How to Restrict Enabling of Dynamic Firewall Rules

https://campus.barracuda.com/doc/96026117/

Dynamic firewall rules can be present in multiple rulesets, so it may be necessary to set time restrictions for these rules to be active and enabled. Administrators can also prevent certain users from enabling firewall rules in one ruleset but allow it in another ruleset. User groups that are allowed to use the Dynamic Firewall Rules resource can then enable and/or disable the rules via the SSL VPN portal or CudaLaunch as configured in the Dynamic Firewall Rules settings . Admins can also apply time restrictions to dynamic rules and, to prevent users from enabling a rule forever, set a time frame by entering a minimum and maximum time for the rule to be enabled.

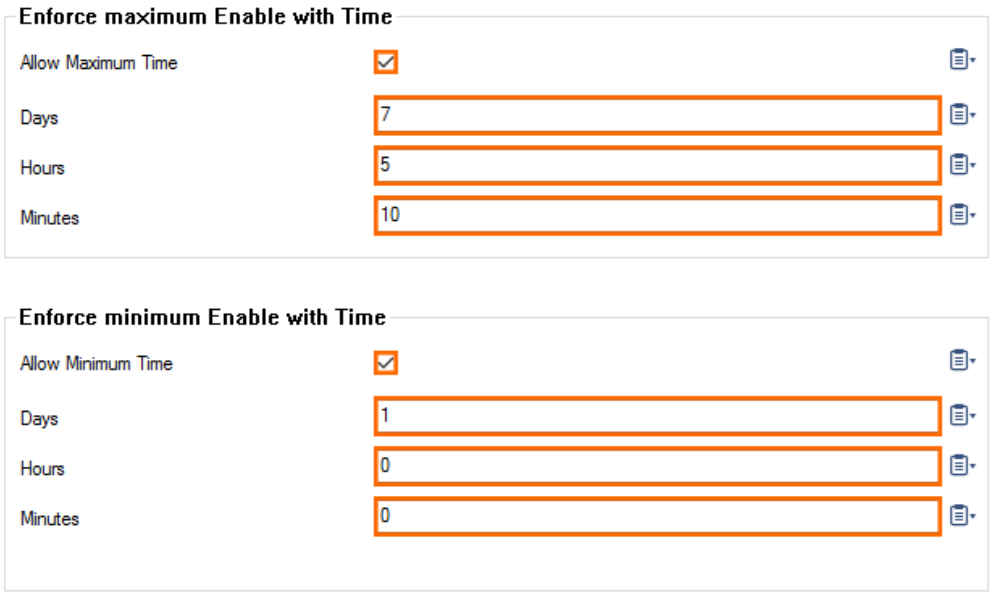
Before You Begin

- Configure SSL VPN for the CloudGen Firewall. For more information, see How to Configure the SSL VPN Service.
- Create a dynamic access or application rule. For more information, see How to Create and Activate a Dynamic Access Rule.
- Create the Dynamic Rule Resource for SSL VPN. For more information, see How to Activate Dynamic Firewall Rules for Remote Connections via SSL VPN.

Set Restrictions to Dynamic Firewall Rules

1. Go to **CONFIGURATION > Configuration Tree > Box > Assigned Services > VPN-Service > SSL-VPN**.
2. In the left menu, select **Dynamic Firewall Rules**.
3. Click **Lock**.
4. In the **Firewall Rule Activation table**, edit the rule you wish to apply the restrictions to. The **Firewall Rule Activation** window opens.
   (You can also click **+** to add a new entry for a dynamic rule. For more information, see How to Create and Activate a Dynamic Access Rule .)
5. Verify the **Active** check box is selected.
6. In the **Allowable Actions** section, select which actions should be allowed for the user group who can access the dynamic rule resource:
   - **Allow Enabling** – Allow users to enable the rule.
   - **Allow Enabling with Time** – Allow users to enable the rule for a specified time frame.
   - **Allow Disabling** – Allow users to disable the rule.

7. (Optional) When selecting **Allow Enabling with Time**, set a minimum and/or maximum time for the rule to be enabled:
   - To allow a maximum time in days, hours, and minutes:
     1. Select the **Allow Maximum Time** check box.
     2. Enter the maximum time for the rule to be enabled:
        - **D ays** – Enter a value from 0 - 999.
        - **Hours** – Enter a value from 0 - 23.
        - **Minutes** – Enter a value from 0 - 59.
   - To allow a minimum time in days, hours, and minutes:
     1. Select the **Allow Minimum Time** check box.
     2. Enter the time for the rule to be enabled:
        - **D ays** – Enter a value from 0 - 999.
        - **Hours** – Enter a value from 0 - 23.
        - **Minutes** – Enter a value from 0 - 59.



When choosing to set both a maximum and minimum time, the maximum time entered must be greater than the maximum time, otherwise the timeframe conflicts and you cannot save the configuration.

8. Click **OK**.
9. Click **Send Changes** and **Activate**.

Users that are allowed to use this Dynamic Firewall Rule resource can now enable and/or disable the firewall rule according to the configured settings, in Barracuda Firewall Admin, from the SSL VPN web portal, and on CudaLaunch.

For more information, see SSL VPN Web Portal User Guide and CudaLaunch for Windows and macOS.

Figures

1. rule_activation01.png
2. rule_activation02.png