🔐 Simplifying VLAN Management Using Zones

🔍 What is a Zone in FortiGate?

- A Zone is a logical grouping of interfaces that share similar security requirements.
- Zones help in segmenting the network into distinct security domains such as LAN, WAN, DMZ, etc.
- Using zones ensures consistent enforcement of security rules across all interfaces in that group.
- FortiGate comes with predefined zones like Internal, External, and DMZ, which can be customized.
- You can also create custom zones tailored to your specific network design and security requirements.
- Zones are especially useful in larger networks with multiple VLANs or interface types, as they reduce configuration overhead.

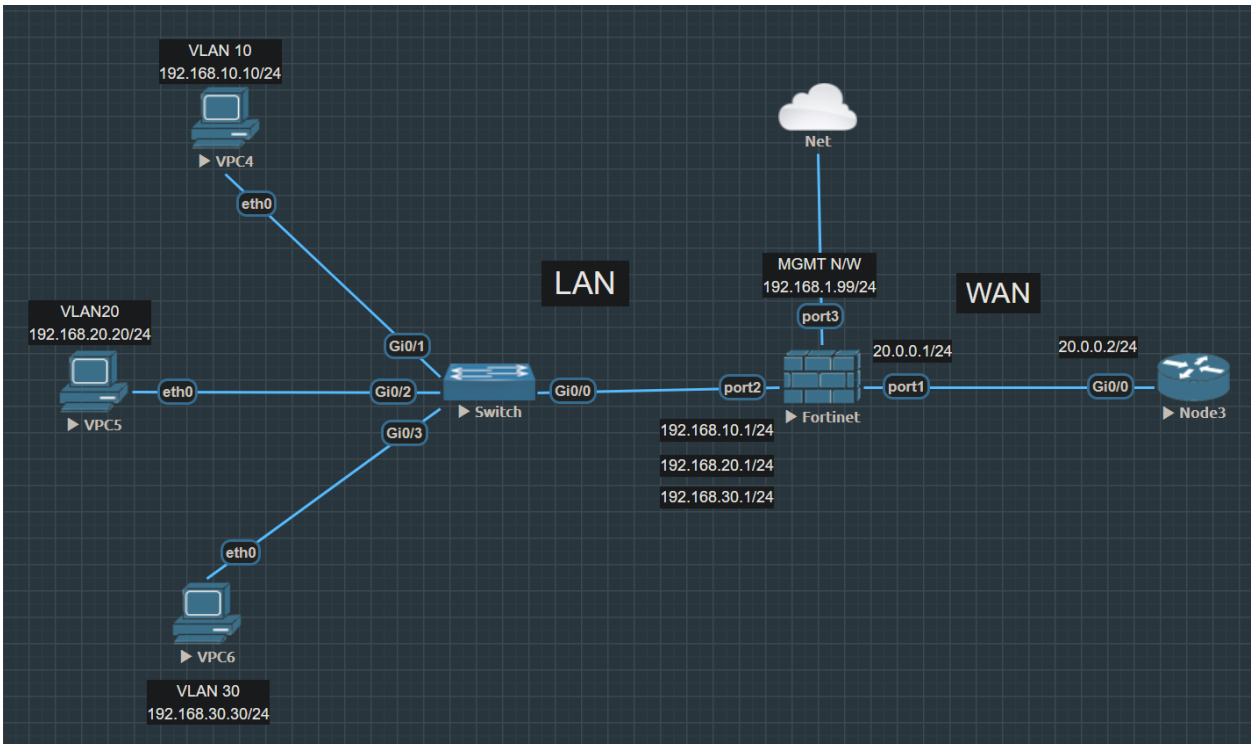
🧠 Concept Overview

Let's consider a scenario:

- You have 3 VLANs: VLAN 10, VLAN 20, VLAN 30.
- These are mapped to different departments or user groups (e.g., HR, Finance, IT).
- Instead of creating separate policies for each VLAN, we group them under a LAN Zone.
- Then, we just create 2 policies:
    - LAN-to-WAN
    - WAN-to-LAN

This saves time, reduces errors, and simplifies troubleshooting.

🧪 Lab Setup



🔧 Network Topology

- PC1: 192.168.10.10 (VLAN 10)
- PC2: 192.168.20.20 (VLAN 20)
- PC3: 192.168.30.30 (VLAN 30)

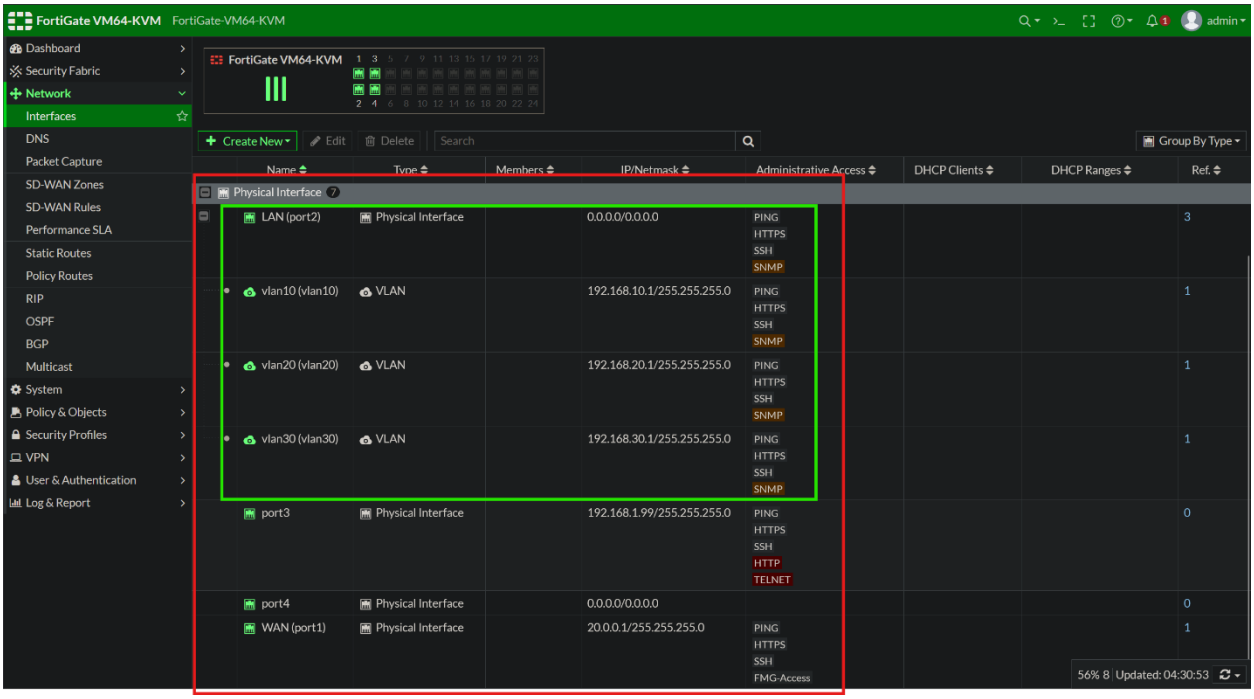
These PCs are connected to a Cisco switch with VLANs configured:

- VLAN 10, VLAN 20, VLAN 30
- PC ports: Access ports
- Firewall port: Trunk port

```
Switch#
Switch#show vlan bri
Switch#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Gi1/0, Gi1/1, Gi1/2, Gi1/3
10   VLAN0010                         active    Gi0/1
20   VLAN0020                         active    Gi0/2
30   VLAN0030                         active    Gi0/3
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup
Switch#
Switch#
Switch#show inter
Switch#show interfaces trunk

Port        Mode             Encapsulation  Status        Native vlan
Gi0/0       on               802.1q         trunking      1

Port        Vlans allowed on trunk
Gi0/0       1-4094

Port        Vlans allowed and active in management domain
Gi0/0       1,10,20,30

Port        Vlans in spanning tree forwarding state and not pruned
Gi0/0       1,10,20,30
Switch#
```

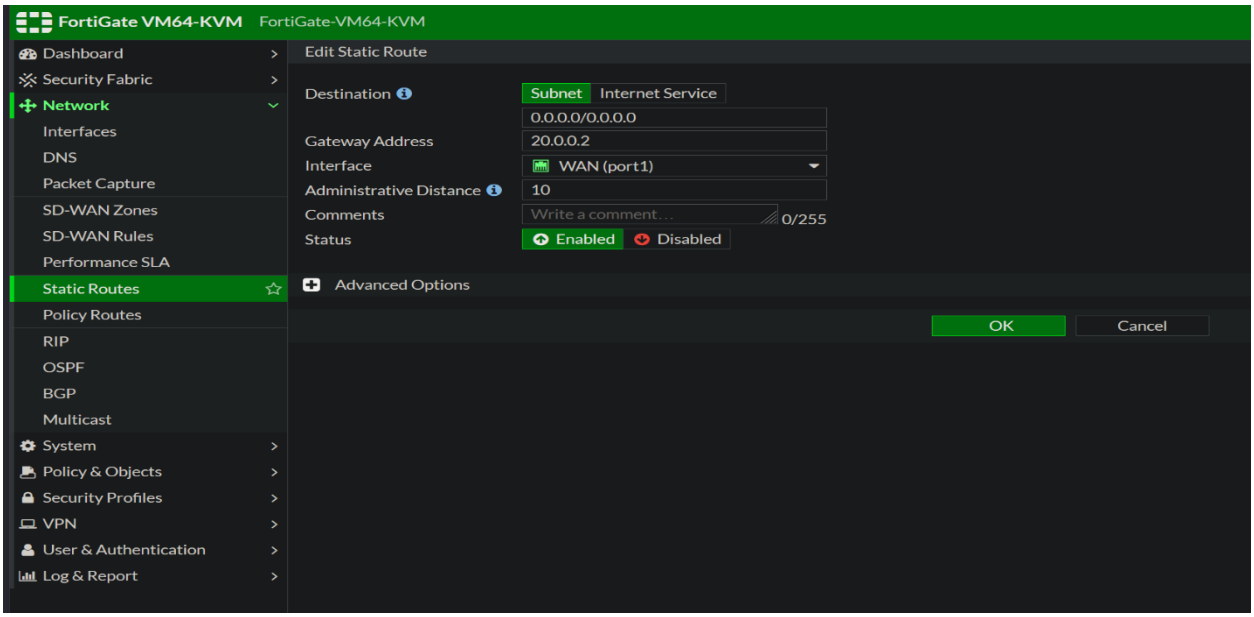
🌐 FortiGate Firewall Configuration

- LAN interface: Trunk port (with sub-interfaces for VLAN 10, 20, 30)
  - lan.10 – 192.168.10.1
  - lan.20 – 192.168.20.1
  - lan.30 – 192.168.30.1
- **WAN interface: 20.0.0.1 (connected to Cisco WAN router)**



The interfaces marked with a red are physical interfaces, while the ones marked with a green are VLANs created under the LAN port.

- **The static route has been created.**



🌐 Cisco Router Configuration

Configured the WAN interface with IP 20.0.0.2 and added a static route pointing to the FortiGate for internet-bound traffic.

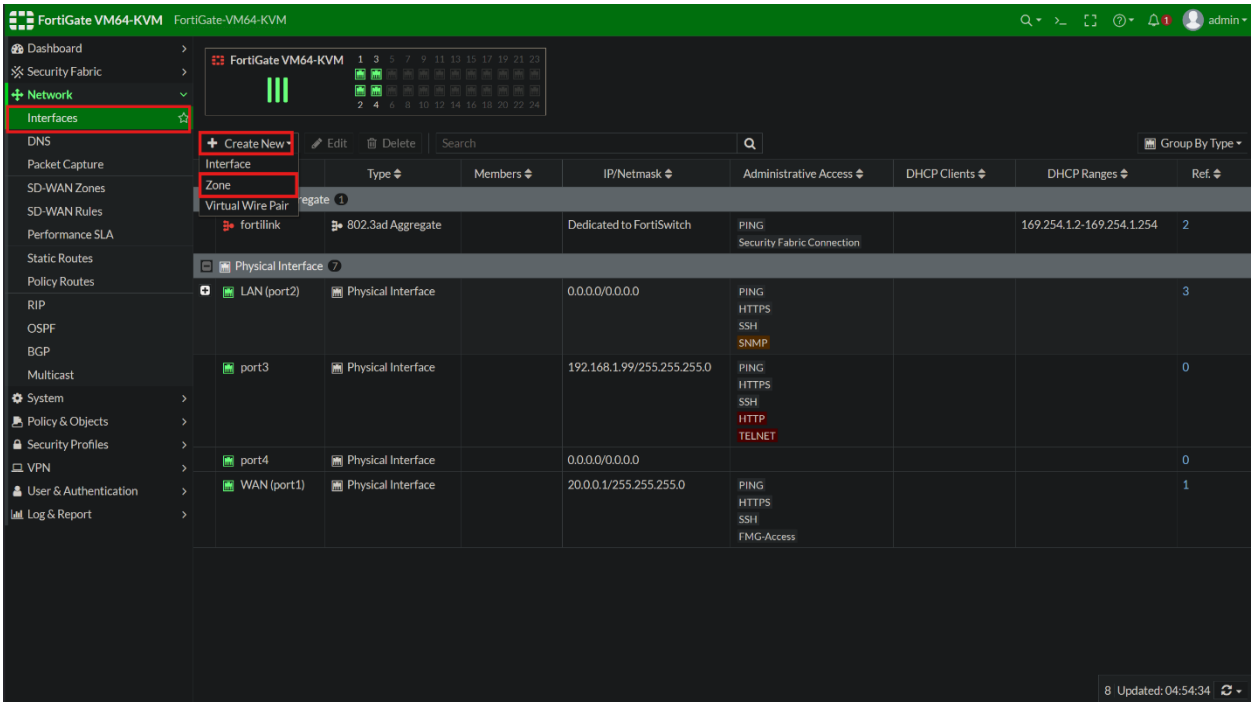
```
Router#
Router#
Router#
Router#show ip inter
Router#show ip interface bri
Router#show ip interface brief
Interface                  IP-Address      OK? Method Status                Prot
ocol
GigabitEthernet0/0         20.0.0.2        YES manual up                    up

GigabitEthernet0/1         unassigned      YES unset  administratively down down

GigabitEthernet0/2         unassigned      YES unset  administratively down down

GigabitEthernet0/3         unassigned      YES unset  administratively down down

Router#show ip rou
Router#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       a - application route
       + - replicated route, % - next hop override, p - overrides from PfR

Gateway of last resort is 20.0.0.1 to network 0.0.0.0

S*    0.0.0.0/0 [1/0] via 20.0.0.1
                is directly connected, GigabitEthernet0/0
      20.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        20.0.0.0/24 is directly connected, GigabitEthernet0/0
L        20.0.0.2/32 is directly connected, GigabitEthernet0/0
Router#
```

Upon testing network connectivity, we were able to successfully ping the FortiGate LAN interface (marked in green) from the LAN PC. However, we were unable to establish connectivity from the LAN PC to the WAN interface (marked in red)

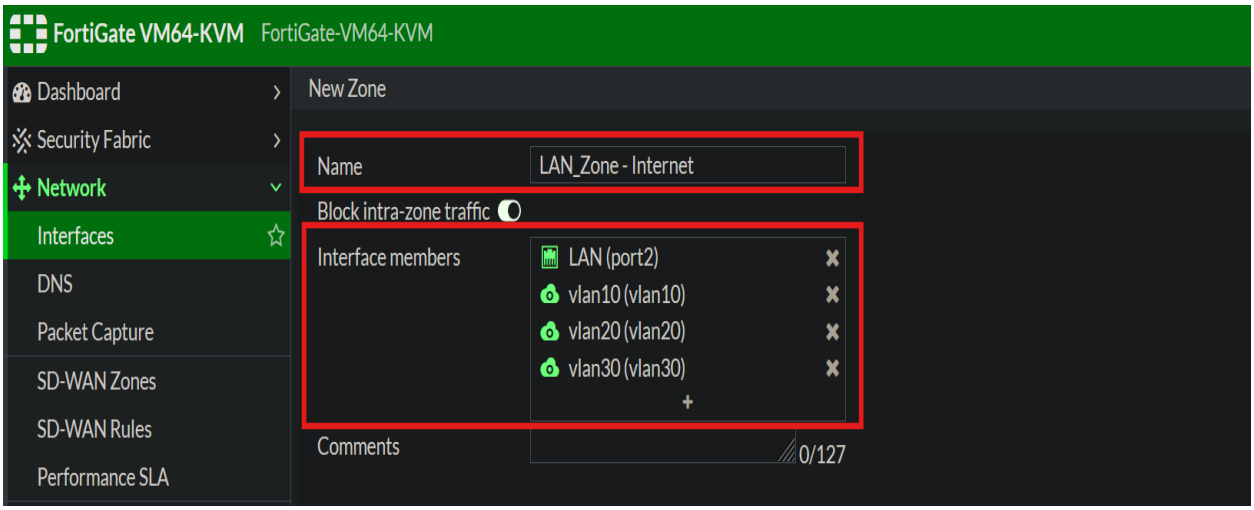
```
VPCS>
VPCS>
VPCS>
VPCS>
VPCS>
VPCS> ping 192.168.10.1

84 bytes from 192.168.10.1 icmp_seq=1 ttl=255 time=4.647 ms
84 bytes from 192.168.10.1 icmp_seq=2 ttl=255 time=4.513 ms
84 bytes from 192.168.10.1 icmp_seq=3 ttl=255 time=5.251 ms
84 bytes from 192.168.10.1 icmp_seq=4 ttl=255 time=4.710 ms
84 bytes from 192.168.10.1 icmp_seq=5 ttl=255 time=1.613 ms

VPCS> ping 20.0.0.2

20.0.0.2 icmp_seq=1 timeout
20.0.0.2 icmp_seq=2 timeout
20.0.0.2 icmp_seq=3 timeout
20.0.0.2 icmp_seq=4 timeout
20.0.0.2 icmp_seq=5 timeout

VPCS>
VPCS>
VPCS>
```

The lack of connectivity is due to the absence of a security policy.
Now, we're going to implement the **zone concept** to manage and simplify policy creation.

To create a zone in FortiGate:Click **Network**, then select **Interfaces**. Click **Create New**, and choose **Zone**.



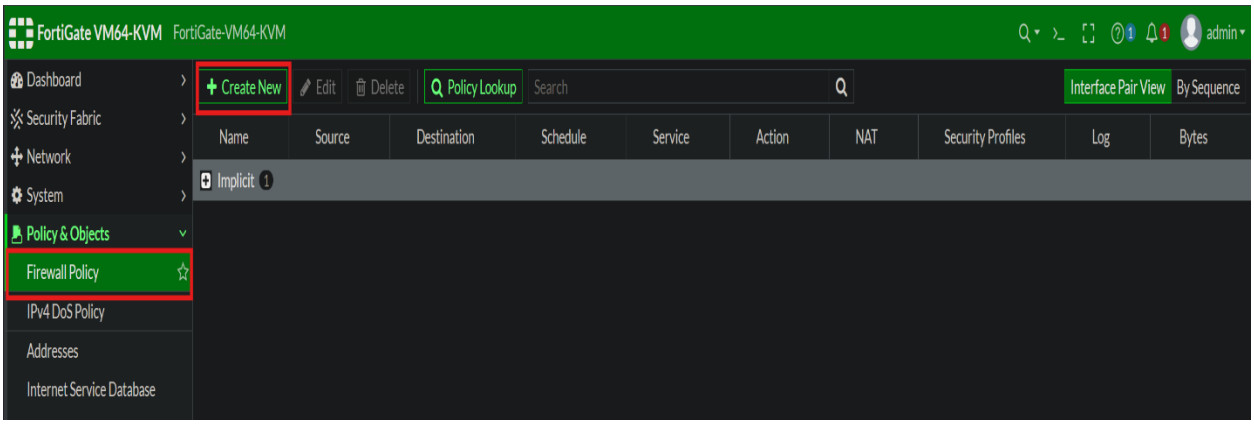
Give the zone a name of your choice, then add LAN Port, VLAN 10, VLAN 20, and VLAN 30 as interface members. This allows traffic coming through these interfaces to flow freely within the zone.

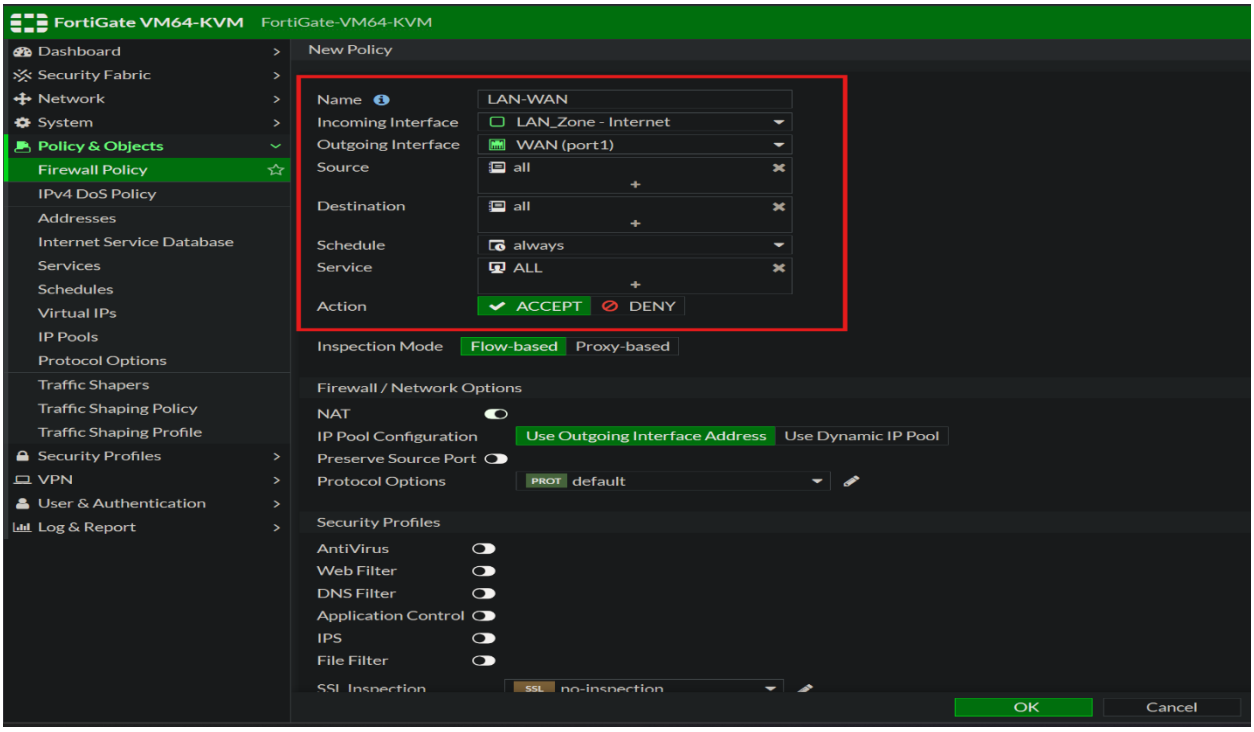


To create a policy, go to **Policy & Objects → Firewall Policy** and click **Create New**.

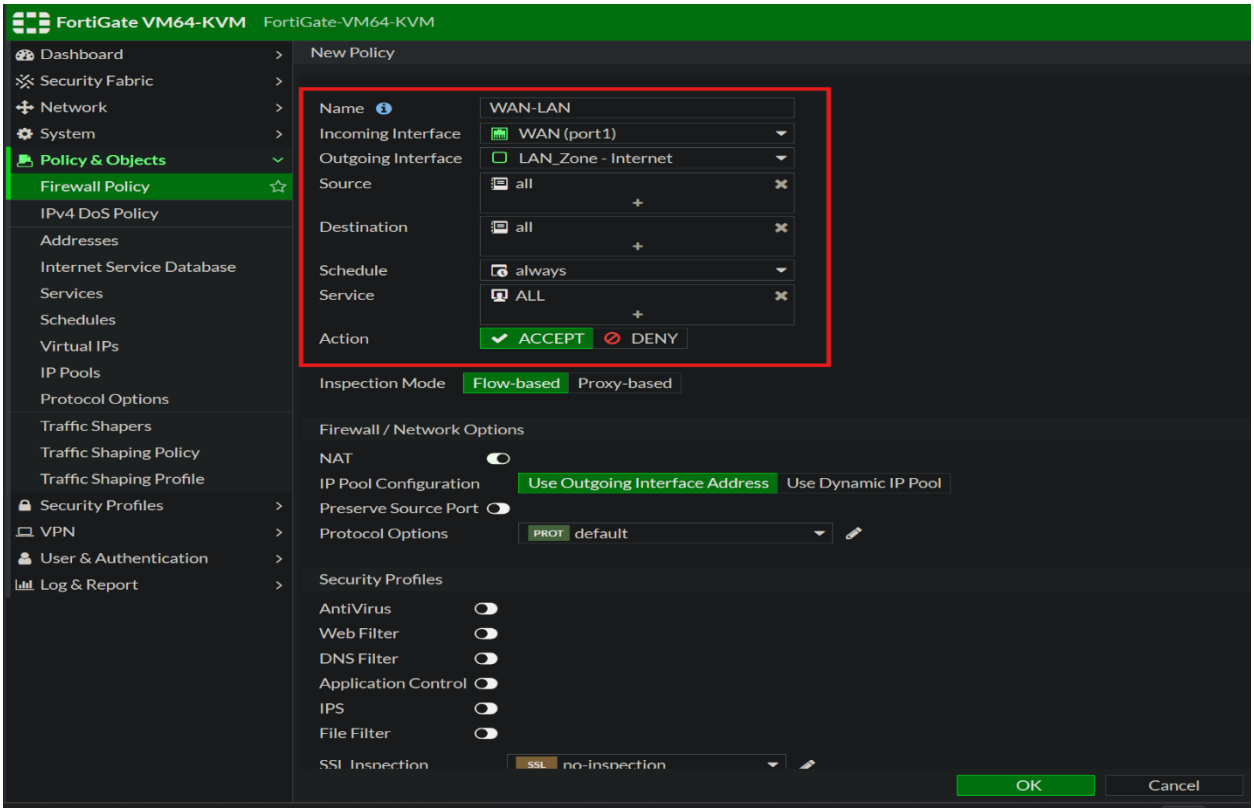
First, we are going to create a policy for LAN to WAN connectivity.

Enter a name for the policy, set the incoming interface to the zone you created, the outgoing interface to WAN, and configure the source, destination, and service as needed

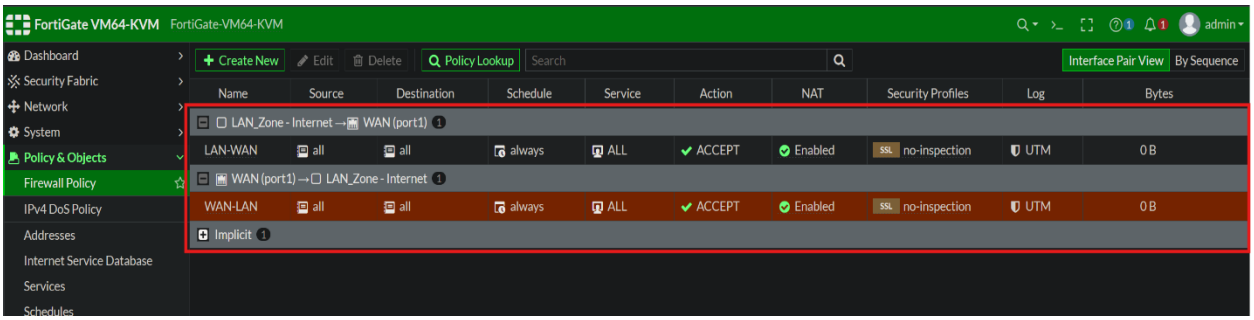




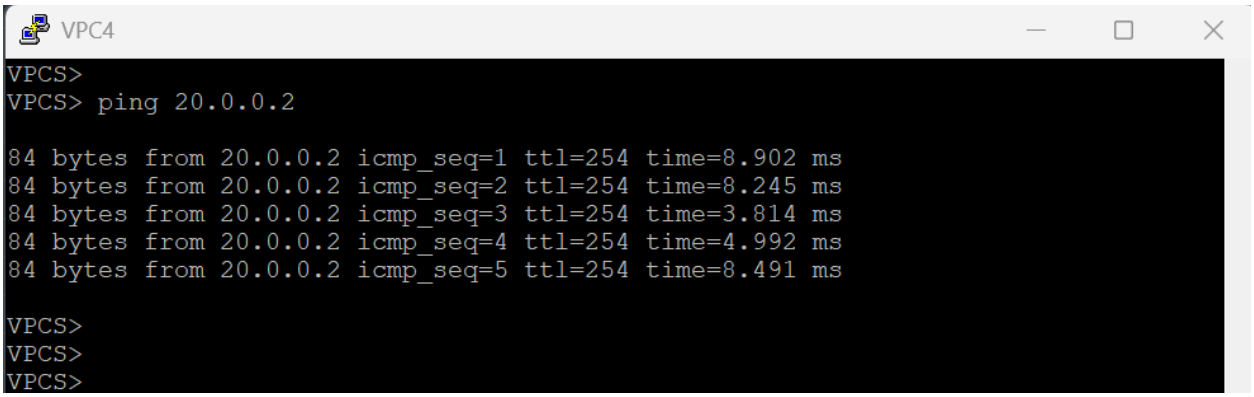
Let’s create a policy for traffic from WAN to LAN.

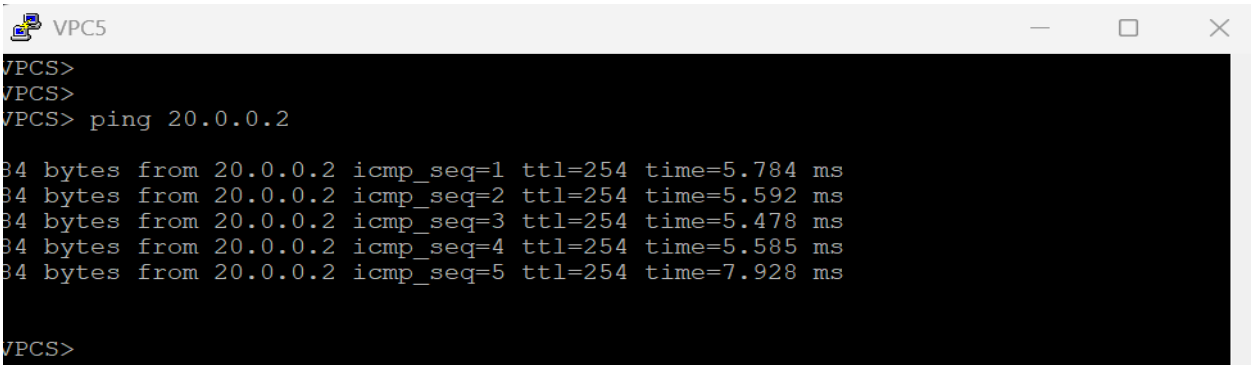


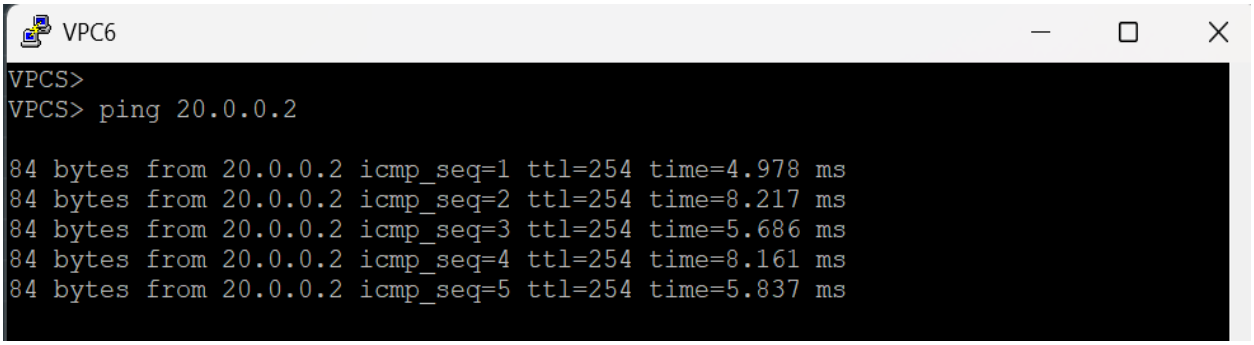
Here, you can see both policies that we have created.



We have now successfully created the policies using the zone. Let's verify connectivity from each LAN PC to the WAN.

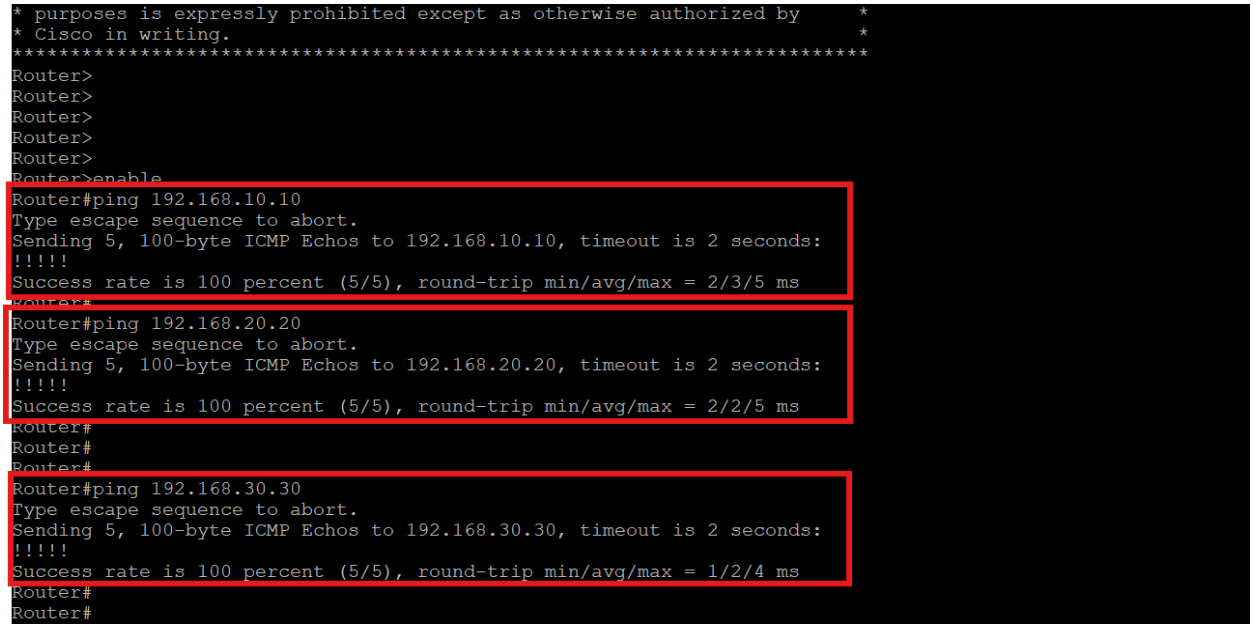






Yes! We're successfully getting connectivity from all LAN PCs to the WAN 😎 🎉.

Next, let’s test the connectivity **from the WAN router to the LAN PCs** to ensure bidirectional communication is working properly.



.Awesome! Ping successful from WAN to LAN PCs 😎🎉
The zone-based policy setup is working perfectly!

✅ Outcome

- All VLANs have internet access.
- Policies are simplified using Zones.
- Easier to scale when adding more VLANs—just add them to the zone.

💡 Use Cases for Zones in FortiGate

- Grouping **LAN VLANs** for simplified policy creation.
- Separating **DMZ**, **Guest**, or **IoT networks**.
- Grouping **WAN interfaces** when multi-WAN setup is used.
- Applying **inspection profiles** uniformly to all zone members.

🔚 Conclusion

Using **Zones in FortiGate** improves network manageability, reduces admin overhead, and enhances security policy consistency. This lab demonstrates how even a basic multi-VLAN network can benefit from Fortinet's zone-based approach.

Thanks

for your time!

Keep learning, and keep growing!....

Submitted by: Rahul K G

www.linkedin.com/in/rahul-k-gopi-a703ba16a