How to Create File Content Policies

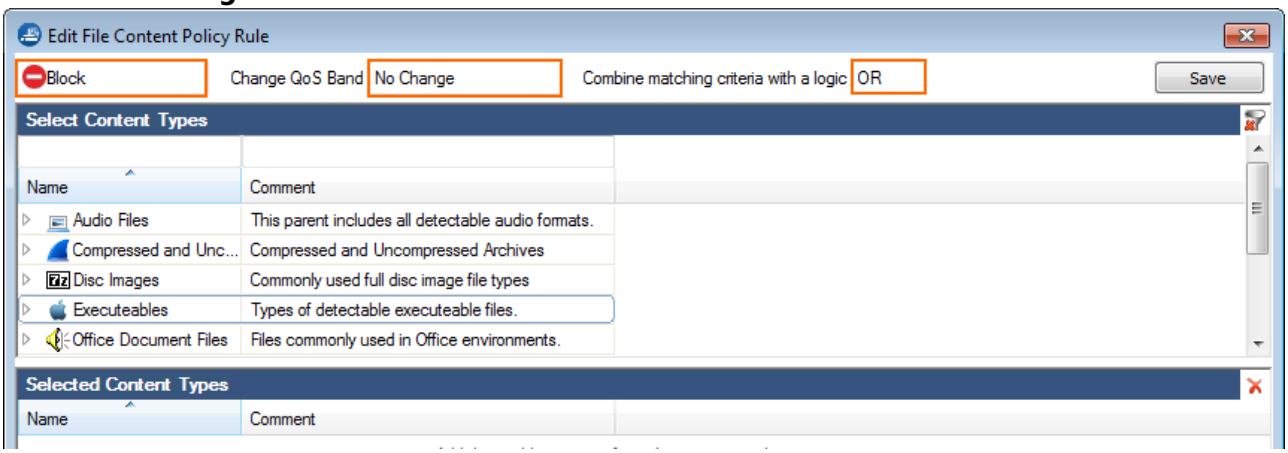
https://campus.barracuda.com/doc/46209109/

File content policies contain a list of policy rules that are evaluated from top to bottom. The action set in the first matching policy rule is executed. You must include at least one of the following criteria and define if the criteria are combined with a Boolean AND or OR. Empty criteria are ignored.

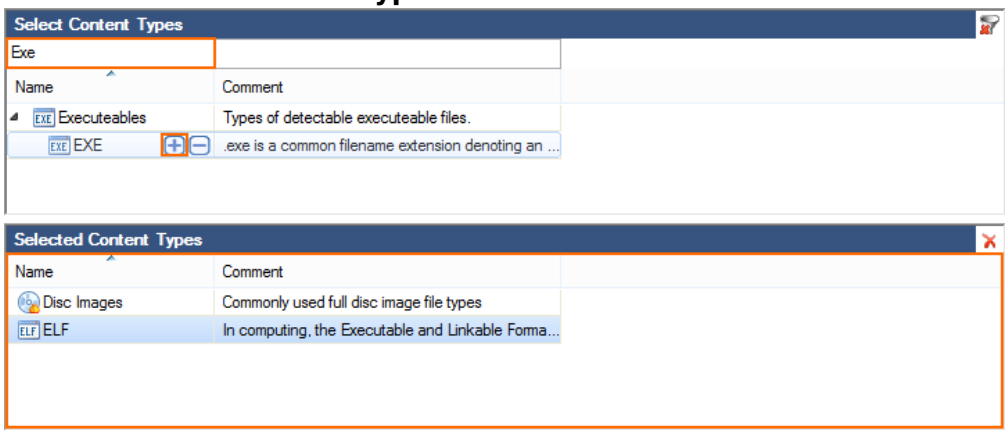
- **Content Type** – You can add file types by category or individually.
- **File Name patterns** – Pattern matching the file name.
- **MIME Type patterns** – Pattern matching the MIME type patterns for HTTP and SMTP. If a MIME type pattern is configured, HTTP, SMTP, and FTP connections that do not include a MIME type will cause the file content policy rule to not match if used with a Boolean AND.

In this article

9. (optional) Select the logic operator how the matching criteria are combined: AND or OR. Default: OR.
10. (optional) Change the QoS Band.
11. Select the policy for the **File Content Policy rule**. For more information, see File Content Filtering in the Firewall.
    - **Allow** – allow and log (logfile and NextGen Admin)
    - **Block** – block and log (logfile and NextGen Admin)
    - **Alert** – allow and silently log (logfile only)
    - **Do not log** – allow

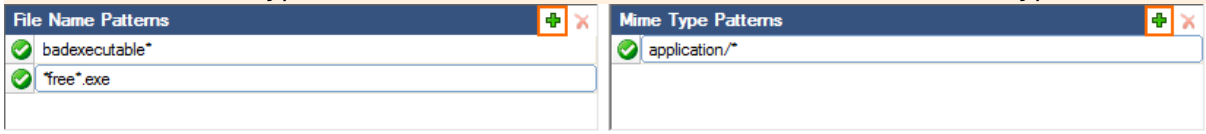


12. Configure at least one of the following:
    - **Content Type** – Use the filter to find the content type and double-click the entry to add it to the **Selected Content Types** section.



    - **File Name Pattern** – In the **File Name Patterns** section, click **+** to add one or more file name patterns. File name patterns may contain * and **?** wildcard characters.
    - **MIME Type Pattern** – In the **Mime Types Patterns** section, click **+** to add one or more MIME type patterns. MIME type patterns may contain * and **?** wildcard characters.

If MIME type patterns are used in combination with a Boolean AND, all connections without a MIME type are blocked. FTP connections never include a MIME type.



13. Click **Save**.
14. (optional) Add additional **File Content Policy Rules**.
15. Use the up and down arrows ( ) to sort the policy rules so that the policy rule that should match first is on top.
16. Click **Save**.
17. Click **Send Changes** and **Activate**.

To use the file content policy in an application rule, see How to Configure File Content Filtering in the Firewall.

Figures

1. file_content_00.png
2. file_content_01.png
3. file_content_02.png
4. file_content_03.png
5. file_content_up_down.png