Managed Firewall

Service Description

Conterra allows customers to request changes to device profiles during the Managed Firewall complete customer lifecycle. Customers can request, via the Managed Services Portal, a change of category. Any change implemented through the portal that does not require Conterra to implement the change does not count towards the monthly change quota. The following defines what is considered to be a Firewall policy change:

- Firewall Policy
- Application Control
- Web Filtering
- DNS Filtering

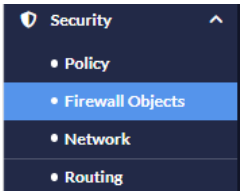
Any change request that varies from the default configuration or Firewall change policy listed above may be completed by Conterra on a time and materials basis. Conterra reserves the right to determine, within its reasonable discretion, whether a change falls within the scope of the Customer's service.

Firewall Policy

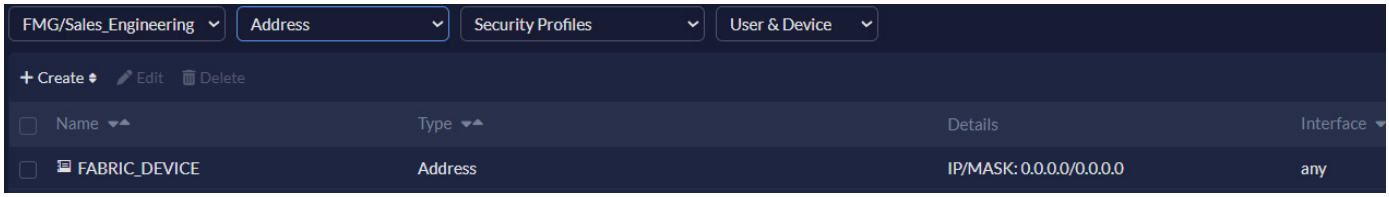
Creating a new policy is a two-step process as outlined in this section.

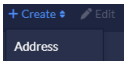
Firewall Policy Step 1

Under the **Security tab**, select **Firewall Objects**.



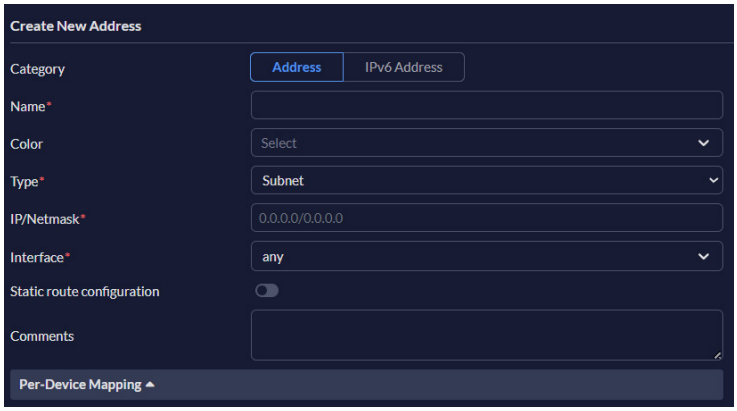
The underlying screen will appear:

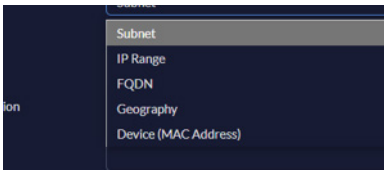


Select **Create**  then **Address** 

1. Enter the name of the asset or category you wish to create a rule around
2. Select the Type. Choices are:
   - **Subnet**
   - **IP Range**
   - **FQDN**
   - **Geography**
   - **Device (Mac Address)**
3. Enter the IP/Netmask
4. Select Interface (recommend leaving this set as “any”)
5. Add Comments for easy identification

Select **Save** at the bottom of the screen.



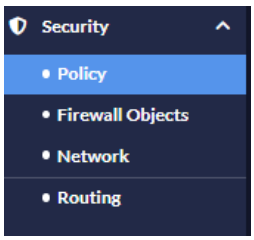


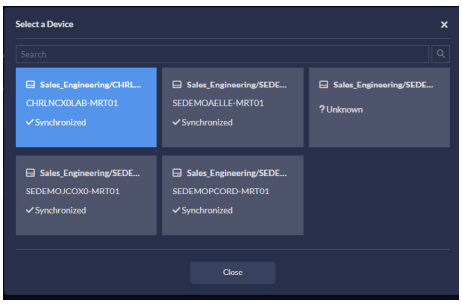
Firewall Policy Step 2

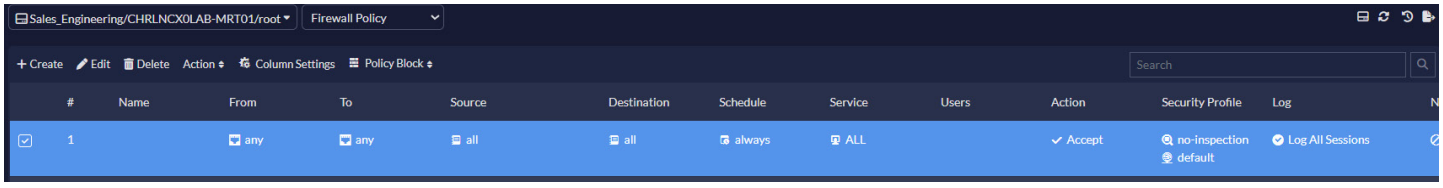
Under the Security tab, select **Policy** to View, **Edit** or **Create a New Policy**.

Select the applicable device.

Once selected, the existing Firewall Policies will be displayed.







Editing an existing Policy

Editing an existing policy is **not** recommended. Any adjustments to firewall policies should be done via the creation of a new policy. Editing an existing rule may result in conflicts and an increased probability of tickets.

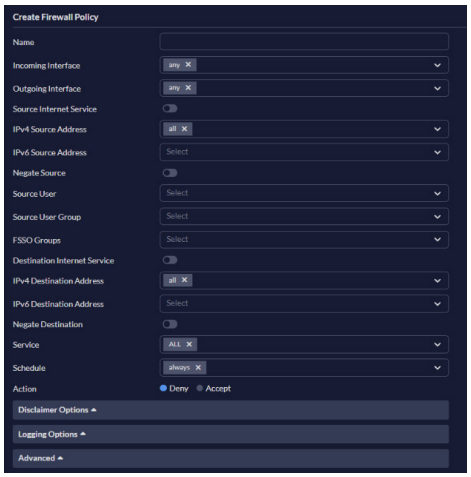
Creating a New Policy

All changes to the Firewall Policy should be done by selecting

Create + Create the key on the page header.

Required field selections to successfully create a firewall policy include:

- Name
- Incoming Interface
- Outgoing Interface
- IPV4 Source
- IPV4 Destination
- Service
- Action



Name

When selecting a Name for your new Policy, be short and as descriptive as possible.

Incoming Interface

The Incoming Interface will always default to "Any," meaning the Policy will be applied to all incoming interfaces. If you need to apply the Policy to specific interfaces, click the dropdown arrow to view all available options. From there, select one or multiple interfaces to which the Policy should apply.

Outgoing Interface

The Outgoing Interface will always default to "Any," meaning the Policy will be applied to all outgoing interfaces. If you need to apply the Policy to specific interfaces, click the dropdown arrow to view all available options. From there, select one or multiple interfaces to which the Policy should apply.

IPV4 Source Address

The IPV4 Source Address will always default to "All," meaning the policy will be applied to all IPV4 sources. If you need to apply the policy to specific IPV4 addresses, click the dropdown arrow to view all available IPV4 source addresses. From there, select one or multiple addresses to which the policy should apply.

IPV4 Destination Address

The IPV4 Destination Address will always default to "All," meaning the policy will be applied to all IPV4 destinations. If you need to apply the policy to specific IPV4 addresses, click the dropdown arrow to view all available IPV4 destination addresses. From there, select one or multiple addresses to which the policy should apply.

Tip: The Object you created in Step 1 should appear in the drop-down list. Select this if applicable.

Service

The Service setting will always default to "All," meaning the policy will be applied to all services. If you need to apply the policy to specific services, click the dropdown arrow to view all available services. From there, select one or multiple services to which the policy should apply.

Action

Action indicates whether you are creating the rule to accept or deny traffic. Select the action based on how the rule should be applied.

Comments

The Comments section is a free-form field where you can provide a detailed description of the rule. This description is visible in the Firewall Policy tab, helping you easily identify the rule's purpose. Although optional, including comments is highly recommended.

Finalizing the Policy

At the bottom of the screen, you are given an option to **Cancel** or **Save**

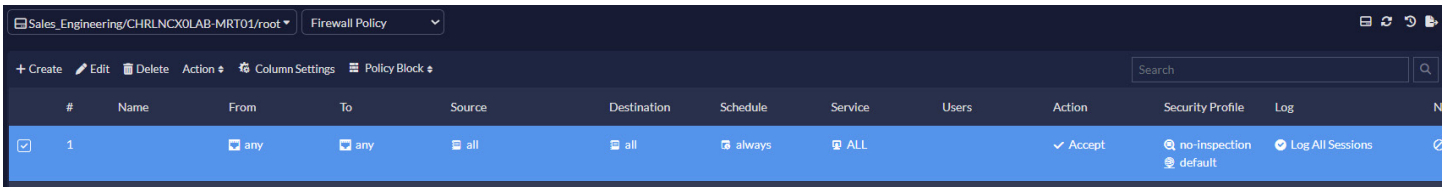
- **Cancel** will return you to the Firewall Policy Tab and all work will be lost
- **Save** will save the Policy and return you to the Firewall Policy Tab

IMPORTANT – To implement the policy you must select the 

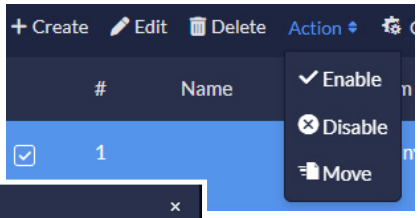
at the top right of the screen. If not implemented, the policy will still appear in the Firewall Policy tab but will not be active.

Firewall Policy Ordering

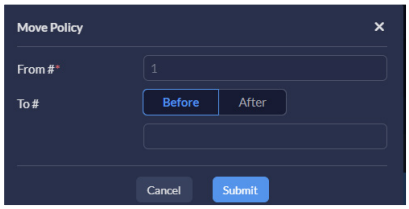
Firewall Policies are enforced in order from top to bottom. How they appear on the Firewall Policy Screen will impact the effectiveness of the Firewall.



To change the order of the Firewall Policies, select the policy you wish to change the order of by choosing **Action** then **Move** from the drop-down screen.

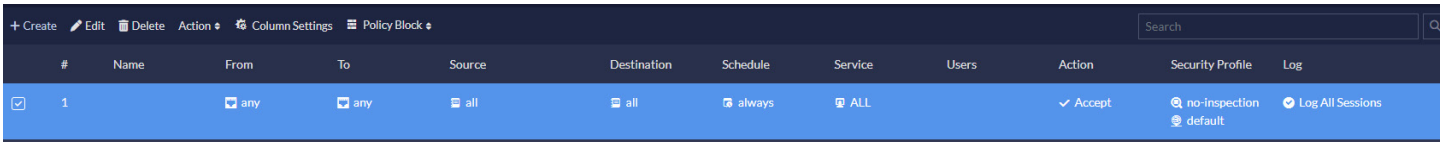


1. Enter the number of the rule placement currently
2. Select **before** or **after**. Select the number from the drop-down box for final placement
3. Select **Submit**



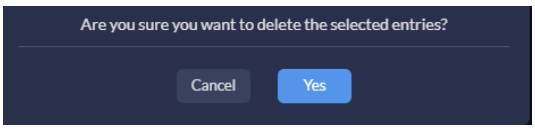
Deleting a Policy

Customer Administrators can delete a Firewall Policy at any time. This can be done by selecting the **applicable policy** from the Firewall Policy Tab.



And then selecting 

The following window will appear. Select the appropriate value.



IMPORTANT – To implement the policy you must select the 

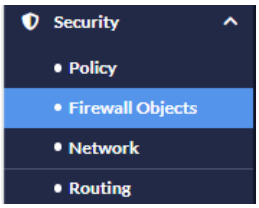
at the top right of the screen. If not implemented, the policy will remain inactive. It will appear in the Firewall Policy Tab but will not be active.

Application Control

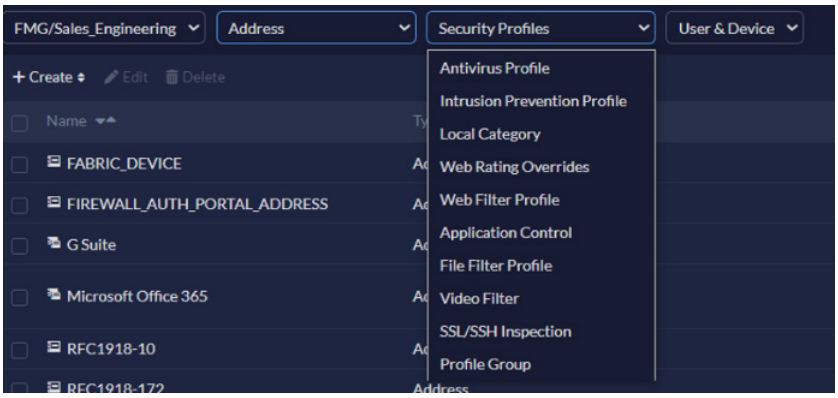
This section outlines the change management options available through the Managed Services Portal. Standard changes are limited to:

- Modifying category treatment to a predefined setting, such as Allow, Block, or Quarantine
- Modifying or adding application overrides
- Modifying or adding filter overrides

Under the **Security tab**, select **Firewall Objects**.



The first selection box will default to Address. Leave selection as is. In second selection box, select **Application Control**.



Application Control Profiles assigned to the Firewall can be seen on this screen.

For first-time users, this will be one of the three (3) default profiles you selected during your initial activation.

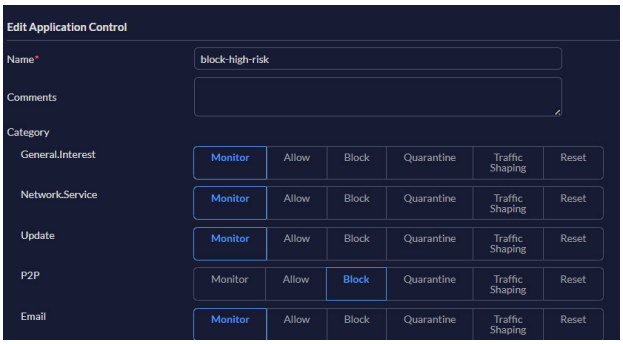
It is highly recommended that users edit the existing profile and not create a new profile.

Select the profile you wish to make changes to and then select **Edit** 

Categories will appear on the screen with current treatment.

To change treatment, select the desired treatment.

Please note that selecting **"Quarantine"** will only function if the device has available internal storage. The Managed Services Portal does not restrict users from choosing the "**Quarantine"** option in any scenario.



Application and Filter Overrides

By default, all application controls are limited to their assigned categories upon initial installation. If an application needs to be treated differently than its defined category, an Application and Filter Override Rule can be created to customize its handling.

Creating an Application Override Rule

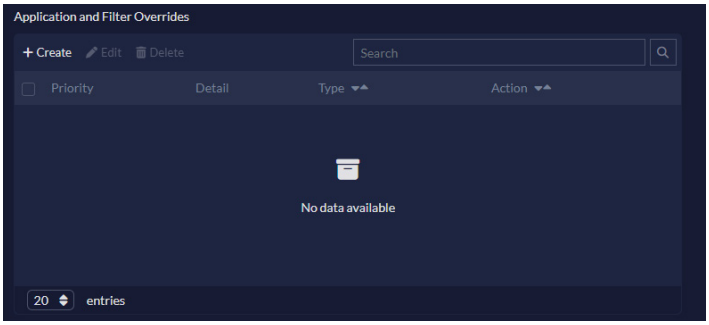
Select the action to be applied.

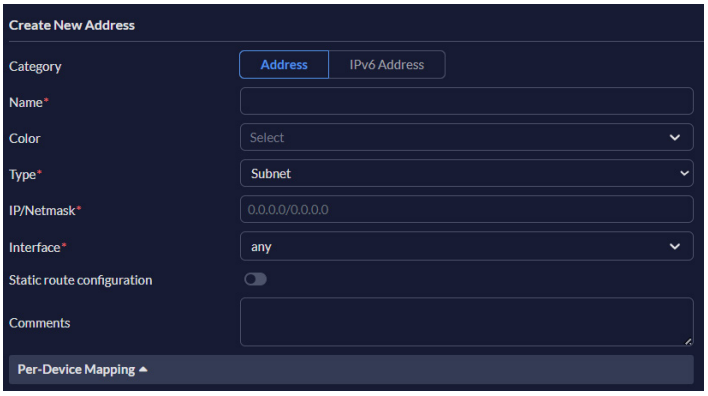
Select the application(s) to apply the rule.

Filters available are:

- Category
- Popularity
- Technology
- Behavior
- Vendor
- Protocols
- Risk

Select all applicable filters.



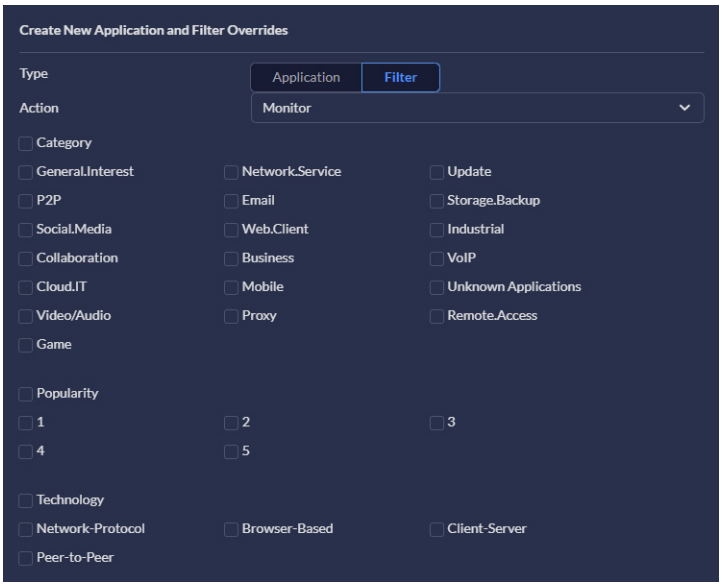


Creating a Filter Override Rule

Select the action to be applied.

Filters available are:

- Category
- Popularity
- Technology
- Behavior
- Vendor
- Protocols
- Risk



Select all applicable filters.

Finalizing the Policy

At the bottom of the screen, you are given an option to **Cancel** or **Save**

- **Cancel** will return you to the Firewall Policy Tab and all work will be lost.
- **Save** will save the policy and return you to the Firewall Policy Tab.

IMPORTANT – To implement the policy you must select the 

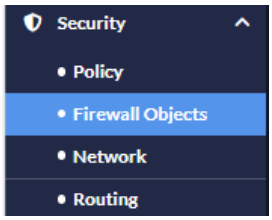
at the top right of the screen. If not implemented, the policy will remain inactive. It will appear in the Firewall Policy Tab but will not be active.

Web Filter

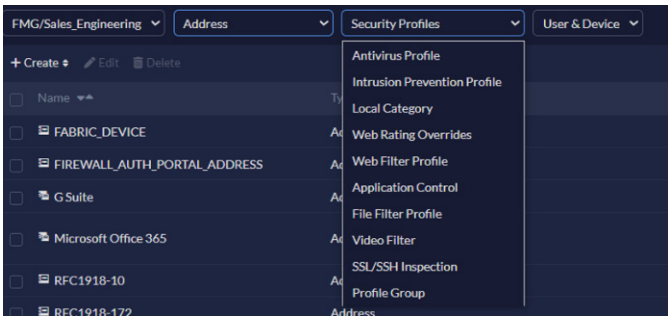
This section outlines what change management is available through the Managed Services Portal. Standard changes are limited to:

- Modification of Category treatment to a standard defined treatment including Allow & Block

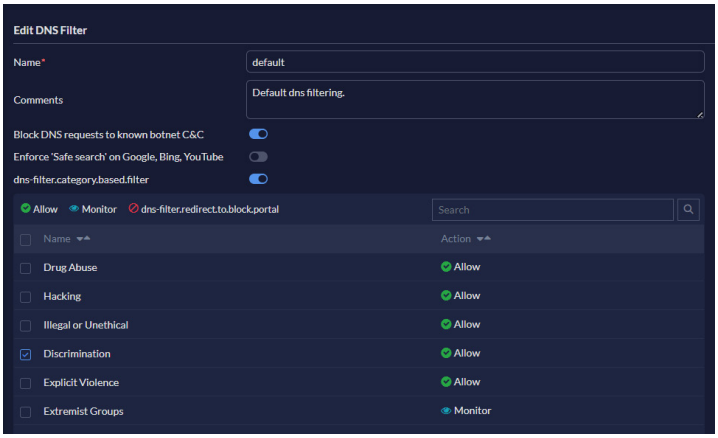
Under the **Security tab**, select **Firewall Objects**.



The first selection box will default to Address. Leave selection as is. In second selection box, **Select Web Filter Profile**.



Web Filtering Profiles assigned to the Firewall can be seen on this screen.



For first-time users, this will be one of the three (3) default profiles you selected during your initial activation.

It is highly recommended that users edit the existing profile and not create a new profile.

Select the profile you wish to make changes to and then select **Edit** 

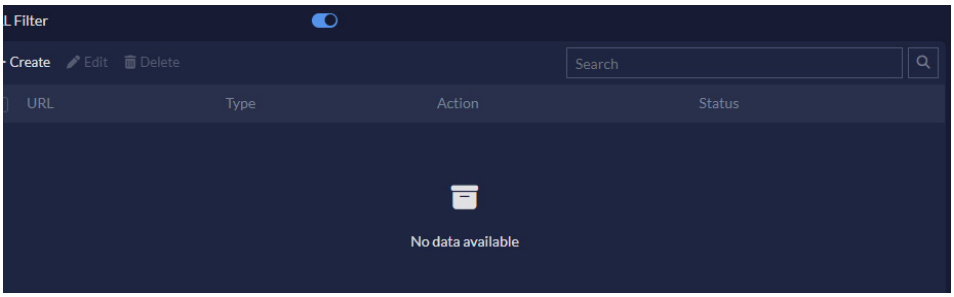
A list of category-based filters will be shown along with the Action.

To change Actions, select the category you want to change and then select the Action you want to be applied.

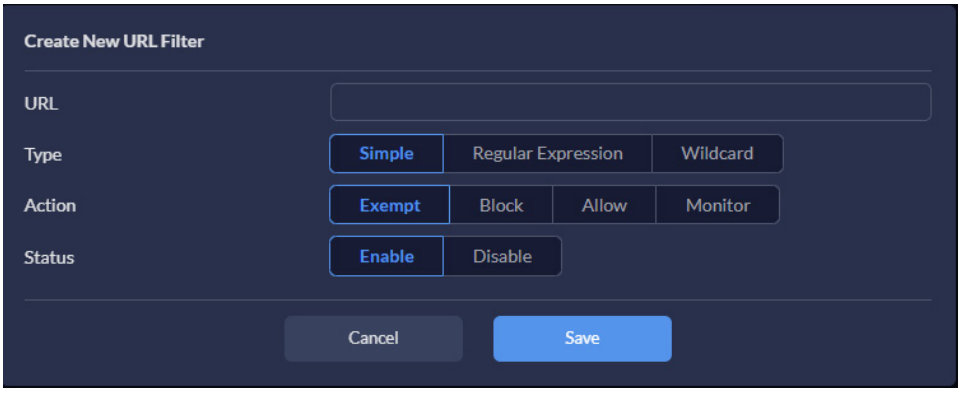
URL Filtering

There are three Static URL Filters available. Block invalid URLs and Block malicious URLs discovered by sandbox are toggles. They are by default turned off but can be changed by toggling this to ON. When turned on the button next to the category will appear as 

Where specific URLs within a category are allowed or blocked and the desire is to change treatment for only that URL, then Select **URL Filter.**



By default, there will be no URL filters at installation. Any rules created post-install will appear on this screen. To add a URL filter, select the **Create button**.



1. Type in the URL to create a rule around
2. Select the Type
3. Choose the Action or treatment desired
4. Select the Status:
    - Select **Enable** if the identified site belongs to a category that is blocked
    - Select **Disable** if the identified site belongs to a category that is allowed
5. Select **Save**

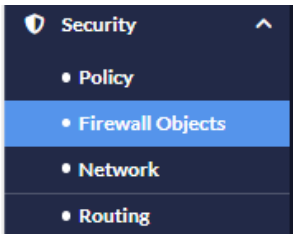
IMPORTANT – To implement the filters you must select the 

at the top right of the screen. If not implemented, the filters will remain inactive. They will appear in the Web Filter Tab but will not be active.

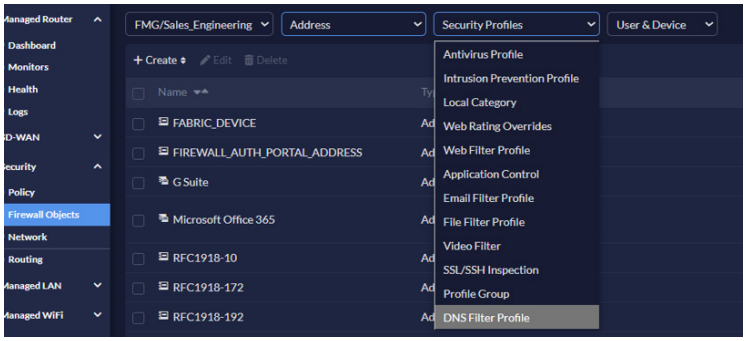
DNS Filter

- Modification of Category treatment to a standard defined treatment including Allow, Monitor, Block
- Requests for whitelisting or blacklisting of domains

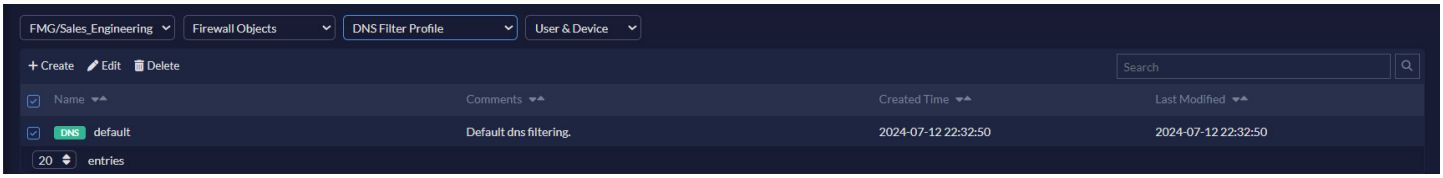
Under the **Security tab**, select **Firewall Objects**.



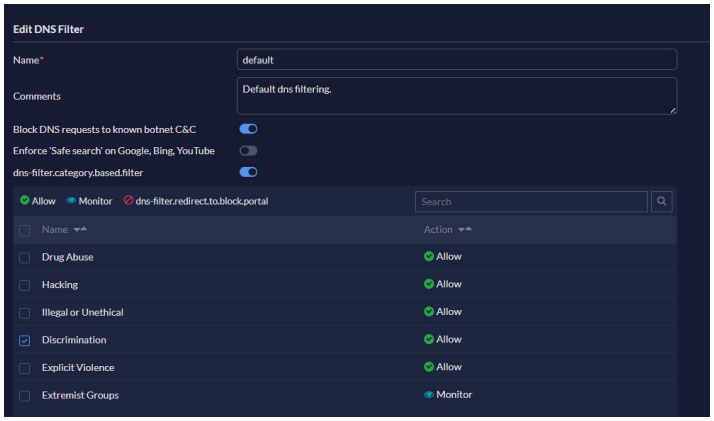
The first selection box will default to Address. Leave selection as is. In the second selection box, Select **DNS Filter Profile**.



DNS Filter Profiles can be seen on this screen.



First-time users will have a single DNS Filter profile available. This profile is one of the three identified during installation. To adjust the profile, select **Edit** 



A list of category based filters will be shown along with the Action.

To change Actions, select the category you want to change and then select the Action you want to be applied.

Static Domain Filters

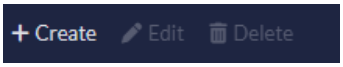
Enable to define local static domain filters to allow or block specific domains. The local domain filter has a higher priority than the FortiGuard category-based domain filter.

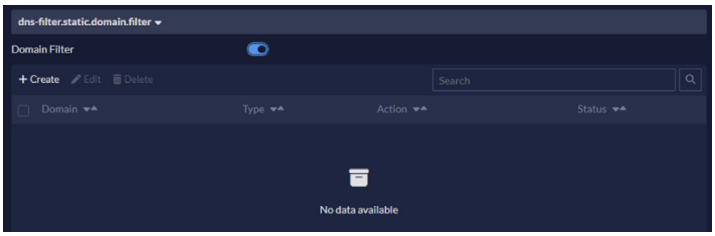
Available options can be viewed towards the bottom of the DNS Filter Profile tab.

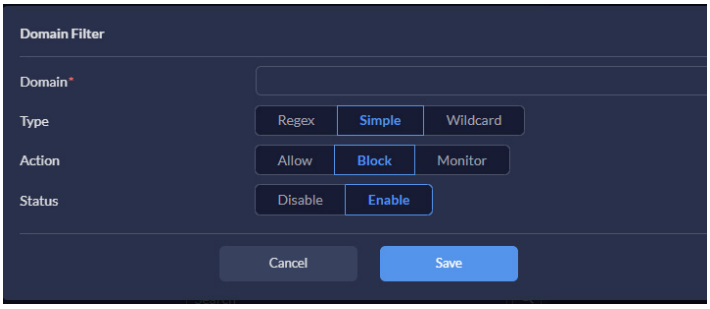
Creating a Domain Filter

Toggle the Domain Filter button to appear as 

Select **Create**







1. **Domain:** Enter a domain.
2. **Type:** Select Simple, Regex, or Wildcard.
3. **Action:** Select Block, Allow, or Monitor.
4. **Status:** Enable or Disable this domain filter.
5. **Select Save**

IMPORTANT – To implement the filters you must select the 

at the top right of the screen. If not implemented, the filters will remain inactive. They will appear in the Web Filter Tab but will not be active.