



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**



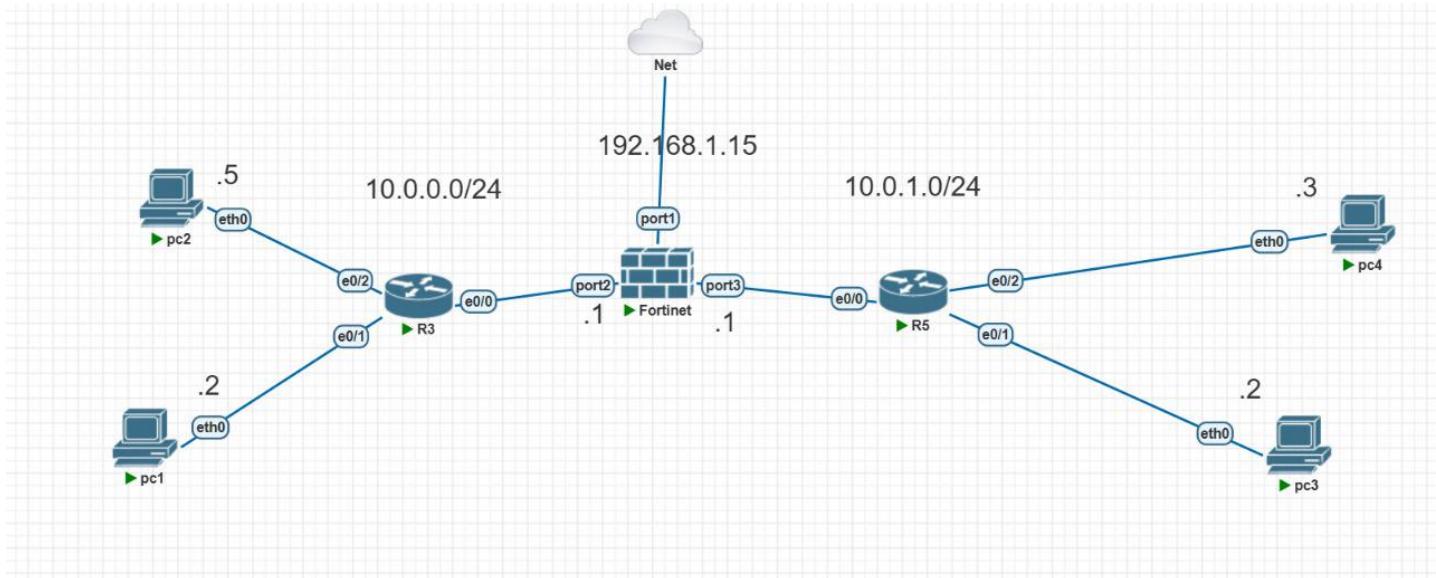
1. Introduction

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.

```
boundary
==[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	<input type="text"/> 0/255	
Access Permissions		
Access Control	Permissions	Set All ▾
Security Fabric	<input checked="" type="radio"/> None <input checked="" type="radio"/> Read <input type="radio"/> Read/Write	
FortiView	<input checked="" type="radio"/> None <input checked="" type="radio"/> Read <input type="radio"/> Read/Write	
User & Device	<input checked="" type="radio"/> None <input checked="" type="radio"/> Read <input type="radio"/> Read/Write	
Firewall	<input checked="" type="radio"/> None <input checked="" type="radio"/> Read <input type="radio"/> Read/Write <input type="radio"/> Custom	
Log & Report	<input checked="" type="radio"/> None <input checked="" type="radio"/> Read <input type="radio"/> Read/Write <input type="radio"/> Custom	
Network	<input checked="" type="radio"/> None <input checked="" type="radio"/> Read <input type="radio"/> Read/Write <input type="radio"/> Custom	
System	<input checked="" type="radio"/> None <input checked="" type="radio"/> Read <input type="radio"/> Read/Write <input type="radio"/> Custom	
Security Profile	<input checked="" type="radio"/> None <input checked="" type="radio"/> Read <input checked="" type="radio"/> Read/Write <input type="radio"/> Custom	
VPN	<input checked="" type="radio"/> None <input checked="" type="radio"/> Read <input type="radio"/> Read/Write	

OK Cancel



Creating administrator and giving it the Trainee admin profile.

The screenshot shows the FortiGate VM64 KVM interface. The left sidebar is a navigation menu with the following items:

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

The main window title is "New Administrator". The configuration fields are as follows:

Username	trainee
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	trainee
Confirm Password	trainee
Comments	Write a comment... 0/255
Administrator profile	trainee

Below these fields are three toggle buttons:

- Two-factor Authentication
- Restrict login to trusted hosts
- Restrict admin to guest account provisioning only

At the bottom right are two buttons: "OK" (green) and "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 shows the FortiGate management interface. The left sidebar is the navigation menu with various options like Dashboard, Network, Policies, and Reports. The main window is titled 'Edit Interface' for 'wan.management-port (port1)'. The configuration tabs include Name, Address, Administrative Access, Traffic Shaping, and Miscellaneous. In the 'Address' tab, the 'Addressing mode' is set to 'Manual' with IP/Netmask '192.168.1.29/255.255.255.0'. Under 'Administrative Access', several protocols are checked: HTTPS, HTTP, SSH, PING, and SNMP. The 'Receive LLDP' and 'Transmit LLDP' sections both have 'Use VDOM Setting' and 'Enable' selected. There is no 'Outbound shaping profile' or 'Comments' entered. At the bottom right 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

S Fx

St

M

50

A

Edit Interface

Name: lan-1 (port2)

Alias: lan-1

Type: Physical Interface

VRF ID: 0

Role: LAN

Address

Addressing mode: Manual

IP/Netmask: 10.0.0.1/255.255.255.0

Create address object matching subnet:

Secondary IP address:

Administrative Access

IPv4: HTTPS, PING, SSH, SNMP, 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: 10.0.0.2-10.0.0.254

Netmask: 255.255.255.0

Default gateway: Same as Interface IP, Specify

OK Cancel



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

The screenshot shows the FortiGate VM64-KVM interface configuration for Port 3. The interface is named 'port3' with an alias 'lan2'. It is set as a Physical Interface (VRF ID 0, Role LAN). The IP address is configured in Manual mode with the subnet '10.0.1.0/24'. Under Administrative Access, various protocols like HTTPS, SSH, PING, and SNMP are enabled. The DHCP Server section shows that DHCP is Enabled, with an address range of 10.0.1.2-10.0.1.254, netmask 255.255.255.0, and default gateway set to 'Same as Interface IP'.



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

The image shows four terminal windows side-by-side, each representing a different host (pc3, pc4, pc1, pc2). Each window displays the VPCS (Virtual PC Simulator) version 1.0 (0.8c) welcome screen, which includes the build date (Dec 31 2016 01:22:17), copyright information (Copyright (c) 2007-2015, Paul Meng (mirnshi@gmail.com)), and a note about the BSD license. The windows then show the command-line interface (CLI) of VPCS. In the first three windows (pc3, pc4, pc1), the user runs the 'dhcp' command, which outputs the assigned IP address (e.g., 10.0.0.5/24 for pc3, 10.0.0.6/24 for pc4, 10.0.0.7/24 for pc1) and the gateway (10.0.0.1). The fourth window (pc2) shows the 'show' command output, which lists the assigned IP/MASK and GATEWAY for each interface:

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



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
10.0.1.2 icmp_seq=3 timeout
10.0.1.2 icmp_seq=4 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]

The screenshot shows the FortiGate VM 64 KVM interface. On the left, the navigation menu is expanded to show the 'Policy & Objects' section, specifically the 'Firewall Policy' tab. The main panel displays the configuration for a policy named 'Lan1_to_Lan2'. The policy details are as follows:

- Name:** Lan1_to_Lan2
- Incoming Interface:** Lan-1 (port2)
- Outgoing Interface:** Lan2 (port3)
- Source:** pcc1
- Destination:** Lan2
- Schedule:** always
- Service:** PING
- Action:** ✓ ACCEPT (selected)

Below the policy details, there are tabs for 'Inspection Mode' (Flow-based selected), 'Firewall / Network Options', and 'Protocol Options' (PROT default selected). To the right, there is a 'Statistics (since last reset)' table and a 'Last 7 Days' traffic graph. The graph shows minimal traffic, with most values at 0 kB. The statistics table includes the following data:

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

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

After the Policy

PC1 can Reach LAN 2 devices

```
Terminal
Fortinet x pc3 x pc2 x pc1 x pc4 x
VPCSI 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 ✘ pc4 ✘ pc1 ✘ pc2 ✘
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 management interface with the following details:

- Left Sidebar:** Shows the navigation menu with "Policy & Objects" selected, specifically "Firewall Policy". Other options include Dashboard, Network, IPv4 DoS Policy, Addresses, Internet Service Database, Services, Schedules, Virtual IPs, IP Pools, Protocol Options, Traffic Shaping, Security Profiles, VPN, User & Authentication, System (with a red notification badge), Security Fabric, and Log & Report.
- Main Content Area:** A "New Policy" dialog box is open.
 - Name:** lan1_to_internet
 - Incoming Interface:** lan1 (port2)
 - Outgoing Interface:** wan,management-port (port1)
 - Source:** lan1
 - Destination:** all
 - Schedule:** always
 - Service:** ALL
 - Action:** ✓ ACCEPT (selected)
 - Inspection Mode:** Flow-based (selected)
 - Firewall / Network Options:** NAT is enabled. IP Pool Configuration shows "Use Outgoing Interface Address" selected. Protocol Options are set to PROT default.
- Right Sidebar:** Contains links for API Preview, Documentation, Online Help, Video Tutorials, and Consolidated Reports.



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
VPCS>
```

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
VPCS>
```



7. Public Private IP resolution (SOURCE NATing)

The screenshot shows the FortiGate VM64-KVM interface. The left sidebar is collapsed, and the main area displays a log table and detailed log information.

Log Table Headers: Date/Time, Source, Device, Destination, Application Name, Result, Policy ID

Log Details:

Category	Value
General	Absolute Date/Time: 2025/11/13 10:27:11 Time: 10:27:11 Duration: 60s 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.management-port (port1)



Static Routing

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

The screenshot shows the FortiGate-VM64-KVM interface. The left sidebar menu is as follows:

- Dashboard
- Network
 - Interfaces
 - DNS
 - Packet Capture
- SD-WAN
- Static Routes
- Policy Routes
- RIP
- OSPF
- BGP
- Routing Objects
- Multicast

Policy & Objects

Security Profiles

The main panel title is "Edit Static Route". The configuration details are:

Destination	Subnet	Internet Service
0.0.0.0/0.0.0.0		
Gateway Address	192.168.1.1	
Interface	wan,management-port (port1)	
Administrative Distance	10	
Comments	Write a comment... 0/255	
Status	Enabled	Disabled

Advanced Options are available at the bottom.



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).

The screenshot shows the FortiGate VM64-KVM interface. The left sidebar menu is visible, with 'Virtual IPs' selected. The main window displays a 'New Virtual IP' configuration dialog. The 'Name' field is set to 'pc2_vip'. Under the 'Network' section, the 'Interface' is set to 'wan,management-port (port1)' and 'Type' is 'Static NAT'. The 'External IP address/range' is '192.168.1.15' and the 'Map to' address is '10.0.0.5'. In the 'Optional Filters' section, 'Port Forwarding' is enabled. The 'Protocol' tab is selected, showing 'TCP' as the chosen protocol, with 'External service port' set to '80' and 'Map to IPv4 port' also set to '80'. At the bottom right of the dialog are 'OK' and 'Cancel' buttons.



DNAT Firewall Policy

Allows Traffic from Internet to PC2 only using DNATing

The screenshot shows the FortiGate management interface for policy configuration. The left sidebar navigation menu includes: Dashboard, Network, Policy & Objects (selected), Firewall Policy (selected), IPv4 DoS Policy, Addresses, Internet Service Database, Services, Schedules, Virtual IPs, IP Pools, Protocol Options, Traffic Shaping, Security Profiles, VPN, User & Authentication, System (with a red '1' notification), Security Fabric, and Log & Report.

The main configuration window is titled "Edit Policy". The "Name" field is set to "http_to_PC2". The "Incoming Interface" is "wan,management-port (port1)". The "Outgoing Interface" is "lan-1 (port2)". The "Source" is "all". The "Destination" is "pc2_vip". The "Schedule" is "always". The "Service" is "HTTP". The "Action" is "ACCEPT".

Below the main configuration, there are sections for "Inspection Mode" (Flow-based selected), "Firewall / Network Options", "NAT" (disabled), "Protocol Options" (PROT default), "Security Profiles" (Antivirus, Web Filter, DNS Filter, Application Control, IPS, File Filter all disabled), and "SSL Inspection" (SSL no-inspection).

At the bottom right of the configuration window are "OK" and "Cancel" buttons.



Public Private IP Resolving

The screenshot shows the FortiGate-VM64-KVM interface. The left sidebar is the navigation menu, and the main area is the 'Log & Report' section under 'Forward Traffic'. A single log entry is selected, showing a connection from 'pc1' to '8.8.8.8' at '17 seconds ago'. The log details pane on the right provides comprehensive information about the session, including General, Source, and Destination details.

Date/Time	Source	Device	Destination	Application Name	Result	Policy ID
17 seconds ago	10.0.0.5	pc1	8.8.8.8		✓ 84 B / 84 B	lan1_to_internet (1)
18 seconds ago	10.0.0.5	pc1	8.8.8.8		✓ 84 B / 84 B	lan1_to_internet (1)
20 seconds ago	10.0.0.5	pc1	8.8.8.8		✓ 84 B / 84 B	lan1_to_internet (1)
20 seconds ago	10.0.0.5	pc1	8.8.8.8		✓ 84 B / 84 B	lan1_to_internet (1)
21 seconds ago	10.0.0.5	pc1	8.8.8.8		✓ 84 B / 84 B	lan1_to_internet (1)

Log Details

General

- Absolute Date/Time: 2025/11/13 10:27:11
- Time: 10:27:11
- Duration: 60s
- Session ID: 4537
- Virtual Domain: root
- NAT Translation: Source

Source

- IP: 10.0.0.5
- NAT IP: 192.168.129
- 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.management-port (port1)

Back Up File

The screenshot shows a file download dialog box. It displays the file name 'FortiGate-VM64-KVM_7-0_0234_2025111...' and the download date and time '11/13/2025 2:23 AM'. The 'Cancel' button is visible on the right side of the dialog.



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