

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

Before You Begin

Verify that the **Feature Level** of the Forwarding Firewall is **6.2** or higher.

Create a File Content Policy Object

1. Go to **CONFIGURATION > Configuration Tree > Box > Virtual Servers > your virtual server > Assigned Services > Firewall > Forwarding Rules**.
2. Click **Lock**.
3. From the left menu, select **File Content**.
4. Right-click the table and select **New File Content Policy**. The **Edit File Content Policy Object** window opens.
5. Enter a **Name**.
6. Select the default policy:
 - **Allow**
 - **Alert**
 - **Do not log**
7. Click **+** to add a **File Content Policy Rule**.
8. Double-click the new file content policy rule. The **Edit File Content Policy Rule** windows opens.

Name: Save

Comment:

Default Action:

File Content Policy Rules		
Action	QoS	Match
Block	No Change	

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](#).
 - o **Allow** – allow and log (logfile and NextGen Admin)
 - o **Block** – block and log (logfile and NextGen Admin)
 - o **Alert** – allow and silently log (logfile only)
 - o **Do not log** – allow

Block No Change OR Save

Select Content Types	
Name	Comment
Audio Files	This parent includes all detectable audio formats.
Compressed and Unc...	Compressed and Uncompressed Archives
Disc Images	Commonly used full disc image file types
Executeables	Types of detectable executable files.
Office Document Files	Files commonly used in Office environments.

Selected Content Types	
Name	Comment

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

Select Content Types	
Name	Comment
Exe	
Executeables	Types of detectable executable files.
EXE	.exe is a common filename extension denoting an ...

Selected Content Types	
Name	Comment
Disc Images	Commonly used full disc image file types
ELF	In computing, the Executable and Linkable Forma...

- o **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.
- o **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.

File Name Patterns	Mime Type Patterns
<input checked="" type="checkbox"/> badexecutable*	<input checked="" type="checkbox"/> application/*
<input checked="" type="checkbox"/> *tree*.exe	

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

© Barracuda Networks Inc., 2019 The information contained within this document is confidential and proprietary to Barracuda Networks Inc. No portion of this document may be copied, distributed, publicized or used for other than internal documentary purposes without the written consent of an official representative of Barracuda Networks Inc. All specifications are subject to change without notice. Barracuda Networks Inc. assumes no responsibility for any inaccuracies in this document. Barracuda Networks Inc. reserves the right to change, modify, transfer, or otherwise revise this publication without notice.