How to Create Rules

https://campus.barracuda.com/doc/91985195/

Create a firewall rule and select an application as source or target. When assigned to a firewall and implemented, changes made to a rule take immediate effect for all traffic the rule applies to. When selecting a firewall for rule assignment, Barracuda CloudGen Firewalls can be searched in the asset database; third-party firewalls need to be searched using their DNS name.

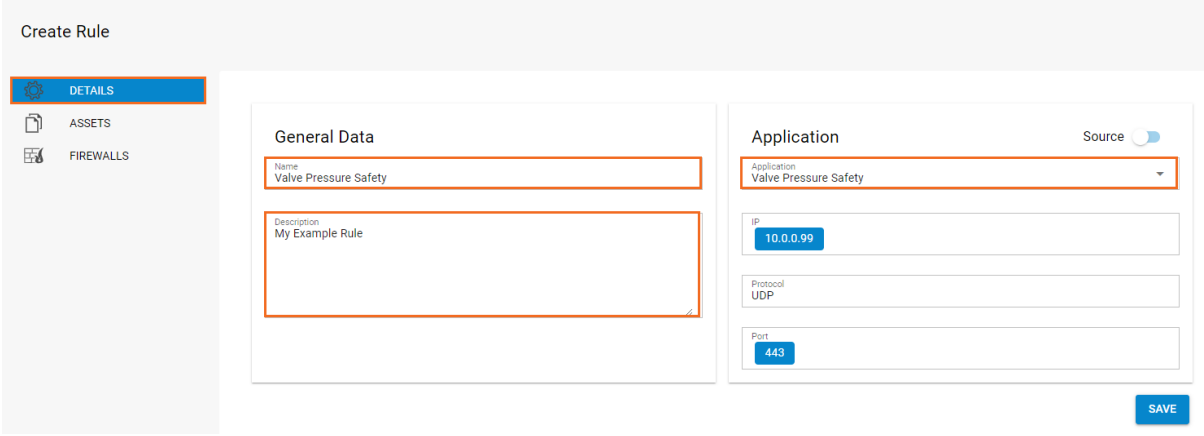
The asset database, a Microsoft SQL database used to query assets such as PLC, robots, etc., is primarily used to import the IP address or DNS of the asset as well as the responsible service provider and creator. Information about firewalls and control centers, and the assignment between firewalls and asset, are also queried from the asset management.

Create a Rule

1. Log into the Barracuda Policy Manager.
2. Click the **Rules** tab.
3. In the top-right corner, click **+** to add a rule. The **Create Rule** window opens.

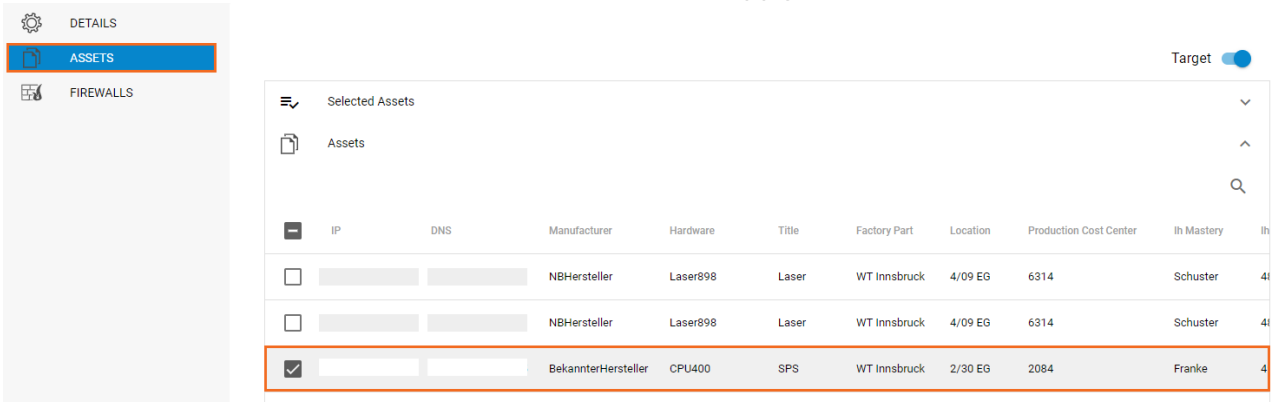
Configure the Rule Details

1. In the **General Data** section:
    1. Enter a **Name** for the rule.
    2. Enter a **Description**.
2. In the **Application** section:
    1. Use the blue button on the top right to specify if the application is used as **Source** or **Target** in the rule.
    2. Select the application the rule should apply to. **IP address**, **Protocol**, and **Port** are filled in automatically.



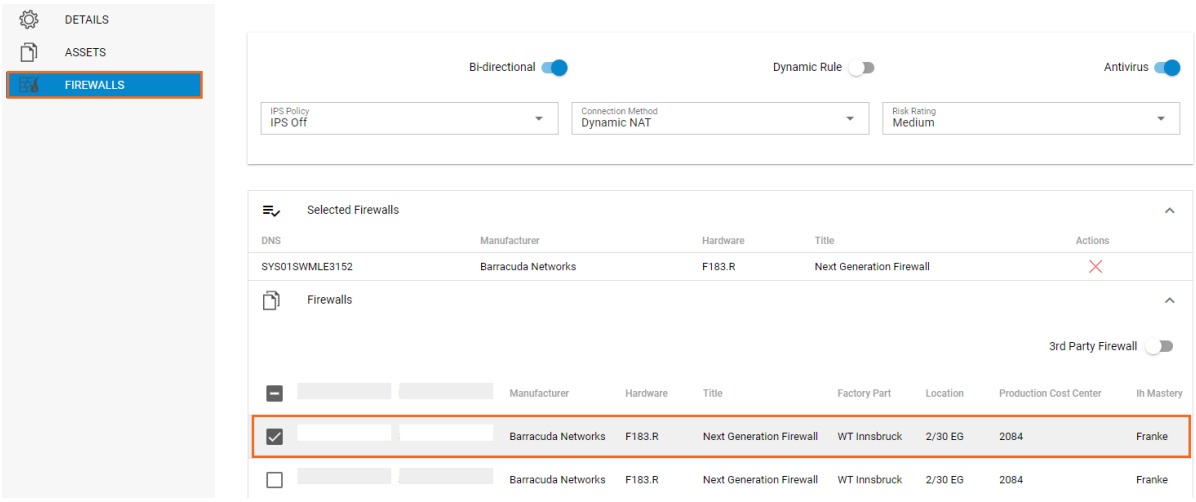
Configure Assets for the Rule

1. Click the **Assets** link on the left. The **Assets** window opens.
2. Use the blue button on the top right to specify if the asset is used as **Source** or **Target** in the rule.
3. Expand the **Assets** list by clicking the arrow icon on the right.
4. Select the check box next to the asset the rule should apply to.



Apply the Rule to a Firewall

1. Click the **Firewalls** link on the left. The **Firewalls** window opens.
2. In the top section, define the following settings:
   - **Bi-Directional** – Select the check box if the rule applies in both directions.
   - **Dynamic Rule** – Select if the rule applies according to a time schedule.
   - **Antivirus** – Enable virus scanning for traffic that passes the rule.
   - **IPS Policy** – Select an Intrusion Prevention System (IPS) profile for the rule.
   - **Connection Method** – Select the connection method:
     - **Dynamic NAT** – The firewall uses the routing table to find a suitable interface for routing the packet and uses the IP address of the relevant interface as the new source IP address.
     - **Mapped** – The firewall rewrites both the destination and the source address of the connection, using a NAT table.
     - **Original Source** – The source IP address of the packet is not modified.
   - **Risk Rating** – Assess the risk of the rule based on criteria depending on the network dependency, rated from **Critical** (highest risk) to **Very Low** (lowest).



3. Click **Save** to save your configuration

After completing these steps, the rule is listed under **Rules** with the status "Open". Existing applications and policies can be viewed in list views by users with corresponding permissions. The rule applicant can now assign the ticket to 'Architect' for review and further processing. To access the settings, click the edit icon ( ) on the right of an entry in the list. To request approval for the rule, expand the status (**Open**) on the top right of the window and select **Request**. For more information on the processing of rules, see Application and Rules Assignment.

Customizing Rule Details

When editing a rule, a new sidebar becomes available, offering a settings menu similar to the applications configuration. Here, users with appropriate permissions can change details, add comments and attachments, view the ticket history, and process the rule. For more information on how to customize ticket entries, see How to Create Applications.

Figures