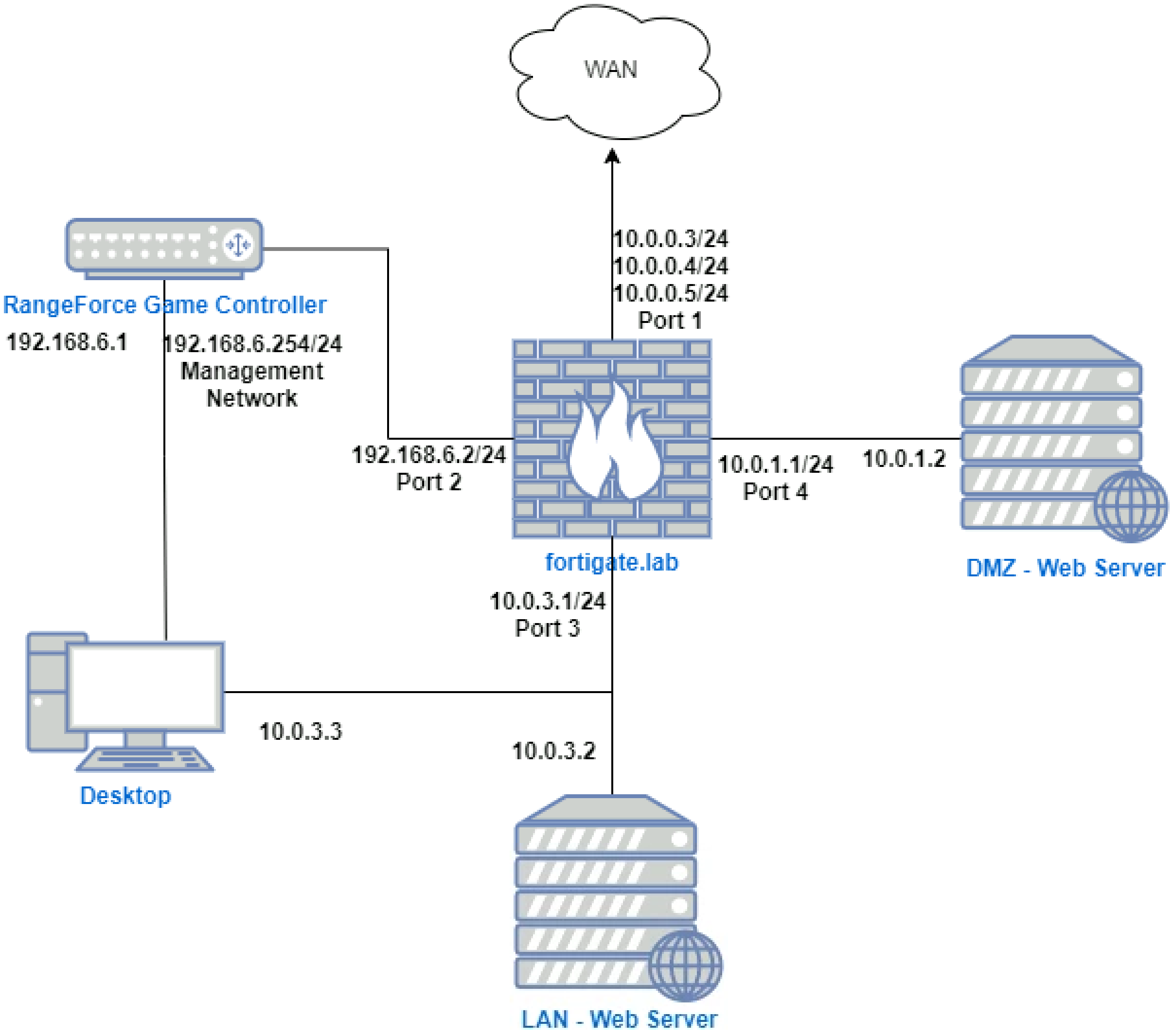
Network Topology



Module Description

- You have been recently hired as a junior network engineer at Commensurate Technology. It is your first day and you met your supervisor, the senior network administrator.
- The corporation is setting up a new location protected by a Fortinet firewall. This project is very important for the company because it will help ensure perimeter security standards across all sites.
- You are going to configure several forms of **Source NAT** in this module. This improves on ***having one single NAT rule for the whole LAN*** because separating out the SNAT rules for servers and other specific hosts gives more control and visibility.
- For example, it allows for more filtering rules and protection profiles for different classes of systems.

NAT Review

- To review from the NAT concepts module, **Network Address Translation(NAT)** is an important function performed by firewalls.
- When working with IPv4, NAT is done to permit private LAN addresses (e.g., 192.186.1.45) to reach the Internet, or to let Internet clients access servers inside local LANs.

  - So I guess in this case, the firewall in here both act as a router and a firewall? But mainly firewall? Or does the "WAN" part in the topology section assumes that it includes the router? Is the router in default mode or in bridge mode? (???)
- **Source NAT** is the process that ***enables*** the firewall to translate the local private IP addresses into a publicly-routable IP address to permit Internet access.

  ```
  - Note that technically, when a request is sent by a client from a local LAN to
  the outside world(Internet), in this case, it is the firewall that sends it to
  the Internet on the client's behalf. Thus, when the response from the Internet is
  sent back to the client, it does NOT know who the client is, but the **publicly
  facing** router/firewall.
  ```
- The public IP addresses are configured on the firewall and are assigned by the ISP.
  → This is why its important to protect your public IP otherwise, you'll become susceptible to so much attacks!
  → But what if the case is that everyone knows your public IP address? Can you create a computer system such that it can withstand attacks? Like **Bastion** from Azure?
- To handle **Source Network Address Translation**(SNAT), the firewall keeps track of the relation between private IP addresses and public IP addresses.
- This data is added into a table and stored in the memory.

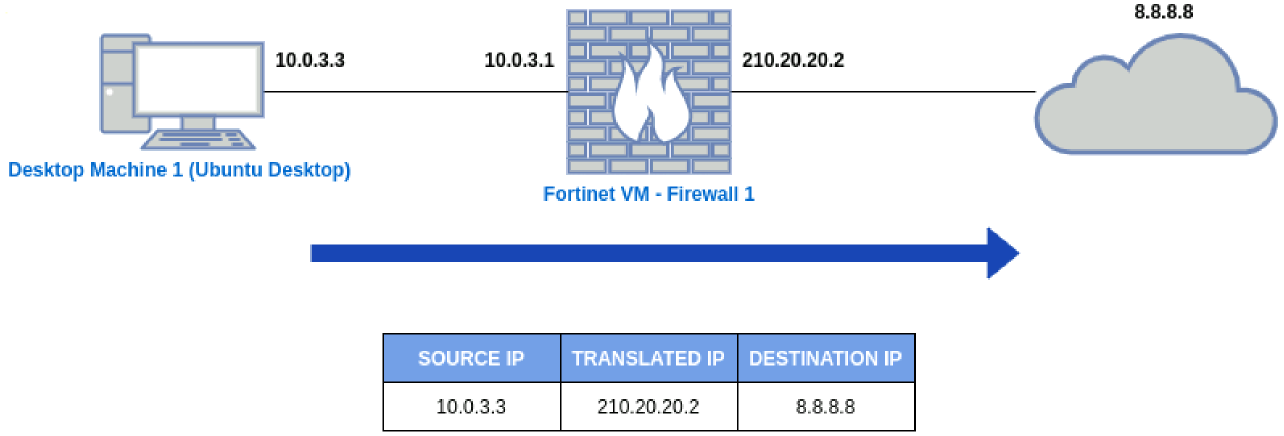
  ```
  - Since firewalls have memories, shouldn't it be susceptible to attacks as well
  instead of something hackers have to circumvent? How exactly are firewall OSes
  different than of normal OSes like Linux or Windows?
  ```
- We can distinguish between different typees of source NAT, mainly:

1. **One-to-one**
2. **Many-to-many**
3. **Overload NAT** (Port Address Translation(PAT))

One-To-One

- This translation is done from one single private IP address to one only public IP address.

- It is usually done to map private server addresses to public ones.



SOURCE IP	TRANSLATED IP	DESTINATION IP
10.0.3.3	210.20.20.2	8.8.8.8

Many-to-Many

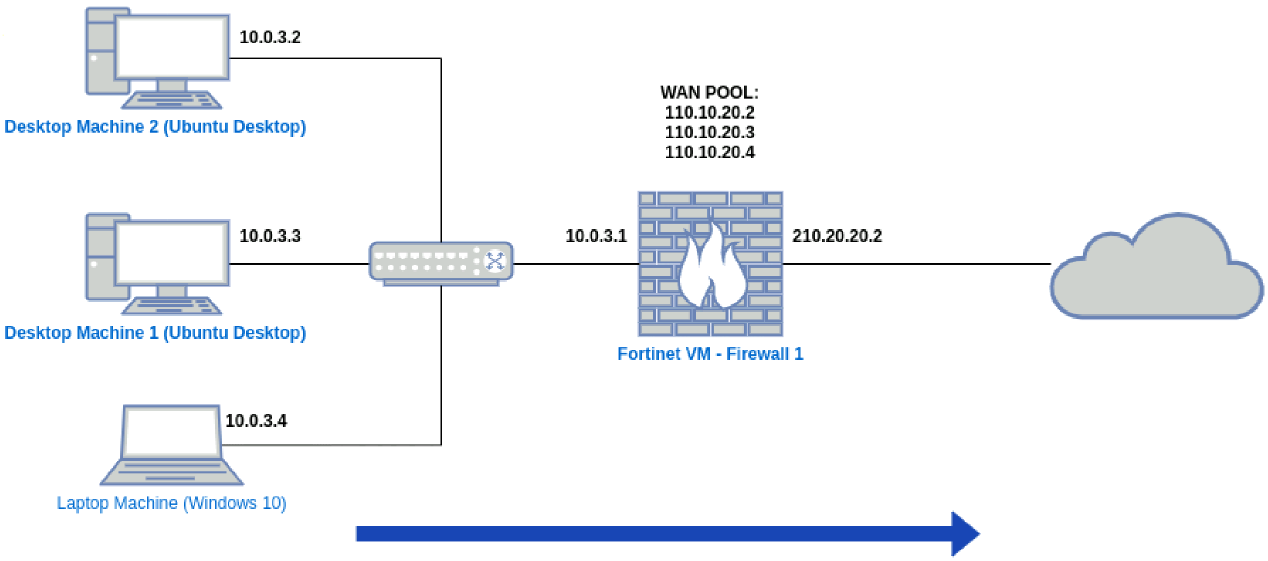
- Many-to-many NAT expands upon one-to-one when there are many addresses or even an entire network that needs to be translated.

- However, it still requries the same number of public and private IP addresses, thus, if there are 10 hosts on the LAN that need to reach the Internet, it would be ***necessary*** to have 10 public IP addresses.

```
- How can one have multiple public IP addresses? Do I ask my ISP and request for
different public IP address for multiple users in my network?
```

- Public IP addresses are handled and assigned by ***pools***. (what pools? like thread pool?)

- A **public pool** is a group of IP addresses that are assigned by the ISP from network segments.



SOURCE IP	TRANSLATED IP	DESTINATION IP
10.0.3.2	110.10.20.2	8.8.8.8
10.0.3.3	110.10.20.3	8.8.8.8
10.0.3.4	110.10.20.4	8.8.8.8

```
 - Notice that in this case, the public IP of the firewall wasn't applied to the
clients but different IP addresses from the WAN pool. Is this something that ISP
"normally" does? Or do you have to request for it?

- Also, if you try to check your public IP address, say from "whatsmyip" or
"dnsleaktest", would it show the IP provided to you by the ISP from the WAN pool?
```

Overload NAT

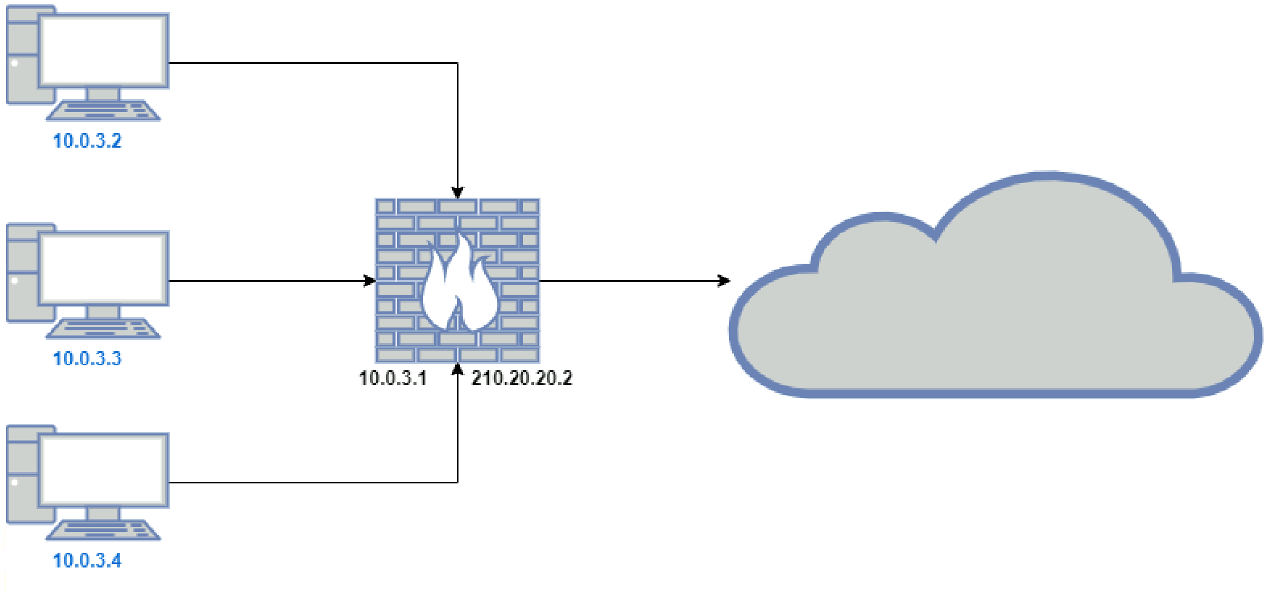
- **Overload NAT** enables us to overcome the restrictions(what restrictions?) of the **many-to-many** NAT.
- Using this technique, it is possible to translate many private LAN addresses to just one public IP.

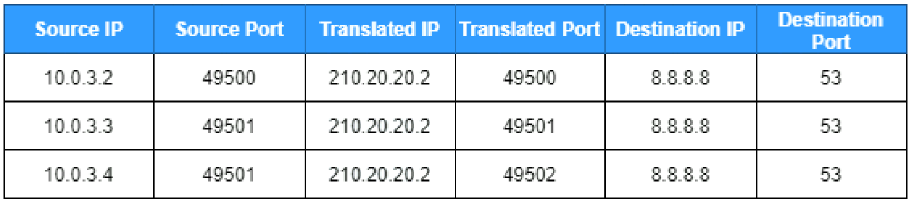
```
- So basically a **many-to-one** type of translation?
```

- This technique requires rewriting the source ports of outbound packets so that connections coming from different LAN hosts will have different source ports when sent out over the WAN.

```
- Does this make the "source ports" the identifier for each of different LAN
hosts? Yes.
```

- This then allows determining the correct destination LAN IP for incoming reply packets by checking their destination port against the mapping of source LAN IP to source port.





Source IP	Source Port	Translated IP	Translated Port	Destination IP	Destination Port
10.0.3.2	49500	210.20.20.2	49500	8.8.8.8	53
10.0.3.3	49501	210.20.20.2	49501	8.8.8.8	53
10.0.3.4	49501	210.20.20.2	49502	8.8.8.8	53

```
- So the only difference between Overload NAT and Many-to-many is that the
overload NAT does not use multiple IP addresses but uses different source ports
instead which makes it more convenient in a way?
```

Configuring Firewall

- It is time to configure the policies for the new firewall to protect the LAN and corporate servers located behind it.

- The network administrator created a network scheme with a three-zone distribution:

```
 1. LAN
 2. WAN
 3. DMZ
```

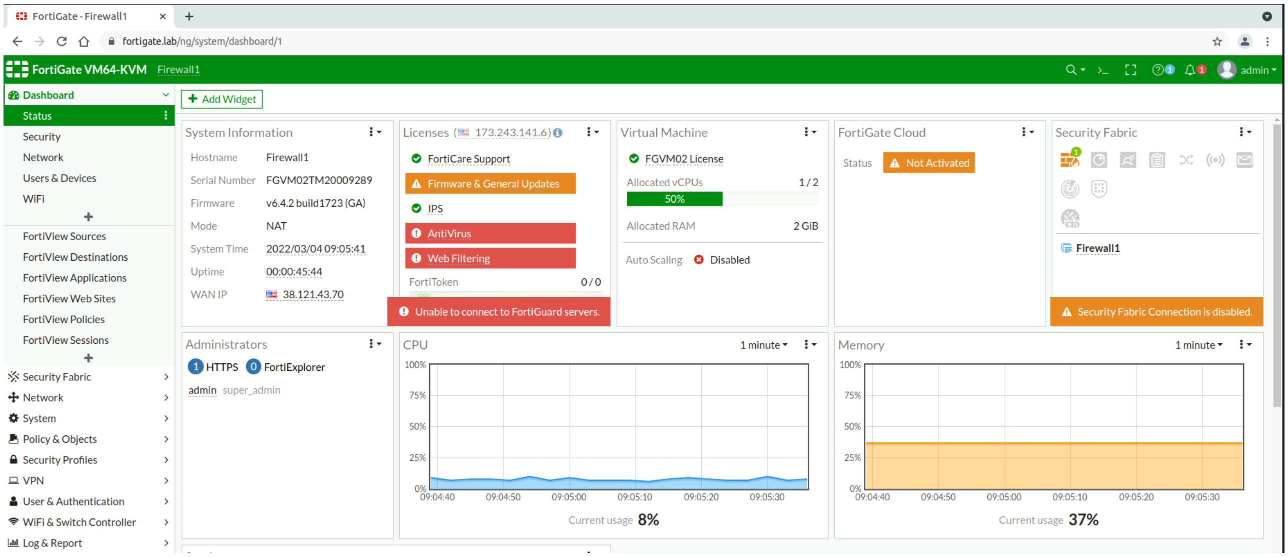
- There are two servers that form part of a vacation planner system for company employees.

- These servers are configured in a frontend-backend architecture.

- The **DMZ - Web Server** is going to act as the frontend, receiving the connections from the Internet.

Objective:

- Just login!



System Information

Hostname Firewall1
Serial Number FGVM02TM20009289
Firmware v6.4.2 build1723 (GA)
Mode NAT
System Time 2022/03/04 09:05:41
Uptime 00:00:45:44
WAN IP 38.121.43.70

Licenses (173.243.141.6)

FortiCare Support
Firmware & General Updates
IPS
AntiVirus
Web Filtering
FortiToken 0 / 0
Unable to connect to FortiGuard servers.

Virtual Machine

FGVM02 License
Allocated vCPUs 1 / 2
50%
Allocated RAM 2 GiB
Auto Scaling Disabled

FortiGate Cloud

Status Not Activated

Security Fabric

Firewall1
Security Fabric Connection is disabled.

Administrators

1 HTTPS 0 FortiExplorer
admin super_admin

CPU Current usage 8%

Memory Current usage 37%

Objects Creation (Note that this is under "Addresses"!)

- You need to start by creating 3 different objects for each **source NAT policies**.

- These objects will refer to the:

  - **DMZ - Web Server**
  - **LAN - Web Server**
  - **LAN (users)**

Objectives:

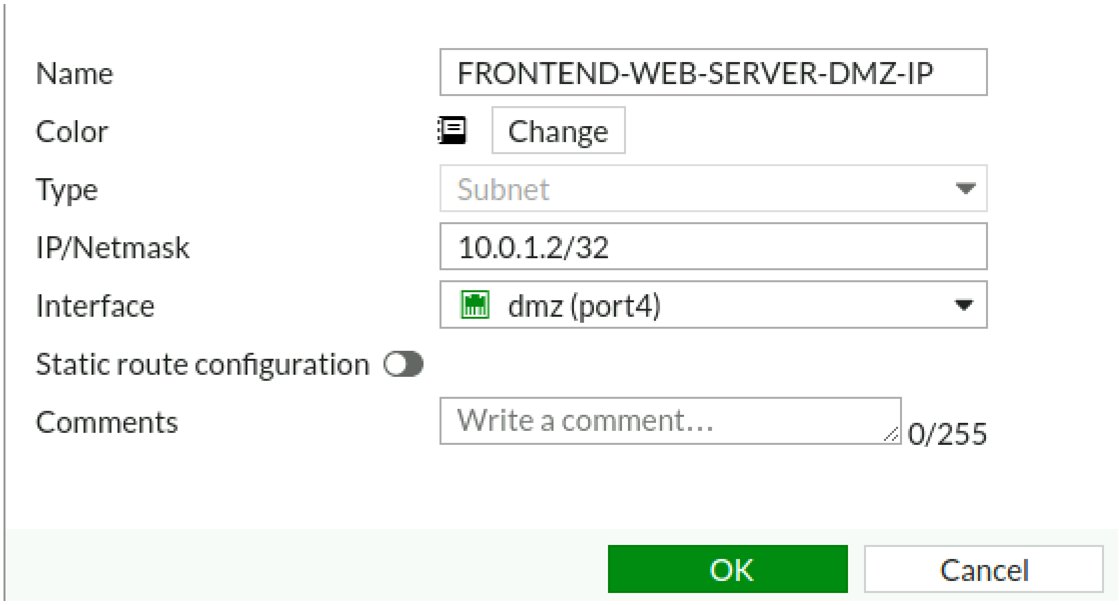
- Create an object for the IP address of **DMZ - Web Server**.
  - Create a new object with the following data:
    - Name: **FRONTEND-WEB-SERVER-DMZ-IP**
    - Subnet/IP Range: DMZ - Web Server IP
    - Interface: **DMZ (port4)**

- Create an object for the IP address of **LAN - Web Server**.
  - Create a new object with the following data:
    - Name: **BACKEND-WEB-SERVER-LAN-IP**
    - Subnet/IP Range: LAN - Web Server IP
    - Interface: **LAN (port3)**

- Create an object for the IP address of the **LAN** machines (the IP address of the network).
  - Create a new object with the following data:
    - Name: **LAN-machines**
    - Subnet/IP Range: LAN Network IP
    - Interface: **LAN (port3)**

0. First, go to the **Policy & Objects > IP Pools > "+Create New"**

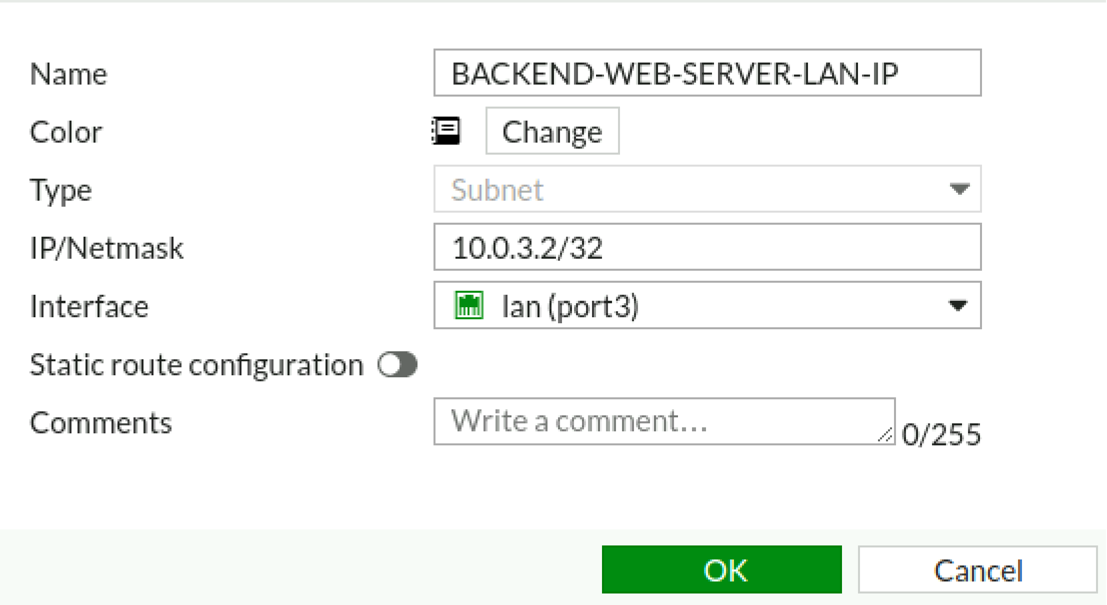
1. Setup for the DMZ (frontend)



Name	FRONTEND-WEB-SERVER-DMZ-IP
Color	Change
Type	Subnet
IP/Netmask	10.0.1.2/32
Interface	dmz (port4)
Static route configuration	○
Comments	Write a comment… 0/255

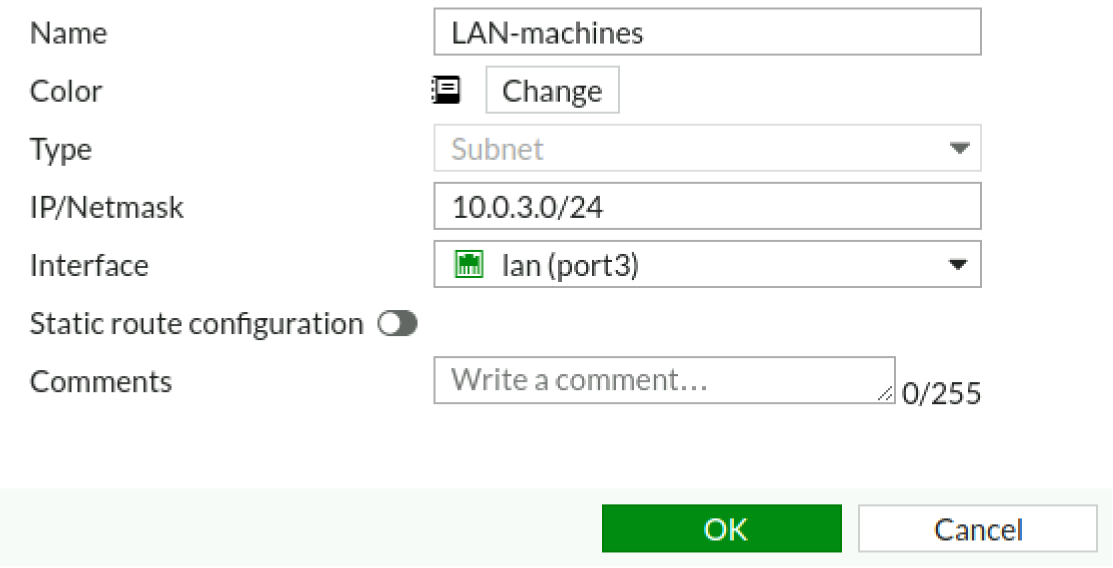
→ Note that since there is only a single machine for the DMZ, we use /32 as it states that in that network, there is only a **single** IPv4 address that we are referring to! (/24 means that there are 256 machines in the network. (I think?))

2. Setup for the LAN server (backend)



Name	BACKEND-WEB-SERVER-LAN-IP
Color	Change
Type	Subnet
IP/Netmask	10.0.3.2/32
Interface	lan (port3)
Static route configuration	○
Comments	Write a comment… 0/255

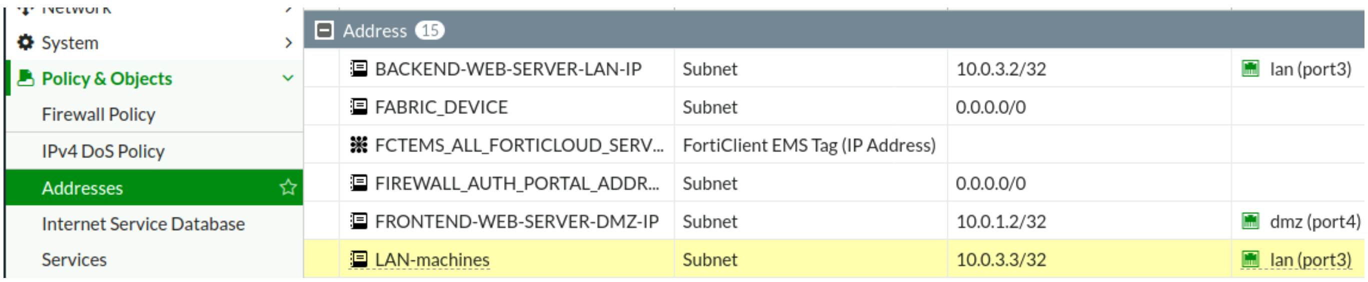
3. Setup for the LAN machine (LAN users)



Name	LAN-machines
Color	Change
Type	Subnet
IP/Netmask	10.0.3.0/24
Interface	lan (port3)
Static route configuration	○
Comments	Write a comment... 0/255

→ Notice that for the LAN machines, we use /24 since we expect the network to have multiple users!

New Addresses Added:



Address 15

BACKEND-WEB-SERVER-LAN-IP	Subnet	10.0.3.2/32	lan (port3)
FABRIC_DEVICE	Subnet	0.0.0.0/0	
FCTEMS_ALL_FORTICLOUD_SERV...	FortiClient EMS Tag (IP Address)		
FIREWALL_AUTH_PORTAL_ADDR...	Subnet	0.0.0.0/0	
FRONTEND-WEB-SERVER-DMZ-IP	Subnet	10.0.1.2/32	dmz (port4)
LAN-machines	Subnet	10.0.3.3/32	lan (port3)

IP Pools Creation

- **IP pools** are similar to objects but the key difference is that they are always related to public IP addresses.
- They are used when there is a need to link a group of private IP addresses (objects) to a group of public IP addresses (pools).

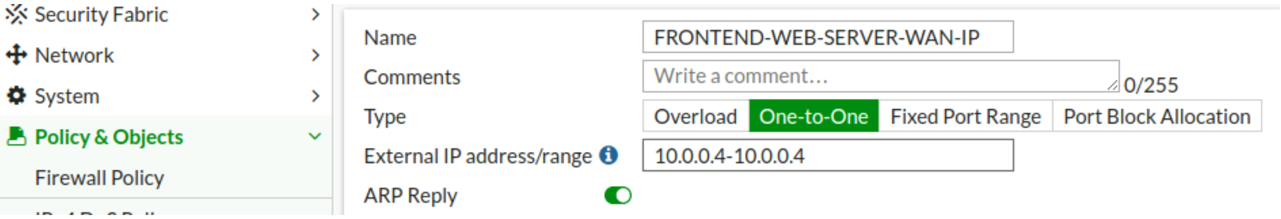
```
- Here comes the SNAT!
```

→ In this step, you have to create two IP pools in order to NAT the DMZ and LAN Web servers ***to two separate public IP addresses***.

Objectives:

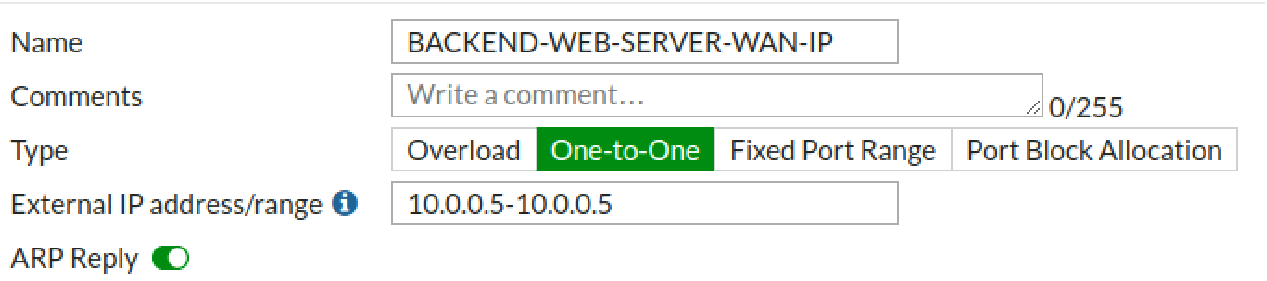
- Create an **IP pool** for the WAN IP address of the **DMZ - Web Server**.
  - Name: **FRONTEND-WEB-SERVER-WAN-IP**
  - Type: **One-to-One**
  - Define an **External Pool** with the first and last IP to the address **10.0.0.4**.
- Create an **IP Pool** for the WAN IP address of the **LAN - Web Server**.
  - Name: **BACKEND-WEB-SERVER-WAN-IP**
  - Type: **One-to-One**
  - Define an **External Pool** with the first and last IP to the address **10.0.0.5**.

1. Creating a public IP for the DMZ server:



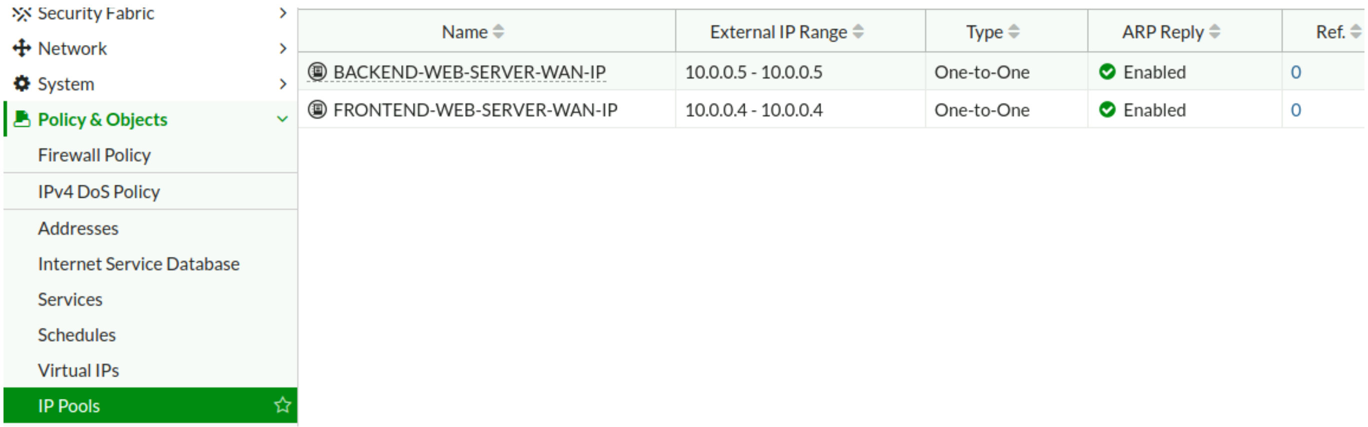
Name	FRONTEND-WEB-SERVER-WAN-IP
Comments	Write a comment... 0/255
Type	Overload [✓ One-to-One] Fixed Port Range Port Block Allocation
External IP address/range	10.0.0.4-10.0.0.4
ARP Reply	●

2. Creating a public IP for the LAN web server:



Name	BACKEND-WEB-SERVER-WAN-IP
Comments	Write a comment... 0/255
Type	Overload [✓ One-to-One] Fixed Port Range Port Block Allocation
External IP address/range	10.0.0.5-10.0.0.5
ARP Reply	●

Result:



Name	External IP Range	Type	ARP Reply	Ref.
BACKEND-WEB-SERVER-WAN-IP	10.0.0.5 - 10.0.0.5	One-to-One	✓ Enabled	0
FRONTEND-WEB-SERVER-WAN-IP	10.0.0.4 - 10.0.0.4	One-to-One	✓ Enabled	0

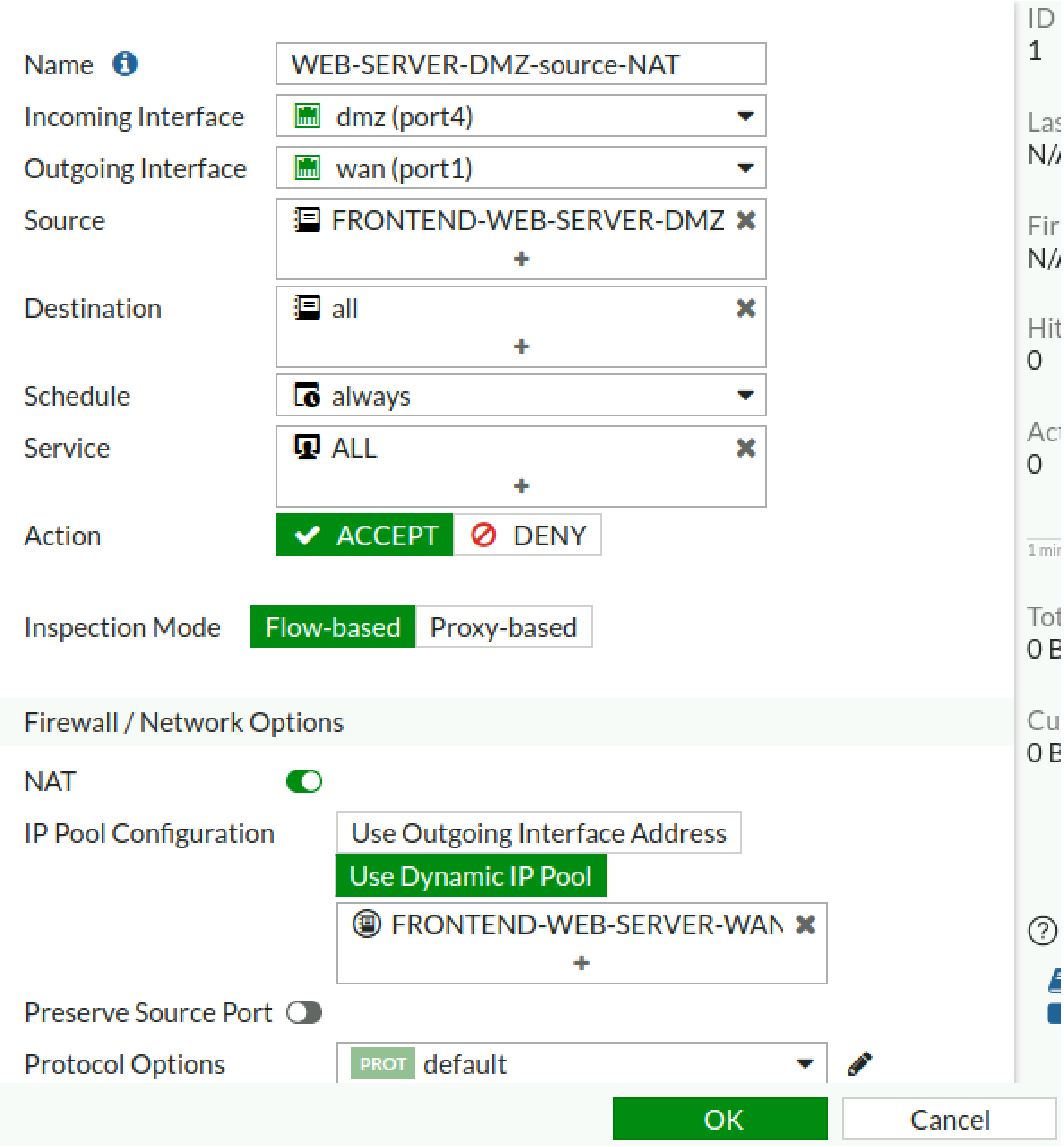
DMZ Server NAT Policy

- It is important that the **DMZ-Web Server** can reach(and be reached) the Internet with its own IP public address so you need to configure that next.

Objectives:

- Create a firewall policy with the following information to configure source NAT:
  - Name: **WEB-SERVER-DMZ-source-NAT**
  - Incoming Interface: **DMZ (port4)**
  - Outgoing Interface: **WAN (port1)**
  - Source: **FRONTEND-WEB-SERVER-DMZ-IP** (the created object)
  - Destination: **all** (since we want to access the Internet)
  - Schedule: **always**
  - Service: **ALL**
  - Action: Make sure that **ACCEPT** is marked here.
  - NAT: **enabled**
  - IP Pool Configuration: **FRONTEND-WEB-SERVER-WAN-IP**

Modification:



Name: WEB-SERVER-DMZ-source-NAT

Incoming Interface: dmz (port4)

Outgoing Interface: wan (port1)

Source: FRONTEND-WEB-SERVER-DMZ ✖ +

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]

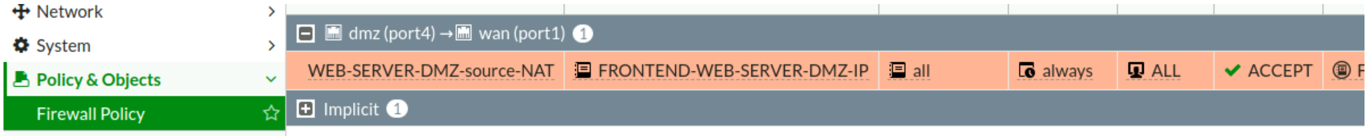
FRONTEND-WEB-SERVER-WAN ✖ +

Preserve Source Port: ○

Protocol Options: PROT default

→ In this way, the DMZ can now access the Internet and users from the Internet can access the web application provided by the web server.

Result:



Network
System
Policy & Objects
Firewall Policy

dmz (port4) → wan (port1) 1

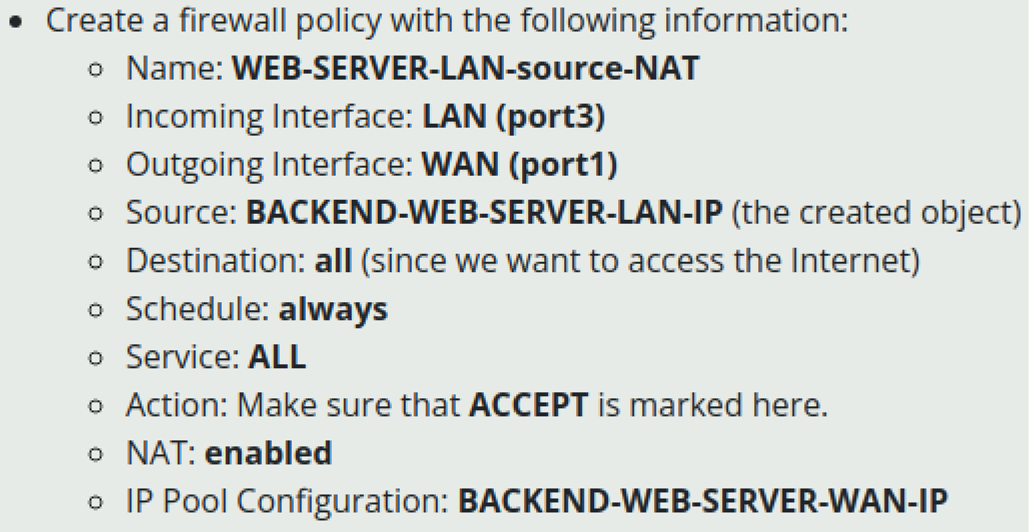
WEB-SERVER-DMZ-source-NAT	FRONTEND-WEB-SERVER-DMZ-IP	all	always	ALL	✓ ACCEPT	F

Implicit 1

LAN Server NAT Policy

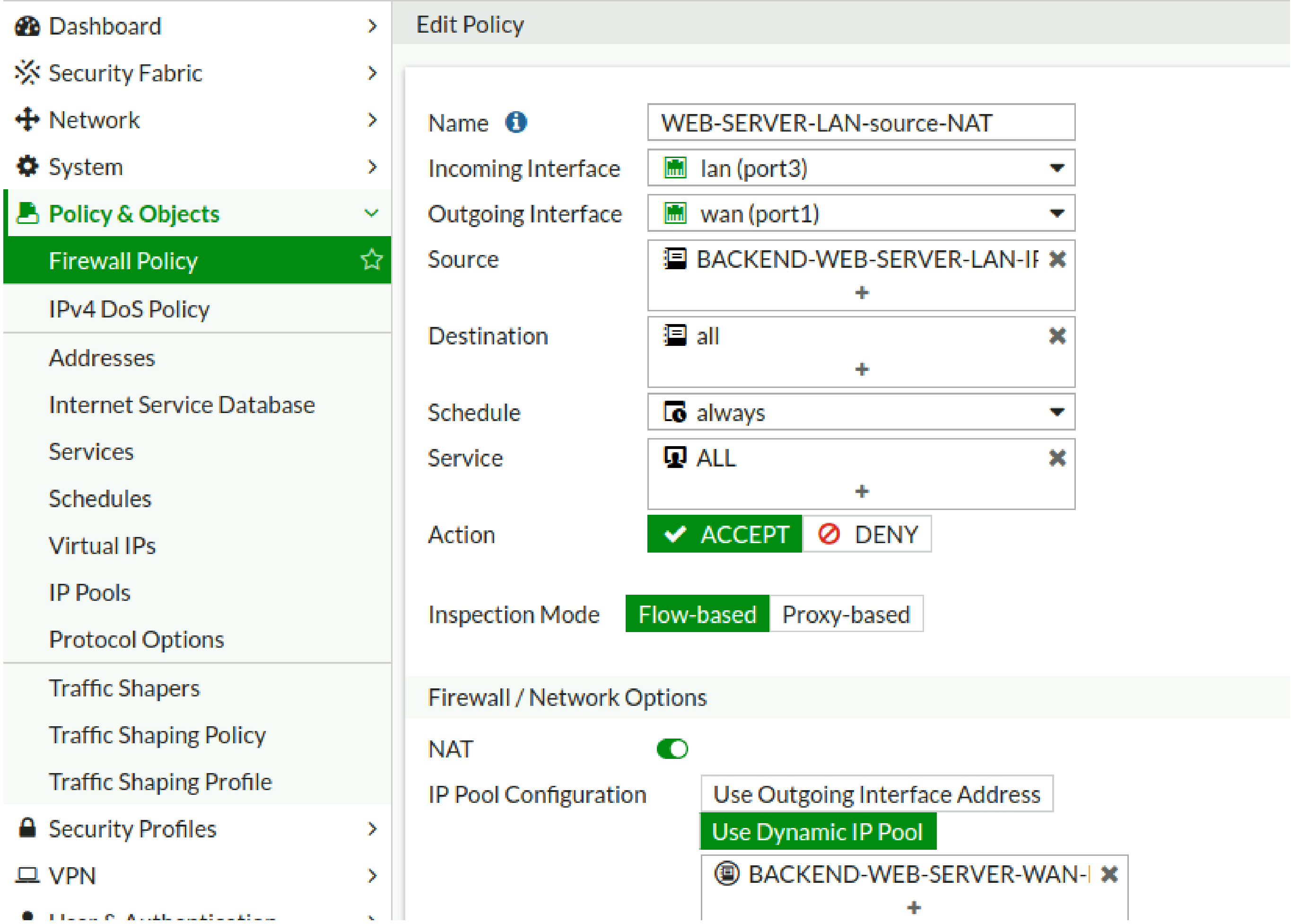
- Next, you need to configure the necessary rules to allow the **LAN Web Server** to access the Internet with its separate IP address.

Objectives:



- Create a firewall policy with the following information:
  - Name: **WEB-SERVER-LAN-source-NAT**
  - Incoming Interface: **LAN (port3)**
  - Outgoing Interface: **WAN (port1)**
  - Source: **BACKEND-WEB-SERVER-LAN-IP** (the created object)
  - Destination: **all** (since we want to access the Internet)
  - Schedule: **always**
  - Service: **ALL**
  - Action: Make sure that **ACCEPT** is marked here.
  - NAT: **enabled**
  - IP Pool Configuration: **BACKEND-WEB-SERVER-WAN-IP**

Result:



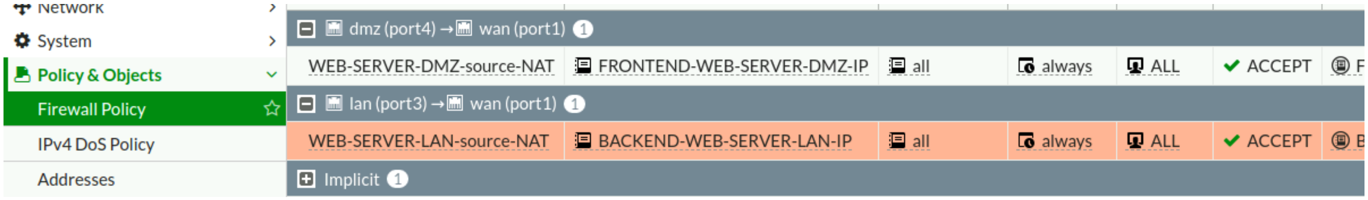
Edit Policy

Name: WEB-SERVER-LAN-source-NAT
Incoming Interface: lan (port3)
Outgoing Interface: wan (port1)
Source: BACKEND-WEB-SERVER-LAN-IF
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
BACKEND-WEB-SERVER-WAN-I

Final:



dmz (port4) → wan (port1) 1						
WEB-SERVER-DMZ-source-NAT	FRONTEND-WEB-SERVER-DMZ-IP	all	always	ALL	✓ ACCEPT	F
lan (port3) → wan (port1) 1						
WEB-SERVER-LAN-source-NAT	BACKEND-WEB-SERVER-LAN-IP	all	always	ALL	✓ ACCEPT	B
Implicit 1						

Question: How can the web application be connected to the backend then?

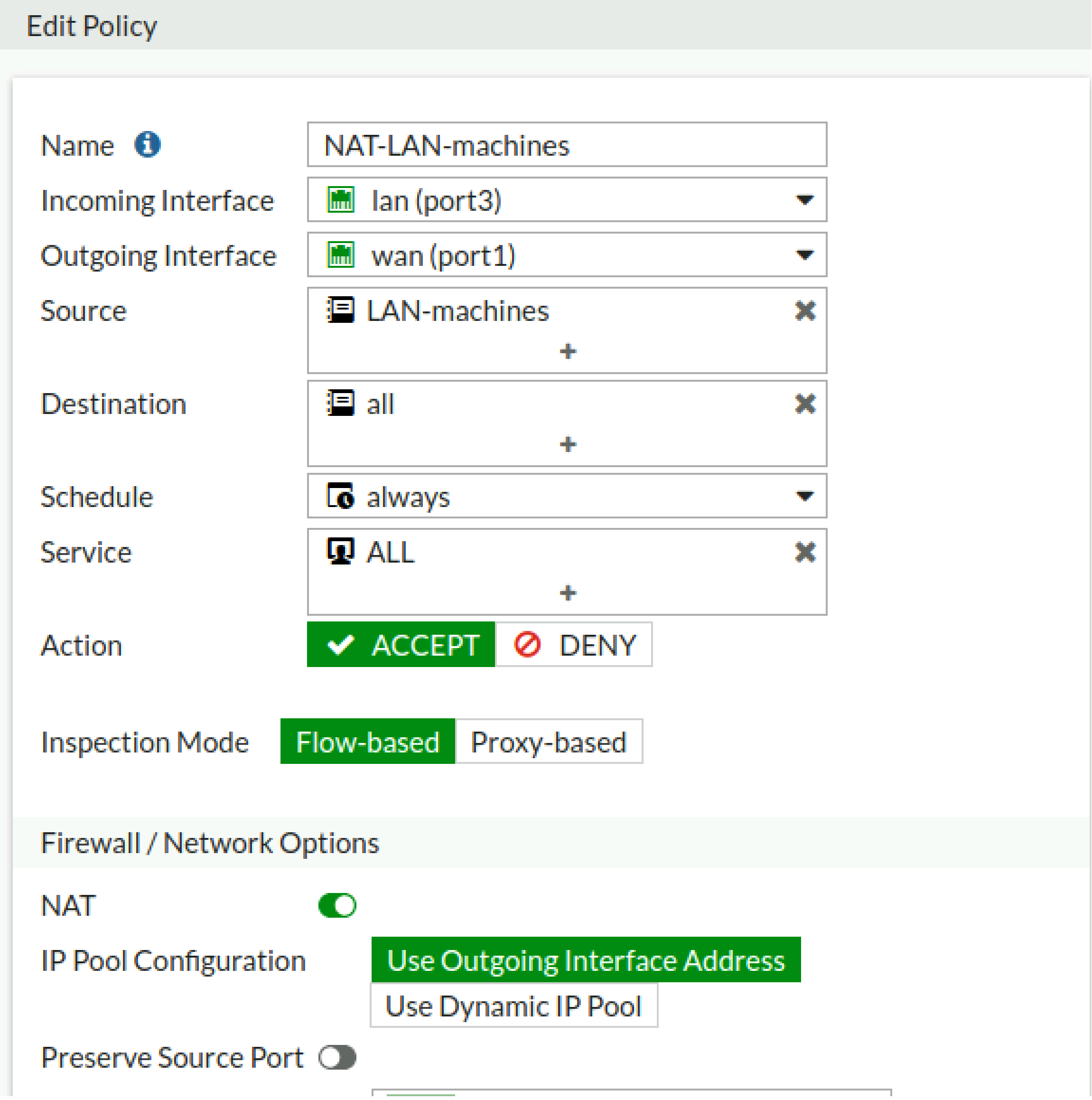
LAN Machines NAT Policy

- Finally, set up a rule to permit the rest of the LAN of Firewall1 to browse the Internet with the default WAN IP of the firewall.

Objectives:

- Create a firewall policy with the following information to permit the rest of the LAN machines:
  - Name: **NAT-LAN-machines**
  - Incoming Interface: **LAN (port3)**
  - Outgoing Interface: **WAN (port1)**
  - Source: **LAN-machines** (the created object)
  - Destination: **all** (since we want to access the Internet)
  - Schedule: **always**
  - Service: **ALL**
  - Action: Make sure that **ACCEPT** is marked here.
  - NAT: **enabled**
  - IP Pool Configuration: **Use Outgoing Interface Address**

Setup:



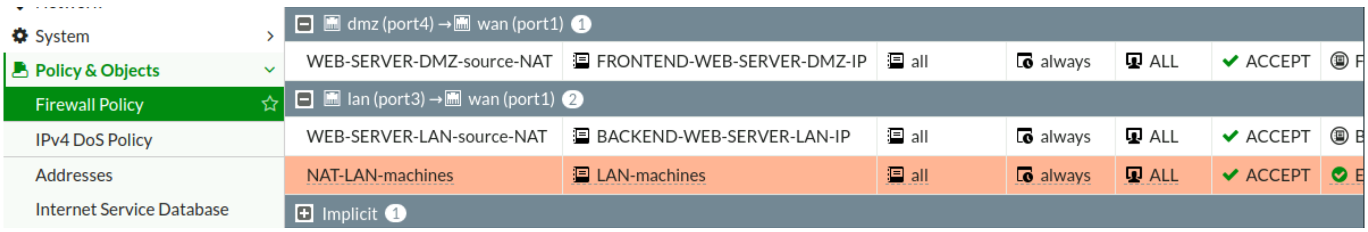
Edit Policy

Name	NAT-LAN-machines
Incoming Interface	lan (port3)
Outgoing Interface	wan (port1)
Source	LAN-machines
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	☐

Final:



⊟ dmz (port4) → wan (port1) 1						
WEB-SERVER-DMZ-source-NAT	FRONTEND-WEB-SERVER-DMZ-IP	all	always	ALL	✓ ACCEPT	F
⊟ lan (port3) → wan (port1) 2						
WEB-SERVER-LAN-source-NAT	BACKEND-WEB-SERVER-LAN-IP	all	always	ALL	✓ ACCEPT	B
NAT-LAN-machines	LAN-machines	all	always	ALL	✓ ACCEPT	✓ E
⊞ Implicit 1						