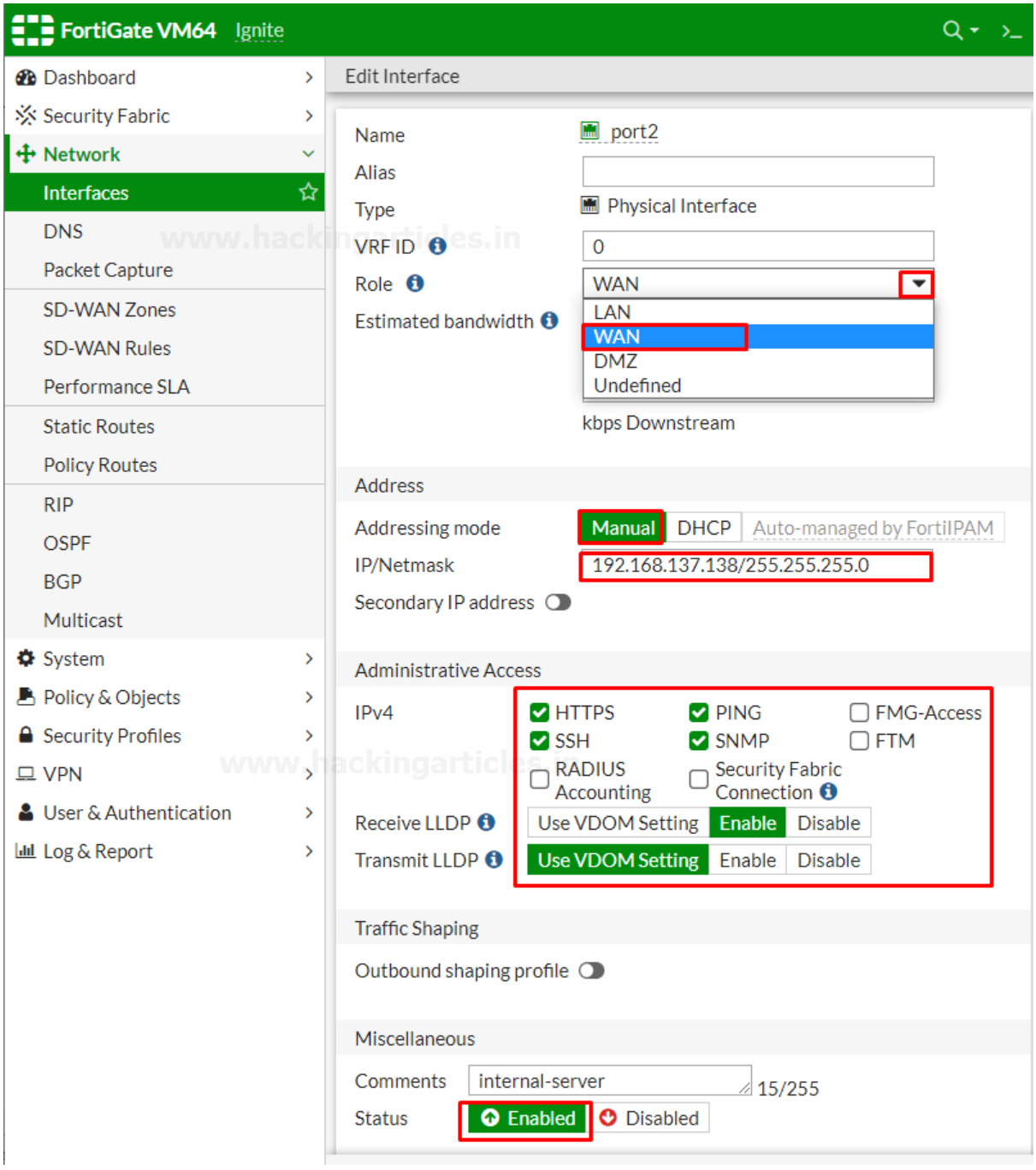
Configure Network Interfaces

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

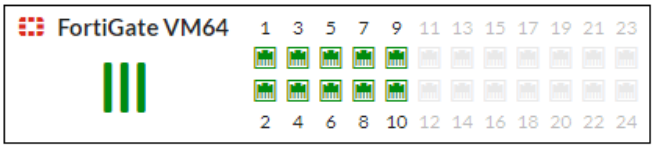
Go to network > Interfaces



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



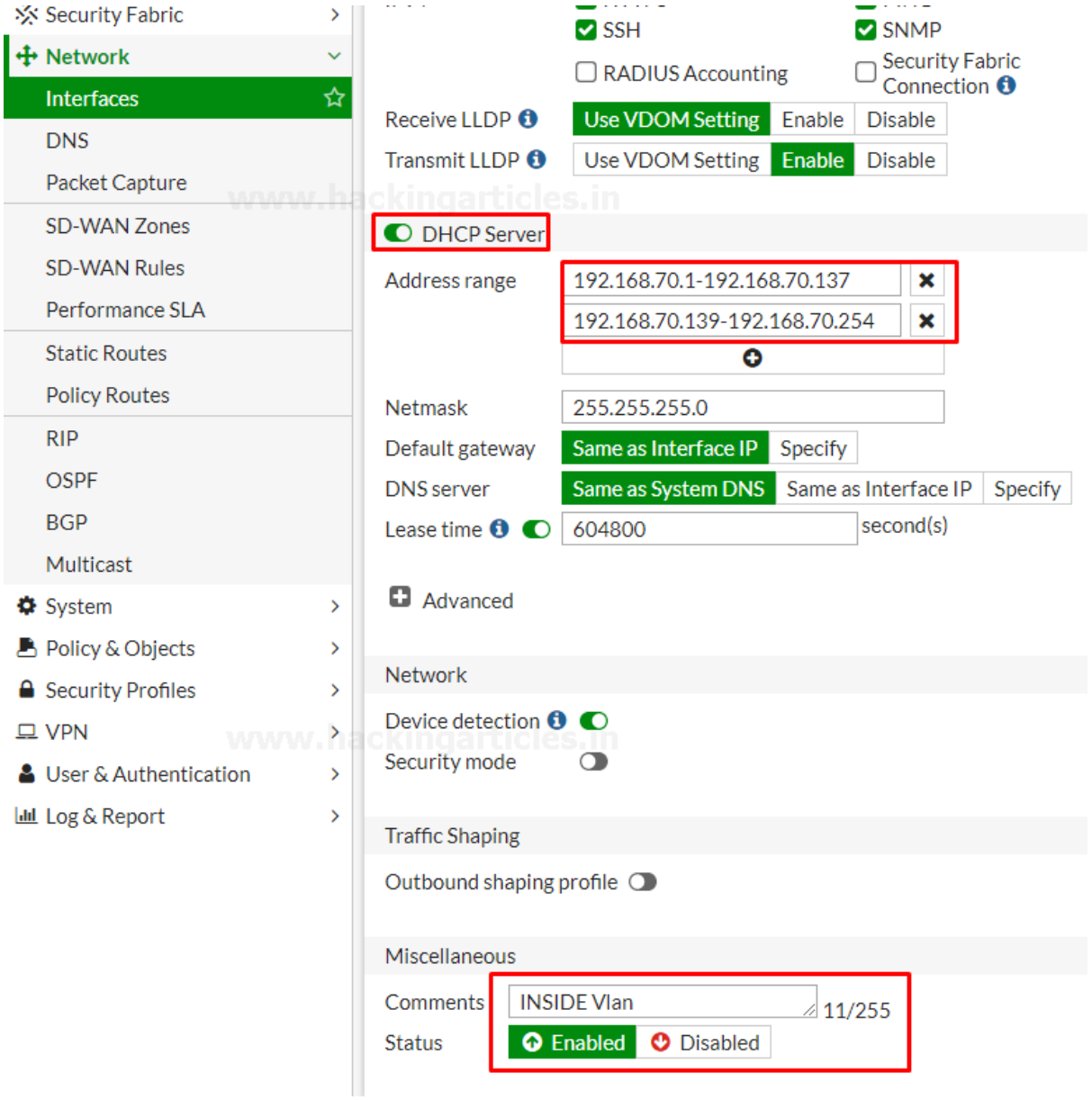
Then save the configuration and then similarly edit the LAN interface which may be called internal network. Set the interfaces Role to the LAN or WAN and then set the addressing mode to manual and set the IP/Netmask to the private IP address that you want to assign to the FortiGate



Create New | Edit | Delete | Search | Group By Type

Name	Type	Members	IP/Netmask	Administrative Acce
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	

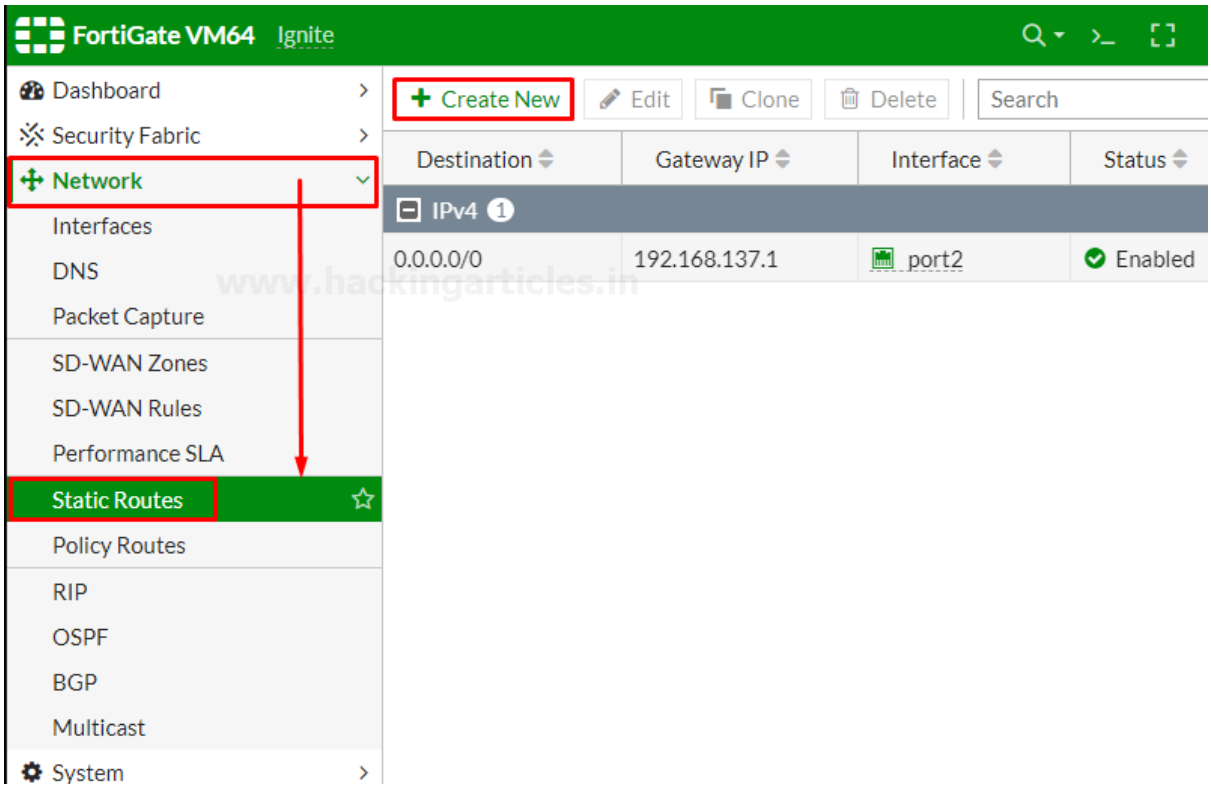
If you need your FortiGate to provide IP addresses to devices connected to internal network enable the DHCP server and then save the configuration as shown below.



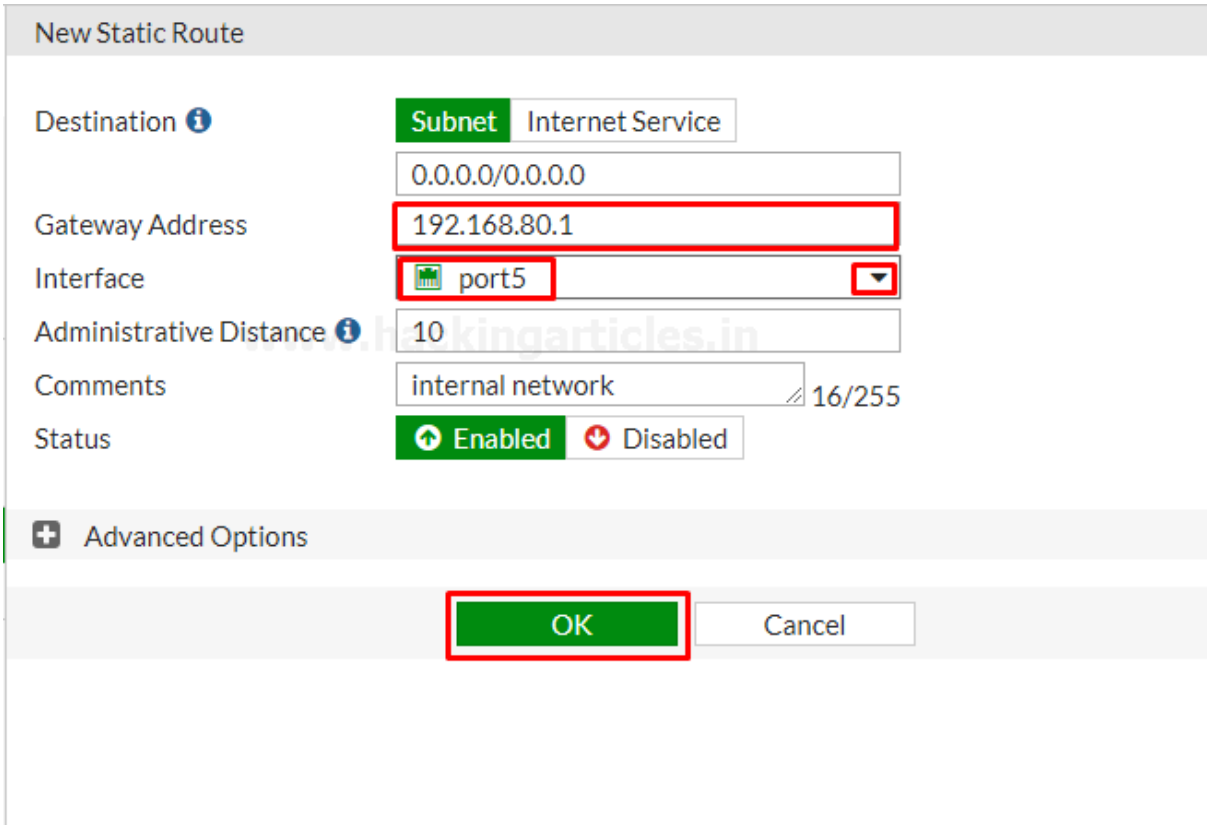
Changing the default IP of your interfaces is recommended for the security measures. But you are connected to the FortiGate through that interface the FortiGate will log you out and you must navigate to the new IP address assigned to the interface and login again.

Add a Default Route

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

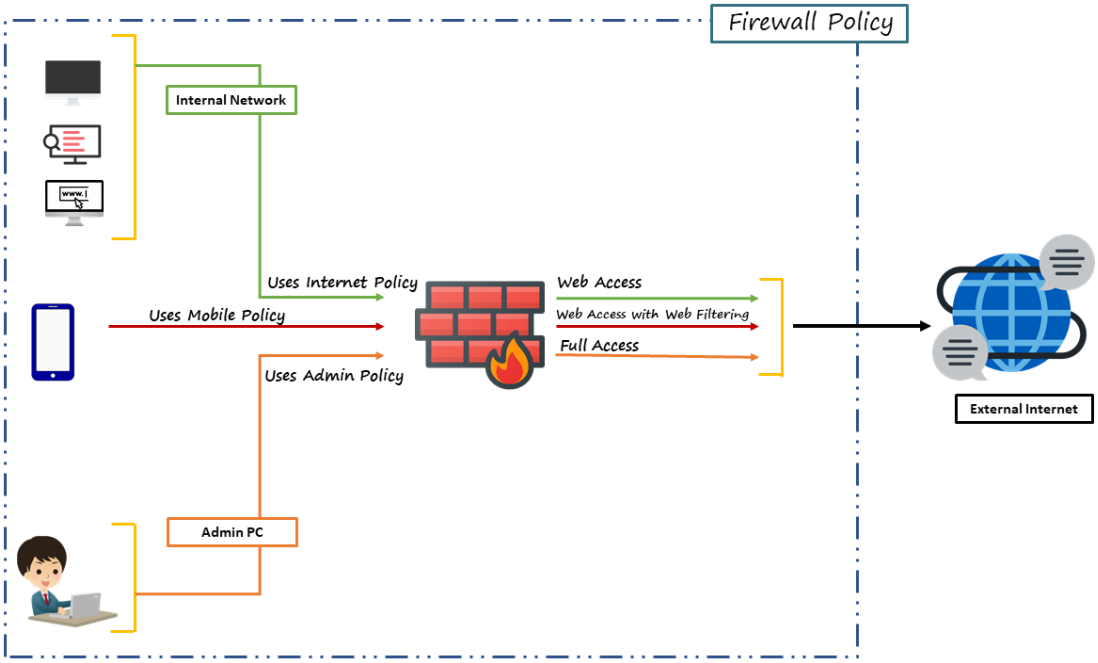


Set destination to subnet and enter IP/Netmask of Eight Zeros. Set the Gateway to the Gateway IP provided by your ISP and the interfaces to the internet-facing interface then save the Route.

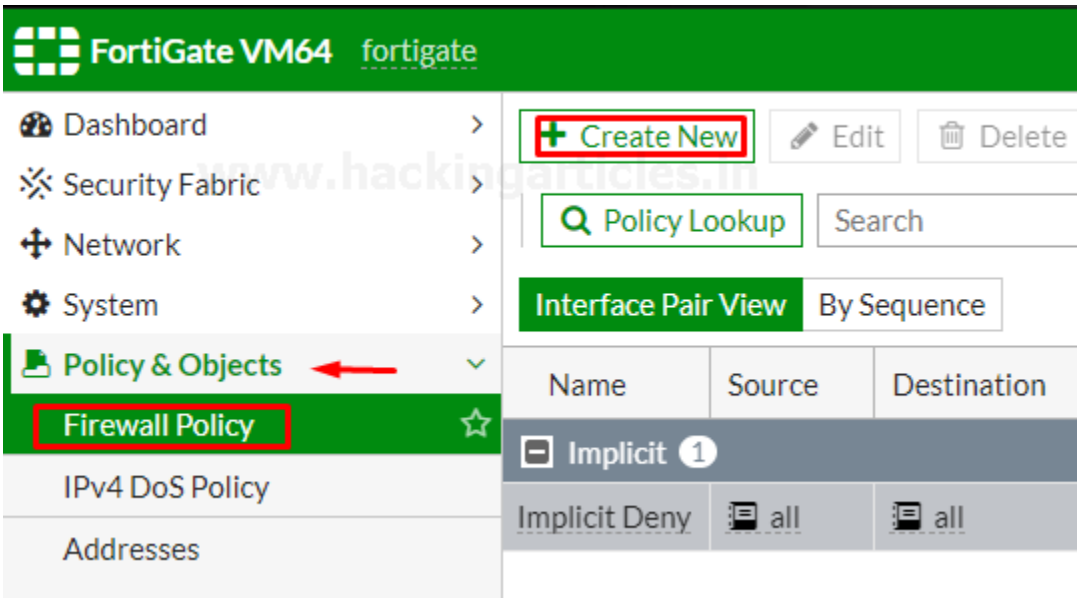


Create an IPV4 Firewall Policy

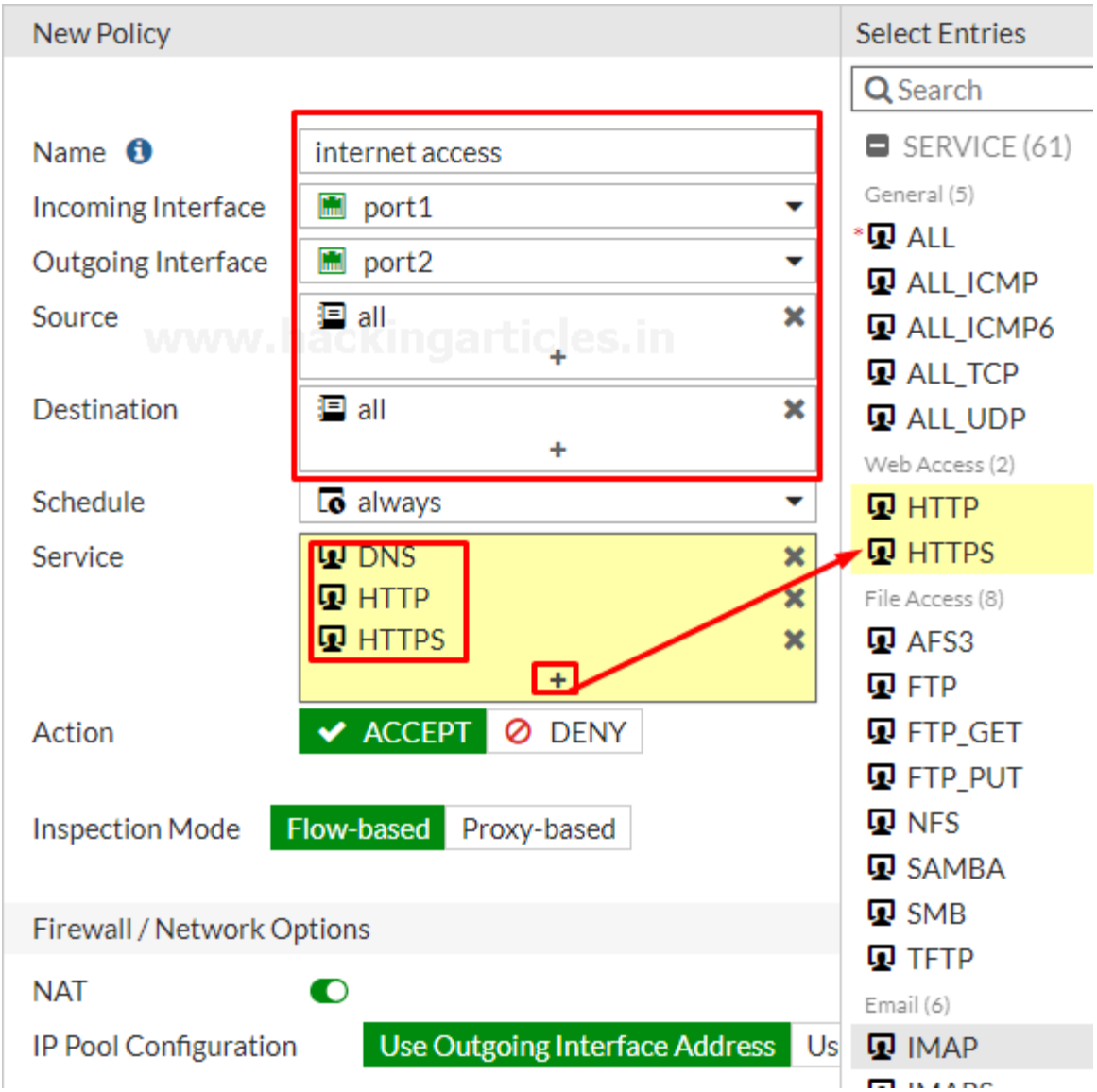
Firewall policy designed in a manner to examine Network Traffic using policy statements to block unauthorized access while permitting authorized communication.



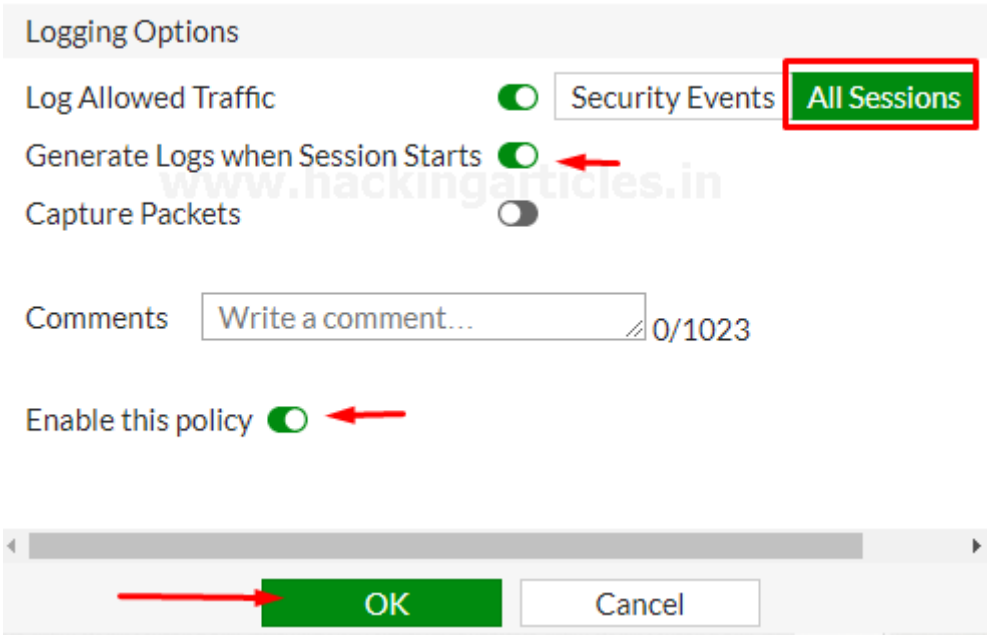
Go to **Policy & Objects > Firewall Policy** and **create** a new policy which allow internet traffic through the FortiGate.



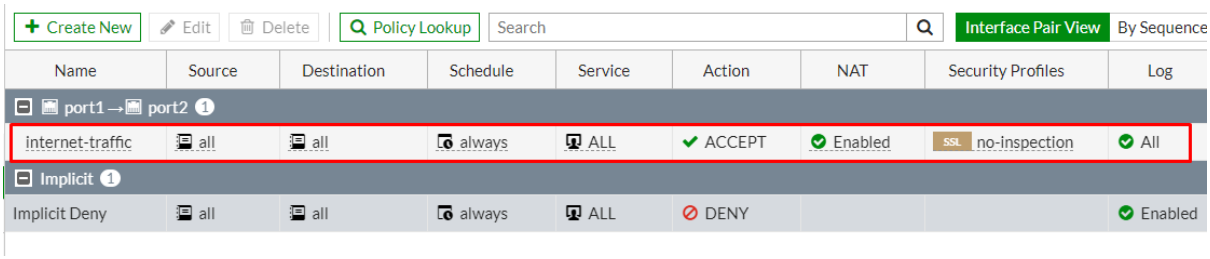
Name the policy as **"Internet-Traffic"** or whatever you want. Set the incoming interface to the **"Internal interface"** and outgoing interface to the internet facing interface. Set the rest to allow **"ALL"** Traffic or you can select multiple rules by selecting **the + icon** and the action to **"Accept"**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



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



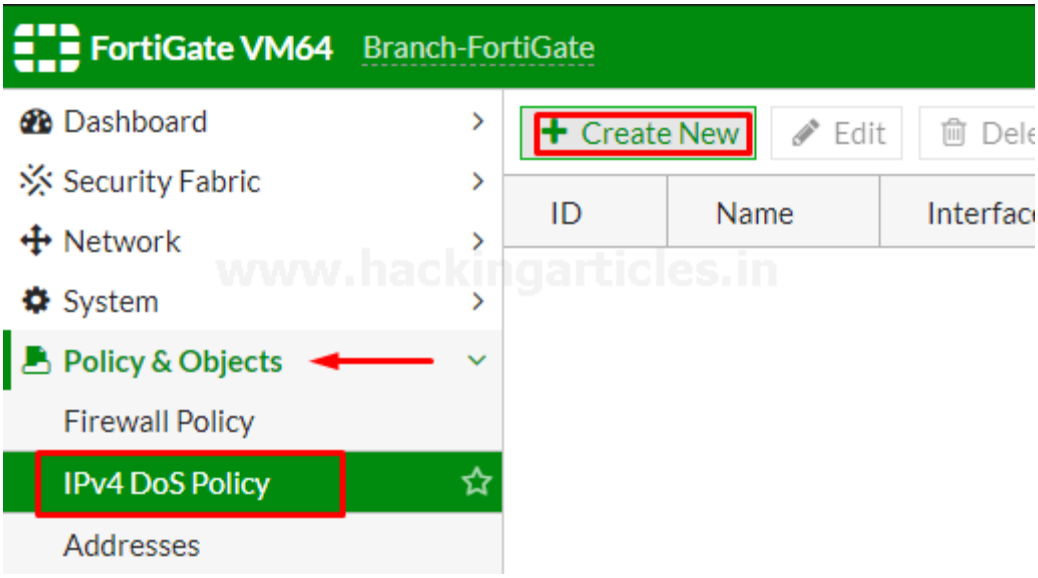
As you can see the policy successfully enabled.

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.



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.

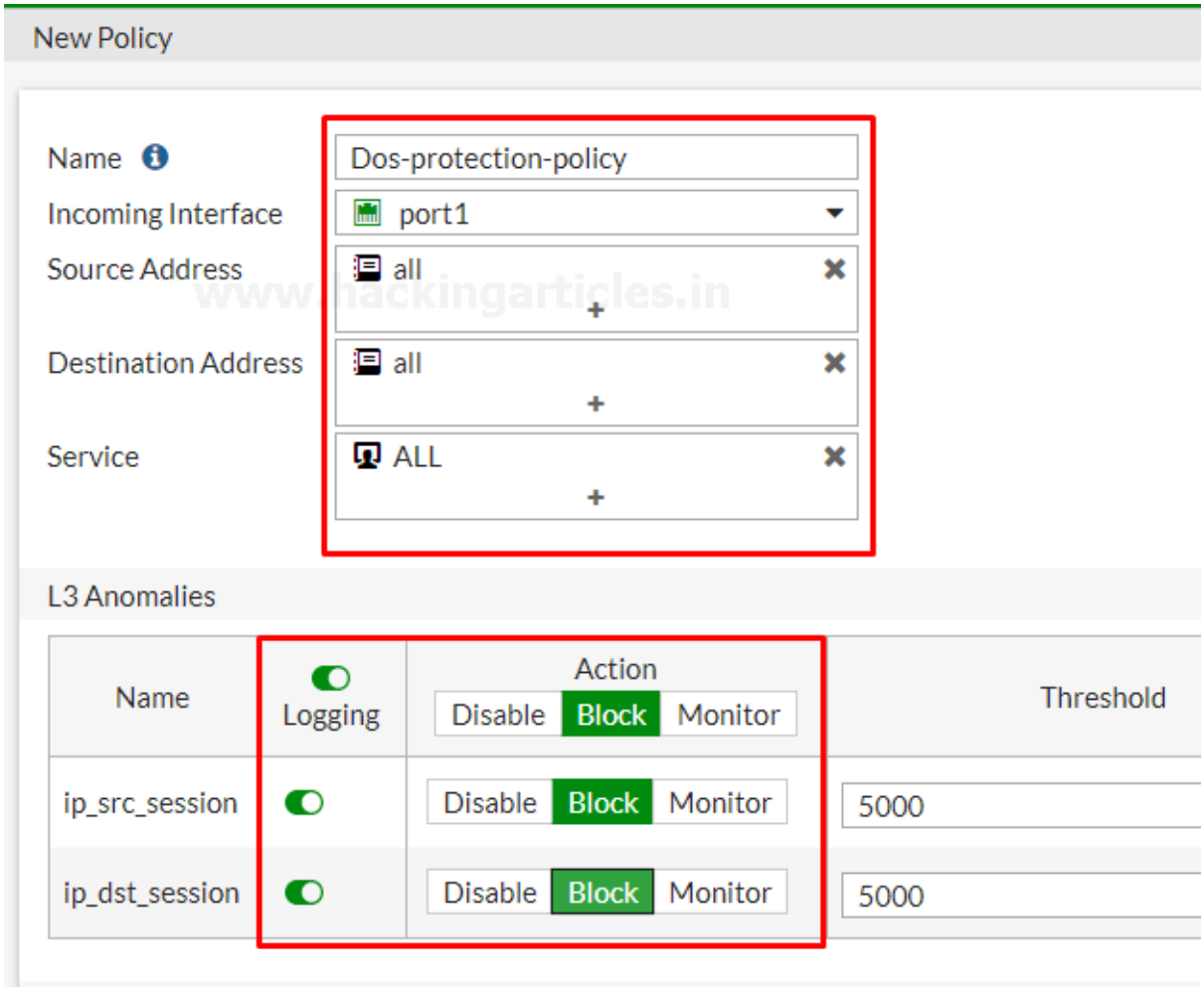
The breakup of traffic anomalies table is divided into 2 parts.

- L3 Anomalies
- L4 Anomalies

Here is the list of Anomaly profile that includes:

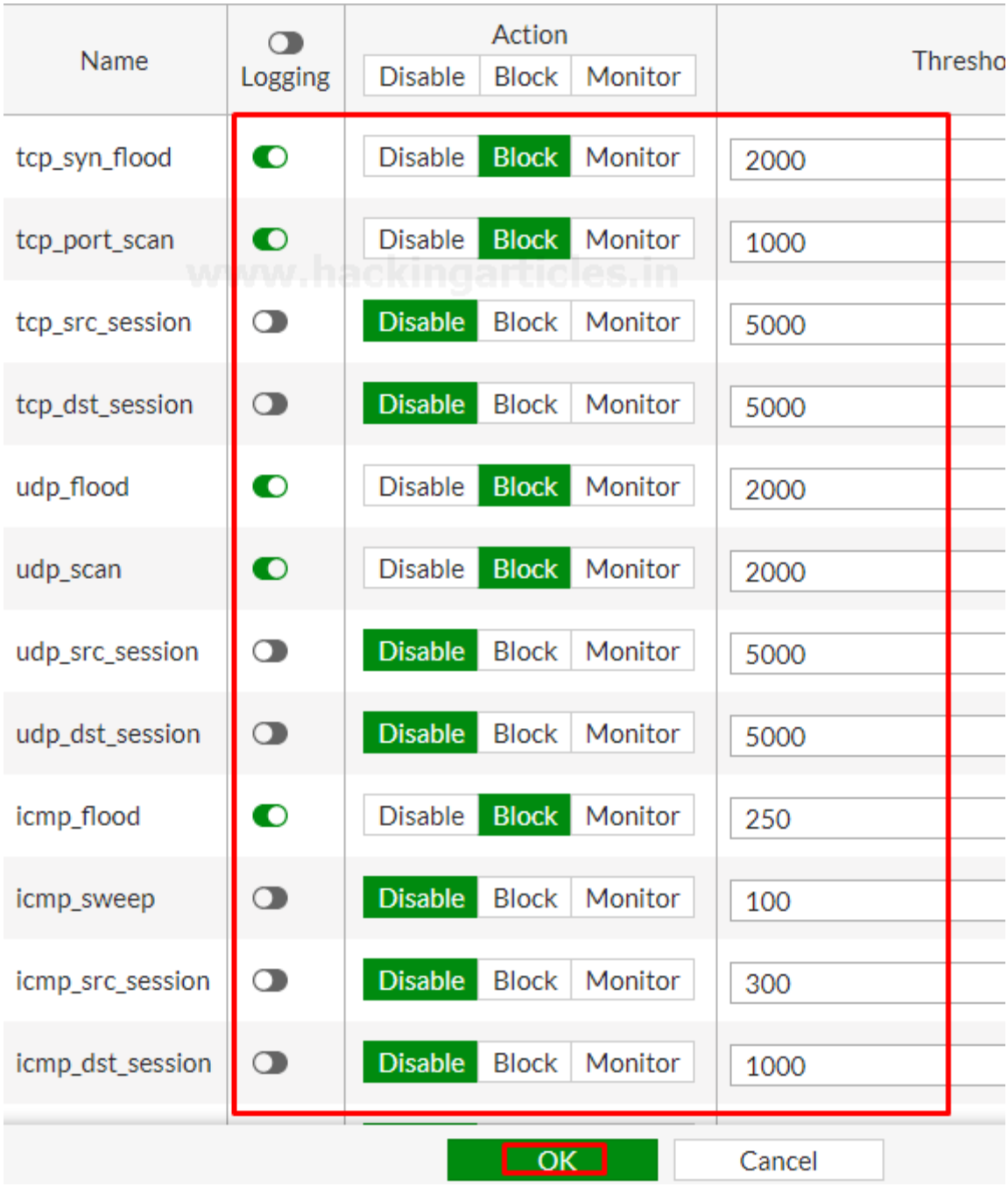
L3 Anomalies

- Ip_src_session
- Ip_dst_session



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

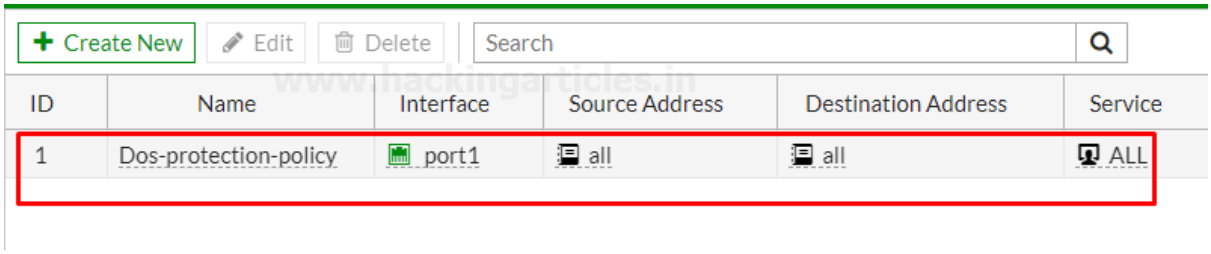


It all your choice whether or not to enable this policy and default is enabled. Here in our case, we have blocked some of the actions with the limited threshold values to check whether these policies working or not.

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.



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.

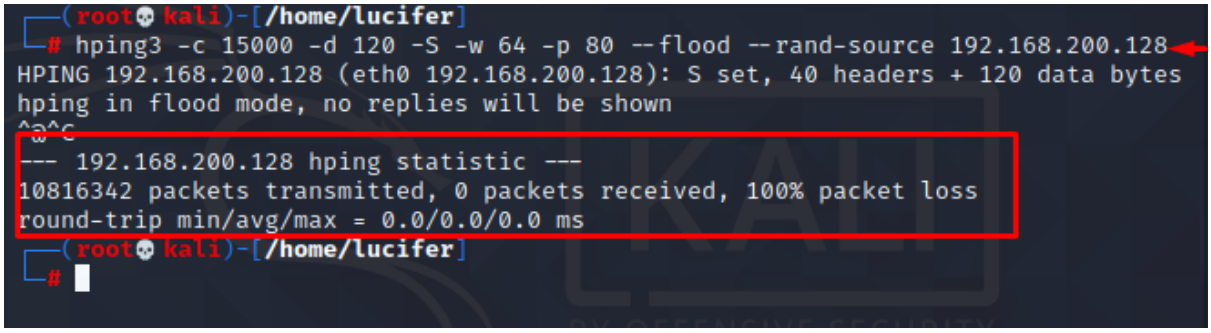
Hmm, exited

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

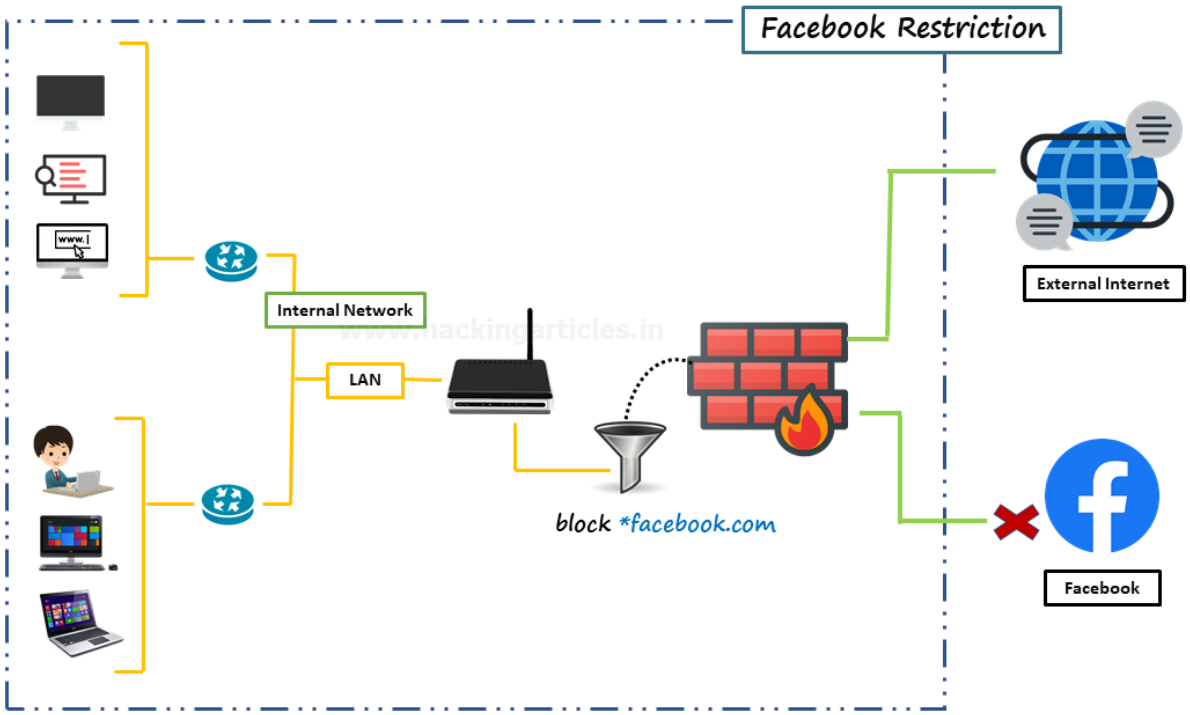


As we can see it blocks whole traffic that means it works properly.

Blocking Facebook with Web filter

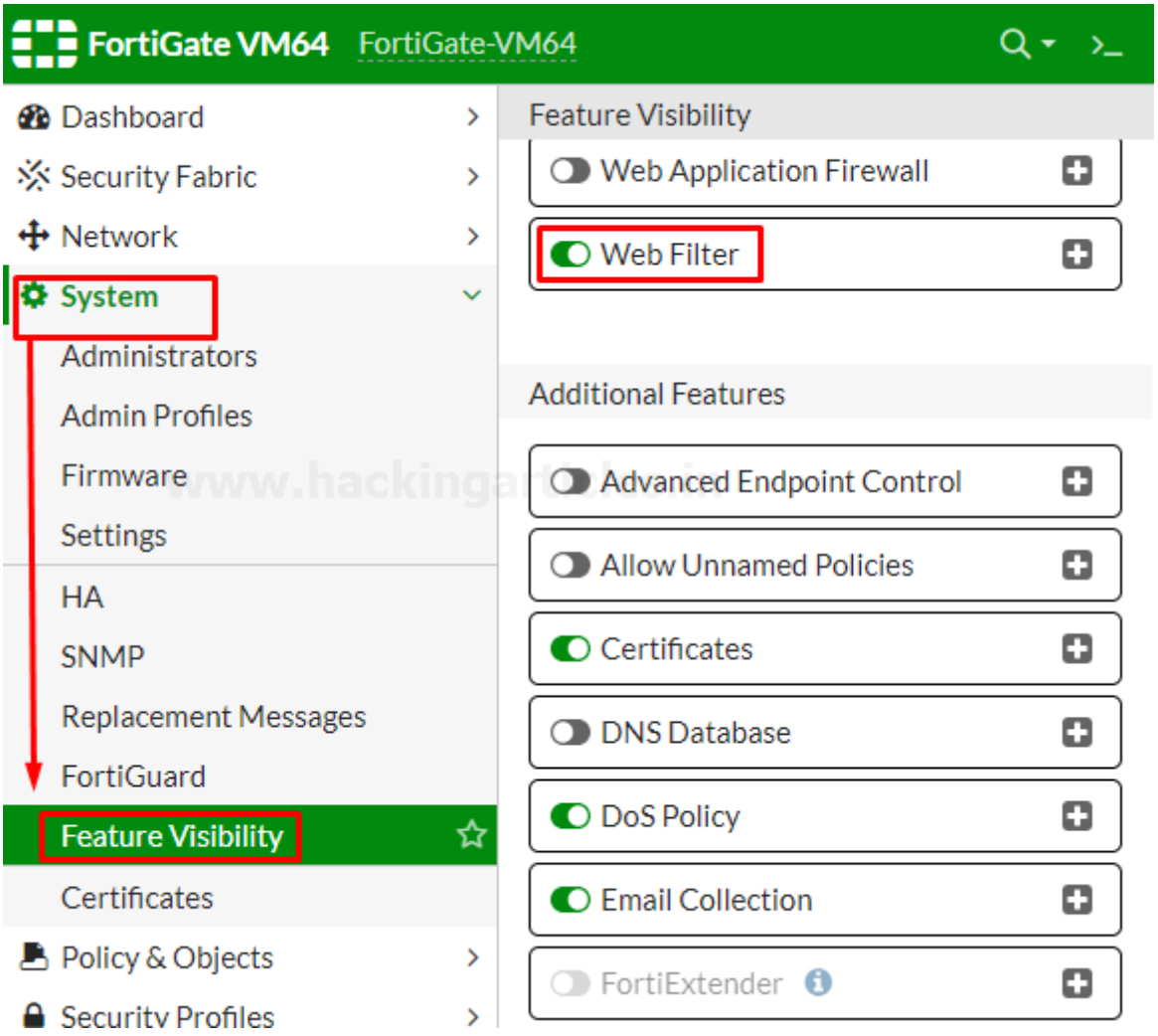
In this part, we are going to explain how to use a static URL filter to block access to Facebook and its subdomain in our network.

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.



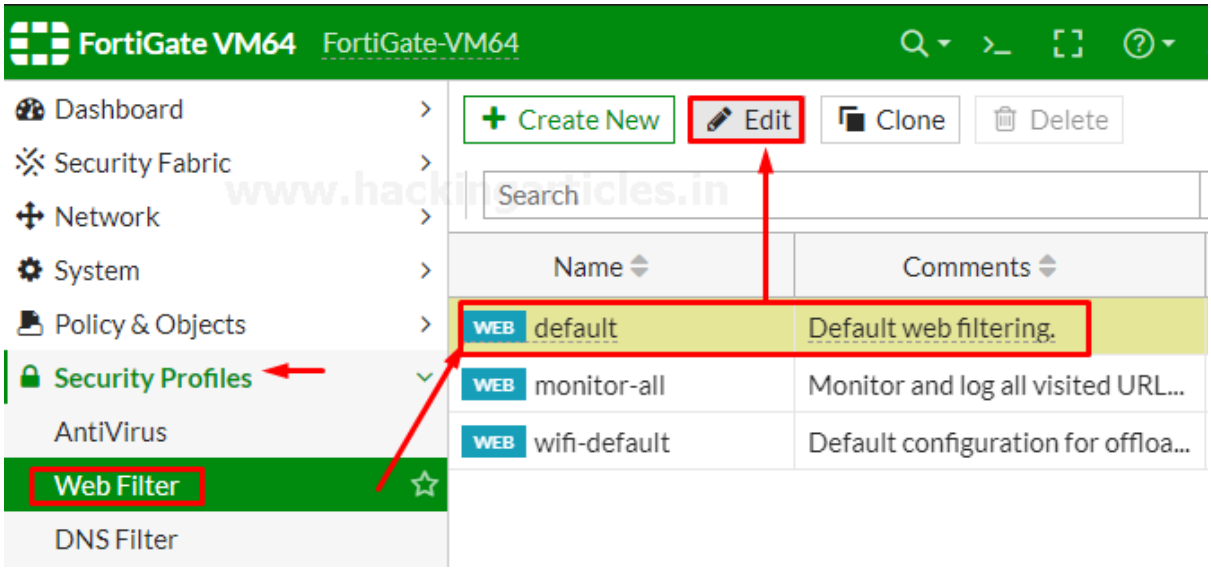
Enable Web filter

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

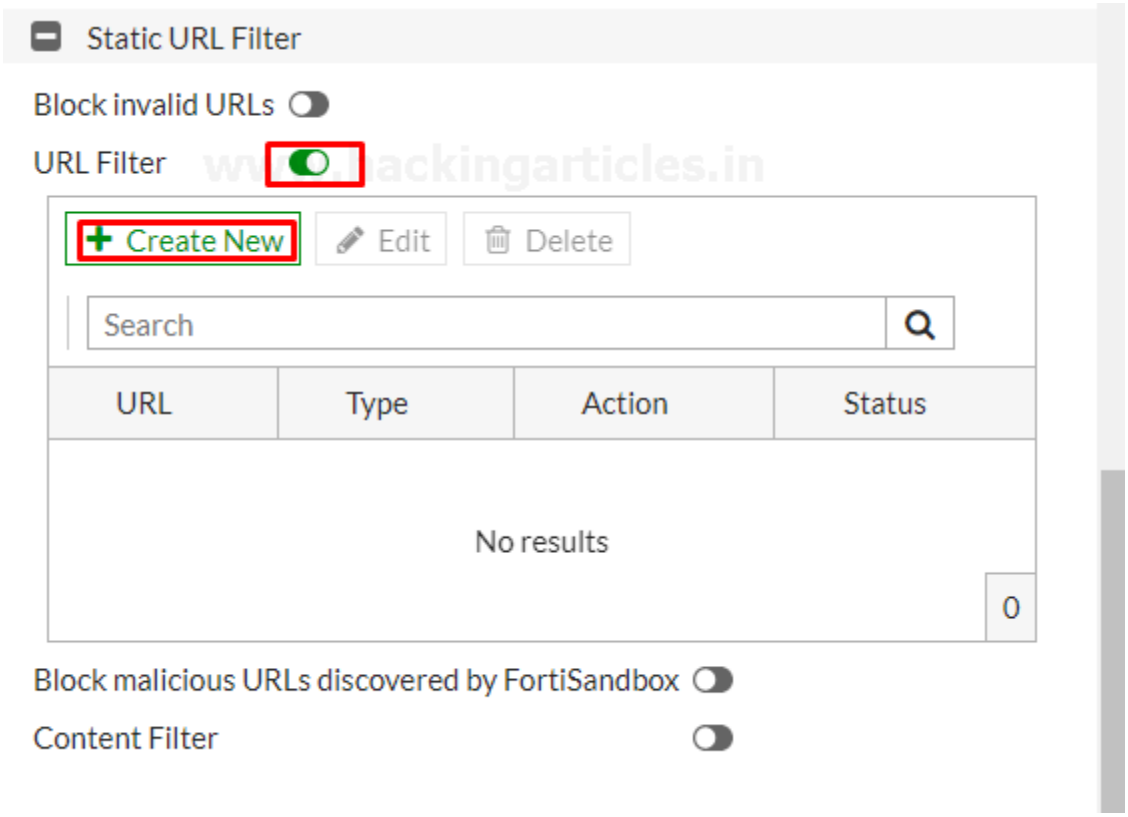


Enable Default Web Filter Profile

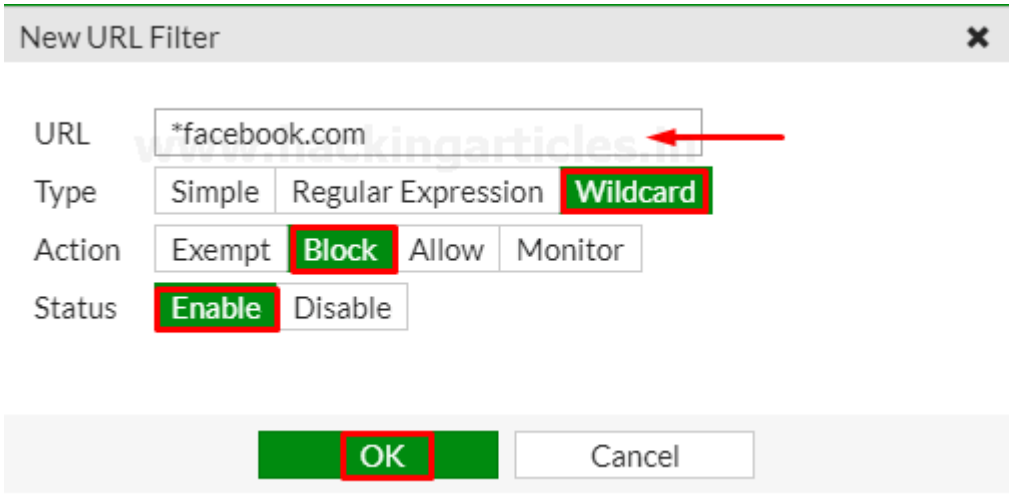
Go to **Security profiles** > **Web filter** and edit the default Web filter profile



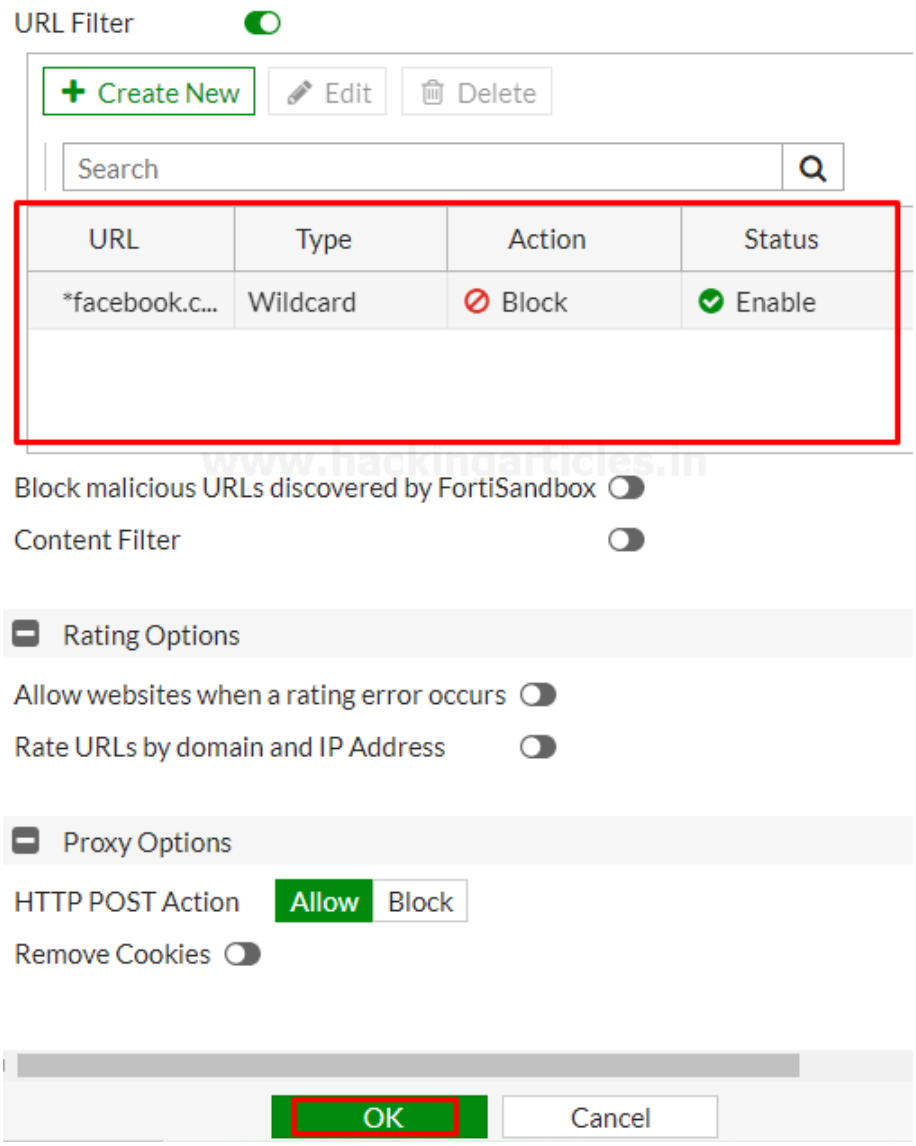
Now go to Static URL filter, select the URL filter and then select **"create"**.



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



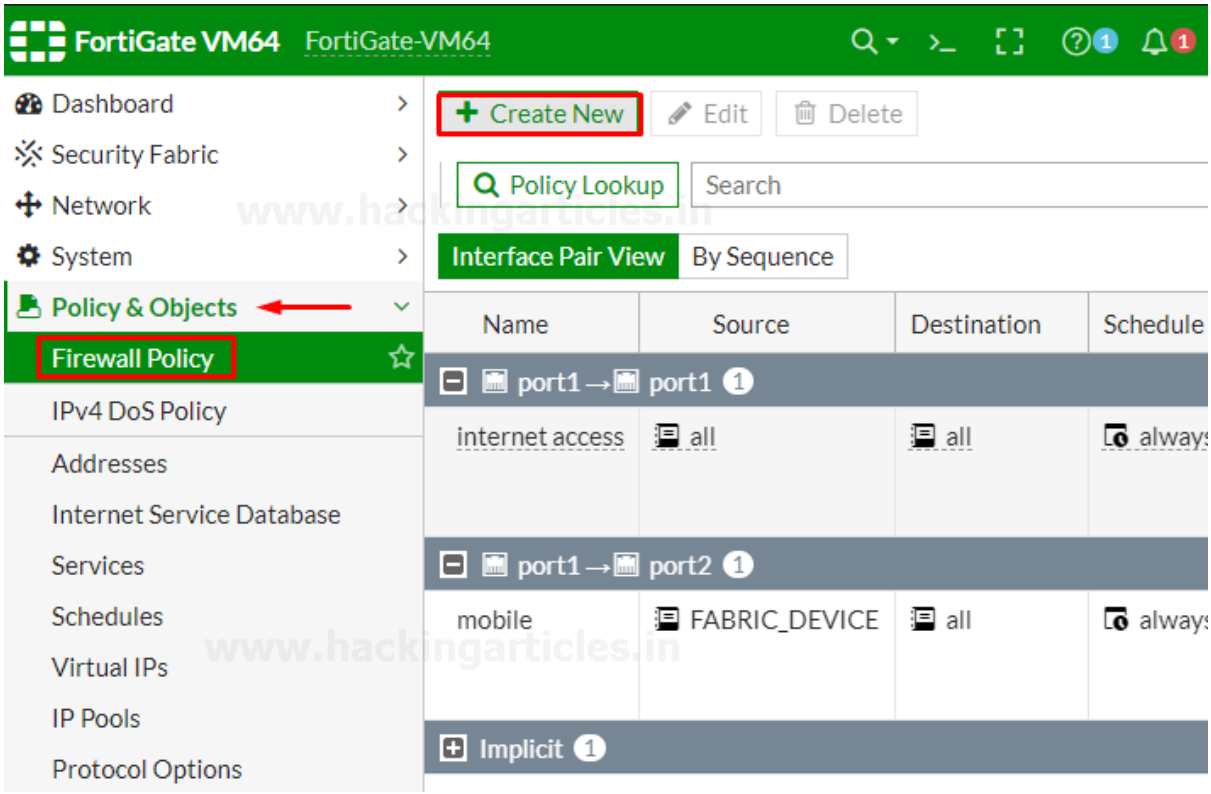
save it by selecting OK



Now you have successfully enabled web filter to block Facebook.

Create Web Filter Security Policy

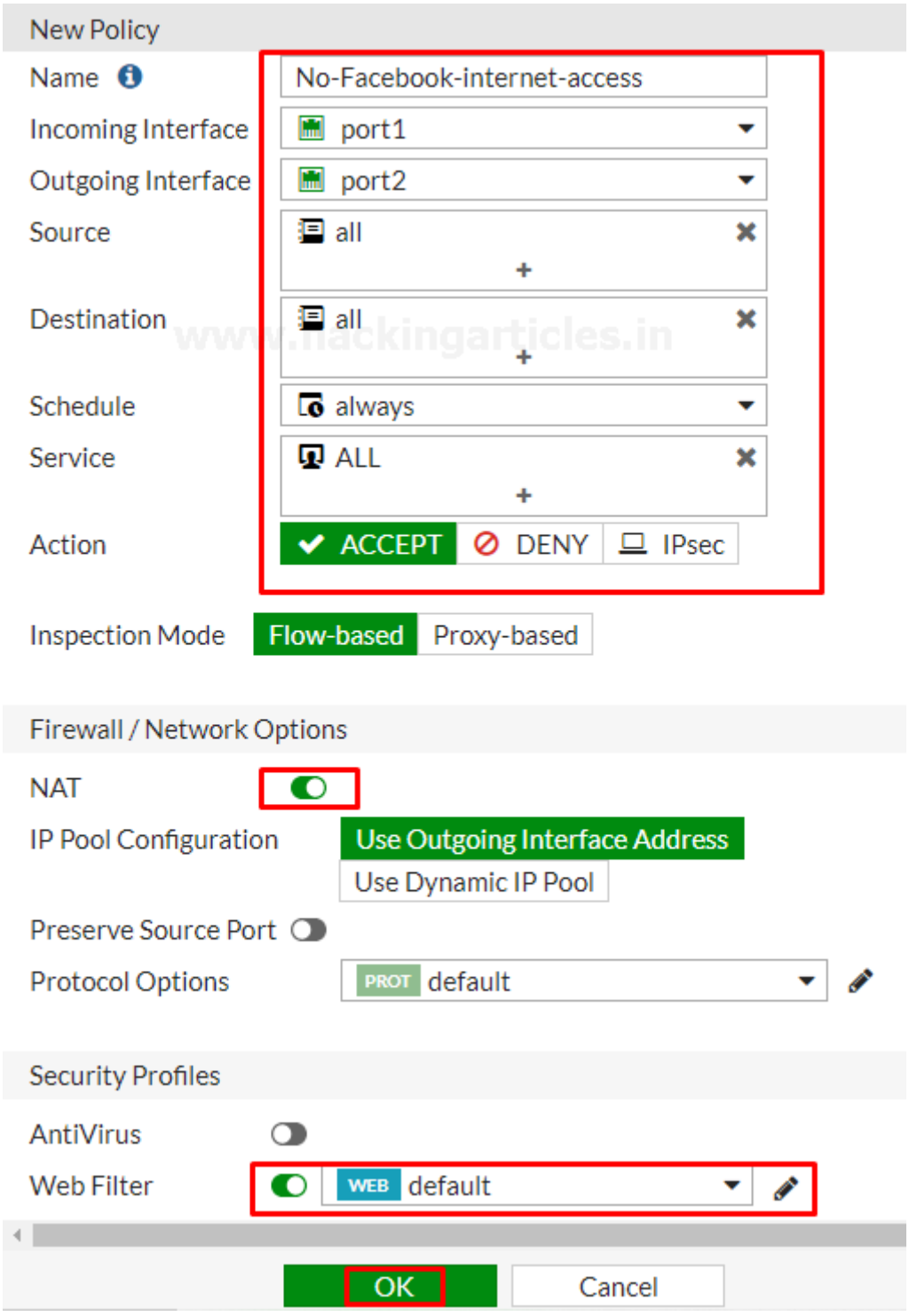
Go to **Policy & Objects** > **Firewall Policy** and **Create a New policy**.



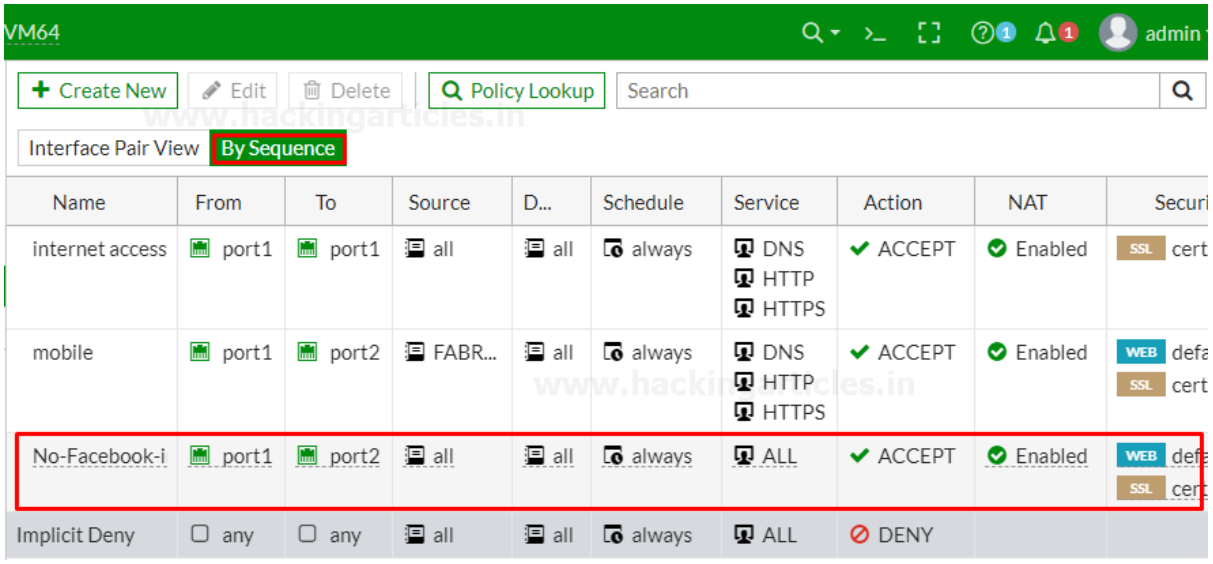
Give the name to the policy "No-Facebook-Internet-Access" to make it identifiable.

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"**

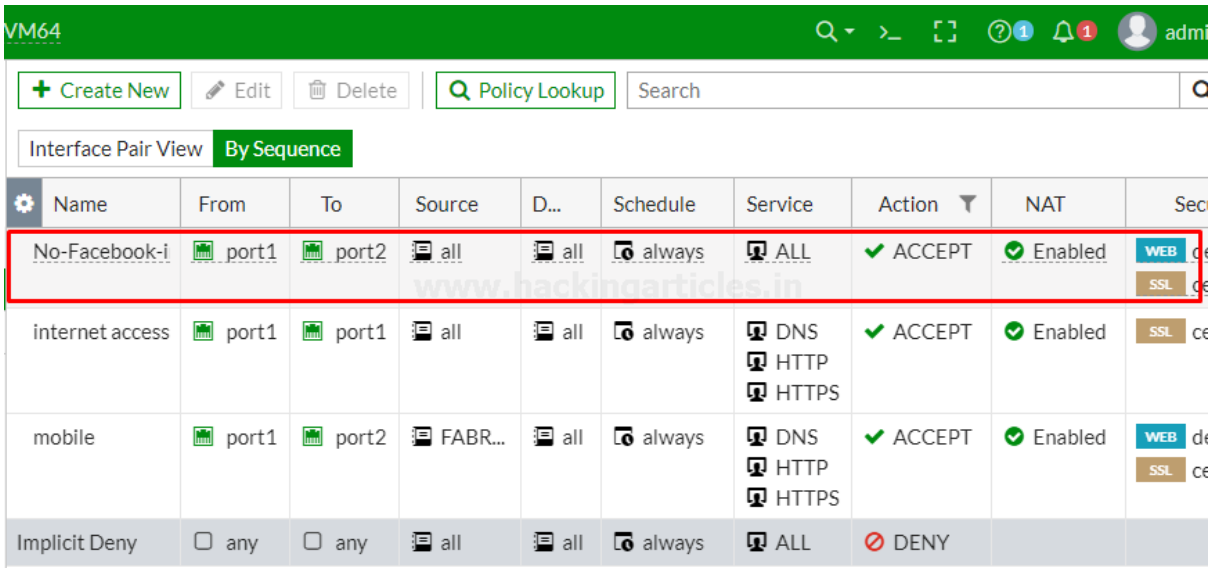
Under **Security Profiles**, enable **"Web Filter"** and select the default web filter profile.



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".**



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



Now this policy is in effect and successfully enabled.

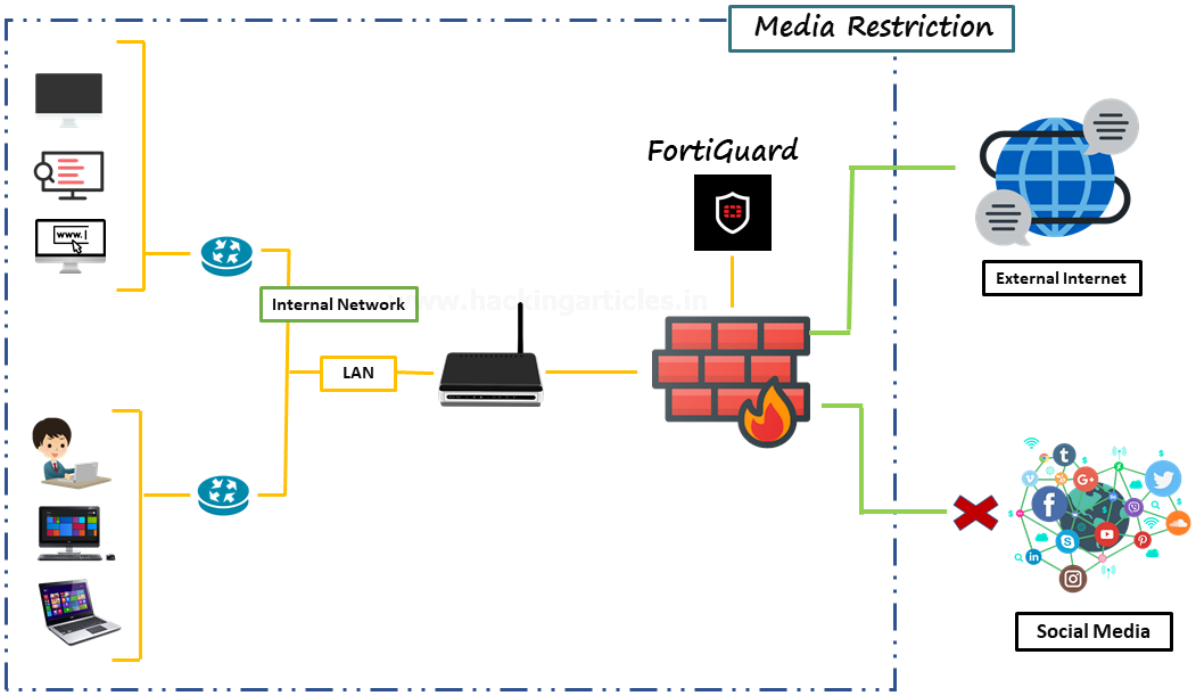
So, in this part, we have covered some basic policies that is much needed to save you network from unauthorized traffic.

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.



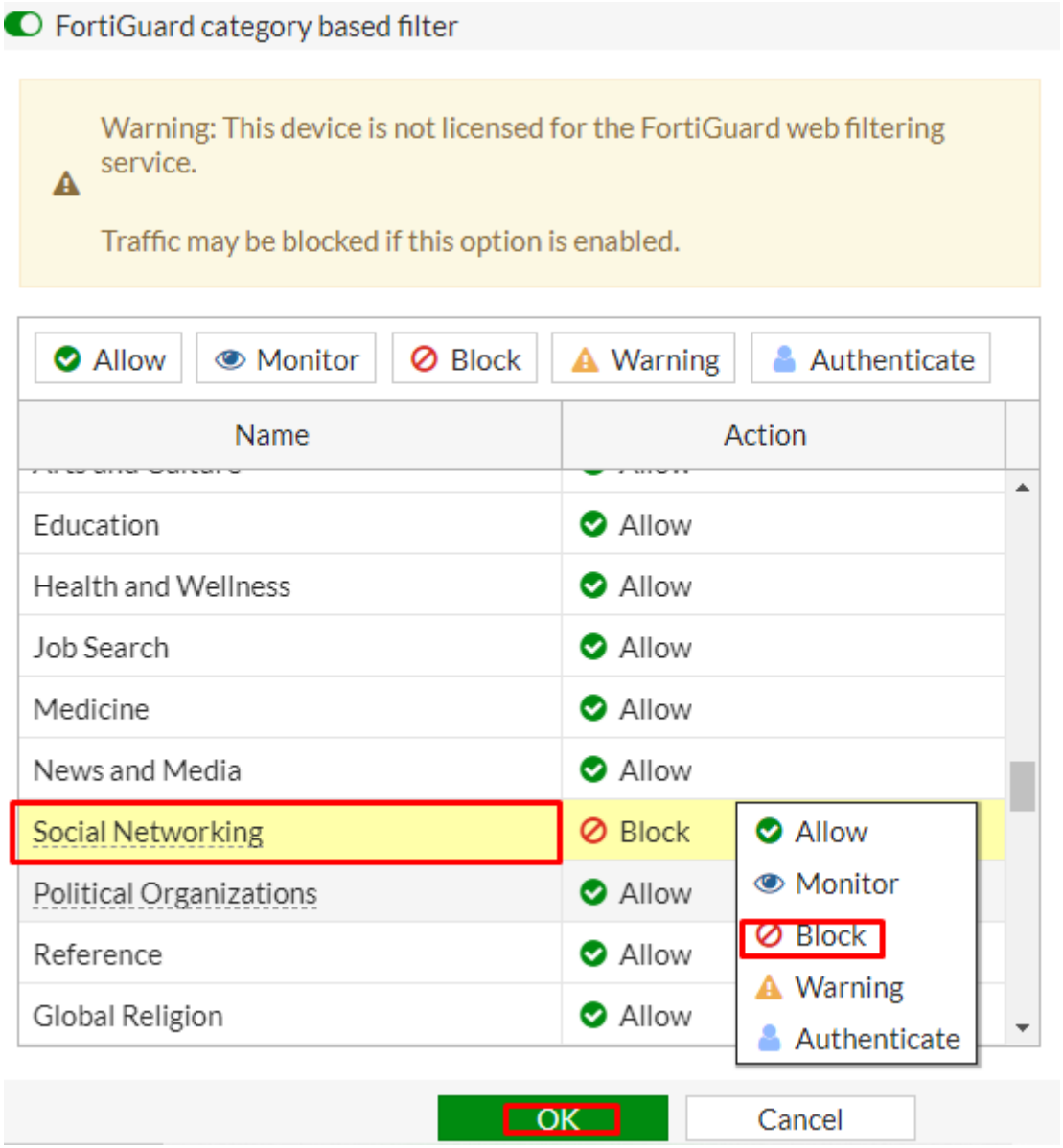
Enable web Filter

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

Edit Default Web Filter Profile

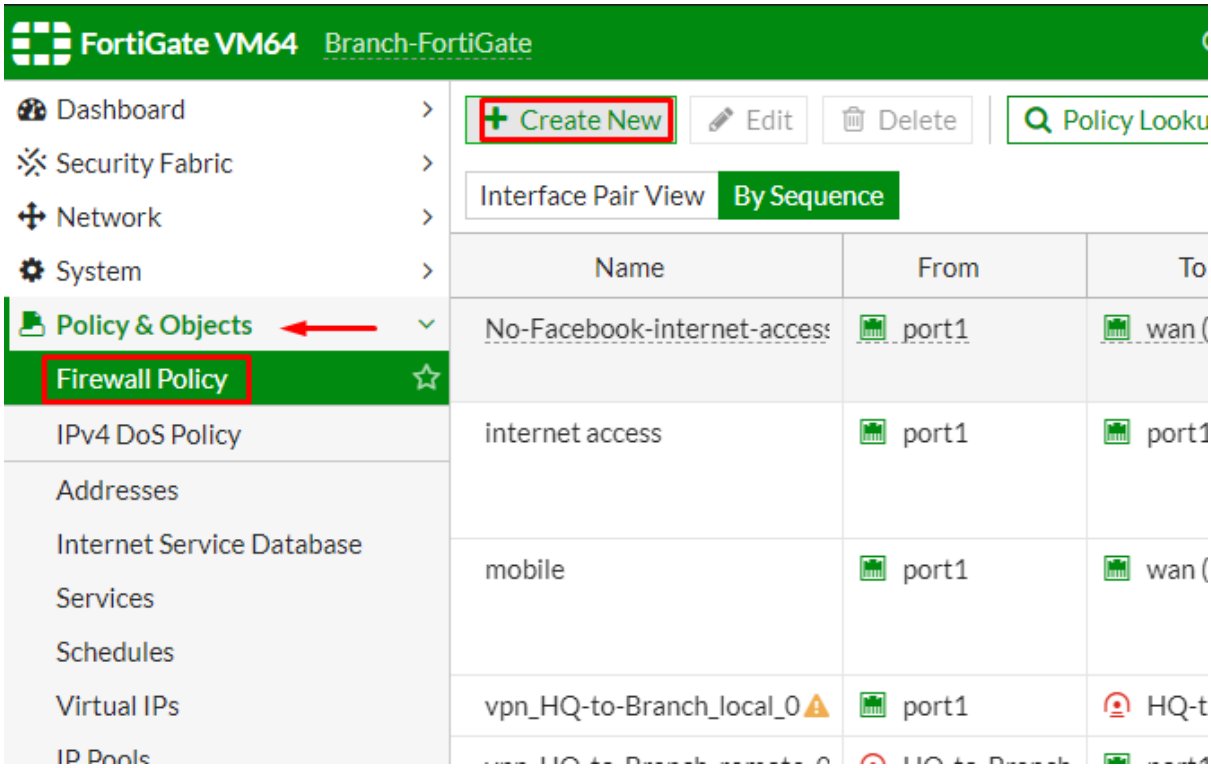
Go to **Security Profiles > Web Filter** and edit the Default web filter profile and make sure that "**FortiGuard category-based**" filter service is enabled.

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



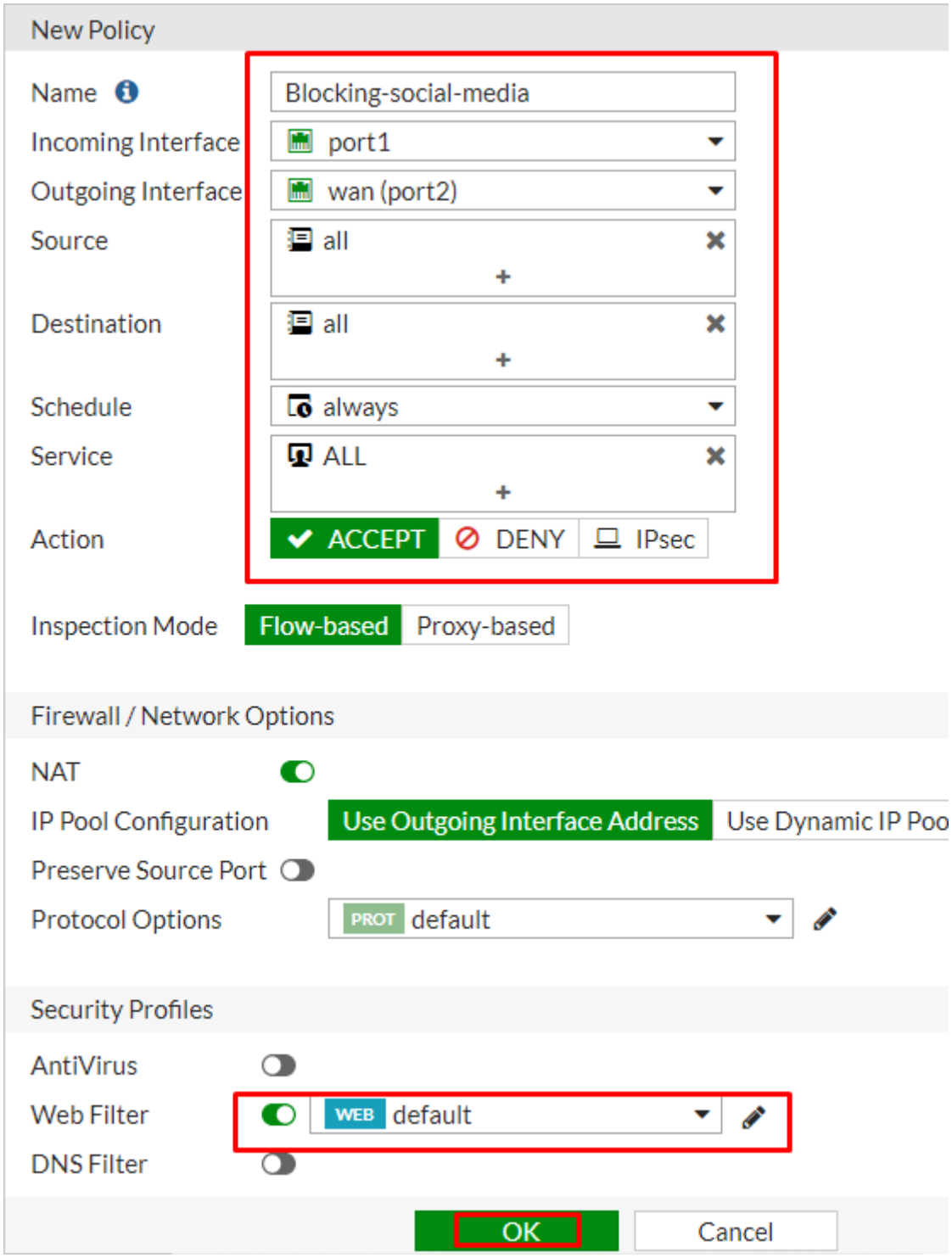
Add Web Filter Profile to Internet Access Policy

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

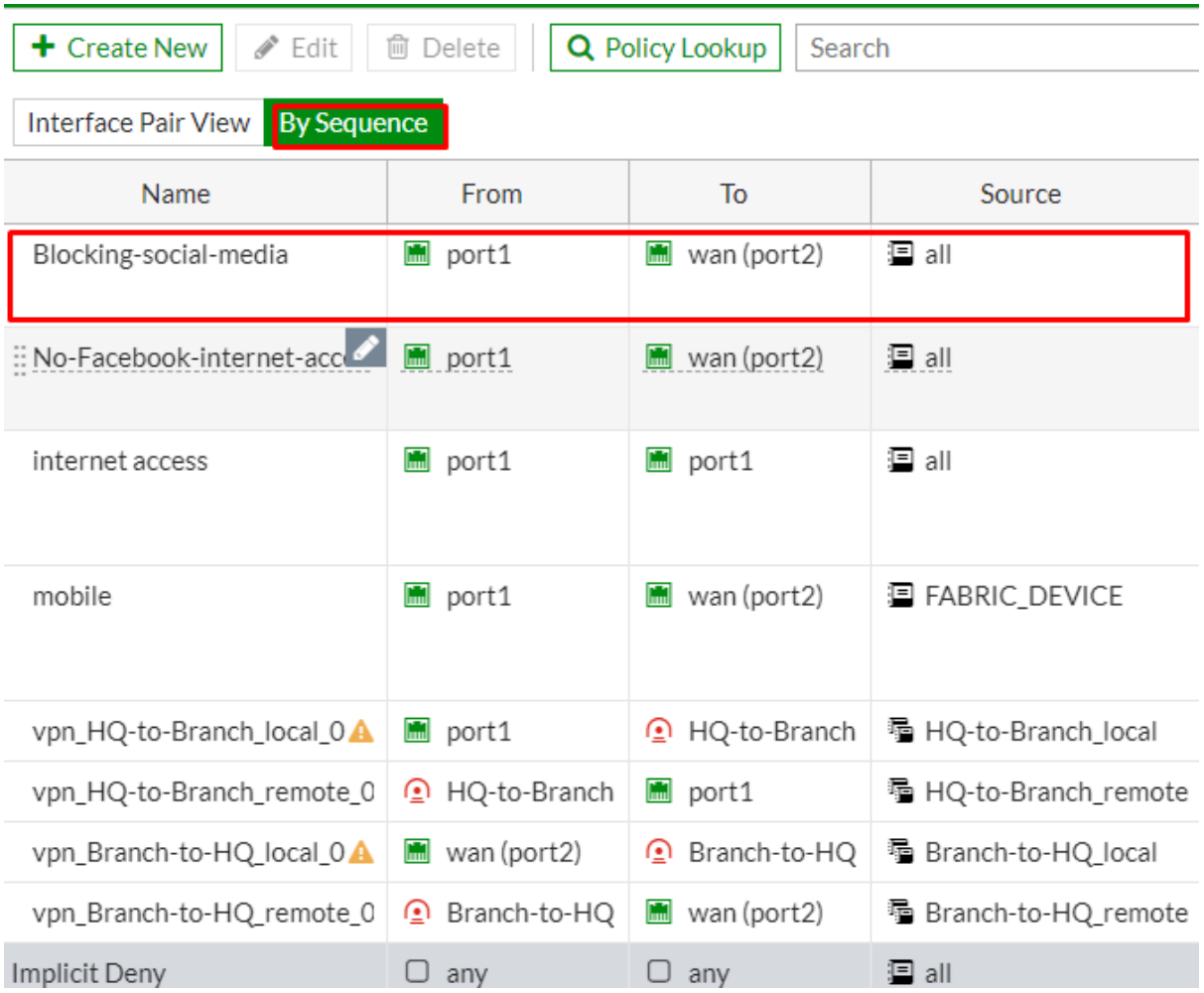


Give the name to the policy "Blocking-social-media" to make it identifiable. Set incoming interface to internal network and outgoing interface to internet facing interface. Set the rest to allow **"ALL"** Traffic or you can select multiple rules by selecting the + icon and the action to **"Accept"** 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.



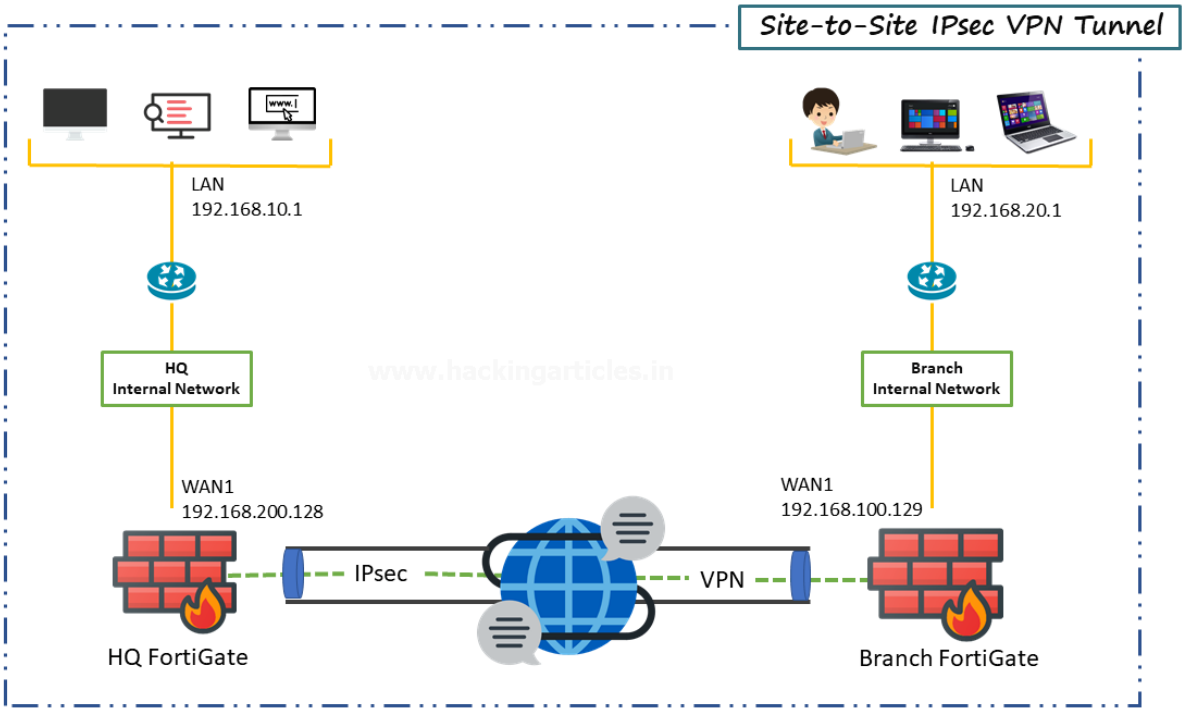
Now you have successfully enabled the social media blocking policy to move this policy to Top of the list to make it effective.



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 a situated behind different FortiGates.

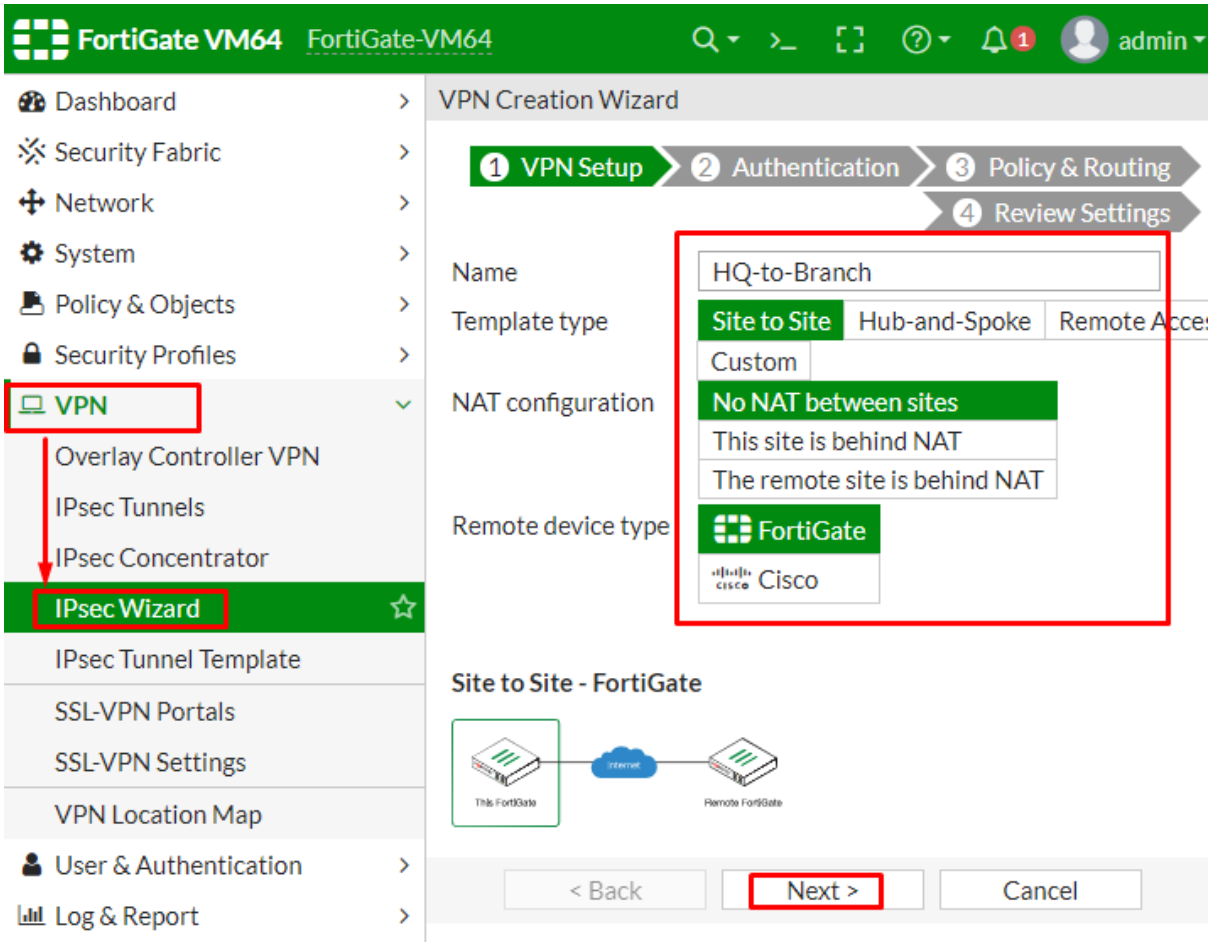
We are going to create an IPsec VPN tunnel between two FortiGates one is called HQ (Headquarter) another is called Branch.



Configure IPsec VPN on HQ

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

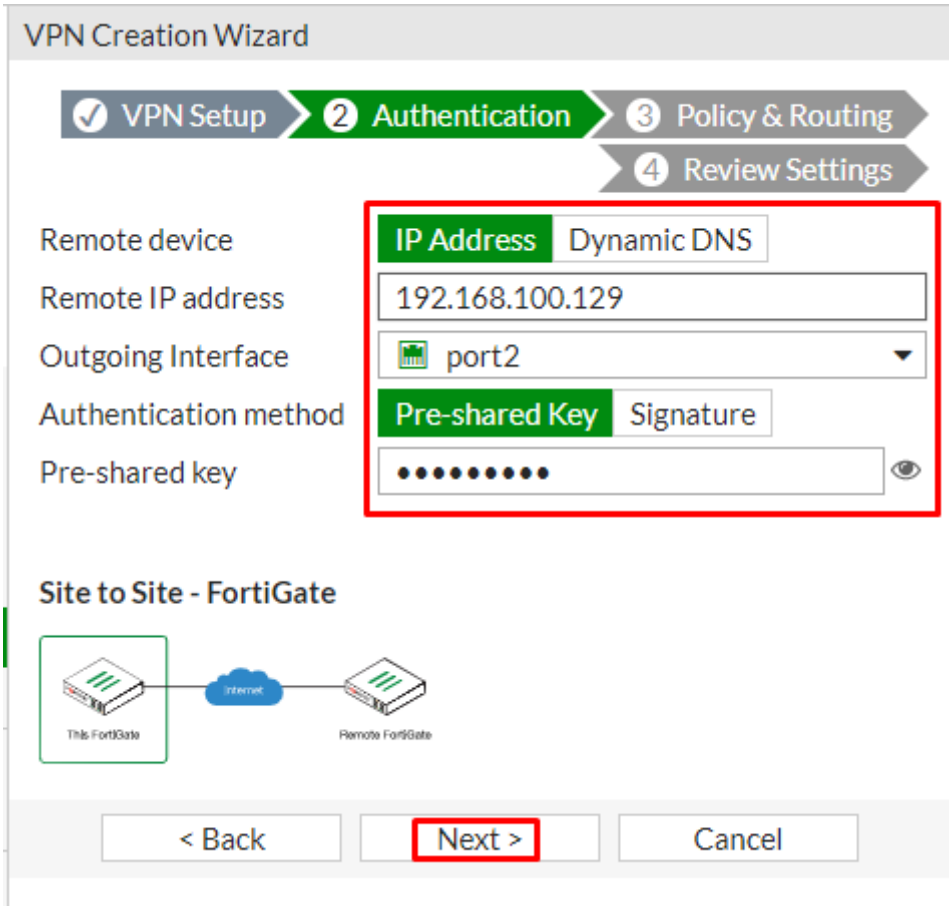
In the section, VPN setup describe a VPN name to make it identifiable, set Template type to Site-to-Site, set NAT configuration to NO NAT between sites and set Remote Device type to FortiGate.



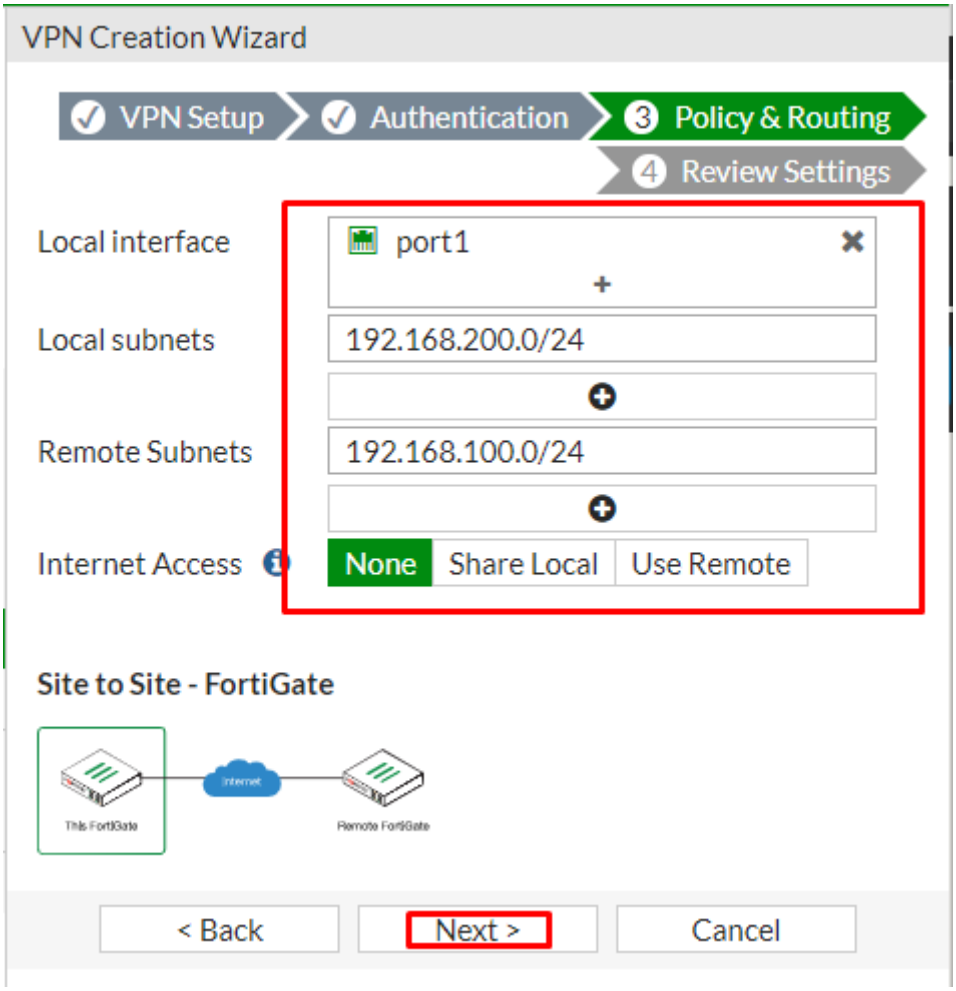
In the Authentication Section, set IP address to Public IP address of the Branch FortiGate.

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.

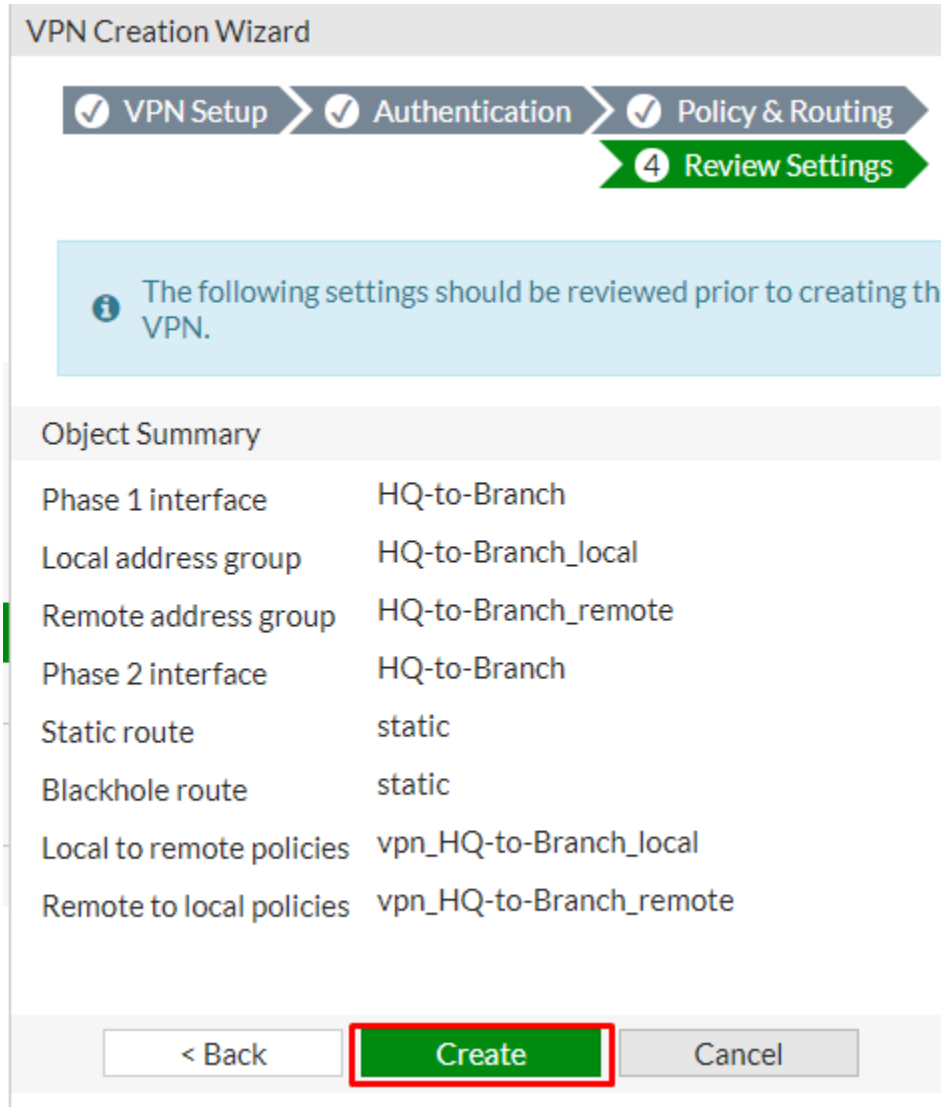
Set a secure **Pre-shared** key that is used to connect and verification for both FortiGates.



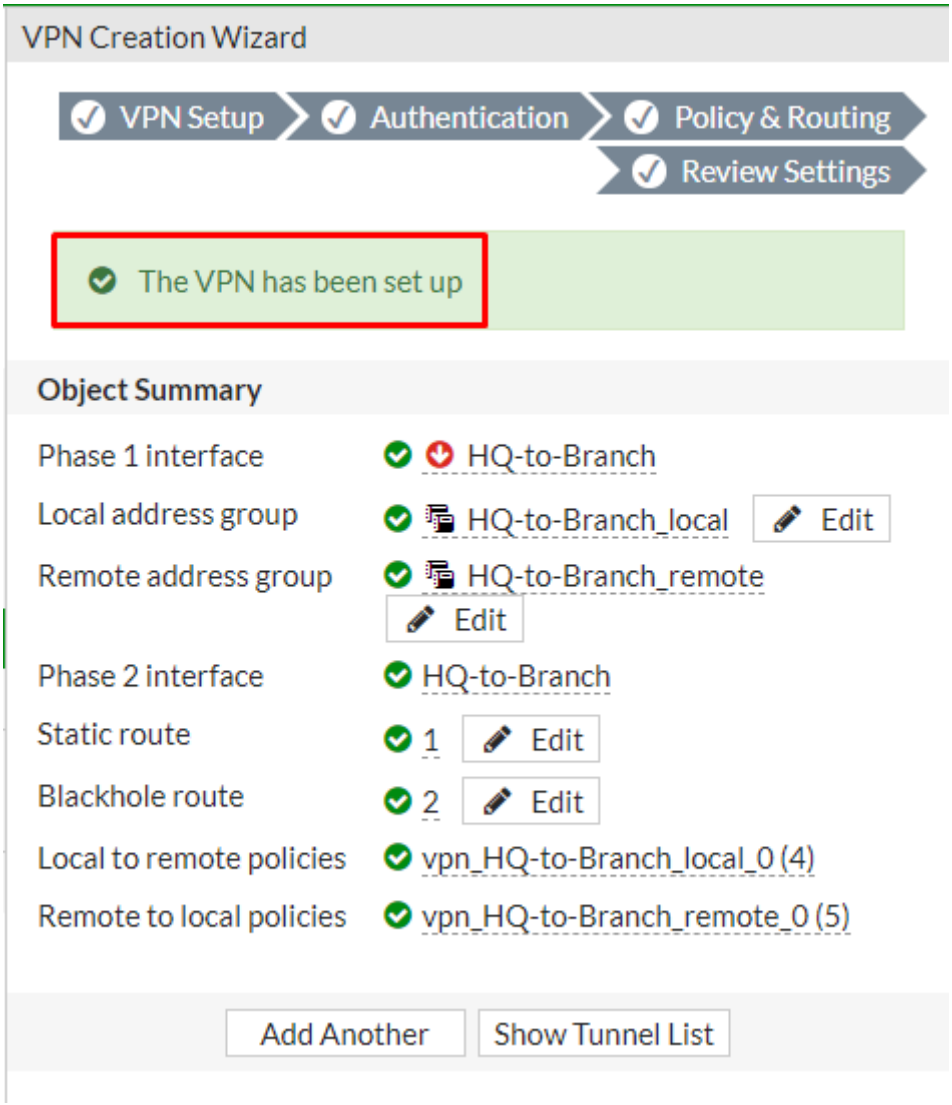
In the section of **Policy and Routing** set Local interface to **"LAN"** in my case **"Port1"** is dedicated to the LAN and local subnets will add automatically further then set **"Remote Subnets"** to the Branch network and set internet access to "**None"** as shown below



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



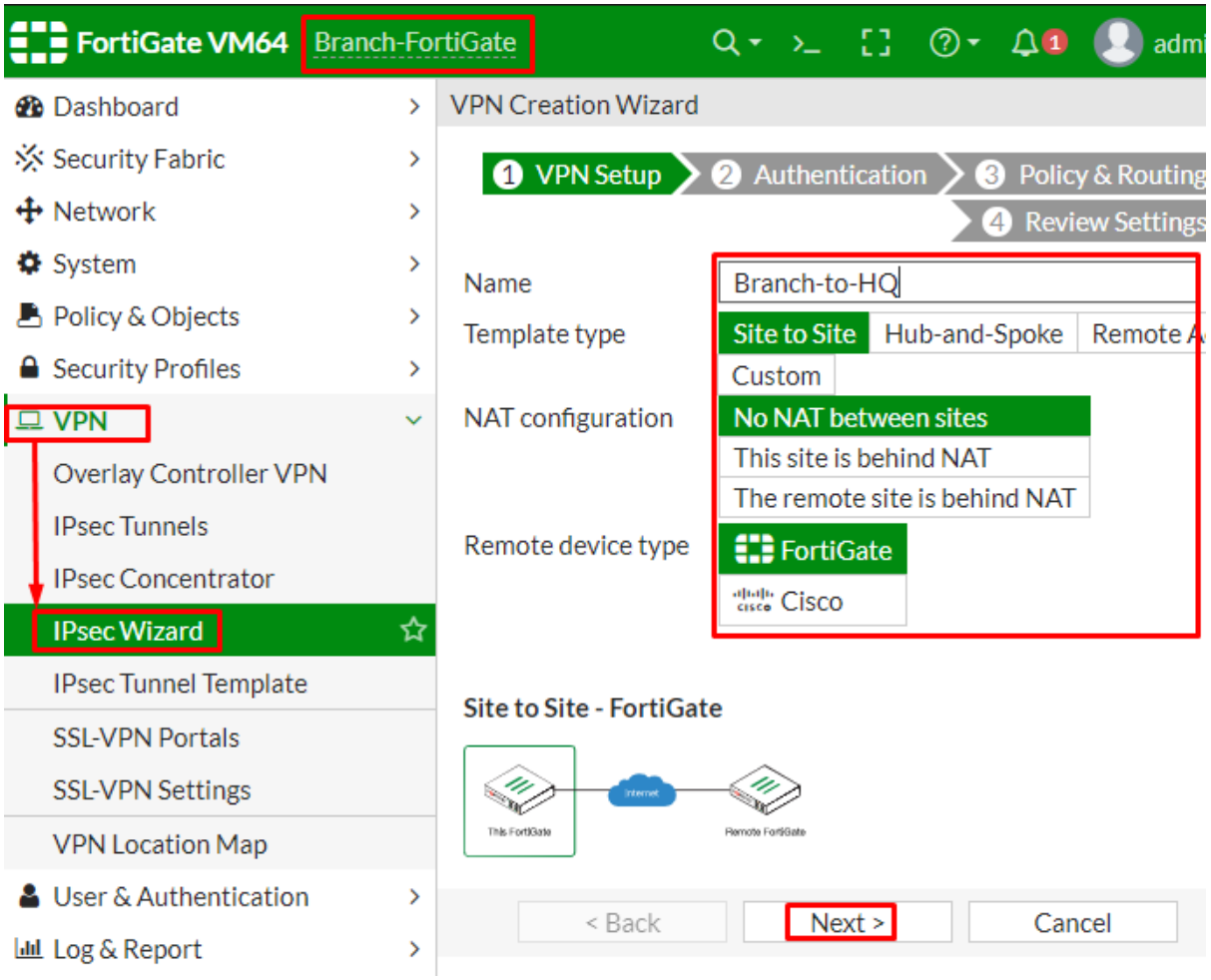
After creating the VPN, you can verify the details as shown below.



Configure IPsec VPN on a branch

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

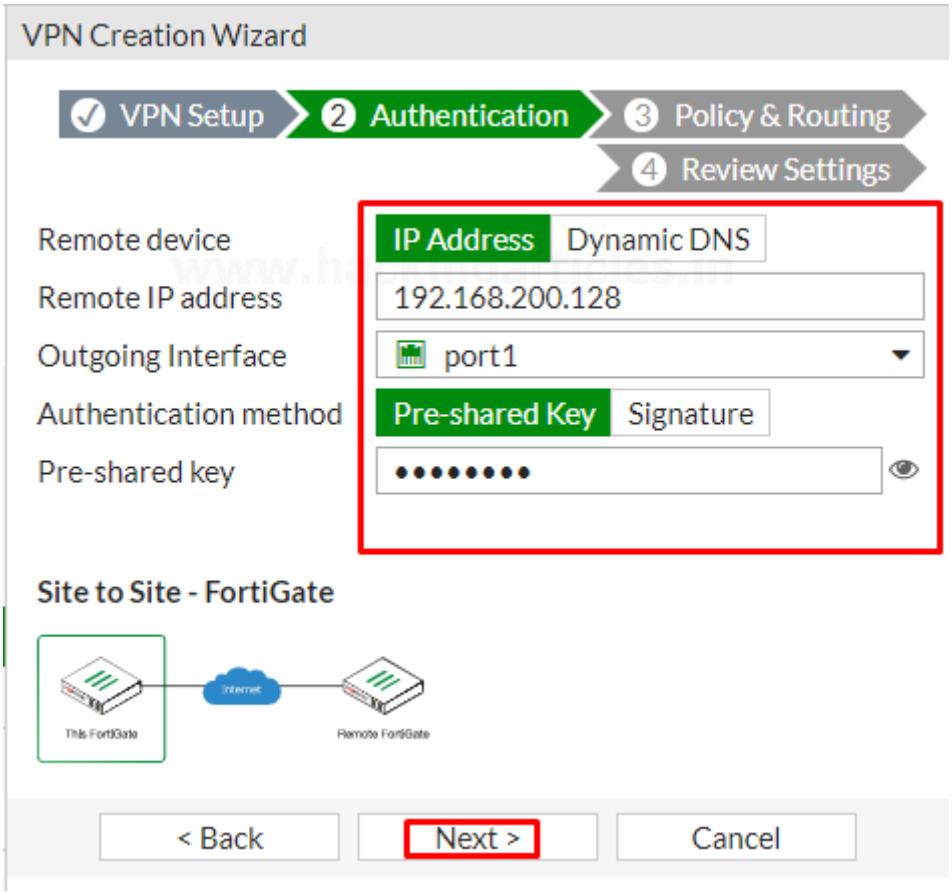
In the section, VPN setup describes a VPN name to make it identifiable, set Template type to Site-to-Site, set NAT configuration to "**NO NAT**" between sites and set Remote Device type to FortiGate.



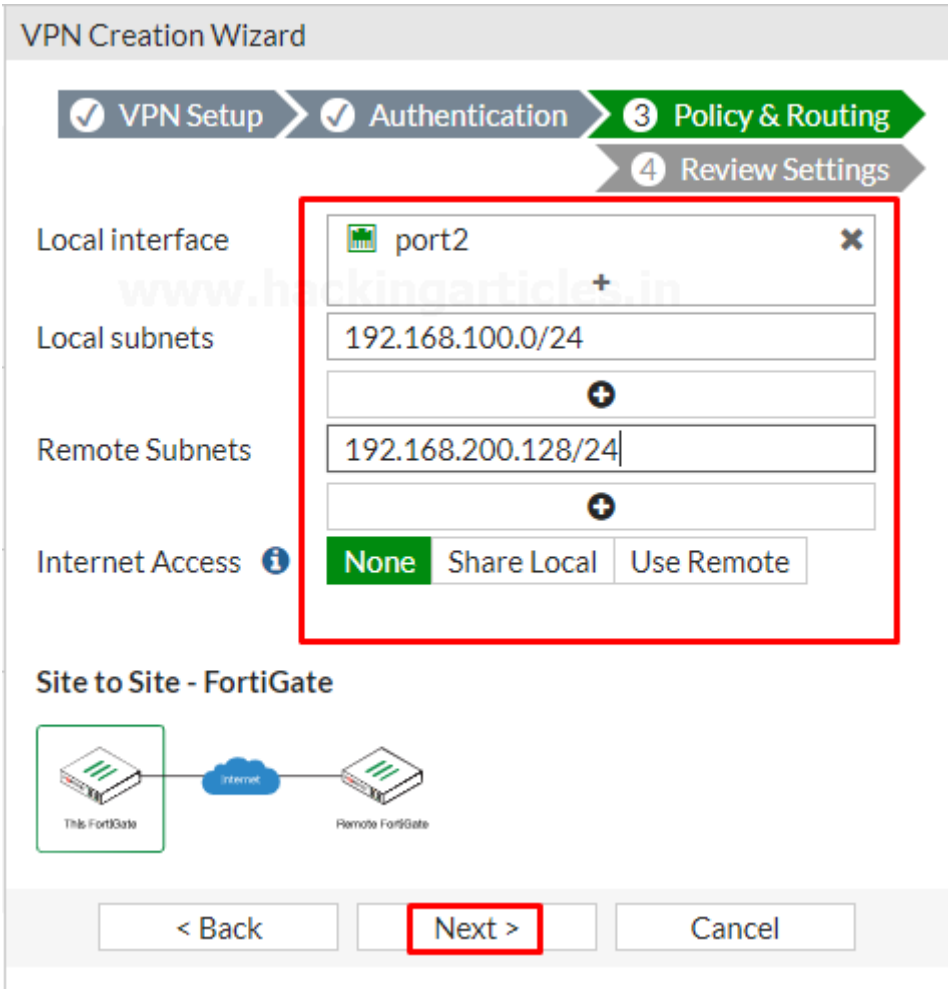
In the Authentication Section, set IP address to Public IP address of the Branch FortiGate.

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.

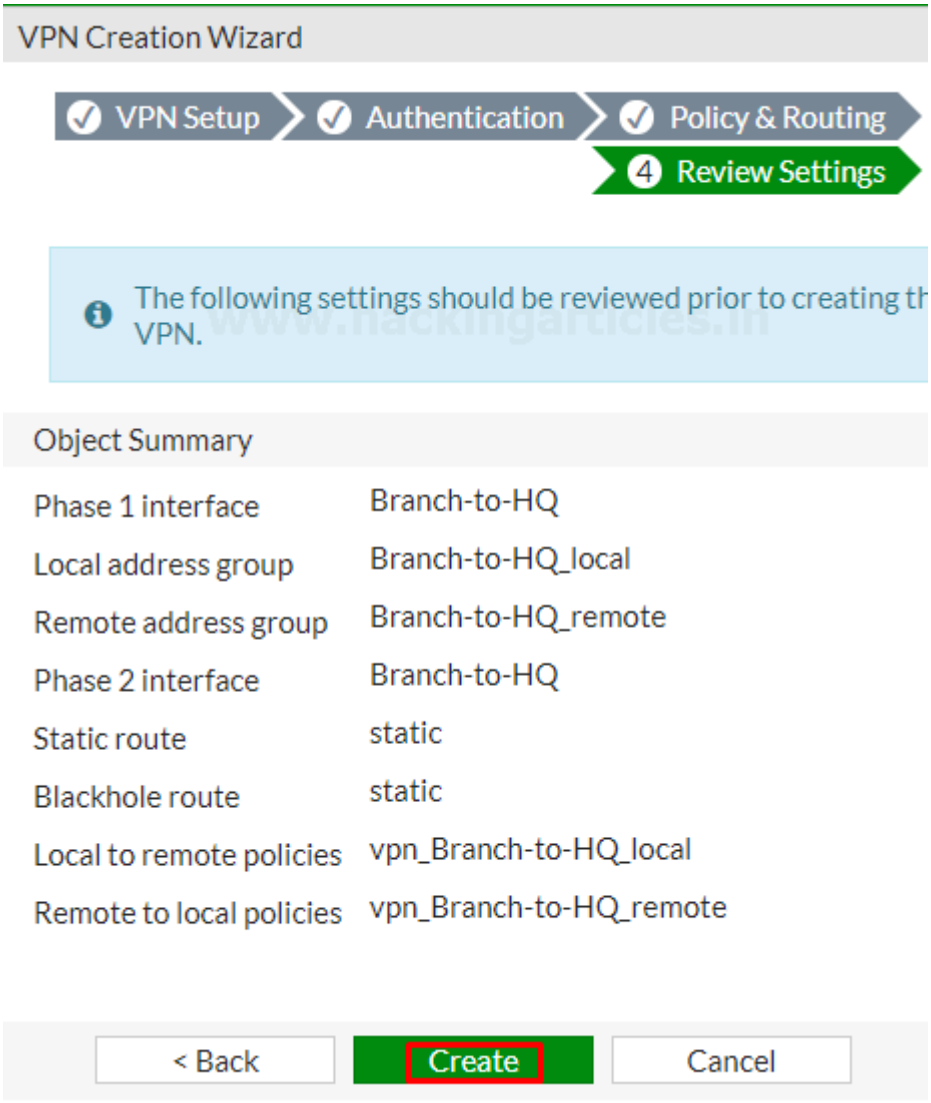
Set a secure **Pre-shared** key that was used on the VPN of HQ FortiGate.



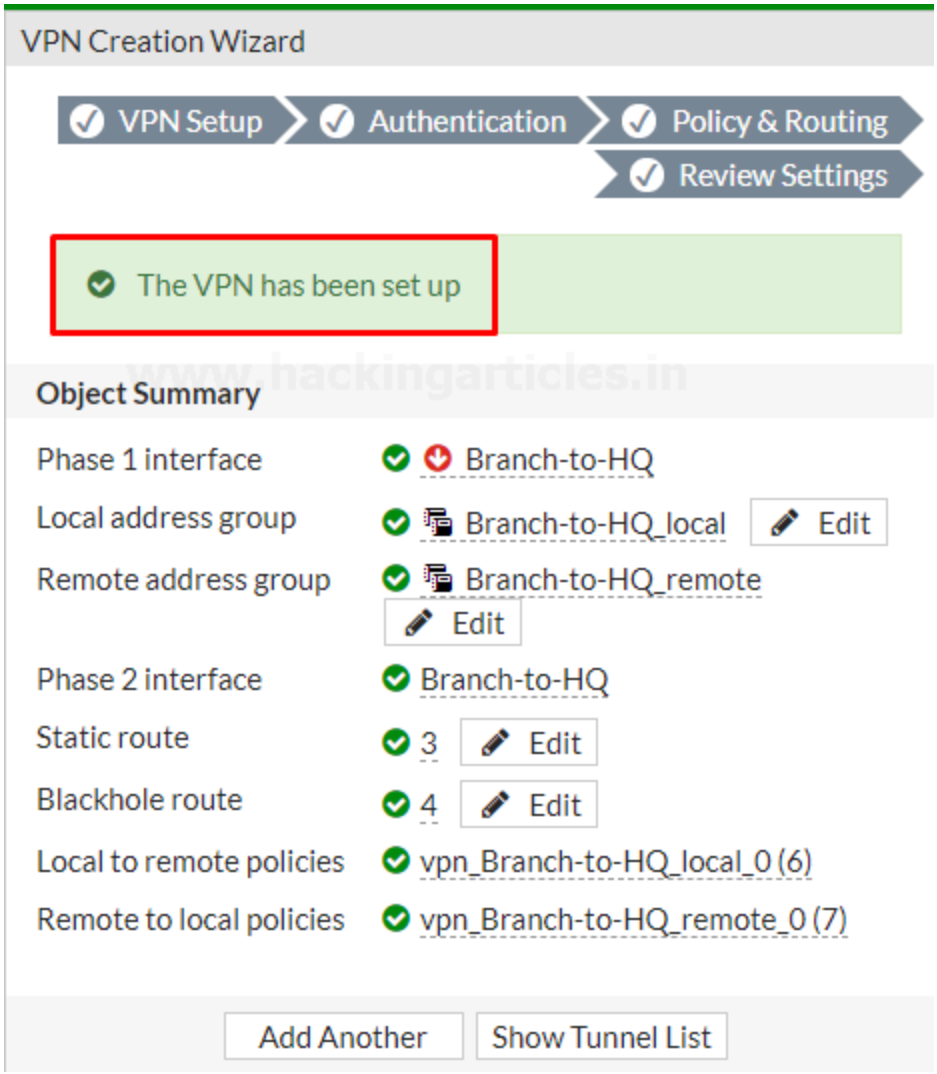
In the section of **Policy and Routing** set Local interface to **"LAN"** in my case **"Port2"** is dedicated to the LAN and local subnets will add automatically further then set **"Remote Subnets"** to the HQ (Headquarter) network and set internet access to "**None"** as shown below



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



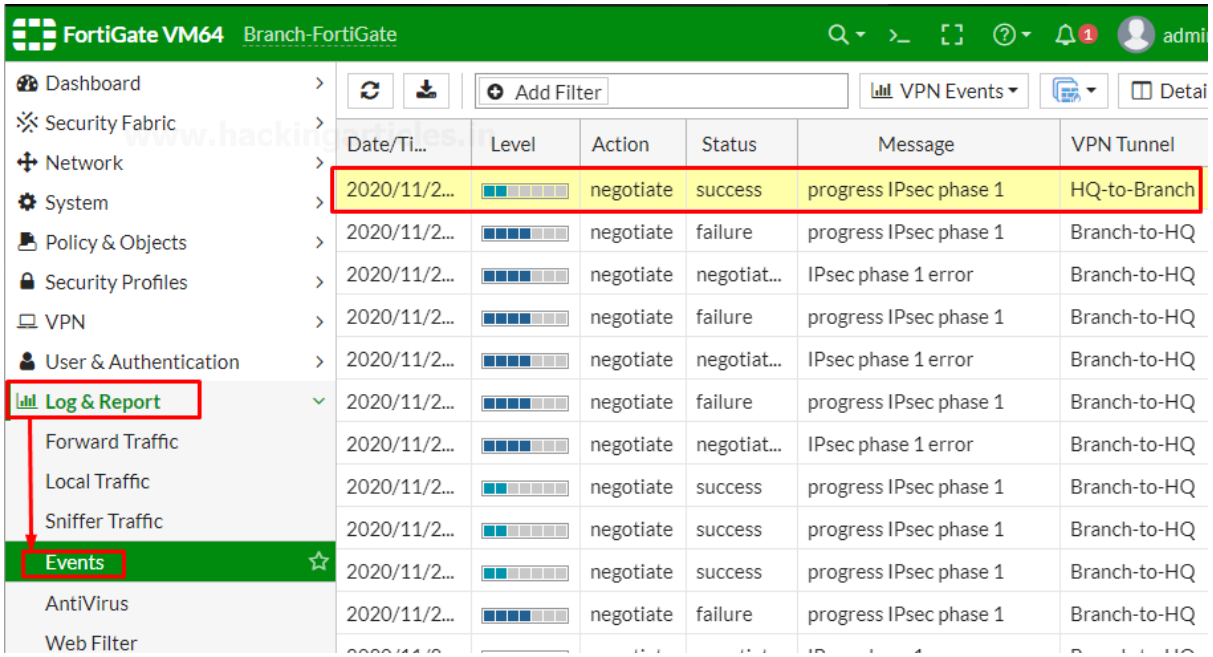
After creating the VPN, you can verify the details as shown below.



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.



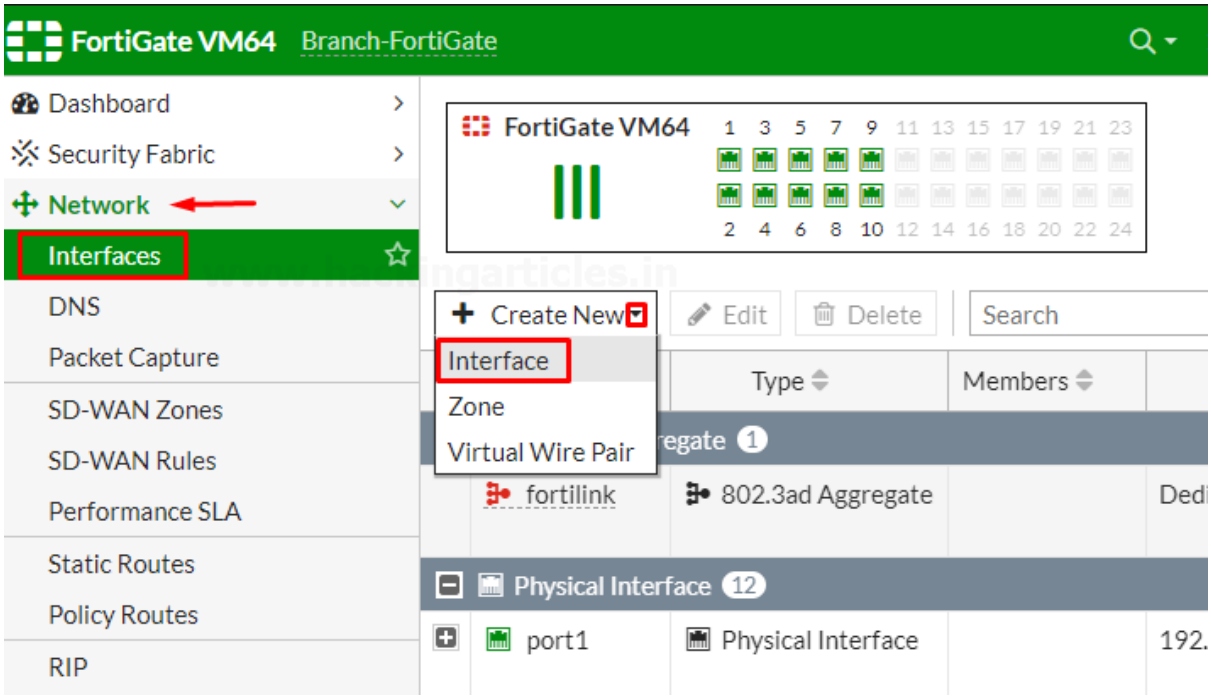
Simplifying Policies with Zone

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

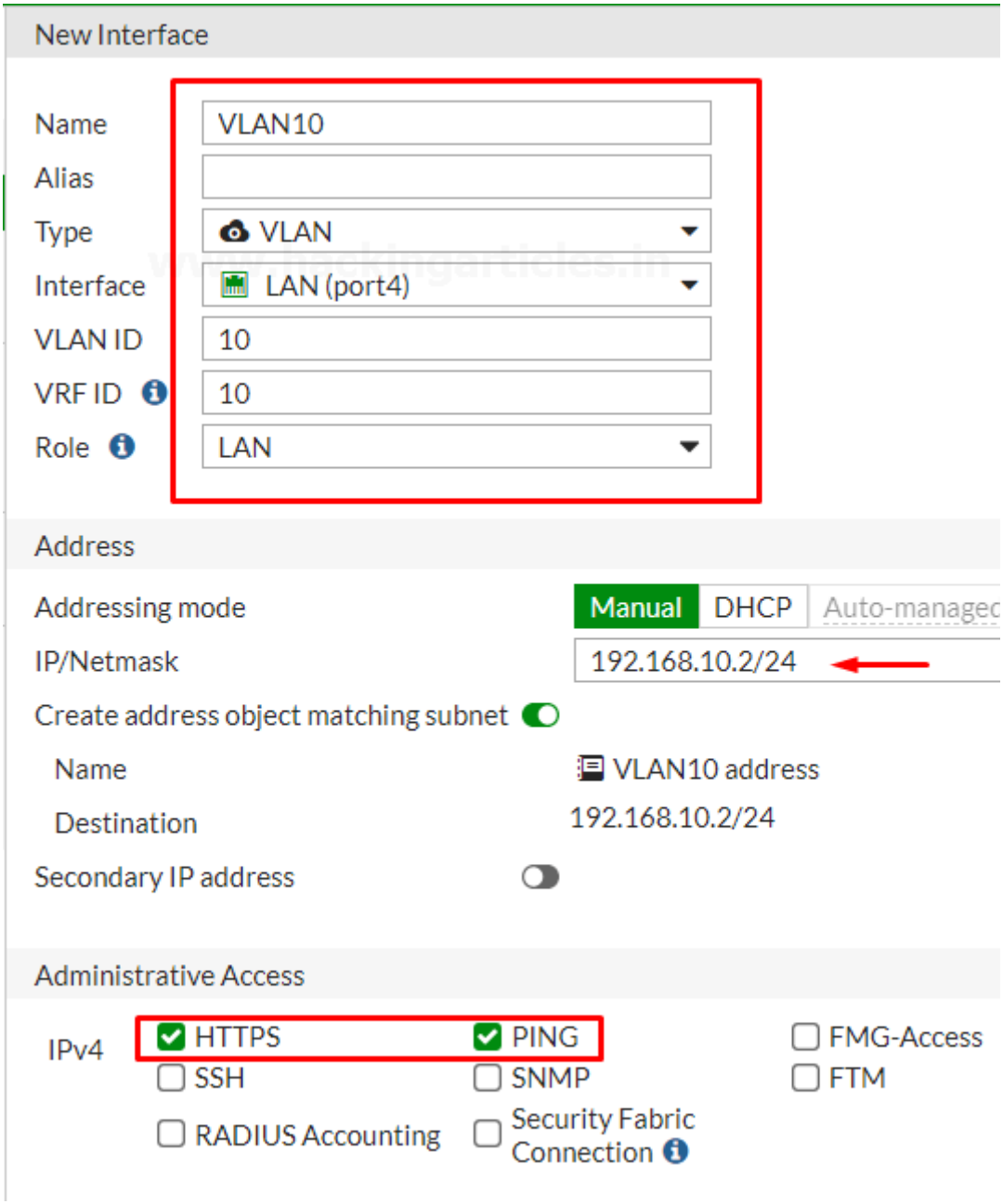
By creating multiple VLANs we are going to add them into a zone, so that we can just use the single zone object as a source interface in our firewall policy, rather than having to reference each interface separately.

Create VLAN Interfaces

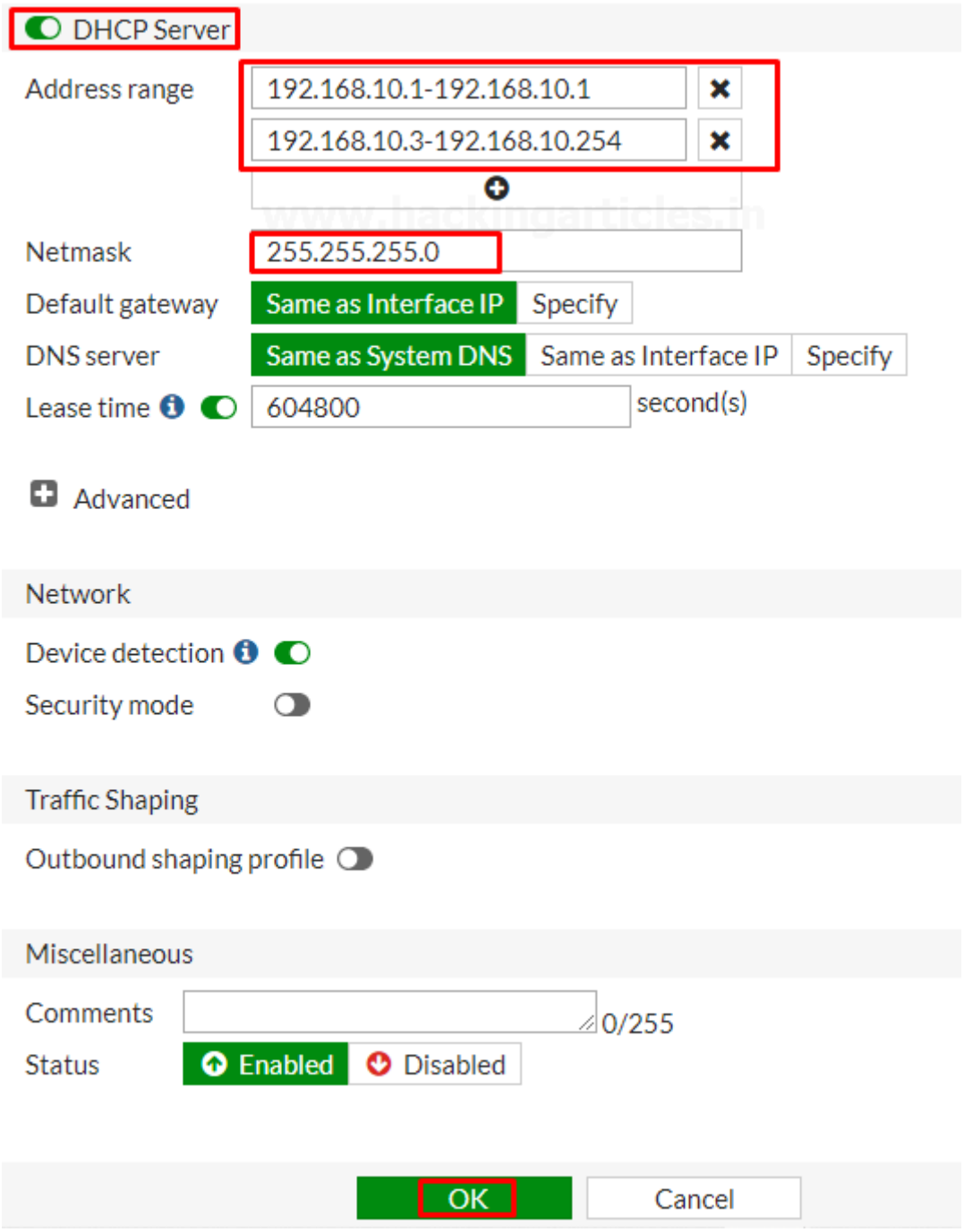
Go to Network > interfaces and create a new interface



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



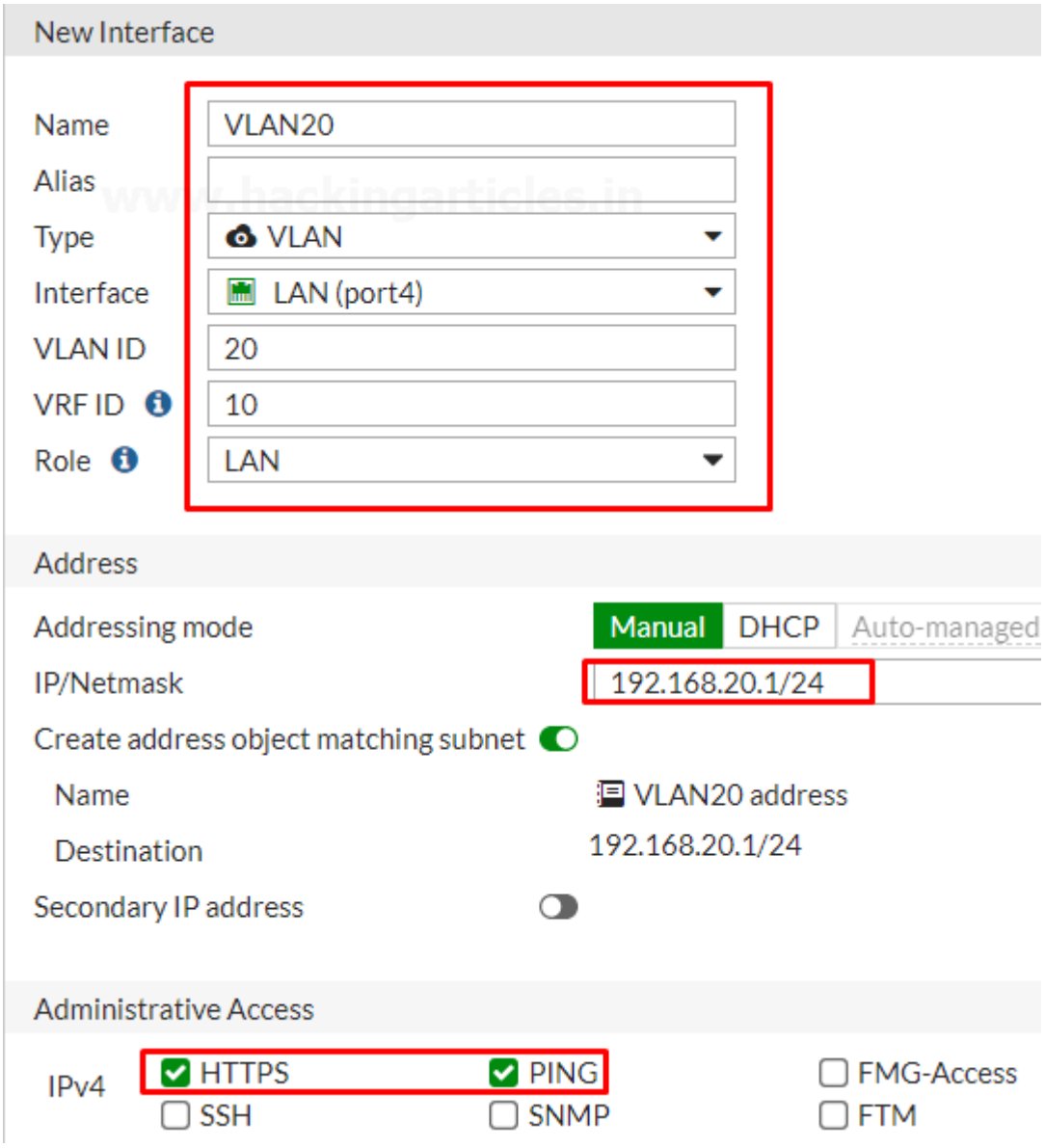
Enable the DHCP server and assign the address range further then save the configuration.



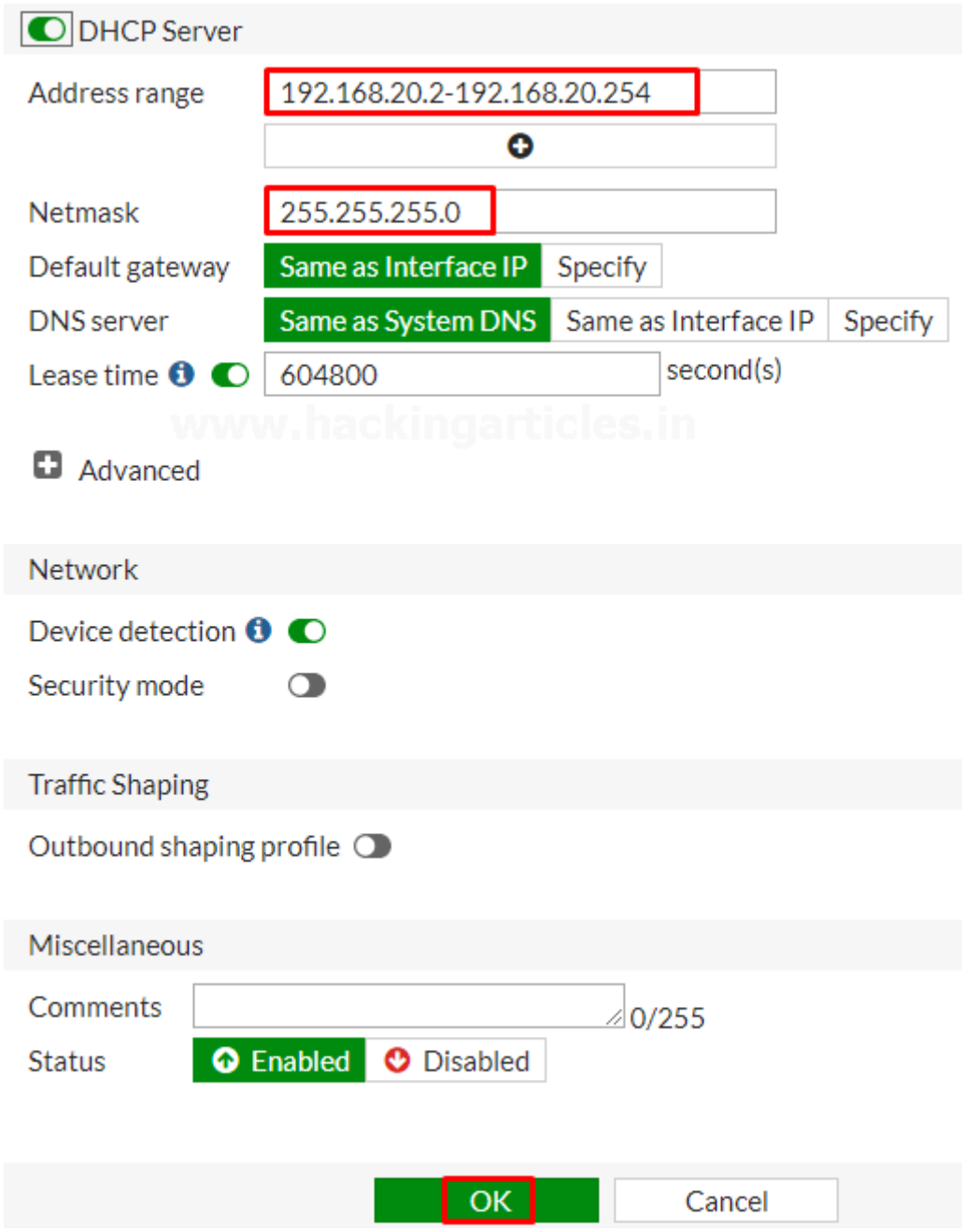
Next, create another by making the same selections…

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



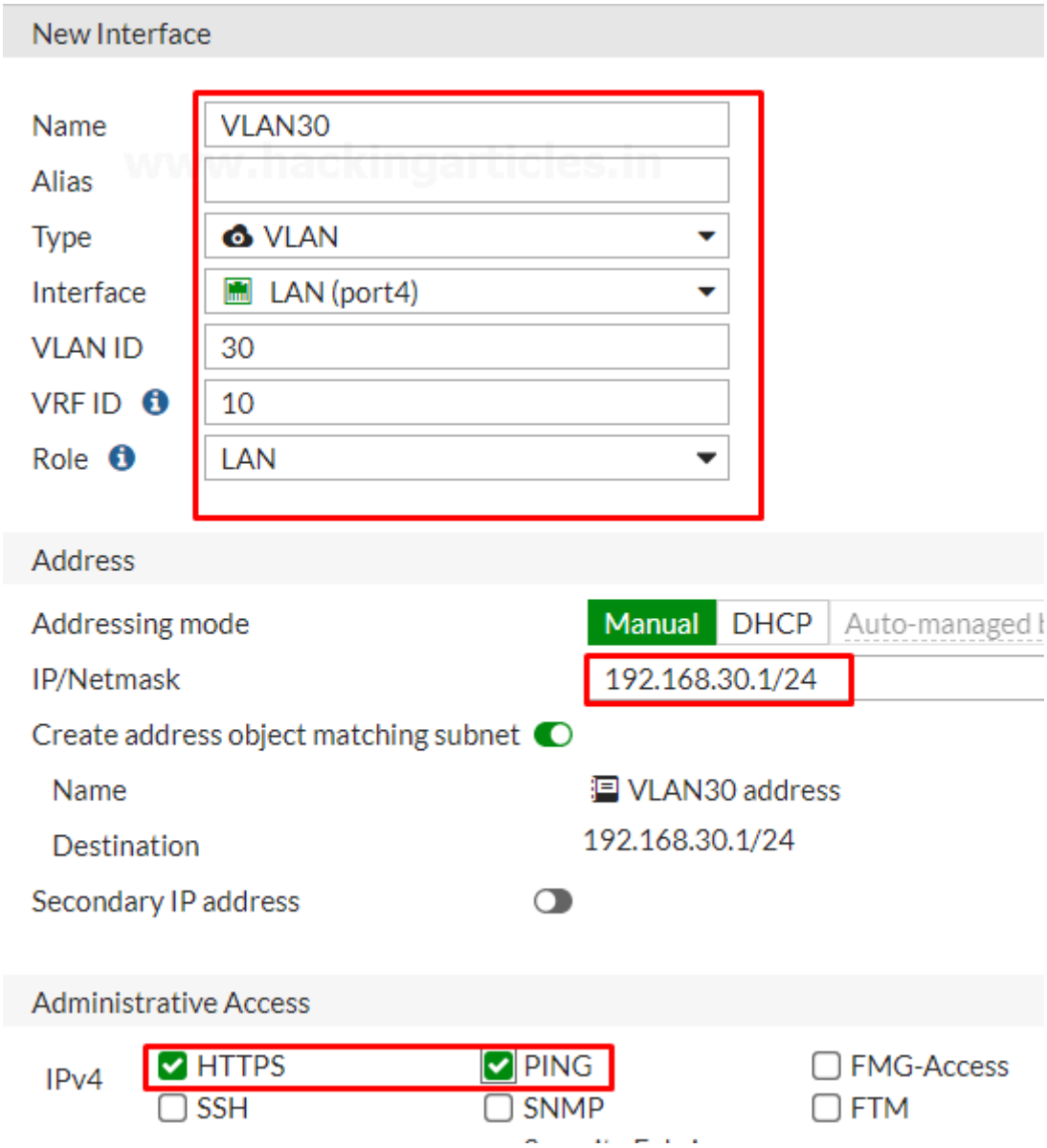
Enable the DHCP server and assign the address range further then save the configuration.



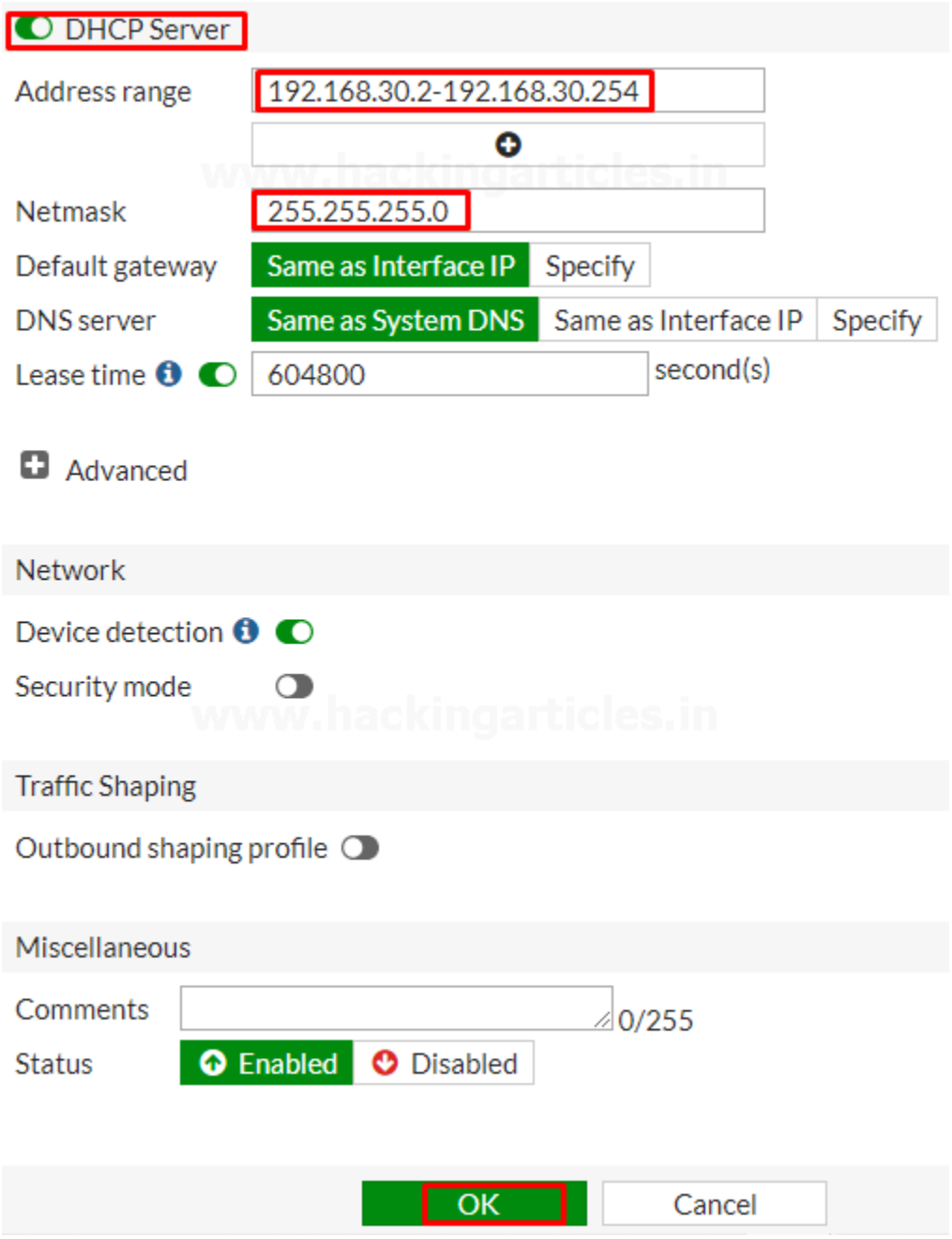
Finally, **create a 3rd VLAN** by making the same selection

Go to Network > interfaces and create a new interface.

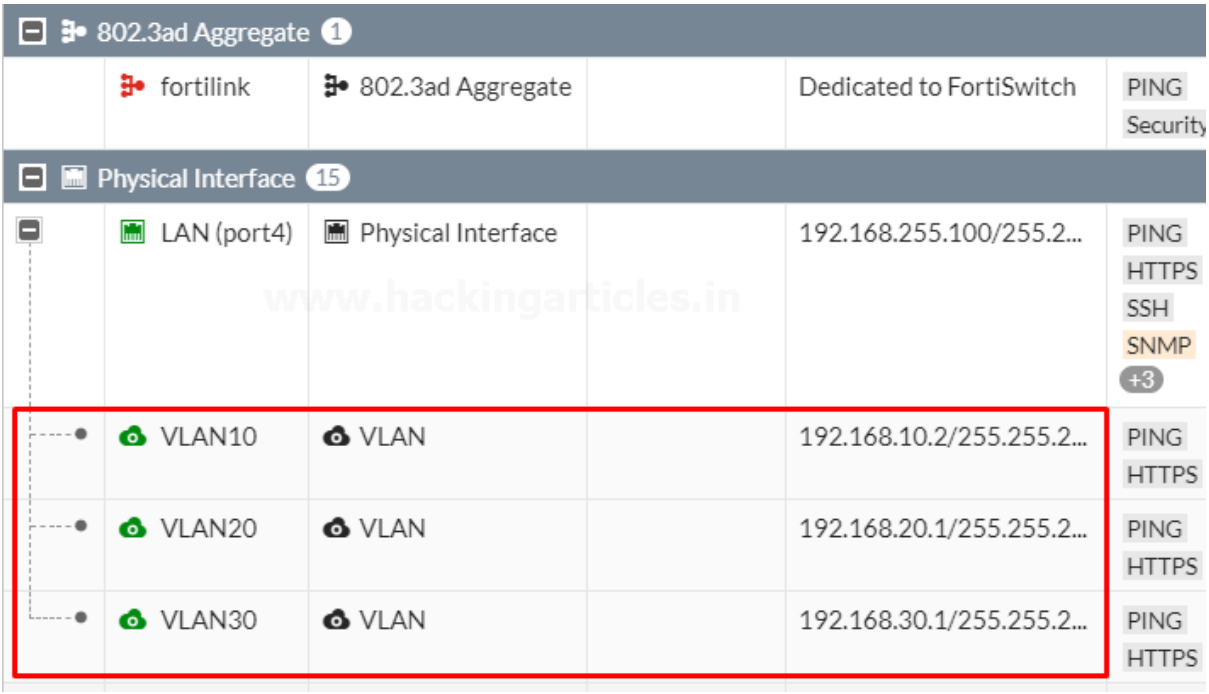
Enter the name for the interface VLAN30 or whatever you want, select the type to VLAN, select Interface to LAN, enter the VLAN ID, enter the VRF Id. assign the Role to LAN, set the Addressing mode to manual, enter the IP/Netmask provided by your ISP and select the Administrative Access to HTTPS, PING



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

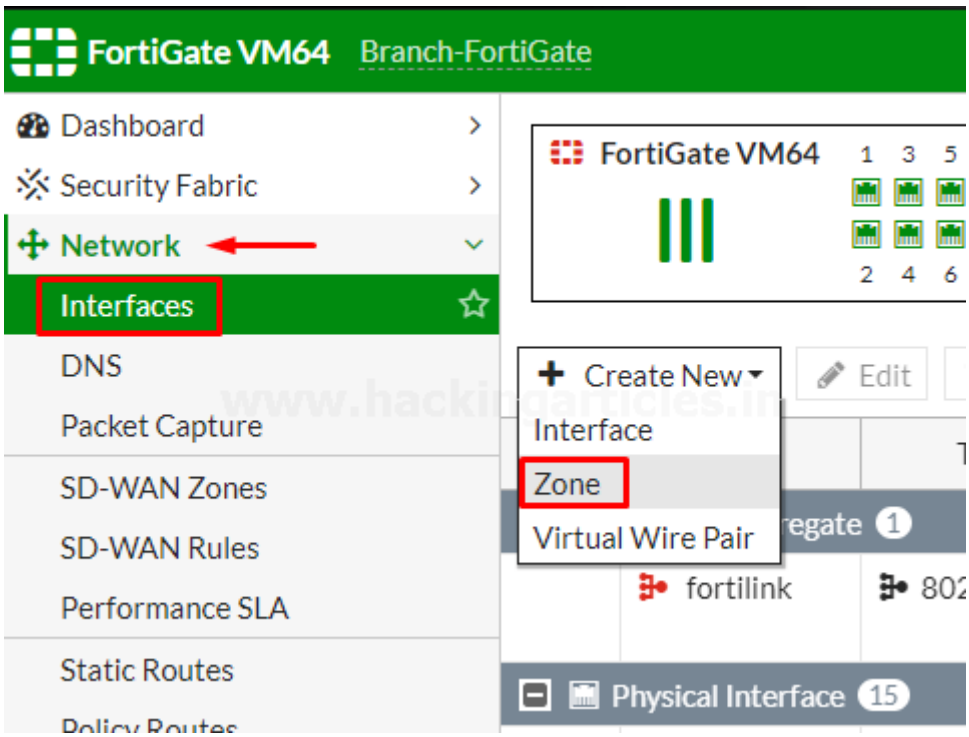


Review the Interface list to see the VLAN's that you have created

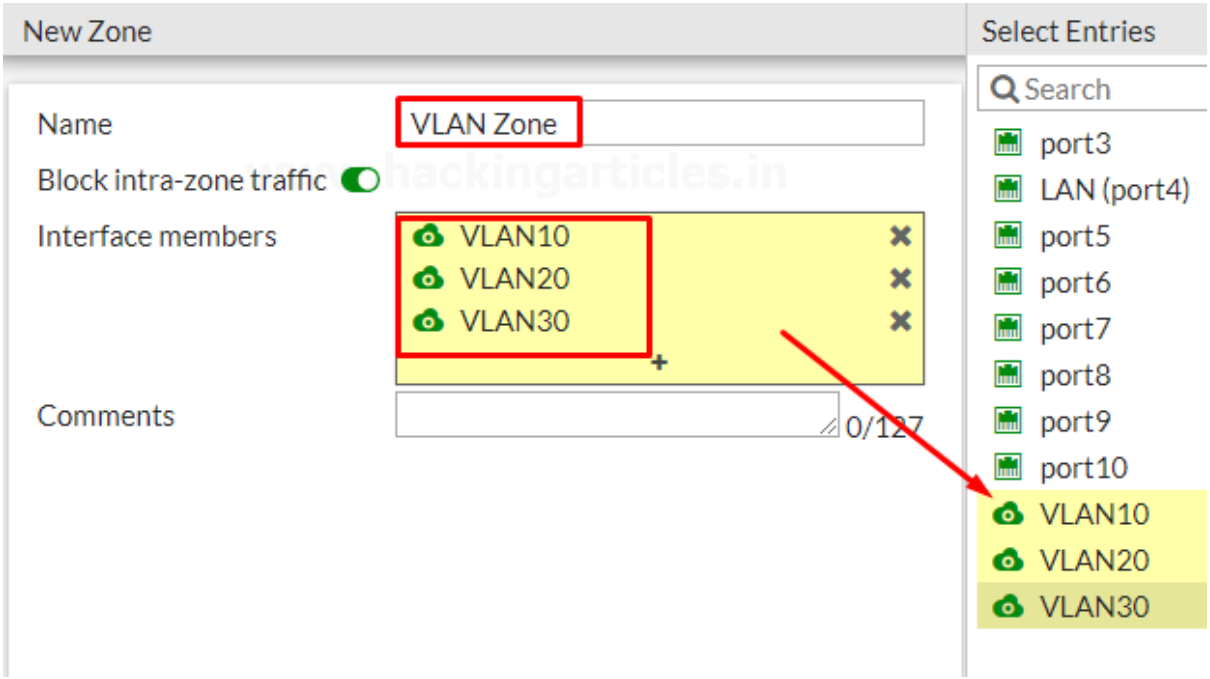


Create an Interface Zone

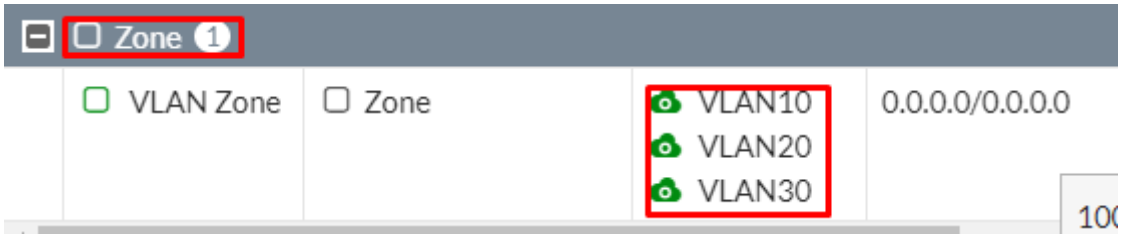
GO to the **Network > Interfaces** and select **create new Zone**



Name the zone to **"VLAN Zone"** to make it identifiable and add the newly created VLAN's to it as shown below.

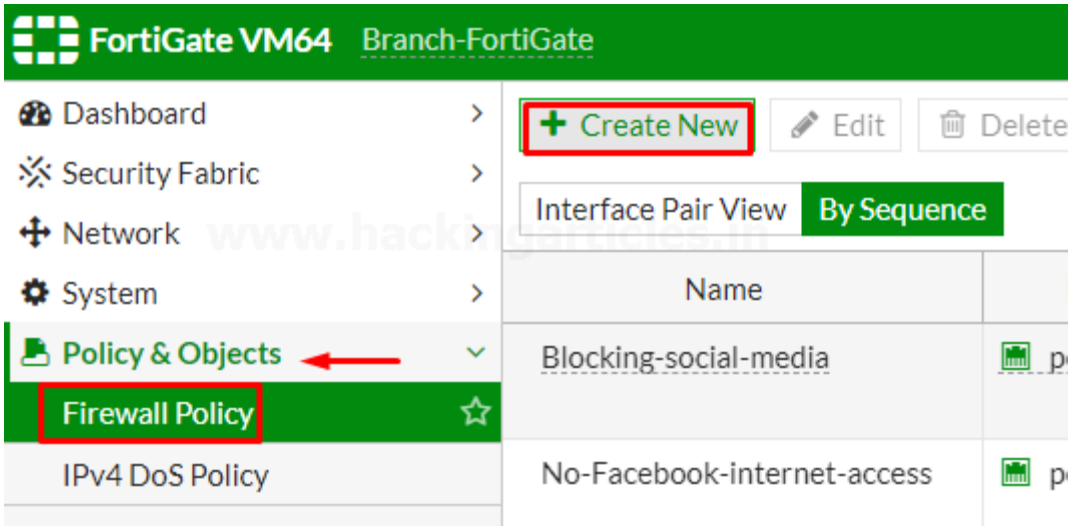


Review the Zone list to see the VLAN's that you have Added.

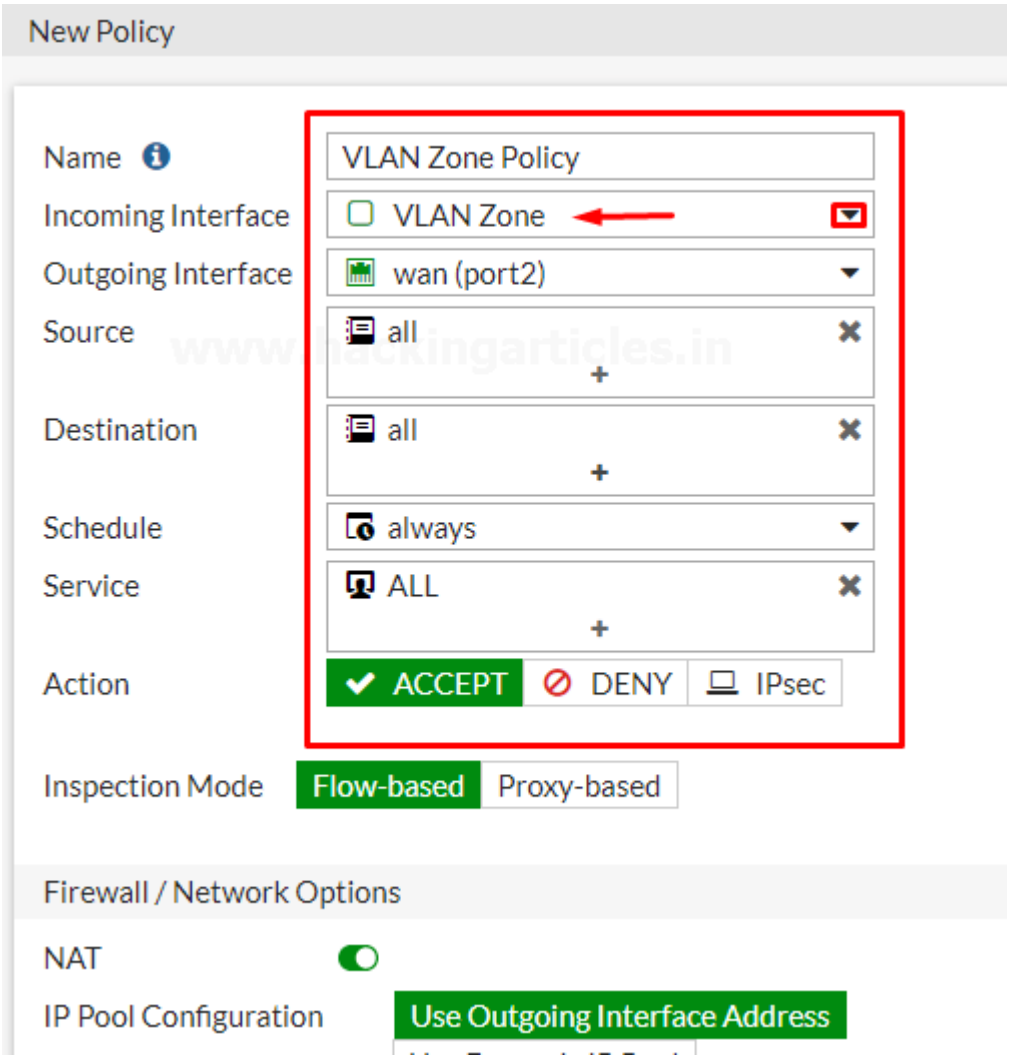


Create a Zone Firewall Policy

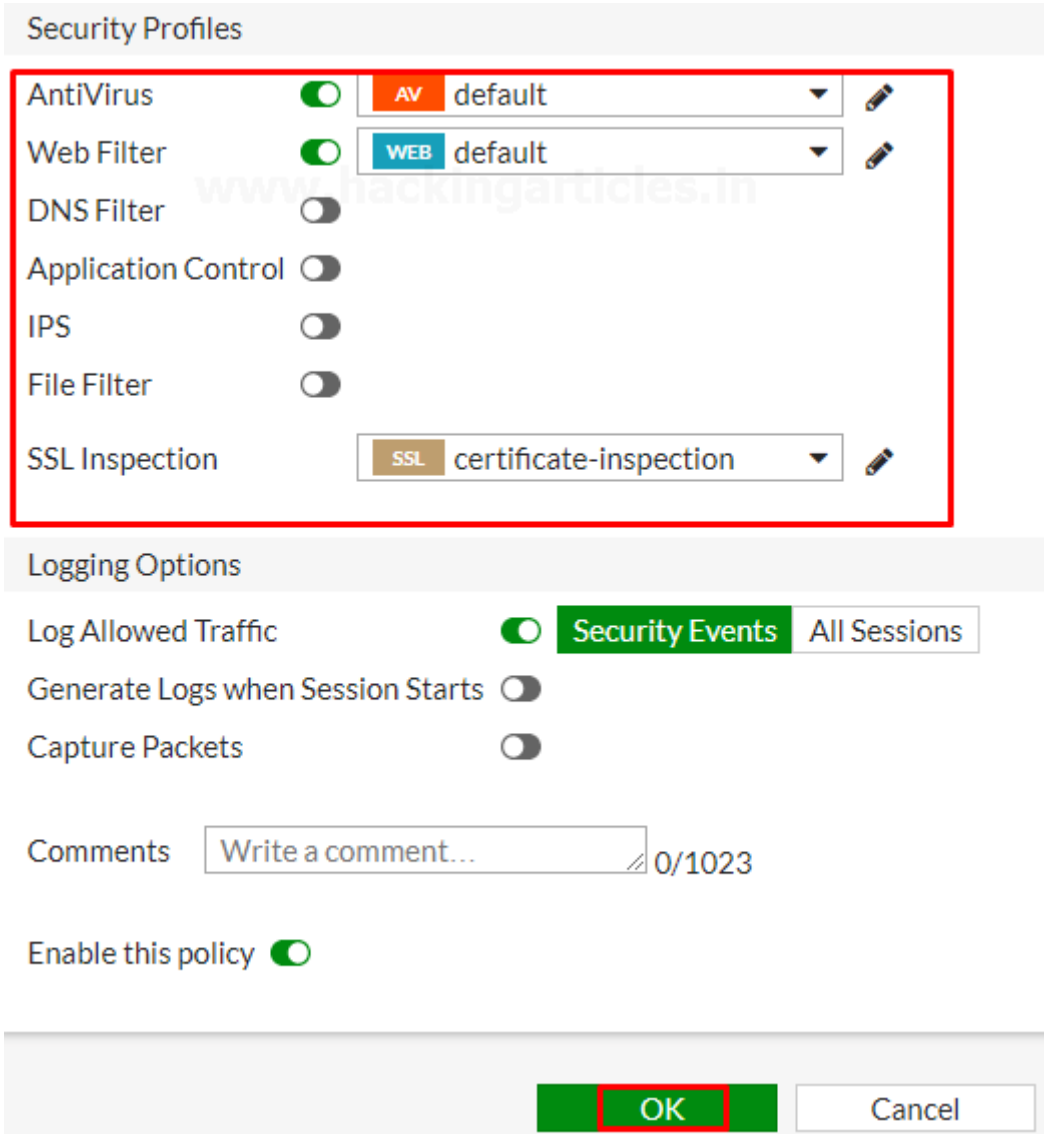
Go to Policy & Objects > Firewall Policy and create a new policy that will allow any VLAN in the Zone that we have created to access the internet.



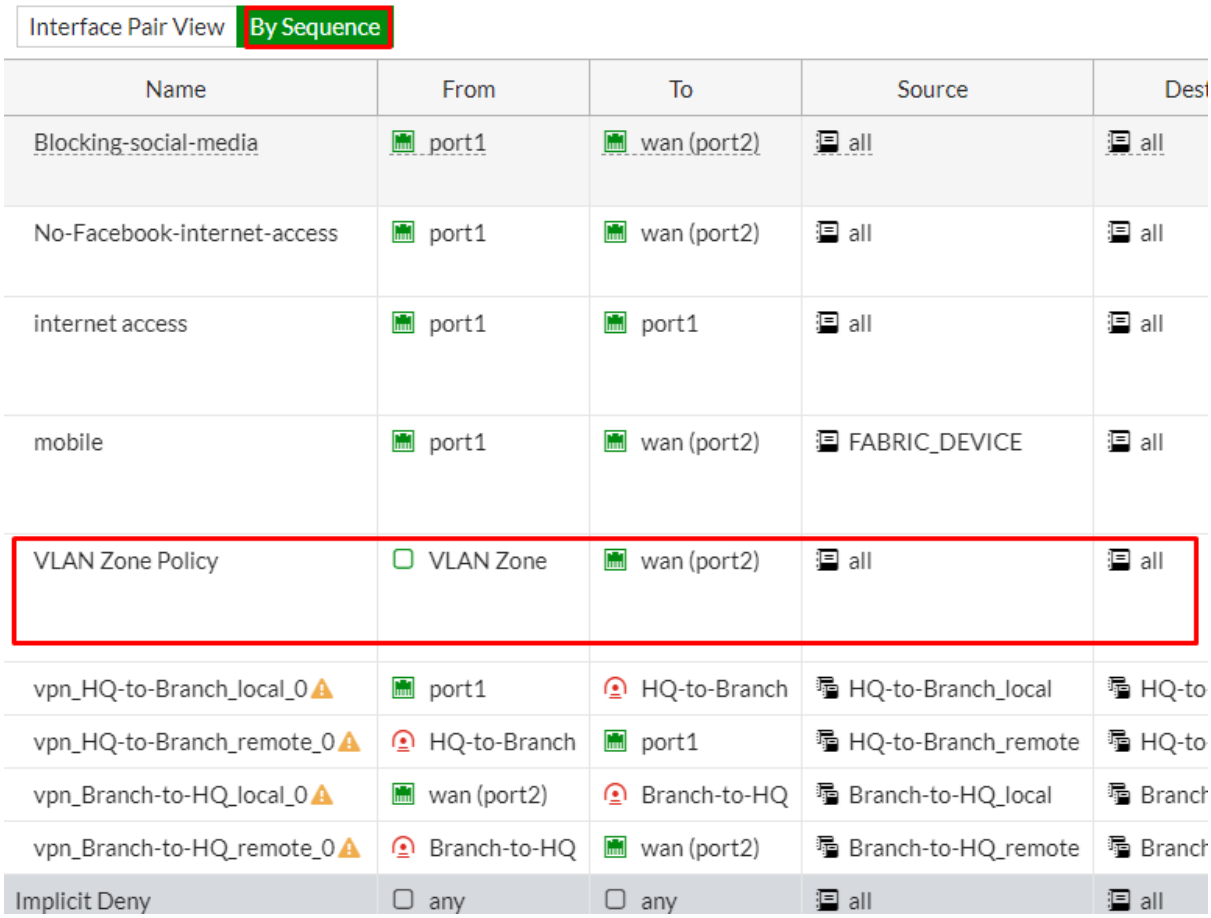
Assign a name to **"VLAN Zone Policy"** make it identifiable, set the **Incoming interface to your Zone** and the **outgoing interface to the internet-facing interface**. configure the rest as needed or as per your requirement.



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



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



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/