COMPLETE ENTERPRISE HOMELAB MANUAL — FINAL EDITION

This is the **final, fully rebuilt, production-ready version** of your enterprise homelab manual. It includes:

- **IP Variable System** (IP-1 → IP-**COMPLETE ENTERPRISE HOMELAB MANUAL — FINAL EDITION**

This is the **final, fully rebuilt, production-ready version** of your enterprise homelab manual. It includes:

- **IP Variable System** (IP-1 → IP-13)
- **Dual Cockpit GUIs** (dashboard on mini-screen + full GUI on host)
- **Start/Stop Automation** (VMs, Cockpit, FortiGate, VMware)
- **Captive Portal Setup** (full instructions)
- **VM-Specific Steps** (every section begins with “You are now working on: <VM>”)
- **FortiGate Initialization & Security**
- **Cockpit Initialization & Dashboard Setup**
- **Correct LCD Mini-Screen Instructions**
- **VMware Workstation Pro Requirement**
- **Full VM List With Specs**

This manual is written to be ultra-beginner-friendly, explicit, and impossible to break.

---

0. IP VARIABLE SYSTEM (READ FIRST)

Throughout this manual, you will discover IP addresses and assign them variable names.

This prevents confusion later.

Example:

When you find the ER605 router’s LAN IP:

Record this as IP-1: ER605 LAN IP

Later:

Enter **IP-1** as the upstream gateway.

IP Variables Used

Variable	Meaning
IP-1	ER605 LAN IP
IP-2	PoE Router IP
IP-3	Switch 1 IP
IP-4	Switch 2 IP
IP-5	Access Point IP
IP-6	Gaming PC LAN IP
IP-7	LOG01 (Cockpit) IP
IP-8	FortiGate WAN IP
IP-9	FortiGate LAN IP
IP-10	DC01 IP

IP-11 FS01 IP

IP-12 MGMT01 IP

IP-13 CLIENT01 IP

Every time you discover an IP, the manual will tell you to record it.

---

1. PHYSICAL SETUP AND WIRING

1.1 Identify All Devices

- ER605 Router
- PoE Router
- Switch 1
- Switch 2
- Access Point (AP)
- Gaming PC (VMware Host)
- ISP Modem (EERO)
- HDMI LCD Mini-Screen

1.2 Power On All Devices

- Plug everything in.
- Turn on the power strip.
- Wait 60 seconds.

1.3 Connect ISP to Router

- EERO → ER605 WAN1 (pink cable)

Find ER605 LAN IP

You are now working on: GAMING PC

1. Connect Gaming PC to Switch 1.
2. Open a browser.
3. Try: `192.168.0.1` or `192.168.1.1`.
4. Log in.

Record this as IP-1: ER605 LAN IP

1.4 Connect Router to PoE Router

- ER605 LAN2 → PoE Router Port 1 (pink cable)

Find PoE Router IP

You are now working on: GAMING PC

- Check ER605 DHCP leases.

Record this as IP-2: PoE Router IP

1.5 Connect PoE Router to Switches

- PoE Router Port 3 → Switch 1 Port 5 (white cable)
- PoE Router Port 5 → Switch 2 Port 6 (white cable)
- PoE Router Port 6 → ER605 LAN4 (white cable)

Find Switch IPs

You are now working on: GAMING PC

- Check ER605 DHCP leases.

Record this as IP-3: Switch 1 IP Record this as IP-4: Switch 2 IP

1.6 Connect AP to Switch 1

- AP Ports 1–4 → Switch 1 Ports 1–4 (green cables)

Find AP IP

You are now working on: GAMING PC

- Check ER605 DHCP leases.

Record this as IP-5: Access Point IP

1.7 Connect Gaming PC

- Gaming PC → Switch 1

Find Gaming PC IP

You are now working on: GAMING PC

- Run `ipconfig`.

  Record this as IP-6: Gaming PC LAN IP

---

2. LCD MINI-SCREEN SETUP (HDMI DISPLAY)

2.1 Connect the Screen

- USB → Gaming PC
- HDMI → GPU

2.2 Configure Windows Display Settings

You are now working on: GAMING PC

1. Right-click desktop → **Display Settings**
2. Select **Extend These Displays**
3. Drag the mini-screen to match physical layout
4. Set native resolution

2.3 Cockpit Dashboard on Mini-Screen

You are now working on: GAMING PC

The mini-screen will show:

- Cockpit in Chrome kiosk mode
- Auto-refresh every 10 seconds
- Dashboard-only view

- Always on top

2.4 Auto-Launch Dashboard on Boot

You are now working on: GAMING PC

Place a shortcut to the dashboard launcher script in:

C:\Users\<YourUser>\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup

---

3. VMWARE WORKSTATION PRO SETUP

3.1 Workstation Pro Requirement

You are now working on: GAMING PC

You must use **VMware Workstation Pro**.

3.2 Install VMware Workstation Pro

- Run installer
- Accept defaults

3.3 Configure Virtual Network Editor

Create:

- **VMnet0** → Bridged to physical NIC
- **VMnet2** → Host-only (FortiGate internal LAN)

---

4. VM INVENTORY AND SPECIFICATIONS

4.1 DC01 — Domain Controller

- Windows Server 2022
- 2 vCPU, 4 GB RAM, 60 GB disk
- VMnet0
- Will become **IP-10**

4.2 FS01 — File Server

- Windows Server 2022
- 2 vCPU, 4 GB RAM, 60 GB disk
- VMnet0
- Will become **IP-11**

4.3 MGMT01 — Admin Workstation

- Windows 11
- 2 vCPU, 4 GB RAM, 40 GB disk
- VMnet0
- Will become **IP-12**

4.4 CLIENT01 — User Workstation

- Windows 11
- 2 vCPU, 4 GB RAM, 40 GB disk
- VMnet0
- Will become **IP-13**

4.5 LOG01 — Cockpit Server

- Ubuntu Server 22.04 LTS
- 2 vCPU, 2 GB RAM, 40 GB disk
- VMnet0
- Will become **IP-7**

4.6 FGT01 — FortiGate Firewall

- FortiGate VM (FortiOS 7.2.x)
- 2 vCPU, 2 GB RAM, 10 GB disk
- NIC1 = VMnet0, NIC2 = VMnet2
- Will become **IP-8** and **IP-9**

---

5. VM CREATION PROCESS

5.1 Create Each VM

You are now working on: GAMING PC

1. Open VMware Workstation Pro
2. Create New VM
3. Select ISO
4. Assign CPU, RAM, disk
5. Select network:
    - VMnet0 for servers
    - VMnet2 for FortiGate internal
6. Finish

---

6. WINDOWS SERVER CONFIGURATION — DC01

6.1 Install Windows Server

You are now working on: DC01

6.2 Set Static IP

You are now working on: DC01

Set:

- IP: `10.0.30.10` → **Record as IP-10**
- Mask: `255.255.255.0`
- Gateway: `10.0.30.1`
- DNS: `10.0.30.10`

6.3 Install AD DS

You are now working on: DC01

- Promote to Domain Controller
- Domain: `lab.local`

---

7. WINDOWS SERVER CONFIGURATION — FS01

7.1 Install Windows Server

You are now working on: FS01

7.2 Join Domain

You are now working on: FS01

7.3 Set Static IP

You are now working on: FS01

- IP: `10.0.20.10` → **Record as IP-11**

7.4 Create File Shares

You are now working on: FS01

---

8. WINDOWS 11 CONFIGURATION — MGMT01 & CLIENT01

8.1 Install Windows 11

You are now working on: MGMT01 / CLIENT01

8.2 Join Domain (MGMT01)

You are now working on: MGMT01

8.3 Set Static IPs

You are now working on: MGMT01

- IP: `10.0.30.50` → **Record as IP-12**

You are now working on: CLIENT01

- DHCP or static → **Record as IP-13**

---

9. UBUNTU SERVER CONFIGURATION — LOG01 (COCKPIT)

9.1 Install Ubuntu Server

You are now working on: LOG01

9.2 Set Static IP

You are now working on: LOG01

- IP: `10.0.30.20` → **Record as IP-7**

9.3 Install Cockpit

You are now working on: LOG01

- sudo apt update

  sudo apt install cockpit -y

9.4 Enable Cockpit Service

You are now working on: LOG01

- sudo systemctl enable cockpit

sudo systemctl start cockpit

9.5 Allow Cockpit Through Firewall

You are now working on: LOG01

- sudo ufw allow 9090/tcp

sudo ufw enable

9.6 Access Cockpit

You are now working on: MGMT01 or GAMING PC

Go to:

```
https://IP-7:9090
```

9.7 Configure Cockpit Dashboard

You are now working on: LOG01

Enable:

- Storage monitoring
- Networking monitoring
- Logs
- System Health
- CPU / RAM / Disk I/O widgets

---

10. FORTIGATE CONFIGURATION — FGT01

10.1 Initial Access

You are now working on: MGMT01

Go to:

```
https://192.168.1.99
```

10.2 First-Boot Initialization

You are now working on: FGT01

- Change admin password
- Enable HTTPS only
- Disable HTTP
- Set idle timeout to 5 minutes
- Set hostname: `FGT01`
- Set DNS servers (1.1.1.1 / 8.8.8.8)

10.3 Configure WAN Interface

You are now working on: FGT01

- WAN IP: `192.168.50.30` → **Record as IP-8**
- Gateway: **IP-1**

10.4 Configure LAN Interface

You are now working on: FGT01

- LAN IP: `10.0.10.1` → **Record as IP-9**

10.5 Create VLAN Interfaces

You are now working on: FGT01

- VLAN20 Trusted → `10.0.20.1`
- VLAN30 Management → `10.0.30.1`
- VLAN40 IoT → `10.0.40.1`
- VLAN50 Guest → `10.0.50.1`
- VLAN60 Ops → `10.0.60.1`

10.6 Assign DHCP to VLANs

You are now working on: FGT01

Example:

- VLAN20: `10.0.20.50–10.0.20.200`
- DNS: **IP-10**

10.7 Create Firewall Policies

You are now working on: FGT01

- Trusted → WAN (allow)
- Management → WAN (allow)
- Guest → WAN (allow)
- Guest → Internal (deny)
- IoT → Internal (deny)
- Ops → WAN (allow)

10.8 Beginner Security Hardening

You are now working on: FGT01

- Disable unused interfaces
- Enable logging on ALL firewall policies
- Enable Anomaly Protection
- Enable Botnet C&C Block
- Enable Web Filtering (Free Mode)
- Enable DNS Filter (Free Mode)
- Enable IPS (Free Mode)

---

11. SSID CONFIGURATION — ACCESS POINT

11.1 Create SSIDs

You are now working on: AP

- MGMT-WiFi → VLAN30

- Trusted-WiFi → VLAN20
- IoT-WiFi → VLAN40
- Guest-WiFi → VLAN50
- Ops-WiFi → VLAN60

11.2 Set Security

You are now working on: AP

- WPA2 or WPA3

---

12. CAPTIVE PORTAL — FORTIGATE

12.1 Enable Captive Portal

You are now working on: FGT01

- User & Authentication → Authentication Settings
- Select VLAN50
- Enable Captive Portal

12.2 Create Guest User Group

You are now working on: FGT01

- User Groups → Create New → Guest

12.3 Customize Portal

You are now working on: FGT01

- Add Terms & Conditions
- Add branding
- Add redirect page

12.4 Test Portal

You are now working on: CLIENT01

- Connect to Guest WiFi
- Attempt to browse
- Portal should appear

---

13. START/STOP AUTOMATION — GAMING PC

13.1 StartServers.bat

You are now working on: GAMING PC

This script will:

- Launch VMware Workstation
- Start all VMs in correct order
- Wait for LOG01
- Open Cockpit dashboard on mini-screen
- Open Cockpit full GUI on host
- Open FortiGate GUI on host
- Bring VMware to front

13.2 StopServers.bat

You are now working on: GAMING PC

This script will:

- Close Cockpit windows
- Close FortiGate window
- Stop all VMs
- Close VMware

13.3 Pin to Taskbar

You are now working on: GAMING PC

- Right-click → Pin to Taskbar

---

14. FINAL VERIFICATION

- All VMs online
- Cockpit dashboard visible on mini-screen
- Cockpit full GUI visible on host
- FortiGate GUI visible on host
- VLANs working
- SSIDs broadcasting
- Captive portal functional
- Firewall rules enforced
- Start/Stop automation working
- 13)
- **Dual Cockpit GUIs** (dashboard on mini-screen + full GUI on host)
- **Start/Stop Automation** (VMs, Cockpit, FortiGate, VMware)
- **Captive Portal Setup** (full instructions)
- **VM-Specific Steps** (every section begins with “You are now working on: <VM>”)
- **FortiGate Initialization & Security**
- **Cockpit Initialization & Dashboard Setup**
- **Correct LCD Mini-Screen Instructions**
- **VMware Workstation Pro Requirement**
- **Full VM List With Specs**

This manual is written to be ultra-beginner-friendly, explicit, and impossible to break.

---

0. IP VARIABLE SYSTEM (READ FIRST)

Throughout this manual, you will discover IP addresses and assign them variable names.

This prevents confusion later.

Example:

When you find the ER605 router’s LAN IP:

> **Record this as IP-1: ER605 LAN IP**

Later:

> Enter **IP-1** as the upstream gateway.

IP Variables Used

Variable	Meaning
IP-1	ER605 LAN IP
IP-2	PoE Router IP
IP-3	Switch 1 IP
IP-4	Switch 2 IP
IP-5	Access Point IP
IP-6	Gaming PC LAN IP
IP-7	LOG01 (Cockpit) IP
IP-8	FortiGate WAN IP
IP-9	FortiGate LAN IP
IP-10	DC01 IP
IP-11	FS01 IP
IP-12	MGMT01 IP

IP-13 CLIENT01 IP

Every time you discover an IP, the manual will tell you to record it.

---

1. PHYSICAL SETUP AND WIRING

1.1 Identify All Devices

- ER605 Router
- PoE Router
- Switch 1
- Switch 2
- Access Point (AP)
- Gaming PC (VMware Host)
- ISP Modem (EERO)
- HDMI LCD Mini-Screen

1.2 Power On All Devices

- Plug everything in.
- Turn on the power strip.
- Wait 60 seconds.

1.3 Connect ISP to Router

- EERO → ER605 WAN1 (pink cable)

Find ER605 LAN IP

You are now working on: GAMING PC

1. Connect Gaming PC to Switch 1.
2. Open a browser.
3. Try: `192.168.0.1` or `192.168.1.1`.
4. Log in.

Record this as IP-1: ER605 LAN IP

1.4 Connect Router to PoE Router

- ER605 LAN2 → PoE Router Port 1 (pink cable)

Find PoE Router IP

You are now working on: GAMING PC

- Check ER605 DHCP leases.

  Record this as IP-2: PoE Router IP

1.5 Connect PoE Router to Switches

- PoE Router Port 3 → Switch 1 Port 5 (white cable)
- PoE Router Port 5 → Switch 2 Port 6 (white cable)
- PoE Router Port 6 → ER605 LAN4 (white cable)

Find Switch IPs

You are now working on: GAMING PC

- Check ER605 DHCP leases.

  Record this as IP-3: Switch 1 IP Record this as IP-4: Switch 2 IP

1.6 Connect AP to Switch 1

- AP Ports 1–4 → Switch 1 Ports 1–4 (green cables)

Find AP IP

You are now working on: GAMING PC

- Check ER605 DHCP leases.

  Record this as IP-5: Access Point IP

1.7 Connect Gaming PC

- Gaming PC → Switch 1

Find Gaming PC IP

You are now working on: GAMING PC

- Run `ipconfig`.

  Record this as IP-6: Gaming PC LAN IP

---

2. LCD MINI-SCREEN SETUP (HDMI DISPLAY)

2.1 Connect the Screen

- USB → Gaming PC
- HDMI → GPU

2.2 Configure Windows Display Settings

You are now working on: GAMING PC

1. Right-click desktop → **Display Settings**
2. Select **Extend These Displays**
3. Drag the mini-screen to match physical layout
4. Set native resolution

2.3 Cockpit Dashboard on Mini-Screen

You are now working on: GAMING PC

The mini-screen will show:

- Cockpit in Chrome kiosk mode
- Auto-refresh every 10 seconds
- Dashboard-only view
- Always on top

2.4 Auto-Launch Dashboard on Boot

You are now working on: GAMING PC

Place a shortcut to the dashboard launcher script in:

C:\Users\<YourUser>\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup

---

3. VMWARE WORKSTATION PRO SETUP

3.1 Workstation Pro Requirement

You are now working on: GAMING PC

You must use **VMware Workstation Pro**.

3.2 Install VMware Workstation Pro

- Run installer
- Accept defaults

3.3 Configure Virtual Network Editor

Create:

- **VMnet0** → Bridged to physical NIC
- **VMnet2** → Host-only (FortiGate internal LAN)

---

4. VM INVENTORY AND SPECIFICATIONS

4.1 DC01 — Domain Controller

- Windows Server 2022
- 2 vCPU, 4 GB RAM, 60 GB disk
- VMnet0
- Will become **IP-10**

4.2 FS01 — File Server

- Windows Server 2022
- 2 vCPU, 4 GB RAM, 60 GB disk
- VMnet0
- Will become **IP-11**

4.3 MGMT01 — Admin Workstation

- Windows 11
- 2 vCPU, 4 GB RAM, 40 GB disk
- VMnet0
- Will become **IP-12**

4.4 CLIENT01 — User Workstation

- Windows 11
- 2 vCPU, 4 GB RAM, 40 GB disk
- VMnet0
- Will become **IP-13**

4.5 LOG01 — Cockpit Server

- Ubuntu Server 22.04 LTS
- 2 vCPU, 2 GB RAM, 40 GB disk
- VMnet0
- Will become **IP-7**

4.6 FGT01 — FortiGate Firewall

- FortiGate VM (FortiOS 7.2.x)
- 2 vCPU, 2 GB RAM, 10 GB disk
- NIC1 = VMnet0, NIC2 = VMnet2
- Will become **IP-8** and **IP-9**

---

5. VM CREATION PROCESS

5.1 Create Each VM

You are now working on: GAMING PC

1. Open VMware Workstation Pro
2. Create New VM
3. Select ISO
4. Assign CPU, RAM, disk
5. Select network:
    - VMnet0 for servers
    - VMnet2 for FortiGate internal
6. Finish

---

6. WINDOWS SERVER CONFIGURATION — DC01

6.1 Install Windows Server

You are now working on: DC01

6.2 Set Static IP

You are now working on: DC01

Set:

- IP: `10.0.30.10` → **Record as IP-10**
- Mask: `255.255.255.0`
- Gateway: `10.0.30.1`
- DNS: `10.0.30.10`

6.3 Install AD DS

You are now working on: DC01

- Promote to Domain Controller
- Domain: `lab.local`

---

7. WINDOWS SERVER CONFIGURATION — FS01

7.1 Install Windows Server

You are now working on: FS01

7.2 Join Domain

You are now working on: FS01

7.3 Set Static IP

You are now working on: FS01

- IP: `10.0.20.10` → **Record as IP-11**

7.4 Create File Shares

You are now working on: FS01

---

8. WINDOWS 11 CONFIGURATION — MGMT01 & CLIENT01

8.1 Install Windows 11

You are now working on: MGMT01 / CLIENT01

8.2 Join Domain (MGMT01)

You are now working on: MGMT01

8.3 Set Static IPs

You are now working on: MGMT01

- IP: `10.0.30.50` → **Record as IP-12**

You are now working on: CLIENT01

- DHCP or static → **Record as IP-13**

---

9. UBUNTU SERVER CONFIGURATION — LOG01 (COCKPIT)

9.1 Install Ubuntu Server

You are now working on: LOG01

9.2 Set Static IP

You are now working on: LOG01

- IP: `10.0.30.20` → **Record as IP-7**

9.3 Install Cockpit

You are now working on: LOG01

```
sudo apt update
sudo apt install cockpit -y
```

9.4 Enable Cockpit Service

You are now working on: LOG01

```
sudo systemctl enable cockpit
sudo systemctl start cockpit
```

9.5 Allow Cockpit Through Firewall

You are now working on: LOG01

sudo ufw allow 9090/tcp
sudo ufw enable

9.6 Access Cockpit

You are now working on: MGMT01 or GAMING PC

Go to:

```
https://IP-7:9090
```

9.7 Configure Cockpit Dashboard

You are now working on: LOG01

Enable:

- Storage monitoring
- Networking monitoring
- Logs
- System Health
- CPU / RAM / Disk I/O widgets

---

10. FORTIGATE CONFIGURATION — FGT01

10.1 Initial Access

You are now working on: MGMT01

Go to:

```
https://192.168.1.99
```

10.2 First-Boot Initialization

You are now working on: FGT01

- Change admin password
- Enable HTTPS only
- Disable HTTP
- Set idle timeout to 5 minutes
- Set hostname: `FGT01`
- Set DNS servers (1.1.1.1 / 8.8.8.8)

10.3 Configure WAN Interface

You are now working on: FGT01

- WAN IP: `192.168.50.30` → **Record as IP-8**
- Gateway: **IP-1**

10.4 Configure LAN Interface

You are now working on: FGT01

- LAN IP: `10.0.10.1` → **Record as IP-9**

10.5 Create VLAN Interfaces

You are now working on: FGT01

- VLAN20 Trusted → `10.0.20.1`
- VLAN30 Management → `10.0.30.1`
- VLAN40 IoT → `10.0.40.1`
- VLAN50 Guest → `10.0.50.1`
- VLAN60 Ops → `10.0.60.1`

10.6 Assign DHCP to VLANs

You are now working on: FGT01

Example:

- VLAN20: `10.0.20.50–10.0.20.200`
- DNS: **IP-10**

10.7 Create Firewall Policies

You are now working on: FGT01

- Trusted → WAN (allow)
- Management → WAN (allow)
- Guest → WAN (allow)
- Guest → Internal (deny)
- IoT → Internal (deny)
- Ops → WAN (allow)

10.8 Beginner Security Hardening

You are now working on: FGT01

- Disable unused interfaces
- Enable logging on ALL firewall policies
- Enable Anomaly Protection
- Enable Botnet C&C Block
- Enable Web Filtering (Free Mode)
- Enable DNS Filter (Free Mode)
- Enable IPS (Free Mode)

---

11. SSID CONFIGURATION — ACCESS POINT

11.1 Create SSIDs

You are now working on: AP

- MGMT-WiFi → VLAN30
- Trusted-WiFi → VLAN20
- IoT-WiFi → VLAN40
- Guest-WiFi → VLAN50
- Ops-WiFi → VLAN60

11.2 Set Security

You are now working on: AP

- WPA2 or WPA3

---

12. CAPTIVE PORTAL — FORTIGATE

12.1 Enable Captive Portal

You are now working on: FGT01

- User & Authentication → Authentication Settings
- Select VLAN50
- Enable Captive Portal

12.2 Create Guest User Group

You are now working on: FGT01

- User Groups → Create New → Guest

12.3 Customize Portal

You are now working on: FGT01

- Add Terms & Conditions
- Add branding
- Add redirect page

12.4 Test Portal

You are now working on: CLIENT01

- Connect to Guest WiFi
- Attempt to browse
- Portal should appear

---

13. START/STOP AUTOMATION — GAMING PC

13.1 StartServers.bat

You are now working on: GAMING PC

This script will:

- Launch VMware Workstation
- Start all VMs in correct order
- Wait for LOG01
- Open Cockpit dashboard on mini-screen
- Open Cockpit full GUI on host
- Open FortiGate GUI on host
- Bring VMware to front

13.2 StopServers.bat

You are now working on: GAMING PC

This script will:

- Close Cockpit windows
- Close FortiGate window
- Stop all VMs
- Close VMware

13.3 Pin to Taskbar

You are now working on: GAMING PC

- Right-click → Pin to Taskbar

---

14. FINAL VERIFICATION

- All VMs online
- Cockpit dashboard visible on mini-screen

- Cockpit full GUI visible on host
- FortiGate GUI visible on host
- VLANs working
- SSIDs broadcasting
- Captive portal functional
- Firewall rules enforced
- Start/Stop automation working