



# 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.



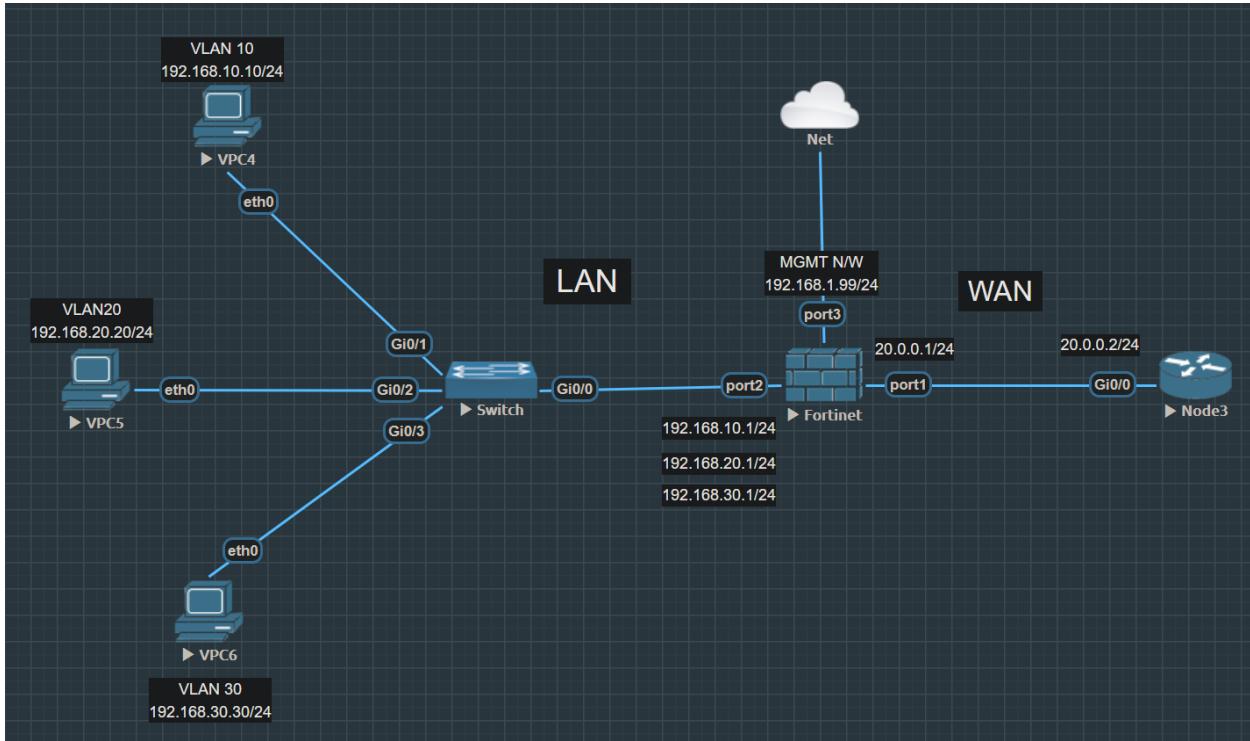
## Concept Overview

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 screenshot shows the FortiGate VM64-KVM interface configuration. The left sidebar navigation includes: Dashboard, Security Fabric, Network (selected), Interfaces, DNS, Packet Capture, SD-WAN Zones, SD-WAN Rules, Performance SLA, Static Routes, Policy Routes, RIP, OSPF, BGP, Multicast, System, Policy & Objects, Security Profiles, VPN, User & Authentication, and Log & Report.

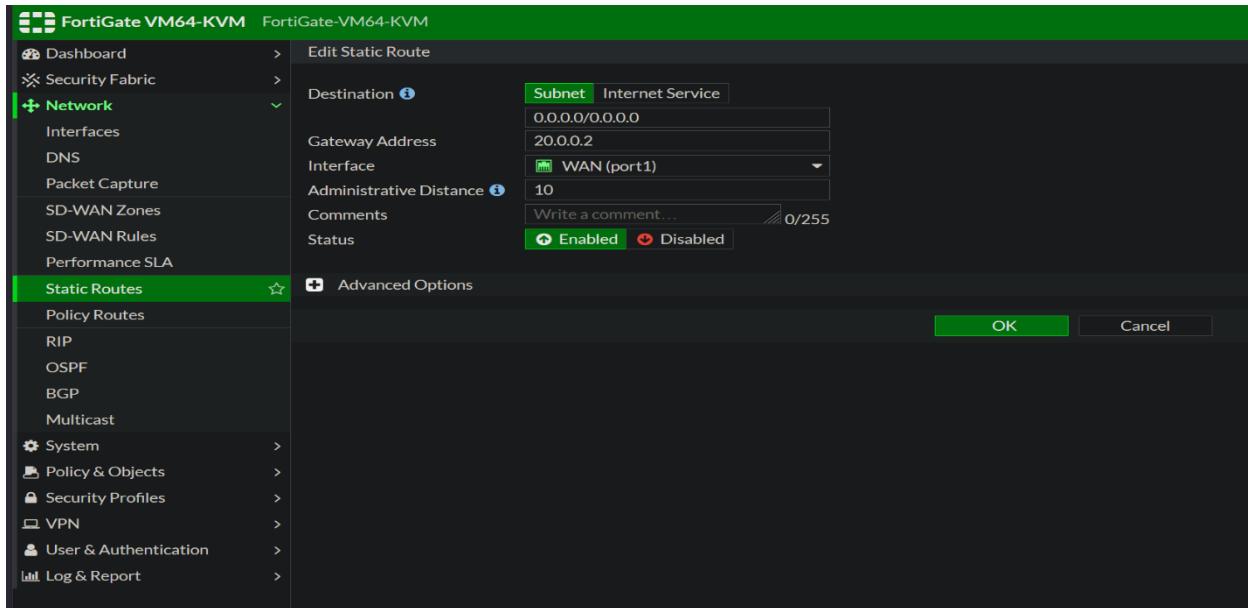
The main interface view displays a table of network interfaces:

Name	Type	Members	IP/Netmask	Administrative Access	DHCP Clients	DHCP Ranges	Ref.
Physical Interface 7	Physical Interface		0.0.0/0.0.0	PING HTTPS SSH SNMP	3		
LAN (port2)	Physical Interface	vlan10 (vlan10), vlan20 (vlan20), vlan30 (vlan30)	192.168.10.1/255.255.255.0	PING HTTPS SSH SNMP	1		
port3	Physical Interface		192.168.20.1/255.255.255.0	PING HTTPS SSH SNMP	1		
port4	Physical Interface		192.168.30.1/255.255.255.0	PING HTTPS SSH HTTP TELNET	1		0
WAN (port1)	Physical Interface		200.0.1/255.255.255.0	PING HTTPS SSH FMG-Access	1		

A red box highlights the Physical Interface row and the three VLAN sub-interfaces under the LAN port. A green box highlights the three VLAN sub-interfaces under the LAN port.

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
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**.

Interface	Type	Members	IP/Netmask	Administrative Access	DHCP Clients	DHCP Ranges	Ref.
fortilink	Virtual Wire Pair			PING Security Fabric Connection		169.254.1.2-169.254.1.254	2
802.3ad Aggregate	Virtual Wire Pair						
Virtual Wire Pair	Virtual Wire Pair						
Physical Interface							
LAN (port2)	Physical Interface		0.0.0/0.0.0	PING HTTPS SSH SNMP			3
port3	Physical Interface		192.168.1.99/255.255.255.0	PING HTTPS SSH HTTP TELNET			0
port4	Physical Interface		0.0.0/0.0.0				0
WAN (port1)	Physical Interface		20.0.0.1/255.255.255.0	PING HTTPS SSH FMG-Access			1

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.

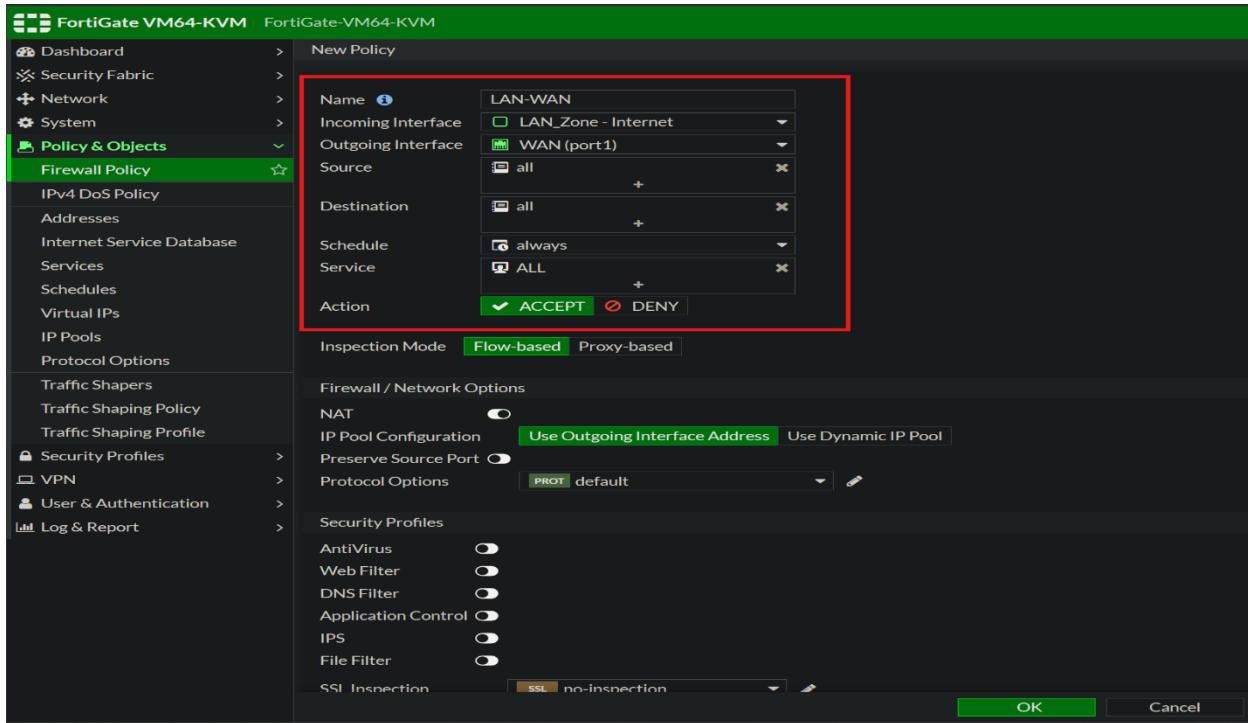
The screenshot shows the FortiGate VM64-KVM interface. On the left, the navigation menu is visible with items like Dashboard, Security Fabric, Network (selected), Interfaces, DNS, Packet Capture, SD-WAN Zones, SD-WAN Rules, and Performance SLA. The main area is titled 'New Zone' and contains fields for 'Name' (set to 'LAN\_Zone - Internet'), 'Block intra-zone traffic' (unchecked), and 'Interface members' (a list containing LAN (port2), vlan10 (vlan10), vlan20 (vlan20), and vlan30 (vlan30)). A red box highlights the 'Name' field and the 'Interface members' list.

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

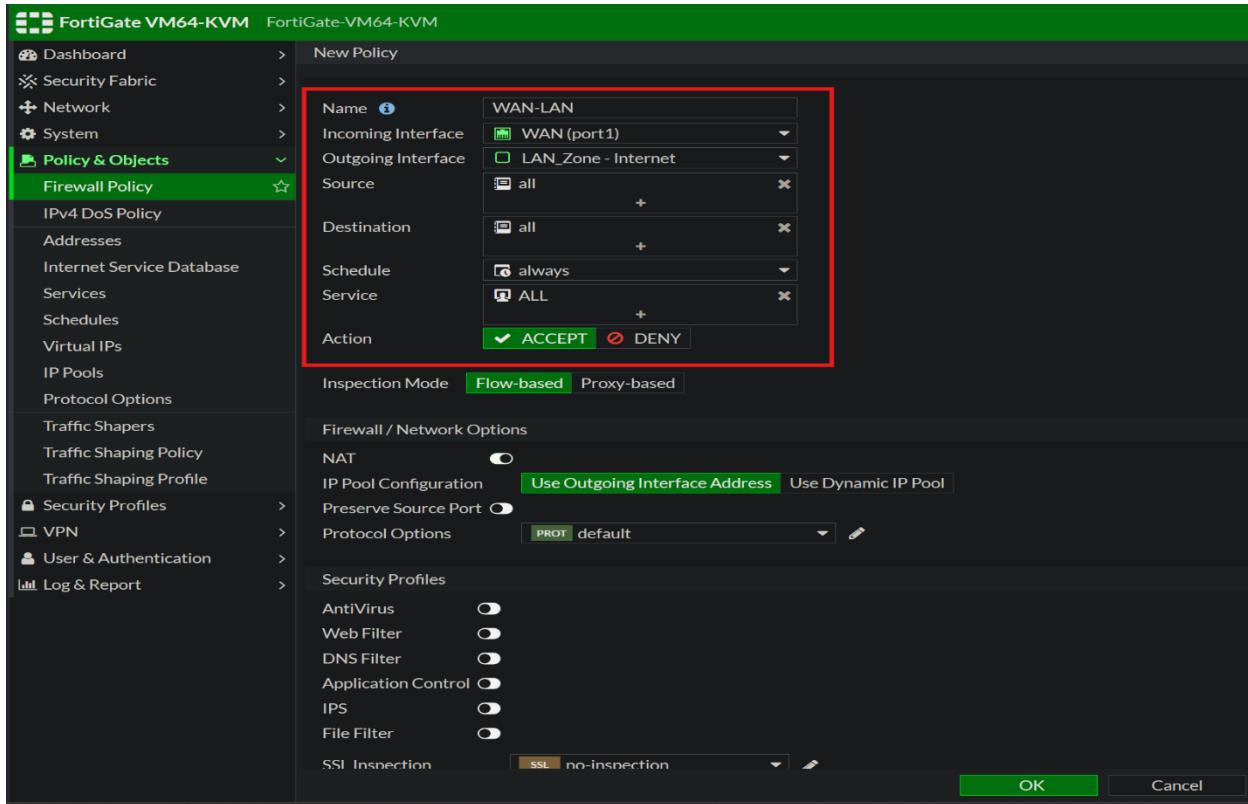
First, we are going to create a policy for LAN to WAN connectivity.

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

The screenshot shows the FortiGate VM64-KVM interface. The navigation menu on the left includes Policy & Objects (selected) and Firewall Policy (highlighted with a red box). The main area displays a table for Firewall Policy with columns: Name, Source, Destination, Schedule, Service, Action, NAT, Security Profiles, Log, and Bytes. A row for 'Implicit 1' is shown. A red box highlights the 'Create New' button in the top-left corner of the main content area.



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



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

The screenshot shows the FortiGate VM64-KVM interface under the 'Policy & Objects' section, specifically the 'Firewall Policy' tab. A red box highlights the first two policies in the list:

Name	Source	Destination	Schedule	Action	NAT	Security Profiles	Log	Bytes	
LAN-Zone - Internet → WAN (port1)	all	all	always	ALL	ACCEPT	Enabled	no-inspection	UTM	0 B
WAN (port1) → LAN_Zone - Internet	WAN-LAN	all	always	ALL	ACCEPT	Enabled	no-inspection	UTM	0 B
Implicit									

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

```
VPCS>
VPCS> ping 20.0.0.2

84 bytes from 20.0.0.2 icmp_seq=1 ttl=254 time=8.902 ms
84 bytes from 20.0.0.2 icmp_seq=2 ttl=254 time=8.245 ms
84 bytes from 20.0.0.2 icmp_seq=3 ttl=254 time=3.814 ms
84 bytes from 20.0.0.2 icmp_seq=4 ttl=254 time=4.992 ms
84 bytes from 20.0.0.2 icmp_seq=5 ttl=254 time=8.491 ms
```

```
VPCS>
VPCS>
VPCS> ping 20.0.0.2

84 bytes from 20.0.0.2 icmp_seq=1 ttl=254 time=5.784 ms
84 bytes from 20.0.0.2 icmp_seq=2 ttl=254 time=5.592 ms
84 bytes from 20.0.0.2 icmp_seq=3 ttl=254 time=5.478 ms
84 bytes from 20.0.0.2 icmp_seq=4 ttl=254 time=5.585 ms
84 bytes from 20.0.0.2 icmp_seq=5 ttl=254 time=7.928 ms
```

```
VPCS>
VPCS>
VPCS> ping 20.0.0.2

84 bytes from 20.0.0.2 icmp_seq=1 ttl=254 time=4.978 ms
84 bytes from 20.0.0.2 icmp_seq=2 ttl=254 time=8.217 ms
84 bytes from 20.0.0.2 icmp_seq=3 ttl=254 time=5.686 ms
84 bytes from 20.0.0.2 icmp_seq=4 ttl=254 time=8.161 ms
84 bytes from 20.0.0.2 icmp_seq=5 ttl=254 time=5.837 ms
```

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.

```
* purposes is expressly prohibited except as otherwise authorized by      *
* Cisco in writing.                                                 *
*****
Router>
Router>
Router>
Router>
Router>
Router>enable
Router#ping 192.168.10.10
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.10.10, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 2/3/5 ms
Router#
Router#ping 192.168.20.20
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.20.20, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 2/2/5 ms
Router#
Router#
Router#ping 192.168.30.30
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.30.30, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
Router#
Router#
```

.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](https://www.linkedin.com/in/rahul-k-gopi-a703ba16a)