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

**How do firewall Works?**

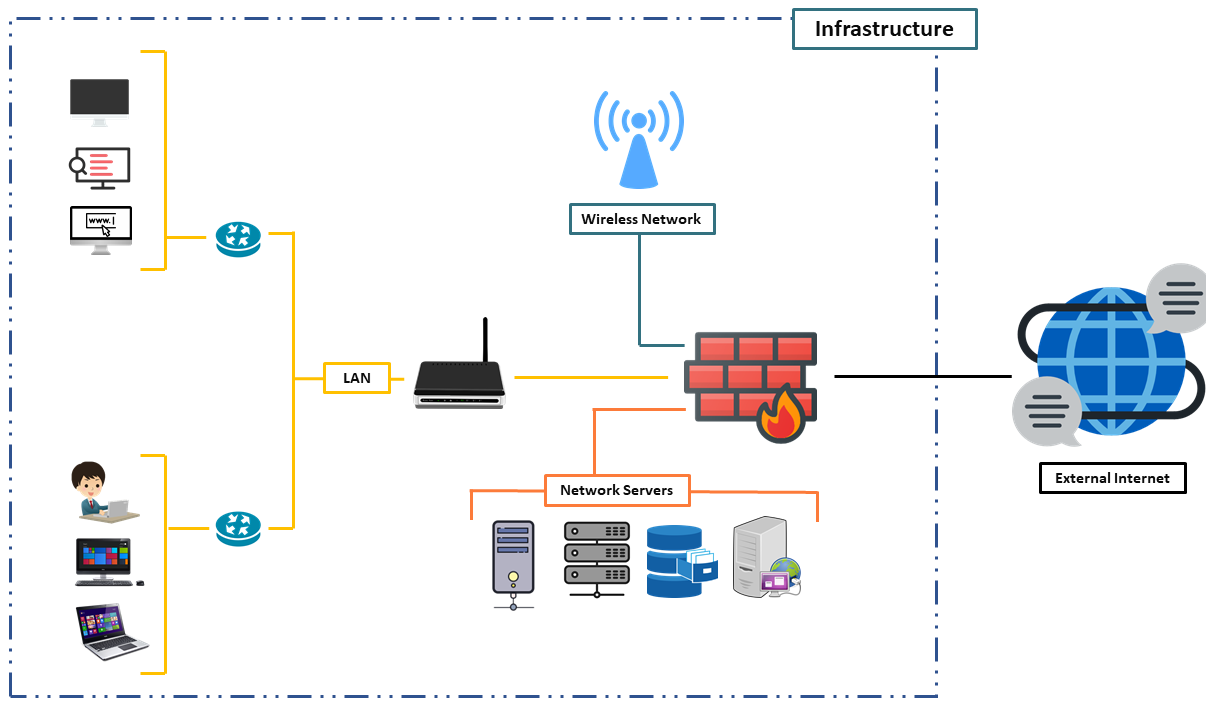
Basically, firewalls are divided into two parts

* 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.

**1. 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.

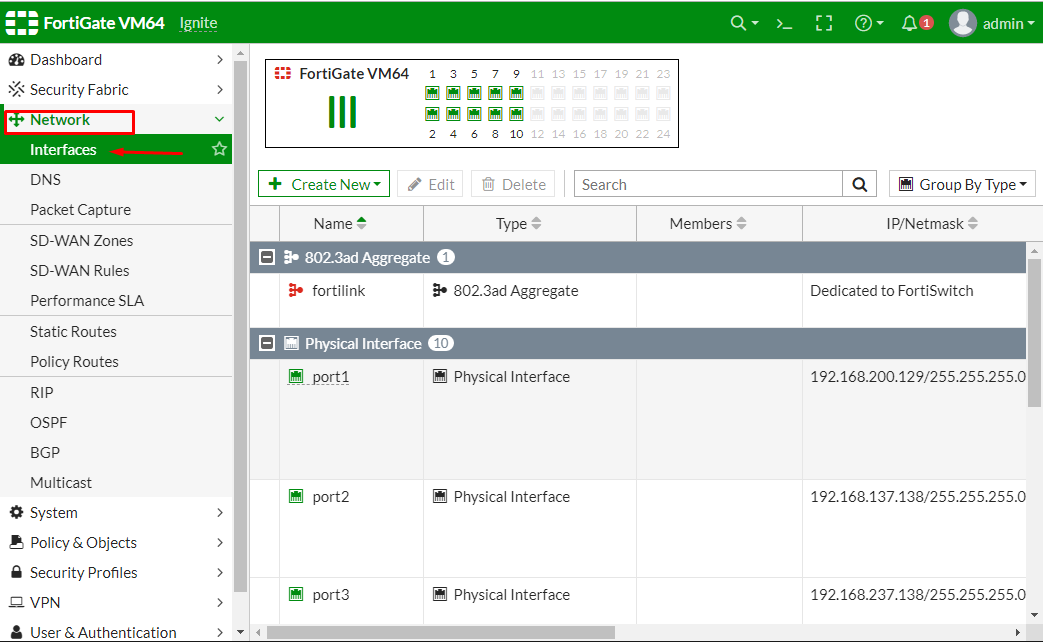
Connect the FortiGate internet facing interface usually WAN1 to your ISP supplied equipment and connect the PC to FortiGate using an internal port usually port 1 or as per your requirement.

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

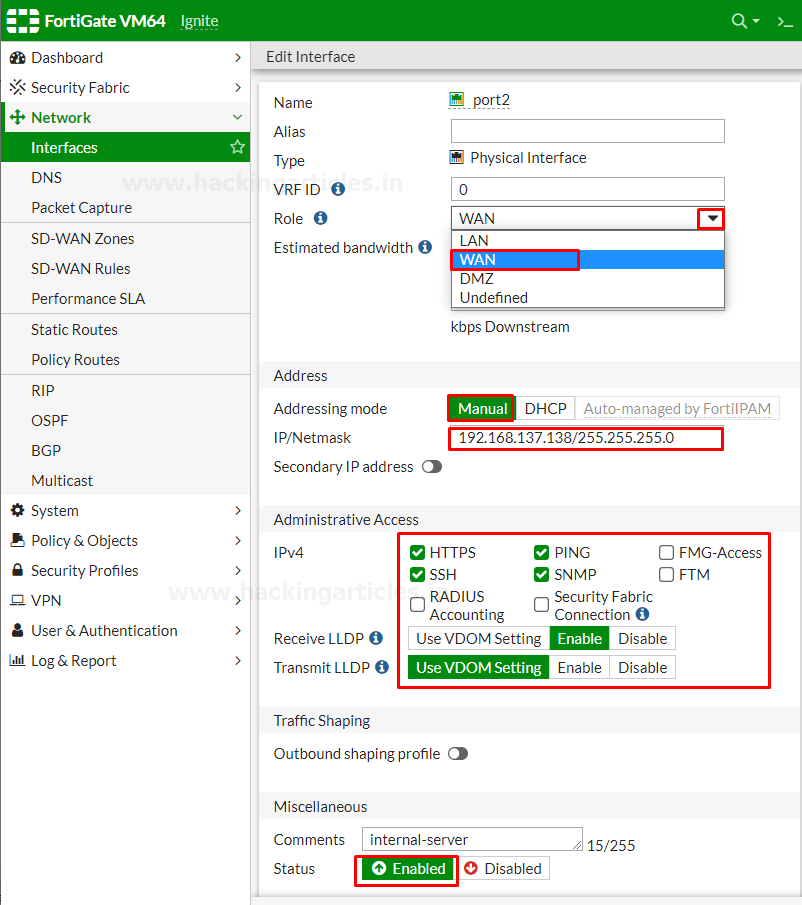
* 1. **Configure Network Interfaces**

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

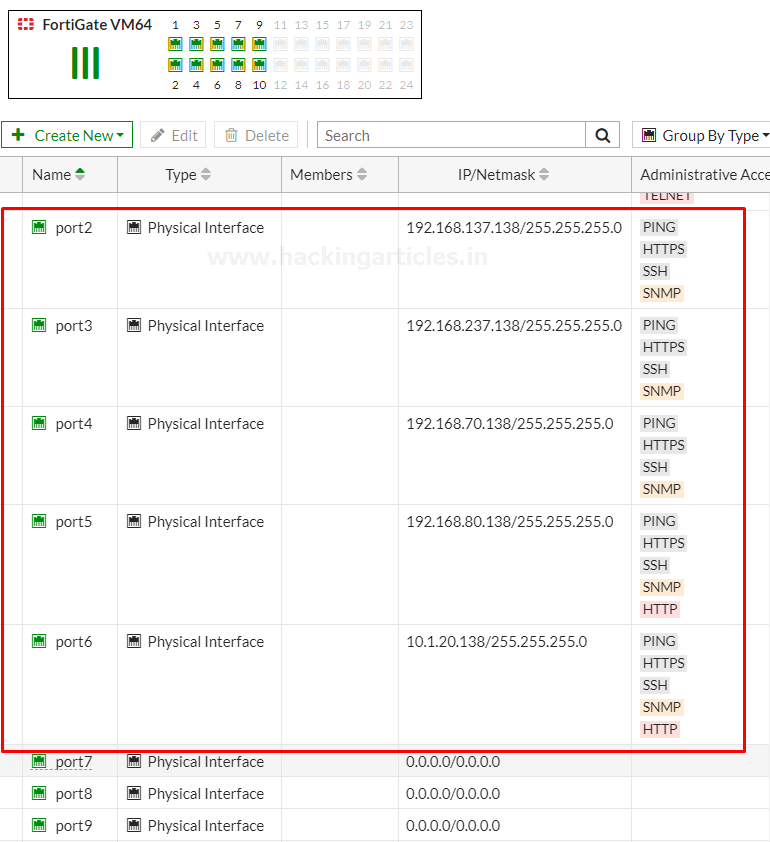
**Go to network > Interfaces**



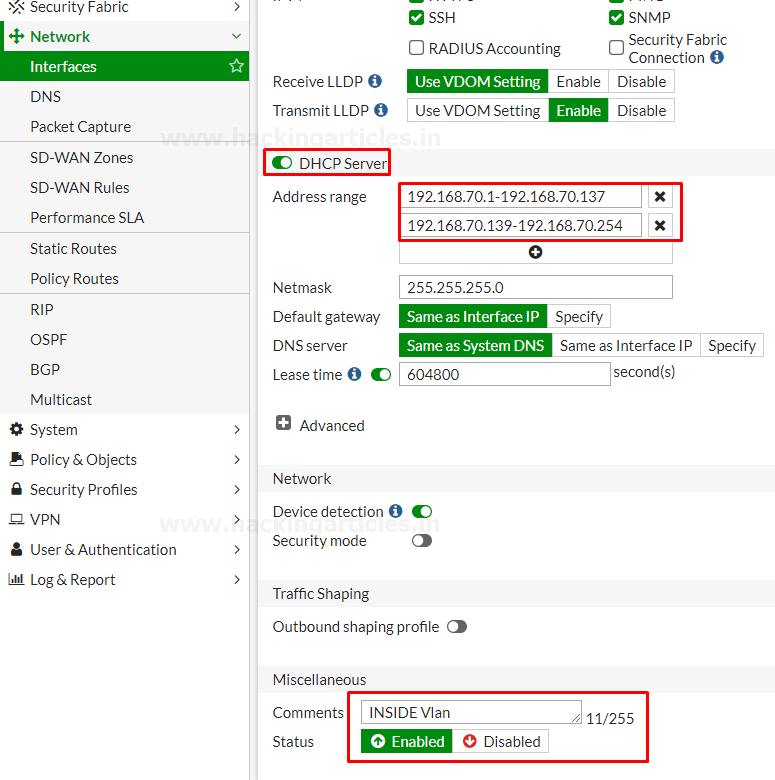
and edit the internet-facing interface set the addressing mode to manual and the IP/Netmask to the public IP address provided by your ISP. Here in my case, I’m considering port2 as an internet-facing interface. Provide Administrative access as per your requirement to the network



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



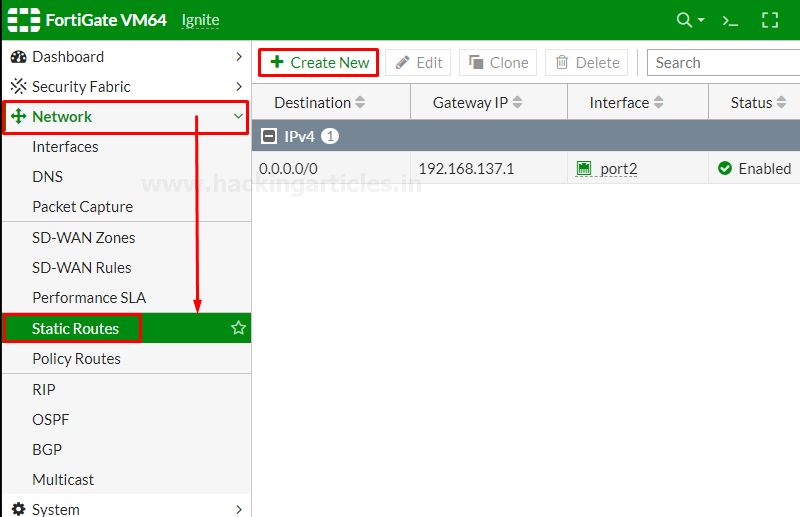
If you need your FortiGate to provide IP addresses to devices connected to internal network enable the DHCP server and then save the configuration as shown below.



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.

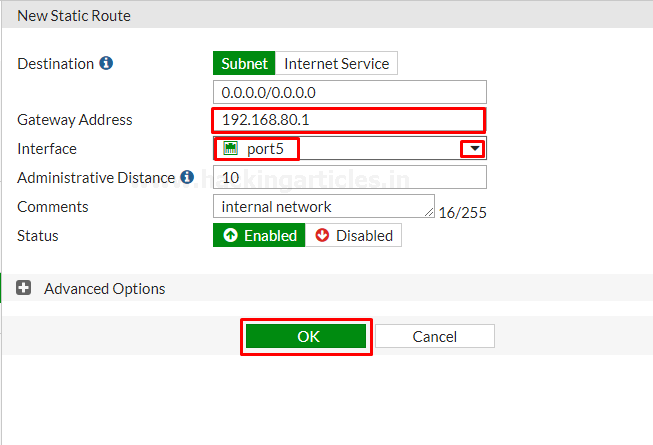
* 1. **Add a Default Route**

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



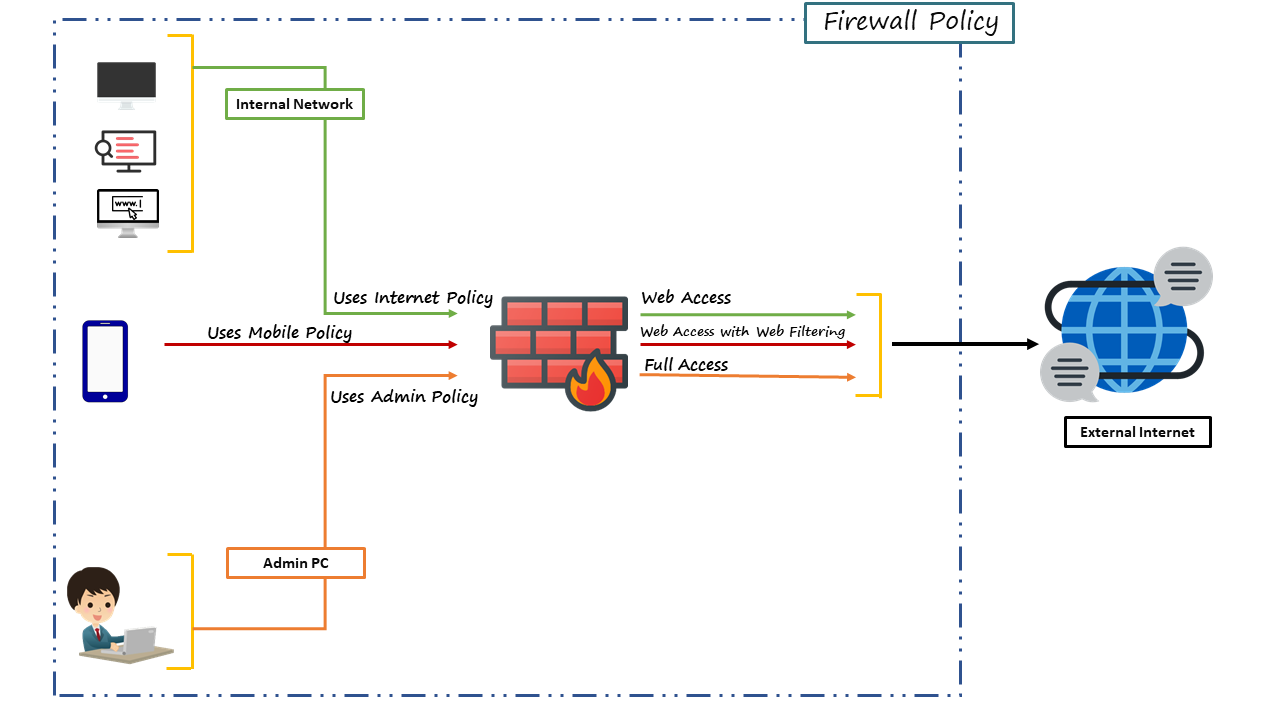
Set destination to subnet and enter IP/Netmask of Eight Zeros. Set the Gateway to the Gateway IP

provided by your ISP and the interfaces to the internet-facing interface then save the Route.

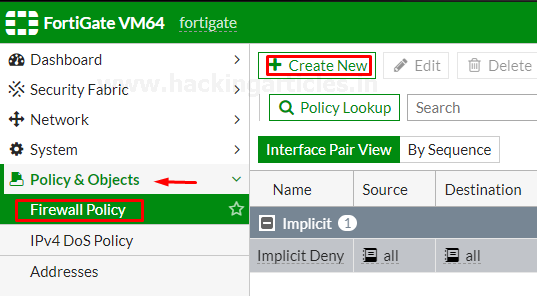


* 1. **Create an IPV4 Firewall Policy**

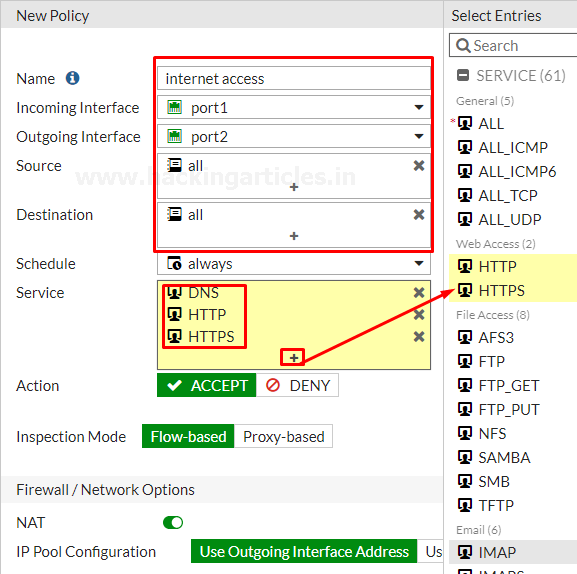
Firewall policy designed in a manner to examine Network Traffic using policy statements to block unauthorized access while permitting authorized communication.



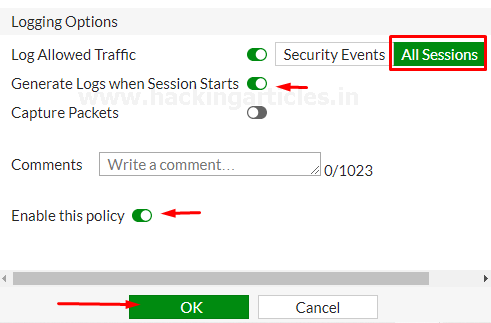
Go to **Policy & Objects > Firewall Policy** and **create** a new policy which allow internet traffic through the FortiGate.



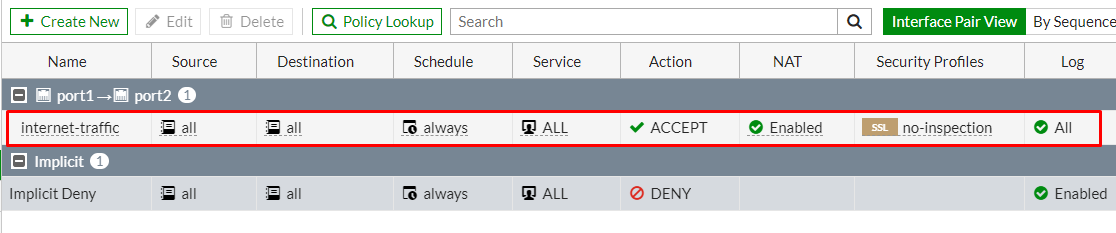
Name the policy as **“Internet-Traffic”** or whatever you want. Set the incoming interface to the **“Internal interface”** and outgoing interface to the internet facing interface. Set the rest to allow **“ALL”**  Traffic or you can select multiple rules by selecting **the + icon** and the action to **“Accept”**enable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



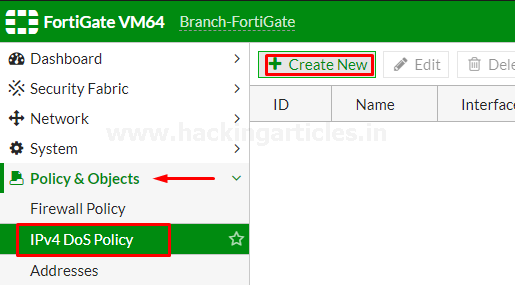
As you can see the policy successfully enabled.

* 1. **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.

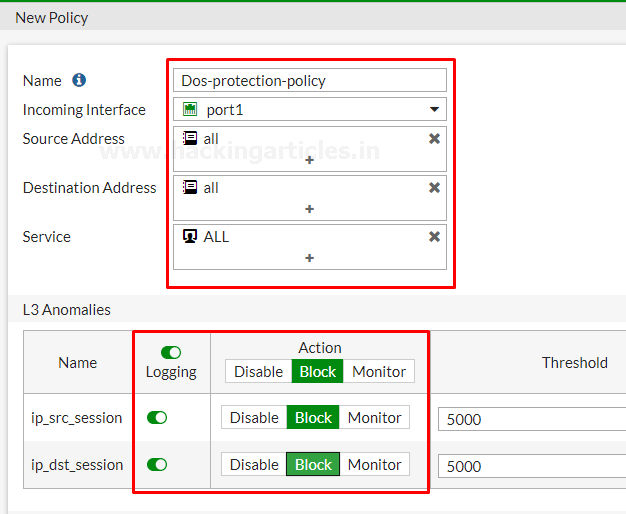
The breakup of traffic anomalies table is divided into 2 parts.

* 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

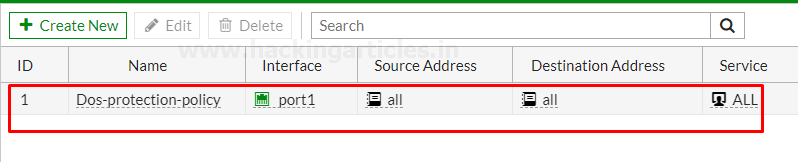


It all your choice whether or not to enable this policy and default is enabled. Here in our case, we have blocked some of the actions with the limited threshold values to check whether these policies working or not.

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.



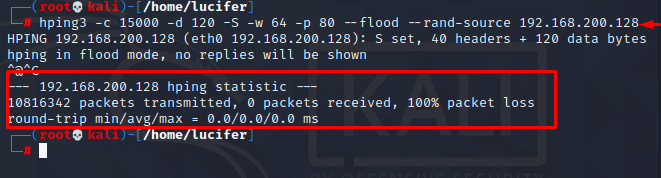
As we can see Dos-protection-Policy is successfully deployed.

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

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

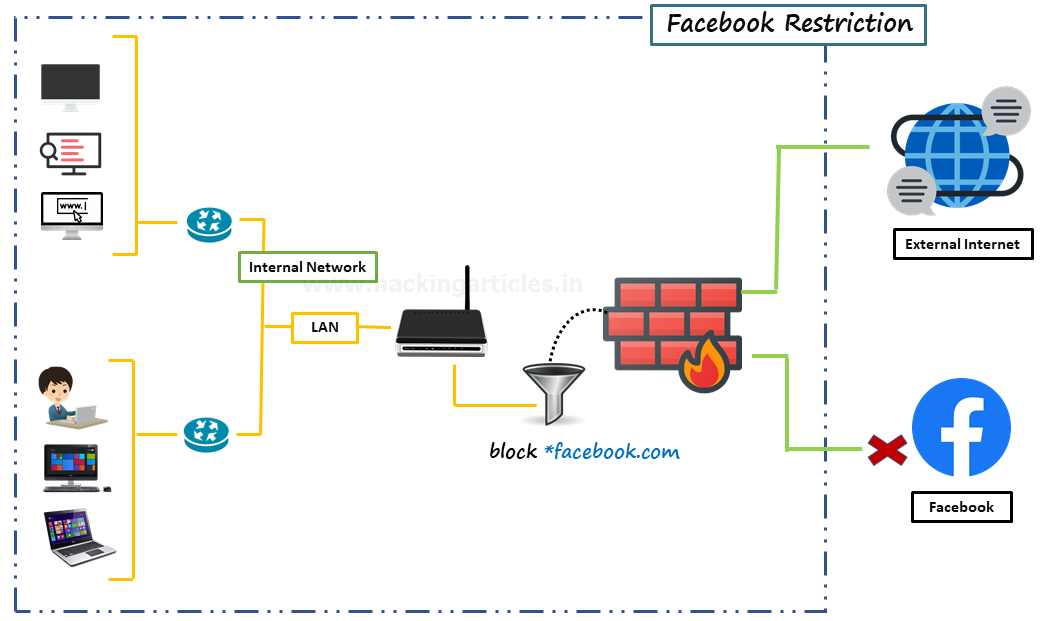


As we can see it blocks whole traffic that means it works properly.

* 1. **Blocking Facebook with Web filter**

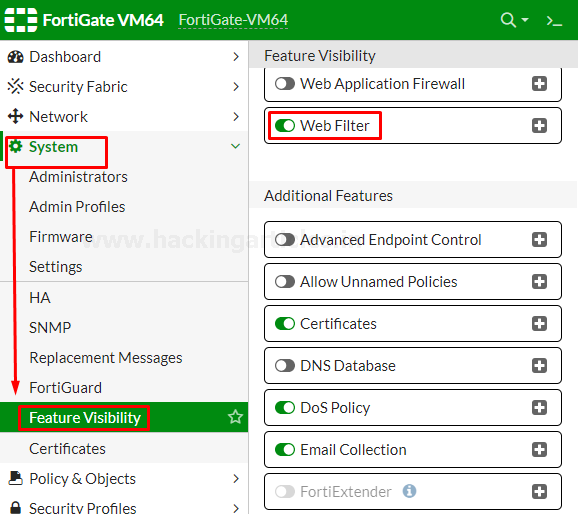
In this part, we are going to explain how to use a static URL filter to block access to Facebook and its subdomain in our network.

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.



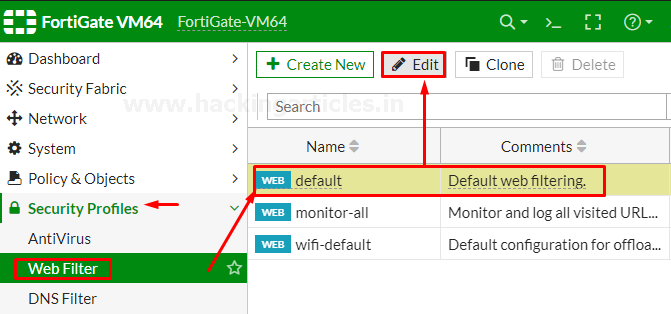
* 1. **Enable web Filter**

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

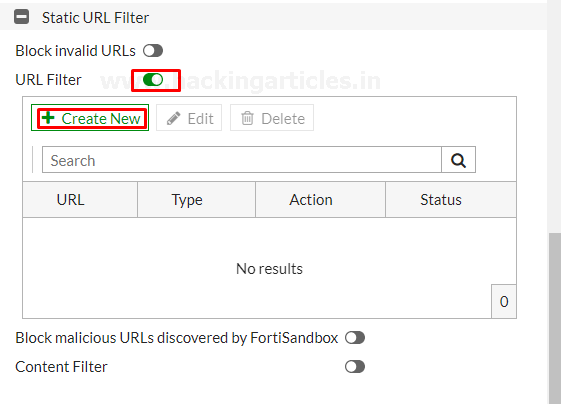


**Enable Default Web Filter Profile**

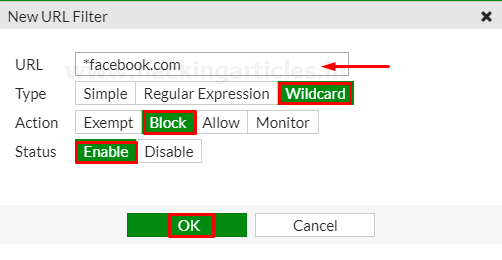
Go to **Security profiles > Web filter** and edit the default Web filter profile



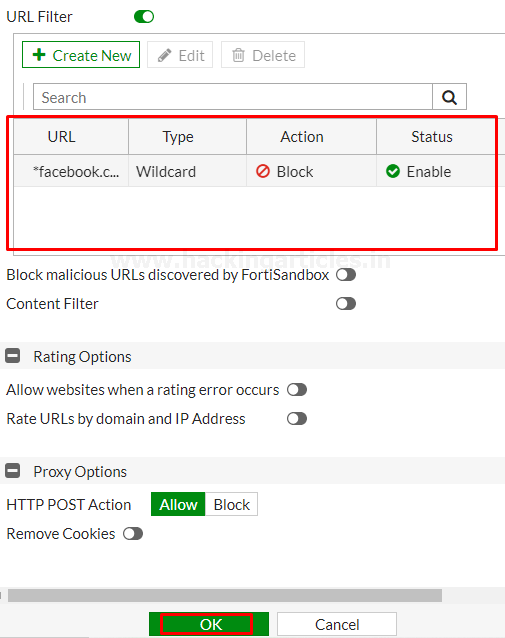
Now go to Static URL filter, select the URL filter and then select**“create”**.



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



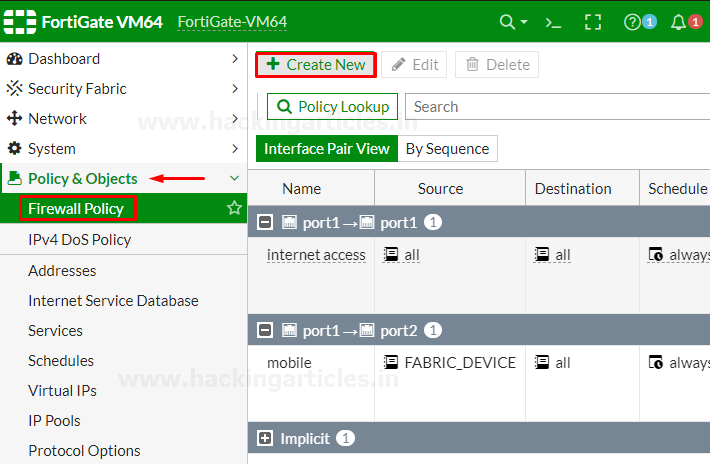
save it by selecting OK



Now you have successfully enabled web filter to block Facebook.

* 1. **Create Web Filter Security Policy**

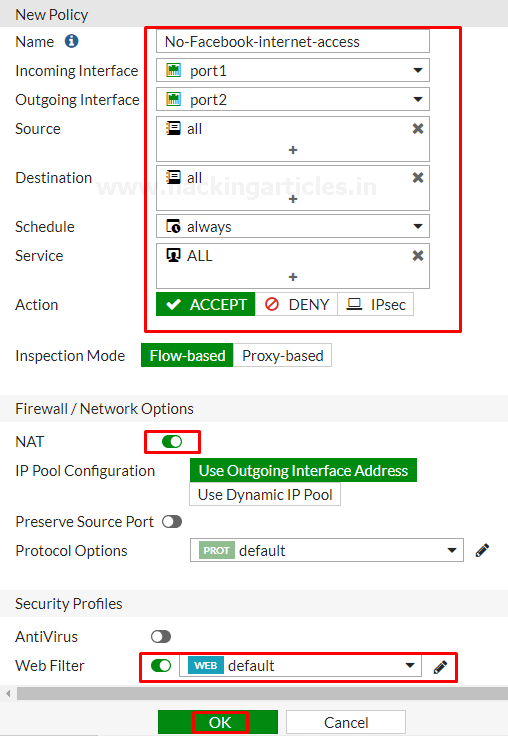
Go to **Policy & Objects > Firewall Policy** and **Create a New policy**.



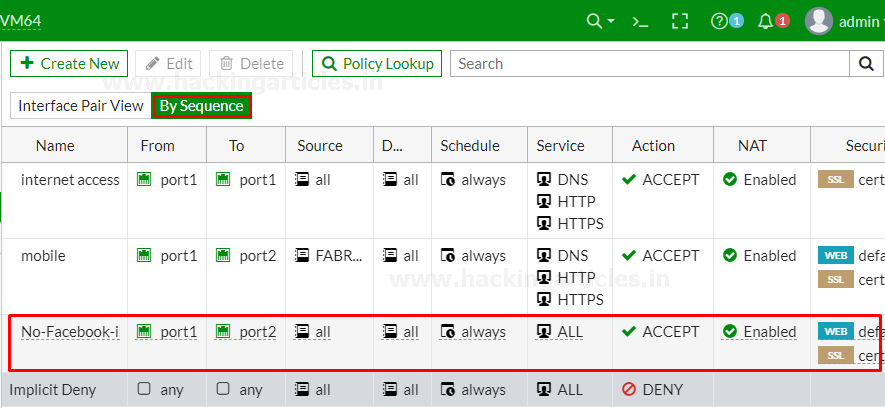
Give the name to the policy “No-Facebook-Internet-Access” to make it identifiable.

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”**

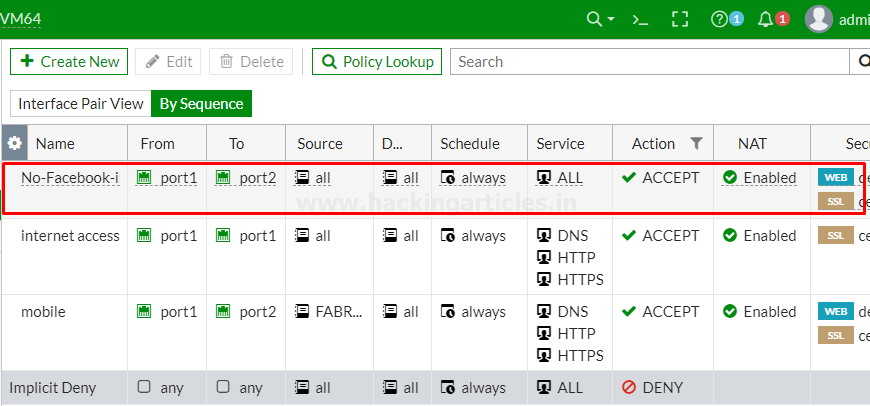
Under **Security Profiles**, enable **“Web Filter”** and select the default web filter profile.



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.

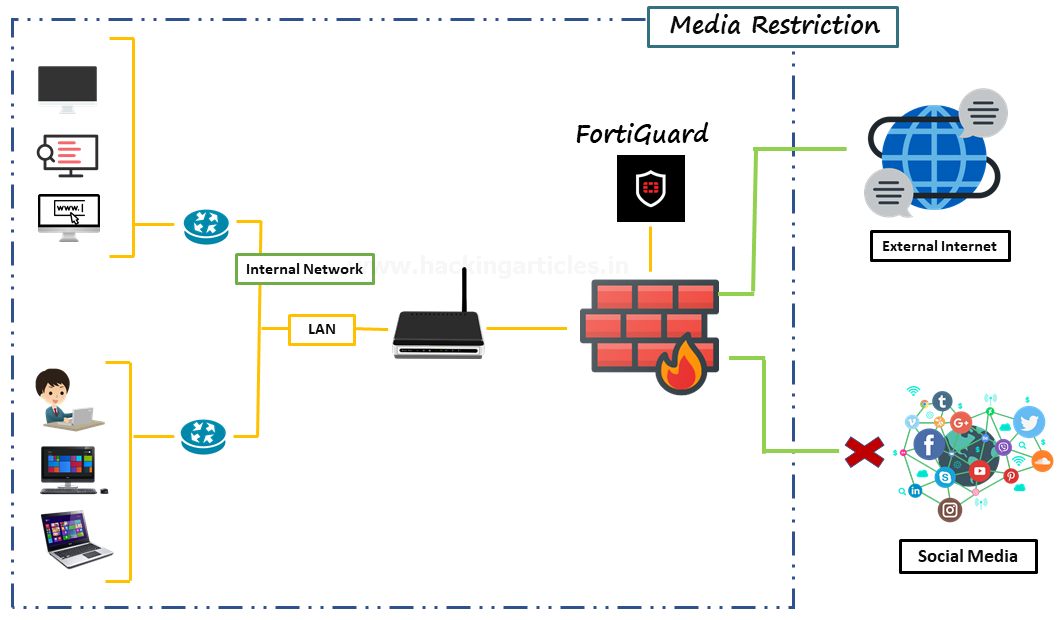
In next part, we are going to create some policies that is much required to make safe your network from unauthorized access or also safe from bad traffics.

**2. 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.



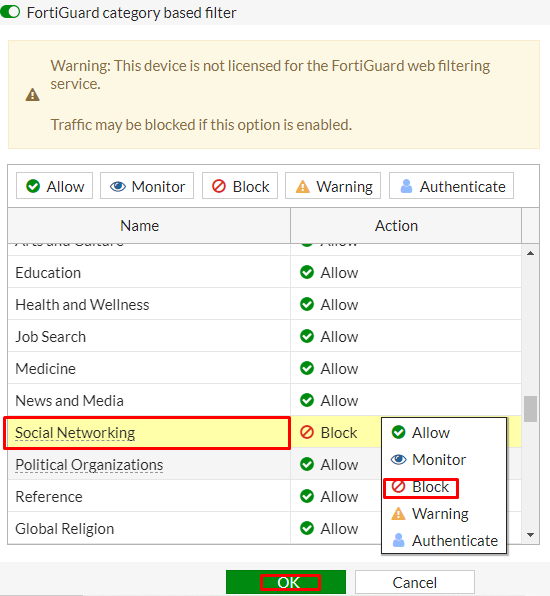
**2.1. Enable web Filter**

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

**2.2. Edit Default Web Filter Profile**

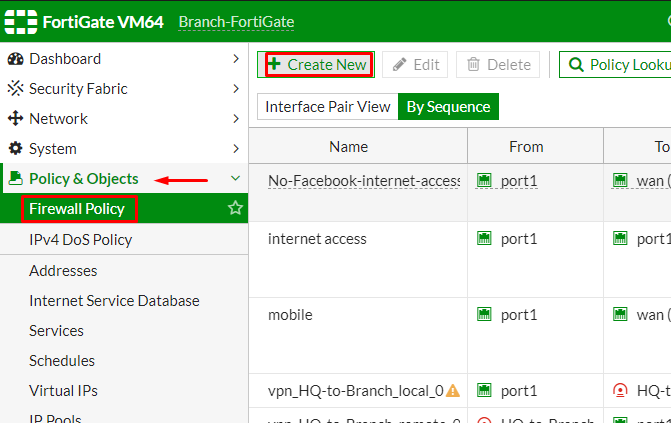
Go to **Security Profiles > Web Filter** and edit the Default web filter profile and make sure that “**FortiGuard category-based**” filter service is enabled.

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



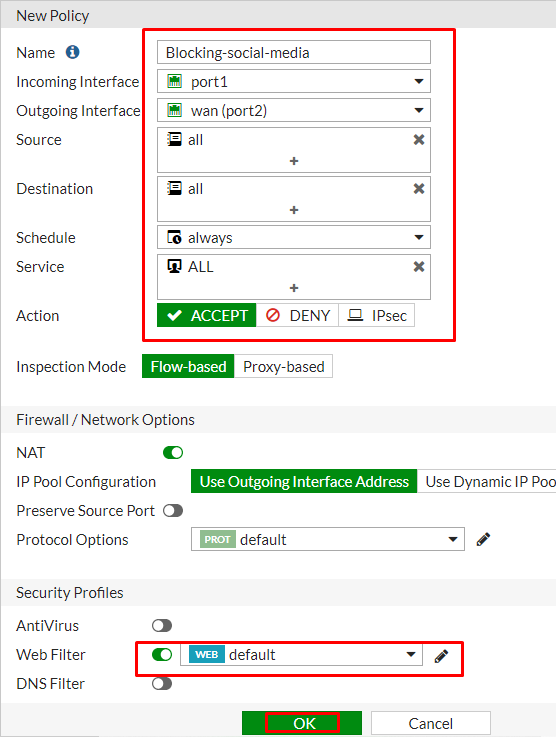
**Add Web Filter Profile to Internet Access Policy**

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

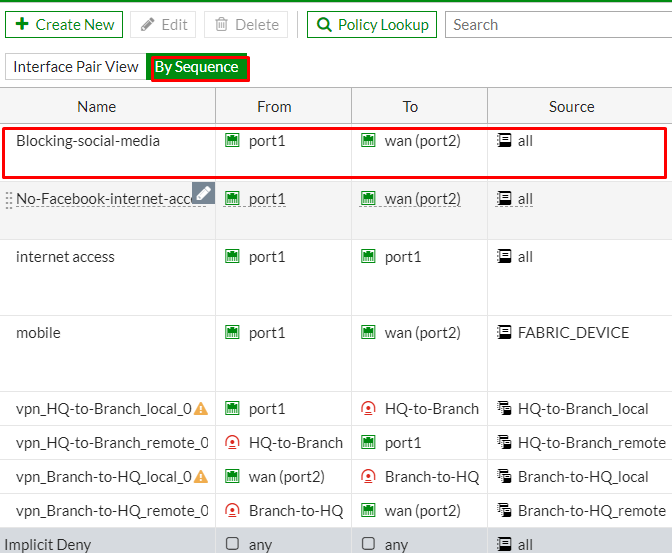


Give the name to the policy “Blocking-social-media” to make it identifiable. Set incoming interface to internal network and outgoing interface to internet facing interface. Set the rest to allow **“ALL”**  Traffic or you can select multiple rules by selecting the + icon and the action to **“Accept”**enable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



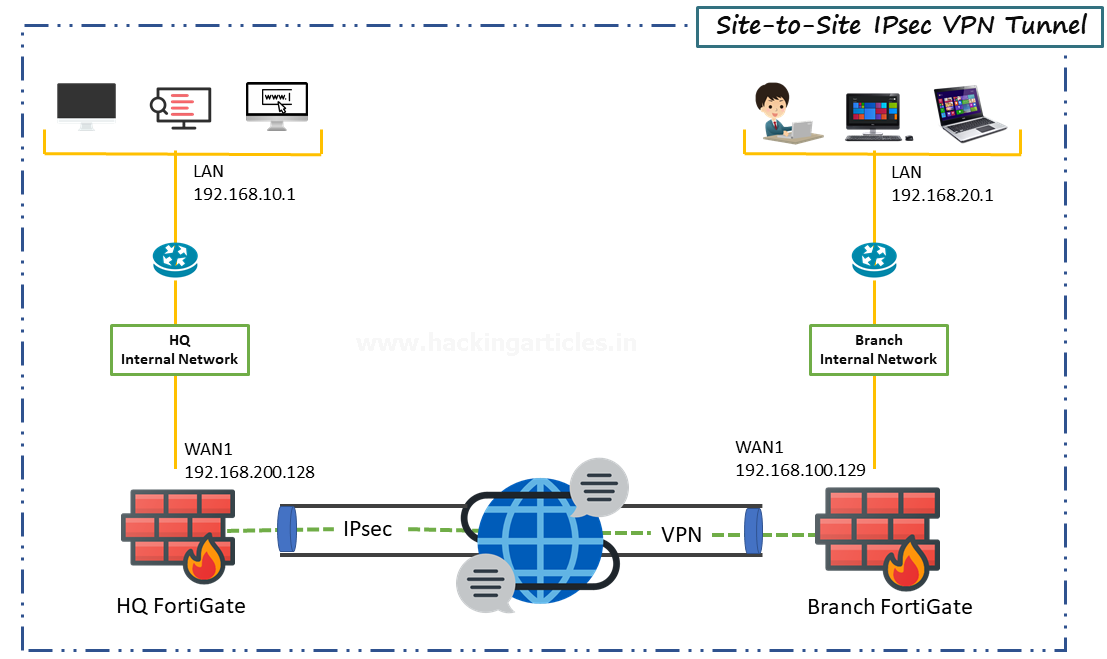
Now you have successfully enabled the social media blocking policy to move this policy to Top of the list to make it effective.



**2.3. Site-to-Site IPsec VPN Tunnel with two 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.

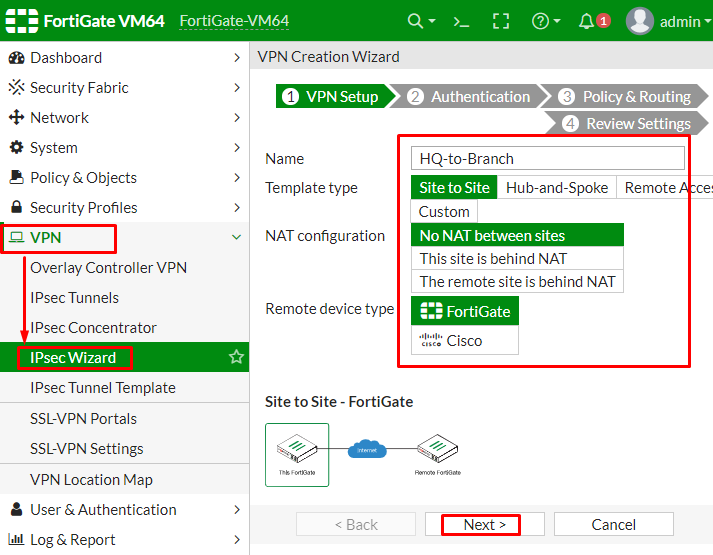
We are going to create an IPsec VPN tunnel between two FortiGates one is called HQ (Headquarter) another is called Branch.



**2.4. Configure IPsec VPN on HQ**

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

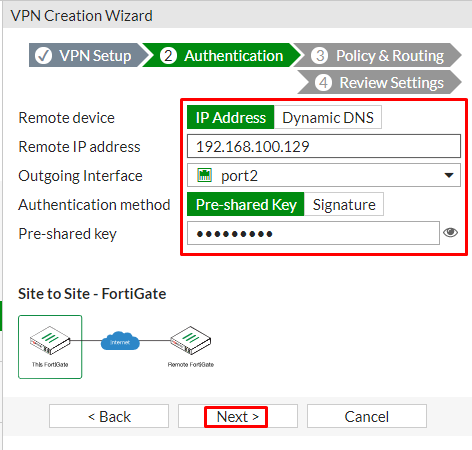
In the section, VPN setup describe a VPN name to make it identifiable, set Template type to Site-to-Site, set NAT configuration to NO NAT between sites and set Remote Device type to FortiGate.



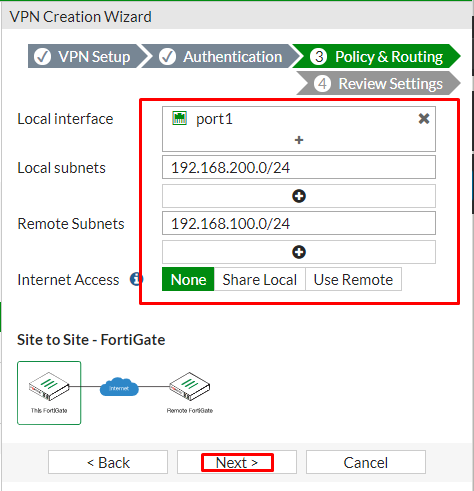
In the Authentication Section, set IP address to Public IP address of the Branch FortiGate.

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.

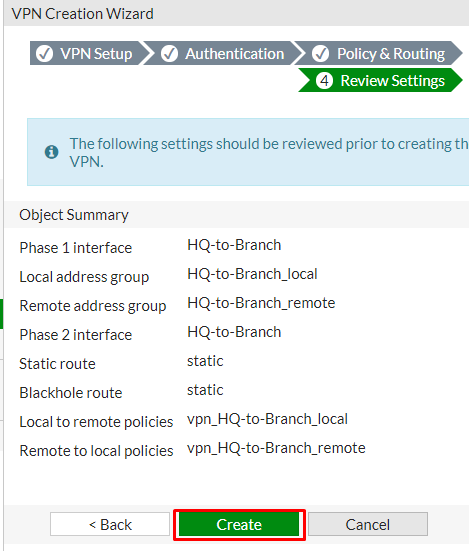
Set a secure **Pre-shared** key that is used to connect and verification for both FortiGates.



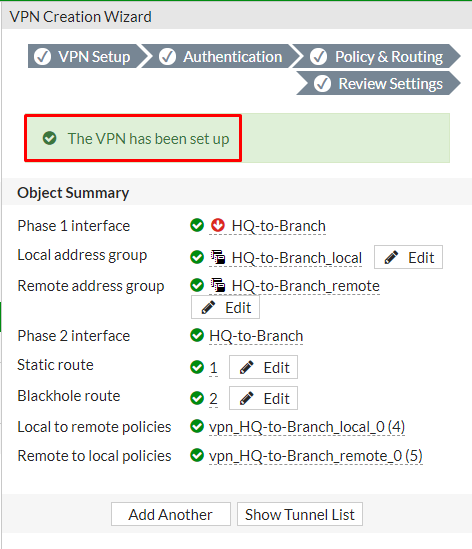
In the section of **Policy and Routing** set Local interface to **“LAN”** in my case **“Port1”** is dedicated to the LAN and local subnets will add automatically further then set **“Remote Subnets”** to the Branch network and set internet access to “**None”** as shown below



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



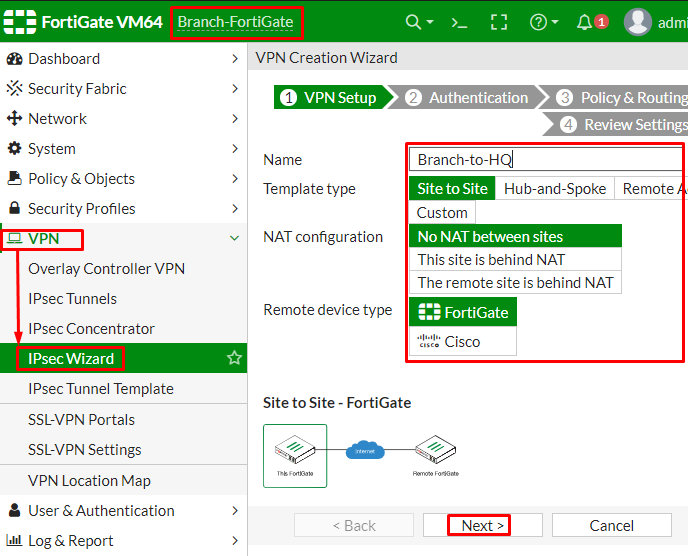
After creating the VPN, you can verify the details as shown below.



**2.5. Configure IPsec VPN on a branch**

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

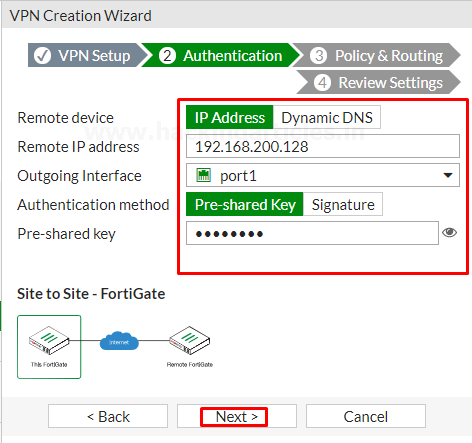
In the section, VPN setup describes a VPN name to make it identifiable, set Template type to Site-to-Site, set NAT configuration to “**NO NAT”** between sites and set Remote Device type to FortiGate.



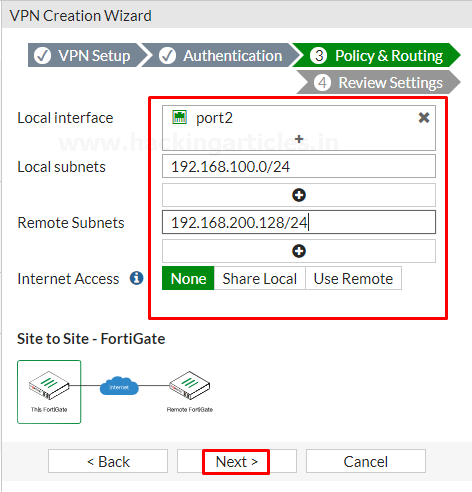
In the Authentication Section, set IP address to Public IP address of the Branch FortiGate.

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.

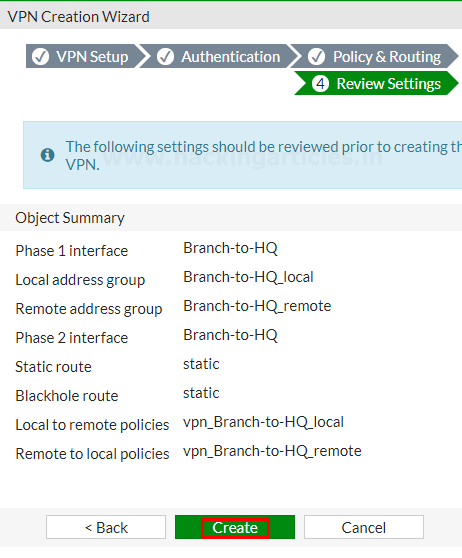
Set a secure **Pre-shared** key that was used on the VPN of HQ FortiGate.



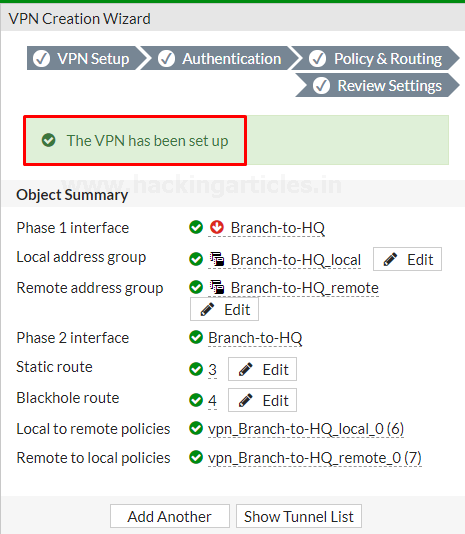
In the section of **Policy and Routing** set Local interface to **“LAN”** in my case **“Port2”** is dedicated to the LAN and local subnets will add automatically further then set **“Remote Subnets”** to the HQ (Headquarter) network and set internet access to “**None”** as shown below



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



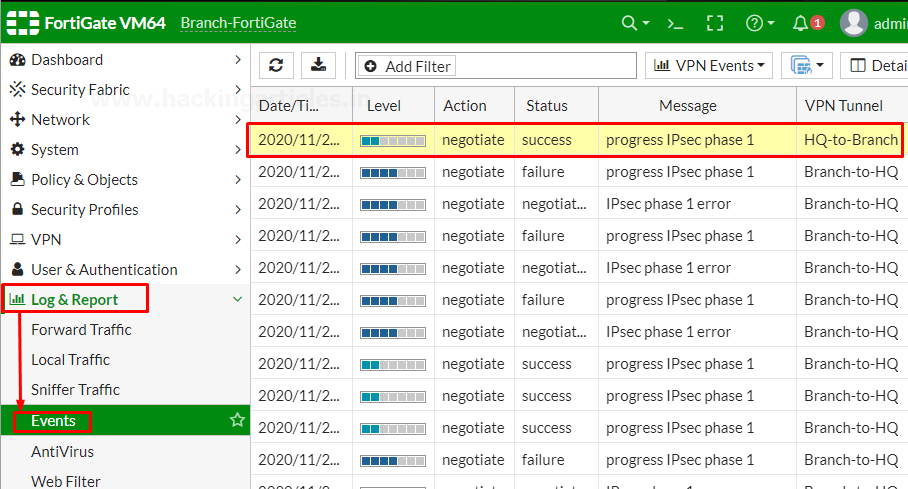
After creating the VPN, you can verify the details as shown below.



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.



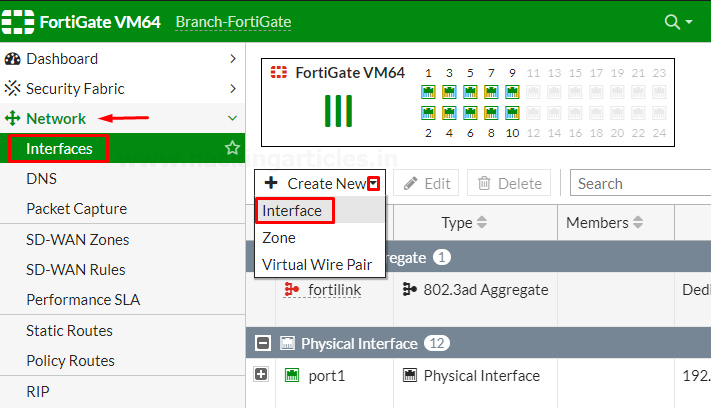
**2.6. Simplifying Policies with Zone**

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

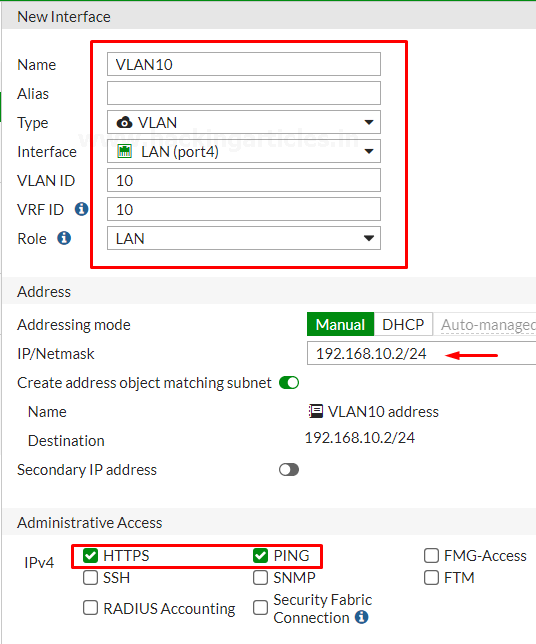
By creating multiple VLANs we are going to add them into a zone, so that we can just use the single zone object as a source interface in our firewall policy, rather than having to reference each interface separately.

**Create VLAN Interfaces**

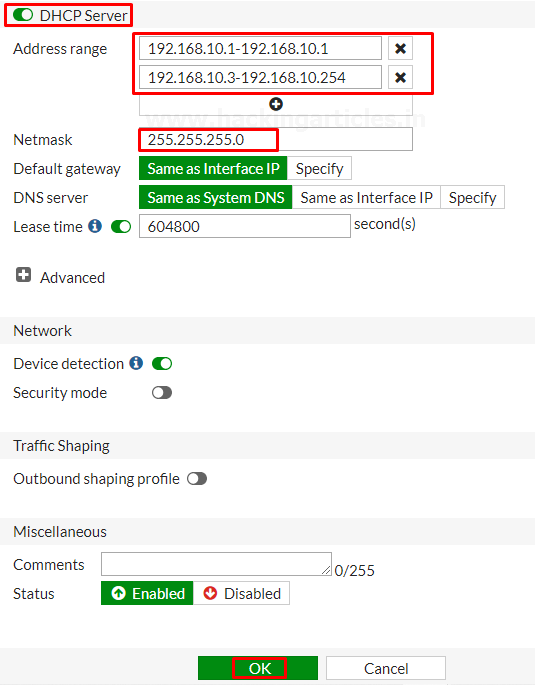
Go to Network > interfaces and create a new interface



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



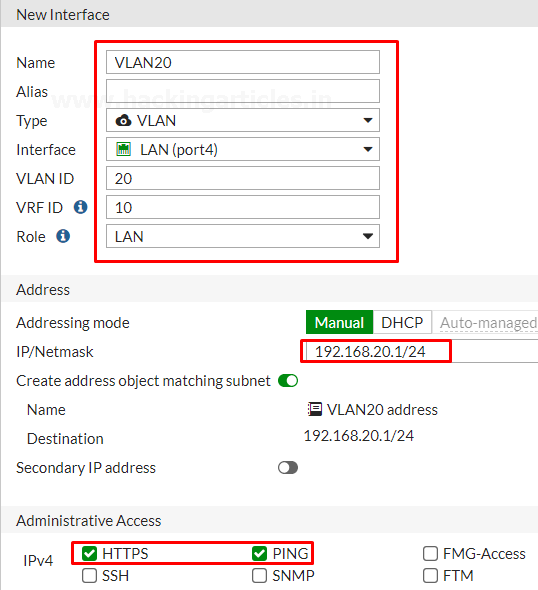
Enable the DHCP server and assign the address range further then save the configuration.



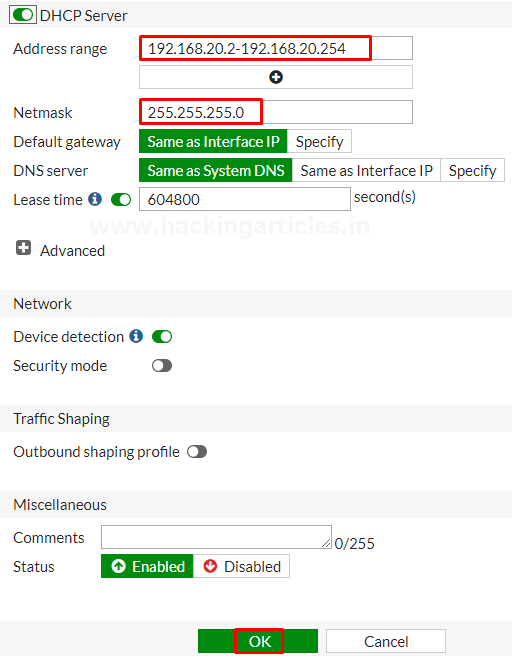
Next, create another by making the same selections…

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



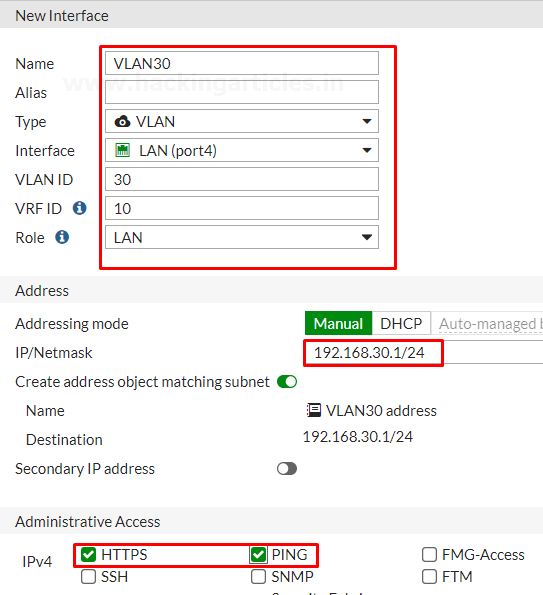
Enable the DHCP server and assign the address range further then save the configuration.



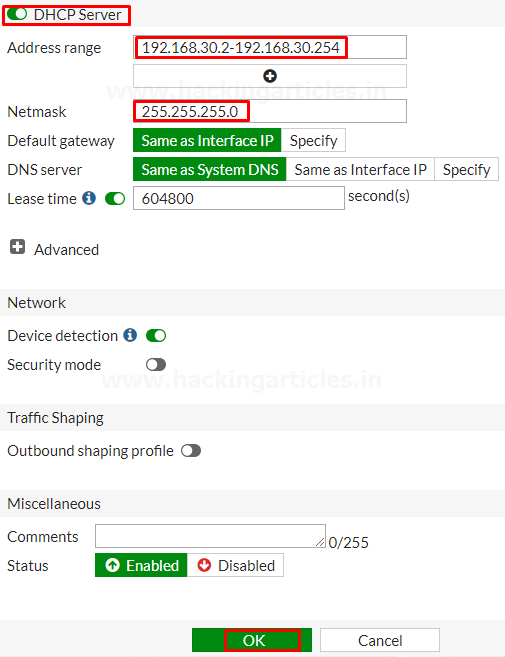
Finally, **create a 3rd VLAN** by making the same selection

Go to Network > interfaces and create a new interface.

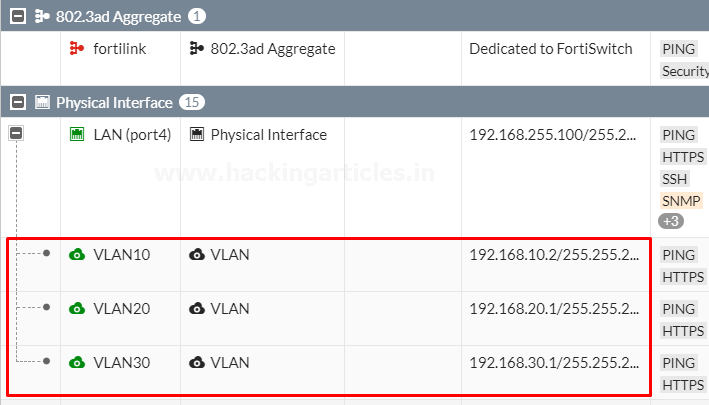
Enter the name for the interface VLAN30 or whatever you want, select the type to VLAN, select Interface to LAN, enter the VLAN ID, enter the VRF Id. assign the Role to LAN, set the Addressing mode to manual, enter the IP/Netmask provided by your ISP and select the Administrative Access to HTTPS, PING



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

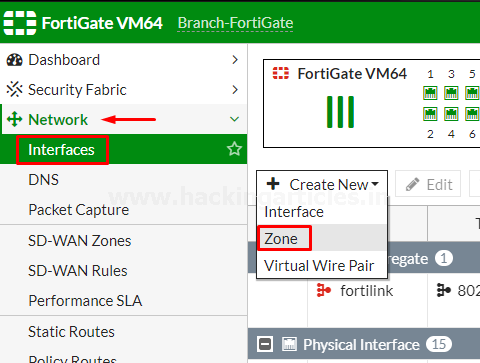


Review the Interface list to see the VLAN’s that you have created

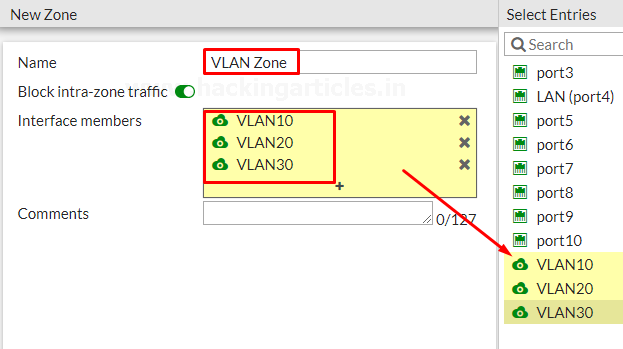


**2.7. Create an Interface Zone**

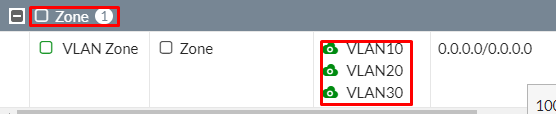
GO to the **Network > Interfaces** and select **create new Zone**



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

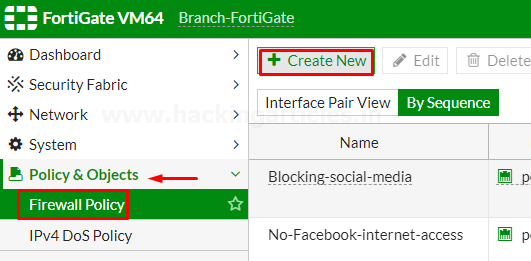


Review the Zone list to see the VLAN’s that you have Added.

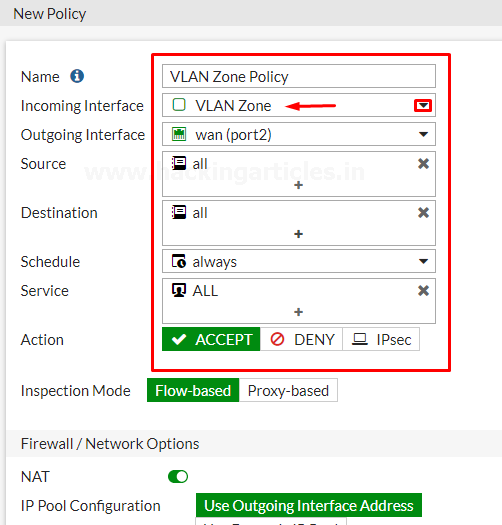


**2.8. Create a Zone Firewall Policy**

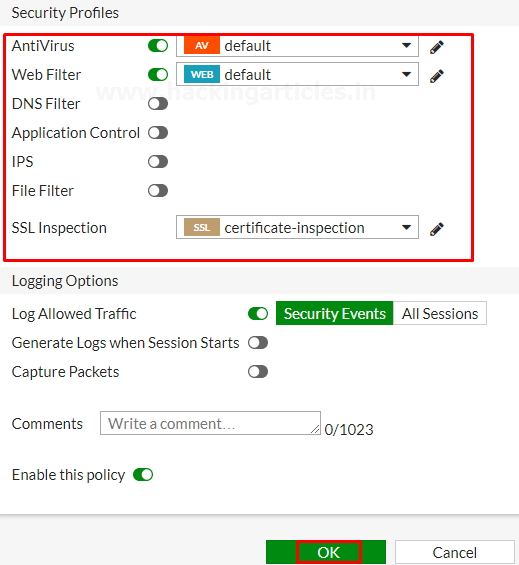
Go to Policy & Objects > Firewall Policy and create a new policy that will allow any VLAN in the Zone that we have created to access the internet.



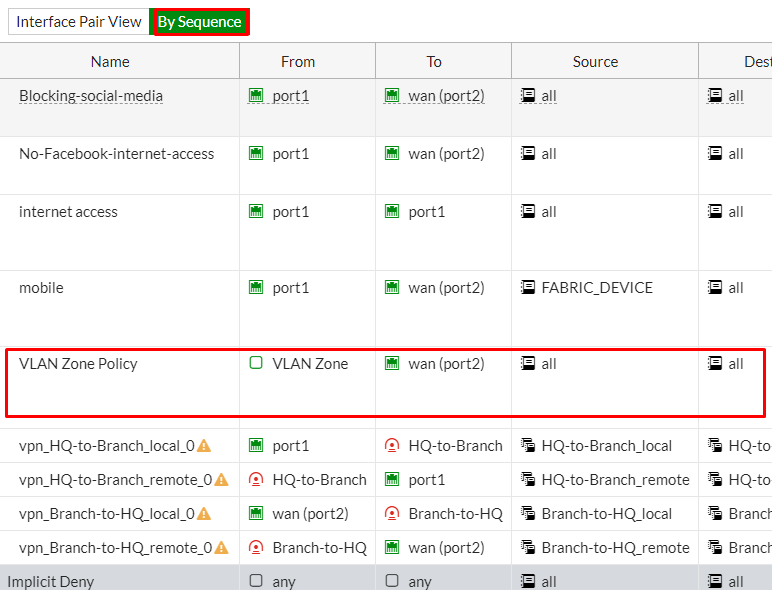
Assign a name to **“VLAN Zone Policy”** make it identifiable, set the **Incoming interface to your Zone** and the **outgoing interface to the internet-facing interface**. configure the rest as needed or as per your requirement.



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.