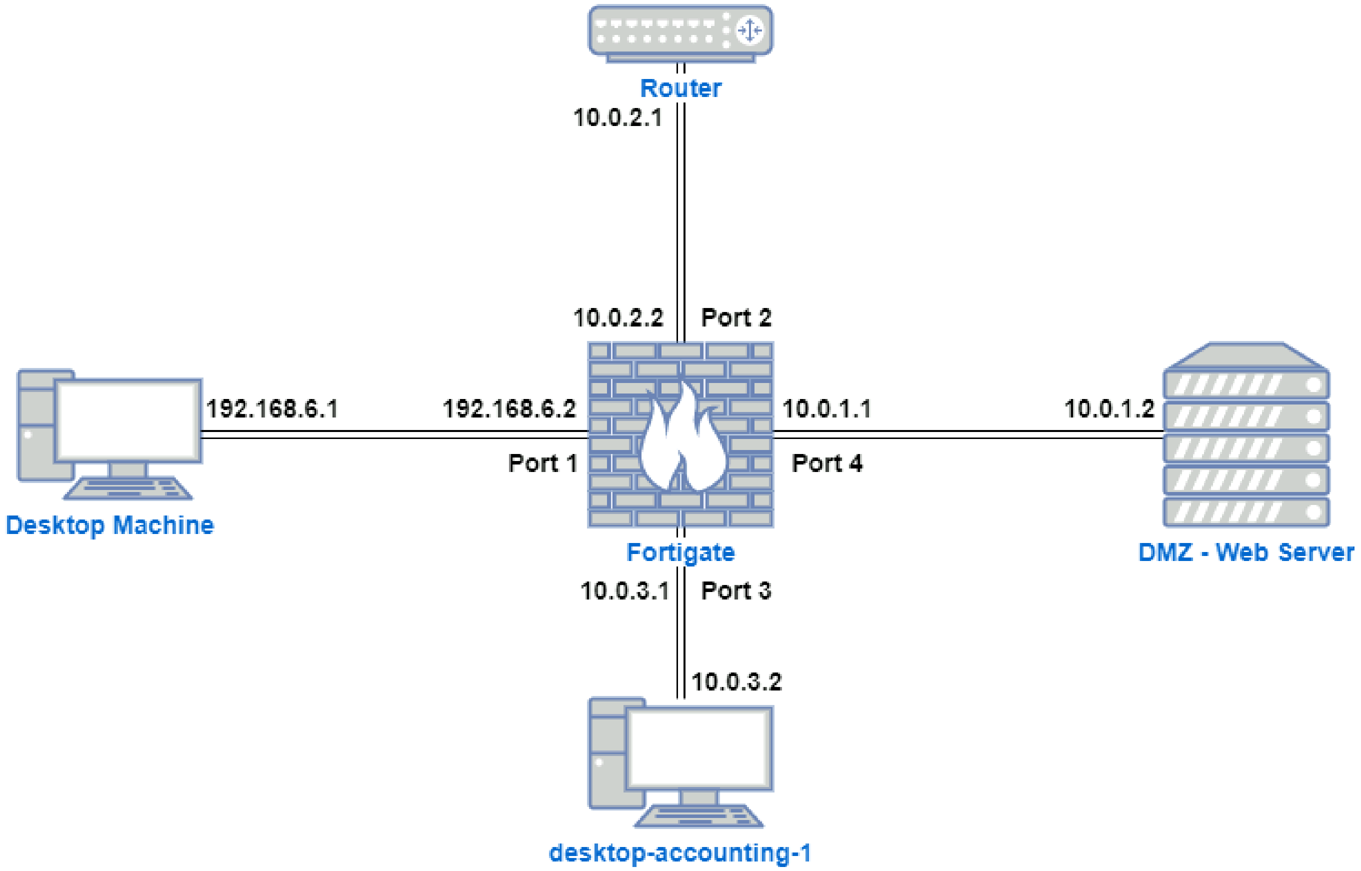
# Topology



# Module Description

- Your company is using a **FortiGate Firewall** to protect your internal and edge networks.
- To make sure that firewalls work exactly as you wish, you use *firewall policies.*

**Firewall Policy** : defines what kind of traffic is allowed in your network.

```
- Basically dictates the kind of stuff you can request from the Internet and receive
response from the Internet. As long as there are stuff that the Firewall policy does
not allow, and a user tries to request that information on the Internet, the firewall
will block it (or not depending on the policy and the action to take given that
policy).
```

- The **firewall policy** consists of one or more **rules** that allow or deny specific kinds of traffic (for example:

  ```
  - always block port 22 from all sources (since this is mostly used for SSH)
  - always allow traffic from the Internet to port 80 of the public web servers.
  ```

```
(since HTTP is the most used)
```

- Your manager has noticed that some of your firewall policies and rules are ***exposing*** your network to external attackers or malicious insiders.
- Most firewalls set a priority order determining how the rules will be applied to network traffic.
- Fortigate lets you ***drag and drop*** to reorder them, making it easier to solve any issues stemming from ordering problems.

# Reordering Policies

- FortiGate lets you **drag and drop** both policies and specific rules to reorder them making the reordering process very easy.
- You can also reorder your rules using the CLI command **"move"** but in this module, you will only be using the GUI interface.
- Be ***careful*** when making changes to a Fortigate Firewall in a production environment.
- Changes made to the firewall configuration are ***saved and activated immediately***.

```
- Why? Is there a way to modify this in such a way that admins can modify and
test things out first?
```

## Rule Ordering

How Rule Ordering works:

- When a packet reaches the firewall, the firewall searches for a matching policy starting from the top of the policy list and works its way down until it finds the first match.

```
- so it find a match like how it traverses a stack? You start from the topmost
then to bottom?
```

- Once a match is found, the firewall will NOT try to find any additional matches.

```
- Lazy Evaluation pfft.
```

- Most of the firewall ***breaches are caused by configuration errors***. This is why you need to pay extra attention to your firewall rule ordering.

# Logging In

- **FortiGate** offer users both the **CLI** and **web GUI** environments.

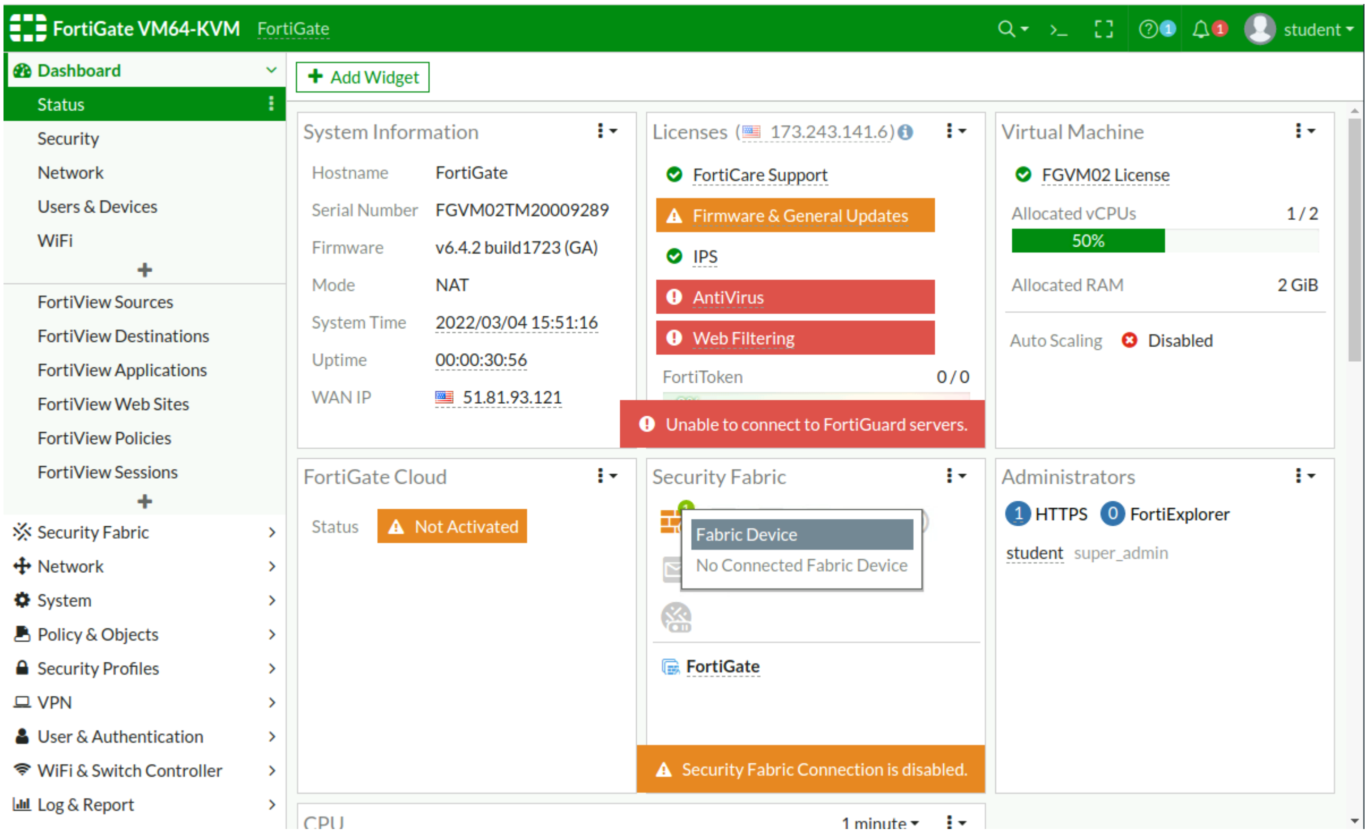
- This module will focus on the web GUI, but you have the liberty to perform all tasks with the CLI via SSH if you prefer.

- You can see the details of the Fortigate infrastructure in the topology section.

**Note:** *As you advance with the module, you will notice that you will be adding some machine objects to your firewall. You can assume that you have other machines under each network but to keep the topology clean, just one machine is added to each network.*

→ Access the firewall to start reordering and configuring firewall rules.

**Note:** *Close FortiOS new features guide upon first login.*



System Information

| | |
|---|---|
| Hostname | FortiGate |
| Serial Number | FGVM02TM20009289 |
| Firmware | v6.4.2 build1723 (GA) |
| Mode | NAT |
| System Time | 2022/03/04 15:51:16 |
| Uptime | 00:00:30:56 |
| WAN IP | 51.81.93.121 |

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

Fabric Device
No Connected Fabric Device
FortiGate

⚠ Security Fabric Connection is disabled.

Administrators

1 HTTPS 0 FortiExplorer

student super_admin

CPU 1 minute

## Reordering Policies

- The accounting department uses an application that automatically sends a downloadable payslip for all employees to a webserver over SSH. (This is a protocol which basically why accounting department access the webserver in the first place. Does the Accounting dept. have OTHER REASONS to access the webserver?)

- Your information security officer suspects that the workstation of accountant Angela (**desktop-accounting-45**) might be compromised by malware and asked a network engineer to block her access to the webserver just to be safe.

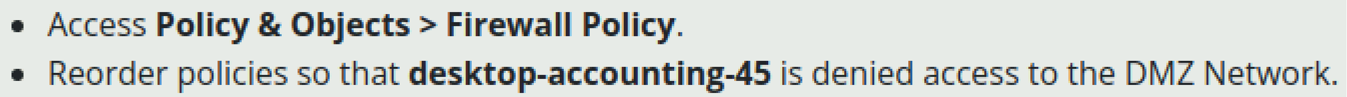
- The network engineer created a rule to block the access but her workstation can still connect to the server. You suspect that this is an issue with the order of firewall policies.

→ You can use the **drag and drop** reordering feature of FortiGate to make sure that Angela's workstation cannot access the DMZ.

**Note: You can only drag by clicking on the left-most column of a row.**

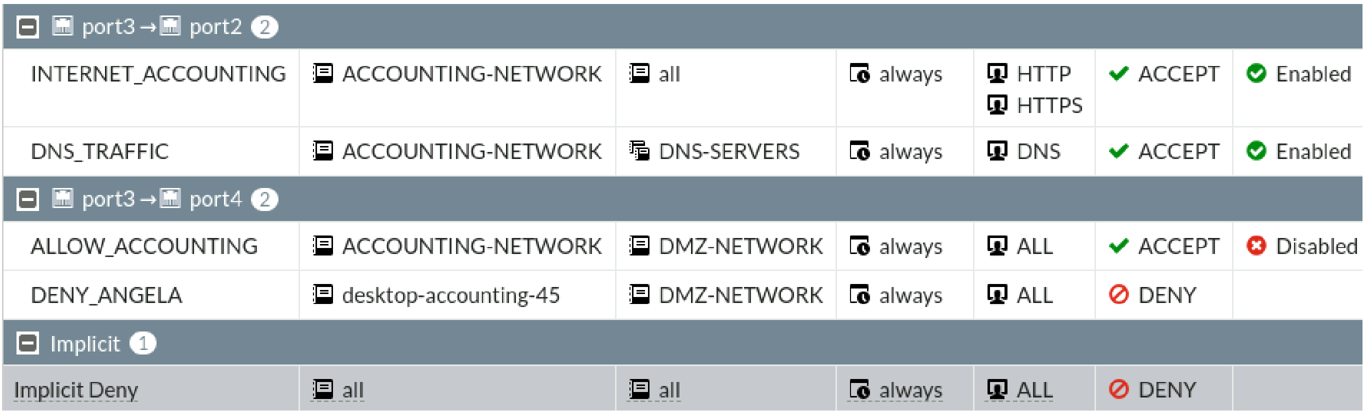
- You'll see the mouse icon change to a "cross" instead of normal.

Objectives:



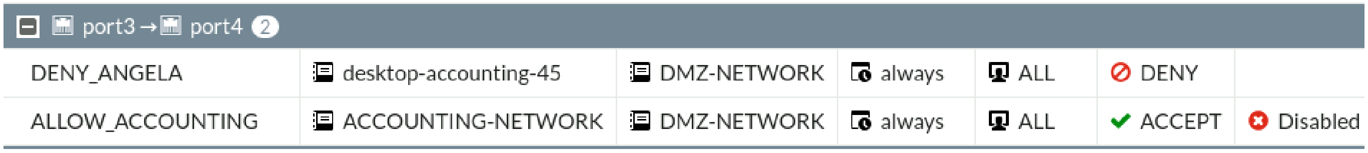
- Access **Policy & Objects > Firewall Policy**.
- Reorder policies so that **desktop-accounting-45** is denied access to the DMZ Network.

This is the initial state: Notice that the WHOLE accounting department is allowed to access the DMZ network FIRST.



| | | | | | | |
|---|---|---|---|---|---|---|
| ⊟ port3→port2 2 | | | | | | |
| INTERNET_ACCOUNTING | ACCOUNTING-NETWORK | all | always | HTTP<br>HTTPS | ✓ ACCEPT | ✓ Enabled |
| DNS_TRAFFIC | ACCOUNTING-NETWORK | DNS-SERVERS | always | DNS | ✓ ACCEPT | ✓ Enabled |
| ⊟ port3→port4 2 | | | | | | |
| ALLOW_ACCOUNTING | ACCOUNTING-NETWORK | DMZ-NETWORK | always | ALL | ✓ ACCEPT | ✖ Disabled |
| DENY_ANGELA | desktop-accounting-45 | DMZ-NETWORK | always | ALL | ⊘ DENY | |
| ⊟ Implicit 1 | | | | | | |
| Implicit Deny | all | all | always | ALL | ⊘ DENY | |

The current state after prioritizing blocking Angela of Accounting since there's a huge possibility that she has malware:



| | | | | | | |
|---|---|---|---|---|---|---|
| ⊟ port3→port4 2 | | | | | | |
| DENY_ANGELA | desktop-accounting-45 | DMZ-NETWORK | always | ALL | ⊘ DENY | |
| ALLOW_ACCOUNTING | ACCOUNTING-NETWORK | DMZ-NETWORK | always | ALL | ✓ ACCEPT | ✖ Disabled |

→ Works!

# Configuring Policies and Addresses

- Firewall policies are a crucial part when it comes to blocking undesirable access to your network.
- ***Only one mistake here and the whole network can be exposed to internal or external attacks.***

## Create a New Network Address

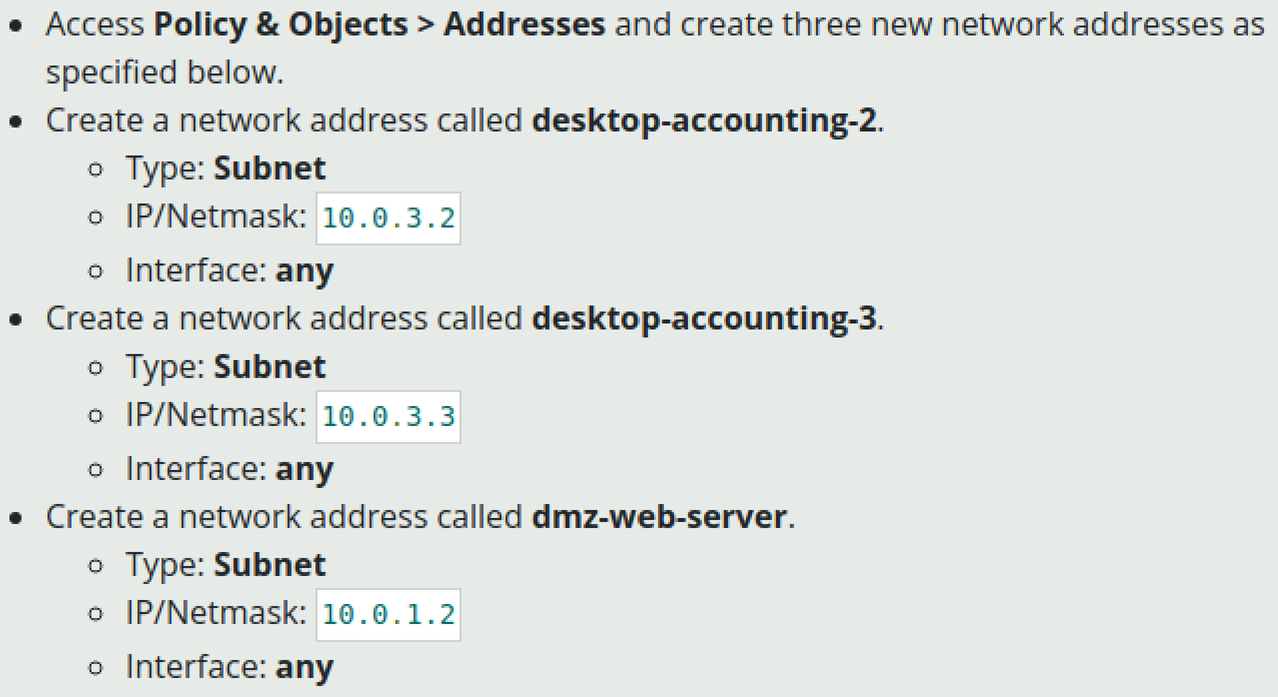
- Upon review of the existing firewall policies, you discovered that the accounting department currently has full network-level access to the entire DMZ network segment,

***but only SSH access on port 22 to the DMZ Web Server is required to publish the payslips.***

```
- So does this mean that blocking Angela on the web server is overkill? That you
can just disable Angela's account to use of port 22? (no idea)
- Wait, so the accounting department ONLY need to access the web server to
publish the payslips?
```

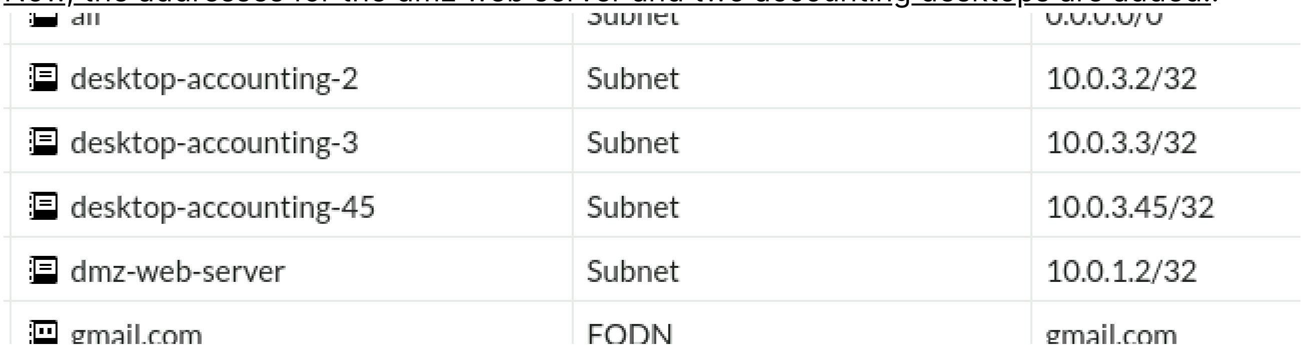
- To limit accidental misuse and potentially malicious activity, you need to create more restrictive and specific firewall policies.
- But first, you need to create the network **addresses** you will be using in your policy.

Objectives:



- Access **Policy & Objects > Addresses** and create three new network addresses as specified below.
- Create a network address called **desktop-accounting-2**.
  - Type: **Subnet**
  - IP/Netmask: `10.0.3.2`
  - Interface: **any**
- Create a network address called **desktop-accounting-3**.
  - Type: **Subnet**
  - IP/Netmask: `10.0.3.3`
  - Interface: **any**
- Create a network address called **dmz-web-server**.
  - Type: **Subnet**
  - IP/Netmask: `10.0.1.2`
  - Interface: **any**

Now, the addresses for the dmz web server and two accounting desktops are added!:



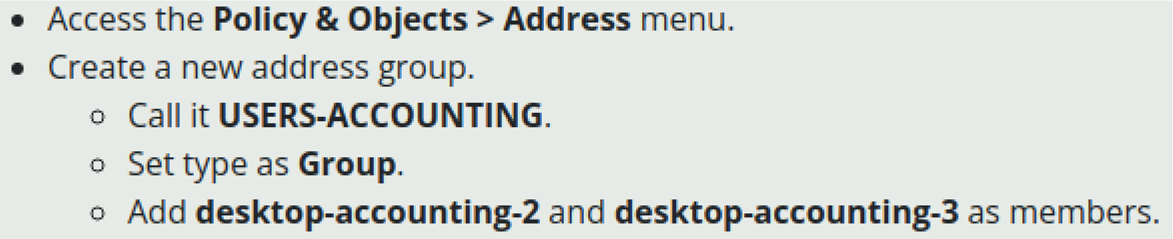
| | | |
|---|---|---|
| all | Subnet | 0.0.0.0/0 |
| desktop-accounting-2 | Subnet | 10.0.3.2/32 |
| desktop-accounting-3 | Subnet | 10.0.3.3/32 |
| desktop-accounting-45 | Subnet | 10.0.3.45/32 |
| dmz-web-server | Subnet | 10.0.1.2/32 |
| gmail.com | FQDN | gmail.com |

## Create a New Address Group

- FortiGate lets you create address groups to group network address objects.
- This is very helpful when you need to add a lot of individual machines into a single policy.

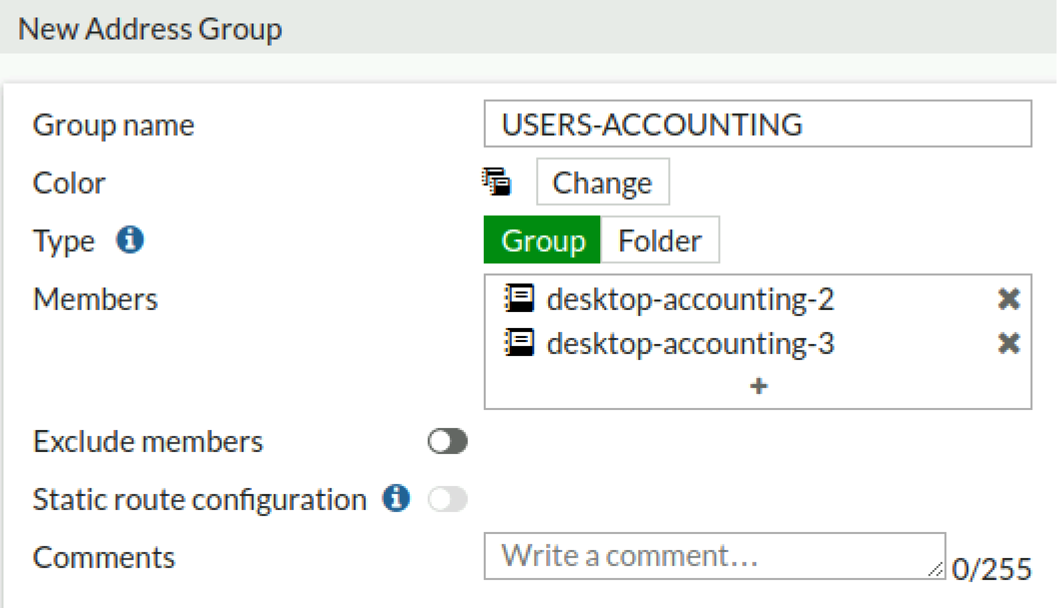
- That feature will help you to keep your rules organized.

Objectives:



- Access the **Policy & Objects > Address** menu.
- Create a new address group.
  - Call it **USERS-ACCOUNTING**.
  - Set type as **Group**.
  - Add **desktop-accounting-2** and **desktop-accounting-3** as members.

Setting up the new address group:



New Address Group

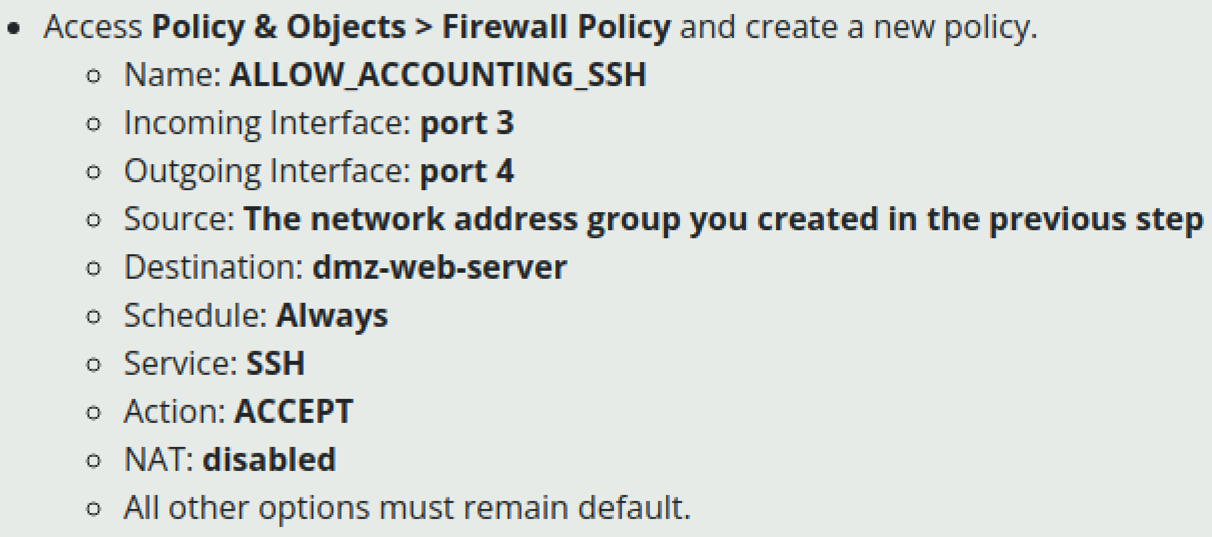
| | |
|---|---|
| Group name | USERS-ACCOUNTING |
| Color | Change |
| Type | [✓ Group] Folder |
| Members | desktop-accounting-2 ✖<br>desktop-accounting-3 ✖<br>+ |
| Exclude members | ○ |
| Static route configuration | ○ |
| Comments | Write a comment... 0/255 |

```
- Then press "OK"!
```

## Create a New Policy

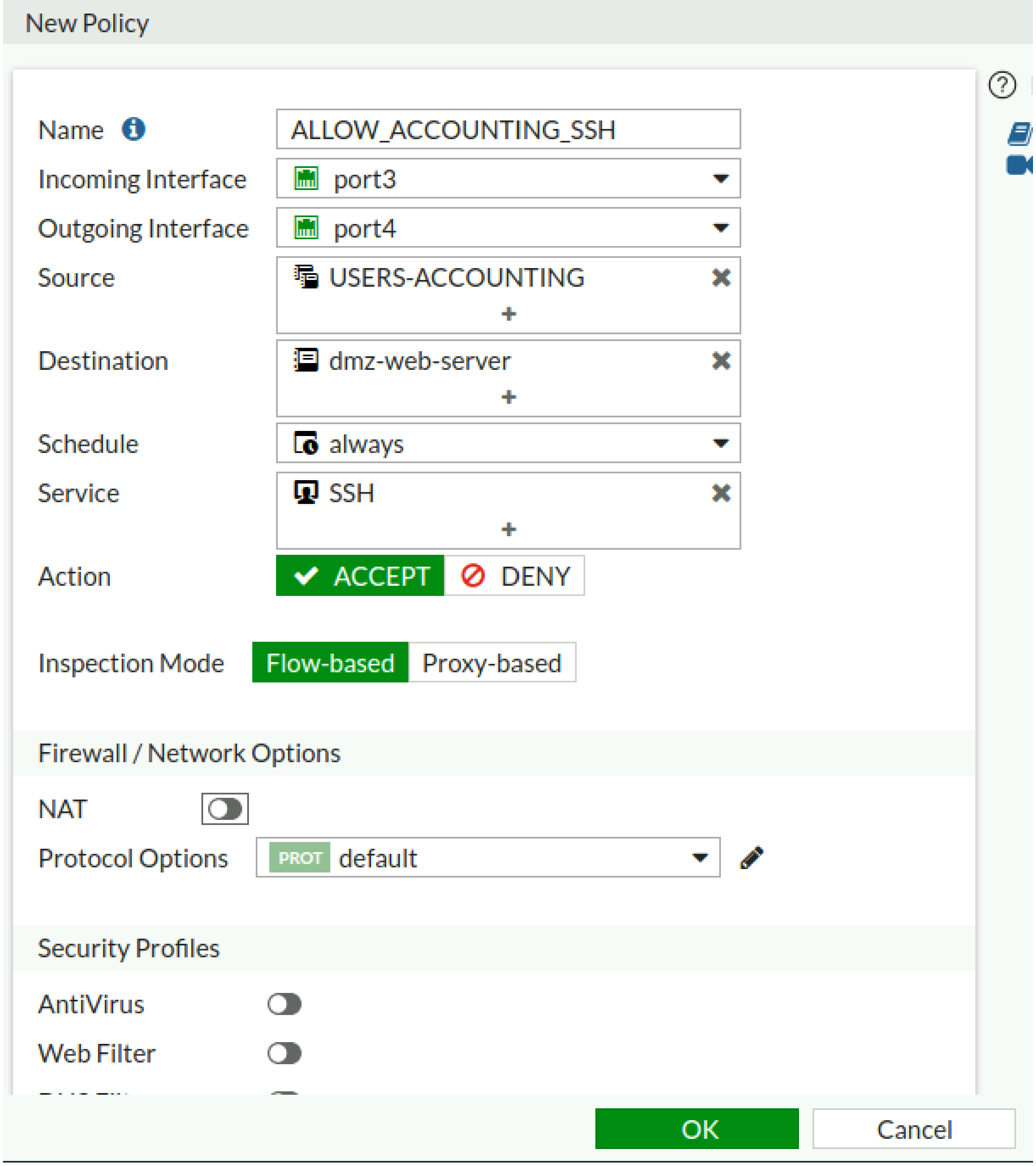
- Now you need to allow these accounting machines to access SSH protocol at the DMZ server.

Objectives:



- Access **Policy & Objects > Firewall Policy** and create a new policy.
  - Name: **ALLOW_ACCOUNTING_SSH**
  - Incoming Interface: **port 3**
  - Outgoing Interface: **port 4**
  - Source: **The network address group you created in the previous step**
  - Destination: **dmz-web-server**
  - Schedule: **Always**
  - Service: **SSH**
  - Action: **ACCEPT**
  - NAT: **disabled**
  - All other options must remain default.

Modified setup:


New Policy

Name: ALLOW_ACCOUNTING_SSH

Incoming Interface: port3

Outgoing Interface: port4

Source: USERS-ACCOUNTING

Destination: dmz-web-server

Schedule: always

Service: SSH

Action: [✓ ACCEPT] DENY

Inspection Mode: [✓ Flow-based] Proxy-based

Firewall / Network Options

NAT: ○

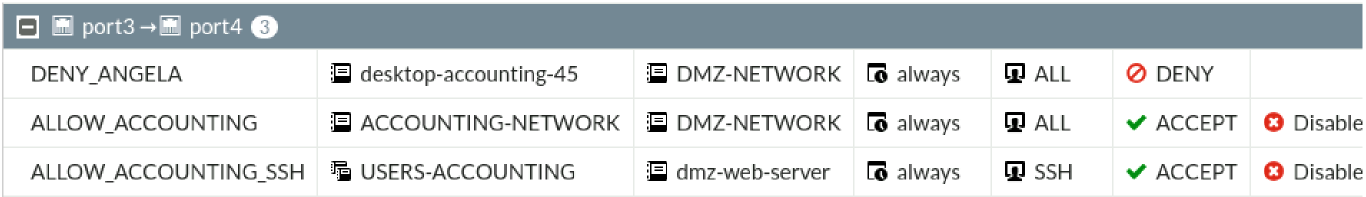
Protocol Options: PROT default

Security Profiles

AntiVirus: ○

Web Filter: ○

Current ordering of Policies:



| | | | | | | |
|---|---|---|---|---|---|---|
| ⊟ port3 → port4 3 | | | | | | |
| DENY_ANGELA | desktop-accounting-45 | DMZ-NETWORK | always | ALL | ⊘ DENY | |
| ALLOW_ACCOUNTING | ACCOUNTING-NETWORK | DMZ-NETWORK | always | ALL | ✓ ACCEPT | ✖ Disable |
| ALLOW_ACCOUNTING_SSH | USERS-ACCOUNTING | dmz-web-server | always | SSH | ✓ ACCEPT | ✖ Disable |

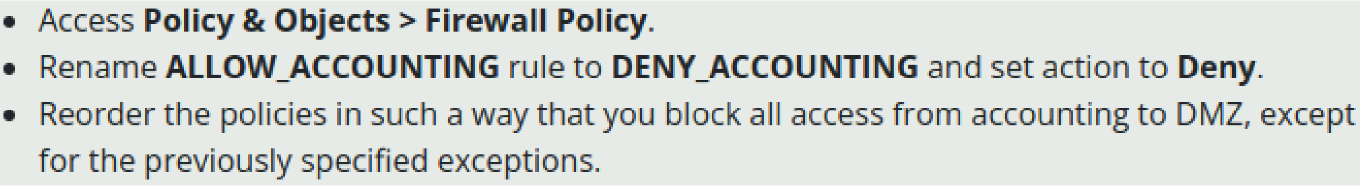
## Reinforcing Policies

- Now that you have created a rule only allowing certain machines to access a specific server DMZ, you need to reorder the policies between the Accounting Network and the DMZ network.

- Firewalls usually have a **deny all** rule at the end of the firewall policies list to block any traffic that wasn't explicitly allowed.
- But, it is good practice to add a **deny all** rule at the end of **each section**, so you can log denied access to the section individually.
- Otherwise, you will have denied access being logged into one single rule and that can slow you odnw if you need to debug, threat hunt, or create alerts.

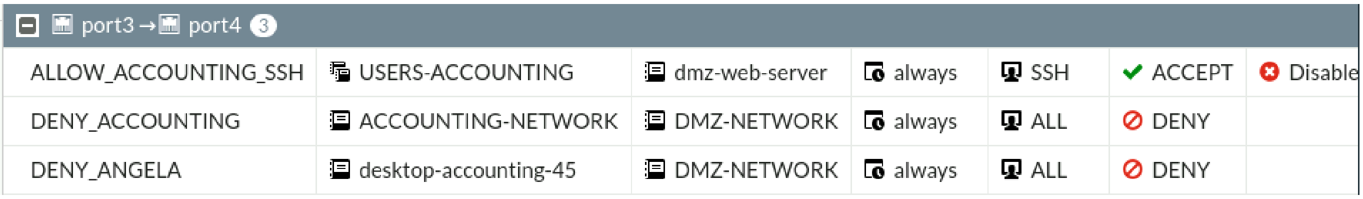
**Note: This means, the more specific the policy is, the more it should be placed at the beginning. The less specific(more general) a Firewall Policy is, the more it should be at the last!** (Imagine the symbol of WiFi!)

Objectives:



- Access **Policy & Objects > Firewall Policy**.
- Rename **ALLOW_ACCOUNTING** rule to **DENY_ACCOUNTING** and set action to **Deny**.
- Reorder the policies in such a way that you block all access from accounting to DMZ, except for the previously specified exceptions.

Final look of the firewall policy order:



⊟ port3 → port4 3

| | | | | | | |
|---|---|---|---|---|---|---|
| ALLOW_ACCOUNTING_SSH | USERS-ACCOUNTING | dmz-web-server | always | SSH | ✓ ACCEPT | ✖ Disable |
| DENY_ACCOUNTING | ACCOUNTING-NETWORK | DMZ-NETWORK | always | ALL | ⊘ DENY | |
| DENY_ANGELA | desktop-accounting-45 | DMZ-NETWORK | always | ALL | ⊘ DENY | |

# Summary of the Whole Process

- Oh, so we still want the WHOLE Accounting department to access the DMZ web server but limit its use so that even though ANY of the machine from the Accounting department is compromised(since we cannot really blame them how they use their computer), it would NOT compromise the web server as well. Basically, limits the surface in which can malware operate. In this case, it can only use port 22(SSH) if it wants to do lateral movement(no idea)?
- From the image just above, we can tell that the accounting department can still access the web server to publish the payslips because it only uses port 22(SSH). Other than that, it is being denied access!
- Also, the last one "DENY_ANGELA" is already captured by "DENY_ACCOUNTING" so you can just delete it! (Don't know how)