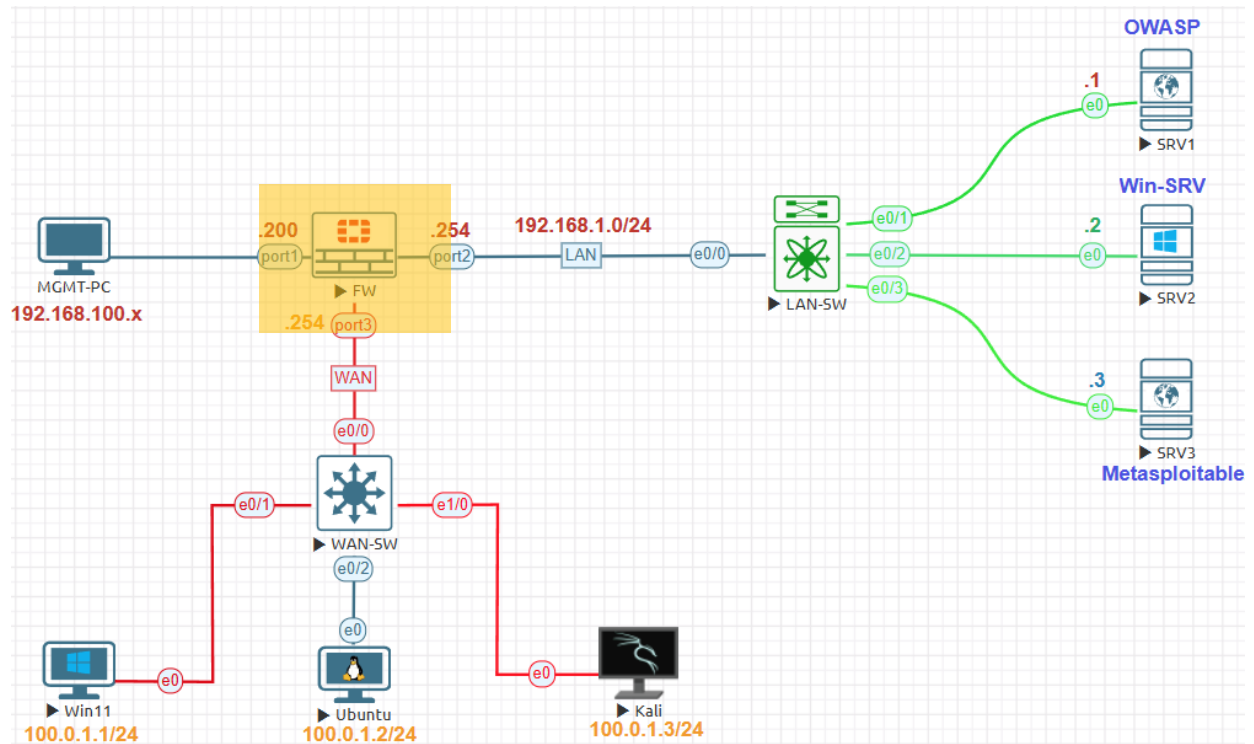


## Firewall Setup Lab:



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

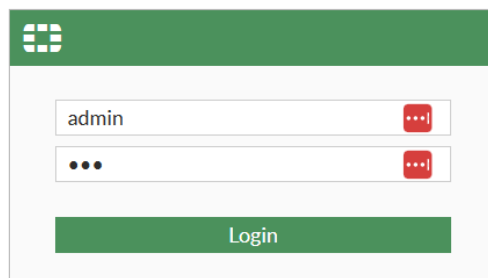
### Hostname Configuration

```
FortiGate-VM64-KVM # config system global  
FortiGate-VM64-KVM (global) # set hostname FW  
FortiGate-VM64-KVM (global) # end
```

### Management Interface Configuration

```
FW # config system interface  
FW (interface) # edit port1  
FW (port1) # set allowaccess https http ping ssh  
FW (port1) # set mode static  
FW (port1) # set ip 192.168.100.200/24  
FW (port1) # end
```

⚠ Not secure 192.168.100.200/login?redir=%2F



### FortiGate Setup

⚠ Perform the following steps to complete the setup of this FortiGate.

- Specify Hostname ✓
- Change Your Password ✓
- Dashboard Setup
- Upgrade Firmware ✓

Begin

Later

### Setup Progress

Specify Hostname ✓

Change Your Password ✓

➤ Dashboard Setup

Upgrade Firmware ✓

### Dashboard Setup

**⚠** Select one of the following options to decide what dashboards will be available by default. You can always change your selection or manually customize your own dashboards later.

**Optimal**  
A set of popular default dashboards and FortiView monitors.

**Comprehensive**  
A set of default dashboards as well as all monitors and FortiViews. This set will be familiar to users coming from previous FortiOS versions

← ↻ 🏠 ⚠ Not secure 192.168.100.200/ng/system/dashboard/1

FW

Dashboard

Status

Security

Network

Users & Devices

+

FortiView Sources

FortiView Destinations

FortiView Applications

FortiView Web Sites

FortiView Policies

FortiView Sessions

+

Network

Policy & Objects

Security Profiles

VPN

User & Authentication

System

Security Fabric

☰ 🔍

#### System Information

Hostname: FW

Serial Number: FGVMEVS3DZRGUG18

Firmware: v7.0.9 build0444 (Mature)

Mode: NAT

System Time: 2024/11/29 11:46:05

Uptime: 00:00:06:39

WAN IP: Unknown

#### Licenses

- FortiCare Support
- Firmware & General Updates
- IPS
- AntiVirus
- Web Filtering

FortiToken: 0/0

⚠ Unable to connect to FortiGuard servers.

#### Security Fabric

🔧 🔄 🛡️ 📄 🔄 🗣️ 📄

🛡️

🔧

FW

#### Administrators

1 Console 1 HTTP 0 FortiExplorer

admin super\_admin

3 | Page Created by Ahmad Ali E-Mail: [ahmadalimsc@gmail.com](mailto:ahmadalimsc@gmail.com) , WhatsApp: 00966564303717

<https://t.me/learningnets>

Name	Type	Members	IP/Netmask	Administrative Access
<b>802.3ad Aggregate 1</b>				
fortilink	802.3ad Aggregate		Dedicated to FortiSwitch	PING Security Fabric Connecti
<b>Physical Interface 4</b>				
port1	Physical Interface		192.168.100.200/255.255.255.0	PING HTTPS SSH HTTP
port2	Physical Interface		0.0.0.0/0.0.0.0	
port3	Physical Interface		0.0.0.0/0.0.0.0	
port4	Physical Interface		0.0.0.0/0.0.0.0	

**Edit Interface**

Name: port1

Alias: **MGMT**

Type: Physical Interface

VRF ID: 0

Role: Undefined

Dedicated Management Port

Address

Addressing mode: **Manual** | DHCP | Auto-managed by IPAM | One-Arm Sniffer

IP/Netmask: 192.168.100.200/255.255.255.0

Dashboard > Network > Interfaces > Edit Interface

Name: LAN (port2)

Alias: LAN

Type: Physical Interface

VRF ID: 0

Role: LAN

Address

Addressing mode: Manual | DHCP | Auto-managed by IPAM

IP/Netmask: 192.168.1.254/255.255.255.0

Create address object matching subnet:

Secondary IP address:

Administrative Access

IPv4:  HTTPS  PING  FMG-Access

Dashboard > Network > Interfaces > Edit Interface

Name: port3

Alias: WAN

Type: Physical Interface

VRF ID: 0

Role: WAN

Estimated bandwidth: 0 kbps Upstream

0 kbps Downstream

Dedicated Management Port

Address

Addressing mode: Manual | DHCP

IP/Netmask: 100.0.1.254/24

Secondary IP address:

Administrative Access

IPv4:  HTTPS  PING  FMG-Access

SSH  SNMP  FTM

+ Create New		Edit	Delete	Integrate Interface	Search
Name	Type	Members	IP/Netmask	Administrative Access	
<b>802.3ad Aggregate 1</b>					
fortilink	802.3ad Aggregate		Dedicated to FortiSwitch	PING Security Fabric Connection	
<b>Physical Interface 4</b>					
LAN (port2)	Physical Interface		192.168.1.254/255.255.255.0	PING	
MGMT (port1)	Physical Interface		192.168.100.200/255.255.255.0	PING HTTPS SSH HTTP	
port4	Physical Interface		0.0.0.0/0.0.0.0		
WAN (port3)	Physical Interface		100.0.1.254/255.255.255.0	PING	

- Dashboard
- Network**
- Interfaces
- DNS**
- Packet Capture
- SD-WAN
- Static Routes
- Policy Routes
- RIP

### DNS Settings

DNS servers Use FortiGuard Servers Specify

Primary DNS server 8.8.8.8

Secondary DNS server 1.1.1.1

Local domain name

+

---

DNS Protocols

DNS (UDP/53) i ●

- Dashboard
- Network**
- Interfaces
- DNS
- Packet Capture
- SD-WAN
- Static Routes**
- Policy Routes
- RIP
- OSPF
- BGP

### New Static Route

Destination i Subnet 0.0.0.0/0.0.0.0 Internet Service

Gateway Address 192.168.100.1

Interface MGMT (port1) ✕

+

Administrative Distance i 10

Comments Write a comment... 0/255

Status Enabled Disabled

+ Advanced Options

- Network** ▼
- Interfaces
- DNS
- Packet Capture
- SD-WAN
- Static Routes ☆
- Policy Routes
- RIP

Destination ⓘ Subnet Internet Service

192.168.1.0/255.255.255.0

Gateway Address 0.0.0.0

Interface ✕

LAN (port2) +

Administrative Distance ⓘ 10

Comments Write a comment... 0/255

Status Enabled Disabled

- Network** ▼
- Interfaces
- DNS
- Packet Capture
- SD-WAN
- Static Routes ☆
- Policy Routes
- RIP

Destination ⓘ Subnet Internet Service

100.0.1.0/255.255.255.0

Gateway Address 0.0.0.0

Interface ✕

WAN (port3) +

Administrative Distance ⓘ 10

Comments Write a comment... 0/255

Status Enabled Disabled

- Policy & Objects
- Firewall Policy
- IPv4 DoS Policy
- Addresses
- Internet Service Database
- Services
- Schedules
- Virtual IPs
- IP Pools
- Protocol Options
- Traffic Shaping
- Security Profiles
- VPN
- User & Authentication
- System
- Security Fabric
- Log & Report

Name: Allow-WAN-to-Internet

Incoming Interface: WAN (port3)

Outgoing Interface: MGMT (port1)

Source: all

Destination: all

Schedule: always

Service: ALL

Action:  ACCEPT  DENY

Inspection Mode:  Flow-based  Proxy-based

Firewall / Network Options

NAT:

IP Pool Configuration:  Use Outgoing Interface Address  Use Dynamic IP Pool

Preserve Source Port:

Protocol Options: PROT default

- Policy & Objects
- Firewall Policy
- IPv4 DoS Policy
- Addresses
- Internet Service Database
- Services
- Schedules
- Virtual IPs
- IP Pools
- Protocol Options
- Traffic Shaping
- Security Profiles
- VPN
- User & Authentication
- System

Name: Allow-WAN-to-LAN

Incoming Interface: WAN (port3)

Outgoing Interface: LAN (port2)

Source: all

Destination: all

Schedule: always

Service: ALL

Action:  ACCEPT  DENY

Inspection Mode:  Flow-based  Proxy-based

Firewall / Network Options

NAT:

Protocol Options: PROT default

- Policy & Objects ▼
- Firewall Policy ☆
- IPv4 DoS Policy
- Addresses
- Internet Service Database
- Services
- Schedules
- Virtual IPs
- IP Pools
- Protocol Options
- Traffic Shaping
- Security Profiles >
- VPN >
- User & Authentication >
- System 1 >

Name ⓘ

Incoming Interface

Outgoing Interface

Source  ✕

+

Destination  ✕

+

Schedule

Service  ✕

+

Action  ACCEPT  DENY

Inspection Mode  Flow-based  Proxy-based

Firewall / Network Options

NAT

Protocol Options  ✎

- Network >
- Policy & Objects ▼
- Firewall Policy ☆
- IPv4 DoS Policy
- Addresses
- Internet Service Database
- Services
- Schedules
- Virtual IPs
- IP Pools
- Protocol Options
- Traffic Shaping
- Security Profiles >
- VPN >
- User & Authentication >
- System 1 >

Name ⓘ

Incoming Interface

Outgoing Interface

Source  ✕

+

Destination  ✕

+

Schedule

Service  ✕

+


Action  ACCEPT  DENY


Inspection Mode  Flow-based  Proxy-based


Firewall / Network Options


NAT


Protocol Options  ✎


Name 


Incoming Interface  MGMT (port1) ▼

Outgoing Interface  LAN (port2) ▼

Source  all ✕  
+

Destination  all ✕  
+

Schedule  always ▼


Service  ALL ✕  
+









































Action  ACCEPT  DENY

Inspection Mode  Flow-based  Proxy-based

#### Firewall / Network Options

NAT

Protocol Options  PROT default ▼ 

Name	From	To	Source	Destination	Schedule	Service	Action	NAT
Allow-WAN-to-LAN	 WAN (port3)	 LAN (port2)	 all	 all	 always	 ALL	<input checked="" type="checkbox"/> ACCEPT	<input type="checkbox"/> Disabled
Allow-LAN-to-WAN	 LAN (port2)	 WAN (port3)	 all	 all	 always	 ALL	<input checked="" type="checkbox"/> ACCEPT	<input type="checkbox"/> Disabled
Allow-WAN-to-Internet	 WAN (port3)	 MGMT (port1)	 all	 all	 always	 ALL	<input checked="" type="checkbox"/> ACCEPT	<input checked="" type="checkbox"/> Enabled
Allow-LAN-to-Internet	 LAN (port2)	 MGMT (port1)	 all	 all	 always	 ALL	<input checked="" type="checkbox"/> ACCEPT	<input checked="" type="checkbox"/> Enabled
Allow-MGMT-to-WAN	 MGMT (port1)	 WAN (port3)	 all	 all	 always	 ALL	<input checked="" type="checkbox"/> ACCEPT	<input type="checkbox"/> Disabled
Allow-MGMT-to-LAN	 MGMT (port1)	 LAN (port2)	 all	 all	 always	 ALL	<input checked="" type="checkbox"/> ACCEPT	<input type="checkbox"/> Disabled
Implicit Deny	<input type="checkbox"/> any	<input type="checkbox"/> any	 all	 all	 always	 ALL	<input type="checkbox"/> DENY	