



# Network Security Fundamentals and FortiGate Integration

## Team Members:

1. Ziad Mohamed Ibraheem Saad
2. Ahmed Mohamed Abdelnaser
3. Nada Amna
4. Rawan Ashraf
5. Nour Khaled Kholief



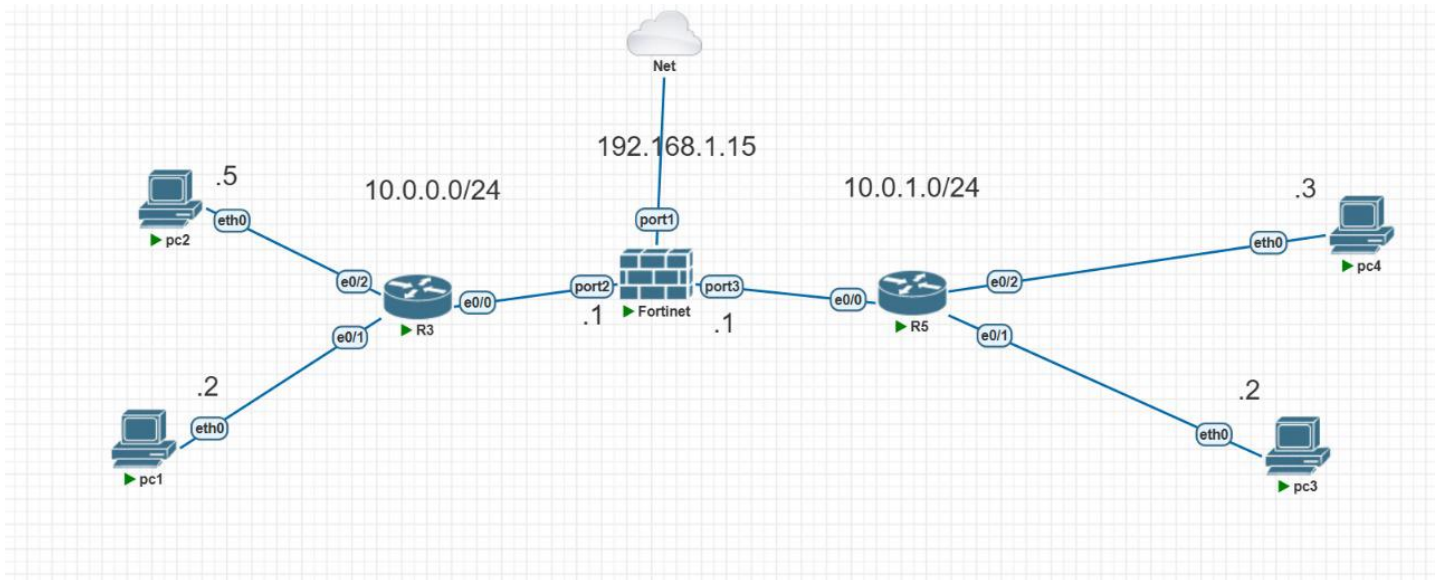
## 1. Introduction

This document presents a structured, professional report of the FortiGate network security project. It covers network topology, configuration steps, security controls, NAT, routing, firewall policies, and verification tests. The goal is to demonstrate secure segmentation, controlled access, and proper network design practices.

## 2. Project Objectives

- Build a secure network topology consisting of two LANs and an Internet uplink.
- Configure FortiGate interfaces, DHCP services, admin profiles, and routing.
- Enforce access control between LANs.
- Implement Source NAT (SNAT) for outbound Internet access.
- Implement Destination NAT (DNAT) to publish an internal server externally.
- Validate the network through connectivity and security tests.

### 3. Network Topology:



### Components:

- 2 LANs each LAN containing 2 PCs
  - LAN 1: Subnet 10.0.0.0/24 (two PCs connected to Switch 1)
  - LAN 2: Subnet 10.0.1.0/24 (two PCs connected to Switch 2)
- 2 Switches
- Fortigate Firewall
- Cloud as Internet

## 4. Fortigate firewall Configuration:

Initial access was performed over CLI. Port1 was configured to obtain an IP via DHCP to enable GUI access. Once inside the GUI, a new admin profile named 'Trainee' was created with limited privileges, and a corresponding administrator account was assigned to follow the principle of least privilege.

```
FortiGate-VM64-KVM # show system interface port1
config system interface
    edit "port1"
        set vdom "root"
        set mode dhcp
        set allowaccess ping https ssh http
        set type physical
        set snmp-index 1
    next
end
```

To access the GUI, we first entered the CLI and edited port1 settings to enable DHCP mode, allowing it to obtain an IP address automatically from our network.

We now Can access Fortigate firewall GUI using this IP address.

```
board]
==[port1]
    mode: dhcp
    ip: 192.168.137.129 255.255.255.0
    ipv6: ::/0
    status: up
    speed: 10000Mbps (Duplex: full)
```

## Setting Up New Admin Profile and giving Less privileges “Trainee”:

Edit Admin Profile

Name

trainee

Comments

0/255

Access Permissions

Access Control	Permissions	Set All
Security Fabric	<input type="radio"/> None <input checked="" type="radio"/> Read <input type="radio"/> Read/Write	
FortiView	<input type="radio"/> None <input checked="" type="radio"/> Read <input type="radio"/> Read/Write	
User & Device	<input type="radio"/> None <input checked="" type="radio"/> Read <input type="radio"/> Read/Write	
Firewall	<input type="radio"/> None <input checked="" type="radio"/> Read <input type="radio"/> Read/Write <input type="radio"/> Custom	
Log & Report	<input type="radio"/> None <input checked="" type="radio"/> Read <input type="radio"/> Read/Write <input type="radio"/> Custom	
Network	<input type="radio"/> None <input checked="" type="radio"/> Read <input type="radio"/> Read/Write <input type="radio"/> Custom	
System	<input type="radio"/> None <input checked="" type="radio"/> Read <input type="radio"/> Read/Write <input type="radio"/> Custom	
Security Profile	<input type="radio"/> None <input type="radio"/> Read <input checked="" type="radio"/> Read/Write <input type="radio"/> Custom	
VPN	<input type="radio"/> None <input checked="" type="radio"/> Read <input type="radio"/> Read/Write	

OK

Cancel



Creating administrator and giving it the Trainee admin profile.

FortiGate-VM64-KVM

- Dashboard
- Network
- Policy & Objects
- Security Profiles
- VPN
- User & Authentication
- System** (1)
- Administrators** (☆)
- Admin Profiles
- Firmware
- Fabric Management
- Settings
- HA
- SNMP
- Replacement Messages
- FortiGuard (1)
- Feature Visibility

### New Administrator

Username:

Type: **Local User**  
Match a user on a remote server group  
Match all users in a remote server group  
Use public key infrastructure (PKI) group

Password:

Confirm Password:

Comments:  0/255

Administrator profile:

☐ Two-factor Authentication

☐ Restrict login to trusted hosts

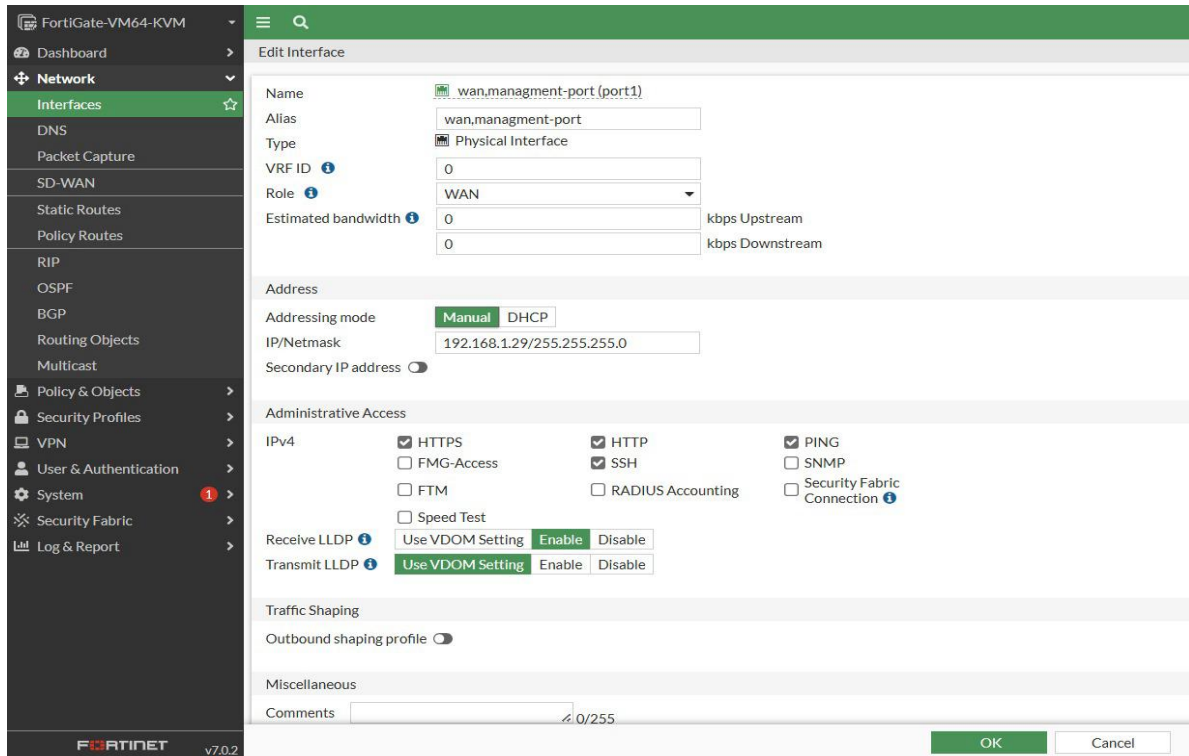
☐ Restrict admin to guest account provisioning only

**OK** Cancel

## 5.Interfaces Configurations:

The following FortiGate interface settings were applied:

- Port1 (WAN + Management): Assigned a static IP for consistent GUI access and Internet reachability.
  - Port2 (LAN 1): Configured as a DHCP server for subnet 10.0.0.0/24.
  - Port3 (LAN 2): Configured as a DHCP server for subnet 10.0.1.0/24.
- Each LAN interface successfully leased IP addresses to connected hosts.



The screenshot displays the FortiGate VM64-KVM web interface. The left sidebar shows the 'Network' menu with 'Interfaces' selected. The main panel is titled 'Edit Interface' and shows the configuration for 'wan,managment-port (port1)'. The configuration includes:

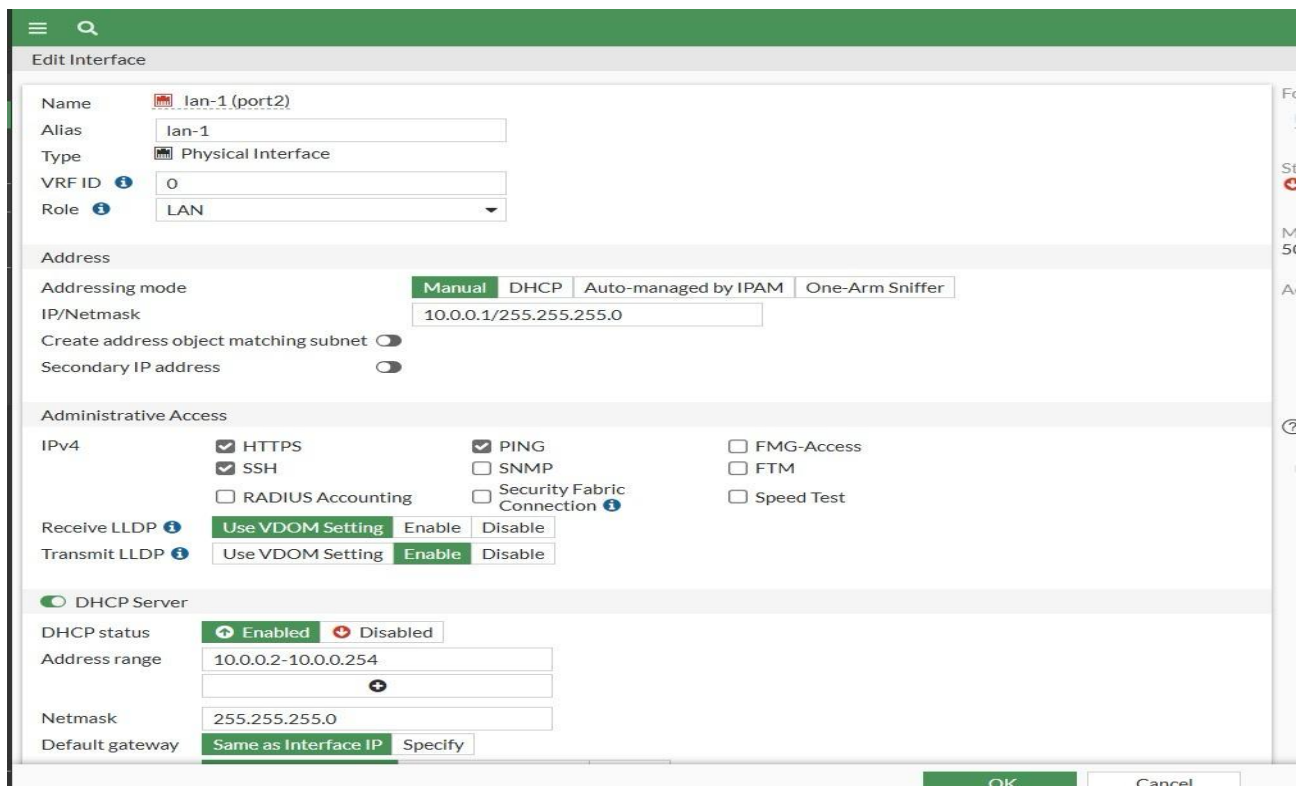
- Name:** wan,managment-port (port1)
- Alias:** wan,managment-port
- Type:** Physical Interface
- VRF ID:** 0
- Role:** WAN
- Estimated bandwidth:** 0 kbps Upstream, 0 kbps Downstream
- Addressing mode:** Manual (selected), DHCP
- IP/Netmask:** 192.168.1.29/255.255.255.0
- Secondary IP address:** Disabled
- Administrative Access:**
  - IPv4: ☒ HTTPS, ☐ FMG-Access, ☐ FTM, ☐ Speed Test
  - ☒ HTTP, ☒ SSH, ☐ RADIUS Accounting
  - ☒ PING, ☐ SNMP, ☐ Security Fabric Connection
- Receive LLDP:** Use VDOM Setting, Enable (selected), Disable
- Transmit LLDP:** Use VDOM Setting, Enable (selected), Disable
- Traffic Shaping:** Outbound shaping profile: Disabled
- Miscellaneous:** Comments: 0/255

At the bottom, there are 'OK' and 'Cancel' buttons.

Setting Up Port 1 As Wan and Management Port and Giving it Static IP Address to access Management port with the Same IP Every time and accessing Internet.

## Interfaces Ports 2&3 Configurations

Port 2 Connected to LAN 1 and Act as DHCP server in the range 10.0.0.0/24



The screenshot shows the 'Edit Interface' configuration window for 'lan-1 (port2)'. The window is divided into several sections:

- Name:** lan-1 (port2)
- Alias:** lan-1
- Type:** Physical Interface
- VRF ID:** 0
- Role:** LAN
- Addressing mode:** Manual (selected), DHCP, Auto-managed by IPAM, One-Arm Sniffer
- IP/Netmask:** 10.0.0.1/255.255.255.0
- Create address object matching subnet:** ☐
- Secondary IP address:** ☐
- Administrative Access:**
  - IPv4:
    - ☒ HTTPS
    - ☒ SSH
    - ☐ RADIUS Accounting
    - ☒ PING
    - ☐ SNMP
    - ☐ Security Fabric Connection
    - ☐ FMG-Access
    - ☐ FTM
    - ☐ Speed Test
  - Receive LLDP: Use VDOM Setting, Enable, Disable
  - Transmit LLDP: Use VDOM Setting, Enable, Disable
- DHCP Server:**
  - ☒ DHCP Server
  - DHCP status: Enabled (selected), Disabled
  - Address range: 10.0.0.2-10.0.0.254
  - Netmask: 255.255.255.0
  - Default gateway: Same as Interface IP (selected), Specify

At the bottom right, there are 'OK' and 'Cancel' buttons.

## Port 3 Connected to LAN 2 and Act as DHCP server in the range 10.0.1.0/24

FortiGate-VM64-KVM
Dashboard
Network
Interfaces
DNS
Packet Capture
SD-WAN
Static Routes
Policy Routes
RIP
OSPF
BGP
Routing Objects
Multicast
Policy & Objects
Security Profiles
VPN
User & Authentication
System
Security Fabric
Log & Report

### Edit Interface

Name: port3

Alias: lan2

Type: Physical Interface

VRF ID: 0

Role: LAN

Address

Addressing mode: Manual DHCP Auto-managed by IPAM One-Arm Sniffer

IP/Netmask: 10.0.1.1/24

Create address object matching subnet: ☐

Secondary IP address: ☐

Administrative Access

IPv4: ☒ HTTPS ☒ SSH ☒ PING ☐ SNMP ☐ FMG-Access ☐ FTM ☐ Speed Test ☐ RADIUS Accounting ☐ Security Fabric Connection

Receive LLDP: Use VDOM Setting Enable Disable

Transmit LLDP: Use VDOM Setting Enable Disable

DHCP Server

DHCP status: ☒ Enabled ☐ Disabled

Address range: 10.0.1.2-10.0.1.254

Netmask: 255.255.255.0

Default gateway: Same as Interface IP Specify



**Each interface Leased out IP addresses to the connected PCs from the Assigned DHCP pool addresses in their network.**

```
Terminal
pc3 x pc4 x pc1 x R3 x pc2 x

Welcome to Virtual PC Simulator, version 1.0 (0.8c)
Dedicated to Daling.
Build time: Dec 31 2016 01:22:17
Copyright (c) 2007-2015, Paul Meng (mirnshi@gmail.com)
All rights reserved.

VPCS is free software, distributed under the terms of the "BSD" licence.
Source code and license can be found at vpcs.sf.net.
For more information, please visit wiki.freecode.com.cn.
Modified version supporting unetlab by unetlab team

Press '?' to get help.

VPCS>
VPCS> dhcp
DDORA IP 10.0.0.5/24 GW 10.0.0.1

VPCS>

Terminal
pc3 x pc4 x pc1 x pc2 x

All rights reserved.

VPCS is free software, distributed under the terms of the "BSD" licence.
Source code and license can be found at vpcs.sf.net.
For more information, please visit wiki.freecode.com.cn.
Modified version supporting unetlab by unetlab team

Press '?' to get help.

VPCS> show

NAME IP/MASK GATEWAY GATEWAY
VPCS1 0.0.0.0/0 0.0.0.0
fe80::250:79ff:fe66:6802/64

VPCS> dhcp
DDO
Can't find dhcp server

VPCS> dhcp
DDORA IP 10.0.0.2/24 GW 10.0.0.1

VPCS>

Terminal
pc3 x pc4 x pc1 x pc2 x

Welcome to Virtual PC Simulator, version 1.0 (0.8c)
Dedicated to Daling.
Build time: Dec 31 2016 01:22:17
Copyright (c) 2007-2015, Paul Meng (mirnshi@gmail.com)
All rights reserved.

VPCS is free software, distributed under the terms of the "BSD" licence.
Source code and license can be found at vpcs.sf.net.
For more information, please visit wiki.freecode.com.cn.
Modified version supporting unetlab by unetlab team

Press '?' to get help.

VPCS> dhcp
DDORA IP 10.0.1.3/24 GW 10.0.1.1

VPCS>

Terminal
pc3 x pc4 x pc1 x pc2 x

Welcome to Virtual PC Simulator, version 1.0 (0.8c)
Dedicated to Daling.
Build time: Dec 31 2016 01:22:17
Copyright (c) 2007-2015, Paul Meng (mirnshi@gmail.com)
All rights reserved.

VPCS is free software, distributed under the terms of the "BSD" licence.
Source code and license can be found at vpcs.sf.net.
For more information, please visit wiki.freecode.com.cn.
Modified version supporting unetlab by unetlab team

Press '?' to get help.

VPCS> dhcp
DDORA IP 10.0.1.2/24 GW 10.0.1.1

VPCS>
```

## 6.Firewall Policies

Before applying firewall rules, both LANs could reach each other.

To enforce segmentation:

- A firewall policy was created allowing only PC1 (from LAN 1) to access LAN 2.

This demonstrates selective access control and micro-segmentation.

### Before Firewall policy

#### Pc 1 to LAN 2

```
Terminal
Fortinet x pc2 x pc1 x pc3 x pc4 x
Build time: Dec 31 2016 01:22:17
Copyright (c) 2007-2015, Paul Meng (mirnshi@gmail.com)
All rights reserved.

VPCS is free software, distributed under the terms of the "BSD" license.
Source code and license can be found at vpcs.sf.net.
For more information, please visit wiki.freecode.com.cn.
Modified version supporting unetlab by unetlab team

Press '?' to get help.

VPCS> dhcp
DDORA IP 10.0.0.2/24 GW 10.0.0.1

VPCS> ping 10.0.1.2
10.0.1.2 icmp_seq=1 timeout
10.0.1.2 icmp_seq=2 timeout
```

#### Pc 2 to LAN 2

```
Terminal
Fortinet x pc2 x pc1 x pc3 x pc4 x
Copyright (c) 2007-2015, Paul Meng (mirnshi@gmail.com)
All rights reserved.

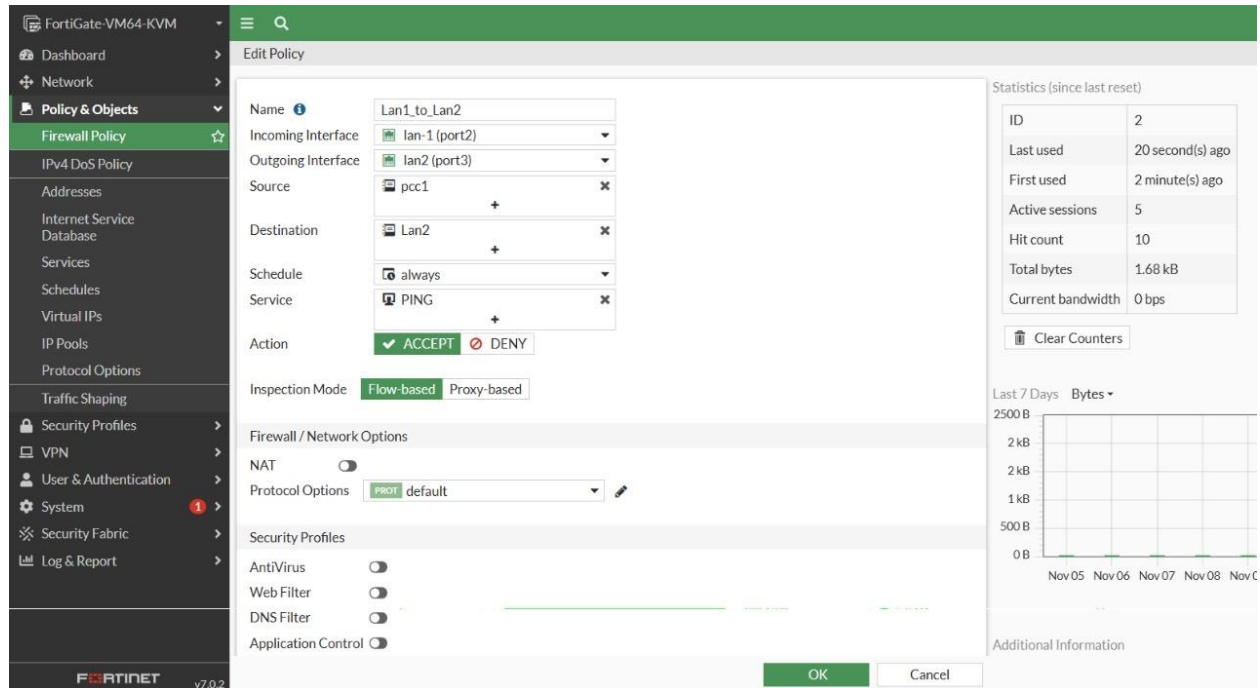
VPCS is free software, distributed under the terms of the "BSD" license.
Source code and license can be found at vpcs.sf.net.
For more information, please visit wiki.freecode.com.cn.
Modified version supporting unetlab by unetlab team

Press '?' to get help.

VPCS>
VPCS> dhcp
DDORA IP 10.0.0.5/24 GW 10.0.0.1

VPCS> ping 10.0.1.2
10.0.1.2 icmp_seq=1 timeout
10.0.1.2 icmp_seq=2 timeout
10.0.1.2 icmp_seq=3 timeout
10.0.1.2 icmp_seq=4 timeout
```

## Firewall Policy [Allowing PC1 only to reach LAN 2 devices]



**FortiGate-VM64-KVM**

**Edit Policy**

Name: Lan1\_to\_Lan2

Incoming Interface: lan-1 (port2)

Outgoing Interface: lan2 (port3)

Source: pcc1

Destination: Lan2

Schedule: always

Service: PING

Action: ☒ ACCEPT ☐ DENY

Inspection Mode: ☒ Flow-based ☐ Proxy-based

Firewall / Network Options

NAT: ☐ NAT

Protocol Options: pcc1 default

Security Profiles

AntiVirus: ☐

Web Filter: ☐

DNS Filter: ☐

Application Control: ☐

Statistics (since last reset)

ID	2
Last used	20 second(s) ago
First used	2 minute(s) ago
Active sessions	5
Hit count	10
Total bytes	1.68 kB
Current bandwidth	0 bps

Clear Counters

Last 7 Days Bytes

Additional Information

OK Cancel

## After the Policy

### PC1 can Reach LAN 2 devices

```

Terminal
Fortinet x pc3 x pc2 x pc1 x pc4 x
VPCS1 0.0.0.0/0 0.0.0.0
fe80::250:79ff:fe66:6802/64

VPCS> dhcp
DDORA IP 10.0.0.2/24 GW 10.0.0.1

VPCS> ping 10.0.1.2

84 bytes from 10.0.1.2 icmp_seq=1 ttl=63 time=5.544 ms
84 bytes from 10.0.1.2 icmp_seq=2 ttl=63 time=3.637 ms
84 bytes from 10.0.1.2 icmp_seq=3 ttl=63 time=4.033 ms
84 bytes from 10.0.1.2 icmp_seq=4 ttl=63 time=2.668 ms
84 bytes from 10.0.1.2 icmp_seq=5 ttl=63 time=3.565 ms

VPCS> ping 10.0.1.3

84 bytes from 10.0.1.3 icmp_seq=1 ttl=63 time=2.880 ms
84 bytes from 10.0.1.3 icmp_seq=2 ttl=63 time=3.770 ms
84 bytes from 10.0.1.3 icmp_seq=3 ttl=63 time=2.347 ms
84 bytes from 10.0.1.3 icmp_seq=4 ttl=63 time=5.871 ms
84 bytes from 10.0.1.3 icmp_seq=5 ttl=63 time=1.789 ms

VPCS>

```

### Pc2 cannot reach LAN 2 devices

```

Terminal
Fortinet x pc3 x pc2 x pc1 x pc4 x
10.0.1.2 icmp_seq=1 timeout
10.0.1.2 icmp_seq=2 timeout
10.0.1.2 icmp_seq=3 timeout
10.0.1.2 icmp_seq=4 timeout
10.0.1.2 icmp_seq=5 timeout

VPCS> ping 10.0.1.2

10.0.1.2 icmp_seq=1 timeout
10.0.1.2 icmp_seq=2 timeout
10.0.1.2 icmp_seq=3 timeout
10.0.1.2 icmp_seq=4 timeout
10.0.1.2 icmp_seq=5 timeout

VPCS> ping 10.0.1.3

10.0.1.3 icmp_seq=1 timeout
10.0.1.3 icmp_seq=2 timeout
10.0.1.3 icmp_seq=3 timeout
10.0.1.3 icmp_seq=4 timeout
10.0.1.3 icmp_seq=5 timeout

VPCS>

```

## Before Static Route and Internet Policy

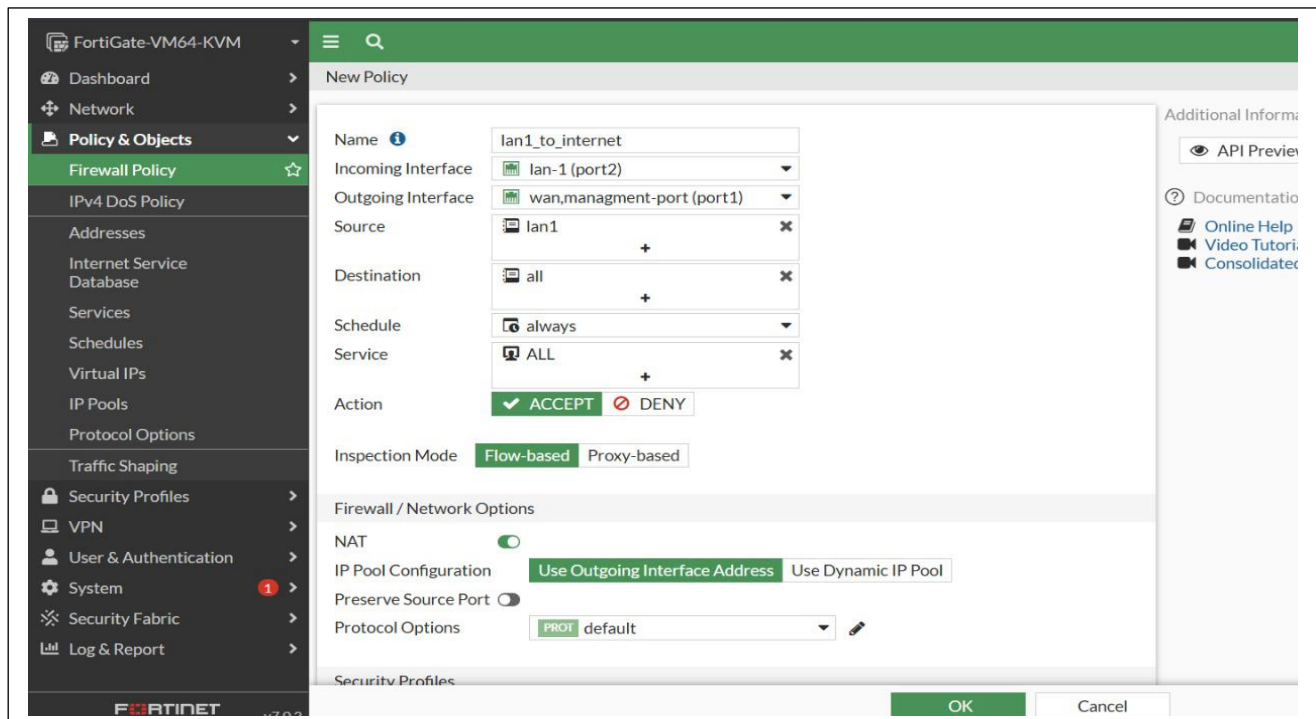
PC2 cannot reach the internet

```
pc3 x pc4 x pc1 x pc2 x
VPCS> ping 10.0.1.2
10.0.1.2 icmp_seq=1 timeout
10.0.1.2 icmp_seq=2 timeout
10.0.1.2 icmp_seq=3 timeout
10.0.1.2 icmp_seq=4 timeout
10.0.1.2 icmp_seq=5 timeout

VPCS> ping 8.8.8.8
*10.0.0.1 icmp_seq=1 ttl=255 time=1.183 ms (ICMP type:3, code:0, Destination network unreachable)
*10.0.0.1 icmp_seq=2 ttl=255 time=1.455 ms (ICMP type:3, code:0, Destination network unreachable)
*10.0.0.1 icmp_seq=3 ttl=255 time=1.437 ms (ICMP type:3, code:0, Destination network unreachable)
*10.0.0.1 icmp_seq=4 ttl=255 time=1.644 ms (ICMP type:3, code:0, Destination network unreachable)
*10.0.0.1 icmp_seq=5 ttl=255 time=1.770 ms (ICMP type:3, code:0, Destination network unreachable)

VPCS>
```

## Firewall policy [Allowing LAN 1 only to reach Internet and enabling Source NATing using WAN port IP address]



The screenshot shows the FortiGate VM64-KVM interface for configuring a new Firewall Policy. The left sidebar contains the navigation menu, and the main area displays the 'New Policy' configuration form.

**Policy Configuration:**

- Name:** lan1\_to\_internet
- Incoming Interface:** lan-1 (port2)
- Outgoing Interface:** wan,management-port (port1)
- Source:** lan1
- Destination:** all
- Schedule:** always
- Service:** ALL
- Action:** ACCEPT (checked), DENY
- Inspection Mode:** Flow-based (selected), Proxy-based

**Firewall / Network Options:**

- NAT:** Enabled (toggle)
- IP Pool Configuration:** Use Outgoing Interface Address (selected), Use Dynamic IP Pool
- Preserve Source Port:** Disabled (toggle)
- Protocol Options:** default

**Additional Information:**

- [API Preview](#)
- [Documentation](#)
- [Online Help](#)
- [Video Tutorial](#)
- [Consolidated](#)

**Buttons:** OK, Cancel



## After Static Route and Internet Policy

### PC1 to internet

```
Terminal
Fortinet x pc3 x pc2 x pc1 x pc4 x
84 bytes from 10.0.1.3 icmp_seq=1 ttl=63 time=2.880 ms
84 bytes from 10.0.1.3 icmp_seq=2 ttl=63 time=3.770 ms
84 bytes from 10.0.1.3 icmp_seq=3 ttl=63 time=2.347 ms
84 bytes from 10.0.1.3 icmp_seq=4 ttl=63 time=5.871 ms
84 bytes from 10.0.1.3 icmp_seq=5 ttl=63 time=1.789 ms

VPCS> ping 8.8.8.8

84 bytes from 8.8.8.8 icmp_seq=1 ttl=116 time=46.710 ms
84 bytes from 8.8.8.8 icmp_seq=2 ttl=116 time=47.317 ms
84 bytes from 8.8.8.8 icmp_seq=3 ttl=116 time=45.004 ms
84 bytes from 8.8.8.8 icmp_seq=4 ttl=116 time=47.791 ms
84 bytes from 8.8.8.8 icmp_seq=5 ttl=116 time=48.316 ms

VPCS> ping 8.8.8.8

8.8.8.8 icmp_seq=1 timeout
84 bytes from 8.8.8.8 icmp_seq=2 ttl=116 time=48.892 ms
84 bytes from 8.8.8.8 icmp_seq=3 ttl=116 time=46.011 ms
84 bytes from 8.8.8.8 icmp_seq=4 ttl=116 time=61.915 ms
84 bytes from 8.8.8.8 icmp_seq=5 ttl=116 time=50.113 ms
```

### PC2 to internet

```
Terminal
Fortinet x pc2 x pc1 x pc3 x pc4 x
Press '?' to get help.

VPCS>
VPCS> dhcp
DDORA IP 10.0.0.5/24 GW 10.0.0.1

VPCS> ping 10.0.1.2

10.0.1.2 icmp_seq=1 timeout
10.0.1.2 icmp_seq=2 timeout
10.0.1.2 icmp_seq=3 timeout
10.0.1.2 icmp_seq=4 timeout
10.0.1.2 icmp_seq=5 timeout

VPCS> ping 8.8.8.8

84 bytes from 8.8.8.8 icmp_seq=1 ttl=116 time=56.213 ms
84 bytes from 8.8.8.8 icmp_seq=2 ttl=116 time=56.391 ms
84 bytes from 8.8.8.8 icmp_seq=3 ttl=116 time=51.678 ms
84 bytes from 8.8.8.8 icmp_seq=4 ttl=116 time=57.374 ms
84 bytes from 8.8.8.8 icmp_seq=5 ttl=116 time=131.222 ms
```

## 7.Public Private IP resolution (SOURCE NATing)

FortiGate-VM64-KVM									
Add Filter									
Date/Time	Source	Device	Destination	Application Name	Result	Policy ID	Log Details		
17 seconds ago	10.0.0.5	pc1	8.8.8.8		✓ 84 B / 84 B	lan1_to_internet (1)	General		
18 seconds ago	10.0.0.5	pc1	8.8.8.8		✓ 84 B / 84 B	lan1_to_internet (1)	Absolute Date/Time 2025/11/13 10:27:11		
20 seconds ago	10.0.0.5	pc1	8.8.8.8		✓ 84 B / 84 B	lan1_to_internet (1)	Time 10:27:11		
20 seconds ago	10.0.0.5	pc1	8.8.8.8		✓ 84 B / 84 B	lan1_to_internet (1)	Duration 60s		
21 seconds ago	10.0.0.5	pc1	8.8.8.8		✓ 84 B / 84 B	lan1_to_internet (1)	Session ID 4537		
							Virtual Domain root		
							NAT Translation Source		
							Source		
							IP 10.0.0.5		
							NAT IP 192.168.1.29		
							NAT Port 0		
							Country/Region Reserved		
							Primary MAC 00:50:79:66:68:04		
							Source Interface lan-1 (port2)		
							Source Host Name VPCS1		
							User		
							Destination		
							IP 8.8.8.8		
							Country/Region United States		
							Destination Interface wan,managment-port (port1)		

## Static Routing

Configured a default static route to enable outbound traffic through the WAN interface for internet access.

FortiGate-VM64-KVM
Dashboard
Network
Interfaces
DNS
Packet Capture
SD-WAN
Static Routes
Policy Routes
RIP
OSPF
BGP
Routing Objects
Multicast
Policy & Objects
Security Profiles

Edit Static Route

Destination
Subnet
Internet Service
0.0.0.0/0.0.0.0

Gateway Address
192.168.1.1

Interface
wan,managment-port (port1)

Administrative Distance
10

Comments
Write a comment...
0/255

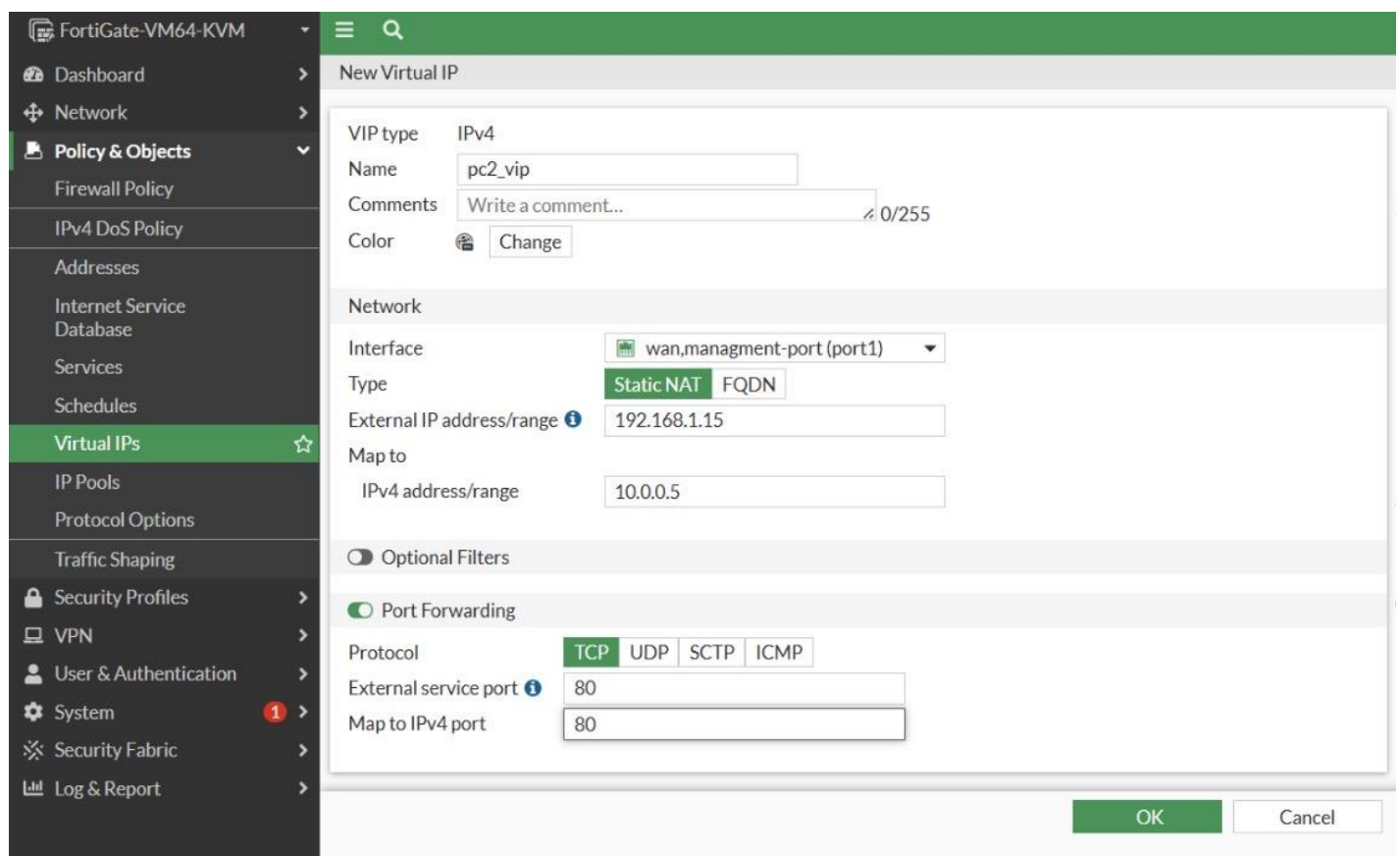
Status
Enabled
Disabled

Advanced Options

## 8. Destination NAT

This configuration creates a Destination NAT (DNAT) rule on the FortiGate.

When an external user sends a request to 192.168.1.15:80, the FortiGate automatically translates it to 10.0.0.5:80 and forwards it to the internal web server (PC2).



FortiGate-VM64-KVM

Dashboard

Network

Policy & Objects

Firewall Policy

IPv4 DoS Policy

Addresses

Internet Service Database

Services

Schedules

Virtual IPs

IP Pools

Protocol Options

Traffic Shaping

Security Profiles

VPN

User & Authentication

System

Security Fabric

Log & Report

New Virtual IP

VIP type: IPv4

Name: pc2\_vip

Comments: Write a comment... 0/255

Color: Change

Network

Interface: wan,managment-port (port1)

Type: Static NAT FQDN

External IP address/range: 192.168.1.15

Map to:

IPv4 address/range: 10.0.0.5

Optional Filters

Port Forwarding

Protocol: TCP UDP SCTP ICMP

External service port: 80

Map to IPv4 port: 80

OK Cancel



FortiGate-VM64-KVM

Dashboard

Network

Policy & Objects

Firewall Policy

IPv4 DoS Policy

Addresses

Internet Service Database

Services

Schedules

Virtual IPs

IP Pools

Protocol Options

Traffic Shaping

Security Profiles

VPN

User & Authentication

System

Security Fabric

Log & Report

Edit Policy

Name

http\_to\_PC2

Incoming Interface

wan\_management-port (port1)

Outgoing Interface

lan-1 (port2)

Source

all

Destination

pc2\_vip

Schedule

always

Service

HTTP

Action

ACCEPT

DENY

Inspection Mode

Flow-based

Proxy-based

Firewall / Network Options

NAT

Protocol Options

default

Security Profiles

AntiVirus

Web Filter

DNS Filter

Application Control

IPS

File Filter

SSL Inspection

no-inspection

OK

Cancel



## Back Up File

Page 20 of 21



## 9. Testing & Verification

Multiple tests were conducted:

- ✓ PC1 reached LAN 2 successfully.
- ✓ PC2 was blocked from LAN 2 as intended.
- ✓ Internet access worked for allowed LANs.
- ✓ DNAT successfully forwarded external requests to the internal server.

All results confirmed correct configuration and policy enforcement.

## 10. Conclusion

This project demonstrates core network security principles using a FortiGate firewall. Through segmentation, NAT, routing, and privilege-controlled administration, a secure and