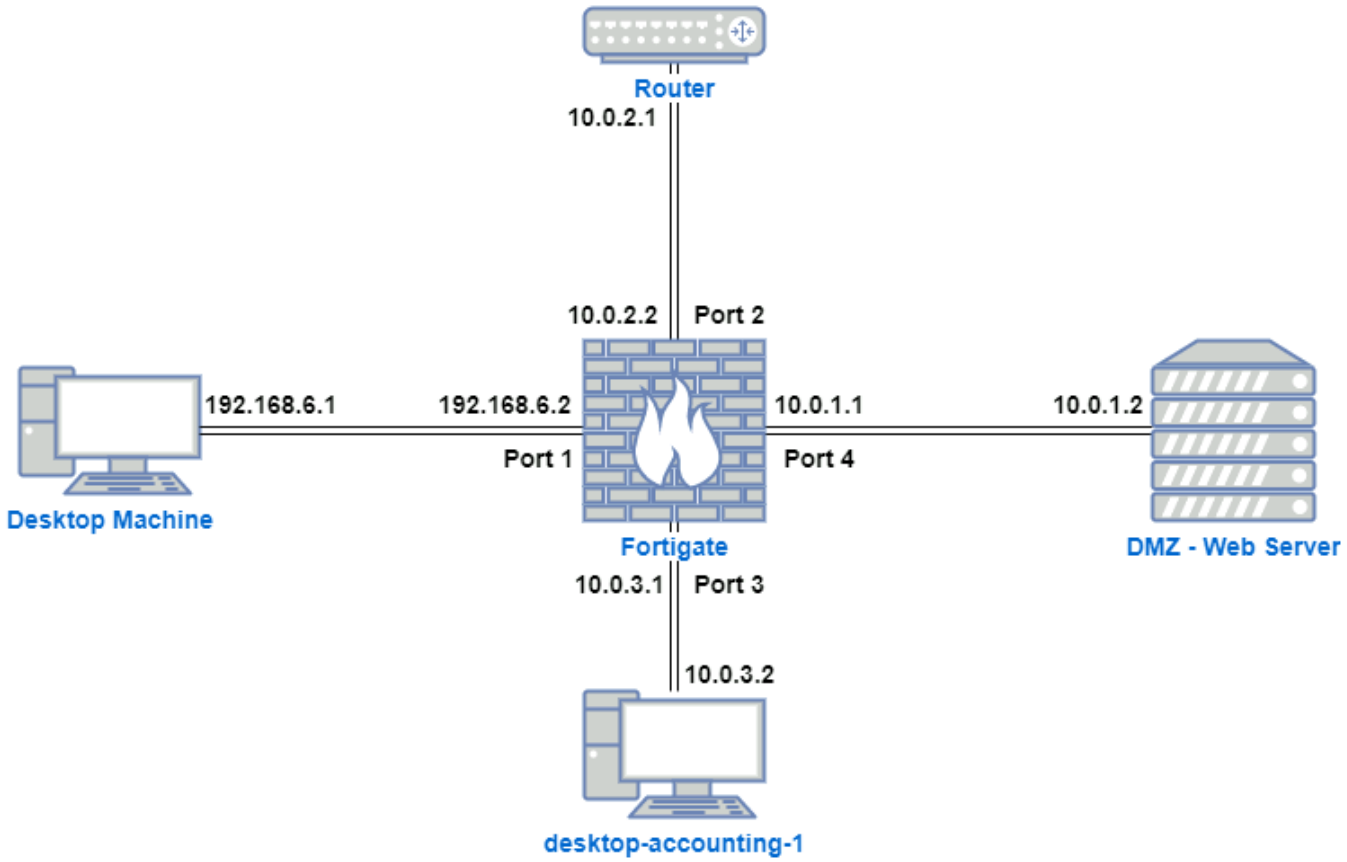
Network Topology



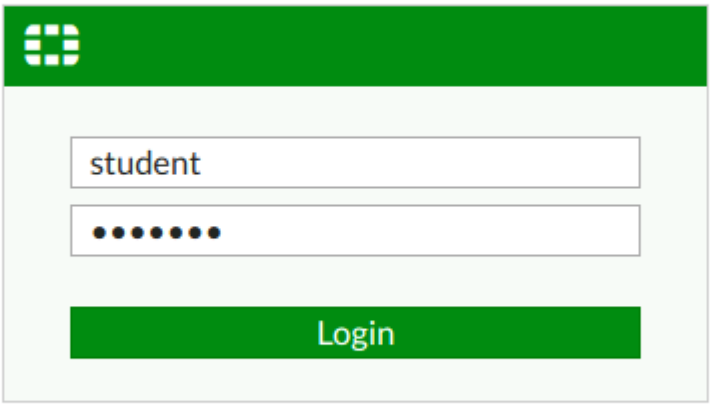
Module Description

- In your organization, the CISO asked you to create some web filtering rules following the directives of the internal Internet Security Policy.
- This step is one of many others needed to comply with the ISMS (Information Security Management System)
- Also, the accounting manager is complaining about the internet in their department and asking you to block internet access to some specific websites that seem to be reducing the team performance.
- Your company uses a Fortigate Firewall to control the users' Internet access and provide a lot of other security enforcement to your organization's environment. Let's take a look at all the options this provides you.

Logging In

- **Fortigate VM** offers users both the **CLI** and **web GUI** environments.

- This module will focus on the web GUI, but you have the liberty of performing all tasks with the CLI via SSH if you prefer.
- Take a look at the topology above. You will see that the desktop is behind Fortigate and all internet access is passing through the firewall.
- In order to comply with the organizational Internet Policy, you need to reinforce the user access rules already in place. To start doing that, log in first in to the firewall.

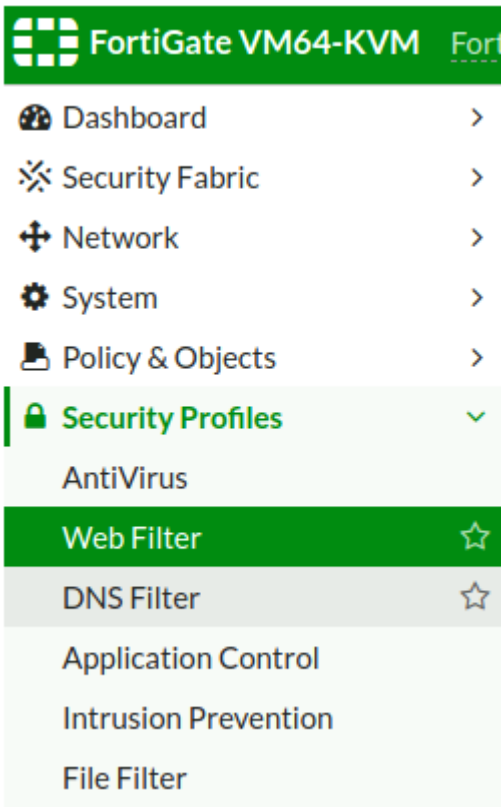


Web Filtering

- **Web Filtering** controls and restricts user's internet access. You can apply filtering using policy-based or profile-based firewall policies.

→ FortiOS has three main components for web filtering:
- **Web Content Filter** : Blocks traffic based on patterns or specific words that you can specify.
- **URL Filter** : Uses specific URLs and URL patterns to block content or to block malicious URLs discovered by FortiSandbox.
- **FortiGuard Web Filtering** : Provides the ability to choose between categories when filtering web traffic.

- You can manage web filter profiles and configurations at the **Web Filter** option in the FortiGate menu, as seen in the image below:



→ Basically, go to **Security Profiles** → **Web Filter**

FortiGate Web Filtering

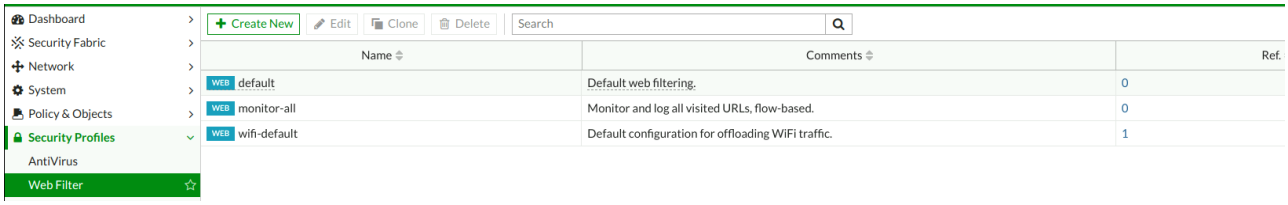
- **FortiGate Web Filter** features are applied in the following order:

    1. URL Filter
    2. FortiGuard web filtering
    3. Web content Filter
    4. Web Script Filter
    5. AV Scanning

- These five components interact with each other to give you more security and the ability to create granular filters.

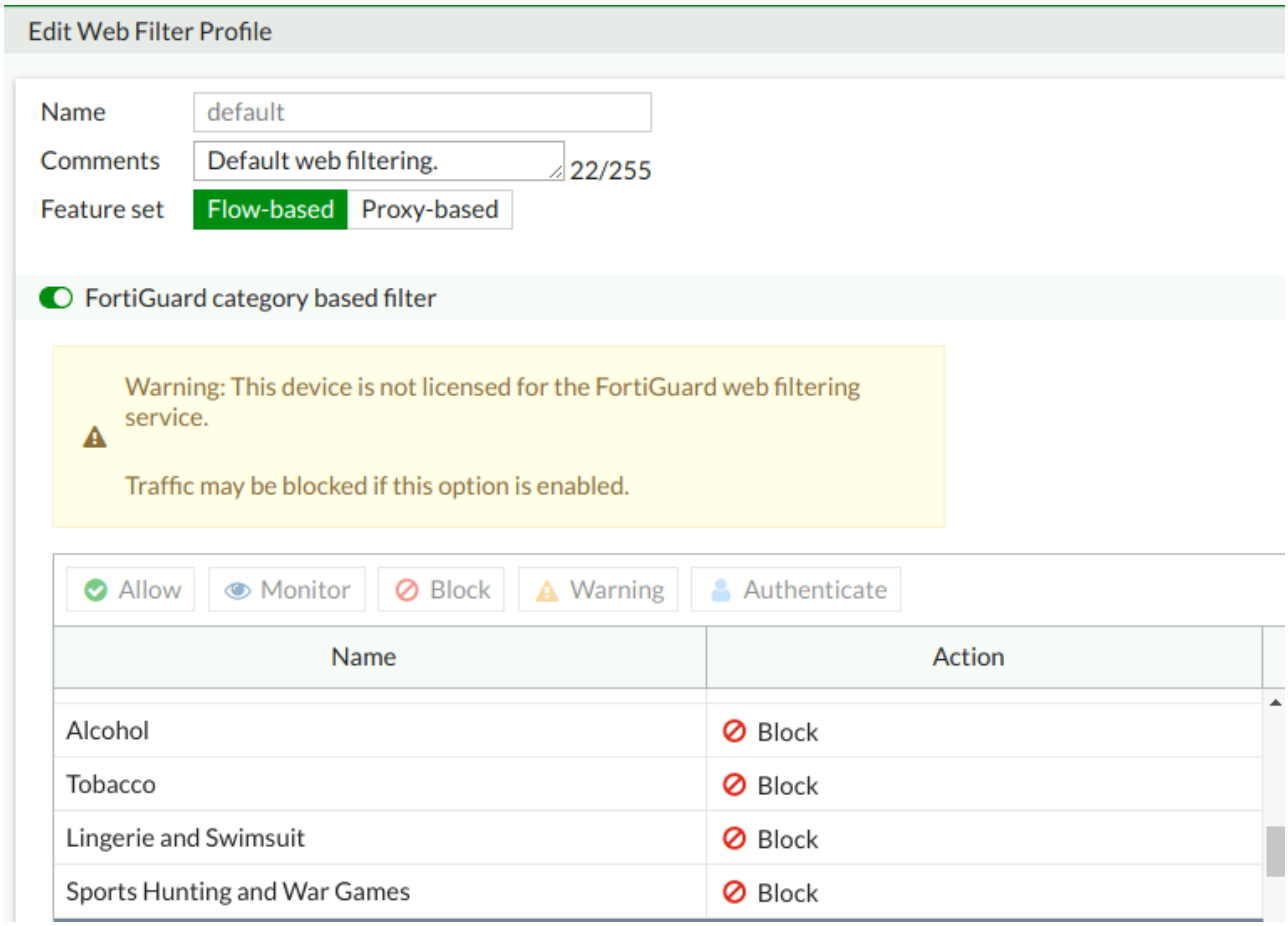
<u>Objectives</u>: Answer the ff. questions

1. Default Web Filter profiles:



2. What is the second **Potentially Liable** category allowed under the **default** web filter profile?
   → Hacking

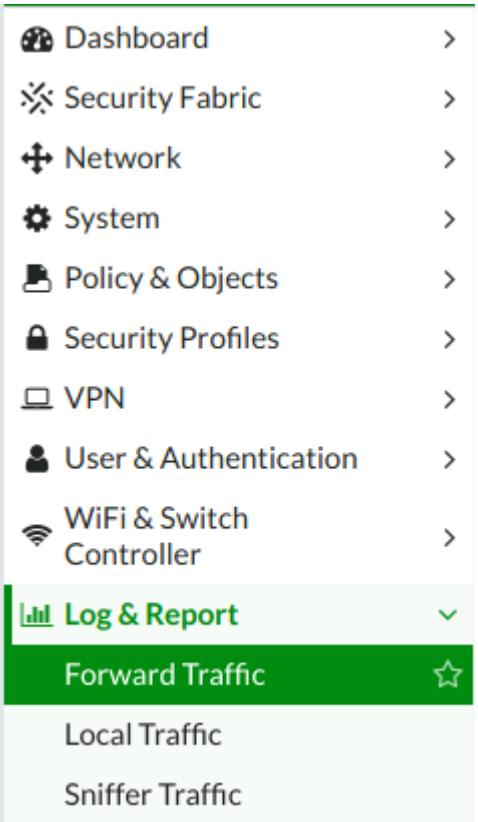
3. In the **Action** section of log details, what is the action detected by the FortiGate?



→ Block

Log & Report

- The accounting manager opened a ticket with a complaint about their internet access. It appears that they are NOT able to access internet.
- FortiGate gives you details about machines' networking activity, so that you could easily troubleshoot the problems.
- In the **Log & Report** menu, you can find details about **forwarding traffic, events, web filter** and a lot more useful information about other Fortigate features.



Objectives:

- Access **Log & Report > Forward Traffic**.
  - **Filter by source** and search for the machine **10.0.3.**.
  - **Double-click on events** with the destination **1.1.1.1** to see the log details.
- Answer the questions.

Log Details

Source

IP	10.0.3.2
Source Port	58844
Country/Region	Reserved
Source Interface	port3
User	

Destination

IP	8.8.8.8
Port	53
Country/Region	United States
Destination Interface	port2

Application Control

Application Name	
Category	unscanned
Risk	undefined
Protocol	6
Service	DNS

Data

Received Bytes	0 B
Sent Bytes	0 B
Sent Packets	0

Action

Action	Deny: policy violation
Threat	131072
Policy ID	0
Policy Type	Firewall

Security

Level	
Threat Level	High

→ It doesn't exactly say why the Accounting Manager can't connect to the Internet but we know that they cannot do so because:

1. Of a **Policy violation**
2. The firewall itself does NOT let them send their request(s) to the outside world. Notice that the request is blocked at port 2.
3. Also notice that the service being blocked is DNS.

Web Filtering Profiles

- When creating URL filtering, you can use different types of filters:

Simple : Used when you need an exact match, "www.rangeforce.com" for example.

Wildcard : used when you need to cover different URLs from the same domain,

```
- *.rangeforce.com
```

or

```
- www.rangeforce.com/*
```

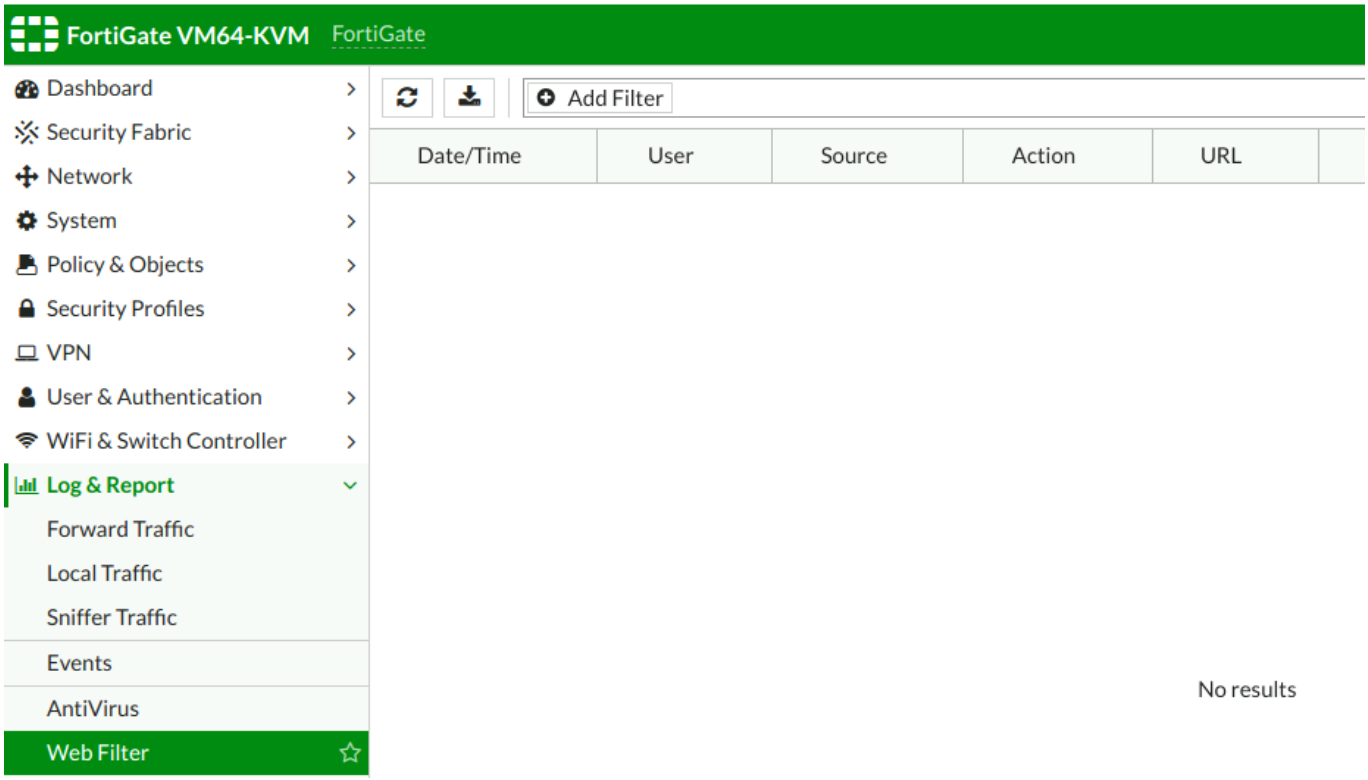
Regular Expressions (regex) : Regex can be used to give you more filtering possibilities, using Perl syntax for example:

```
"*" : matches the character before the symbol 0 or more times, but does NOT match by character. For example: "rangeforce*.com" will match "rangeforceeeeeeee.com" but not "rangeforcelabs.com"

"/i" : turns the pattern case-insensitive. For example: "/RANGEFORCE/i" will also match with "rangeforce"

"^" : Match the beginning of the string. For example: "^ra" will match "rangeforce.com"
```

Web Filter Profile - Simple Type

- The internal Internet Policy of your company defines different URL filtering rules for different departments of the company.

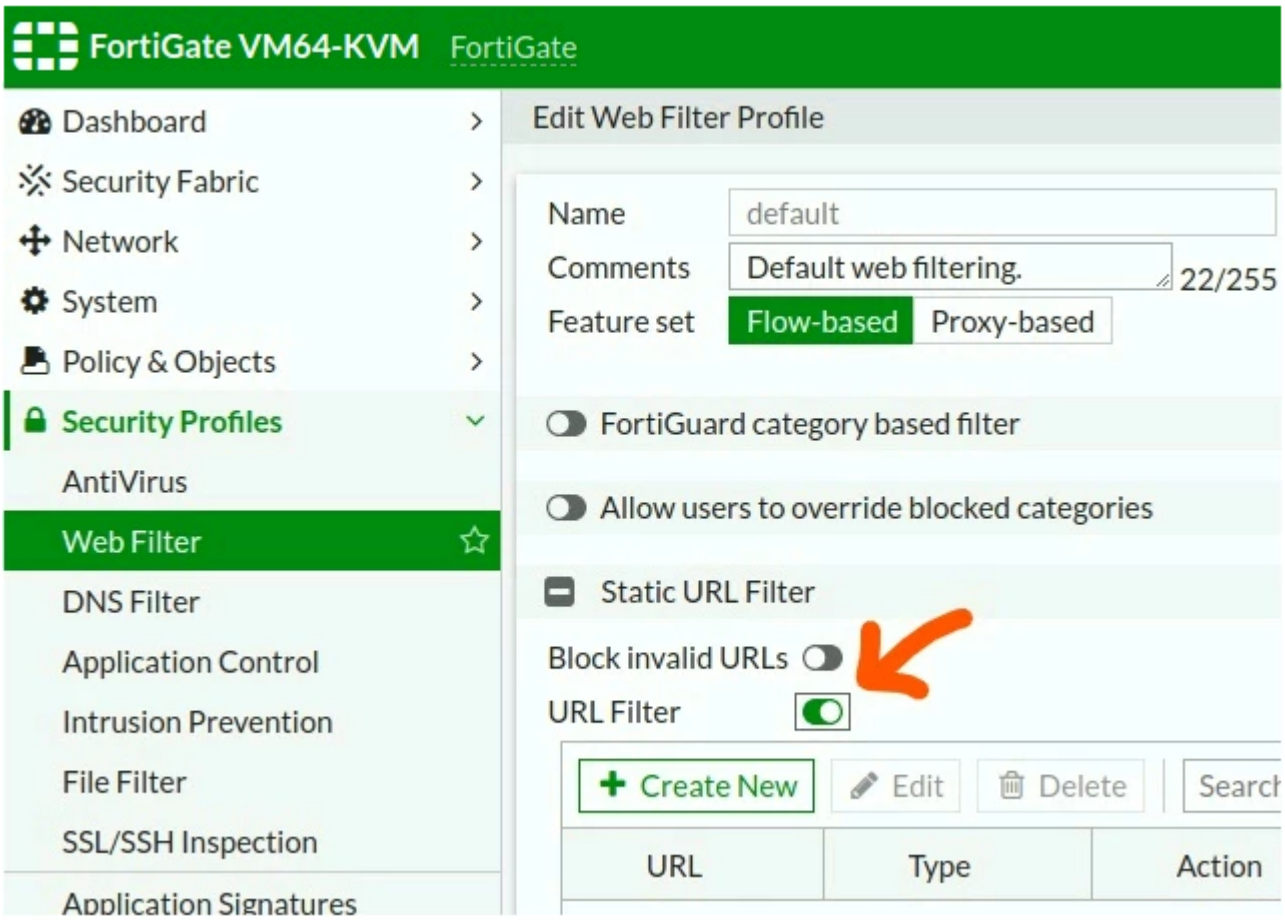
Current Web Filter:



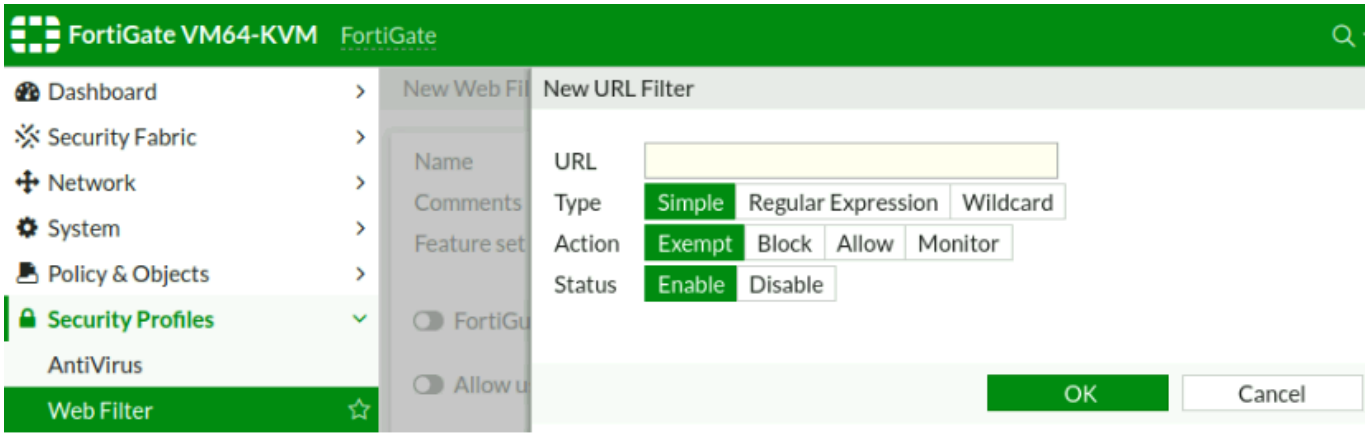
- The first URL filtering you will be creating is for the **accounting department**.
- The **Internet policy** specifies that these sites should be blocked to avoid leaking sensitive information:

```
- www.dropbox.com/business
- www.dropbox.com/individual
- onedrive.live.com
- drive.google.com
- mega.nz
```

→ You can access the **Static URL Filtering Option** as shown in the image below: Notice that it is under "Security Profiles" and NOT under "Log Reports"!



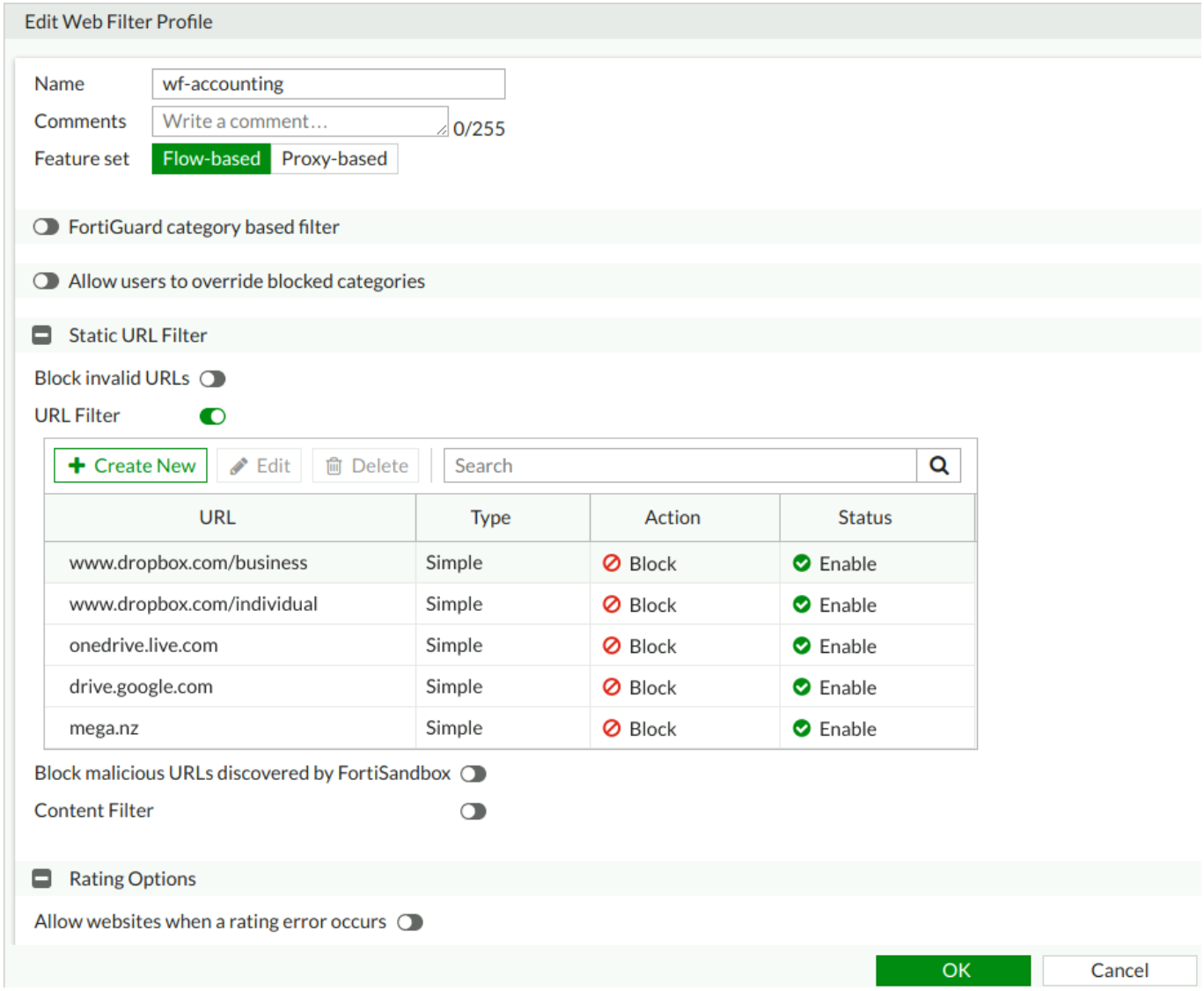
→ The next image shows the options you have when creating a new URL entry:



Objectives:

- Create a **new web filter profile** to block the sites indicated above.
  - Name: **wf-accounting**
  - Use a **flow-based** feature-set.
  - **Disable FortiGuard** category-based filter if it's enabled.
- **Enable the URL Filter option**.
- Add the **websites shown above** to the profile.
  - Create new URL Filter.
  - URL: **Pick a URL from the list above**.
  - Type: **Simple**
  - Action: **Block**
  - Status: **Enable**
  - Click **OK** to add the entry to the URL Filter.
  - Repeat for all URLs in the list.

Result of modification:



Web Filter Profile - Wildcard

- You noticed that the accounting web filtering profile ***has some gaps*** because they can still access the URLs that can lead them to the desired website, like:

```
- dropbox.com/photos/album/
- dropbox.com/content_link/
- g.api.mega.co.nz/cs?id=sequence_number&ak=appkey&[&sid=sessionid|&n=node]
```

- To block access to those URLs as well, you can use wildcards!
- **Wildcard** : used when you need to cover different URLs from the same domain.

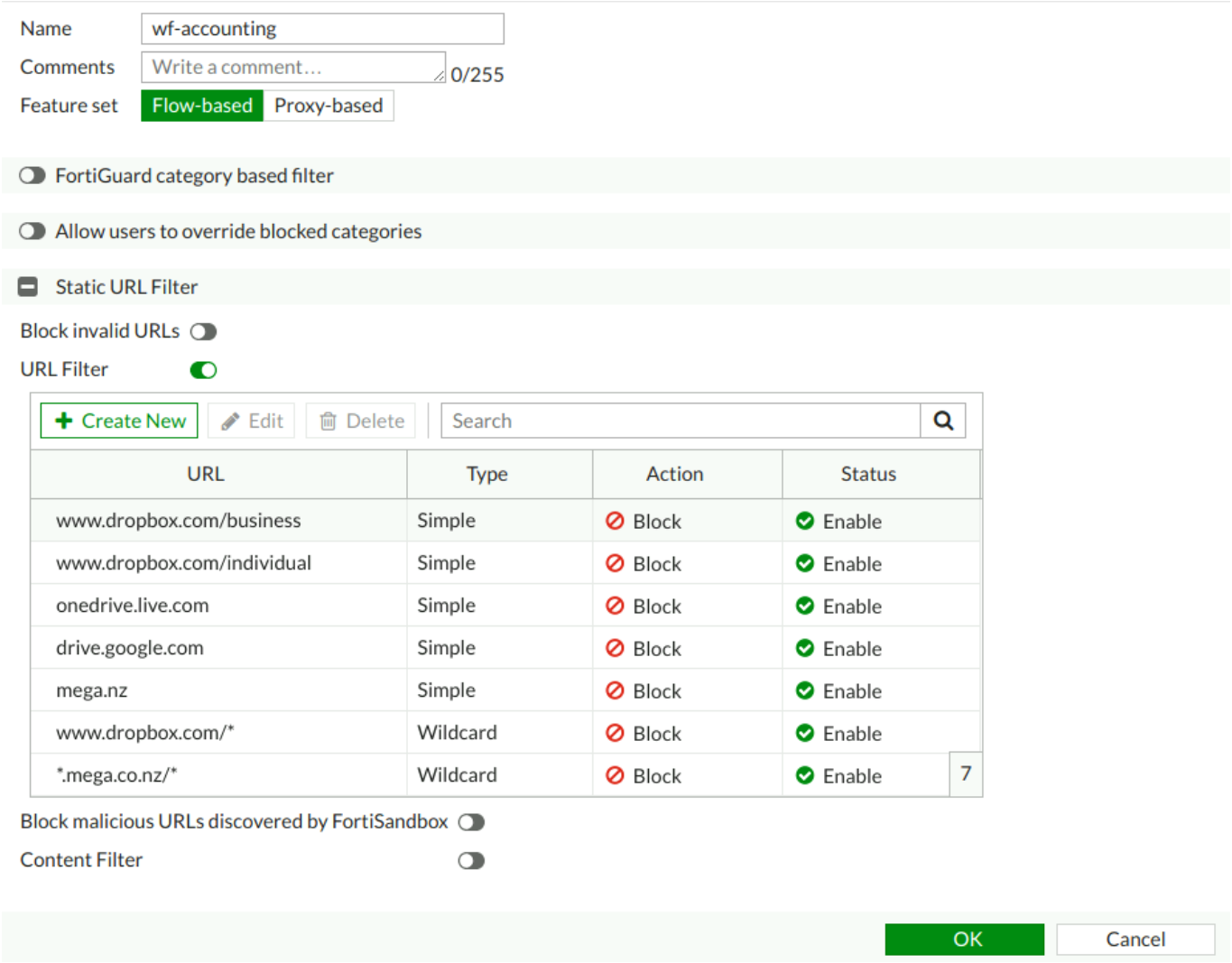
→ For example:

```
- URL : "*.rangeforce.com" (everything before ".rangeforce.com" will match this rule,
like "materials.rangeforce.com").
- URL : "www.rangeforce.com/*" (everything after "www.rangeforce.com/" will match this
rule, like "www.rangeforce.com/contact").
```

<u>Objectives</u>:

- Edit the **wf-accounting** web filter profile and wildcard expressions.
- Create a wildcard expression to block everything **after dropbox.com/**.
  - Type: **Wildcard**
  - Action: **Block**
  - Status: **Enable**
  - Click **OK** to add the entry to the URL Filter.
- Create a wildcard expression to block everything **before and after .mega.co.nz/**.
  - Type: **Wildcard**
  - Action: **Block**
  - Status: **Enable**
  - Click **OK** to add the entry to the URL Filter.

Result:



→ Notice that **two** newly added web filters.

Web Filter Profile - Regex

- The accounting manager opened a ticket asking you to search the firewall logs for their departments most accessed websites because he thinks productivity was down last month.
- You noticed that the users often (maybe even too often) accessing some news websites, like **cnn.com,news.yahoo.com,foxnews.com and nbcnews.com**.
- Thus, you need to block access to those sites.
- ***To avoid creating too many entries, you decided to use regular expressions to deal with it.***
- **Regular Expressions (regex)** : Regex can be used to give you more filtering possibilities, using Perl syntax. for example:

```
- "*" : matches the character before the symbol 0 or more times but does NOT match by character. For example: "rangeforce*.com" will match "rangeforceeeeeee.com" but NOT "rangeforcelabs.com"

- "/i" : Turns the pattern case sensitive. For example: "/RANGEFORCE/i" will not match with "rangeforce".

- "^" : Matches the beginning of the string. For example: "^ra" will match "rangeforce.com"
```

Objectives:

- Edit **wf-accounting** and add a regex to the web filter profile.
  - URL: `(cnn|news|foxnews|nbcnews)\.(com|yahoo.com)`
  - Type: **Regular Expression**
  - Action: **Block**
  - Status: **Enable**
  - Click **OK** to add the entry to the URL Filter.

→ Wouldn't this also block:

1. cnn.yahoo.com
2. foxnews.yahoo.com
3. nbcnews.yahoo.com
   ???

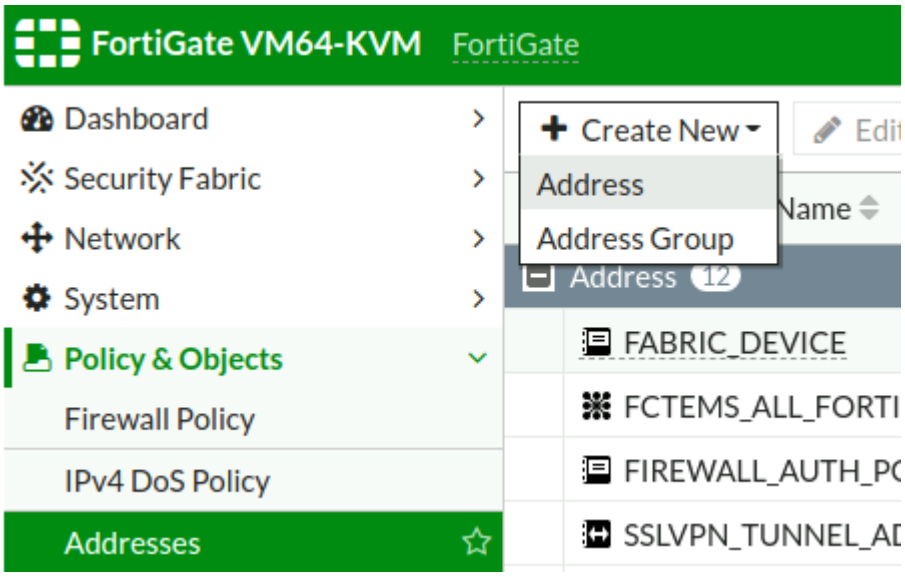
Firewall Rules

- After you create a **web filtering profile**, you need to activate it in the firewall rule so your web filter controls would be applied to the users.

Create a New Network Address

- In order to create a rule that matches the accounting network, you need to create an object in the firewall referencing the network address you wish to include.

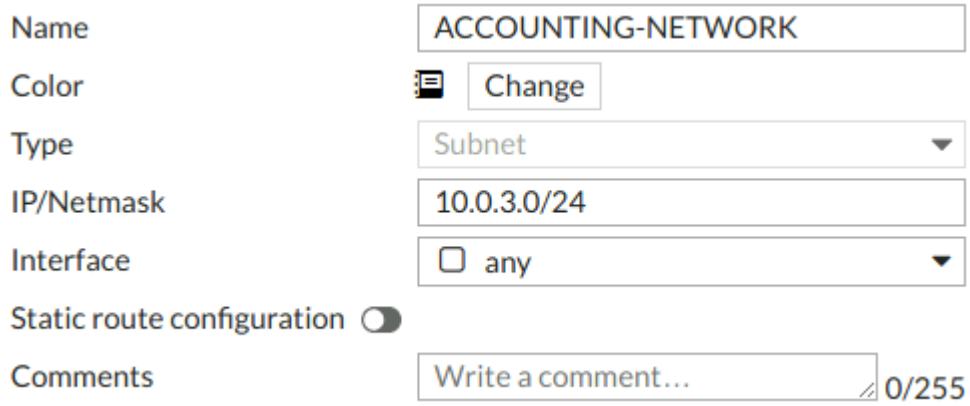
- You can do that by accessing the **Policy & Objects > Addresses**.



Objectives:

- Create a new **network address object**.
  - Name: **ACCOUNTING-NETWORK**
  - Type: **Subnet**
  - IP/Netmask: **10.0.3.0/24**
  - Interface: **any**

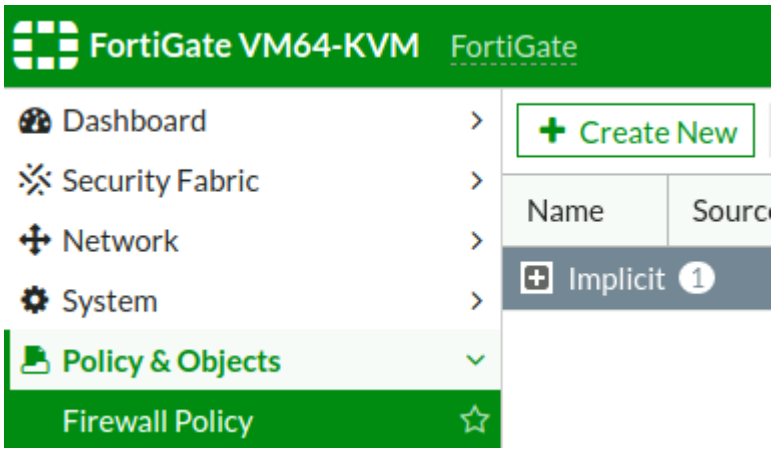
Result:



→ You can see that there is a new address added!

Create a WebFilter Rule

- You can create a new firewall rule by accessing the menu **Policy Objects & Firewall Policy**.

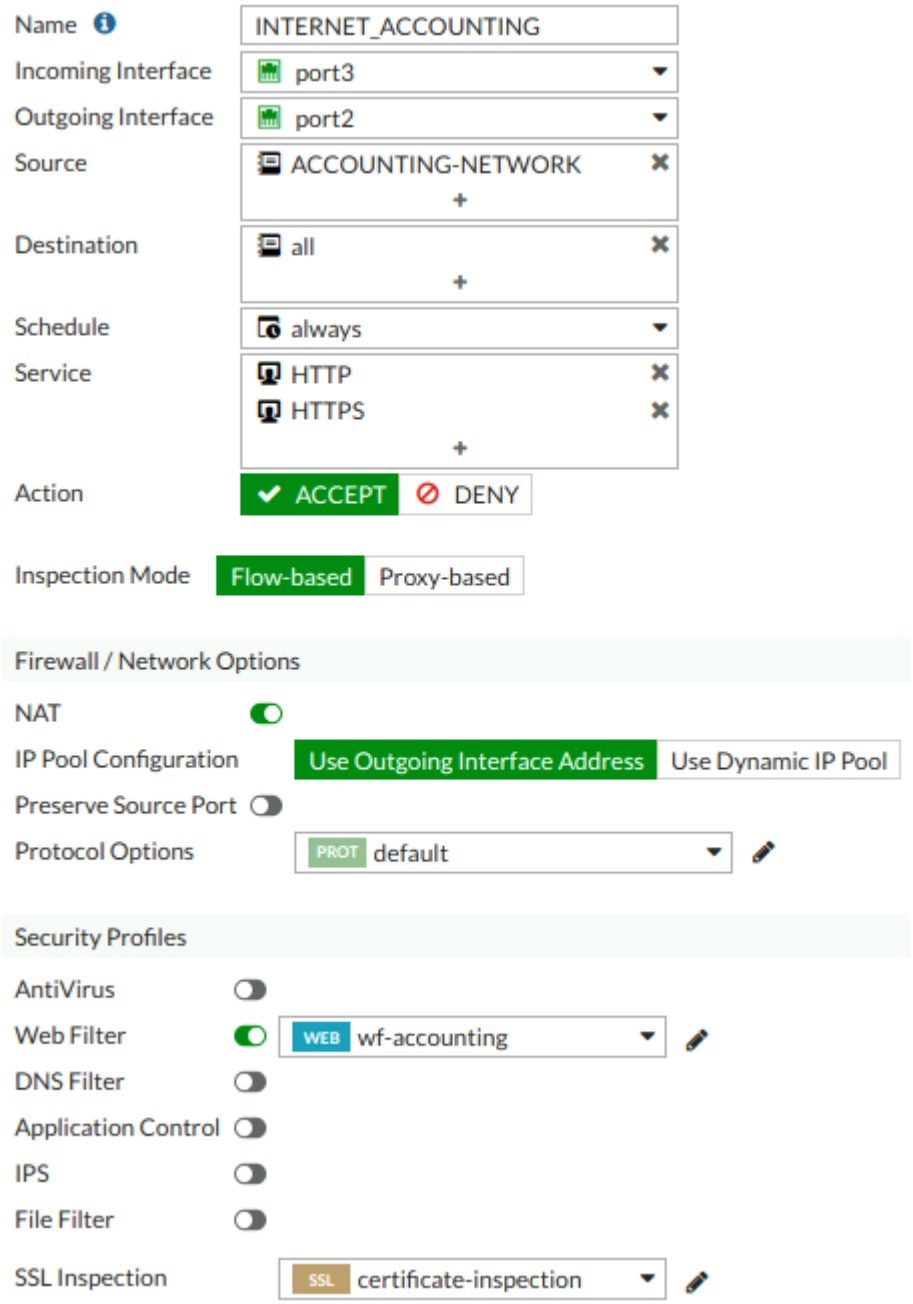


<u>Objectives</u>:

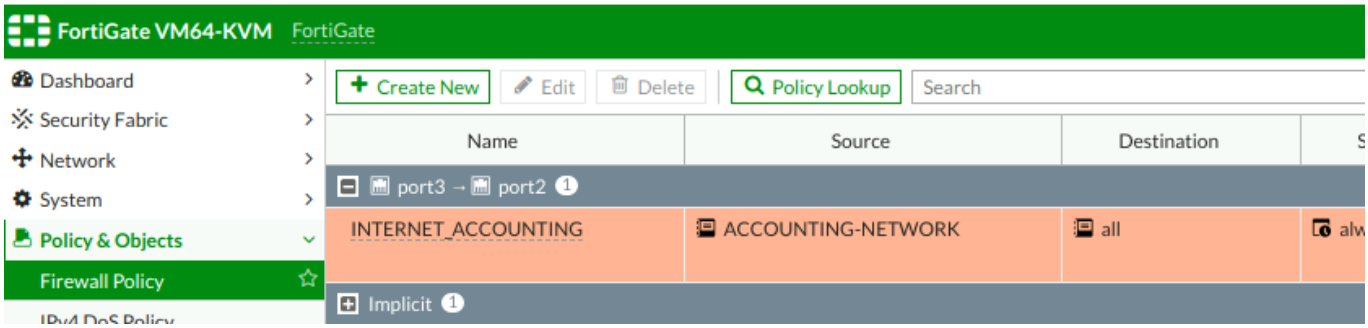
- Create a **new firewall rule**.
  - Name: **INTERNET_ACCOUNTING**
  - Incoming Interface: **port 3**
  - Outgoing Interface: **port 2**
  - Source: **ACCOUNTING-NETWORK**
  - Destination: **all**
  - Service: Both **HTTP** and **HTTPS**
  - Keep **NAT enabled** using outgoing interface address.
  - Under **Security Profiles**:
    - Web Filter: **Enabled**
    - Web Filter Profile: **wf-accounting**
    - SSL Inspection: **SSL certificate-inspection**

→ This basically gives the accounting department internet connection!

Resulting Option: Then press **OK**.



→ Now you have:



Create DNS Network Addresses

- As you noticed before, the accounting network is NOT able to reach the DNS server to resolve websites.
- You need to create two network addresses that contain both DNS servers used by the accounting machines.
- You can do that by accessing the **Policy & Objects > Addresses** menu.

Objectives:

- Create a new **network address object**.
  - Name: **1.1.1.1**
  - Type: **Subnet**
  - IP/Netmask: **1.1.1.1/32**.
  - Interface: **any**
- Create another new **network address object**.
  - Name: **8.8.8.8**
  - Type: **Subnet**
  - IP/Netmask: **8.8.8.8/32**
  - Interface: **any**

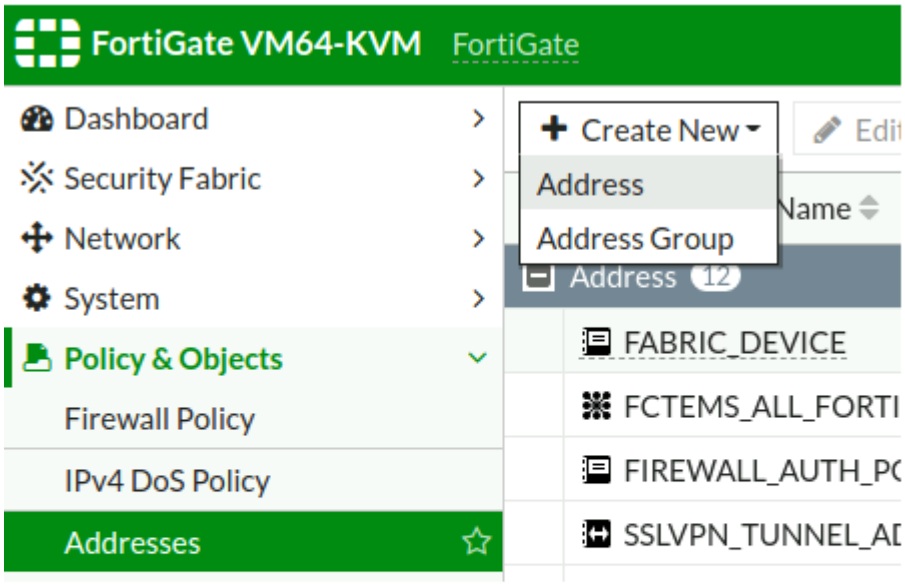
Two new Resulting addresses:

Address 15		
1.1.1.1	Subnet	1.1.1.1/32
8.8.8.8	Subnet	8.8.8.8/32
ACCOUNTING-NETWORK	Subnet	10.0.3.0/24
FABRIC_DEVICE	Subnet	0.0.0.0/0

Create a Network Address Group

- You can create a network address group to better organize your firewall rules. This way you have just one entry containing dozens or hunderds of addresses.

→ You can do that by accessing the **Policy & Objects > Addresses** menu shown below.



- Create a **new address group** object.
  - Group name: **DNS-SERVERS**
  - Members: Both **1.1.1.1** and **8.8.8.8**

Resulting new address group:

Address Group 3		
DNS-SERVERS	Address Group	1.1.1.1 8.8.8.8
G Suite	Address Group	gmail.com wildcard.google.com
Microsoft Office 365	Address Group	login.microsoftonline.com login.microsoft.com login.windows.net

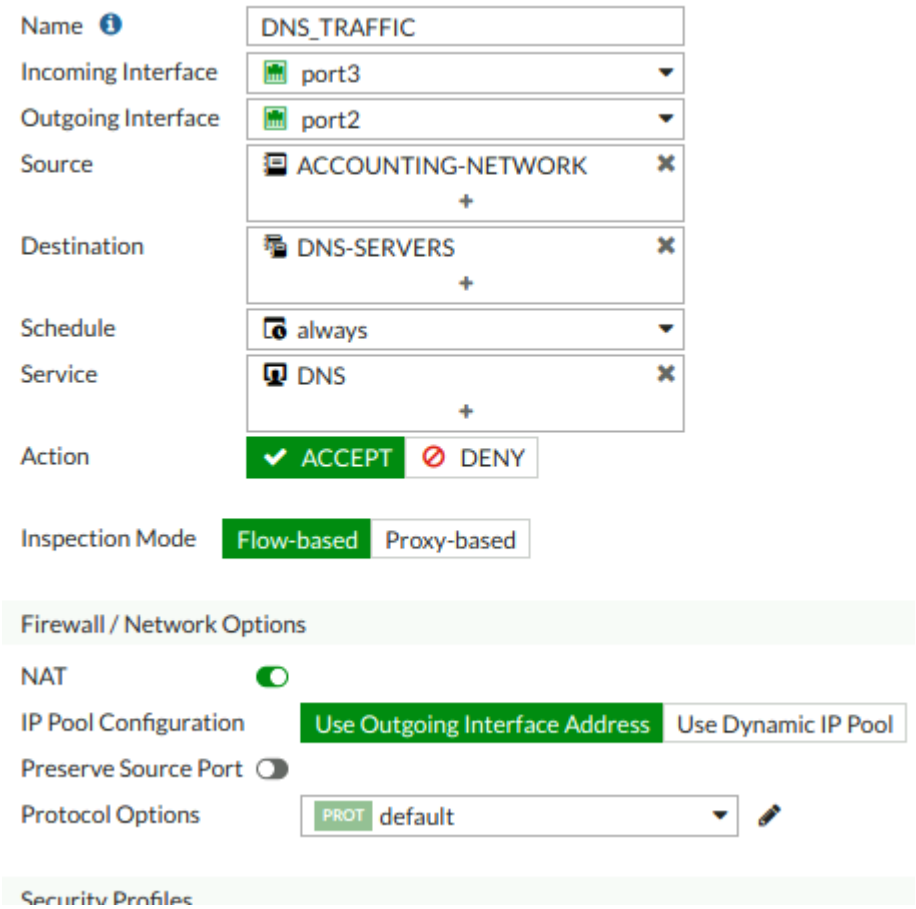
Allow DNS Traffic

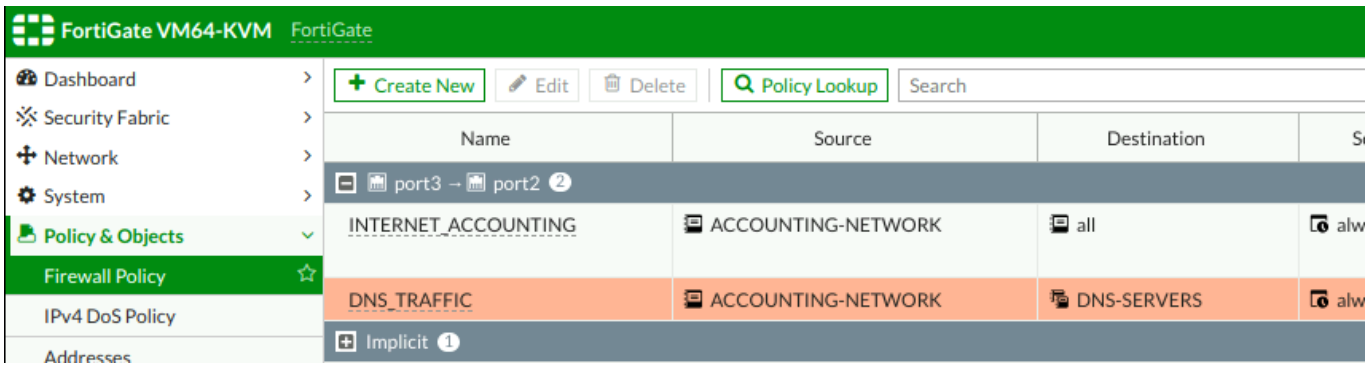
- Now you need to create a rule allowing the DNS traffic. To do that, go back to **Policy & Objects > Firewall Policy**.

Objectives:

- Create a **new firewall rule**.
  - Name: **DNS_TRAFFIC**
  - Incoming Interface: **port 3**
  - Outgoing Interface: **port 2**
  - Source: **ACCOUNTING-NETWORK**
  - Destination: **DNS-SERVERS**
  - Service: **DNS**
  - Keep **NAT enabled** and using the outgoing interface address.
  - All other settings must remain **default**.

Resulting Option:





Validating Firewall Policies

- Now, you need to make sure that your changes are working as expected before you can close both tickets. (Verification)

Access An Accounting Desktop

- Now that you have created the rules, you need to make sure that your changes had the expected outcome in the accounting network.

Objectives:

- Use SSH to connect to the accounting network.
  - Hostname: **desktop-accounting-1**
  - Username: **student**
  - Password: **student**

Action:

```
student@desktop:~$ ssh student@desktop-accounting-1
Warning: Permanently added 'desktop-accounting-1,10.0.3.2' (ECDSA) to the list o
f known hosts.
student@desktop-accounting-1's password:
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

student@desktop-accounting-1:~$
```

Test Internet Access using the Account from the previous step

→ Now that you are connected to a machine under LAN network, you can validate your rules.

Objective:

- Use **curl** to test whether **desktop-accounting-1** has access to **cnn.com**.

Result:

```
student@desktop-accounting-1:~$ curl -Is cnn.com
HTTP/1.1 403 Forbidden
X-Frame-Options: SAMEORIGIN
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff
Content-Security-Policy: frame-ancestors 'self'
Content-Type: text/html; charset="utf-8"
Content-Length: 5014
Connection: Close

student@desktop-accounting-1:~$
```