How to Create Rules

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

Create a firewall rule and select an application as source or target. When selecting a firewall for rule assignment, Barracuda CloudGen Firewalls can be searched in the asset database; third-party firewalls can be searched as well, based on predefined patterns.

> 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, and the assignment between firewalls and asset, are also queried from the asset management.

Before You Begin

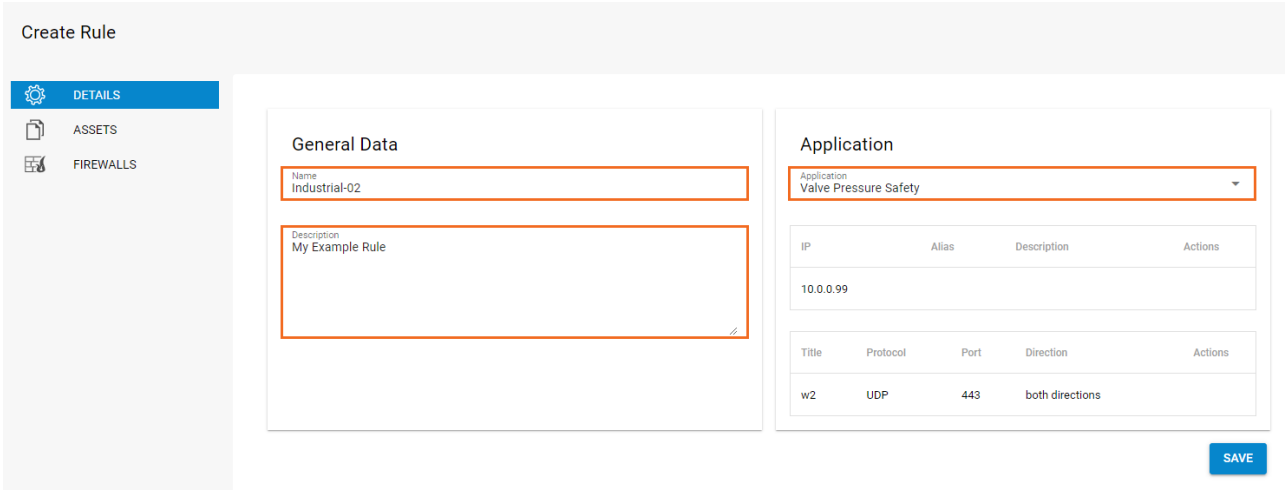
- Create an application. For more information, see How to Create Applications.
- Introduce the Control Center-managed firewalls on the Firewall Policy Manager. For more information, see **Add Your Firewall Control Centers** in Get Started.

Create a Rule

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

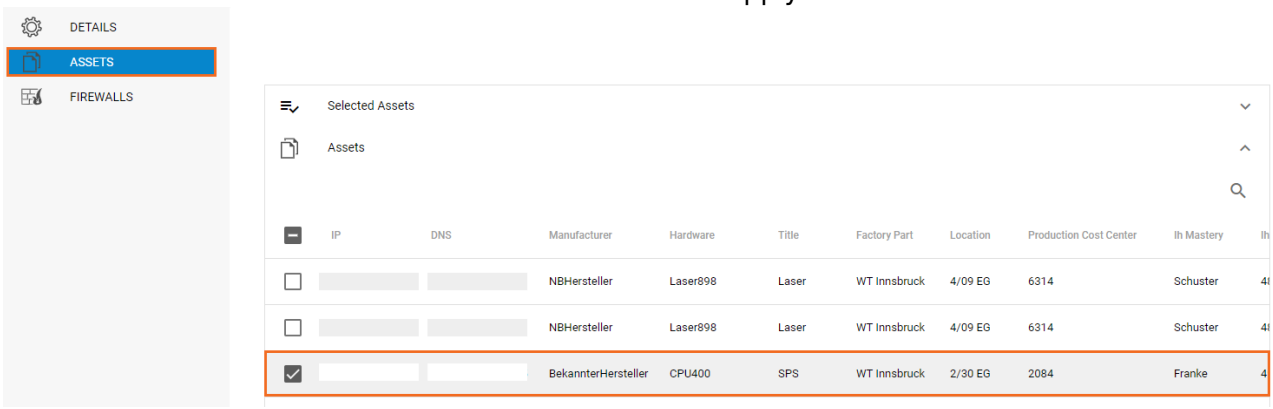
Configure the Rule Details

1. In the **General Data** section:
    1. Enter a **Name** for the rule.
    2. Enter a **Description**.
2. In the **Application** section, select the application the rule should apply to. **IP address**, **Protocol**, and **Port** are filled in automatically.



Configure Assets for the Rule

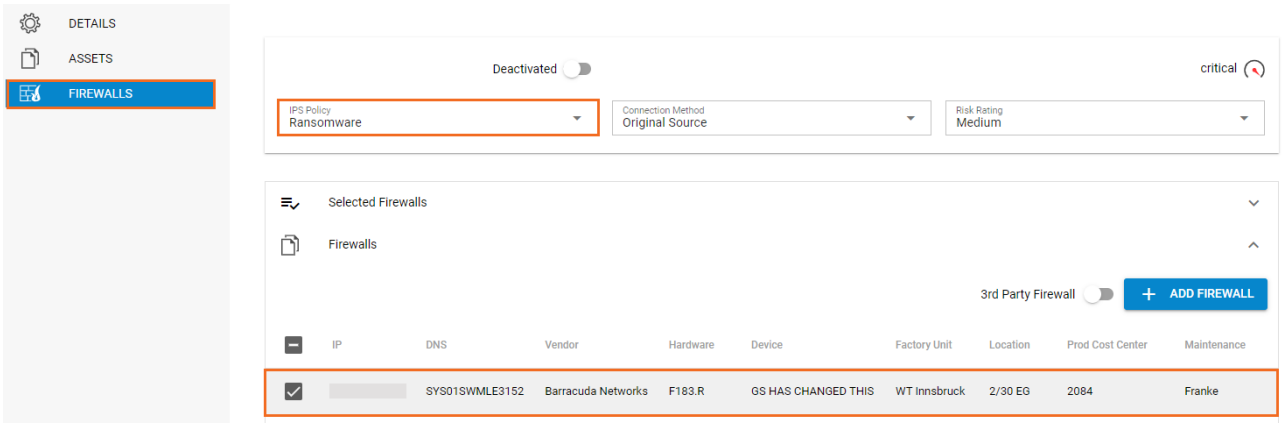
1. Click the **Assets** link on the left. The **Assets** window opens.
2. Expand the **Assets** list by clicking the arrow icon on the right.
3. Select the check box next to the asset the rule should apply to.



Apply the Rule to Your Firewalls

After a rule has been created that contains an application as source or target, and the status of the request was set to "Approved CISO", the rule can be assigned to Control Center-managed firewall units.

1. Click the **Firewalls** link on the left. The **Firewalls** window opens.
2. In the top section, select an Intrusion Prevention System profile (**IPS Policy**) for the rule.
3. Expand the **Firewalls** list below and select the CC-managed units the rule should be applied to.



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

After completing these steps, the rule is listed under **Rules**. To request approval for a 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.

When a rule has been assigned to a Control Center, the ticket is given the status "Queued" until the rule gets successfully implemented on the managed firewall units. If the transfer to a Control Center does not work, set the ticket status to "Return" and re-process the rule. As soon as the rule is successfully processed, it has the status "Implemented" and becomes visible in the ruleset of the selected firewalls. To view the rule, log into a CC-managed Firewall and go to **Forwarding Rules**, or, when using a Distributed Firewall Service, access the **Local Ruleset**.

To guarantee a smooth workflow, and to avoid conflicts, name changes and modifications to rules created on the Firewall Policy Manager must be done only on the Firewall Policy Manager and not on the firewall itself. For information on how to re-process or download rules, see Managing Rules on the Firewall Policy Manager.

Figures