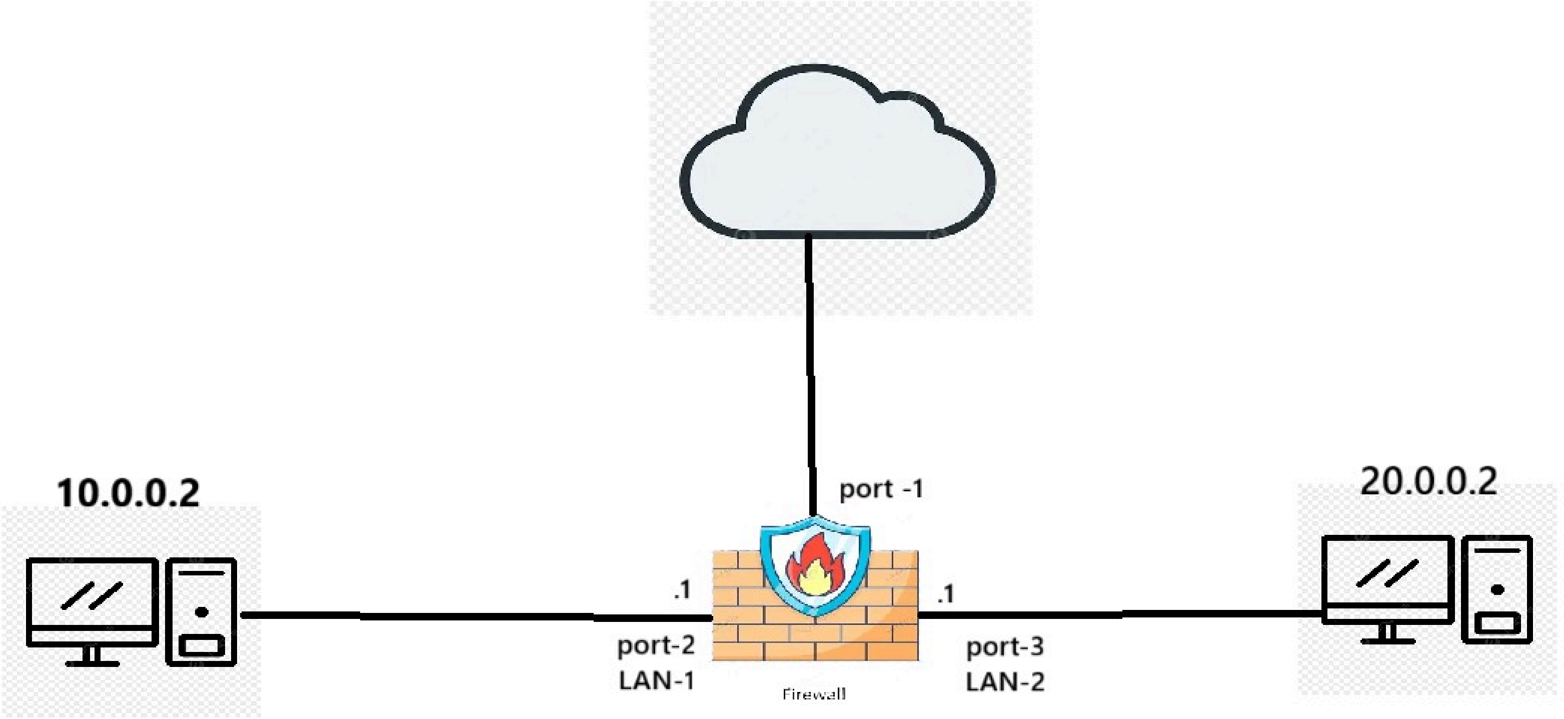
Depi-Project

Network Topology Diagram

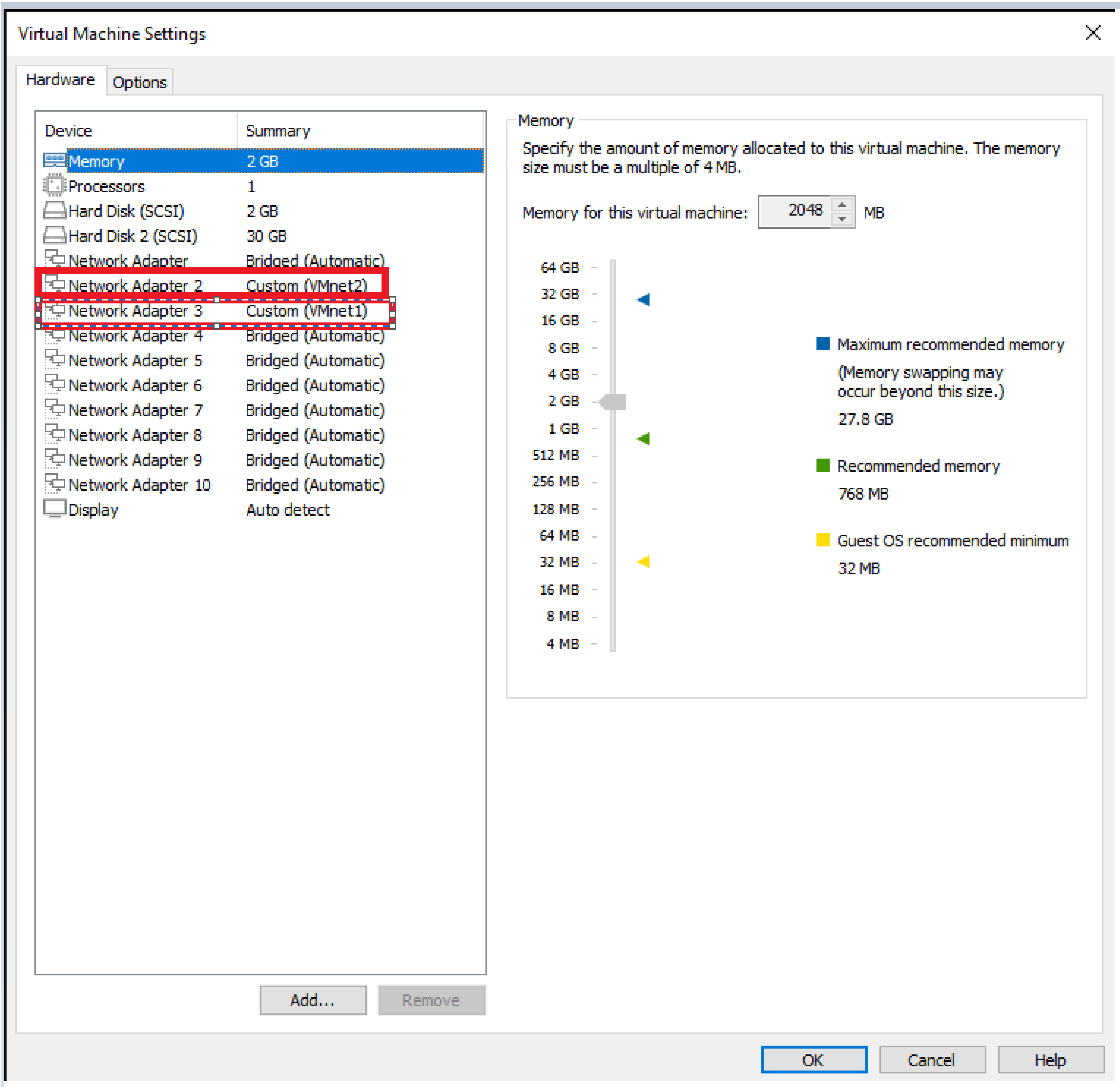


---

1. Virtual Machine Network Configuration

1 :

the FortiGate VM network adapter configuration. The firewall is set up with two custom network adapters, **VMnet2** and **VMnet1**, which segregate the internal LAN from the WAN/Internet segment, enabling the core firewall functionality.



Virtual Machine Settings

Device	Summary
Memory	2 GB
Processors	1
Hard Disk (SCSI)	2 GB
Hard Disk 2 (SCSI)	30 GB
Network Adapter	Bridged (Automatic)
Network Adapter 2	Custom (VMnet2)
Network Adapter 3	Custom (VMnet1)
Network Adapter 4	Bridged (Automatic)
Network Adapter 5	Bridged (Automatic)
Network Adapter 6	Bridged (Automatic)
Network Adapter 7	Bridged (Automatic)
Network Adapter 8	Bridged (Automatic)
Network Adapter 9	Bridged (Automatic)
Network Adapter 10	Bridged (Automatic)
Display	Auto detect

Memory

Specify the amount of memory allocated to this virtual machine. The memory size must be a multiple of 4 MB.

Memory for this virtual machine: 2048 MB

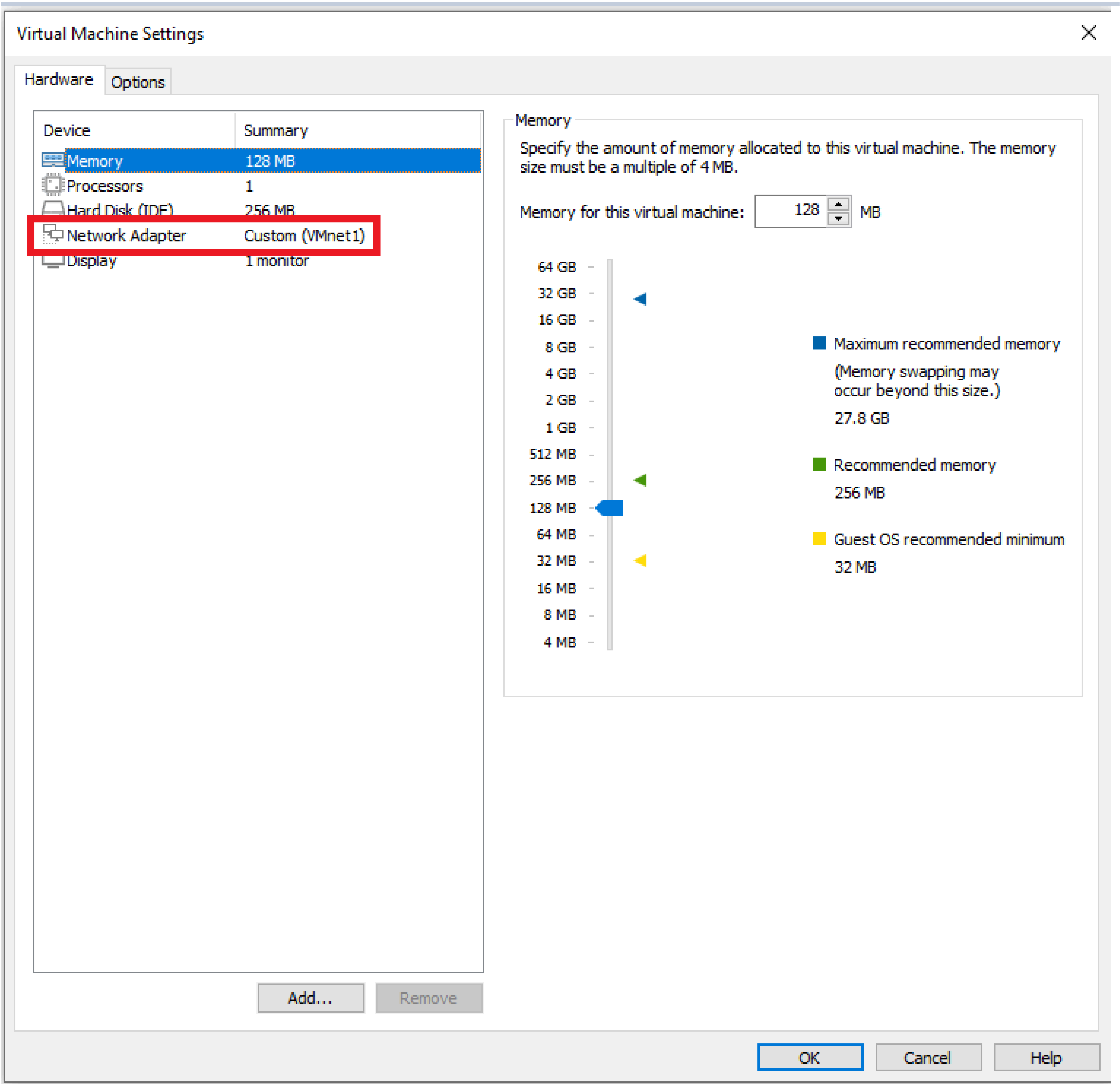
🟦 Maximum recommended memory
(Memory swapping may occur beyond this size.)
27.8 GB

🟩 Recommended memory
768 MB

🟨 Guest OS recommended minimum
32 MB

2 :

the network settings for the Internal Host (PC). It is connected to a **Custom (VMnet1)** adapter, which represents the internal LAN segment the PC belongs to.



Virtual Machine Settings

Device	Summary
Memory	128 MB
Processors	1
Hard Disk (IDE)	256 MB
Network Adapter	Custom (VMnet1)
Display	1 monitor

Memory

Specify the amount of memory allocated to this virtual machine. The memory size must be a multiple of 4 MB.

Memory for this virtual machine: 128 MB

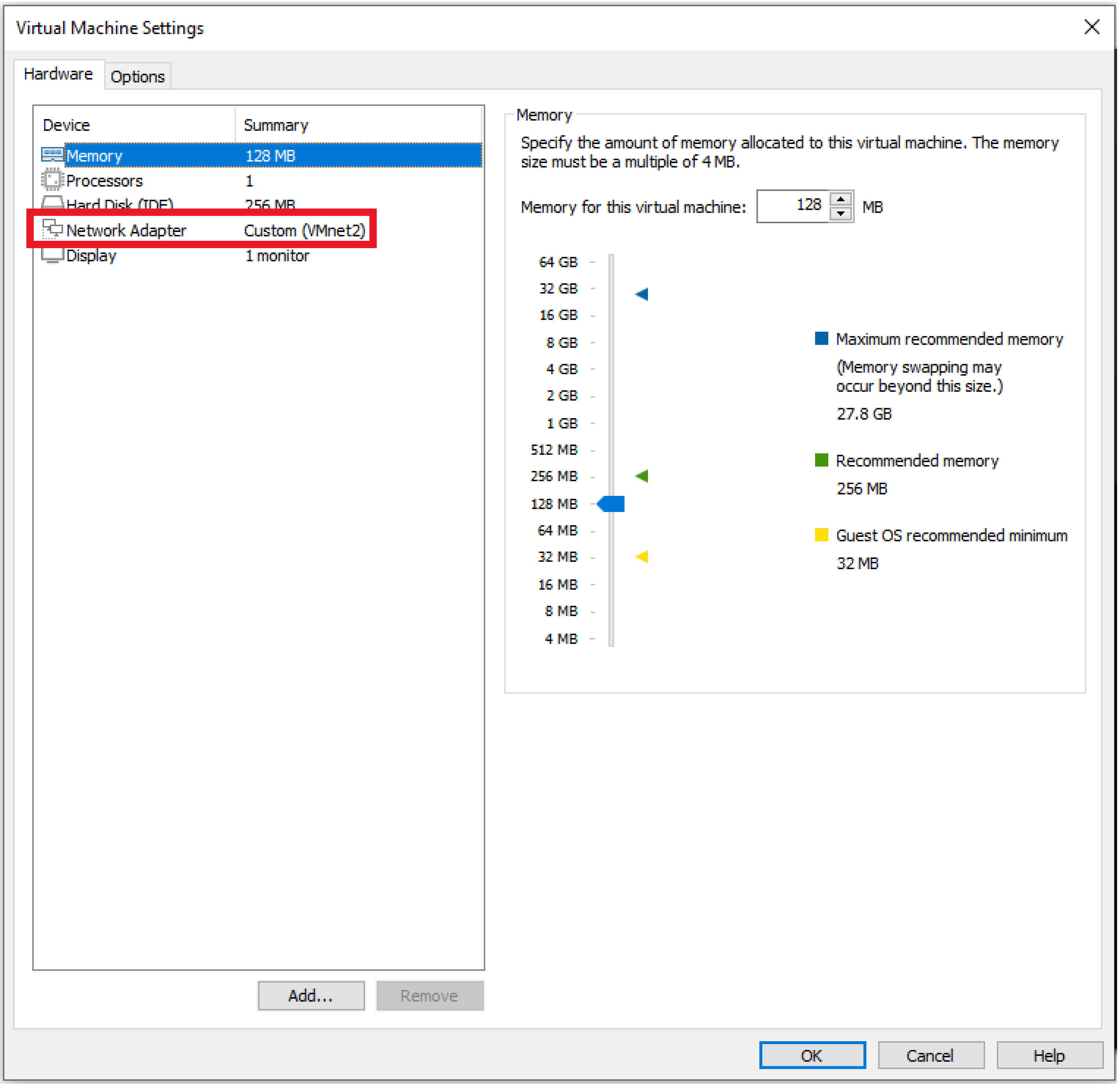
🟦 Maximum recommended memory
(Memory swapping may occur beyond this size.)
27.8 GB

🟩 Recommended memory
256 MB

🟨 Guest OS recommended minimum
32 MB

3:

This illustrates the network configuration for the Web Server host. It is connected to a **Custom (VMnet2)** network adapter, placing it on the internal segment that will be protected by and accessed through the FortiGate firewall.



Virtual Machine Settings

Hardware | Options

Device	Summary
Memory	128 MB
Processors	1
Hard Disk (IDE)	256 MB
Network Adapter	Custom (VMnet2)
Display	1 monitor

Memory

Specify the amount of memory allocated to this virtual machine. The memory size must be a multiple of 4 MB.

Memory for this virtual machine: 128 MB

🟦 Maximum recommended memory

(Memory swapping may occur beyond this size.)

27.8 GB

🟩 Recommended memory

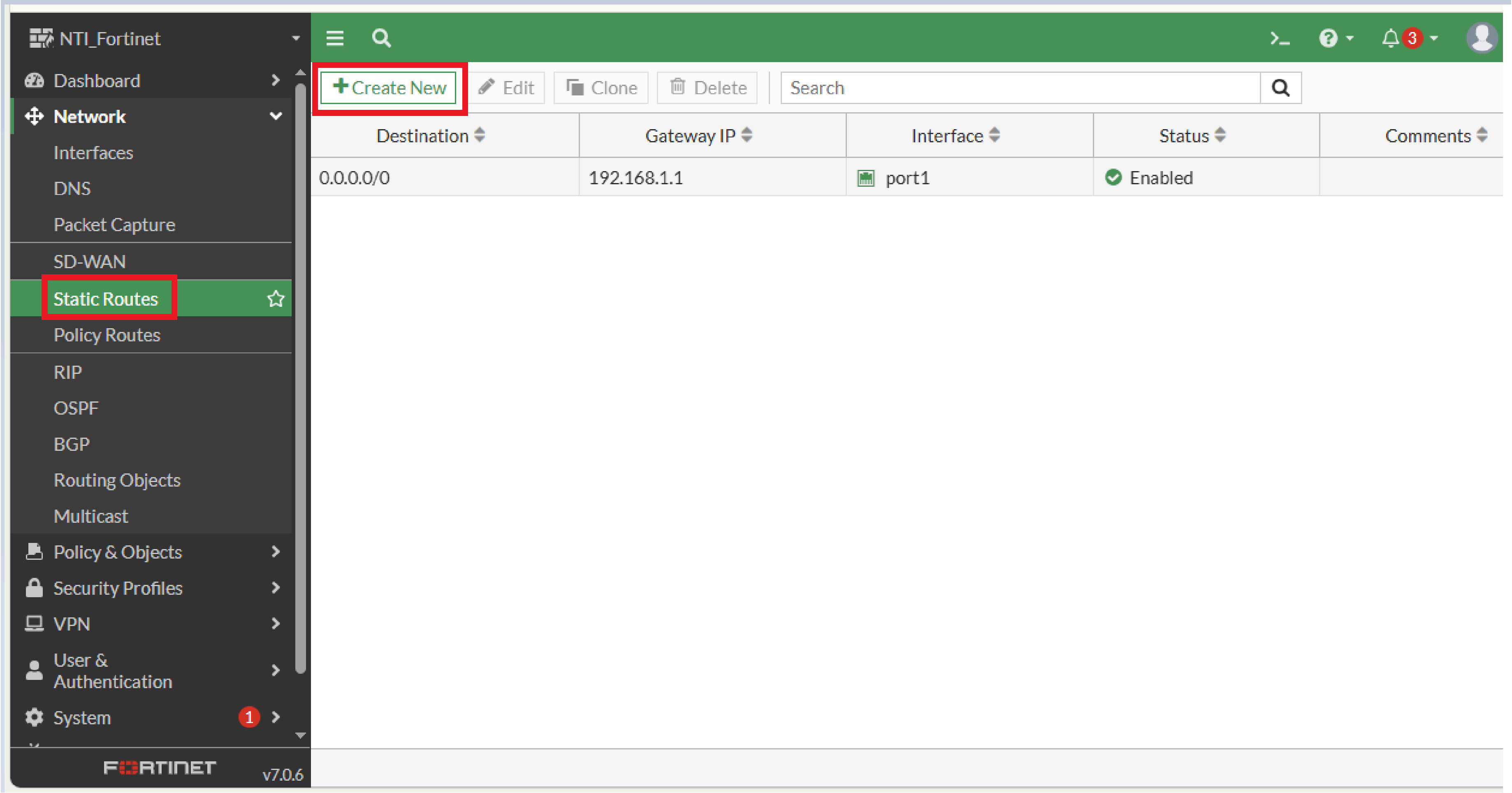
256 MB

🟨 Guest OS recommended minimum

32 MB

2. Static Route Configuration

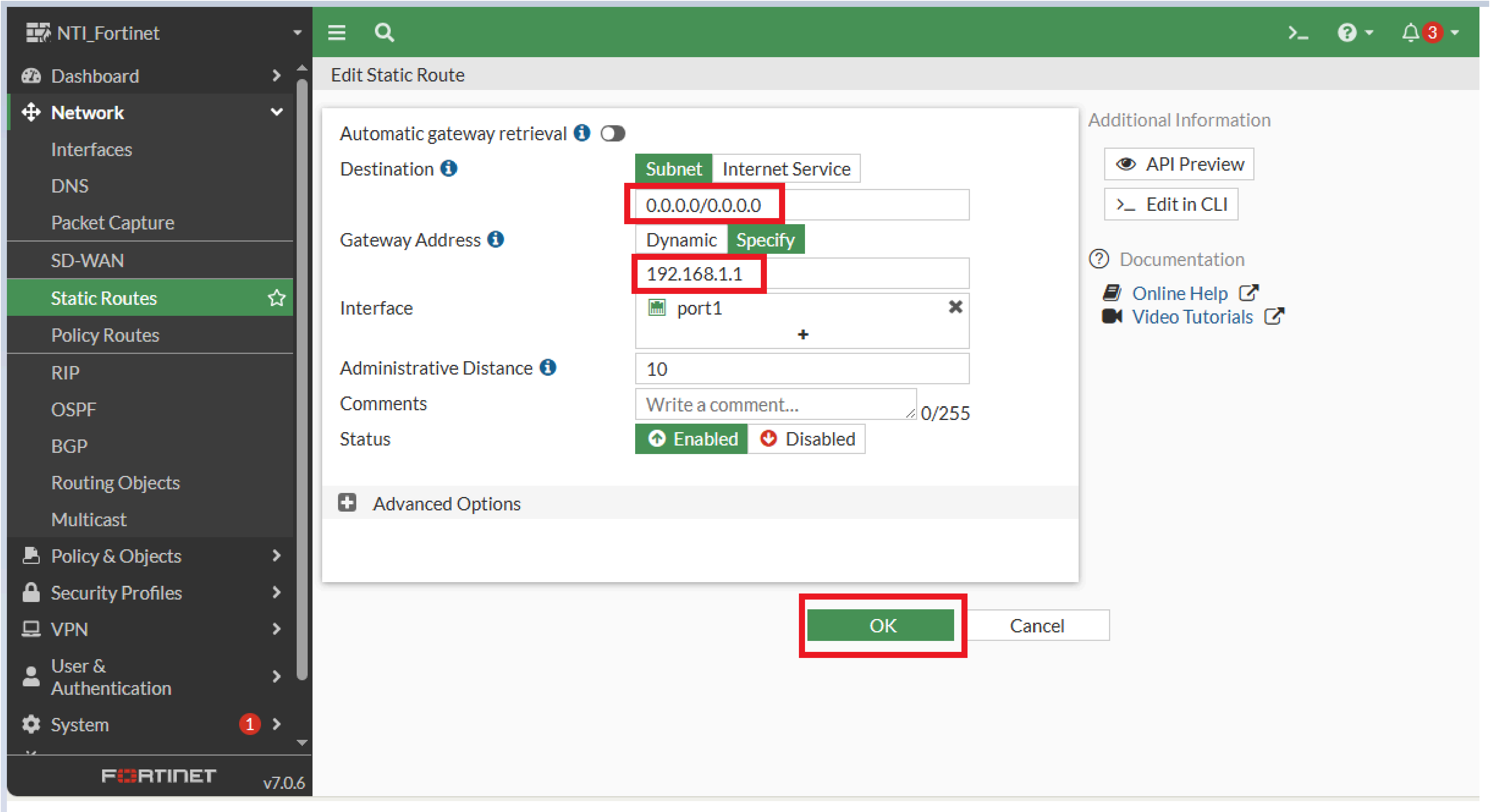
1



Destination	Gateway IP	Interface	Status	Comments
0.0.0.0/0	192.168.1.1	port1	✓ Enabled	

2 :

This configuration establishes the **Default Static Route**. The **Destination is set to** 0.0.0.0/0.0.0.0 (all networks), directing all outbound traffic to the **Gateway Address** 192.168.1.1 via the **port1** (WAN) Interface. This route is essential for enabling Internet access for internal devices.



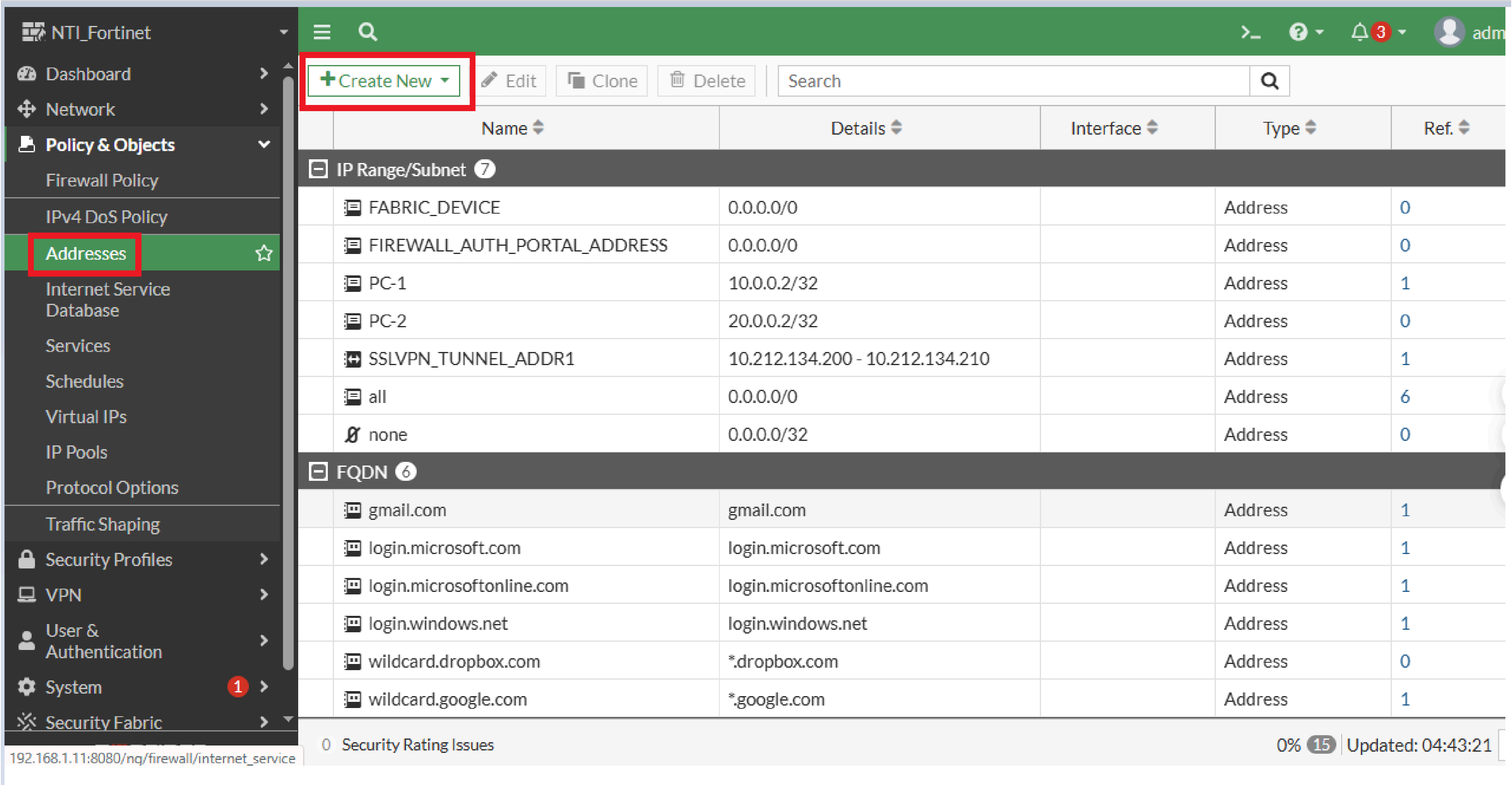
Edit Static Route

Automatic gateway retrieval
Destination: Subnet | Internet Service
0.0.0.0/0.0.0.0
Gateway Address: Dynamic | Specify
192.168.1.1
Interface: port1
Administrative Distance: 10
Comments: Write a comment... 0/255
Status: Enabled | Disabled

2. Source NAT Policy

1) IPv4 Address object

1

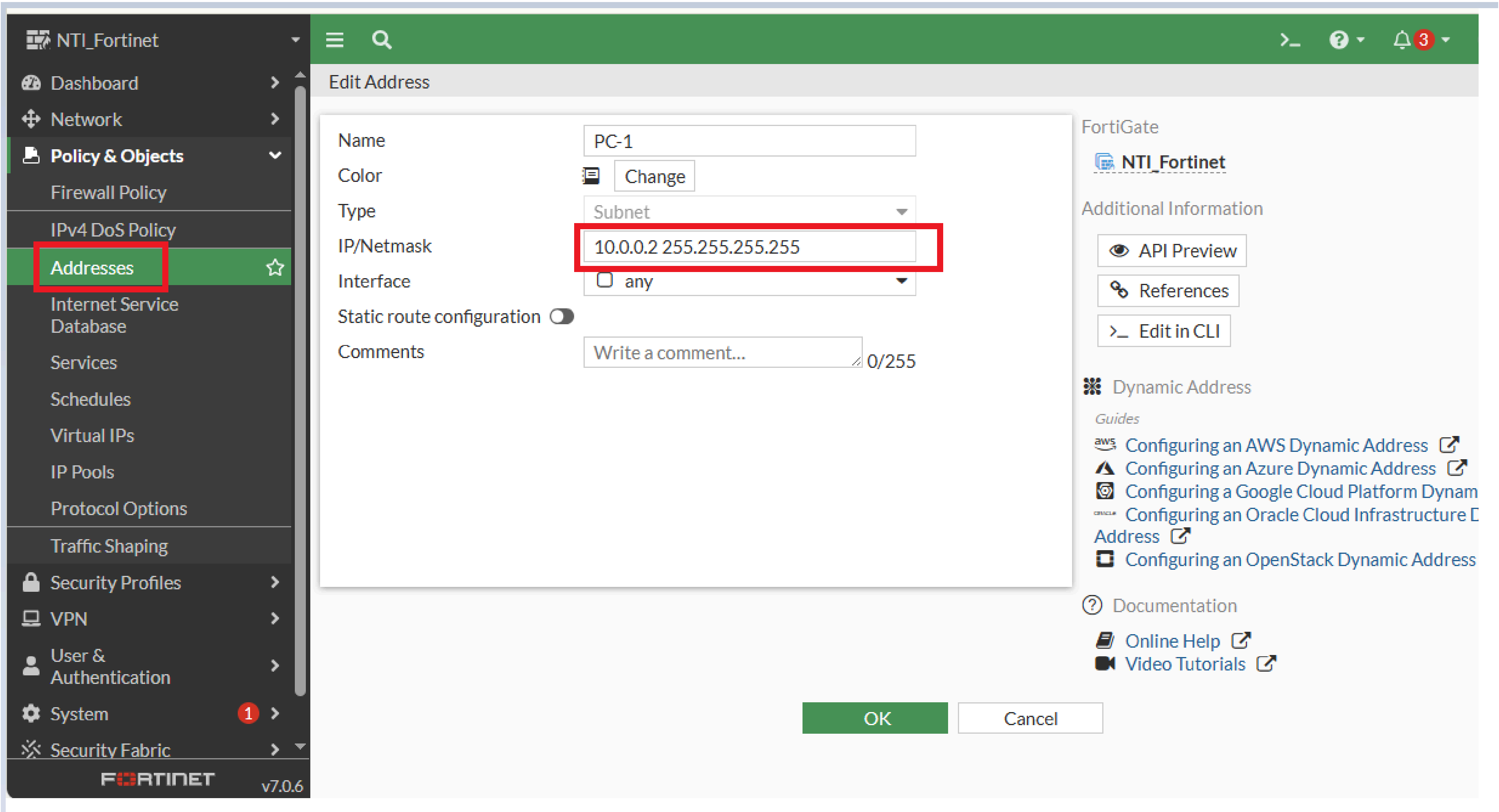


Name	Details	Interface	Type	Ref.
IP Range/Subnet 7				
FABRIC_DEVICE	0.0.0.0/0		Address	0
FIREWALL_AUTH_PORTAL_ADDRESS	0.0.0.0/0		Address	0
PC-1	10.0.0.2/32		Address	1
PC-2	20.0.0.2/32		Address	0
SSLVPN_TUNNEL_ADDR1	10.212.134.200 - 10.212.134.210		Address	1
all	0.0.0.0/0		Address	6
none	0.0.0.0/32		Address	0
FQDN 6				
gmail.com	gmail.com		Address	1
login.microsoft.com	login.microsoft.com		Address	1
login.microsoftonline.com	login.microsoftonline.com		Address	1
login.windows.net	login.windows.net		Address	1
wildcard.dropbox.com	*.dropbox.com		Address	0
wildcard.google.com	*.google.com		Address	1

0 Security Rating Issues 0% 15 Updated: 04:43:21

2 :

An IPv4 Address object named **PC-1** is created under Policy & Objects. It defines the specific internal IP address $10.0.0.2/255.255.255.255$ that is permitted to access external networks.



Edit Address

Name: PC-1

Color: Change

Type: Subnet

IP/Netmask: 10.0.0.2 255.255.255.255

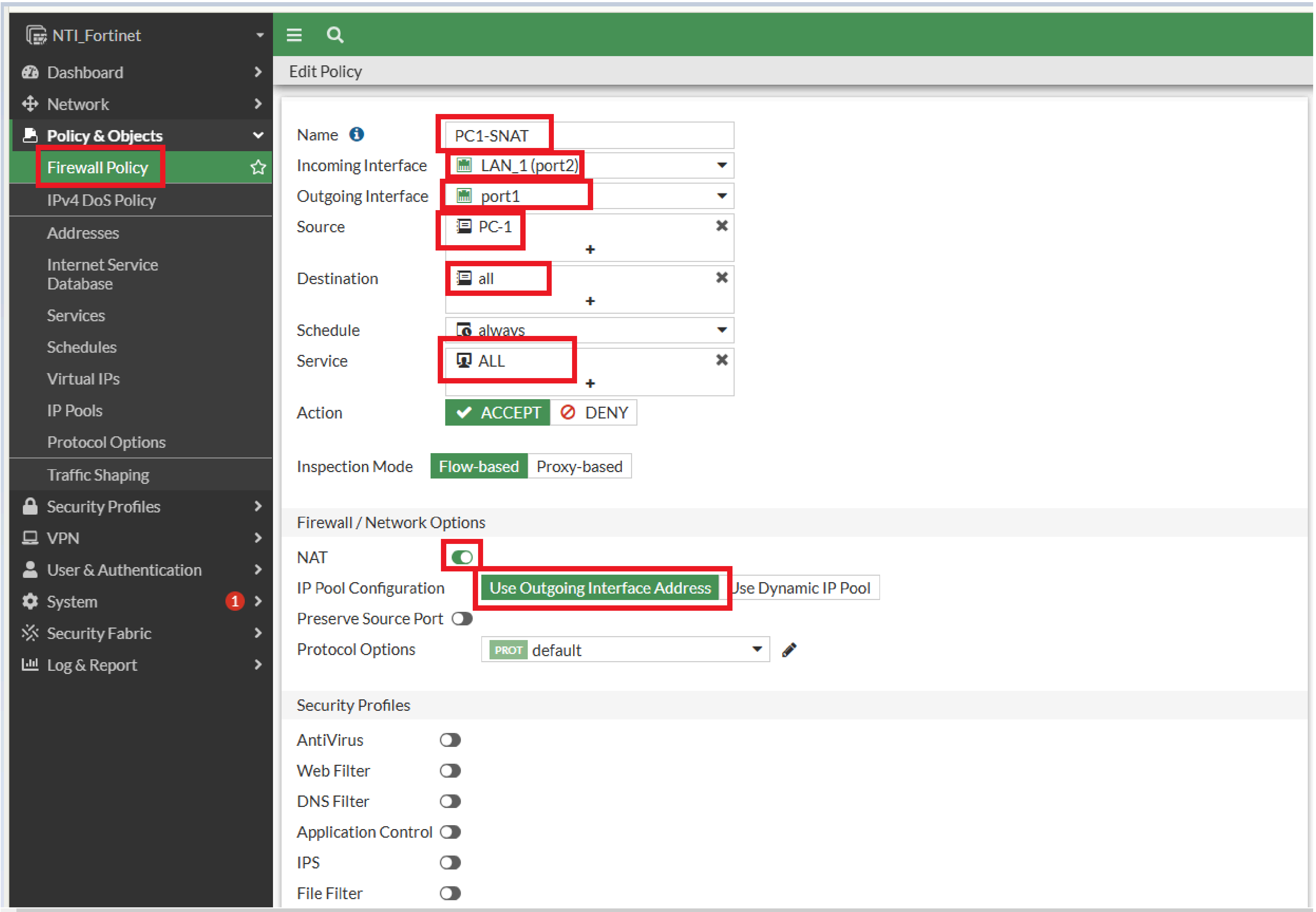
Interface: any

Static route configuration

Comments: Write a comment... 0/255

2) Source NAT Firewall Policy :

This is the **Firewall Policy for LAN to Internet access with Source NAT (SNAT)**. The policy, named **PC1-SNAT**, allows traffic originating from the `PC-1` address object on the **LAN_1 (port2)** interface to exit through the **port1** (WAN) interface. Crucially, **Source NAT is enabled** using the `Use Outgoing Interface Address` setting, which translates the private source IP (10.0.0.2) to the FortiGate's public WAN IP address.



Edit Policy

Name: PC1-SNAT

Incoming Interface: LAN_1 (port2)

Outgoing Interface: port1

Source: PC-1

Destination: all

Schedule: always

Service: ALL

Action: ✓ ACCEPT | DENY

Inspection Mode: Flow-based | Proxy-based

Firewall / Network Options

NAT: ●

IP Pool Configuration: Use Outgoing Interface Address | Use Dynamic IP Pool

Preserve Source Port

Protocol Options: PROT default

Security Profiles

AntiVirus

Web Filter

DNS Filter

Application Control

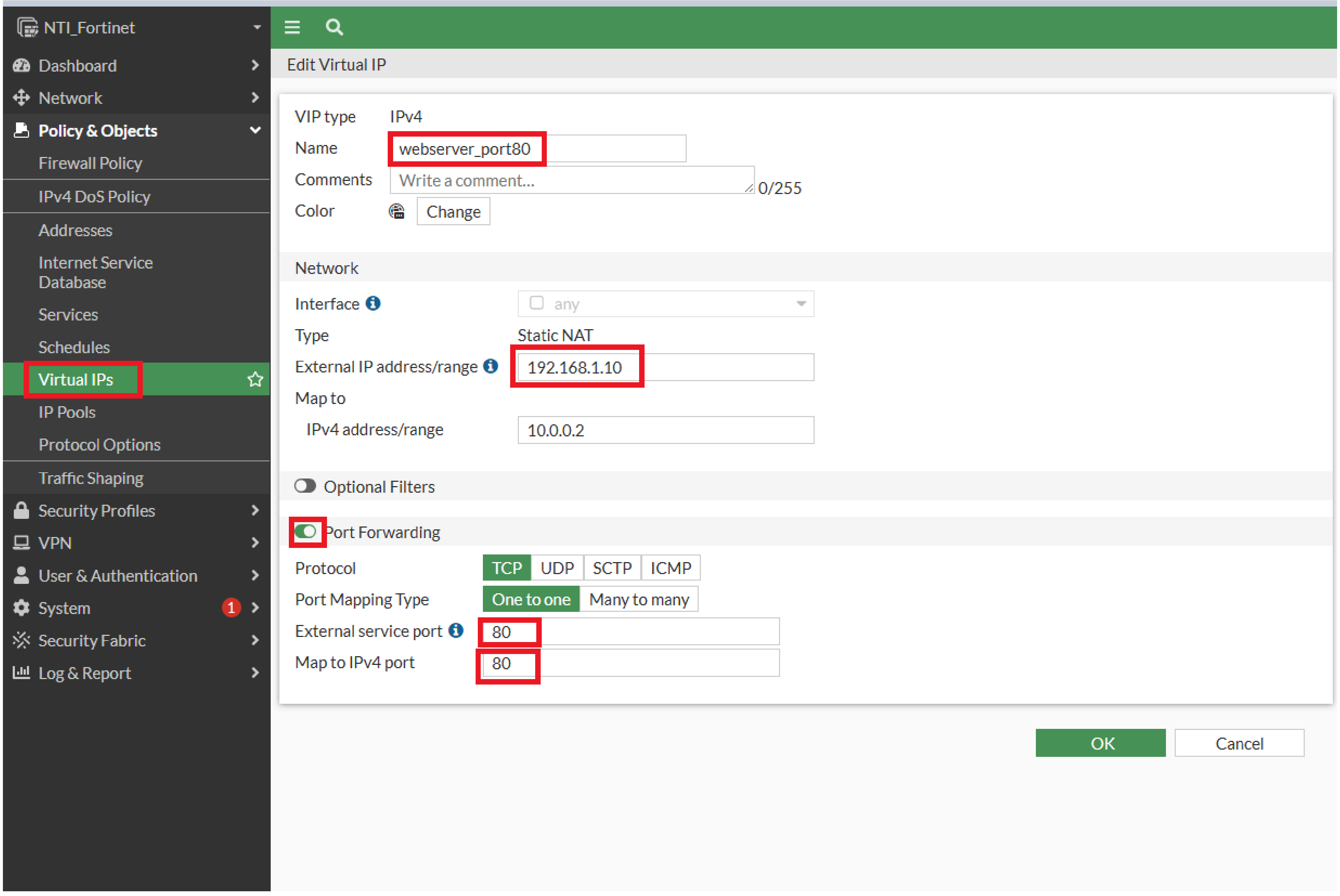
IPS

File Filter

3. Destination NAT / Port Forwarding

VIPs (Virtual IPs)

A **Virtual IP (VIP)** object named **webserver_port80** is created for **Destination NAT (DNAT)** or Port Forwarding. It maps the external WAN IP (192.168.1.10) to the internal web server's IP (10.0.0.2). **Port Forwarding is configured** for **TCP** traffic, translating the **External service port 80** to the **Internal port 80** on the server.



Edit Virtual IP

VIP type IPv4
Name webserver_port80
Comments Write a comment... 0/255
Color Change

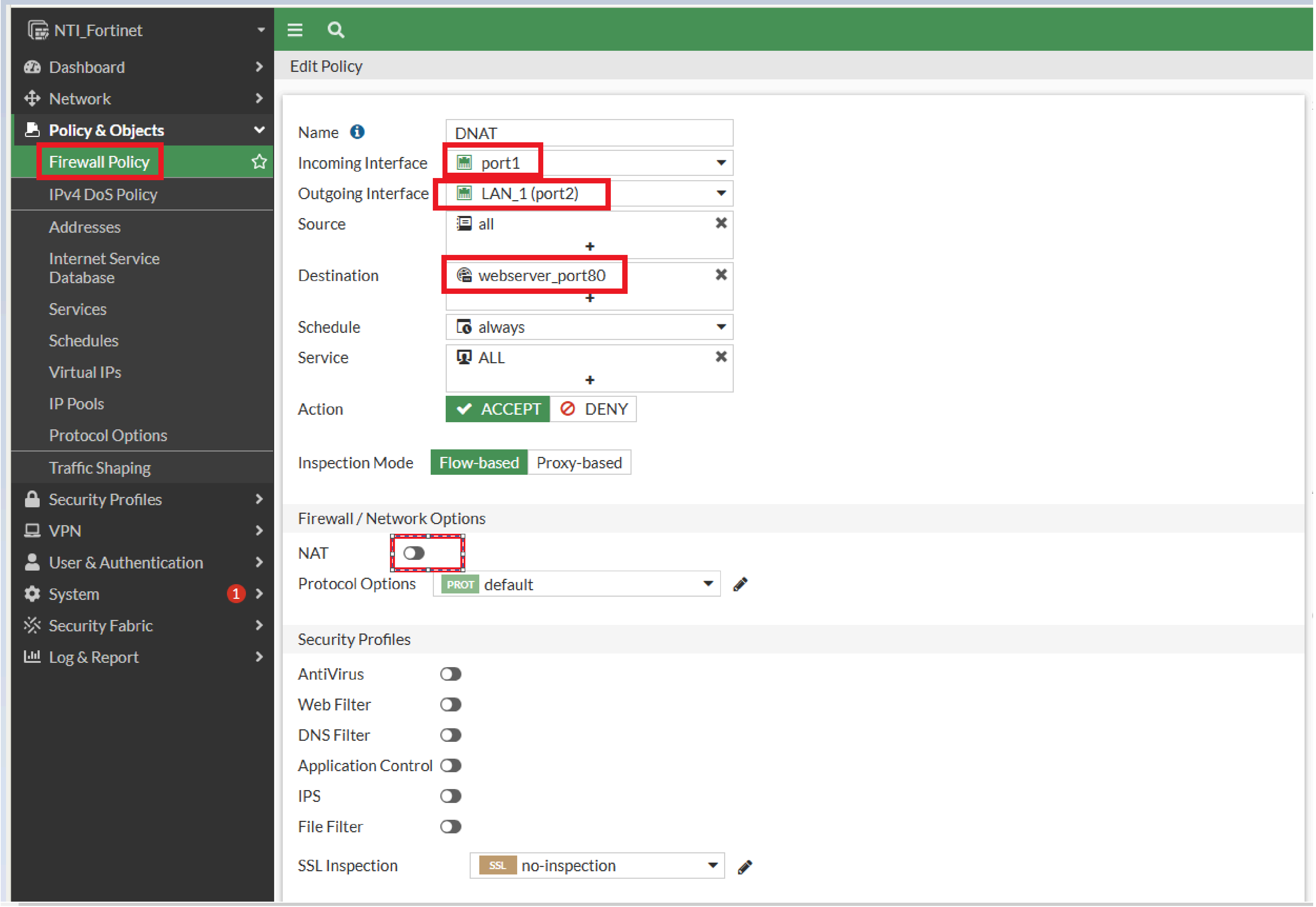
Network
Interface any
Type Static NAT
External IP address/range 192.168.1.10
Map to
IPv4 address/range 10.0.0.2

Optional Filters

Port Forwarding
Protocol TCP UDP SCTP ICMP
Port Mapping Type One to one Many to many
External service port 80
Map to IPv4 port 80

DNAT Policy

This policy, named **DNAT**, facilitates external access to the internal web server. It allows incoming traffic from the **port1** (WAN) interface to the **LAN_1 (port2)** interface. The **Destination** is set to the `webserver_port80` **Virtual IP** object. The use of the VIP handles the IP and port translation (DNAT), so the **NAT option is intentionally disabled** within the policy itself.



Edit Policy

Name DNAT
Incoming Interface port1
Outgoing Interface LAN_1 (port2)
Source all
Destination webserver_port80
Schedule always
Service ALL
Action ✓ ACCEPT ⊘ DENY

Inspection Mode Flow-based Proxy-based

Firewall / Network Options
NAT
Protocol Options PROT default

Security Profiles
AntiVirus
Web Filter
DNS Filter
Application Control
IPS
File Filter
SSL Inspection SSL no-inspection

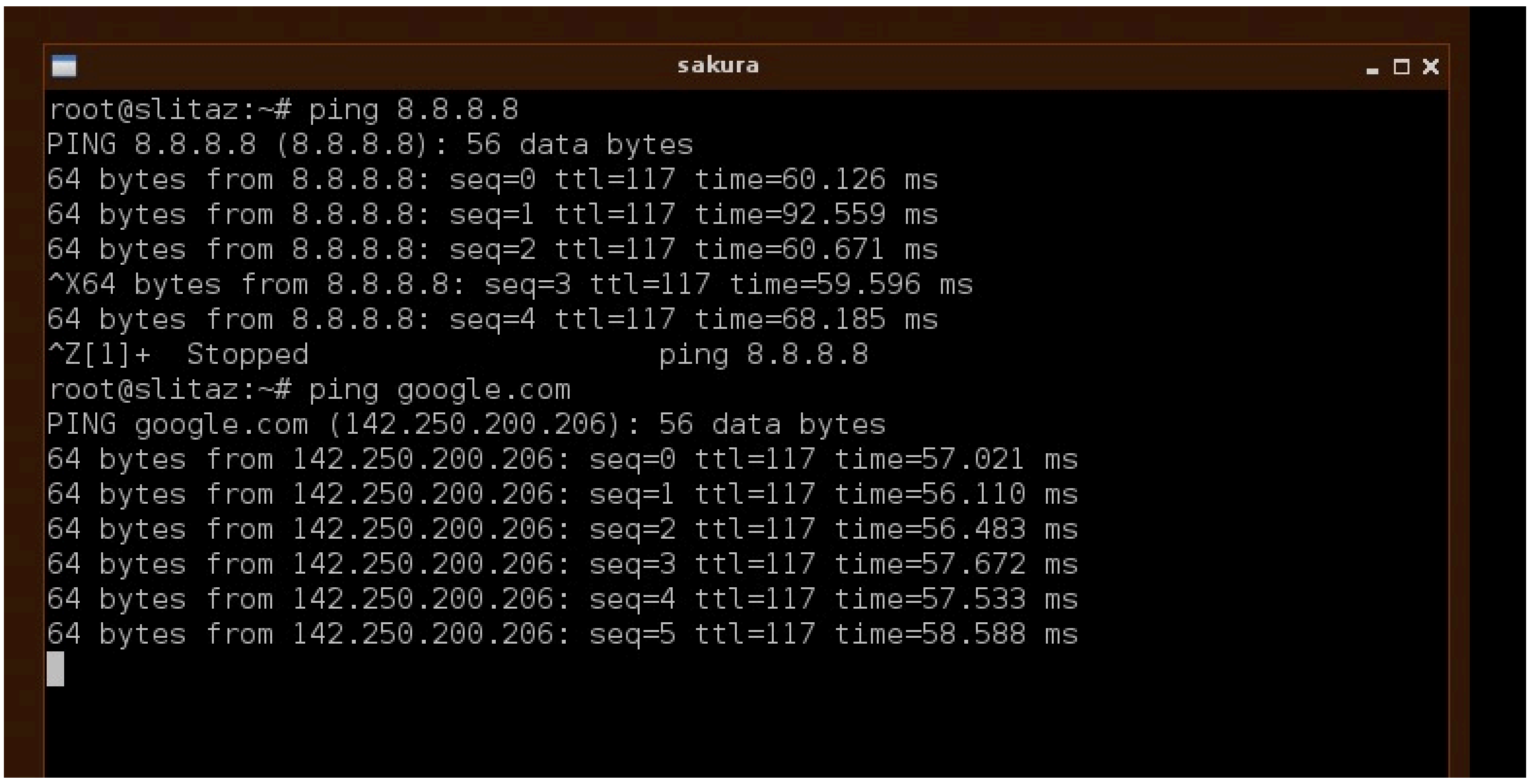
Source NAT Verification

confirms the successful configuration and function of the **Source NAT (SNAT)** policy allowing the internal host (10.0.0.2 or similar internal IP) to reach the Internet.

The host successfully executed two connectivity tests:

1. **Ping to** 8.8.8.8 **(Google DNS):** The internal host received successful replies from the public IP address 8.8.8.8.
2. **Ping to** `google.com` **:** The host successfully resolved the domain name to the public IP address 142.250.200.206 and received successful ping replies.

These results verify that the FortiGate is correctly applying the **PC1-SNAT Policy** and translating the internal private IP address of the source device to its public WAN interface IP, thereby enabling full outbound Internet access.

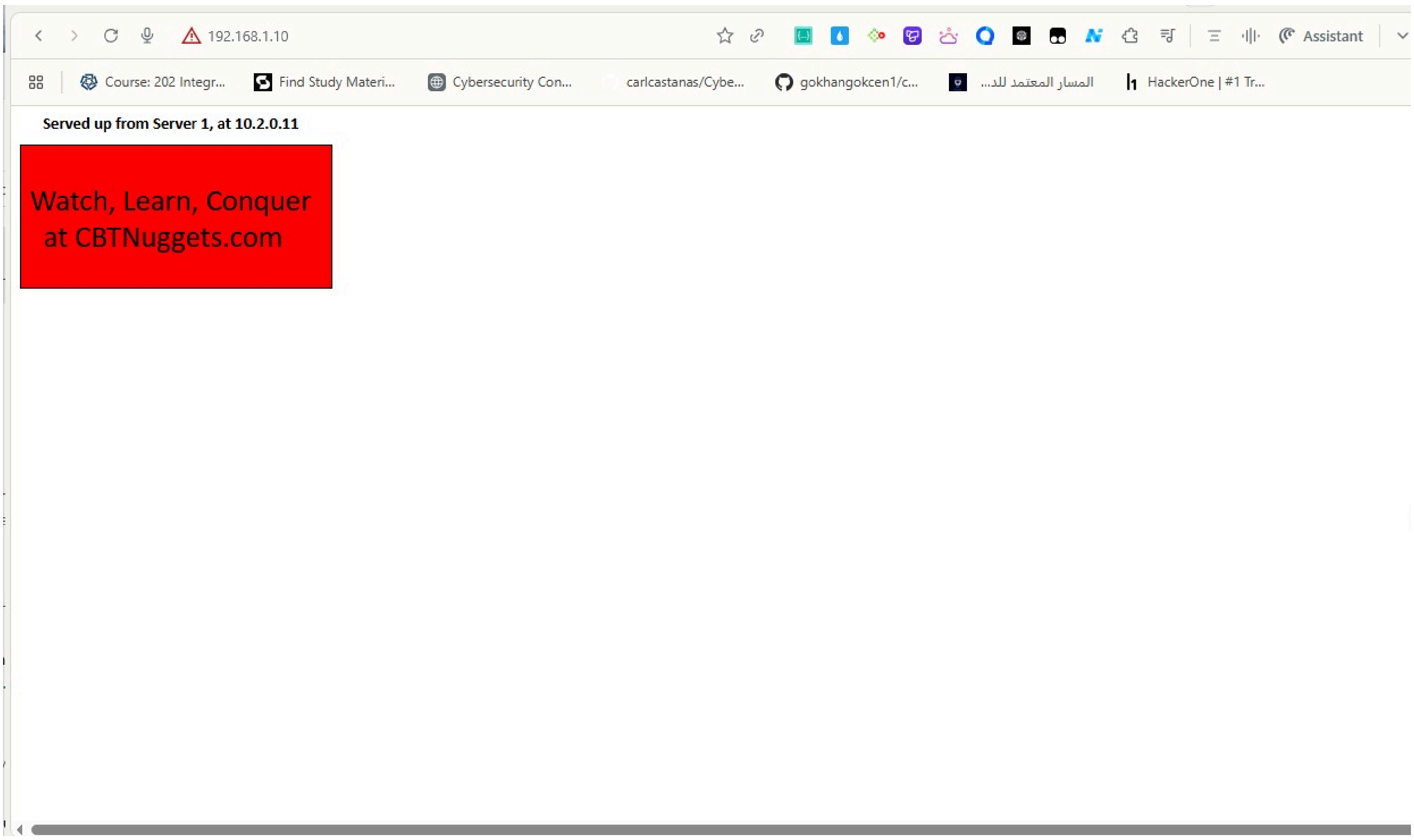


```
root@slitaz:~# ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8): 56 data bytes
64 bytes from 8.8.8.8: seq=0 ttl=117 time=60.126 ms
64 bytes from 8.8.8.8: seq=1 ttl=117 time=92.559 ms
64 bytes from 8.8.8.8: seq=2 ttl=117 time=60.671 ms
^X64 bytes from 8.8.8.8: seq=3 ttl=117 time=59.596 ms
64 bytes from 8.8.8.8: seq=4 ttl=117 time=68.185 ms
^Z[1]+  Stopped                    ping 8.8.8.8
root@slitaz:~# ping google.com
PING google.com (142.250.200.206): 56 data bytes
64 bytes from 142.250.200.206: seq=0 ttl=117 time=57.021 ms
64 bytes from 142.250.200.206: seq=1 ttl=117 time=56.110 ms
64 bytes from 142.250.200.206: seq=2 ttl=117 time=56.483 ms
64 bytes from 142.250.200.206: seq=3 ttl=117 time=57.672 ms
64 bytes from 142.250.200.206: seq=4 ttl=117 time=57.533 ms
64 bytes from 142.250.200.206: seq=5 ttl=117 time=58.588 ms
```

Destination NAT (Port Forwarding) Verification**

verifies the successful configuration and function of the **Destination NAT (DNAT)** or **Port Forwarding** rule using the Virtual IP (VIP)

- **Access Method:** The user successfully accessed the internal web server by browsing the FortiGate's **External WAN IP:** 192.168.1.10.
- **Result:** The browser successfully loaded the web page. The content explicitly states, **"Served up from Server 1, at** 10.2.0.11 **,"** confirming that the traffic was successfully redirected by the FortiGate.
- **Verification:** This confirms that the incoming request on the WAN interface (192.168.1.10:Port 80) was correctly mapped by the **Virtual IP (VIP)** object to the internal server's private IP (10.2.0.11:Port 80) as intended by the **DNAT Policy**.



Served up from Server 1, at 10.2.0.11

Watch, Learn, Conquer at CBTNuggets.com