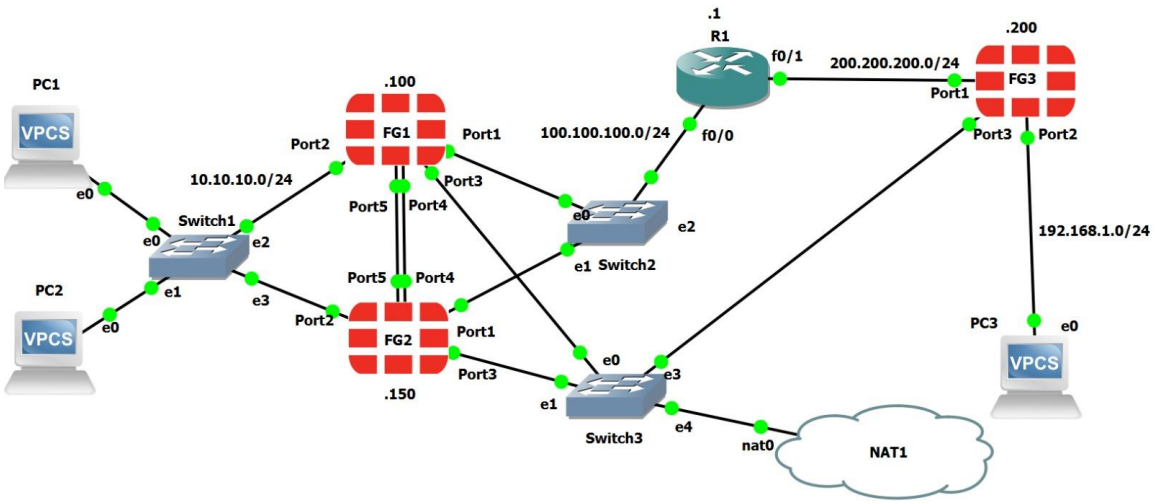
FortiGate Configuration Documentation – HA & IPSec Task

Lab Title: FortiGate HA and IPSec Configuration
Prepared by: Afaf Wael Mohammad Mokhtar

Objective:
To implement and validate HA deployment and IPSec VPN tunnels across multiple FortiGate units including FG2, based on provided configuration files and topology diagrams.

Task: High Availability (HA) & IPSec



Part A: HA Configuration

1. Topology:
- FG1: Primary
- FG2: Secondary (HA.conf)
- HA link via port3, port4

2. HA Mode: Active-Passive (A-P)

3. Priority:
- FG1 priority higher, sync enabled

4. CLI Verification:
- HA status checked on FG2 via CLI

Part B: IPSec VPN

1. Topology:
- Tunnel between FG1 and FG3

2. Firewall Policies:
- Allowed traffic over IPSec interfaces

3. Static Routing:
- Configured to reach remote subnets

4. Troubleshooting:
- Tunnel verified via Phase 1/2 status

5. Result:
- Tunnel established, ping successful

Included Configuration Files:

- **Diagram:** HA&IPSec.jpg
- **FG1:** F1_IPSec.conf
- **FG2:** HA.conf
- **FG3:** F3_IPSec.conf

**Note:

The pdf attached to this documentation has screens for this task includes the HA & SDWAN configuration, health checking & how it affects on the system

Conclusion:

This documentation summarizes the setup of HA and IPSec VPN between FortiGate units. It reflects enterprise-grade redundancy and security best practices.