Understanding Firewall Security Using Fortinet's FortiGate Firewall on Virtual Machine (VMware)

Objective

To demonstrate the fundamentals of firewall security through practical deployment and configuration of a Fortinet FortiGate firewall on a virtual machine. This project will cover real-world use cases like traffic filtering, web protection, VPN setup, and threat detection.

Project Requirements

Software/Tools:

- FortiGate VM (Download from Fortinet Support Portal)
- VMware Workstation / VirtualBox
- Web browser (to access GUI)
- Wireshark (for packet analysis)

Project Structure

1. Introduction to Firewalls

- **What is a firewall?**

A firewall is a network security device or software that monitors and controls incoming and outgoing network traffic based on predetermined security rules.

It acts as a barrier between a trusted internal network and an untrusted external network (like the internet), blocking or allowing data packets based on security policies.

- **Why firewall security is critical**

  Firewall security is crucial because it serves as the first line of defense between your internal network and external threats. Without it, your systems are exposed to unauthorized access, cyberattacks, and data breaches.

- **Types of firewalls (Packet-filtering, Stateful Inspection, NGFW)**

(a) Packet-Filtering Firewall

What it does:

- Inspects individual data packets based on source IP, destination IP, port numbers, and protocols.
- Works at the network layer (Layer 3) of the OSI model.
- Uses simple rules to allow or block traffic.

(b) Stateful Inspection Firewall (Dynamic Filtering)

What it does:

- Tracks the state of active connections.
- Remembers established sessions and makes decisions based on the context of the traffic.
- Works at both the network layer (Layer 3) and the transport layer (Layer 4).

(c) Next-Generation Firewall (NGFW)

What it does:

- Combines traditional firewall functions with deep packet inspection, application awareness, and intrusion prevention.
- Works across multiple OSI layers, especially up to Layer 7 (Application Layer).
- Can identify users, devices, and specific apps (e.g., Facebook, BitTorrent).

- **Introduction to Fortinet and FortiGate**

What is Fortinet?

Fortinet is a global cybersecurity company founded in 2000, headquartered in Sunnyvale, California. It is known for delivering broad, integrated, and high-performance security solutions across the IT infrastructure.

Key Facts:

- Founder: **Ken Xie**
- Flagship product: **FortiGate Firewall**
- Other products: FortiAnalyzer, FortiManager, FortiEDR, FortiSwitch, FortiAP
- Security ecosystem: **Fortinet Security Fabric**

Fortinet's mission is to provide automated, intelligent, and integrated security solutions that protect data, devices, applications, and users.

What is FortiGate?

FortiGate is Fortinet's Next-Generation Firewall (NGFW) product line. It provides advanced network security features for small offices, enterprises, data centers, and cloud environments.

What FortiGate Firewalls Do:

- **Control network traffic** using firewall policies
- Protect against **malware, viruses, ransomware, and intrusion attempts**
- Monitor and log network activity
- Enable secure **VPN access** (IPSec and SSL)
- Inspect encrypted (HTTPS/SSL) traffic

2. Installing FortiGate Firewall on VM

Setup Steps:

1. **Download FortiGate VM Image**
    a. Sign up at Fortinet → Get a VM evaluation license.
    b. Choose the image format for your hypervisor (VMware/VirtualBox).
2. **Create Virtual Machine:**
    a. 2 Network Interfaces: one for LAN, one for WAN
    b. Allocate at least:
        i. RAM: 1 GB
        ii. CPU: 1-2 cores
        iii. Disk: 2 GB
3. **Start VM and Access Console**
    a. Default credentials:

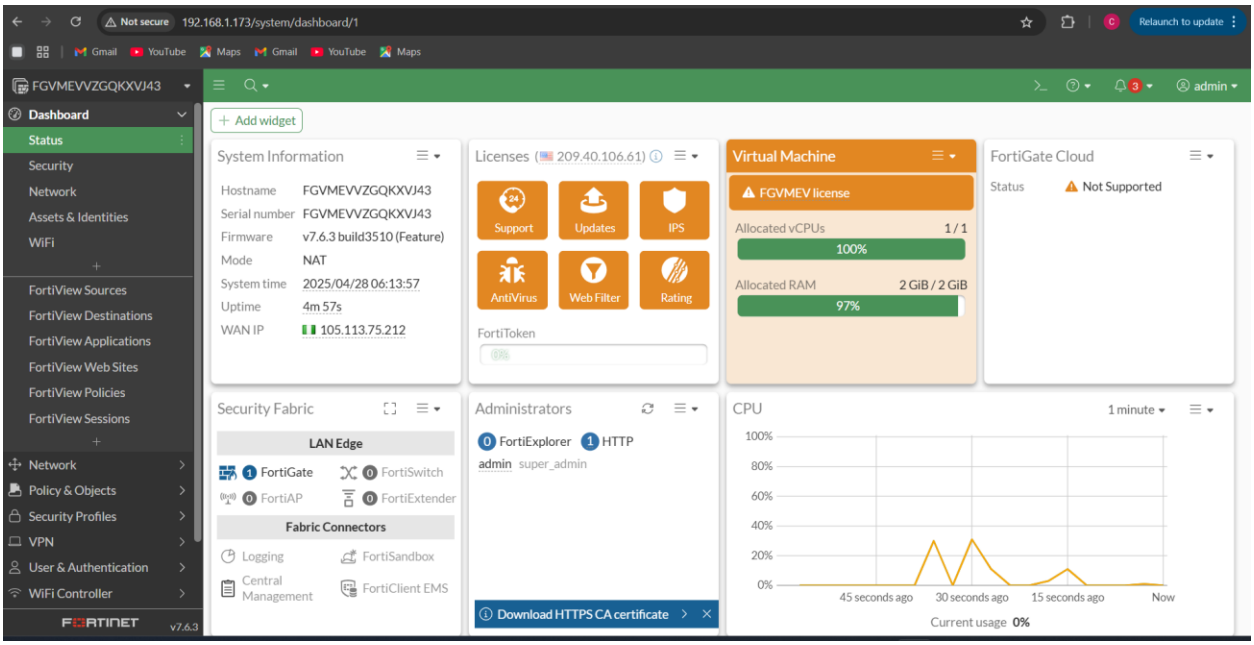
```
makefile
CopyEdit
Username: admin
Password: (blank)
```

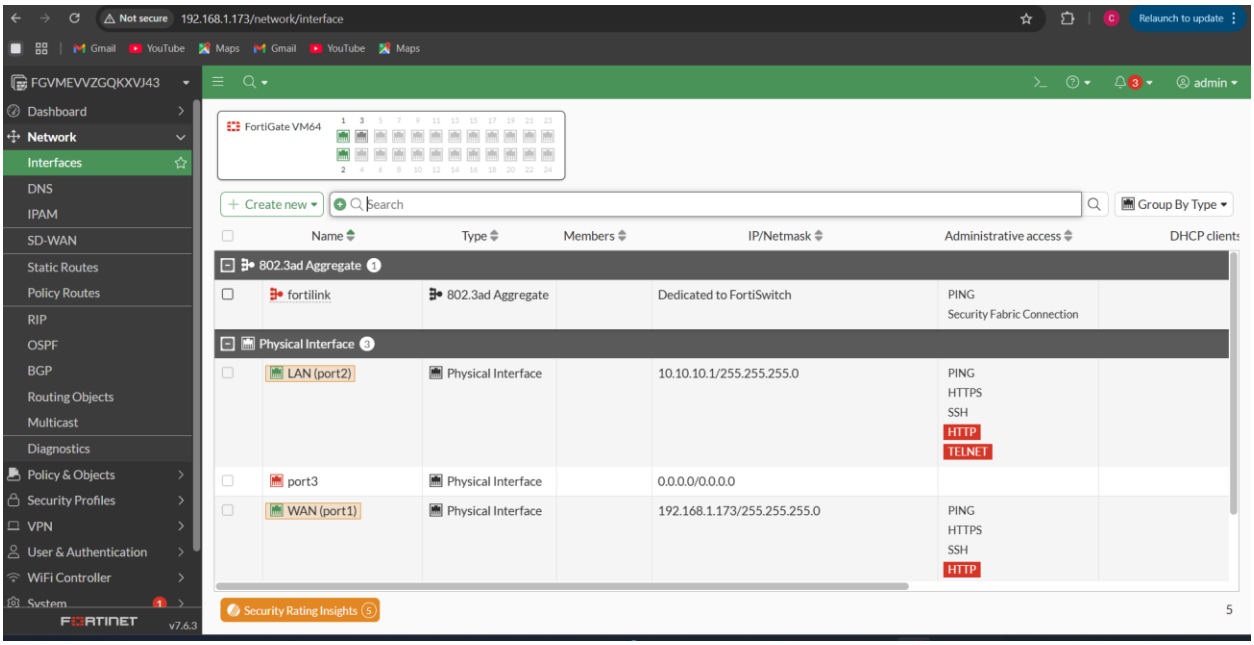
4. **Access GUI:**
    a. Assign a management IP to `port1` interface (LAN).
    b. Access via browser: `https://<ip add..>`

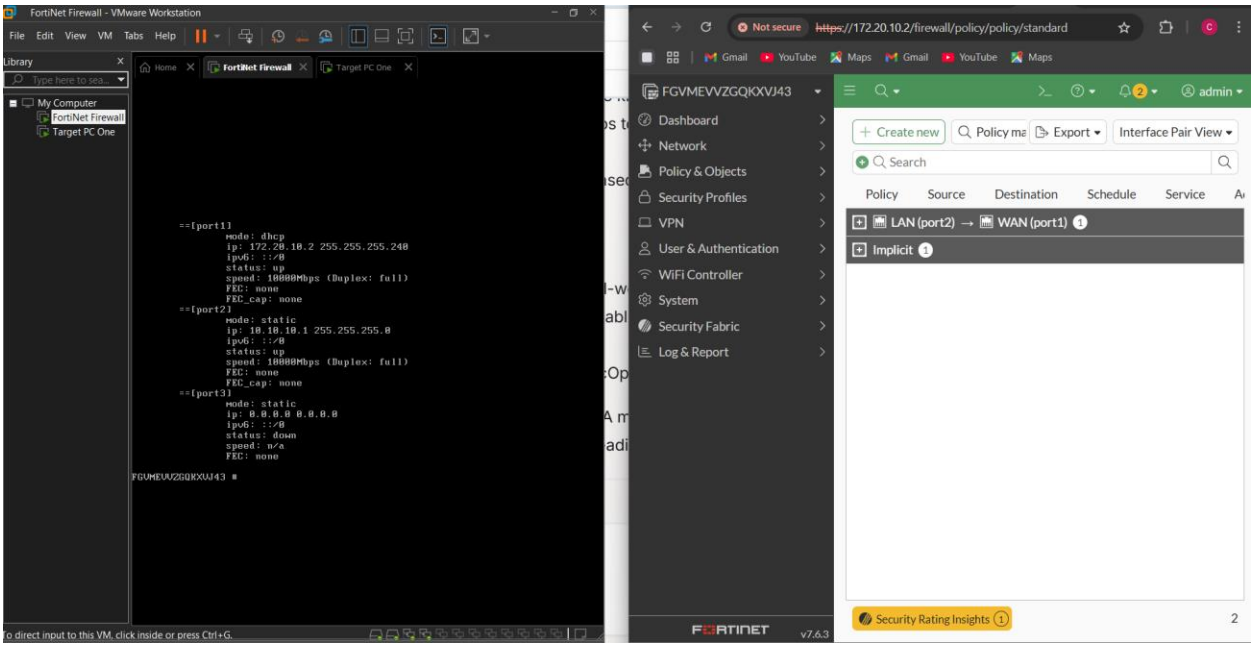
3. Initial Configuration

Tasks:

- Change admin password
- Configure WAN interface (e.g., DHCP/Static)
- Configure LAN interface
- Enable Internet access for LAN
- Configure DNS and NTP
- Add static routes if needed


Not secure
192.168.1.173/system/dashboard/1
Relaunch to update
FGVMEVVZGQKXVJ43
admin
Dashboard
Status
Security
Network
Assets & Identities
WiFi
FortiView Sources
FortiView Destinations
FortiView Applications
FortiView Web Sites
FortiView Policies
FortiView Sessions
Network
Policy & Objects
Security Profiles
VPN
User & Authentication
WiFi Controller
v7.6.3
Add widget
System Information
Hostname FGVMEVVZGQKXVJ43
Serial number FGVMEVVZGQKXVJ43
Firmware v7.6.3 build3510 (Feature)
Mode NAT
System time 2025/04/28 06:13:57
Uptime 4m 57s
WAN IP 105.113.75.212
Licenses (209.40.106.61)
Support
Updates
IPS
AntiVirus
Web Filter
Rating
FortiToken
Virtual Machine
FGVMEV license
Allocated vCPUs 1 / 1
100%
Allocated RAM 2 GiB / 2 GiB
97%
FortiGate Cloud
Status Not Supported
Security Fabric
LAN Edge
1 FortiGate
0 FortiSwitch
0 FortiAP
0 FortiExtender
Fabric Connectors
Logging
FortiSandbox
Central Management
FortiClient EMS
Administrators
0 FortiExplorer
1 HTTP
admin super_admin
Download HTTPS CA certificate
CPU
1 minute
100%
80%
60%
40%
20%
0%
45 seconds ago
30 seconds ago
15 seconds ago
Now
Current usage 0%

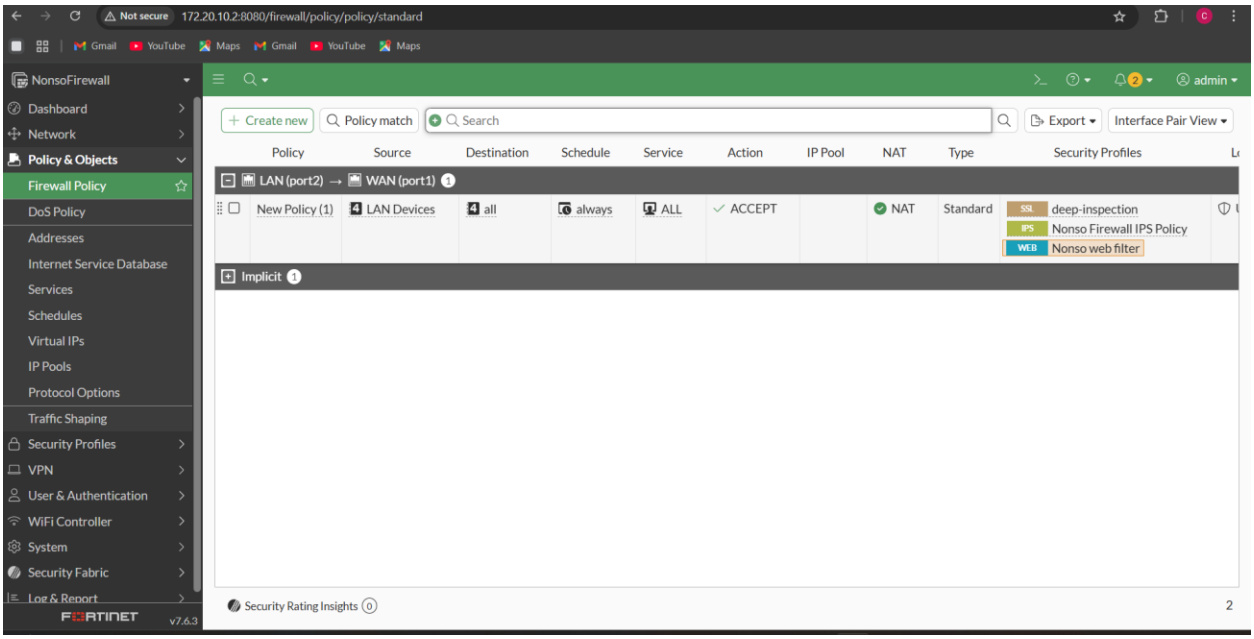

Not secure
192.168.1.173/network/interface
Relaunch to update
FGVMEVVZGQKXVJ43
admin
Dashboard
Network
Interfaces
DNS
IPAM
SD-WAN
Static Routes
Policy Routes
RIP
OSPF
BGP
Routing Objects
Multicast
Diagnostics
Policy & Objects
Security Profiles
VPN
User & Authentication
WiFi Controller
System
v7.6.3
FortiGate VM64
Create new
Search
Group By Type
Name
Type
Members
IP/Netmask
Administrative access
DHCP clients
802.3ad Aggregate 1
fortilink
802.3ad Aggregate
Dedicated to FortiSwitch
PING
Security Fabric Connection
Physical Interface 3
LAN (port2)
Physical Interface
10.10.10.1/255.255.255.0
PING
HTTPS
SSH
HTTP
TELNET
port3
Physical Interface
0.0.0.0/0.0.0.0
WAN (port1)
Physical Interface
192.168.1.173/255.255.255.0
PING
HTTPS
SSH
HTTP
Security Rating Insights 5
5

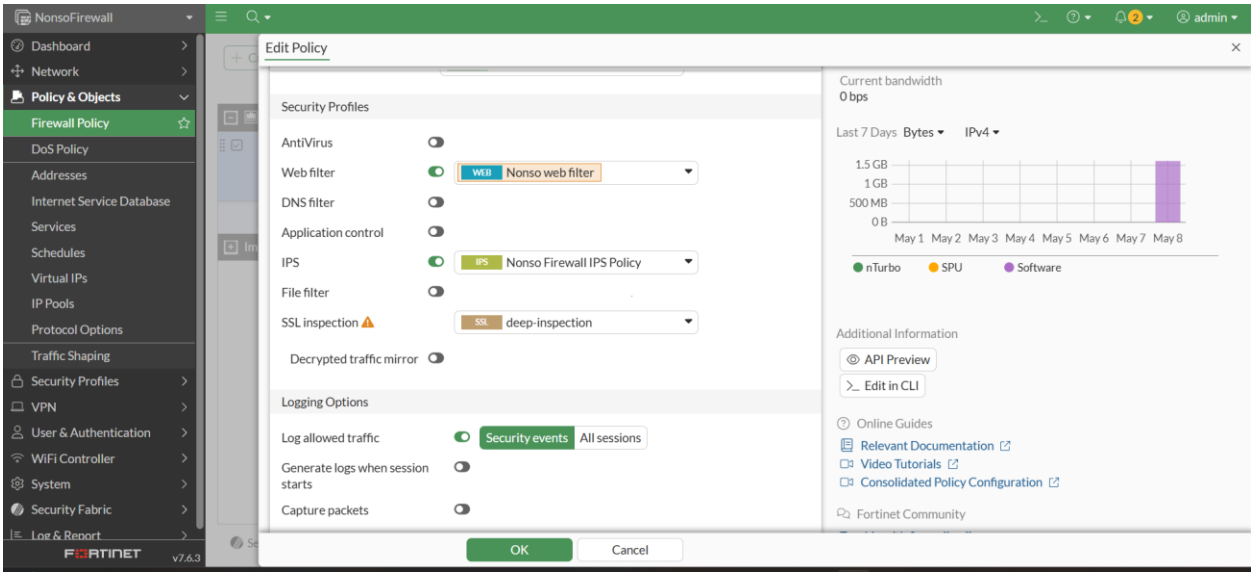


4. Creating Firewall Policies

Lab Tasks:

- Create policy to allow LAN → WAN traffic
- Enable NAT on policy
- Create Deny policies (e.g., block social media)
- Apply Security Profiles:
    - Web Filter (block adult or social content)
    - Antivirus
    - Application Control





5. Testing Firewall Security

Test Cases:

- Connect a test machine on LAN and browse internet
- Try accessing blocked websites
- Generate malware or phishing traffic using Kali Linux
- Run packet capture with Wireshark to analyze firewall behavior

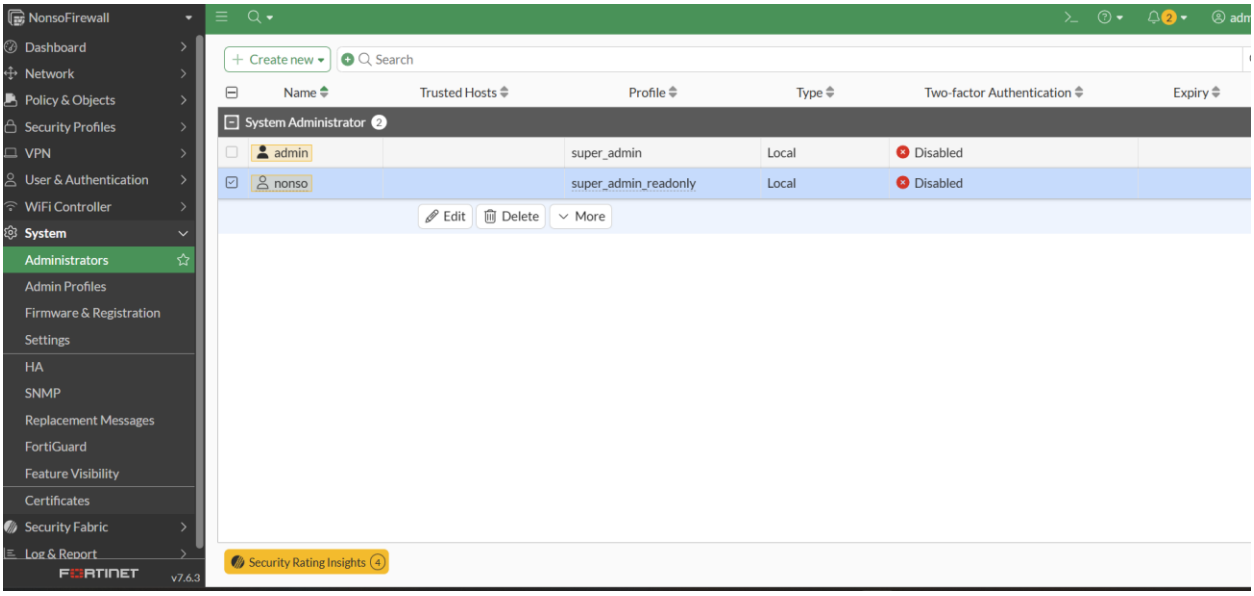
6. Advanced Configurations

Use Cases:

- **VPN Setup:**
  - Configure SSL VPN for remote access
- **IPS (Intrusion Prevention System):**
  - Enable IPS and simulate known attacks
- **Logging & Monitoring:**
  - Enable traffic logs and view in GUI
  - Set up email alerts

7. Firewall Best Practices

- Strong admin passwords
- Disable unused interfaces
- Enable Two-Factor Authentication (2FA)
- Regular firmware updates
- Backups of configuration



8. Challenges and Limitations

- Limited evaluation license
- Performance constraints on low-spec VMs
- Feature restrictions without license

9. Conclusion

- Summary of firewall principles demonstrated - In this project, we explored the core principles of firewall security, including:
  - Traffic control using rules and policies
  - Network segmentation to isolate internal systems
  - Deep packet inspection to analyze data at the application level
  - Stateful inspection to track ongoing sessions and improve accuracy
  - Threat detection and blocking, using tools like web filtering, antivirus, and IPS
  - Logging and monitoring for auditing and forensic analysis

  These principles were applied and tested using the Fortinet FortiGate Firewall in a virtual lab environment.

- Effectiveness of Fortinet FortiGate in securing networks - FortiGate proved to be a robust and versatile security solution. Its features such as:
  - Next-Generation Firewall (NGFW) capabilities
  - Built-in web filtering, antivirus, and application control
  - SSL inspection and IPS (Intrusion Prevention System)
  - User-friendly GUI and detailed logging/reporting
  - …make it effective at preventing unauthorized access, malware infections, and data leaks.
  - Even in a virtualized test setup, FortiGate showed its ability to enforce layered security without significant performance degradation.

- Real-world applicability in home and enterprise networks - **Home Networks:**
  - Protects family members from malicious websites
  - Blocks unwanted or unsafe applications
  - Secures smart home (IoT) devices from external threats

  Enterprise Networks:

- Controls user and device access to critical systems
- Implements granular security policies based on applications and users
- Integrates with Fortinet’s Security Fabric for centralized management
- Supports VPNs, SD-WAN, and high availability for business continuity.