Network Security Fundamentals and FortiGate Integration

R2_DEPI2_ONL2_ISS6_S1_Fortinet Cyber Security Engineer

Spring semester 2024-2025

Beneficiary in Charge:	National Telecommunication Institute (NTI)
Project Group Number:	Group 1
Supervisor:	Dr. Nehal Ahmed &
Project Start:	21 February 2025
Project Duration:	3 months

Report Information:

Document Administrative Information	
Report Full Title:	Network Security Fundamentals and FortiGate Integration
Group Number:	Group 1
Project Supervisor:	Dr. Nehal Ahmed &
Institution:	National Telecommunication Institute (NTI)
Report Version:	v1.0
Submission Date	18/05/2025
Project Duration	Start Date: 24/02/2025 - End Date: 15/05/2025

Team Members:

Team Members Information	
ID:	Name
21077415	ziad waled Ibrahim Hassan
21060209	mazen amr mohamed hassan
3116104706	Nada Ehab Ghorab
21055586	Abdelrahman Ebrahem
3101117779	Ahmed Mohamed Sobhy Khalifa
21071072	Menna Mohamed Sayed

Project Proposal:

1. Executive Summary

This proposal outlines the plan to implement a FortiGate firewall system for enhancing network security. The project addresses the critical need for secure network configurations within academic and professional environments. The main objectives are to configure FortiGate firewalls, implement NAT, and establish firewall policies to minimize vulnerabilities. The project will be completed within four weeks, with a focus on practical implementation and testing. Resources include FortiGate devices, network simulators, and documentation tools. Success will be measured by the proper functioning of security policies and configurations.

2. Background

2.1 History

As cybersecurity threats continue to evolve, the need for efficient firewall configurations is critical. This project, part of the Fortinet Cybersecurity Engineer track, is designed to provide hands-on experience in securing network infrastructures.

2.2 Requirements

The project aims to address common network security challenges, including firewall misconfigurations and inadequate NAT policies. The objective is to mitigate these risks through practical FortiGate deployment and configuration.

2.3 Solution

The solution involves implementing FortiGate firewall settings, NAT configurations, and policy enforcement to ensure a secure network environment. The configuration will include setting up secure access, applying NAT for secure data transfer, and conducting thorough testing.

3. Proposal

3.1 Vision and Goals

Vision: Enhance network security through practical FortiGate configuration and policy management.

Goals:

1. Configure FortiGate firewall from factory settings.
2. Implement NAT and policy configurations.
3. Test and validate the firewall setup.

3.2 Time Frame & Deliverables

Week	Task	Deliverable
One	Research and present on current cybersecurity threats and vulnerabilities, including network attacks and mitigation strategies.	Presentation on Network Security Fundamentals
Two	Configure a basic FortiGate firewall from factory settings and set up initial security policies.	Documented FortiGate configuration with screenshots
Three	Implement and test firewall policies, including NAT configurations for port forwarding and source NAT.	Configuration report and test results
Four	Compile a final report including project findings, configurations, and a presentation summarizing the work done.	Final Report and Presentation

3.4 Resources

Types	Quantity	Notes
FortiGate Devices	1	VM fortinet
Network Simulator	1	VMWare Workstation
Team Members	6	Students from the Cybersecurity track

3.5 Budget

Estimated budget includes device usage, training, and documentation resources. Actual costs to be calculated after project planning.

3.6 Risks & Issues

Risk	Likelihood	Mitigation
Misconfiguration	Low	Pre-configuration testing before implementation
Connectivity Issues	Low	Backup network setup for redundancy.
Data Loss	Medium	Regular backups of configurations and settings.

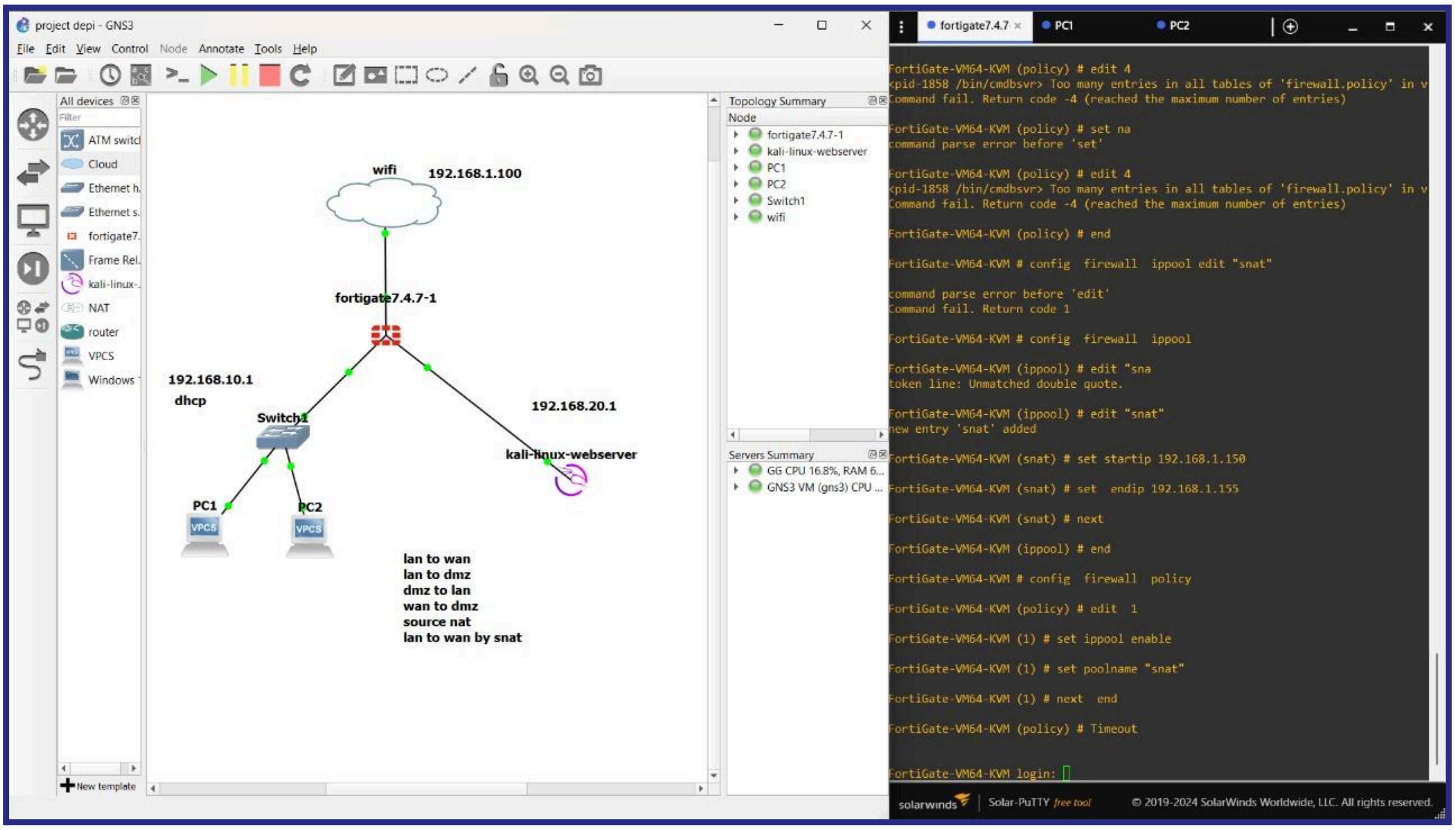
3.7 Success Criteria

1. Correct firewall and NAT configurations
2. Successful network testing and validation
3. Comprehensive final report and presentation

Project Tasks by Week (Weekly Breakdown)

The network topology in Figure 1 is designed to secure and segment the network using the FortiGate firewall as the central gateway. The WAN interface connects to the internet, the LAN interface connects internal devices, and the DMZ hosts public-facing services isolated from the LAN.

This setup allows controlled traffic flow between networks, protecting internal resources while enabling secure external access to specific services through NAT and firewall policies. The topology supports effective implementation of security rules and traffic management, forming the foundation for all project tasks from basic configuration to policy enforcement and testing.



```
FortiGate-VM64-KVM (policy) # edit 4
<pid-1858 /bin/cmdbsvr> Too many entries in all tables of 'firewall.policy' in v
Command fail. Return code -4 (reached the maximum number of entries)

FortiGate-VM64-KVM (policy) # set na
command parse error before 'set'

FortiGate-VM64-KVM (policy) # edit 4
<pid-1858 /bin/cmdbsvr> Too many entries in all tables of 'firewall.policy' in v
Command fail. Return code -4 (reached the maximum number of entries)

FortiGate-VM64-KVM (policy) # end

FortiGate-VM64-KVM # config  firewall  ippool edit "snat"

command parse error before 'edit'
Command fail. Return code 1

FortiGate-VM64-KVM # config  firewall  ippool

FortiGate-VM64-KVM (ippool) # edit "sna
token line: Unmatched double quote.

FortiGate-VM64-KVM (ippool) # edit "snat"
new entry 'snat' added

FortiGate-VM64-KVM (snat) # set startip 192.168.1.150

FortiGate-VM64-KVM (snat) # set  endip 192.168.1.155

FortiGate-VM64-KVM (snat) # next

FortiGate-VM64-KVM (ippool) # end

FortiGate-VM64-KVM # config  firewall  policy

FortiGate-VM64-KVM (policy) # edit  1

FortiGate-VM64-KVM (1) # set ippool enable

FortiGate-VM64-KVM (1) # set poolname "snat"

FortiGate-VM64-KVM (1) # next  end

FortiGate-VM64-KVM (policy) # Timeout


FortiGate-VM64-KVM login: 
```

Week 1 - Exploring Cybersecurity Threats

Task Overview:

During Week 1, we conducted comprehensive research on prevalent cybersecurity threats and their impact on network security, while also identifying key network vulnerabilities and corresponding mitigation strategies. The research focused on common attack types, including phishing, ransomware, DDoS, MITM, zero-day exploits, and SQL injection. Additionally, we examined critical network vulnerabilities, such as weak passwords, unpatched systems, misconfigured firewalls, and insufficient encryption, and proposed effective measures to mitigate these risks.

Challenges:

Understanding Complex Threats: Certain threats, such as zero-day exploits, were difficult to address in the research phase because they exploit vulnerabilities that are not yet publicly known. This required a deeper understanding of how FortiGate's features, like threat intelligence, can proactively mitigate such vulnerabilities.

Researching Advanced Firewall Configurations: While specific configurations weren't made this week, understanding the configurations required to mitigate threats like phishing, DDoS, and ransomware on FortiGate firewalls was complex. It was crucial to explore how FortiGate's features, such as intrusion prevention systems (IPS) and web filtering, could be employed effectively.

Balancing Performance vs. Security: Another challenge was understanding how to achieve a balance between strong security and optimal network performance, especially when configuring detailed firewall rules to protect against threats without causing performance degradation.

Outcomes:

Week 1 focused on researching key cybersecurity threats and vulnerabilities, with a particular emphasis on how FortiGate can help mitigate these issues. Based on the research, the following outcomes were identified:

1- Threat Identification:
We identified six key cybersecurity threats: Phishing, Ransomware, DDoS Attacks, MITM Attacks, Zero-Day Exploits, and SQL Injection. Understanding these threats allowed us to recognize the critical areas where protection is necessary.

2- Vulnerability Assessment:
Network vulnerabilities such as weak passwords, unpatched software, misconfigured firewalls, lack of network segmentation, and insufficient encryption were identified as common entry points for cyberattacks.

3- Mitigation Strategy Framework:
We outlined several effective strategies to mitigate risks, including implementing Multi-Factor Authentication (MFA), regular software updates, and deploying Next-Generation Firewalls (NGFWs) and Intrusion Detection Systems (IDS/IPS). These strategies will guide the upcoming configuration of FortiGate for protecting the network.

4- Firewall Configuration Insights:
The research reinforced the importance of firewalls, especially Next-Generation Firewalls (NGFWs), in defending against modern cyber threats. FortiGate's capabilities, including intrusion prevention, deep packet inspection, and threat intelligence, were identified as essential for comprehensive network security.

5- Best Practices and Policies:
We emphasized the importance of regular firewall updates, a layered security approach, real-time monitoring, and strict access control. Network security policies, such as access control, incident response, and data protection, were also recognized as vital for strengthening defenses.

6- Incident Response Strategy:
A clear incident response plan was outlined, including steps for identifying, containing, eradicating, recovering, and reviewing incidents. This will ensure timely responses to any security breaches.

Week 2: FortiGate Basic Configuration

Task Overview:

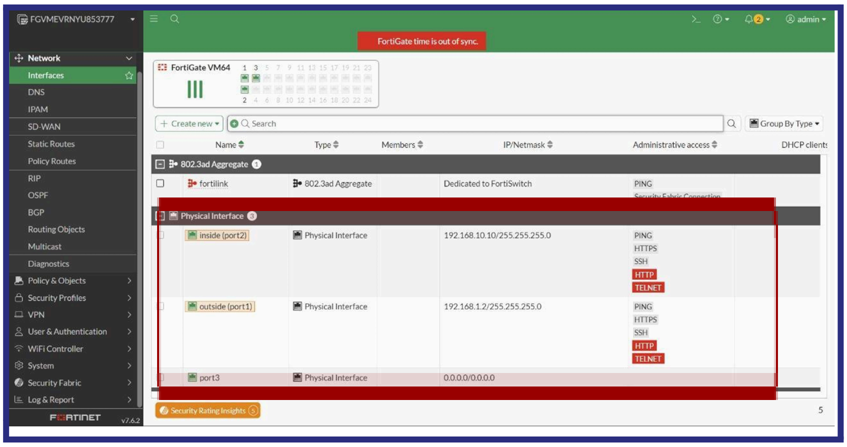
Changing the Default Password:

The factory password was changed to a strong, complex password to prevent unauthorized access.

Configuring FortiGate Ports:

LAN Port Configuration: Set up the LAN port to connect the internal network to the FortiGate firewall.

WAN Port Configuration: Configured the WAN port to enable external internet access for the network.



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					
inside (port2)	Physical Interface		192.168.10.10/255.255.255.0	PING HTTPS SSH HTTP TELNET	
outside (port1)	Physical Interface		192.168.1.2/255.255.255.0	PING HTTPS SSH HTTP TELNET	
port3	Physical Interface		0.0.0.0/0.0.0.0		

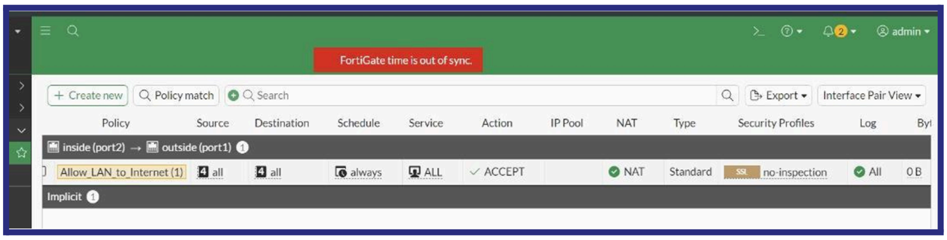
5

“Figure 1.”

"As shown in Figure 1, Configuring LAN and WAN Interfaces: Setting up static IP addresses and enabling secure access protocols on FortiGate for efficient network communication."

Creating Group Policies:

Created a policy to allow the LAN network to securely connect to external networks, ensuring proper traffic management.



Policy	Source	Destination	Schedule	Service	Action	IP Pool	NAT	Type	Security Profiles	Log	Byt
inside (port2) → outside (port1) 1											
Allow_LAN_to_Internet (1)	all	all	always	ALL	✓ ACCEPT		✓ NAT	Standard	SSL no-inspection	✓ All	0 B
Implicit 1											

“Figure 2.”

“As shown in Figure 2, Create a group policy to allow Lan network connect to outside”

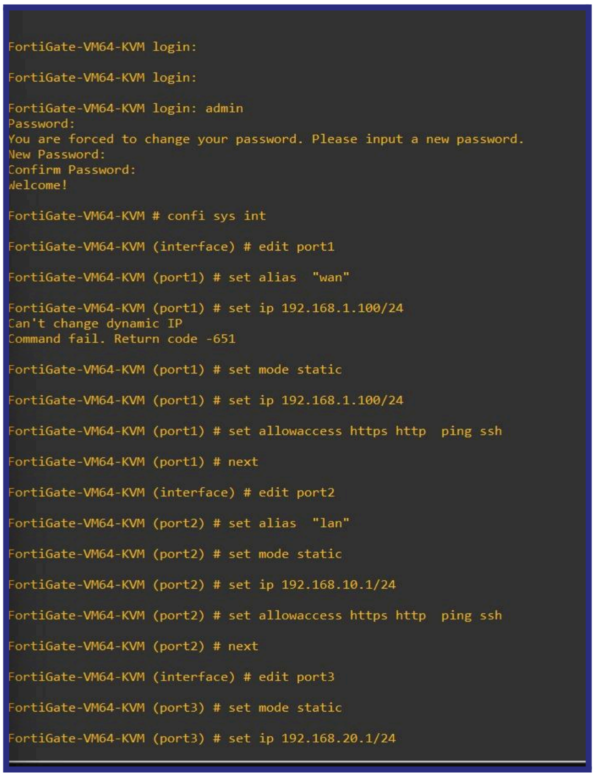
Challenges Encountered:

- **Licensing Issues:** Encountered challenges with licensing setup during the configuration process.
- **VM Setup Issues:** Faced minor problems while setting up FortiGate in VMware, related to compatibility or resource allocation.

Outcomes:

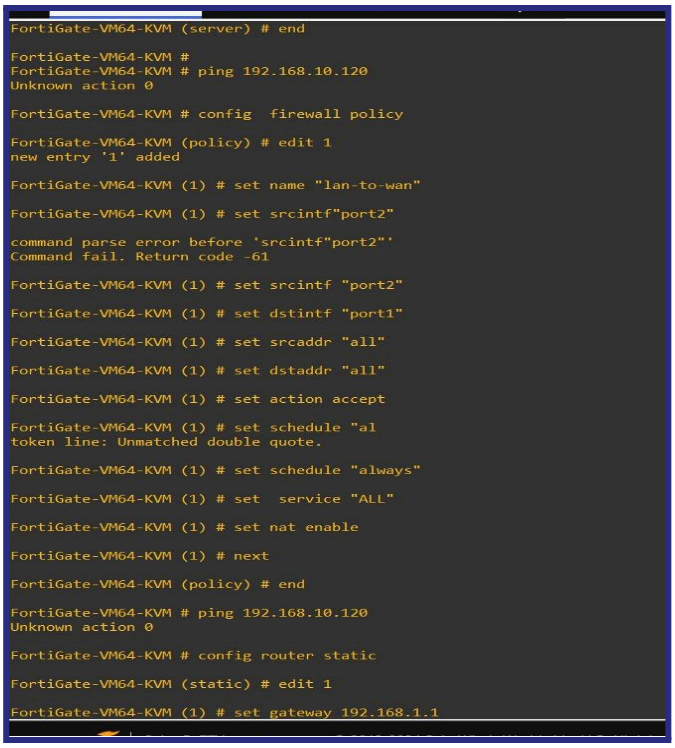
- **Security Enhancement:** The firewall is now secured with a strong, customized password.
- **Network Connectivity Established:** Both the LAN and WAN ports are configured to enable seamless data flow between the internal and external networks.
- **Policy Enforcement:** The LAN network can now securely access external networks through the configured group policy.

“Figure 3, Shows the initial setup of FortiGate, including login, password change, and interface configuration (WAN, LAN, and DMZ).”



```
FortiGate-VM64-KVM login:

FortiGate-VM64-KVM login:

FortiGate-VM64-KVM login: admin
Password:
You are forced to change your password. Please input a new password.
New Password:
Confirm Password:
Welcome!

FortiGate-VM64-KVM # confi sys int

FortiGate-VM64-KVM (interface) # edit port1

FortiGate-VM64-KVM (port1) # set alias  "wan"

FortiGate-VM64-KVM (port1) # set ip 192.168.1.100/24
Can't change dynamic IP
Command fail. Return code -651

FortiGate-VM64-KVM (port1) # set mode static

FortiGate-VM64-KVM (port1) # set ip 192.168.1.100/24

FortiGate-VM64-KVM (port1) # set allowaccess https http  ping ssh

FortiGate-VM64-KVM (port1) # next

FortiGate-VM64-KVM (interface) # edit port2

FortiGate-VM64-KVM (port2) # set alias  "lan"

FortiGate-VM64-KVM (port2) # set mode static

FortiGate-VM64-KVM (port2) # set ip 192.168.10.1/24

FortiGate-VM64-KVM (port2) # set allowaccess https http  ping ssh

FortiGate-VM64-KVM (port2) # next

FortiGate-VM64-KVM (interface) # edit port3

FortiGate-VM64-KVM (port3) # set mode static

FortiGate-VM64-KVM (port3) # set ip 192.168.20.1/24
```

“Figure 3.”



```
FortiGate-VM64-KVM (server) # end

FortiGate-VM64-KVM #
FortiGate-VM64-KVM # ping 192.168.10.120
Unknown action 0

FortiGate-VM64-KVM # config  firewall policy

FortiGate-VM64-KVM (policy) # edit 1
new entry '1' added

FortiGate-VM64-KVM (1) # set name "lan-to-wan"

FortiGate-VM64-KVM (1) # set srcintf"port2"

command parse error before 'srcintf"port2"'
Command fail. Return code -61

FortiGate-VM64-KVM (1) # set srcintf "port2"

FortiGate-VM64-KVM (1) # set dstintf "port1"

FortiGate-VM64-KVM (1) # set srcaddr "all"

FortiGate-VM64-KVM (1) # set dstaddr "all"

FortiGate-VM64-KVM (1) # set action accept

FortiGate-VM64-KVM (1) # set schedule "al
token line: Unmatched double quote.

FortiGate-VM64-KVM (1) # set schedule "always"

FortiGate-VM64-KVM (1) # set  service "ALL"

FortiGate-VM64-KVM (1) # set nat enable

FortiGate-VM64-KVM (1) # next

FortiGate-VM64-KVM (policy) # end

FortiGate-VM64-KVM # ping 192.168.10.120
Unknown action 0

FortiGate-VM64-KVM # config router static

FortiGate-VM64-KVM (static) # edit 1

FortiGate-VM64-KVM (1) # set gateway 192.168.1.1
```

“Figure 4”

“static routing and DHCP server configuration”

Week 3: FortiGate Policies and NAT:

Task Overview:

Configuring Firewall Policies:

1- Implemented firewall policies to control incoming and outgoing traffic, ensuring secure data flow between internal and external networks.

2- Applied access control measures to filter traffic based on IP addresses, ports, and protocols.

3- Verified the effectiveness of policies by testing different traffic scenarios.

NAT Configuration:

1- Port Forwarding: Configured NAT rules to redirect specific external ports to designated internal servers, allowing secure remote access.

2- Source NAT: Implemented source NAT to enable internal devices to access external networks through a single public IP address.

Testing and Verification:

Conducted tests to verify that configured policies and NAT settings were functioning as expected.

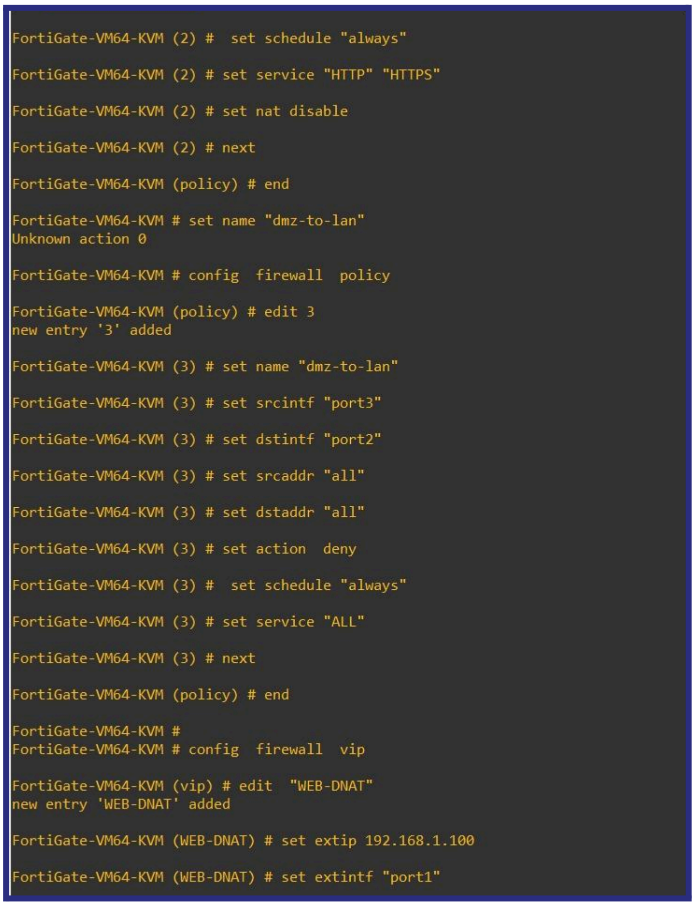
Monitored FortiGate logs to assess traffic patterns and detect any potential issues.

Challenges Encountered:

- Policy Conflicts: Faced challenges while implementing multiple policies with overlapping criteria, resolved by prioritizing rules.
- NAT Loopback: Encountered issues when accessing internal servers using external IP addresses, addressed through proper loopback configuration.

Outcomes:

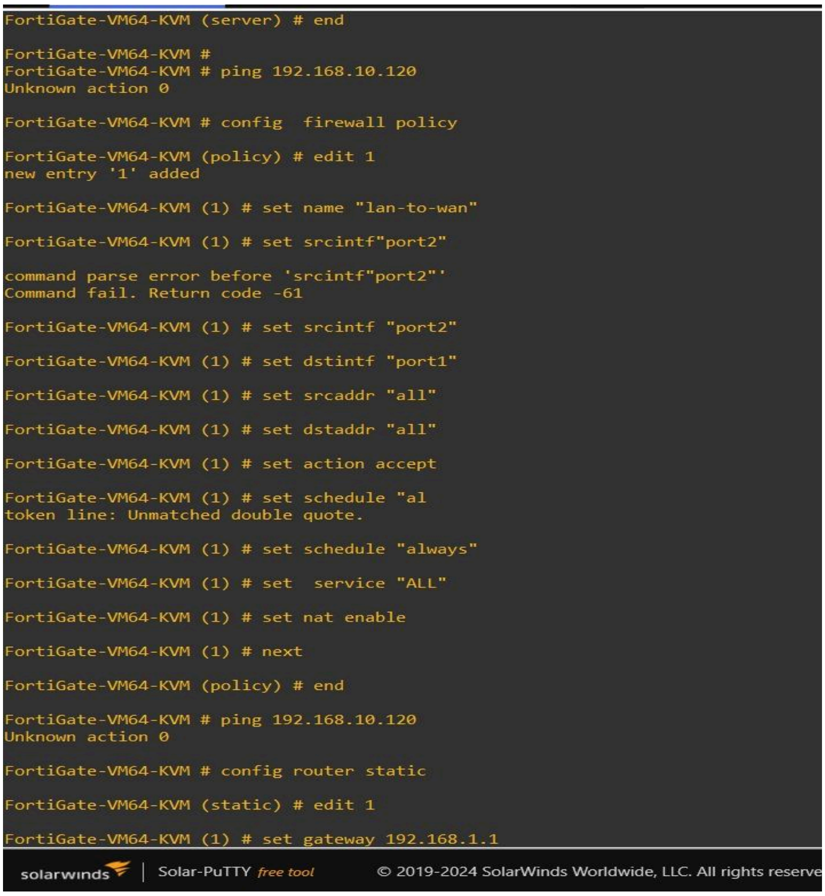
- Enhanced Security: Firewall policies effectively filtered unwanted traffic and secured internal networks.
- Successful NAT Implementation: Port forwarding and source NAT configurations enabled secure external access and smooth internal-external communication.
- Efficient Traffic Management: Optimized network performance through well-structured policies and NAT rules.



```
FortiGate-VM64-KVM (2) #  set schedule "always"

FortiGate-VM64-KVM (2) # set service "HTTP" "HTTPS"

FortiGate-VM64-KVM (2) # set nat disable

FortiGate-VM64-KVM (2) # next

FortiGate-VM64-KVM (policy) # end

FortiGate-VM64-KVM # set name "dmz-to-lan"
Unknown action 0

FortiGate-VM64-KVM # config  firewall  policy

FortiGate-VM64-KVM (policy) # edit 3
new entry '3' added

FortiGate-VM64-KVM (3) # set name "dmz-to-lan"

FortiGate-VM64-KVM (3) # set srcintf "port3"

FortiGate-VM64-KVM (3) # set dstintf "port2"

FortiGate-VM64-KVM (3) # set srcaddr "all"

FortiGate-VM64-KVM (3) # set dstaddr "all"

FortiGate-VM64-KVM (3) # set action  deny

FortiGate-VM64-KVM (3) #  set schedule "always"

FortiGate-VM64-KVM (3) # set service "ALL"

FortiGate-VM64-KVM (3) # next

FortiGate-VM64-KVM (policy) # end

FortiGate-VM64-KVM #
FortiGate-VM64-KVM # config  firewall  vip

FortiGate-VM64-KVM (vip) # edit  "WEB-DNAT"
new entry 'WEB-DNAT' added

FortiGate-VM64-KVM (WEB-DNAT) # set extip 192.168.1.100

FortiGate-VM64-KVM (WEB-DNAT) # set extintf "port1"
```

“Figure 5”

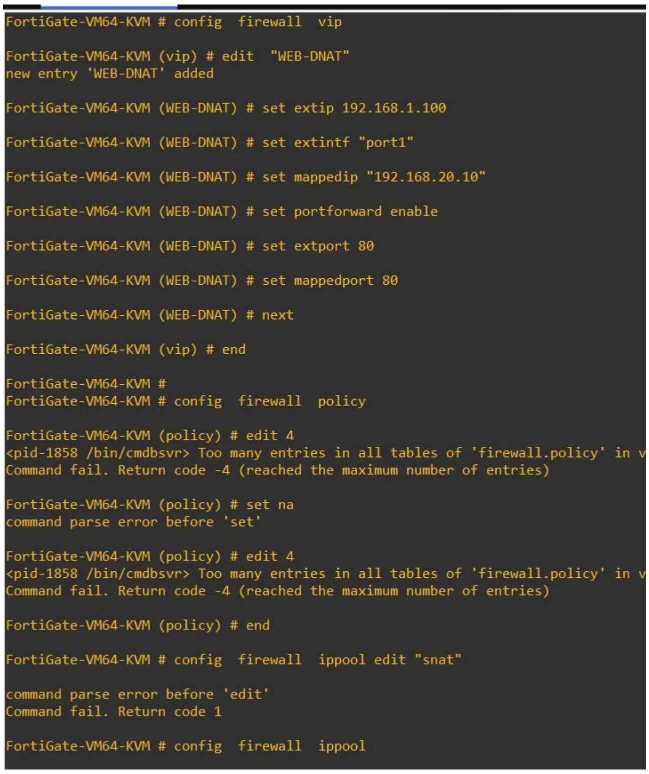
"Implementing Firewall Policies: Configuring a policy to deny traffic from the DMZ to the LAN for enhanced internal security."



```
FortiGate-VM64-KVM (server) # end

FortiGate-VM64-KVM #
FortiGate-VM64-KVM # ping 192.168.10.120
Unknown action 0

FortiGate-VM64-KVM # config  firewall policy

FortiGate-VM64-KVM (policy) # edit 1
new entry '1' added

FortiGate-VM64-KVM (1) # set name "lan-to-wan"

FortiGate-VM64-KVM (1) # set srcintf"port2"

command parse error before 'srcintf"port2"'
Command fail. Return code -61

FortiGate-VM64-KVM (1) # set srcintf "port2"

FortiGate-VM64-KVM (1) # set dstintf "port1"

FortiGate-VM64-KVM (1) # set srcaddr "all"

FortiGate-VM64-KVM (1) # set dstaddr "all"

FortiGate-VM64-KVM (1) # set action accept

FortiGate-VM64-KVM (1) # set schedule "al
token line: Unmatched double quote.

FortiGate-VM64-KVM (1) # set schedule "always"

FortiGate-VM64-KVM (1) # set  service "ALL"

FortiGate-VM64-KVM (1) # set nat enable

FortiGate-VM64-KVM (1) # next

FortiGate-VM64-KVM (policy) # end

FortiGate-VM64-KVM # ping 192.168.10.120
Unknown action 0

FortiGate-VM64-KVM # config router static

FortiGate-VM64-KVM (static) # edit 1

FortiGate-VM64-KVM (1) # set gateway 192.168.1.1
```

“Figure 6”

"Configuring LAN-to-WAN Policy: Allowing secure outbound traffic from the internal LAN to external networks while enabling NAT for address translation."



```
FortiGate-VM64-KVM # config  firewall  vip

FortiGate-VM64-KVM (vip) # edit  "WEB-DNAT"
new entry 'WEB-DNAT' added

FortiGate-VM64-KVM (WEB-DNAT) # set extip 192.168.1.100

FortiGate-VM64-KVM (WEB-DNAT) # set extintf "port1"

FortiGate-VM64-KVM (WEB-DNAT) # set mappedip "192.168.20.10"

FortiGate-VM64-KVM (WEB-DNAT) # set portforward enable

FortiGate-VM64-KVM (WEB-DNAT) # set extport 80

FortiGate-VM64-KVM (WEB-DNAT) # set mappedport 80

FortiGate-VM64-KVM (WEB-DNAT) # next

FortiGate-VM64-KVM (vip) # end

FortiGate-VM64-KVM #
FortiGate-VM64-KVM # config  firewall  policy

FortiGate-VM64-KVM (policy) # edit 4
<pid-1858 /bin/cmdbsvr> Too many entries in all tables of 'firewall.policy' in v
Command fail. Return code -4 (reached the maximum number of entries)

FortiGate-VM64-KVM (policy) # set na
command parse error before 'set'

FortiGate-VM64-KVM (policy) # edit 4
<pid-1858 /bin/cmdbsvr> Too many entries in all tables of 'firewall.policy' in v
Command fail. Return code -4 (reached the maximum number of entries)

FortiGate-VM64-KVM (policy) # end

FortiGate-VM64-KVM # config  firewall  ippool edit "snat"

command parse error before 'edit'
Command fail. Return code 1

FortiGate-VM64-KVM # config  firewall  ippool
```

Port Forwarding Configuration: Mapping external port 80 to internal HTTP server to facilitate remote access."

Week 4: Presentation and Final Report

Task Overview:

- Compile a comprehensive final report that consolidates all project findings, detailed FortiGate configurations, testing results, and analysis.
- Prepare a professional presentation summarizing the entire project workflow, key outcomes, challenges encountered, and lessons learned.
- Ensure that all documentation is clear, well-organized, and includes relevant visuals such as screenshots and diagrams to support understanding.

Deliverable:

- Final Report encompassing the research, configurations, NAT setup, firewall policies, testing, and overall project insights.
- Project Presentation designed to effectively communicate the scope, methodology, and results to stakeholders.

Conclusion

This project successfully explored the fundamentals of network security and the practical integration of FortiGate firewall solutions. Over the course of four weeks, we conducted thorough research on prevalent cybersecurity threats and vulnerabilities, implemented secure FortiGate configurations, and developed effective firewall policies including NAT setups for port forwarding and source NAT.

The configuration and testing phases demonstrated the capability of FortiGate to enforce robust security measures while maintaining seamless network connectivity. Challenges such as policy conflicts and NAT loopback issues were identified and resolved, enhancing our understanding of firewall management complexities.

Overall, this project provided valuable hands-on experience with industry-standard security tools, reinforcing best practices in network protection. The final report and presentation summarize the findings and technical implementations, offering a comprehensive overview that supports future security initiatives.