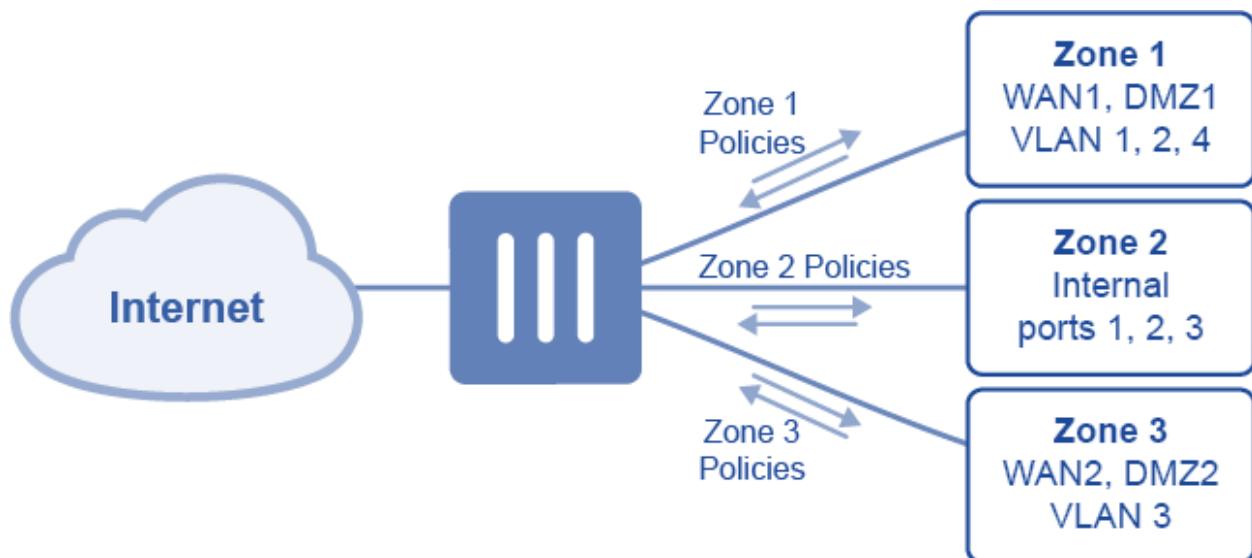
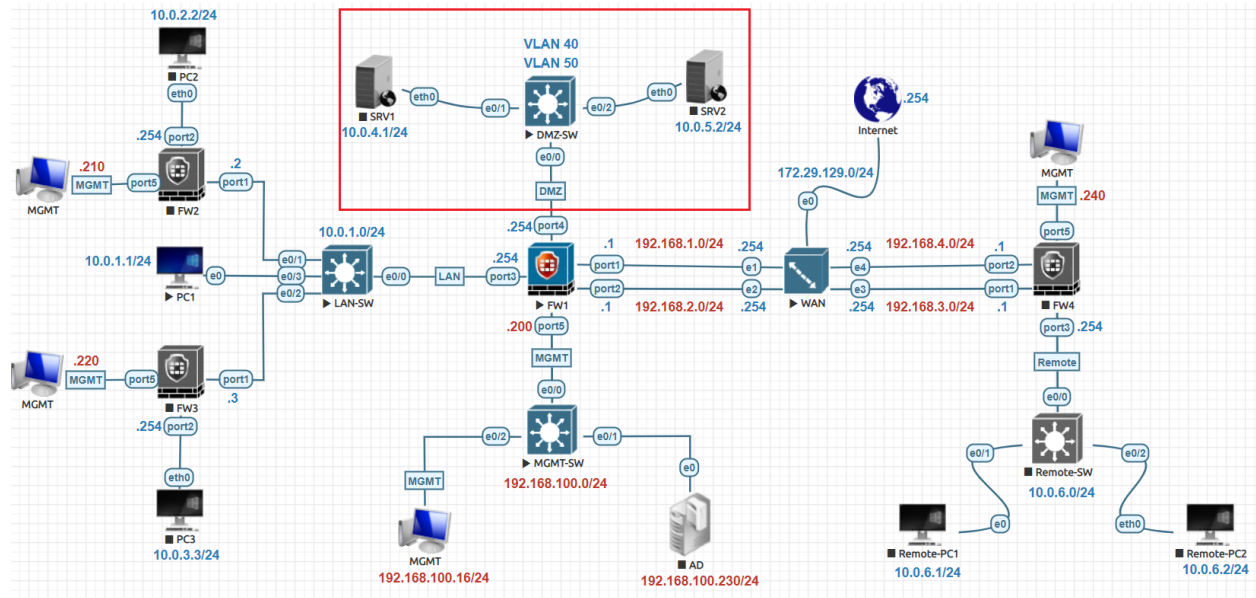


Zone:

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



Zone Lab:



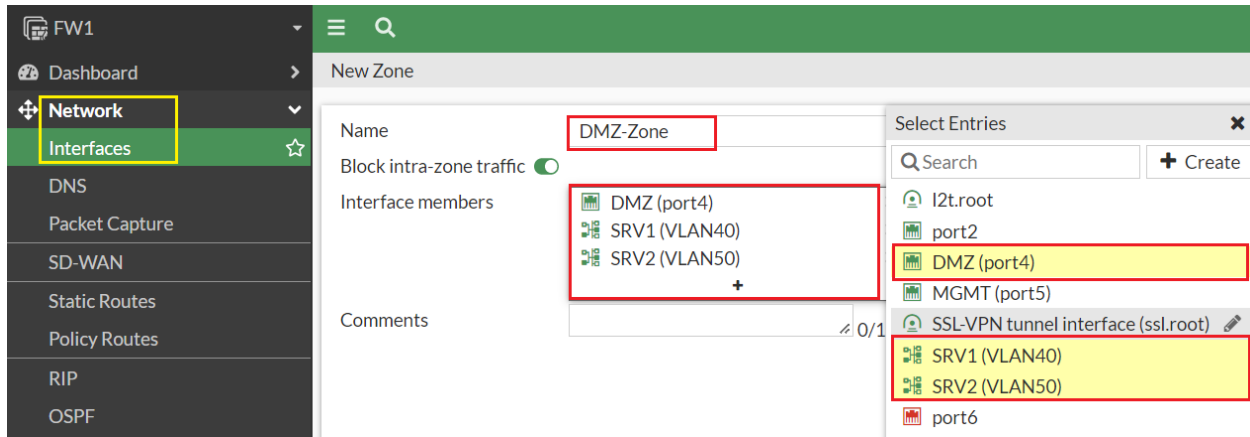
First let's delete the previously created Firewall policies for VLAN 40 and VLAN 50.

Name	Source	Destination	Schedule	Service	Action
LAN (port3) → WAN (port1)					
Allow Internet Access for LAN	all	all	always	ALL	ACCEPT
Allow DMZ SRV1 to Internet	all	all	always	ALL	ACCEPT
Allow DMZ SRV2 to Internet	all	all	always	ALL	ACCEPT
Implicit					

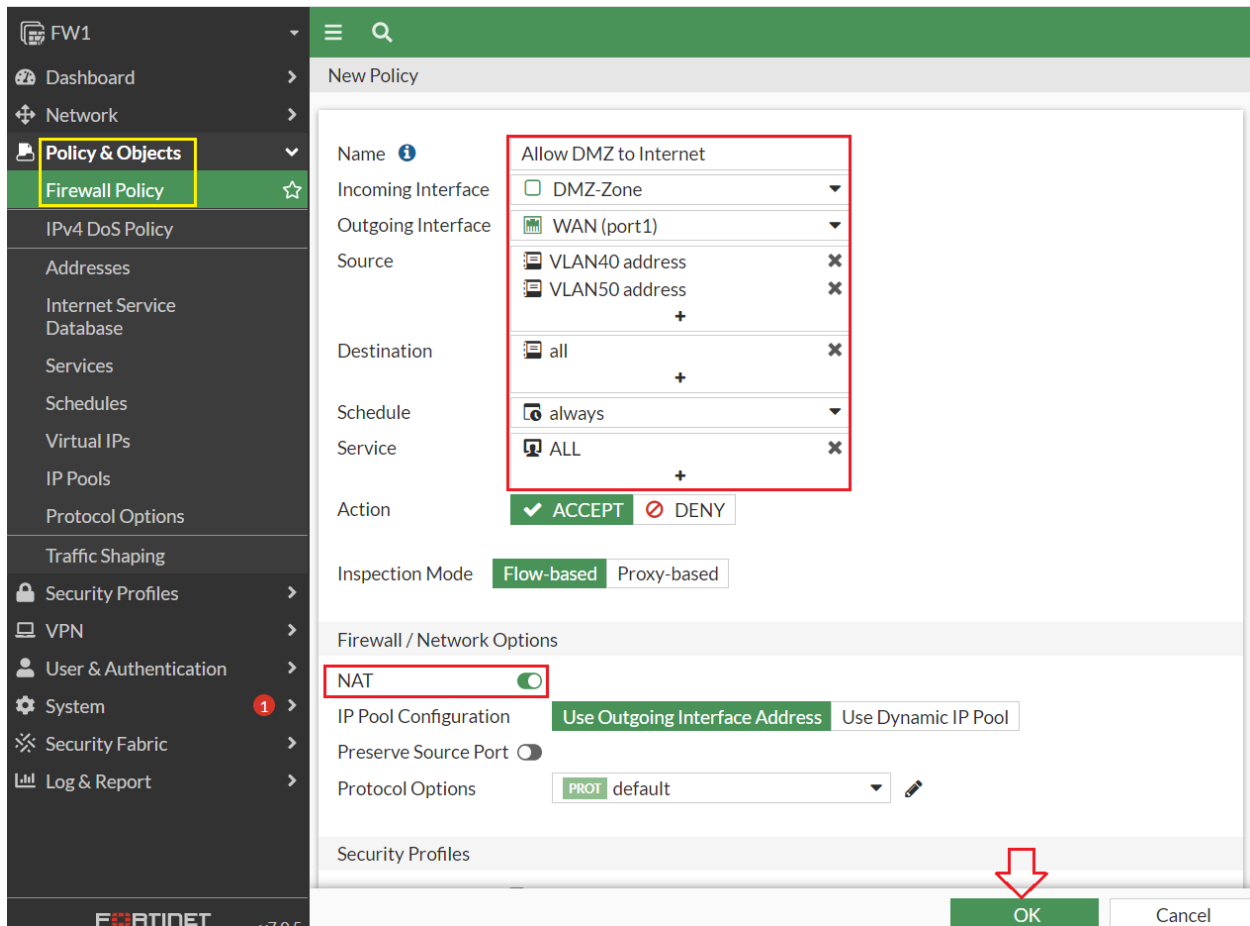
To create a zone in Go to **Network > Interfaces** Click **Create New > Zone**.

Interface	Type	IP/Netmask	Administrative Access
fortilink	802.3ad Aggregate	Dedicated to FortiSwitch	PING Security Fabric Connection

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**.

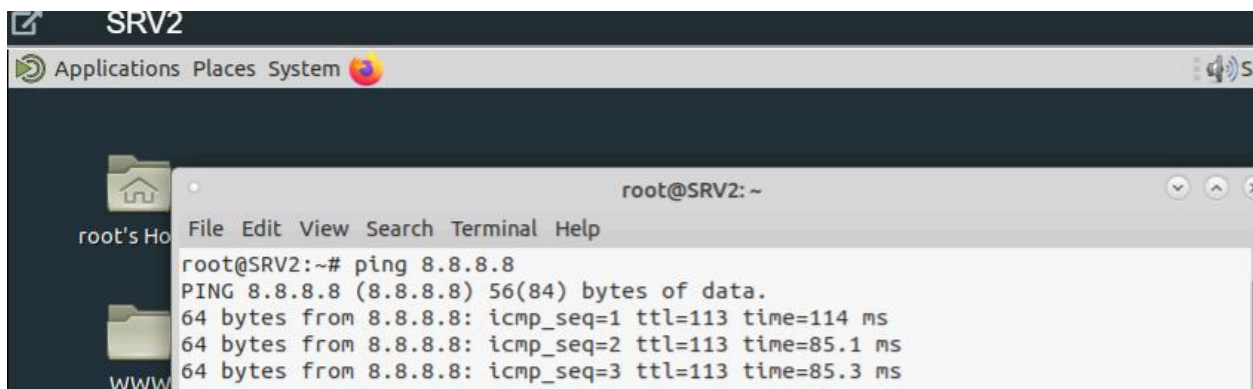
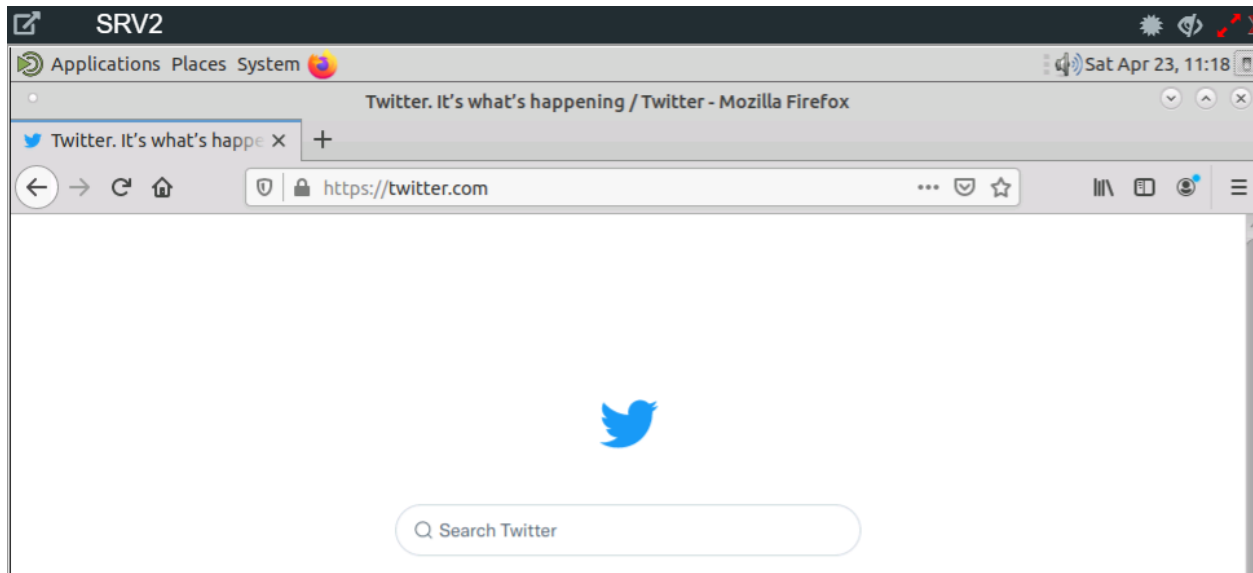


Test and Verification:

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.

FortiView Sources by Bytes

Source	Device	Bytes	Sessions	Bandwidth
10.0.5.2	50:00:00:0c:00:00	5.38 MB	96	1.91 Mbps
10.0.4.1	50:00:00:0b:00:00	549.17 kB	37	80.91 kbps

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

FortiView Destinations by Bytes

Destination	Application	Bytes
safebrowsing.googleapis.com (172.217.171.202)	TCP/443	11.29 MB
static.xx.fbcdn.net (157.240.195.15)	TCP/443	454.11 kB
firefox-settings-attachments.cdn.mozilla.net (18.161.97...)	TCP/443	334.20 kB
firefox.settings.services.mozilla.com (52.84.45.98)	TCP/443	121.78 kB
facebook.com (31.13.69.35)		57.72 kB

Go to **Dashboard > FortiView Policies** to display and verify security policies has been hits & used.

FortiView Policies by Bytes

Policy	Policy Type	Source Interface	Destination Interface
Allow DMZ to Internet (2)	Firewall	SRV2 (VLAN50)	WAN (port1)

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

Source	Device	Destination	Application	Protocol	Source Port
10.0.4.1	50:00:00:0b:00:00	31.13.69.35	TCP/443	TCP	50428
10.0.4.1	50:00:00:0b:00:00	31.13.69.13	TCP/443	TCP	53182
10.0.4.1	50:00:00:0b:00:00	31.13.69.13	TCP/443	TCP	53216
10.0.5.2	50:00:00:0c:00:00	54.149.1.96	TCP/443	TCP	44856
10.0.4.1	50:00:00:0b:00:00	8.8.8.8	UDP/53	UDP	43283
10.0.4.1	50:00:00:0b:00:00	8.8.8.8	UDP/53	UDP	44766
10.0.4.1	50:00:00:0b:00:00	8.8.8.8	UDP/53	UDP	42602
10.0.4.1	50:00:00:0b:00:00	8.8.8.8	UDP/53	UDP	47186

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

Date/Time	Source	Device	Destination
3 seconds ago	10.0.4.1	50:00:00:0b:00:00	31.13.69.35 (facebook.com)
19 seconds ago	10.0.4.1	50:00:00:0b:00:00	52.84.45.98 (firefox.settings.services.mozilla.com)
29 seconds ago	10.0.5.2	50:00:00:0c:00:00	8.8.8.8 (dns.google)
29 seconds ago	10.0.5.2	50:00:00:0c:00:00	8.8.8.8 (dns.google)
33 seconds ago	10.0.5.2	50:00:00:0c:00:00	104.244.42.66 (api.twitter.com)
38 seconds ago	10.0.5.2	50:00:00:0c:00:00	104.244.42.66 (api.twitter.com)
43 seconds ago	10.0.5.2	50:00:00:0c:00:00	8.8.8.8 (dns.google)
43 seconds ago	10.0.5.2	50:00:00:0c:00:00	8.8.8.8 (dns.google)
51 seconds ago	10.0.5.2	50:00:00:0c:00:00	142.251.37.170 (safebrowsing.googleapis.com)
52 seconds ago	10.0.5.2	50:00:00:0c:00:00	142.251.37.170 (safebrowsing.googleapis.com)
Minute ago	10.0.5.2	50:00:00:0c:00:00	8.8.8.8 (dns.google)
2 minutes ago	10.0.4.1	50:00:00:0b:00:00	31.13.69.13 (static.xx.fbcdn.net)
2 minutes ago	10.0.4.1	50:00:00:0b:00:00	34.210.202.253 (push.services.mozilla.com)
4 minutes ago	10.0.5.2	50:00:00:0c:00:00	54.149.1.96 (push.services.mozilla.com)