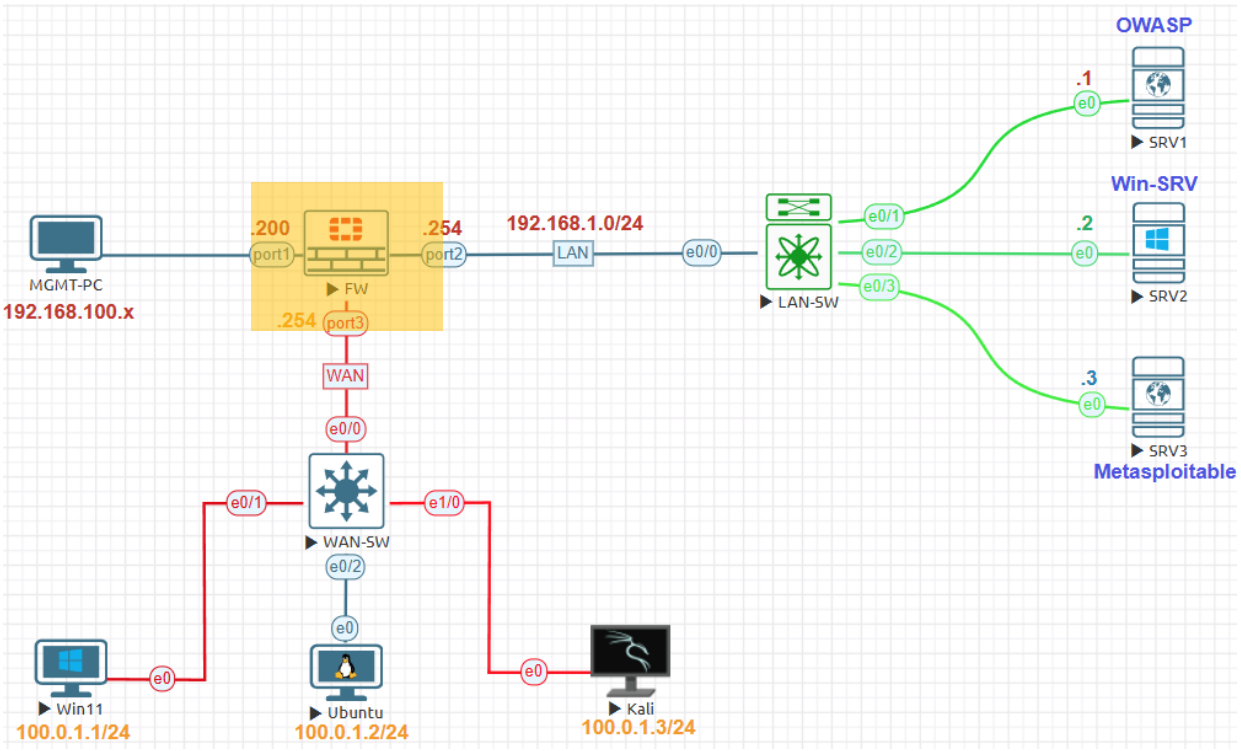
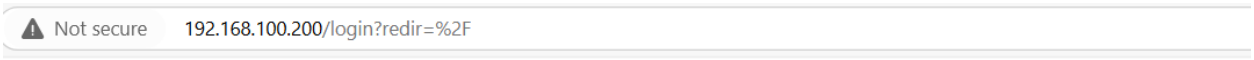
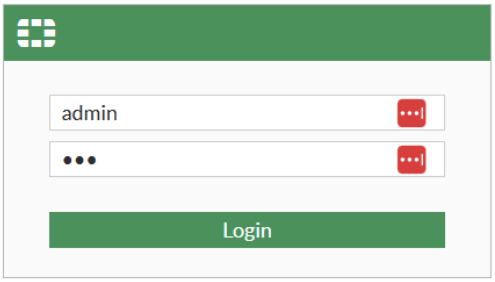
# Firewall Setup Lab:

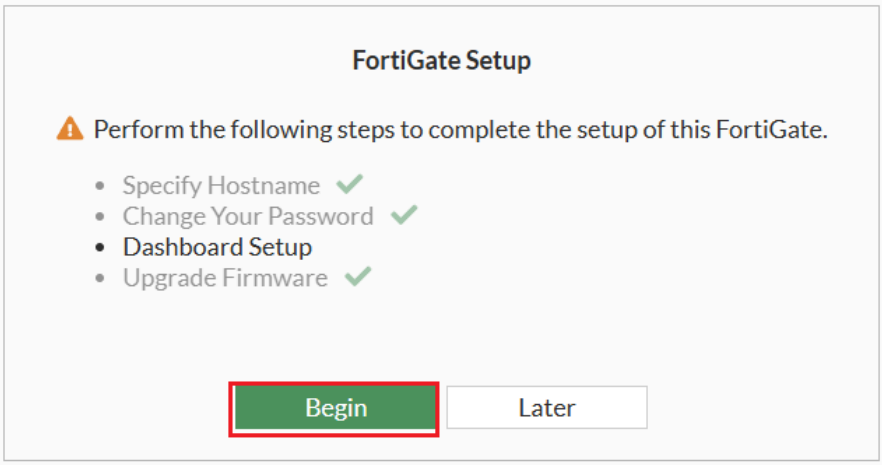


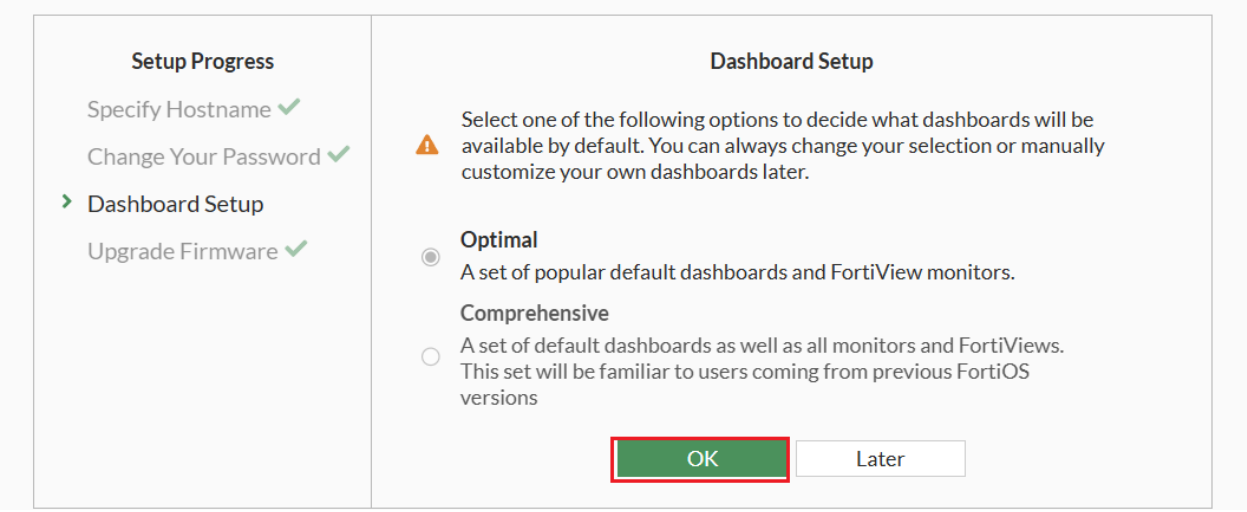

| | |
|---|---|
| Management Subnet | 192.168.100.0/24 |
| FortiGate Management IP | 192.168.100.200 |
| Internal Servers Subnet | 192.168.1.0/24 |
| FortiGate Firewall External | 100.0.1.0/24 |
| FortiGate Firewall Internal IP | 192.168.1.254 |
| FortiGate Firewall External IP | 100.0.1.254 |
| SRV1 IP Address | 192.168.1.1 |
| SRV2 IP Address | 192.168.1.2 |
| SRV3 IP Address | 192.168.1.3 |
| External Win11 IP Address | 100.0.1.1 |
| External Ubuntu IP Address | 100.0.1.2 |
| External Kali IP Address | 100.0.1.3 |

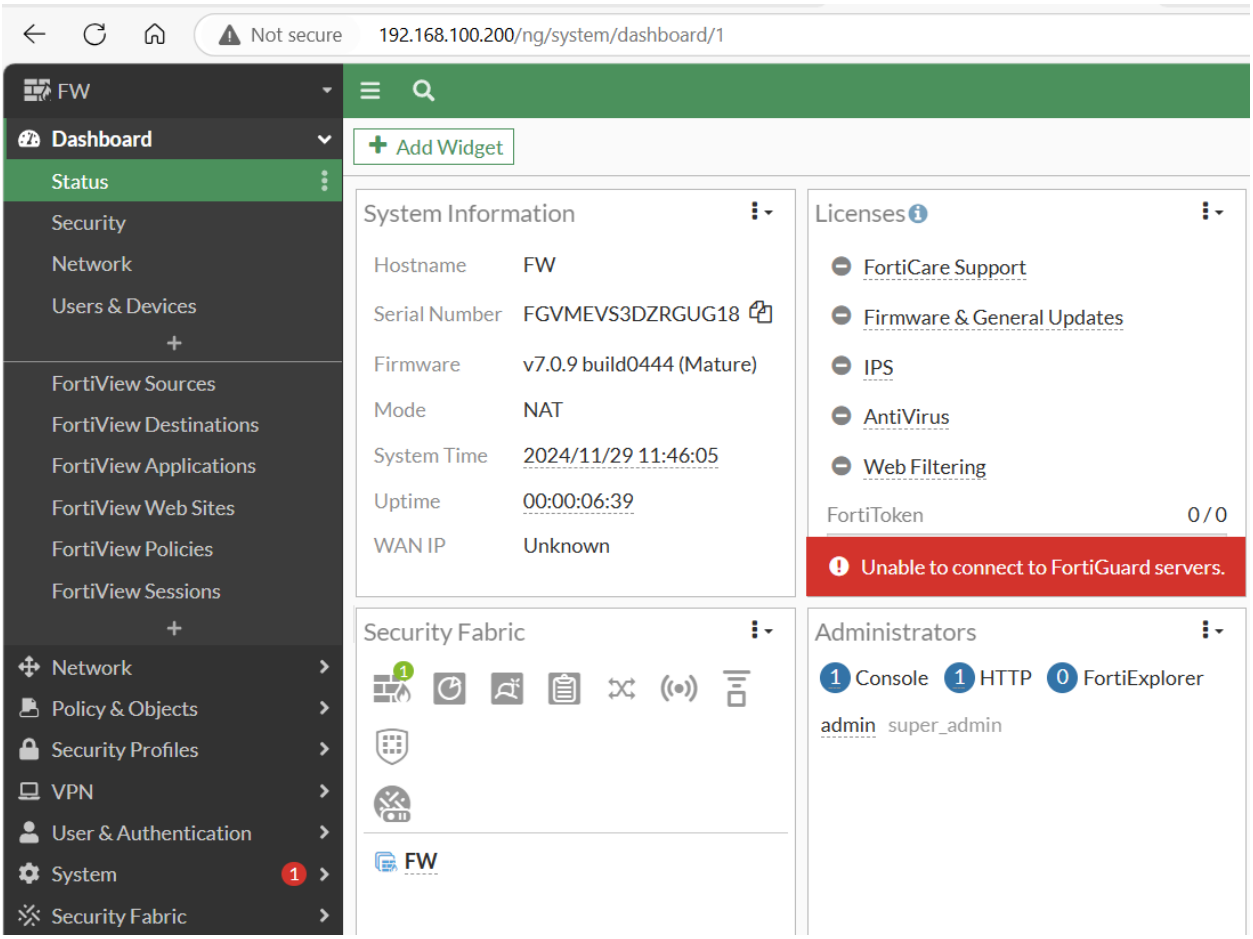
| Hostname Configuration |
| --- |
| FortiGate-VM64-KVM # config system global<br>FortiGate-VM64-KVM (global) # set hostname FW<br>FortiGate-VM64-KVM (global) # end |
| **Management Interface Configuration** |
| FW # config system interface<br>FW (interface) # edit port1<br>FW (port1) # set allowaccess https http ping ssh<br>FW (port1) # set mode static<br>FW (port1) # set ip 192.168.100.200/24<br>FW (port1) # end |

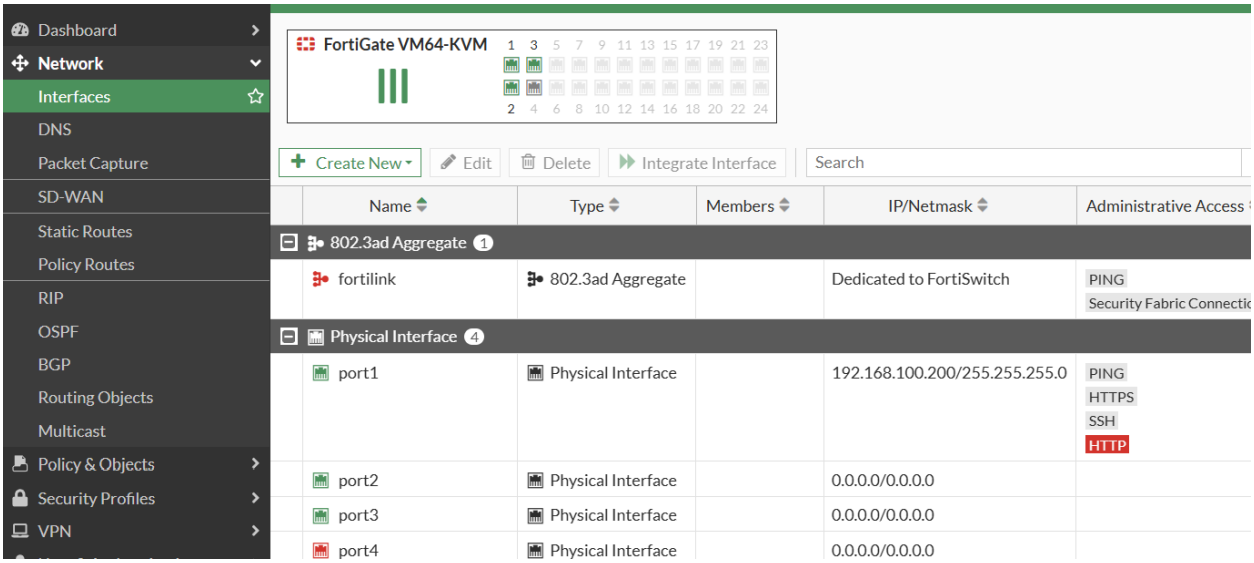


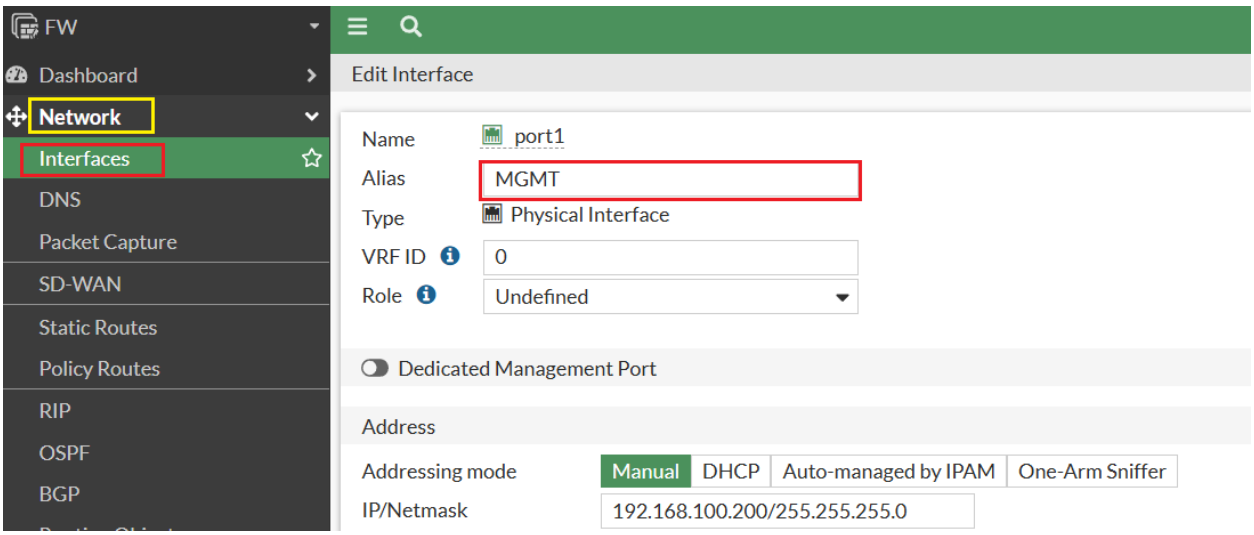



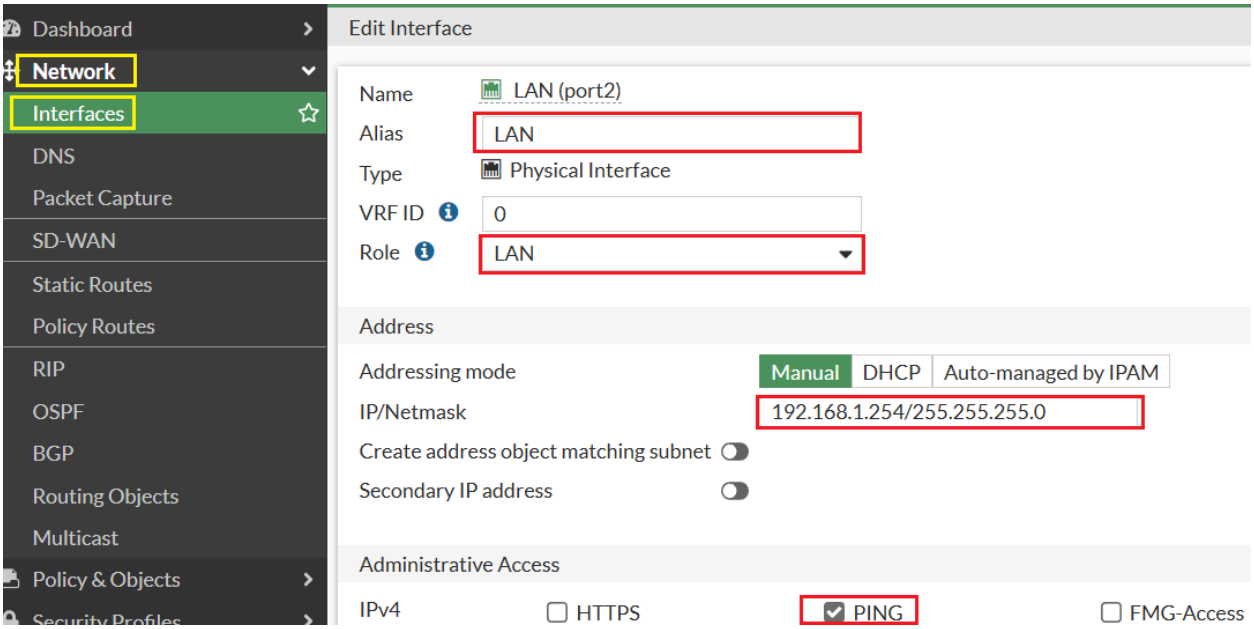



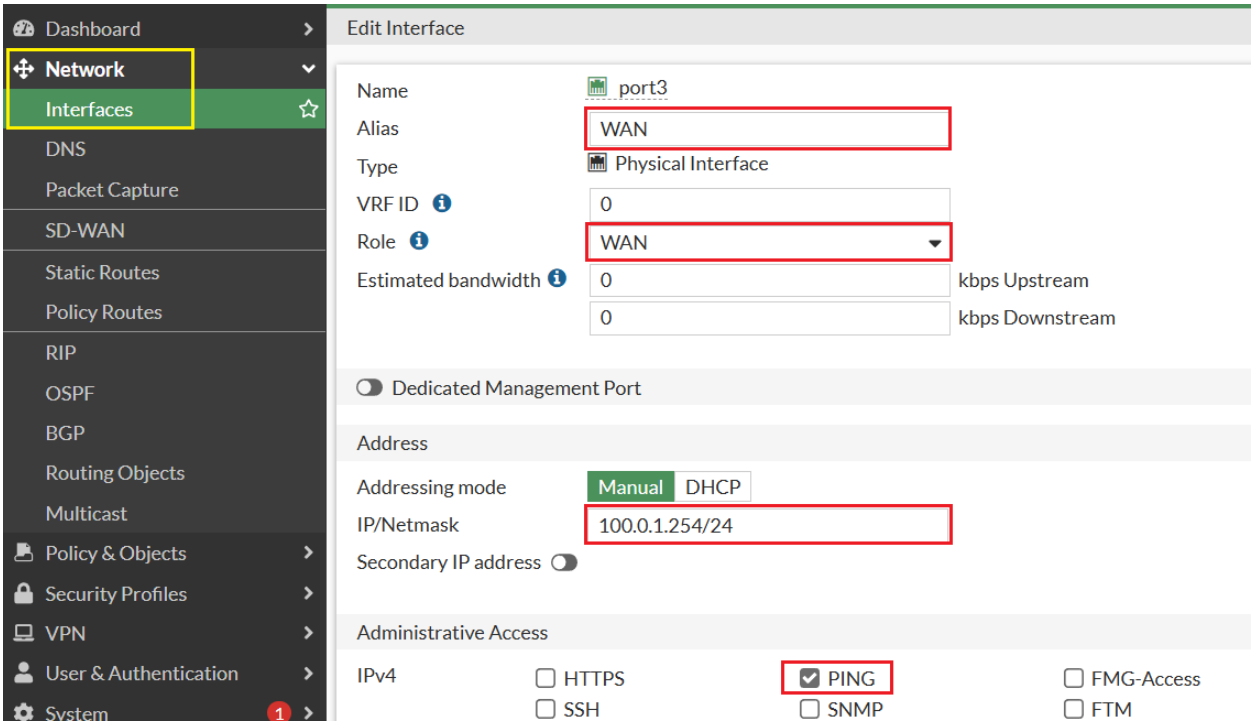


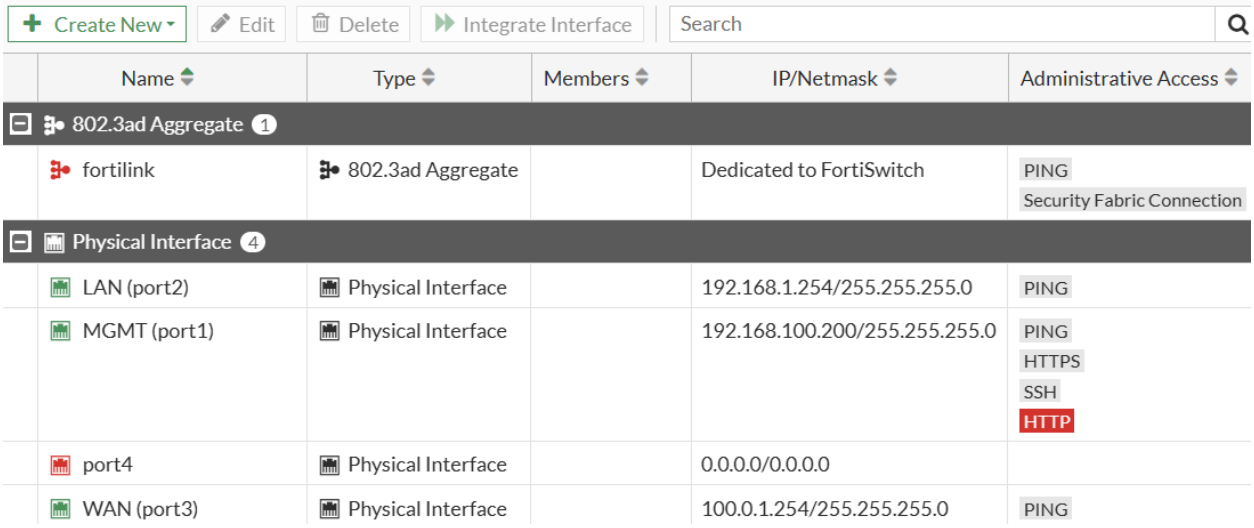



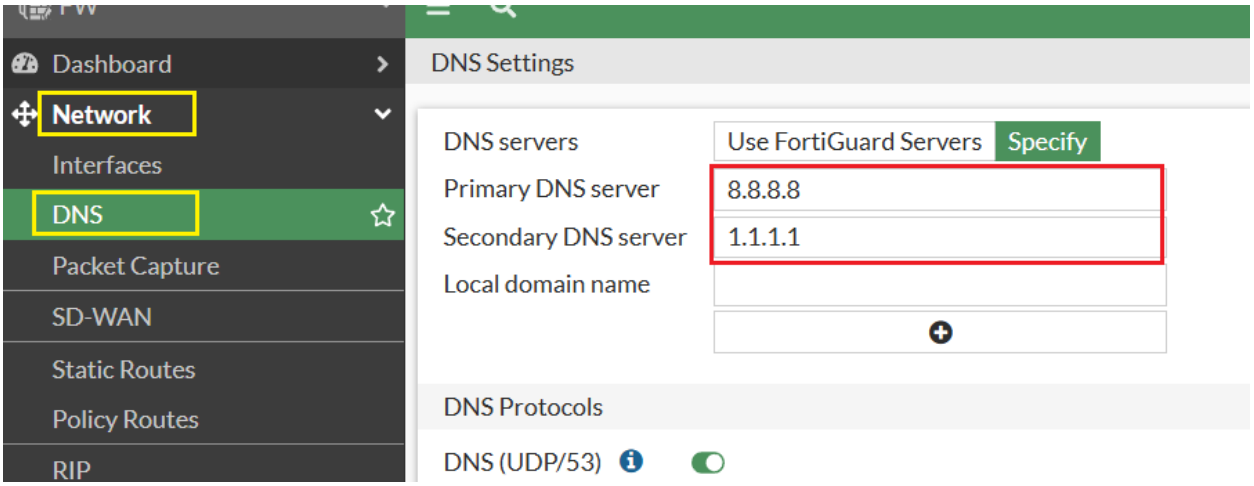


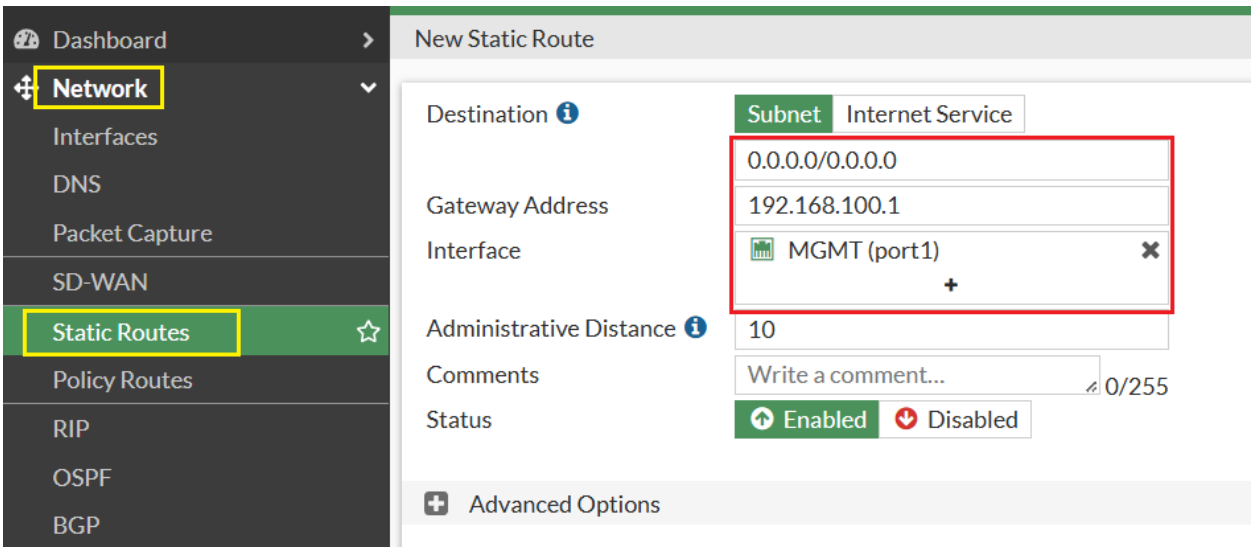



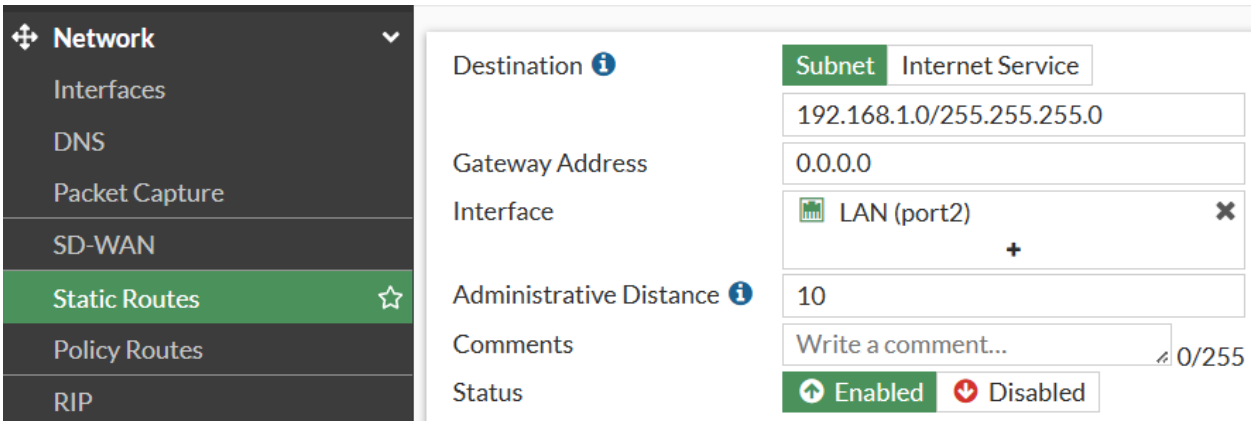


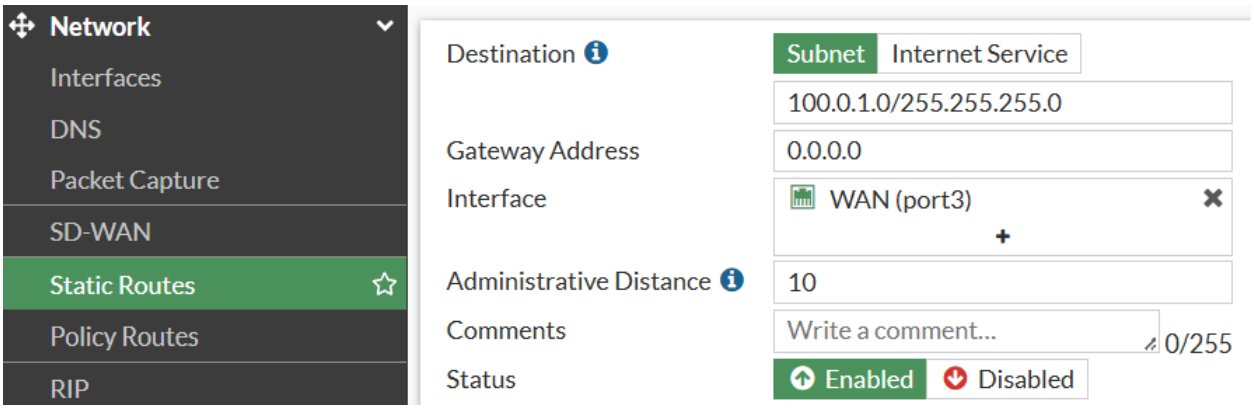



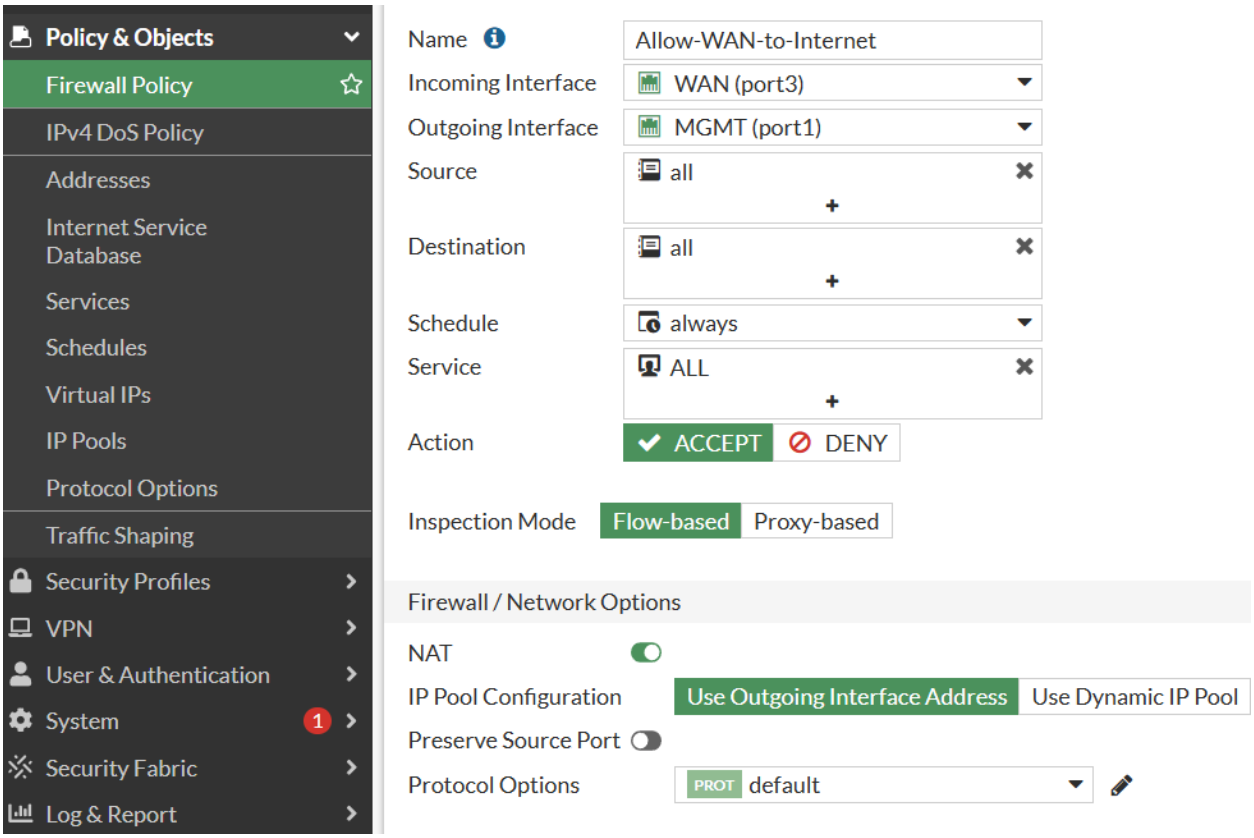


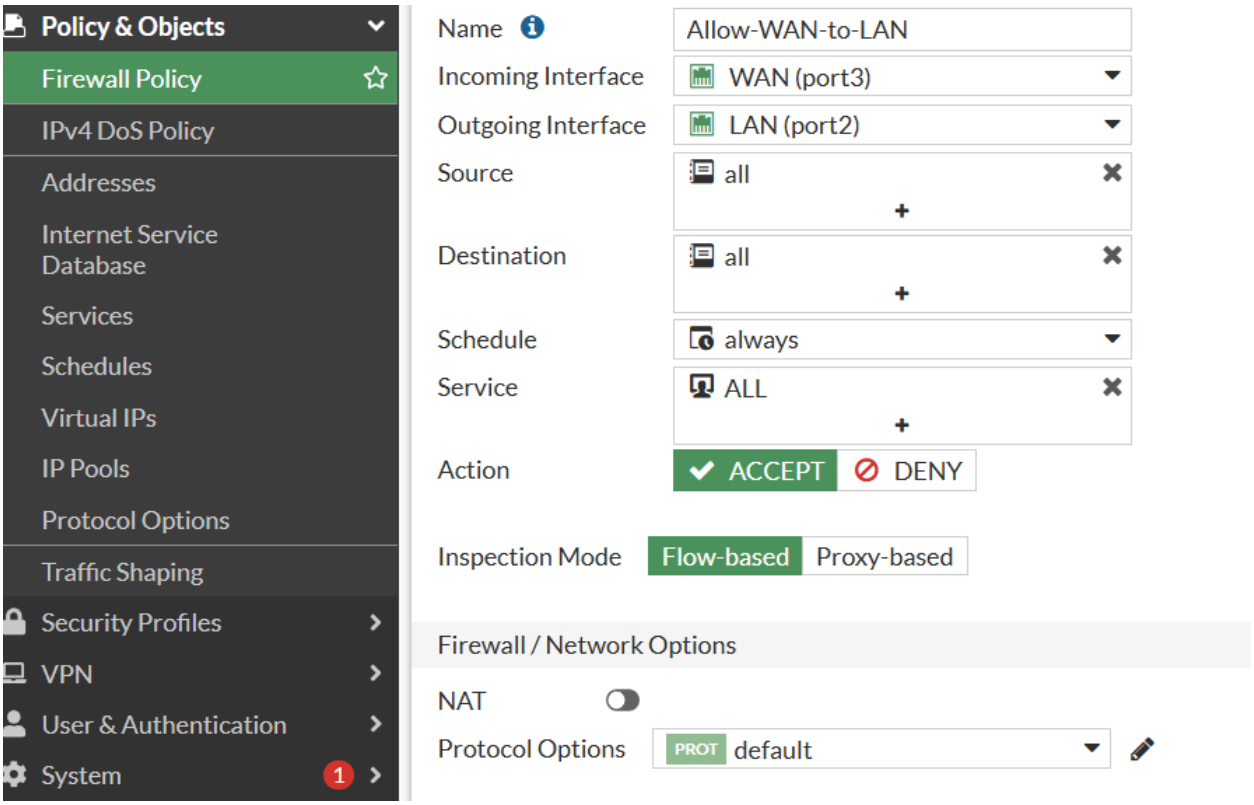



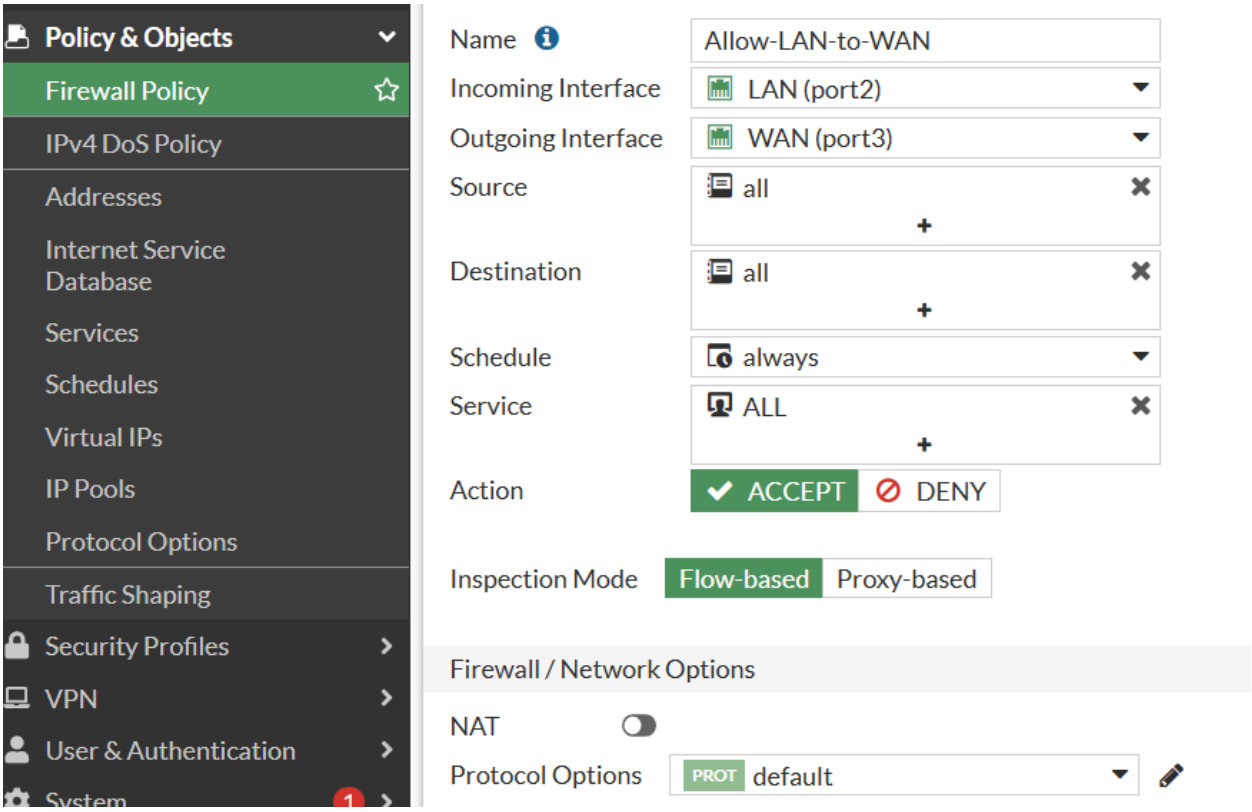



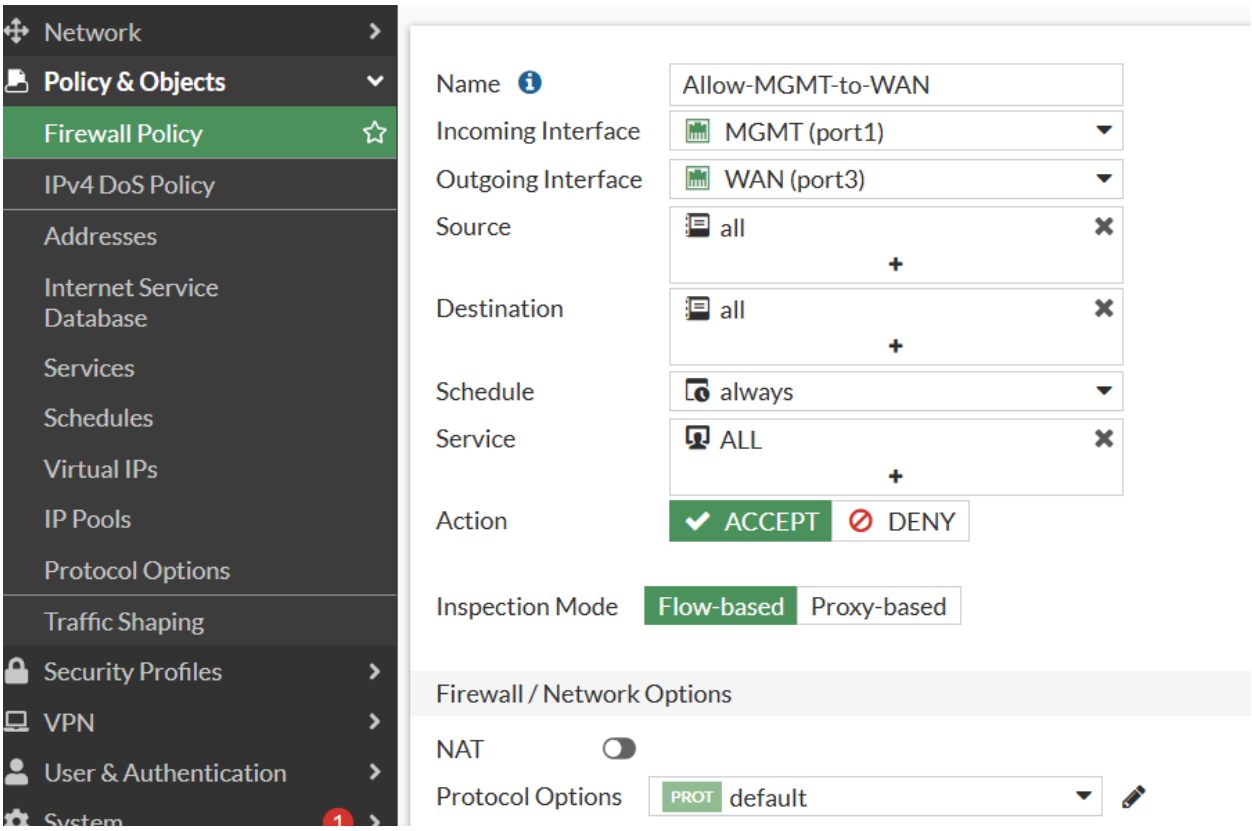


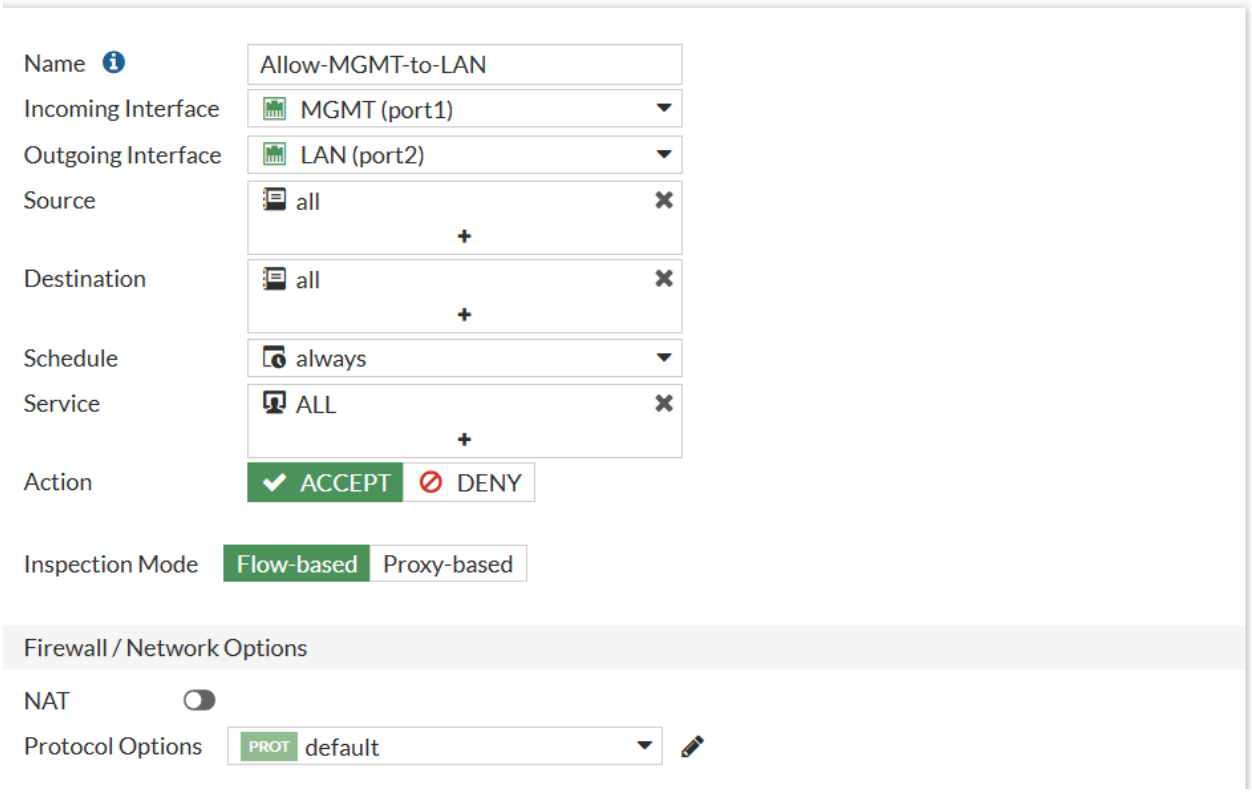



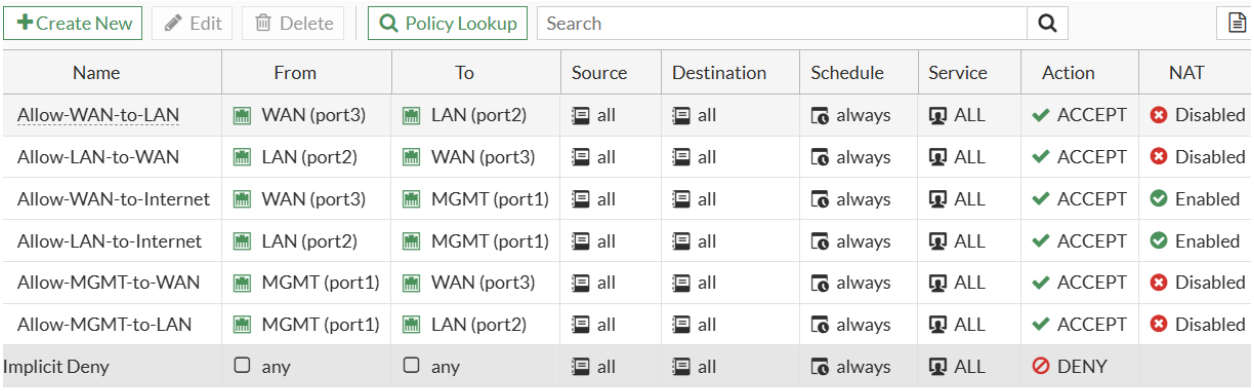







| Name | From | To | Source | Destination | Schedule | Service | Action | NAT |
|---|---|---|---|---|---|---|---|---|
| Allow-WAN-to-LAN | WAN (port3) | LAN (port2) | all | all | always | ALL | ACCEPT | Disabled |
| Allow-LAN-to-WAN | LAN (port2) | WAN (port3) | all | all | always | ALL | ACCEPT | Disabled |
| Allow-WAN-to-Internet | WAN (port3) | MGMT (port1) | all | all | always | ALL | ACCEPT | Enabled |
| Allow-LAN-to-Internet | LAN (port2) | MGMT (port1) | all | all | always | ALL | ACCEPT | Enabled |
| Allow-MGMT-to-WAN | MGMT (port1) | WAN (port3) | all | all | always | ALL | ACCEPT | Disabled |
| Allow-MGMT-to-LAN | MGMT (port1) | LAN (port2) | all | all | always | ALL | ACCEPT | Disabled |
| Implicit Deny | any | any | all | all | always | ALL | DENY | |