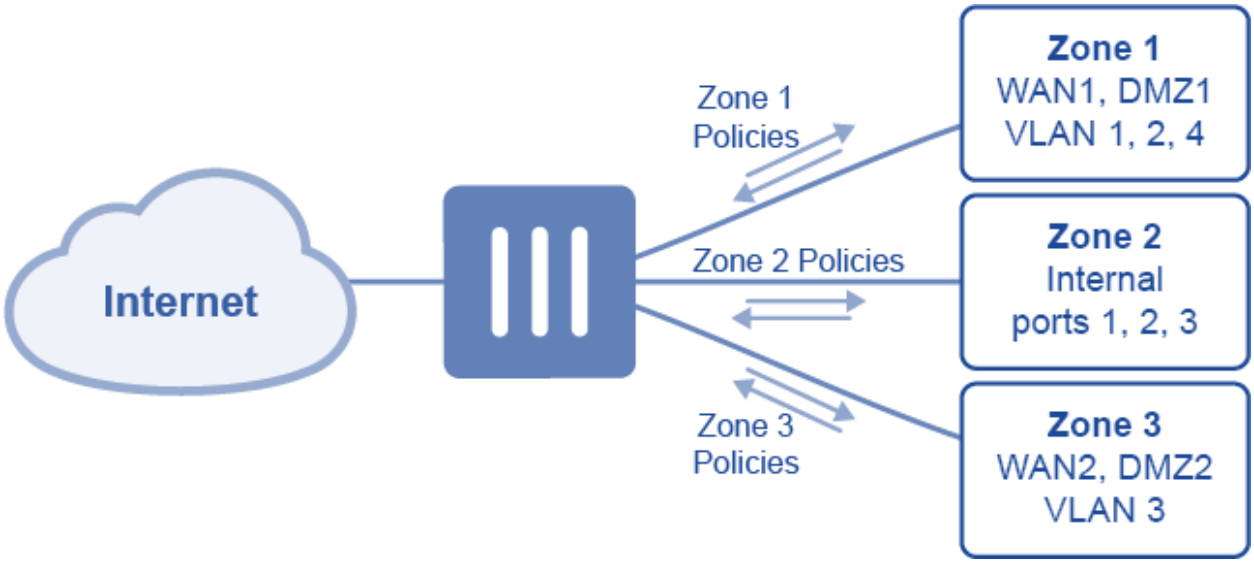
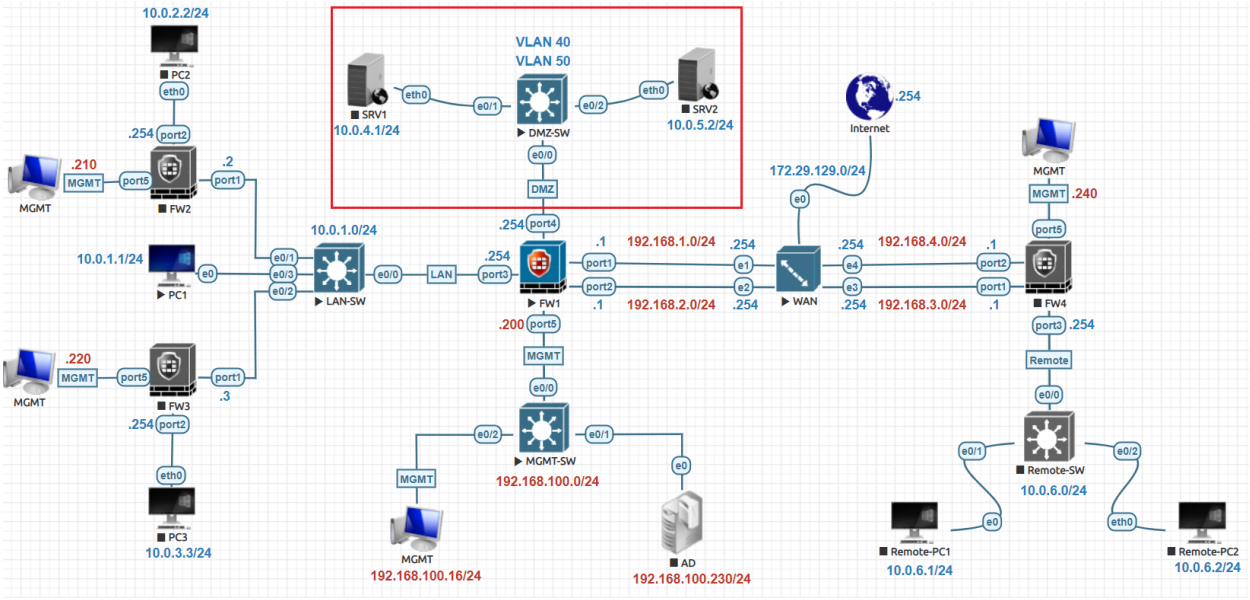
Zone:

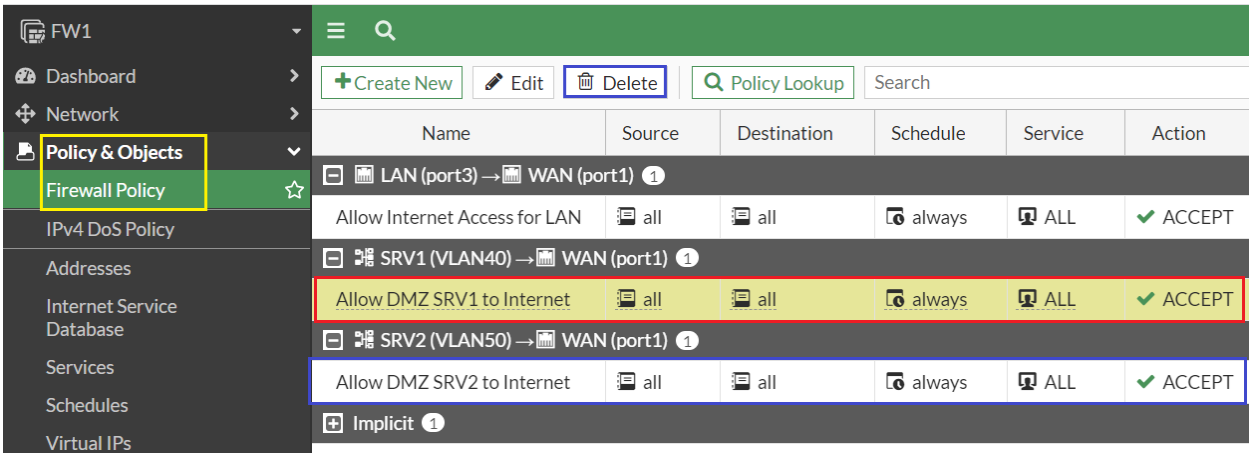
- Zones are a group of one or more physical or virtual FortiGate firewall interfaces.
- To simplify the policy configuration, you can group interfaces into logical zones.
- That you can apply the security policies to control inbound and outbound traffic.
- Grouping interfaces, VLAN subinterfaces into zones simplifies creation security policies.
- Where number of network segments can use same policy settings & protection profiles.
- When add zone, select names of interfaces and VLAN subinterfaces to add to the zone.
- Each interface still has its own address and routing is still done between the interfaces.
- You can use FortiGate Firewall security policies to control the flow of intra-zone traffic.
- Admin making separate security policies make simpler by adding interfaces to a zone.
- However, you should note that an interface in a zone cannot be referenced individually.
- Only configure policies for connections to & from zone but not between interfaces zone.
- You can create a security policy in FortiGate Firewall to go between zone 1 and zone 3.
- but you cannot create security policy between WAN2 and WAN1, or WAN1 and DMZ1.
- In zone configuration set intrazone deny prohibiting different interfaces in same zone.
- Enable Block intra-zone traffic, block different interfaces in same zone to talk each other.



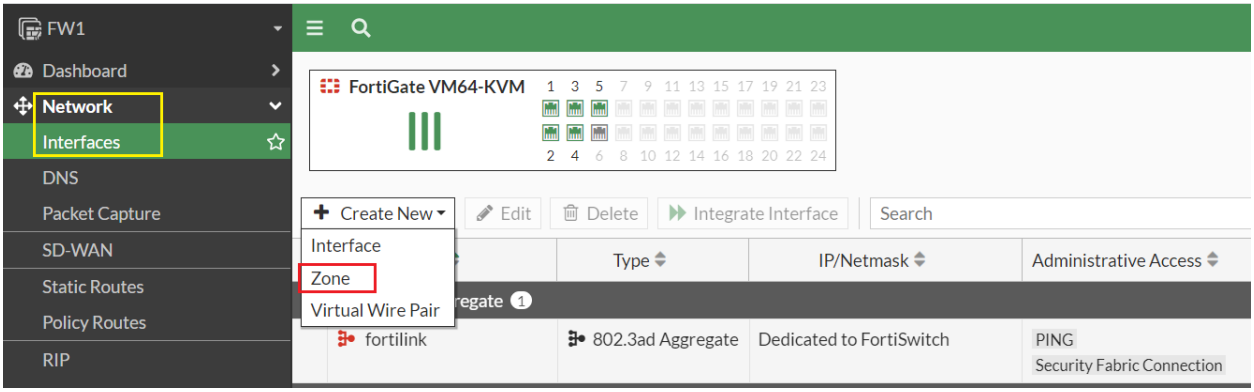
Zone Lab:



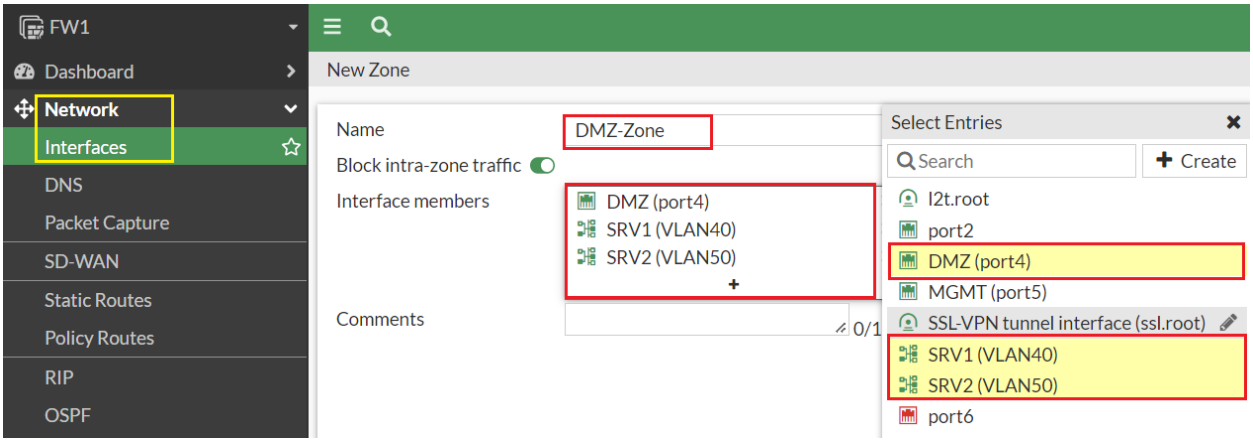
First let's delete the previously created Firewall policies for VLAN 40 and VLAN 50.



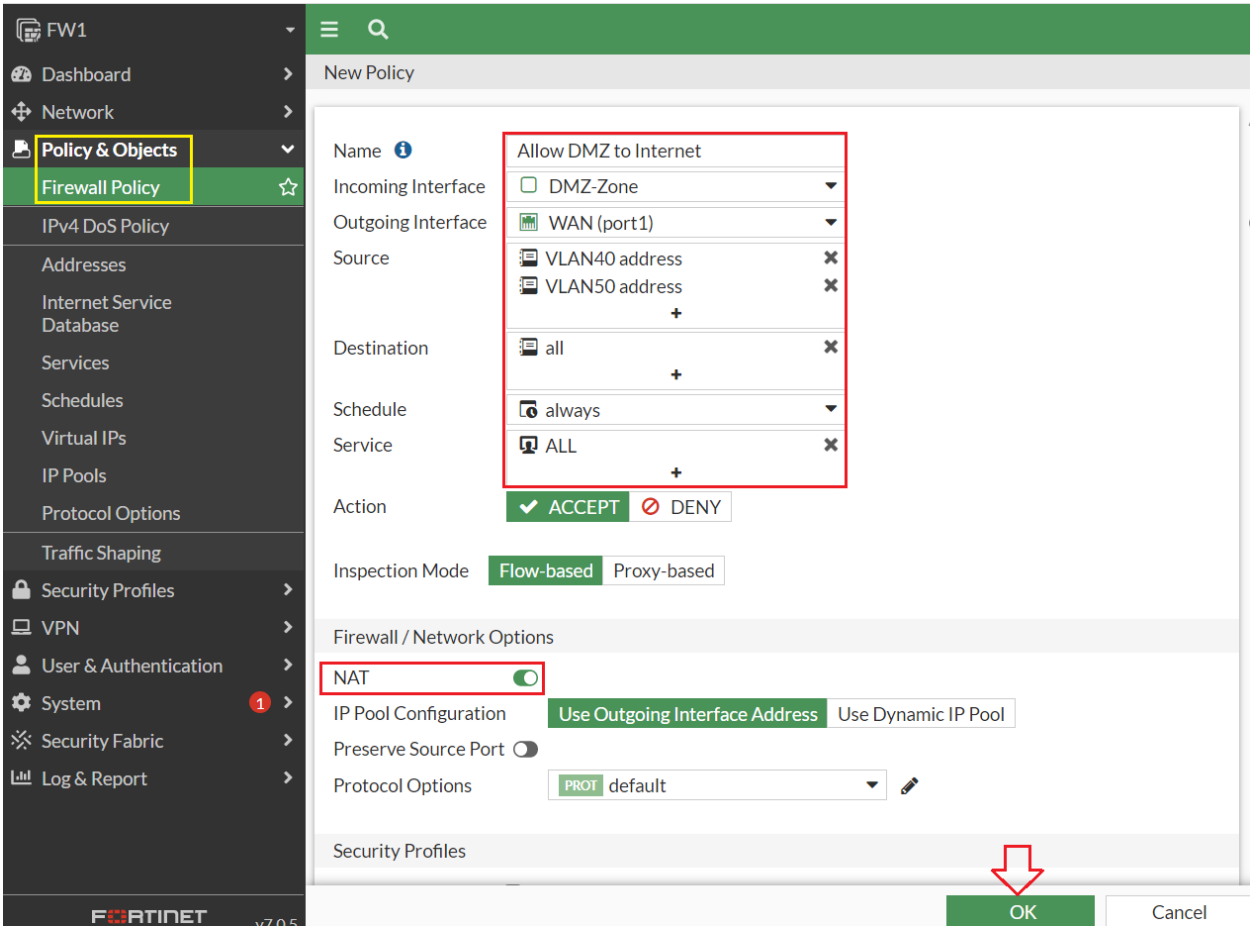
To create a zone in Go to Network > Interfaces Click Create New > Zone.



Configure the Name and add the Interface Members in our case VLAN40 & VLAN50.
Enable Block intra-zone traffic, block different interfaces in same zone to talk each other.



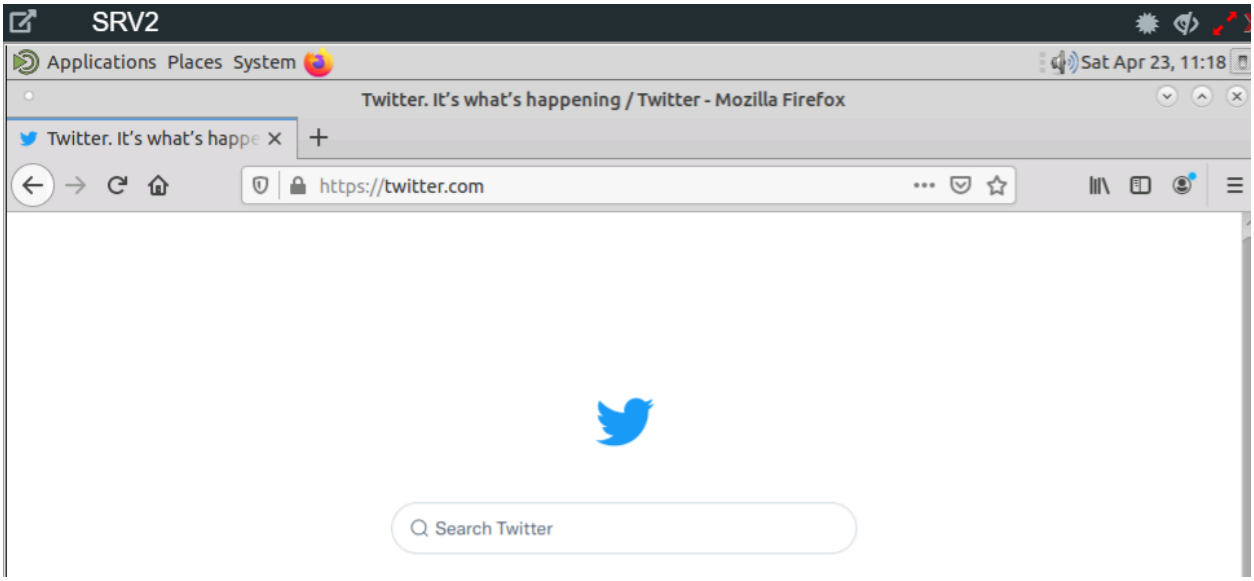
Create a firewall policy, go to Policy & Objects > Firewall Policy, and click Create New.

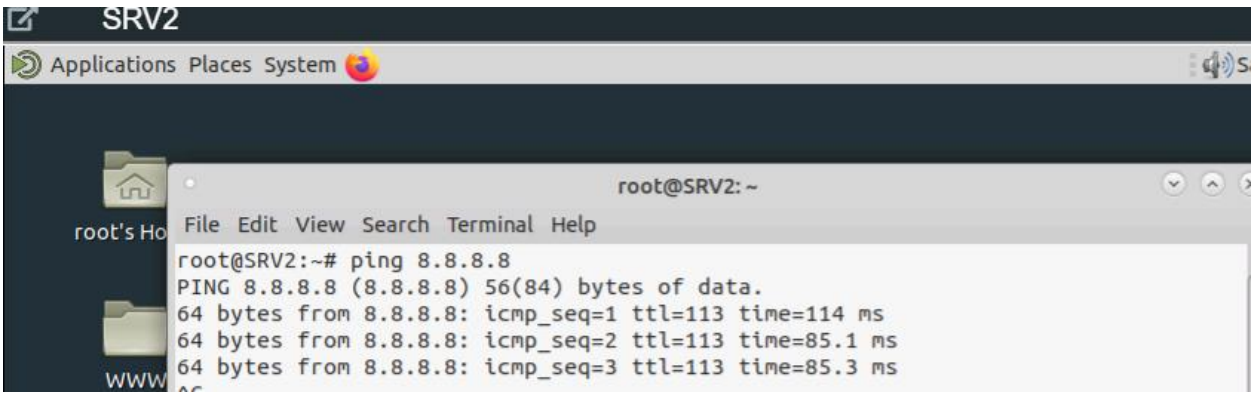


Test and Verification:

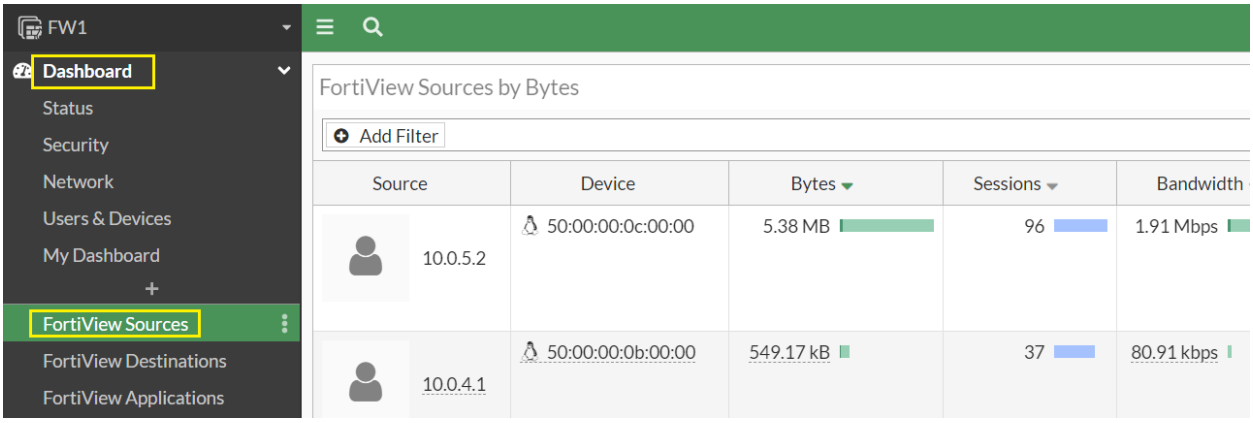
Try to access any website from SRV1 in this case facebook.com it's working.

Now, try to access any website from SRV2 in this case twitter.com it's working.

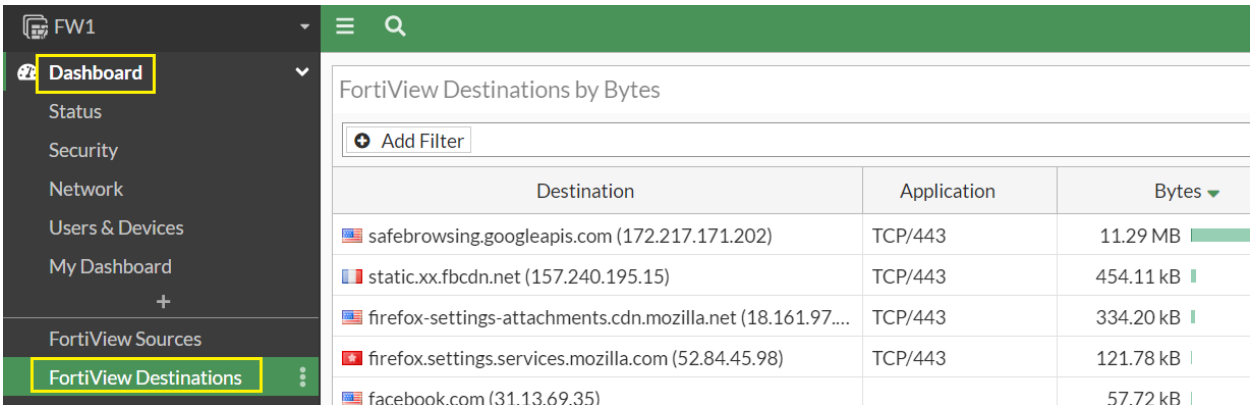




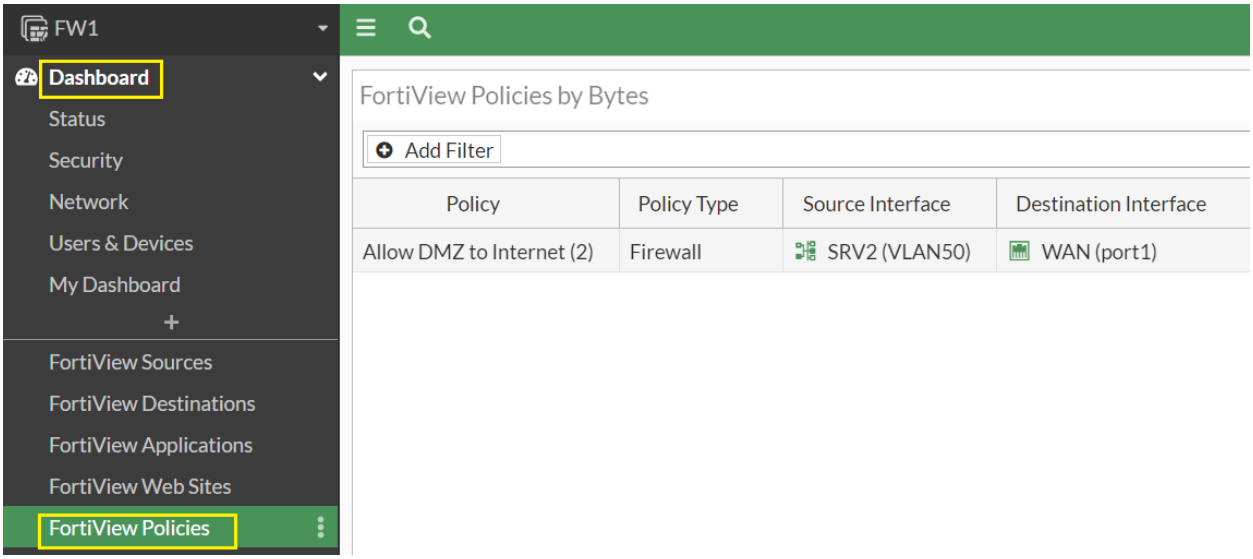
Go to Dashboard> FortiView Sources to display and verify VLAN40 & VLAN50 source IP.



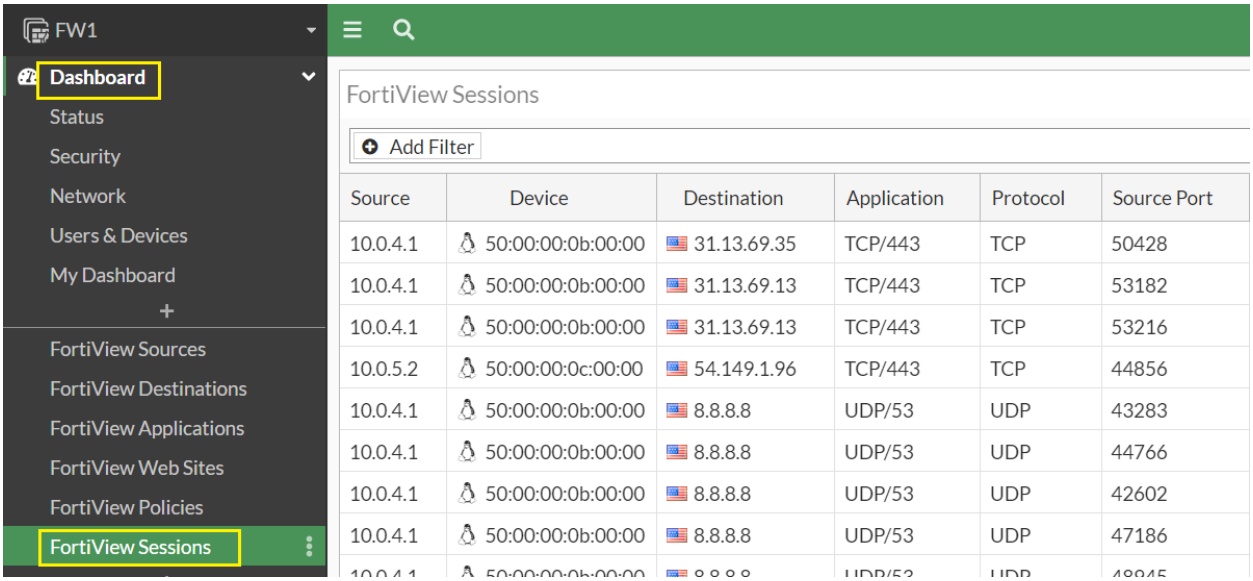
Go to Dashboard> FortiView Destinations to display and verify the destinations domains & IP.



Go to Dashboard> FortiView Polices to display and verify security polices has been hits & used.



Go to Dashboard> FortiView Sessions to display and verify all VLANs visited links sessions.



Go to Log & Report> Forward Traffic to display and verify all VLANs visited links sessions.