# SECTION 1

# PHYSICAL SETUP, VMWARE CONFIGURATION, NETWORK FOUNDATIONS, AND IP PLAN

This section establishes the physical and virtual foundation of the environment. It defines the physical cabling, the VMware Workstation Pro configuration, the creation of VMnet0 and VMnet2, and the complete IP addressing plan that all later sections will rely upon. Completing this section ensures that every subsequent configuration step has a stable, predictable, and professionally structured base.

## Physical Setup

Begin by placing the gaming PC, switches, and mini display in their intended positions. Connect the gaming PC to the ER605 router using a standard Ethernet cable. This connection places the hypervisor on the main LAN, which will serve as the backbone for all server communication. Ensure the ER605 is powered on and functioning normally. If you are using a mini display for monitoring, connect it to the gaming PC using HDMI or DisplayPort. This display will later show Cockpit or Netdata dashboards.

No switch configuration is required at this stage. The only requirement is that the gaming PC has a stable connection to the ER605 LAN, because this LAN will serve as the management and server network for the entire environment.

## VMware Workstation Pro Configuration

Launch VMware Workstation Pro. Before creating any virtual machines, open the Virtual Network Editor. This tool is essential for creating the dedicated Host-Only network that the FortiGate LAN will use. VMware creates VMnet0 and VMnet1 by default. VMnet0 will be used for all server VMs and the FortiGate WAN interface. VMnet1 will not be used in this environment to avoid conflicts with VMware's internal services.

## Creating VMnet2

In the Virtual Network Editor, create a new network and assign it as VMnet2. Configure VMnet2 as a Host-Only network. Disable DHCP on VMnet2 because the FortiGate firewall will control addressing on its LAN interface. VMware may assign VMnet2 an internal address, but this address is irrelevant because the FortiGate will override all addressing for the test subnet. The important requirement is that VMnet2 is isolated and used exclusively for the FortiGate LAN and the Windows test client.

Confirm that VMnet0 remains configured as Bridged. This network will connect your VMs directly to the ER605 LAN, allowing them to communicate with each other and with the physical

network. VMnet0 will be used by DC01, FS01, MGMT01, LOG01, and the WAN interface of the FortiGate VM.

IP Addressing Plan
The IP addressing plan defines the structure of the environment. The main LAN behind the ER605 will use the subnet 192.168.50.0/24. The ER605 will use 192.168.50.1 as its LAN IP. DHCP on the ER605 should be disabled for this environment because all servers will use static IP addresses.

Assign DC01 the IP address 192.168.50.10. Assign FS01 the IP address 192.168.50.11. Assign LOG01 the IP address 192.168.50.12. Assign MGMT01 the IP address 192.168.50.20. Assign the FortiGate WAN interface the IP address 192.168.50.30. All of these addresses will use 255.255.255.0 as the subnet mask and 192.168.50.1 as the default gateway.

The FortiGate LAN will use the subnet 10.0.10.0/24. Assign the FortiGate LAN interface the IP address 10.0.10.1. Assign the Windows test client the IP address 10.0.10.10. The DNS server for the Windows test client will be 192.168.50.10, which is the domain controller.

Summary of IP Assignments
ER605 LAN IP: 192.168.50.1
DC01: 192.168.50.10
FS01: 192.168.50.11
LOG01: 192.168.50.12
MGMT01: 192.168.50.20
FortiGate WAN: 192.168.50.30
FortiGate LAN: 10.0.10.1
Windows Test Client: 10.0.10.10

At this point, the physical environment, VMware networking, and IP addressing plan are fully established. These foundations must be in place before creating or configuring any virtual machines. Once this section is complete, the environment is ready for VM creation, operating system installation, and domain configuration.

## SECTION 2

## VM CREATION, OPERATING SYSTEM INSTALLATION, AND DOMAIN CONFIGURATION

This section establishes every virtual machine in the environment, installs each operating system, assigns static IP addresses according to the plan defined in Section 1, and prepares

the domain infrastructure. By the end of this section, all machines will be fully built, named, configured, and ready for FortiGate integration and advanced firewall policy design.

Creating the Domain Controller (DC01)
Begin by creating a new virtual machine in VMware Workstation Pro and naming it DC01. Assign two virtual CPUs, four gigabytes of memory, and a sixty-gigabyte virtual disk. Connect its network adapter to VMnet0 so that it resides on the main LAN. Attach the Windows Server 2022 ISO and complete the installation using the Standard Edition with Desktop Experience. After installation, log in as the local Administrator, install VMware Tools, and reboot. Rename the computer to DC01 and reboot again.

Assign a static IP address to DC01 using the values defined in Section 1. Set the IP address to 192.168.50.10, the subnet mask to 255.255.255.0, the default gateway to 192.168.50.1, and the DNS server to 192.168.50.10. This DNS configuration is intentional because the domain controller will host DNS services. Open Server Manager, add the Active Directory Domain Services and DNS Server roles, and promote the server to a domain controller by creating a new forest named lab.local. After the promotion completes, reboot and log in using the domain Administrator account. Verify that DNS is functioning by resolving the domain name locally.

Creating the File Server (FS01)
Create a new virtual machine named FS01. Assign two virtual CPUs, four to six gigabytes of memory, and an eighty-gigabyte virtual disk. Connect the network adapter to VMnet0. Install Windows Server 2022, install VMware Tools, and reboot. Rename the computer to FS01 and reboot again. Assign the static IP address 192.168.50.11 with the same subnet mask and gateway as DC01. Set the DNS server to 192.168.50.10. Join FS01 to the lab.local domain and reboot. After joining, log in using a domain account. Install the File and Storage Services role and create a directory such as D:\Shares\Dept. Configure NTFS permissions and share permissions as needed. This server will later be used to validate domain authentication and access control.

Creating the Management Workstation (MGMT01)
Create a new virtual machine named MGMT01. Assign four virtual CPUs, eight gigabytes of memory, and an eighty-gigabyte virtual disk. Connect the network adapter to VMnet0. Install Windows 11, install VMware Tools, and reboot. Rename the computer to MGMT01 and reboot again. Assign the static IP address 192.168.50.20, the subnet mask 255.255.255.0, the gateway 192.168.50.1, and the DNS server 192.168.50.10. Join MGMT01 to the lab.local domain and reboot. After joining, log in using a domain account. Install the Remote Server Administration Tools through the Windows Optional Features interface. This workstation will serve as the primary administrative console for managing Active Directory, DNS, Group Policy, and other server roles.

Creating the Logging and Monitoring Server (LOG01)
Create a new virtual machine named LOG01. Assign two virtual CPUs, four gigabytes of memory, and a sixty-gigabyte virtual disk. Connect the network adapter to VMnet0. Install

Ubuntu Server 22.04 and create a user account during installation. After installation, log in and install VMware Tools for Linux if desired. Configure a static IP address by editing the netplan configuration file. Assign the IP address 192.168.50.12, the subnet mask 255.255.255.0, the gateway 192.168.50.1, and the DNS server 192.168.50.10. Apply the configuration and verify connectivity by pinging DC01 and MGMT01. Install Cockpit using the package manager and enable the Cockpit service so that it starts automatically. This server will later host monitoring dashboards and serve as the central management interface.

Creating the FortiGate Firewall (FGT01)
Import the FortiGate OVF package into VMware Workstation Pro and name the VM FGT01. Assign two virtual CPUs, two to four gigabytes of memory, and a twenty-gigabyte virtual disk. Configure the first network adapter (port1) to use VMnet0 and the second network adapter (port2) to use VMnet2. Power on the VM and complete the initial setup through the console. Assign port1 the IP address 192.168.50.30 with a subnet mask of 255.255.255.0 and a gateway of 192.168.50.1. Assign port2 the IP address 10.0.10.1 with a subnet mask of 255.255.255.0. These assignments match the addressing plan defined in Section 1. After configuration, access the FortiGate web interface from MGMT01 by navigating to https://192.168.50.30.

Creating the Windows Test Client (WIN-CLIENT01)
Create a new virtual machine named WIN-CLIENT01. Assign two virtual CPUs, four gigabytes of memory, and a sixty-gigabyte virtual disk. Connect the network adapter to VMnet2 so that it resides behind the FortiGate LAN interface. Install Windows 11, install VMware Tools, and reboot. Rename the computer to WIN-CLIENT01 and reboot again. Assign the static IP address 10.0.10.10, the subnet mask 255.255.255.0, the gateway 10.0.10.1, and the DNS server 192.168.50.10. Join WIN-CLIENT01 to the lab.local domain and reboot. After joining, log in using a domain account. This machine will serve as the test workstation behind the FortiGate firewall.

Domain Verification
Once all machines are joined to the domain, verify that Group Policy applies correctly by running gpupdate /force on MGMT01 and WIN-CLIENT01. Confirm that DNS resolution works by resolving lab.local from both machines. Ensure that each server can communicate with DC01 and that the FortiGate can reach the domain controller through port1. At this point, the environment is fully built and ready for FortiGate policy configuration, routing, and advanced firewall integration.

## SECTION 3

## FORTIGATE CORE CONFIGURATION, INTERFACE SETUP, ROUTING, DNS, AND FIREWALL POLICY DESIGN

This section establishes the FortiGate firewall as the security boundary between the main LAN and the isolated test subnet. It provides explicit instructions for configuring interfaces, routing, DNS, NAT, and firewall policies using the FortiGate graphical interface. Every action includes the exact GUI path to ensure clarity and repeatability. By the end of this section, the FortiGate will be fully integrated into the environment and capable of routing, filtering, and inspecting traffic between the two networks.

Accessing the FortiGate Web Interface

Once the FortiGate VM is powered on and its initial console configuration is complete, access the web interface from MGMT01 by opening a browser and navigating to https://192.168.50.30. This address corresponds to the WAN interface configured during VM creation. Accept the certificate warning and log in using the administrative credentials created during the initial setup. After logging in, verify that the dashboard loads correctly and that the system information panel displays the expected interface assignments.

Configuring the WAN Interface

Navigate to Network > Interfaces and select port1. This interface represents the WAN side of the firewall and is connected to VMnet0. Confirm that the addressing mode is set to Manual and that the IP address is 192.168.50.30 with a subnet mask of 255.255.255.0. Set the default gateway to 192.168.50.1, which is the ER605 LAN IP. Enable HTTPS and PING under Administrative Access to ensure that the interface remains manageable. Apply the changes and verify that the interface status shows as up.

Configuring the LAN Interface

Still within Network > Interfaces, select port2. This interface represents the internal LAN behind the FortiGate and is connected to VMnet2. Assign the IP address 10.0.10.1 with a subnet mask of 255.255.255.0. If DHCP services are desired for the test subnet, enable DHCP Server within this interface's settings. If static addressing is preferred, leave DHCP disabled. Enable HTTPS and PING under Administrative Access to allow management from the test subnet if needed. Apply the changes and verify that the interface status shows as up.

Configuring the Default Route

Navigate to Network > Static Routes. Confirm that a default route exists with a destination of 0.0.0.0/0, a gateway of 192.168.50.1, and an outgoing interface of port1. This route ensures that all outbound traffic from the FortiGate LAN is forwarded to the ER605. If the route does not exist, create it using the Add button. Apply the configuration and verify that the route appears in the routing table.

Configuring DNS

Navigate to Network > DNS. Set the primary DNS server to 192.168.50.10, which is the domain controller's IP address. This ensures that the FortiGate can resolve internal domain names and that any DHCP clients on the FortiGate LAN receive the correct DNS server. If DHCP is enabled on port2, navigate to Network > Interfaces > port2 and confirm that the DHCP server configuration lists 192.168.50.10 as the DNS server. Apply the changes.

Creating the LAN-to-WAN Firewall Policy
Navigate to Policy & Objects > Firewall Policy. Create a new policy allowing traffic from the LAN interface to the WAN interface. Set the incoming interface to port2 and the outgoing interface to port1. Set the source and destination addresses to all. Set the service to all. Enable NAT to ensure that internal addresses are translated to the FortiGate's WAN address. Enable logging for all sessions to ensure visibility during troubleshooting. Apply the policy and ensure that it appears above any more restrictive policies.

Testing Connectivity from the Test Subnet
Log in to WIN-CLIENT01 and open a command prompt. Ping 10.0.10.1 to verify connectivity to the FortiGate LAN interface. Ping 192.168.50.30 to verify connectivity to the FortiGate WAN interface. Ping 192.168.50.10 to verify connectivity to the domain controller. If all pings succeed, run nslookup lab.local to confirm DNS resolution. Attempt to access \192.168.50.10 to verify SMB connectivity. If all tests succeed, the FortiGate is correctly routing and filtering traffic between the test subnet and the main LAN.

Domain Authentication Verification
Open the System settings on WIN-CLIENT01 and confirm that the computer is joined to the lab.local domain. Log out and log in using a domain account. Run gpupdate /force to verify that Group Policy applies successfully. If Group Policy applies without errors, the FortiGate is correctly passing domain authentication traffic between the two networks.

At this stage, the FortiGate is fully integrated into the environment. The WAN and LAN interfaces are configured, routing is functional, DNS is correctly assigned, NAT is operational, and the test client can authenticate to the domain. The environment is now ready for Cockpit integration, dashboard configuration, and automation scripting, which will be covered in the next section

## SECTION 4

## COCKPIT INSTALLATION, DASHBOARD CONFIGURATION, AUTOMATION SCRIPTS, AND GUI START/STOP CONTROLS

This section completes the operational layer of the environment by configuring Cockpit on LOG01, preparing the monitoring dashboard for continuous display, and implementing the automation system that starts and stops the entire homelab with a single click. The automation system is built using PowerShell scripts on the Windows 11 gaming PC and is integrated into both the taskbar and the Start Menu for immediate access. By the end of this section, the environment will have centralized monitoring, streamlined control, and a professional operational workflow.

Cockpit Installation on LOG01
Begin by logging into LOG01 either through the VMware console or via SSH from MGMT01. Update the package lists and install Cockpit using the standard package manager. Once installed, enable the Cockpit service so that it starts automatically whenever LOG01 boots. Cockpit listens on port 9090 by default. To verify that Cockpit is running, open a browser on MGMT01 and navigate to http://192.168.50.12:9090. Log in using the credentials created during the Ubuntu installation. Once authenticated, confirm that Cockpit displays system metrics, logs, storage information, and network activity. This interface will serve as the central monitoring and management point for the environment.

Cockpit Configuration and Dashboard Preparation
Within Cockpit, enable optional modules such as storage, networking, and system logs to enhance visibility. If you intend to monitor multiple servers from a single Cockpit interface, you may add additional hosts by entering their IP addresses and credentials. For this environment, LOG01 will serve as the primary monitoring node. Configure Cockpit to display CPU, memory, disk, and network graphs prominently. These graphs will later be displayed on the mini screen connected to the gaming PC.

Dashboard Display on the Mini Screen
To configure the mini display as a dedicated monitoring screen, open Microsoft Edge or another browser on the Windows 11 gaming PC and navigate to http://192.168.50.12:9090. Enter full-screen mode using the browser's built-in full-screen function. Drag the browser window to the mini display and leave it open. This provides continuous visibility into system performance. If you prefer more detailed real-time metrics, install Netdata on LOG01 and access it through http://192.168.50.12:19999. Netdata can also be placed on the mini display in full-screen mode.

Overview of the Automation System
The automation system consists of two PowerShell scripts stored on the Windows 11 gaming PC. One script starts all virtual machines in the correct order, and the other script stops them in reverse order. These scripts are then converted into shortcuts and pinned to both the taskbar and the Start Menu. This provides a professional, streamlined method for controlling the entire environment without manually opening VMware Workstation Pro.

Creating the Start Script
Open Notepad on the Windows 11 gaming PC and create a new file. Enter the following PowerShell script, replacing each VMX path with the actual path to your virtual machines:

```
# Start-Lab.ps1
Start-Process "C:\Program Files (x86)\VMware\VMware Workstation\vmrun.exe" -ArgumentList "start `"C:\VMs\DC01\DC01.vmx`" nogui"
Start-Sleep -Seconds 10
```

```
Start-Process "C:\Program Files (x86)\VMware\VMware Workstation\vmrun.exe" -ArgumentList "start `"C:\VMs\FS01\FS01.vmx`" nogui"
Start-Sleep -Seconds 10

Start-Process "C:\Program Files (x86)\VMware\VMware Workstation\vmrun.exe" -ArgumentList "start `"C:\VMs\LOG01\LOG01.vmx`" nogui"
Start-Sleep -Seconds 10

Start-Process "C:\Program Files (x86)\VMware\VMware Workstation\vmrun.exe" -ArgumentList "start `"C:\VMs\MGMT01\MGMT01.vmx`" nogui"
Start-Sleep -Seconds 10

Start-Process "C:\Program Files (x86)\VMware\VMware Workstation\vmrun.exe" -ArgumentList "start `"C:\VMs\FGT01\FGT01.vmx`" nogui"
Start-Sleep -Seconds 20

Start-Process "C:\Program Files (x86)\VMware\VMware Workstation\vmrun.exe" -ArgumentList "start `"C:\VMs\WIN-CLIENT01\WIN-CLIENT01.vmx`" nogui"
```

Save the file as Start-Lab.ps1 in a directory such as C:\LabScripts.

Creating the Stop Script
Create a second file in Notepad and enter the following script:

```
# Stop-Lab.ps1
Start-Process "C:\Program Files (x86)\VMware\VMware Workstation\vmrun.exe" -ArgumentList "stop `"C:\VMs\WIN-CLIENT01\WIN-CLIENT01.vmx`" soft"
Start-Sleep -Seconds 10

Start-Process "C:\Program Files (x86)\VMware\VMware Workstation\vmrun.exe" -ArgumentList "stop `"C:\VMs\FGT01\FGT01.vmx`" soft"
Start-Sleep -Seconds 10

Start-Process "C:\Program Files (x86)\VMware\VMware Workstation\vmrun.exe" -ArgumentList "stop `"C:\VMs\MGMT01\MGMT01.vmx`" soft"
Start-Sleep -Seconds 10

Start-Process "C:\Program Files (x86)\VMware\VMware Workstation\vmrun.exe" -ArgumentList "stop `"C:\VMs\LOG01\LOG01.vmx`" soft"
Start-Sleep -Seconds 10

Start-Process "C:\Program Files (x86)\VMware\VMware Workstation\vmrun.exe" -ArgumentList "stop `"C:\VMs\FS01\FS01.vmx`" soft"
```

```
Start-Sleep -Seconds 10

Start-Process "C:\Program Files (x86)\VMware\VMware Workstation\vmrun.exe" -ArgumentList "stop `"C:\VMs\DC01\DC01.vmx`" soft"
```

Save this file as Stop-Lab.ps1 in the same directory.

Execution Policy Configuration
Open PowerShell as an administrator and run:

```
Set-ExecutionPolicy RemoteSigned
```

This allows the scripts to run without interruption.

Creating GUI Shortcuts
Right-click each PowerShell script and select Create Shortcut. Rename the shortcuts to Start Lab and Stop Lab. Right-click each shortcut, open Properties, and modify the Target field so that it launches PowerShell with the script as an argument:

```
powershell.exe -ExecutionPolicy Bypass -File "C:\LabScripts\Start-Lab.ps1"
```

Apply the changes.

Pinning to the Taskbar
Right-click each shortcut and select Pin to taskbar. This places the automation controls directly on the Windows taskbar for immediate access.

Pinning to the Start Menu
Right-click each shortcut again and select Pin to Start. This adds tiles to the Start Menu for additional accessibility.

Verification
Click the Start Lab button and verify that each VM powers on in the correct order. Once all machines are running, confirm that domain services are available and that Cockpit displays live metrics. Click the Stop Lab button and verify that the machines shut down in the correct order. If any VM fails to start or stop, verify the VMX path and ensure that VMware Workstation Pro is installed correctly.

At this point, the environment is fully operational, monitored, and automated. The next section will introduce advanced FortiGate configuration, including deep inspection, segmentation, logging architecture, and enterprise-grade hardening.

# SECTION 5

# ADVANCED FORTIGATE CONFIGURATION, ENTERPRISE HARDENING, SEGMENTATION, INSPECTION, LOGGING, AND OPERATIONAL PRACTICES

This section transforms the FortiGate from a basic routing device into a fully hardened, enterprise-grade security appliance. It introduces advanced segmentation, VLAN design, deep SSL inspection, intrusion prevention tuning, application control, web filtering, DNS filtering, botnet protection, advanced NAT, virtual IPs, certificate management, logging architecture, administrative hardening, lifecycle management, and operational best practices. Every configuration step includes explicit GUI paths and is written to match professional Fortinet deployment standards.

---

## ADVANCED INTERFACE SEGMENTATION AND VLAN DESIGN

Segmentation is the foundation of a secure enterprise network. It reduces lateral movement, isolates sensitive systems, and allows the firewall to enforce policy boundaries. Begin by navigating to Network > Interfaces. Select port2, which currently serves as the LAN interface for the test subnet. Convert port2 into a trunk interface capable of carrying multiple VLANs. This is done by editing port2 and setting its Role to LAN while ensuring that it is not configured as a hardware switch member.

To create VLANs, navigate to Network > Interfaces and select Create New > Interface. Choose VLAN as the interface type. Assign a VLAN ID and name the interface according to a consistent naming convention such as VLAN20_SERVERS, VLAN30_MANAGEMENT, and VLAN40_TEST. Assign each VLAN interface an IP address appropriate for its subnet. For example, assign VLAN20_SERVERS the IP address 10.0.20.1/24, VLAN30_MANAGEMENT the IP address 10.0.30.1/24, and VLAN40_TEST the IP address 10.0.40.1/24. Set the Interface to port2 so that all VLANs are carried over the same physical link.

Ensure that the switch or virtual switch connected to port2 is configured to pass tagged VLAN traffic. In VMware Workstation, this is handled automatically because VMnet2 does not enforce VLAN restrictions. In a physical environment, the switch port must be configured as a trunk.

---

## INTER-VLAN ROUTING AND POLICY ENFORCEMENT

The FortiGate automatically routes between directly connected networks. However, enterprise security requires explicit firewall policies to control inter-VLAN communication. Navigate to Policy & Objects > Firewall Policy and create policies that define which VLANs may communicate. For example, create a policy allowing the management VLAN to access the server VLAN for administrative purposes. Set the Incoming Interface to VLAN30_MANAGEMENT and the Outgoing Interface to VLAN20_SERVERS. Set the Source and Destination addresses to all or to specific address objects as needed. Enable NAT only when traffic must exit the firewall.

Create a second policy denying traffic from the test VLAN to the management VLAN. Set the Incoming Interface to VLAN40_TEST and the Outgoing Interface to VLAN30_MANAGEMENT. Set the Action to Deny and enable Logging so that any attempted access is recorded. This approach ensures that internal segmentation is enforced with the same rigor as external traffic filtering.

---

## DEEP SSL INSPECTION AND CERTIFICATE DEPLOYMENT

Deep SSL inspection allows the FortiGate to decrypt and inspect encrypted traffic. Navigate to Security Profiles > SSL/SSH Inspection and select the deep inspection profile. The FortiGate uses a built-in CA certificate to re-sign inspected traffic. To avoid certificate warnings, deploy the Fortinet_CA_SSL certificate to all client devices. Navigate to System > Certificates and download the CA certificate. Install the certificate on each Windows client by importing it into the Trusted Root Certification Authorities store.

Apply the deep inspection profile to outbound policies by navigating to Policy & Objects > Firewall Policy and editing the LAN-to-WAN policy. Under Security Profiles, enable SSL/SSH Inspection and select the deep inspection profile. This configuration allows the FortiGate to inspect encrypted traffic for malware, intrusion attempts, and policy violations.

---

## INTRUSION PREVENTION SYSTEM (IPS) TUNING

The IPS engine protects against network-based attacks. Navigate to Security Profiles > Intrusion Prevention and create a custom IPS profile. Enable signatures relevant to your environment, such as server vulnerabilities, client vulnerabilities, and known exploit patterns. Disable signatures that are irrelevant to reduce noise. Apply the IPS profile to outbound and inter-VLAN policies by editing each policy and enabling IPS under Security Profiles. This ensures that all traffic is inspected for malicious behavior.

---

## APPLICATION CONTROL CONFIGURATION

Application control identifies and regulates applications regardless of port or protocol. Navigate to Security Profiles > Application Control and create a custom profile. Enable categories such as cloud services, remote access tools, and peer-to-peer applications. Block or monitor applications based on organizational requirements. Apply the application control profile to outbound and inter-VLAN policies. This configuration provides visibility into application usage and prevents unauthorized applications from operating within the network.

---

## WEB FILTERING AND CONTENT CONTROL

Web filtering allows the FortiGate to categorize and control web traffic. Navigate to Security Profiles > Web Filter and create a custom profile. Enable category-based filtering and block categories such as malware, phishing, and high-risk content. Enable safe search enforcement and URL filtering if needed. Apply the web filter profile to outbound policies. This configuration ensures that users cannot access malicious or inappropriate websites.

---

## DNS FILTERING AND BOTNET PROTECTION

DNS filtering blocks malicious domains before connections are established. Navigate to Security Profiles > DNS Filter and create a custom profile. Enable domain filtering and block categories such as malware, phishing, and botnet command-and-control. Apply the DNS filter profile to outbound policies. Navigate to Security Profiles > AntiVirus and enable botnet C&C detection. This configuration prevents clients from communicating with known malicious domains.

---

## ADVANCED NAT AND VIRTUAL IP CONFIGURATION

Advanced NAT allows the FortiGate to host internal services externally. Navigate to Policy & Objects > Virtual IPs and create a new virtual IP mapping an external address to an internal server. For example, map 192.168.50.30:443 to 192.168.50.11:443 to expose a secure web service. After creating the virtual IP, navigate to Policy & Objects > Firewall Policy and create a policy allowing inbound traffic to the virtual IP. Enable security profiles to inspect inbound traffic. This configuration allows secure external access to internal services.

---

## LOGGING ARCHITECTURE AND REMOTE SYSLOG

Logging is essential for auditing and incident response. Navigate to Log & Report > Log Settings and configure the FortiGate to store logs locally and forward them to a remote syslog server if available. If LOG01 is intended to serve as a syslog receiver, install a syslog daemon on LOG01 and configure it to accept logs from the FortiGate. In the FortiGate GUI, specify the IP address of LOG01 as the syslog destination. Enable logging for all traffic, events, and security incidents. This configuration ensures that logs are preserved even if the FortiGate is rebooted or reset.

---

## CERTIFICATE MANAGEMENT

Certificate management is essential for SSL inspection and secure administration. Navigate to System > Certificates and import any required certificates. For SSL inspection, deploy the Fortinet_CA_SSL certificate to all client devices. For secure administration, import a trusted certificate for the FortiGate's web interface. This ensures that administrators do not encounter certificate warnings when accessing the device.

---

## ADMINISTRATIVE HARDENING

Administrative hardening reduces the attack surface of the FortiGate. Navigate to System > Administrators and create individual administrator accounts for each person who manages the device. Assign roles based on the principle of least privilege. Navigate to System > Settings and enable two-factor authentication for administrative access. Navigate to Network > Interfaces and restrict administrative access to specific trusted IP addresses. Disable any unused interfaces and administrative protocols. These measures ensure that only authorized personnel can manage the device.

---

## BACKUP AND LIFECYCLE MANAGEMENT

Regular maintenance ensures long-term stability. Navigate to System > Maintenance > Backup & Restore and create scheduled backups of the configuration. Store backups securely. Before upgrading firmware, review release notes and perform a configuration backup. Apply firmware updates during maintenance windows. After upgrading, verify that all interfaces, policies, and services function correctly. Periodically review the configuration to remove unused objects, policies, and interfaces.

---

## OPERATIONAL BEST PRACTICES

Operational excellence requires regular review and monitoring. Schedule periodic audits of firewall policies, objects, and interfaces. Review logs for anomalies. Test failover procedures if high availability is configured. Maintain documentation of the network topology, firewall policies, and configuration changes. These practices ensure long-term stability and security.