

Fortinet Device Management Using FortiManager

Course:

Fortinet Cyber Security

Instructor Name:

Eng.Hamada Hegazy

Team Members:

Nourseen Tarek

Rodina Hesham

Lamess Mamdoh

Hazem Wagdy

Abdallah Waleed

Mohamed Omar

TABLE OF CONTENTS

Introduction	3
Project Objectives:	3
1. Overview	4
Network Topology	4
4. Device IP Configuration	5
FortiGate HQ	5
FortiGate Branch 1	5
FortiGate Branch 2	6
FortiManager	6
Firewall Policies Configured	7
5.1 FortiGate HQ – Firewall Policies	7
Policy 1 – LAN → WAN	7
VIP for FortiManager Access	8
Policy 2 – WAN → LAN (For VIP Access)	8
Purpose: Allow FortiManager management GUI access through VIP	8
5.2 FortiGate Branch 1 – Firewall Policies	9
Policy 1 – LAN → WAN	9
Purpose: Allows Branch1 LAN to access the Internet	9
Policy 2 – WAN → LAN	9
Purpose: Allows FortiManager to reach Branch1/2	10
5.3 FortiGate Branch 2 – Firewall Policies the same as branch 1	10
6 Connectivity & Reachability Verification	10
1. Branches → HQ and Forti Manager Connectivity	10
We tested that Branch1 and Branch2 can reach the HQ firewall and Forti Manager :	10
2. HQ → Branches Connectivity and FortiManager Reachability	11
We also ensured that HQ can reach the public IPs of Branch1 , Branch2 and Forti Manager :	12
3. FortiManager → FortiGate Devices Reachability	12
5. Opening FortiManager & Creating ADOM	13
5.1 Accessing FortiManager GUI	13
5.2 Creating a New ADOM	14
6. Adding Devices into FortiManager	15
6.1 Adding a FortiGate Device	15
8. Creating Centralized Policies on FortiManager & Installing Them on FortiGates	17
8.1 Creating a New Policy Package	17

INTRODUCTION

This project focuses on building, configuring, and managing a multi-branch Fortinet security infrastructure using **FortiManager** and **FortiGate firewalls** within a simulated GNS3 environment.

The goal of the project is to understand centralized firewall management, policy deployment, troubleshooting connectivity issues, and ensuring proper communication between FortiManager and distributed FortiGate devices.

Throughout this project, we created a complete topology consisting of:

- One FortiManager appliance
- Three FortiGate devices (HQ, Branch 1, Branch 2)
- A cloud network acting as the WAN/Internet
- LAN segments for each branch

We configured addressing, routing, policies, and management settings to enable:

- Device registration on FortiManager
- Policy installation
- Device reachability
- Centralized monitoring and administration

This documentation explains all steps taken across four weeks, problems encountered, troubleshooting methods used, and the final functional setup.

PROJECT OBJECTIVES:

- Build a functional Fortinet environment using GNS3
- Configure FortiManager for centralized device control
- Register and manage multiple FortiGate devices
- Apply and install firewall policies
- Troubleshoot connectivity and version compatibility issues
- Understand FGFM protocol and ADOM versions
- Document all steps, findings, and results

1. OVERVIEW

During Week 1, the main objective was to set up the complete Fortinet environment inside **GNS3**, deploy all virtual devices, configure basic connectivity, and ensure communication between FortiManager and the different FortiGate firewalls.

The work consisted of importing appliance images, building the topology, assigning IP addressing, configuring policies, and preparing the infrastructure for centralized management.

NETWORK TOPOLOGY

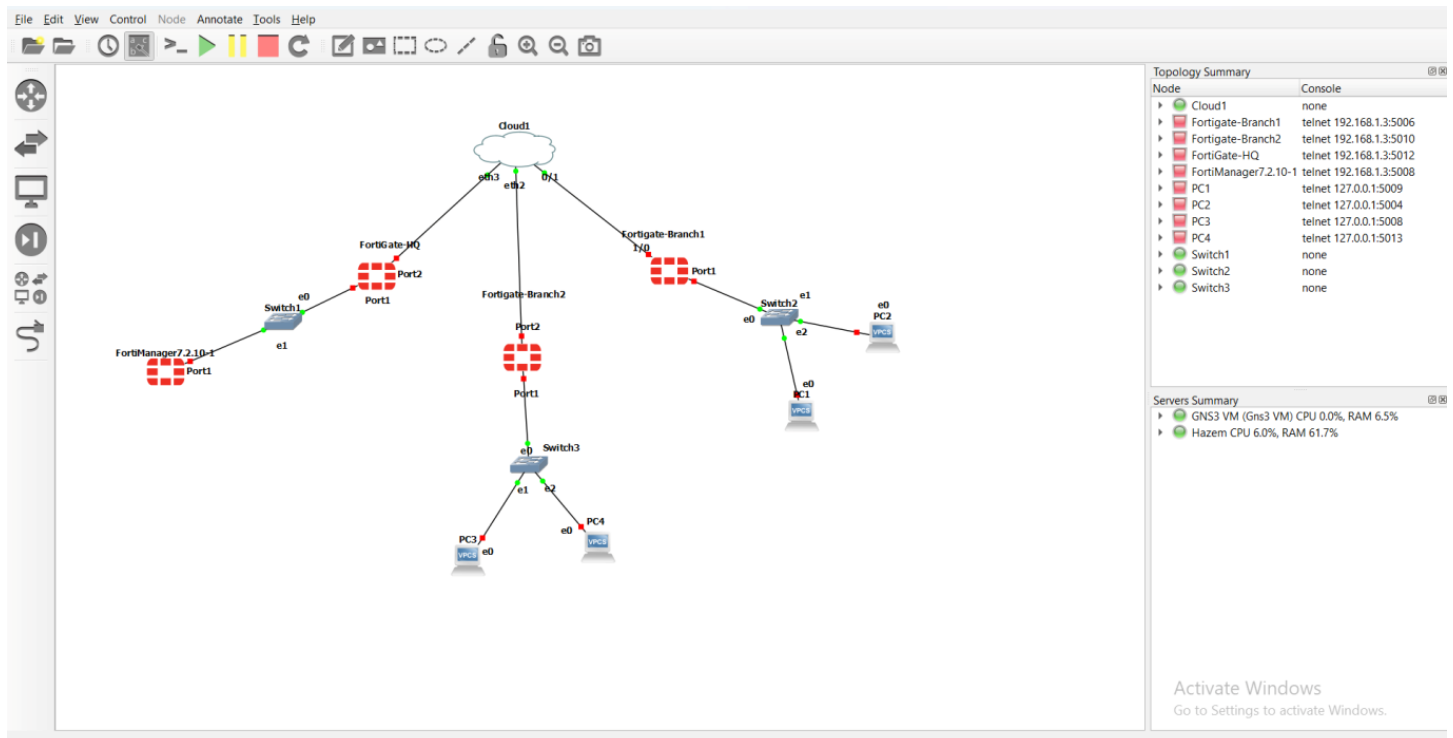


Figure 1 — Project Topology in GNS3

Lab Setup in GNS3

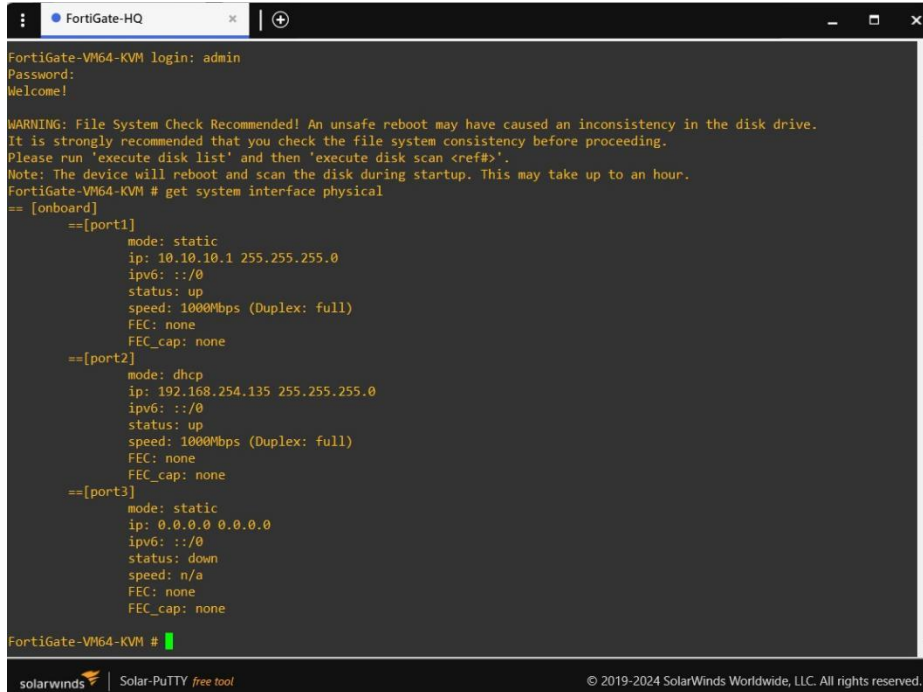
We used **GNS3** to emulate the full network. The following virtual appliances were added:

- **FortiManager** version **7.2.10**
- **FortiGate HQ** – version **7.0.9**
- **FortiGate Branch 1** – version **7.0.9**
- **FortiGate Branch 2** – version **7.0.9**

4. DEVICE IP CONFIGURATION

FORTIGATE HQ

- **WAN (port2):** 192.168.254.135 (DHCP)
- **LAN (port1):** 10.10.10.1



```
FortiGate-VN64-KVM login: admin
Password:
Welcome!

WARNING: File System Check Recommended! An unsafe reboot may have caused an inconsistency in the disk drive.
It is strongly recommended that you check the file system consistency before proceeding.
Please run 'execute disk list' and then 'execute disk scan <ref#>'.
Note: The device will reboot and scan the disk during startup. This may take up to an hour.
FortiGate-VN64-KVM # get system interface physical
== [onboard]
  ==[port1]
    mode: static
    ip: 10.10.10.1 255.255.255.0
    ipv6: ::/0
    status: up
    speed: 1000Mbps (Duplex: full)
    FEC: none
    FEC_cap: none
  ==[port2]
    mode: dhcp
    ip: 192.168.254.135 255.255.255.0
    ipv6: ::/0
    status: up
    speed: 1000Mbps (Duplex: full)
    FEC: none
    FEC_cap: none
  ==[port3]
    mode: static
    ip: 0.0.0.0 0.0.0.0
    ipv6: ::/0
    status: down
    speed: n/a
    FEC: none
    FEC_cap: none
FortiGate-VN64-KVM #
```

FORTIGATE BRANCH 1

- **WAN (port2):** 192.168.254.133 (DHCP)
- **LAN (port1):** 10.20.20.1

```
Fortigate-Branch1
ip: 0.0.0.0 0.0.0.0
ipv6: ::/0
status: down
speed: n/a
FEC: none
FEC_cap: none
==[port4]

FortiGate-VM64-KVM #
FortiGate-VM64-KVM #
FortiGate-VM64-KVM # get system interface physical
== [onboard]
==[port1]
mode: static
ip: 10.20.20.1 255.255.255.0
ipv6: ::/0
status: up
speed: 1000Mbps (Duplex: full)
FEC: none
FEC_cap: none
==[port2]
mode: dhcp
ip: 192.168.254.134 255.255.255.0
ipv6: ::/0
status: up
speed: 1000Mbps (Duplex: full)
FEC: none
FEC_cap: none
==[port3]
mode: static
ip: 0.0.0.0 0.0.0.0
ipv6: ::/0
status: down
speed: n/a
FEC: none
FEC_cap: none
--More--
```

FORTIGATE BRANCH 2

- **WAN (port2):** 192.168.254.134 (DHCP)
- **LAN (port1):** 10.30.30.1

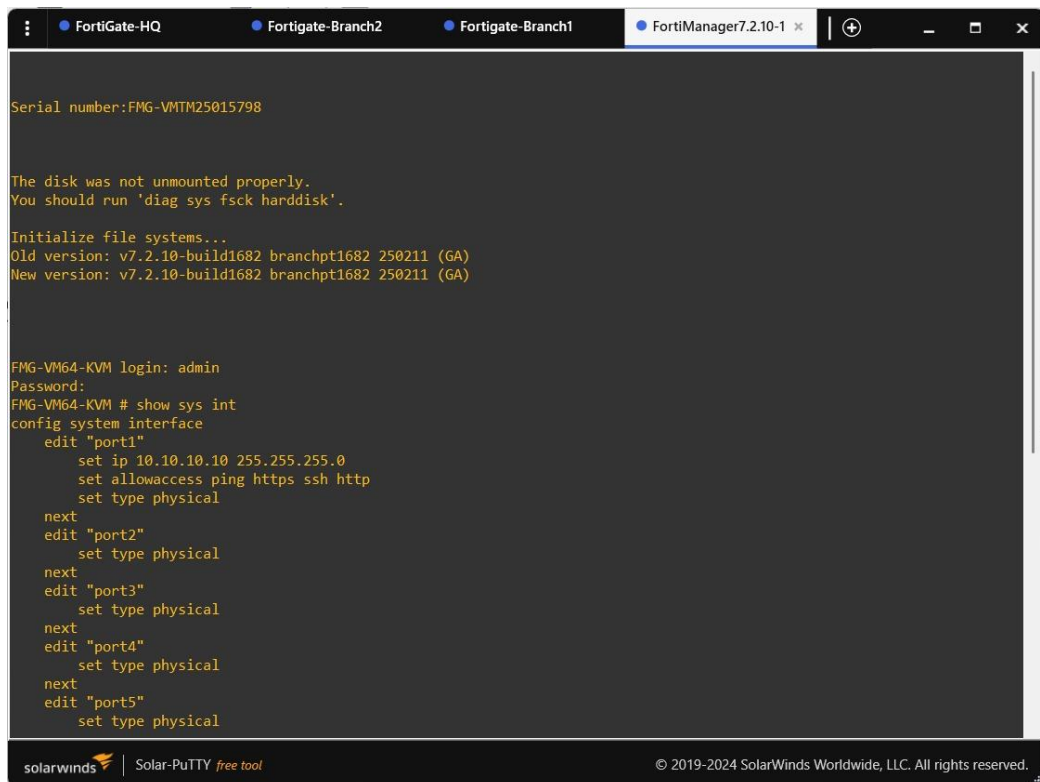
```
Fortigate-Branch2
FortiGate-VM64-KVMadminn:
Password:
Welcome!

WARNING: File System Check Recommended! An unsafe reboot may have caused an inconsistency in the disk drive.
It is strongly recommended that you check the file system consistency before proceeding.
Please run 'execute disk list' and then 'execute disk scan <ref#>'.
Note: The device will reboot and scan the disk during startup. This may take up to an hour.
FortiGate-VM64-KVM # get system interface physical
== [onboard]
==[port1]
mode: static
ip: 10.30.30.1 255.255.255.0
ipv6: ::/0
status: up
speed: 1000Mbps (Duplex: full)
FEC: none
FEC_cap: none
==[port2]
mode: dhcp
ip: 192.168.254.133 255.255.255.0
ipv6: ::/0
status: up
speed: 1000Mbps (Duplex: full)
FEC: none
FEC_cap: none
==[port3]
mode: static
ip: 0.0.0.0 0.0.0.0
ipv6: ::/0
status: down
speed: n/a
FEC: none
FEC_cap: none

FortiGate-VM64-KVM #
```

FORTIMANAGER

- **port1:** 10.10.10.10



```
Serial number:FMG-VMTM25015798

The disk was not unmounted properly.
You should run 'diag sys fsck hddisk'.

Initialize file systems...
Old version: v7.2.10-build1682 branchpt1682 250211 (GA)
New version: v7.2.10-build1682 branchpt1682 250211 (GA)

FMG-VM64-KVM login: admin
Password:
FMG-VM64-KVM # show sys int
config system interface
    edit "port1"
        set ip 10.10.10.10 255.255.255.0
        set allowaccess ping https ssh http
        set type physical
    next
    edit "port2"
        set type physical
    next
    edit "port3"
        set type physical
    next
    edit "port4"
        set type physical
    next
    edit "port5"
        set type physical
```

solarwinds | Solar-PuTTY free tool © 2019-2024 SolarWinds Worldwide, LLC. All rights reserved.

FIREWALL POLICIES CONFIGURED

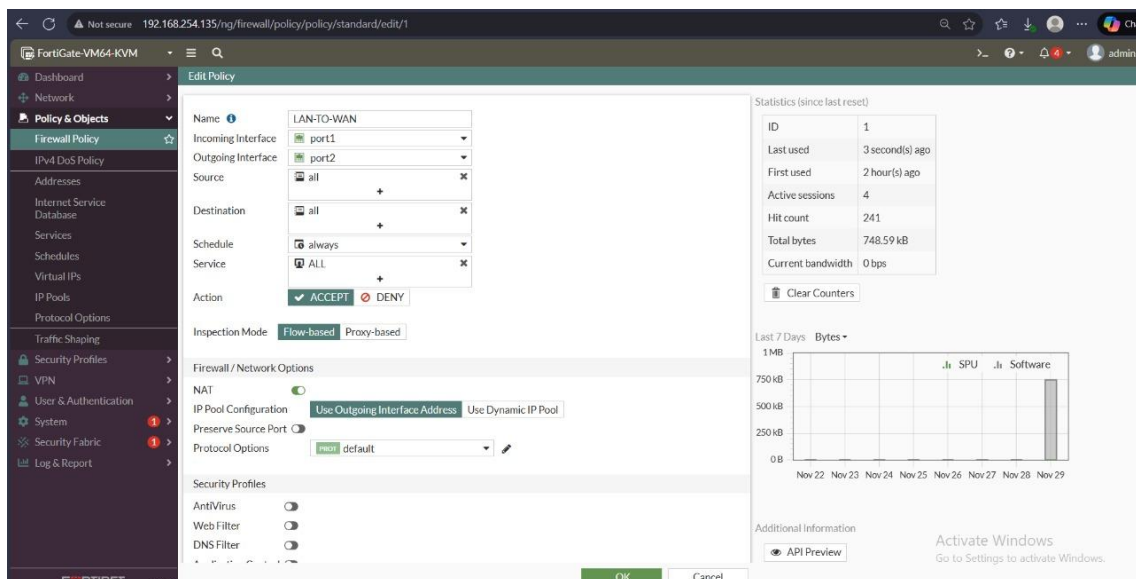
firewall policies were created on each FortiGate device to ensure basic communication between LAN networks, the cloud network, and FortiManager.

Below are the policies **for each device separately**.

5.1 FORTIGATE HQ – FIREWALL POLICIES

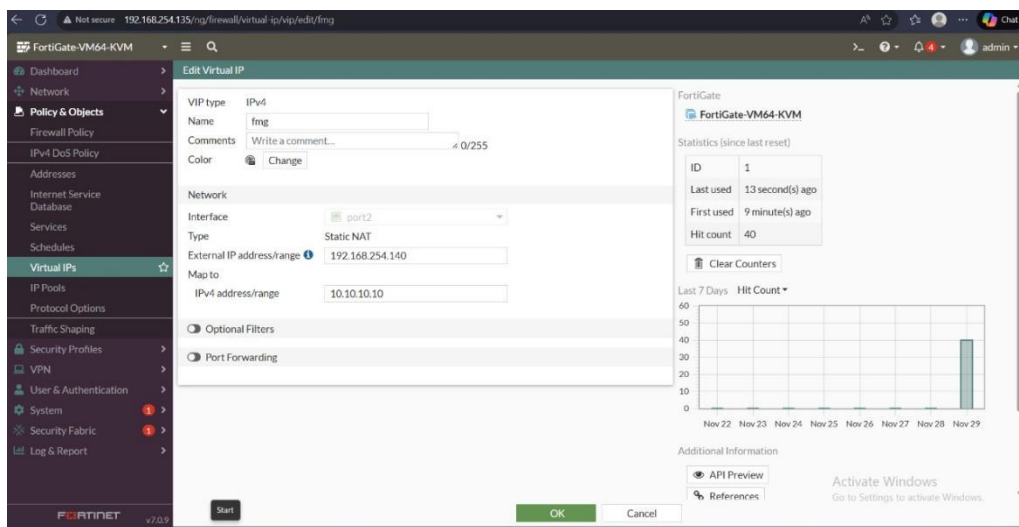
POLICY 1 – LAN → WAN

Allows internal HQ users to access the Internet.



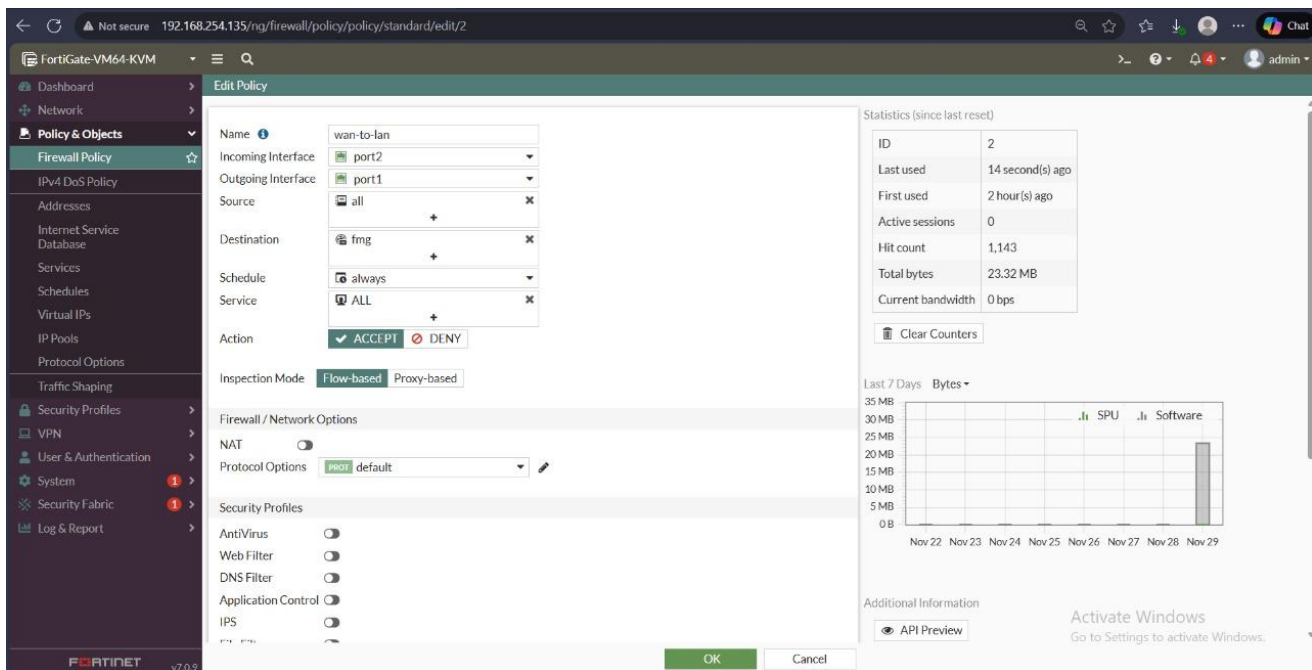
VIP FOR FORTIMANAGER ACCESS

To allow access to the FortiManager GUI from the WAN/Cloud network, we created a VIP:



POLICY 2 — WAN → LAN (FOR VIP ACCESS)

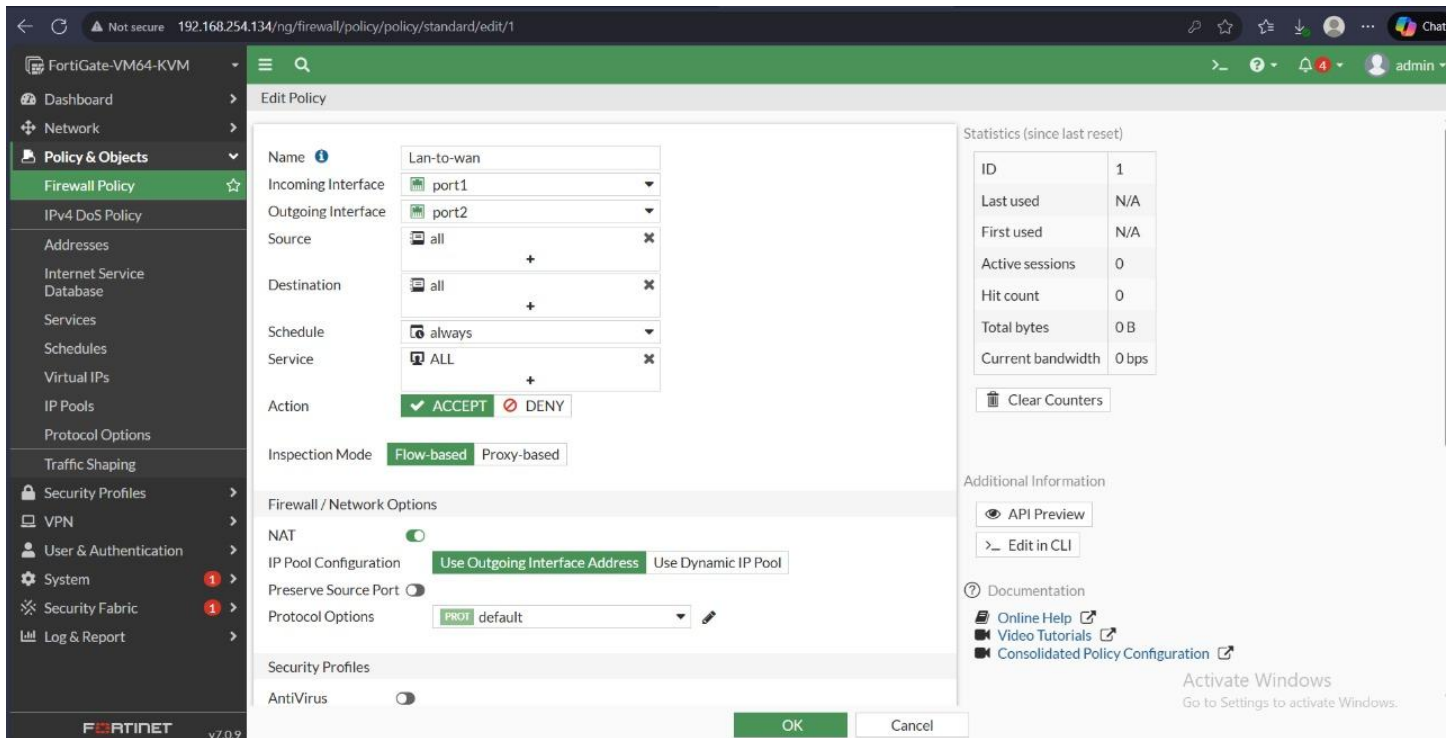
PURPOSE: ALLOW FORTIMANAGER MANAGEMENT GUI ACCESS THROUGH VIP.



5.2 FORTIGATE BRANCH 1 – FIREWALL POLICIES

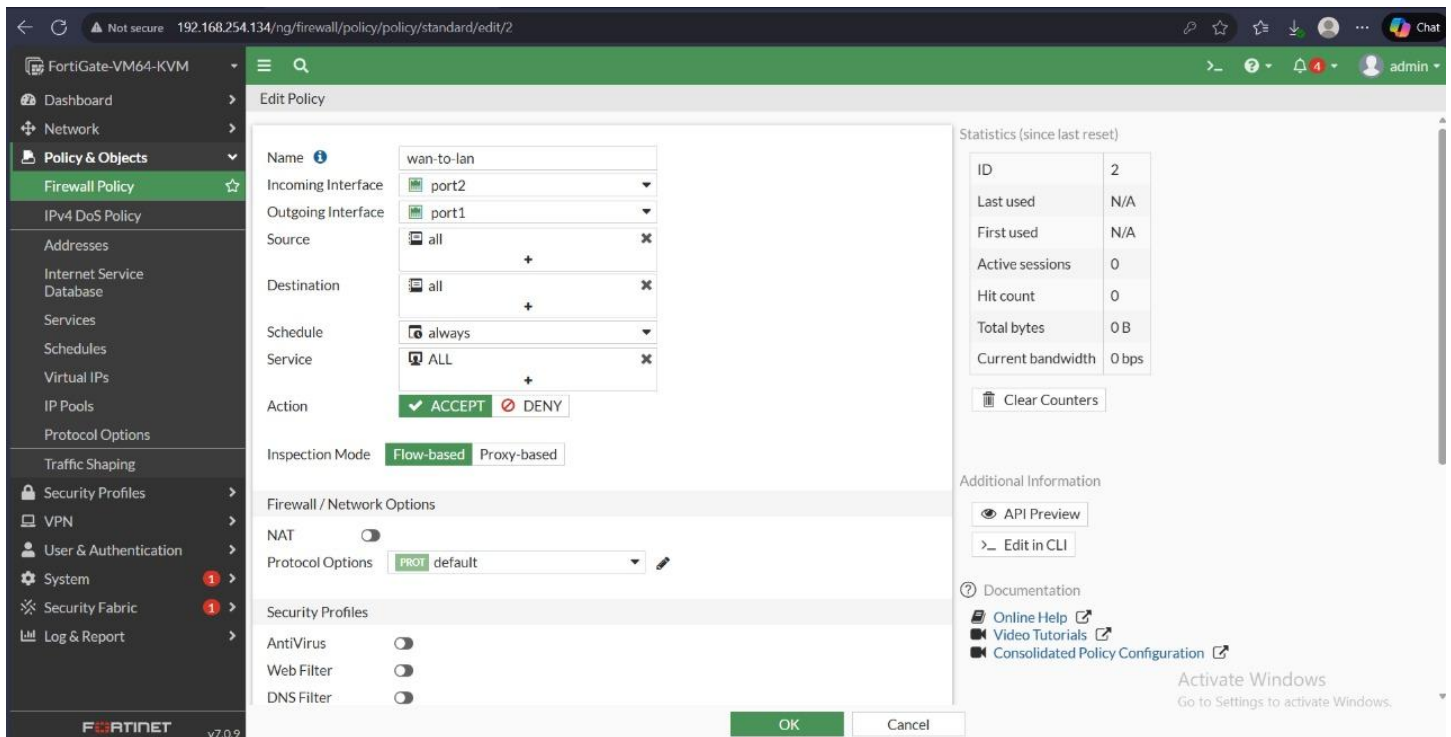
POLICY 1 – LAN → WAN

PURPOSE: ALLOWS BRANCH1 LAN TO ACCESS THE INTERNET.



POLICY 2 – WAN → LAN

PURPOSE: ALLOWS FORTIMANAGER TO REACH BRANCH1/2.



5.3 FORTIGATE BRANCH 2 – FIREWALL POLICIES THE SAME AS BRANCH 1

6 CONNECTIVITY & REACHABILITY VERIFICATION

Before connecting the FortiGate devices to FortiManager, we verified the reachability between all sites to ensure that communication works properly.

1. BRANCHES → HQ AND FORTI MANAGER CONNECTIVITY

WE TESTED THAT BRANCH1 AND BRANCH2 CAN REACH THE HQ FIREWALL AND FORTI MANAGER :

```
Fortigate-Branch1
execute ping 192.168.254.135
PING 192.168.254.135 (192.168.254.135): 56 data bytes
64 bytes from 192.168.254.135: icmp_seq=0 ttl=255 time=3.4 ms
64 bytes from 192.168.254.135: icmp_seq=1 ttl=255 time=2.8 ms
64 bytes from 192.168.254.135: icmp_seq=2 ttl=255 time=2.0 ms
64 bytes from 192.168.254.135: icmp_seq=3 ttl=255 time=1.6 ms
64 bytes from 192.168.254.135: icmp_seq=4 ttl=255 time=1.7 ms

--- 192.168.254.135 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 1.6/2.3/3.4 ms

FortiGate-VM64-KVM # execute ping 192.168.254.140
PING 192.168.254.140 (192.168.254.140): 56 data bytes
64 bytes from 192.168.254.140: icmp_seq=0 ttl=63 time=5.0 ms
64 bytes from 192.168.254.140: icmp_seq=1 ttl=63 time=4.3 ms
64 bytes from 192.168.254.140: icmp_seq=2 ttl=63 time=2.4 ms
64 bytes from 192.168.254.140: icmp_seq=3 ttl=63 time=5.3 ms
64 bytes from 192.168.254.140: icmp_seq=4 ttl=63 time=3.6 ms

--- 192.168.254.140 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 2.4/4.1/5.3 ms

FortiGate-VM64-KVM #
```

```
Fortigate-Branch2
execute ping 192.168.254.135
PING 192.168.254.135 (192.168.254.135): 56 data bytes
64 bytes from 192.168.254.135: icmp_seq=0 ttl=255 time=3.3 ms
64 bytes from 192.168.254.135: icmp_seq=1 ttl=255 time=1.9 ms
64 bytes from 192.168.254.135: icmp_seq=2 ttl=255 time=1.1 ms
64 bytes from 192.168.254.135: icmp_seq=3 ttl=255 time=1.5 ms
64 bytes from 192.168.254.135: icmp_seq=4 ttl=255 time=1.1 ms

--- 192.168.254.135 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 1.1/1.7/3.3 ms

FortiGate-VM64-KVM # execute ping 192.168.254.140
PING 192.168.254.140 (192.168.254.140): 56 data bytes
64 bytes from 192.168.254.140: icmp_seq=0 ttl=63 time=6.2 ms
64 bytes from 192.168.254.140: icmp_seq=1 ttl=63 time=2.7 ms
64 bytes from 192.168.254.140: icmp_seq=2 ttl=63 time=1.9 ms
64 bytes from 192.168.254.140: icmp_seq=3 ttl=63 time=3.9 ms
64 bytes from 192.168.254.140: icmp_seq=4 ttl=63 time=6.0 ms

--- 192.168.254.140 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 1.9/4.1/6.2 ms

FortiGate-VM64-KVM #
```

2. HQ → BRANCHES CONNECTIVITY AND FORTIMANAGER REACHABILITY

WE ALSO ENSURED THAT HQ CAN REACH THE PUBLIC IPS OF BRANCH1 , BRANCH2
AND FORTI MANAGER :

```
FortiGate-HQ
64 bytes from 192.168.254.134: icmp_seq=0 ttl=255 time=1.5 ms
64 bytes from 192.168.254.134: icmp_seq=1 ttl=255 time=2.6 ms
64 bytes from 192.168.254.134: icmp_seq=2 ttl=255 time=2.3 ms
64 bytes from 192.168.254.134: icmp_seq=3 ttl=255 time=1.5 ms
64 bytes from 192.168.254.134: icmp_seq=4 ttl=255 time=1.1 ms

--- 192.168.254.134 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 1.1/1.8/2.6 ms

FortiGate-VM64-KVM #
FortiGate-VM64-KVM # execute ping 192.168.254.133
PING 192.168.254.133 (192.168.254.133): 56 data bytes
64 bytes from 192.168.254.133: icmp_seq=0 ttl=255 time=2.5 ms
64 bytes from 192.168.254.133: icmp_seq=1 ttl=255 time=2.1 ms
64 bytes from 192.168.254.133: icmp_seq=2 ttl=255 time=3.1 ms
64 bytes from 192.168.254.133: icmp_seq=3 ttl=255 time=2.4 ms
64 bytes from 192.168.254.133: icmp_seq=4 ttl=255 time=2.3 ms

--- 192.168.254.133 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 2.1/2.4/3.1 ms

FortiGate-VM64-KVM # execute ping 10.10.10.10
PING 10.10.10.10 (10.10.10.10): 56 data bytes
64 bytes from 10.10.10.10: icmp_seq=0 ttl=64 time=1.9 ms
64 bytes from 10.10.10.10: icmp_seq=1 ttl=64 time=2.4 ms
64 bytes from 10.10.10.10: icmp_seq=2 ttl=64 time=2.8 ms
64 bytes from 10.10.10.10: icmp_seq=3 ttl=64 time=1.8 ms
64 bytes from 10.10.10.10: icmp_seq=4 ttl=64 time=3.0 ms

--- 10.10.10.10 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 1.8/2.3/3.0 ms

FortiGate-VM64-KVM #
```

3. FORTIMANAGER → FORTIGATE DEVICES REACHABILITY

After confirming that all FortiGate devices can reach each other, we verified that **FortiManager can also reach the HQ and Branch firewalls** .

```
FortiManager7.2.10-1 x | +
FMG-VM64-KVM #
FMG-VM64-KVM #
FMG-VM64-KVM # ^?^?^?

FMG-VM64-KVM # execute ping 192.168.254.134
PING 192.168.254.134 (192.168.254.134): 56 data bytes
64 bytes from 192.168.254.134: seq=0 ttl=254 time=5.042 ms
64 bytes from 192.168.254.134: seq=1 ttl=254 time=3.856 ms
64 bytes from 192.168.254.134: seq=2 ttl=254 time=4.296 ms
^C
--- 192.168.254.134 ping statistics ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 3.856/4.398/5.042 ms

FMG-VM64-KVM # execute ping 192.168.254.133
PING 192.168.254.133 (192.168.254.133): 56 data bytes
64 bytes from 192.168.254.133: seq=0 ttl=254 time=6.108 ms
64 bytes from 192.168.254.133: seq=1 ttl=254 time=5.721 ms
64 bytes from 192.168.254.133: seq=2 ttl=254 time=3.739 ms
^C
--- 192.168.254.133 ping statistics ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 3.739/5.189/6.108 ms

FMG-VM64-KVM # execute ping 192.168.254.135
PING 192.168.254.135 (192.168.254.135): 56 data bytes
64 bytes from 192.168.254.135: seq=0 ttl=255 time=4.213 ms
64 bytes from 192.168.254.135: seq=1 ttl=255 time=2.529 ms
64 bytes from 192.168.254.135: seq=2 ttl=255 time=2.136 ms
64 bytes from 192.168.254.135: seq=3 ttl=255 time=1.751 ms

--- 192.168.254.135 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 1.751/2.657/4.213 ms

FMG-VM64-KVM #
```

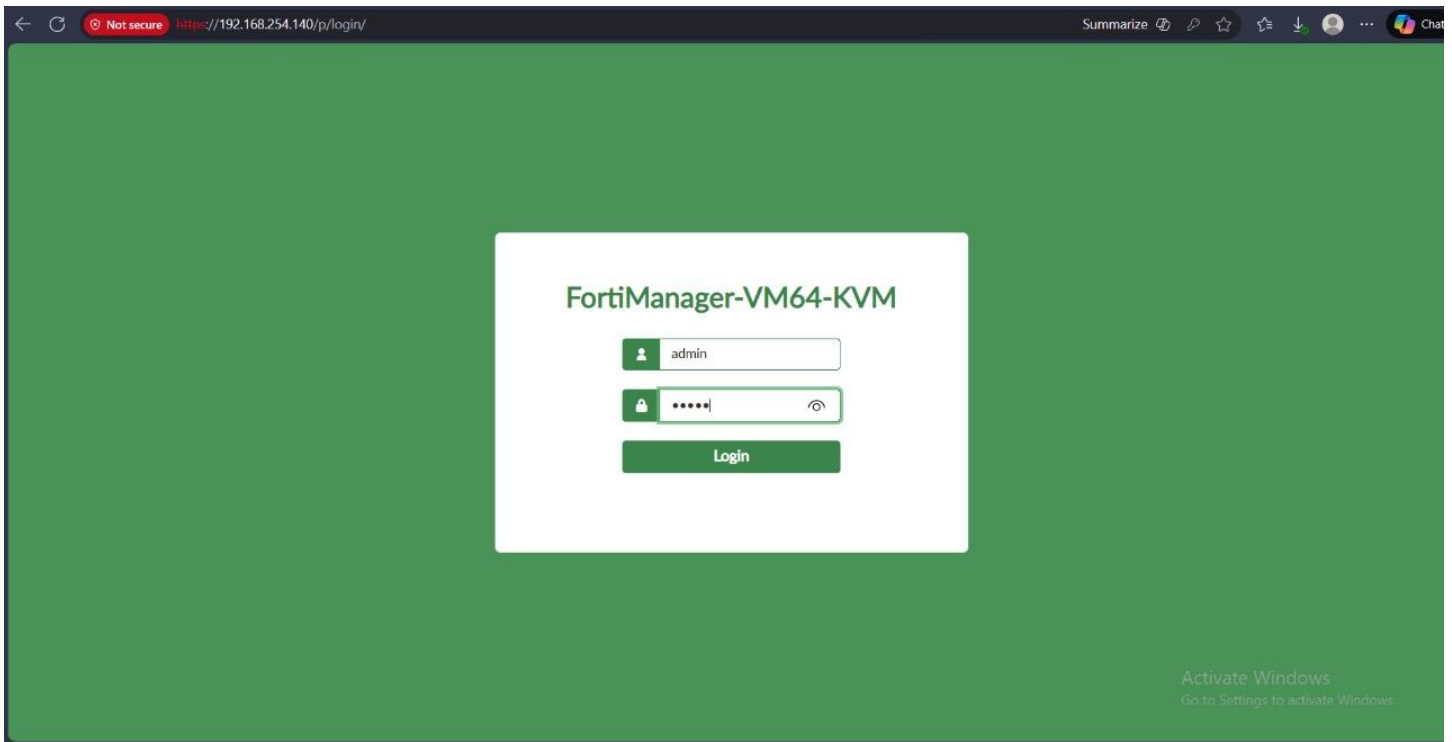
solarwinds | Solar-PuTTY free tool © 2019-2024 SolarWinds Worldwide, LLC. All rights reserved.

5. OPENING FORTIMANAGER & CREATING ADOM

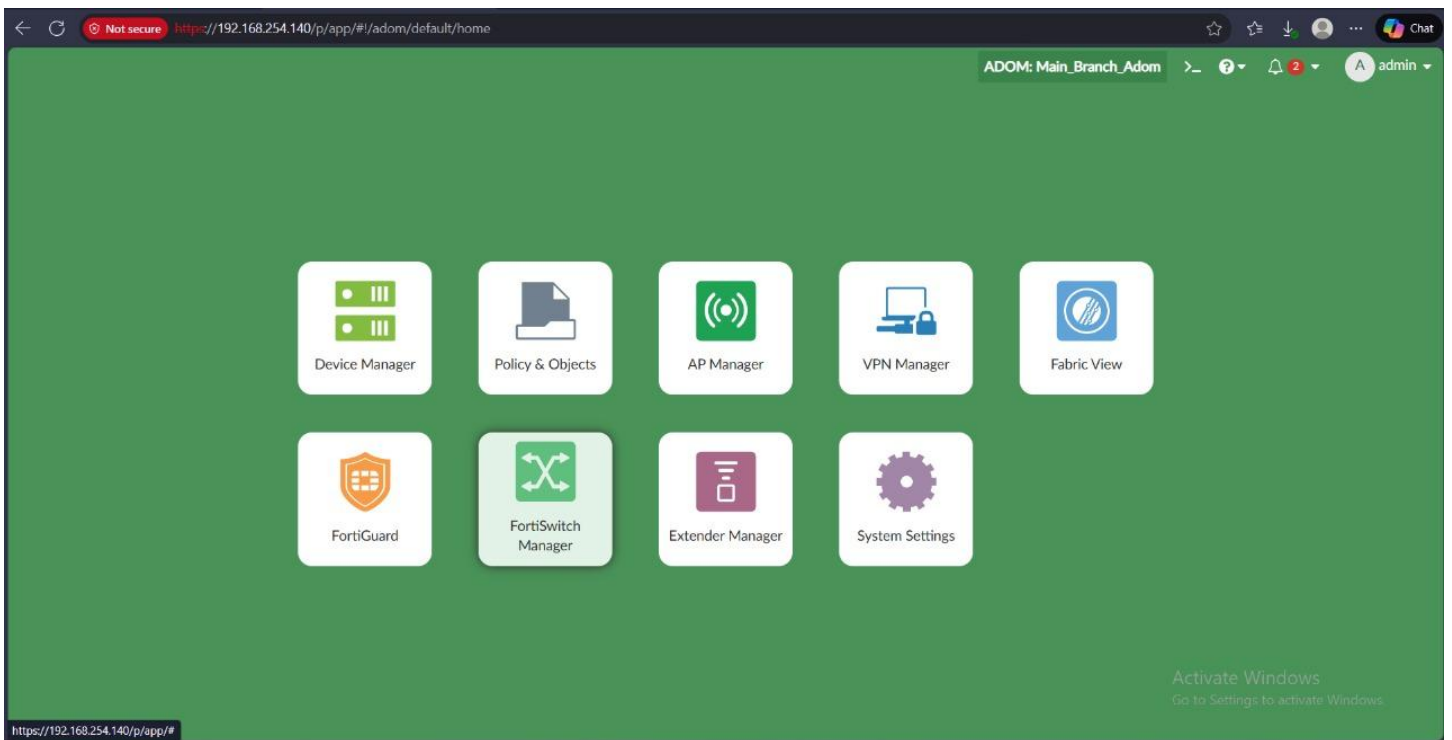
After ensuring full connectivity between FortiGate devices and the FortiManager server, we proceeded to access the FortiManager Web GUI and prepare the management environment.

5.1 ACCESSING FORTIMANAGER GUI

We connected to FortiManager using the assigned VIP:



A successful login indicated that the VIP, policies, and routing were all correctly configured.



5.2 CREATING A NEW ADOM

Inside the FortiManager dashboard, we created a new ADOM to logically separate and manage our FortiGate devices.

Create ADOM

Name

Main_Branch_Adom

Type

FortiGate

6.4 7.0 7.2

Description

Devices

+ Select Device

Search...

☐	Name	IP Address	Platform
No record found.			
			0

Mode

Normal Backup

Central Management

☐ VPN
☒ FortiAP
☒ FortiSwitch

Default Device Selection for Install

Select All

Deselect All

Perform Policy Check Before Every Install

☐

Auto-Push Policy Packages When Device Back Online

☒

Activate Windows

Go to Settings to activate Windows

OK Cancel

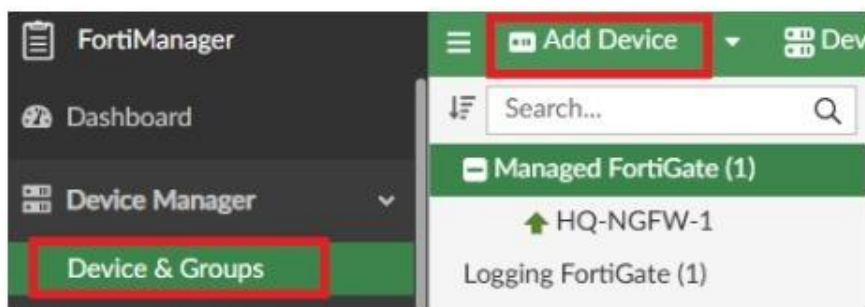
6. ADDING DEVICES INTO FORTIMANAGER

After creating the ADOM, we added the FortiGate devices (HQ, Branch1, Branch2) into FortiManager to begin centralized management.

6.1 ADDING A FORTIGATE DEVICE

Inside the newly created ADOM:

- Navigate to **Device Manager**
- Select **Add Device**



- Enter the device information:
 - **Device IP:** (e.g., HQ → 192.168.254.135)
 - **Login Credentials:** admin account

Add Device - Discover Device (2/3)

The following information has been discovered from the device:

IP Address 192.168.254.135
 Host Name HQ-NGFW-1
 SN FGVM027M24013423
 Model FortiGate-VM64-KVM
 Firmware Version 7.6.0, build 2401 (GA)
 HA Status Standalone
 Administrator admin

Please input the following information to complete addition of the device:

Name
 Description
 Provisioning Templates
 Add To Folder ☐
 Add To Device Group ☐
 Copy Device Dashboard

< Back

Next >

Cancel

FortiGate-VM64-KVM								
Date/Time	Source	Device	Destination	Application Name	Result	Policy ID		
6 seconds ago	192.168.254.134		192.168.254.140		✓ 3.73 kB / 6.05 kB	wan-to-lan (2)		
21 seconds ago	192.168.254.134		192.168.254.140		✓ 3.73 kB / 6.04 kB	wan-to-lan (2)		
38 seconds ago	192.168.254.134		192.168.254.140		✓ 3.69 kB / 6.00 kB	wan-to-lan (2)		
54 seconds ago	192.168.254.134		192.168.254.140		✓ 3.74 kB / 7.79 kB	wan-to-lan (2)		
Minute ago	192.168.254.134		192.168.254.140		✓ 3.74 kB / 7.81 kB	wan-to-lan (2)		
Minute ago	192.168.254.134		192.168.254.140		✓ 3.70 kB / 7.77 kB	wan-to-lan (2)		
Minute ago	192.168.254.134		192.168.254.140		✓ 3.73 kB / 6.04 kB	wan-to-lan (2)		
Minute ago	192.168.254.1		192.168.254.140		✓ 3.24 kB / 440 B	wan-to-lan (2)		
Minute ago	192.168.254.1		192.168.254.140			wan-to-lan (2)		
Minute ago	192.168.254.134		192.168.254.140		✓ 3.69 kB / 6.00 kB	wan-to-lan (2)		
2 minutes ago	192.168.254.1		192.168.254.140		✓ 3.24 kB / 486 B	wan-to-lan (2)		
2 minutes ago	192.168.254.1		192.168.254.140		✓ 3.24 kB / 486 B	wan-to-lan (2)		
2 minutes ago	192.168.254.134		192.168.254.140		✓ 3.74 kB / 7.90 kB	wan-to-lan (2)		
2 minutes ago	192.168.254.134		192.168.254.140		✓ 3.73 kB / 6.05 kB	wan-to-lan (2)		
2 minutes ago	192.168.254.134		192.168.254.140		✓ 3.73 kB / 6.04 kB	wan-to-lan (2)		
3 minutes ago	192.168.254.134		192.168.254.140		✓ 3.73 kB / 6.05 kB	wan-to-lan (2)		
3 minutes ago	192.168.254.134		192.168.254.140		✓ 3.73 kB / 6.05 kB	wan-to-lan (2)		
3 minutes ago	192.168.254.134		192.168.254.140		✓ 3.73 kB / 6.02 kB	wan-to-lan (2)		



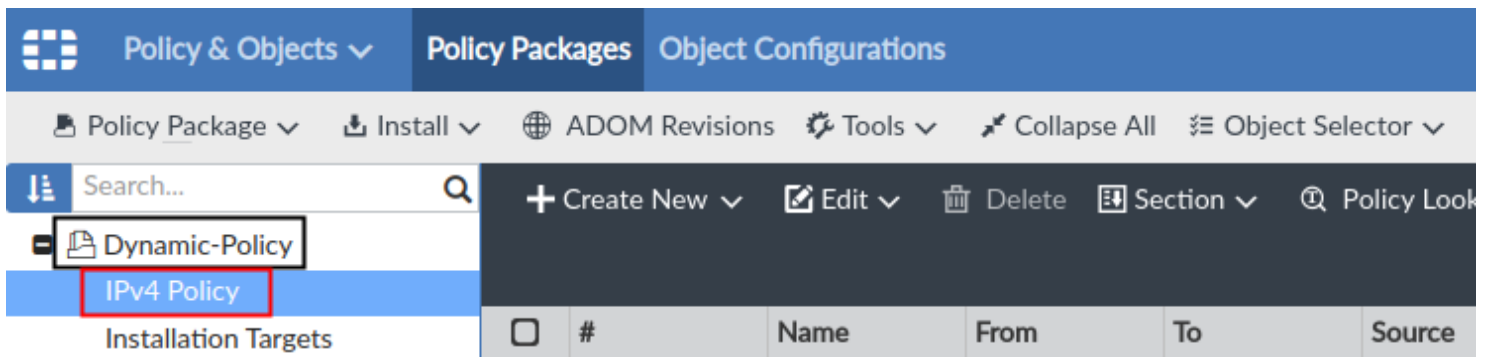
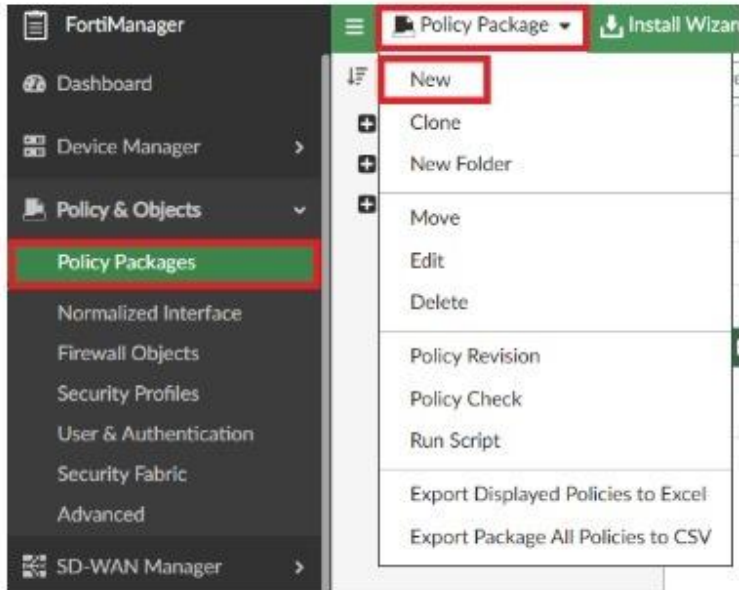
8. CREATING CENTRALIZED POLICIES ON FORTIMANAGER & INSTALLING THEM ON FORTIGATES

After all FortiGate devices were successfully added and authorized in FortiManager, we proceeded to create centralized policies to manage security rules from a single point. These policies were then installed directly on HQ, Branch1, and Branch2.

8.1 CREATING A NEW POLICY PACKAGE

Inside the ADOM:

1. Navigate to **Policy & Objects**
2. Select **Policy Packages**
3. Click **Create New**
4. Name:
 - **HQ-Package** for HQ
 - **Branch1-Package** for Branch 1
 - **Branch2-Package** for Branch 2
5. Assign each package to its corresponding FortiGate device.



Policy & Objects

Policy Package

Install

ADOM Revisions

Tools

cam

Policy Packages

Search...

Branches

Firewall Policy

Installation Targets

default

Object Configurations

Create New Firewall Policy

ID

0

Name

Direct Internet Access

ZTNA

Disable

Full ZTNA

IP/MAC filtering

Incoming Interface

LAN

Outgoing Interface

WAN1

WAN2

Source Internet Service

IPv4 Source Address

Branch Network

IPv6 Source Address

+

Source User

+

Source User Group

+

FSSO Groups

+

Destination Internet Service

IPv4 Destination Address

all

IPv6 Destination Address

+

Service

ALL

Schedule

always

Action

Deny

Accept

IPSEC

Inspection Mode

Flow-based

Proxy-based

Firewall/Network Options

NAT

NAT

NAT46

NAT64

IP Pool Configuration

Use Outgoing Interface Address

Use Dynamic IP Pool

Preserve Source Port

Protocol Options

default

OK

Cancel

FortiManager

Sessions

Policy Package

Save

Install Wizard

Tools

ADOM: My_ADOM

student

Search...

Create New

Edit

Delete

Section

Policy Lookup

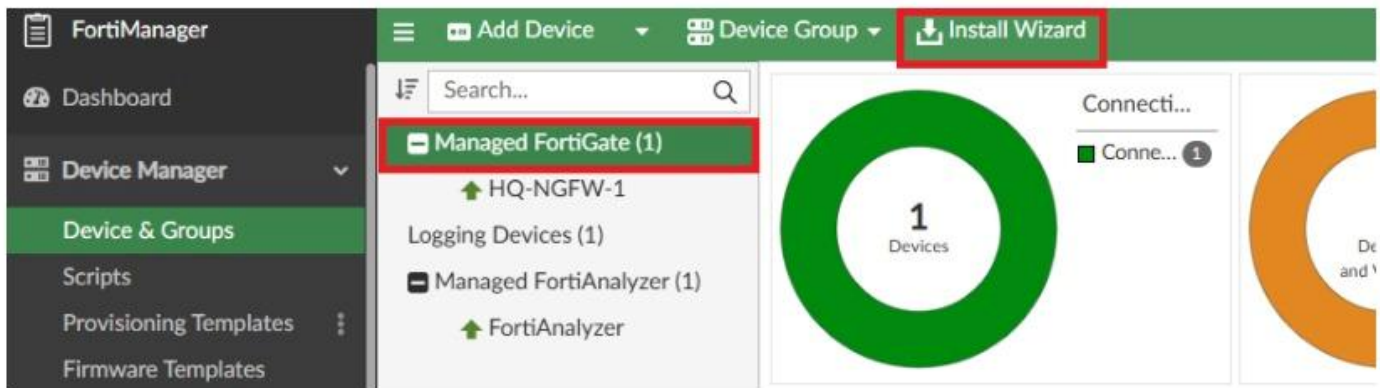
Collapse All

Full Screen

View Mode

Search...

#	Name	From	To	Source	Destination	Schedule	Service
1	Internet	port4	port2	Internal	all	always	ALL
Implicit (2/2 Total:1)							
2	Implicit Deny	any	any	all	all	always	ALL



8. CONCLUSION

This project demonstrated the complete process of deploying and managing multiple FortiGate firewalls using FortiManager within a virtual GNS3 environment. Throughout the implementation, we successfully built a full topology consisting of FortiManager, FortiGate HQ, FortiGate Branch 1, and FortiGate Branch 2, all connected through a cloud network using DHCP addressing.

We configured core network components, including interface settings, static policies (LAN → WAN and WAN → LAN), and VIPs to ensure proper reachability between FortiManager and all FortiGate devices. After resolving version compatibility issues and initial connectivity problems, we were able to access the FortiManager GUI, create an ADOM, import device configurations, and centralize firewall management.

By the end of the project, FortiManager was fully integrated with all FortiGate units, allowing centralized monitoring, policy installation, and configuration control across the entire network.

Overall, this project enhanced our understanding of Fortinet technologies, centralized management concepts, troubleshooting techniques, and the importance of version alignment and network reachability in real-world deployments.