FortiGate Configuration Documentation – SD-WAN Configuration & Routing

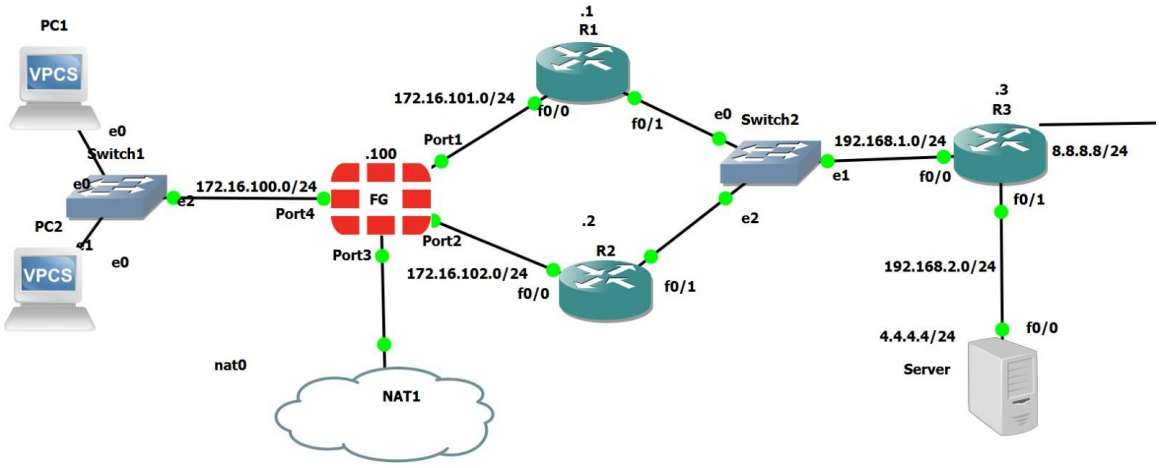
Lab Title: FortiGate SD-WAN Topology and Policy Routing Setup

Prepared by: Afaf Wael Mohammad Mokhtar

Objective:

To configure FortiGate firewall with SD-WAN rules, policy-based routing, and firewall configurations to ensure efficient, redundant, and policy-directed traffic flow.

Part A: Topology-Based Configuration



1. Topology Summary:

- PCs (PC1 and PC2) are connected to Switch1, which uplinks to FortiGate Port4.
- FortiGate has interfaces configured as follows:
- Port1 (LAN): 172.16.100.1/24
- Port2 (WAN2): 172.16.102.1/24 → connects to R2
- Port3 (WAN1): 172.16.101.1/24 → connects to R1
- Port4: 192.168.153.11/24
- R1 and R2 connect to Switch2, which links to R3.
- R3 routes traffic toward public IP 8.8.8.8 and internal server 4.4.4.4 (in 192.168.2.0/24).

2. Interface Configuration:

- Interfaces have alias names such as “LAN”, “WAN1”, and “WAN2”.
- LLDP and SNMP indexing are enabled on all interfaces.
- Allowaccess includes: ping, https, ssh, telnet, and fgfm.

3. Static Routing:

- Default route via R1 (WAN1) using Port3.
- Static route for server 4.4.4.4/24 via R2 (WAN2) using Port2.

4. SD-WAN Configuration:

- WAN1 and WAN2 added to the SD-WAN zone.
- Health-check criteria: latency < 200 ms, jitter < 50 ms, loss < 5%.
- FortiGate fails over to WAN2 if SLA on WAN1 fails.

5. SD-WAN Rules:

- Rule1: General internet traffic uses WAN1 with failover to WAN2.
- Rule2: Traffic to 4.4.4.4 is forced through WAN2.

6. Firewall Policies:

- LAN → SD-WAN zone policy with NAT enabled.
- Reverse policy configured as needed without NAT.

7. Policy-Based Routing:

- Static PBR for 4.4.4.4 traffic to always use WAN2.
- Ensures application-specific routing consistency.

8. Logging:

- Logging is enabled for all firewall policies.

Part B: Troubleshooting and Monitoring

1. Diagnostic Tools:

- diagnose sys virtual-wan-link health-check
- get router info routing-table all
- execute ping, traceroute

2. Failure Testing:

- Disconnect WAN1 or WAN2 to verify auto-failover.
- SLA logs confirm failover behavior.

3. Monitoring:

- GUI dashboards used to monitor bandwidth and link health.
- CLI shows real-time SD-WAN SLA metrics.

**Note:

- DNS servers 208.91.112.53 and 208.91.112.52 set globally.
- The pdf attached to this documentation has screens for this task includes the configuration , troubleshooting and monitoring

Conclusion:

This lab demonstrates SD-WAN configuration, static and policy-based routing, SLA monitoring, and firewall control on FortiGate.