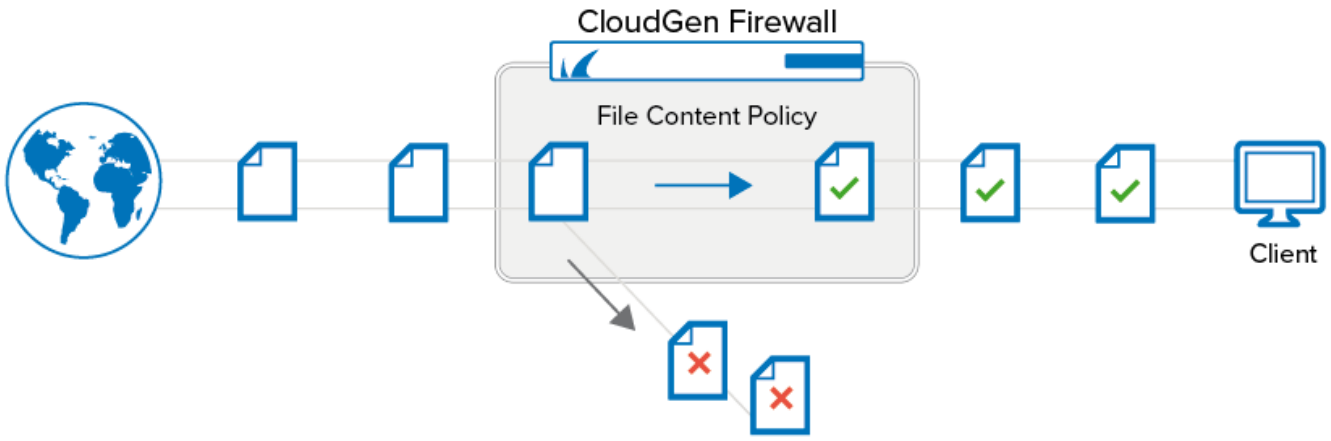
File Content Filtering in the Firewall

https://campus.barracuda.com/doc/96026241/

The CloudGen Firewall offers real-time file content filtering for HTTP, HTTPS, FTP, SMTP, and SMTPS connections. File content policies are evaluated and executed only if the feature is enabled in the matching access rule and the file content policy object is included in the matching application rule. If a file is blocked due to a file content policy, the user will see the following behavior, depending on what type of connection is blocked:

- **HTTP** – Redirect to a customizable block page or connection reset is possible, depending on which Application Control features are used.
- **HTTPS** – Redirect to the customizable content block page. For more information, see How to Configure Custom Block Pages and Texts.
- **FTP** – Connection is reset.
- **SMTP / SMTPS** – Attachment is replaced by an attachment containing a customizable text. For more information, see How to Configure Custom Block Pages and Texts.

File content policies can be applied for uploading and downloading files via FTP and SMTP/S and for downloading via HTTP/S.



File Content Policy Objects

File content policy objects contain a list of policy rules that block or allow the file transfer. Each policy rule defines a set of criteria that can be combined with either a Boolean AND or OR. You can prioritize file transfers by changing the assigned QoS band for the duration of the transfer. Depending on the selected action, matching file transfers are allowed or blocked, with or without logging:

- **Allow** – Allow file transfer, log the traffic, and show file content information in Firewall Live, History, or Monitor.

- **Alert** – Allow the file transfer and show file content information in Firewall Monitor.
- **Block** – Block the file transfer, log the traffic, and show file content information in Firewall Live, History, or Monitor.
- **Do not log** – Allow the transfer, but do not log. Do not show file content information in Firewall Live, History, or Monitor.

If the file content policy object contains multiple policy rules, they are evaluated from top to bottom. The action of the first matching rule is executed. If none of the policy rules match, the default action of the policy action is carried out. Definitions for new file content types are updated regularly via Energize Updates.

For more information, see How to Create File Content Policies.

Content Filtering in the Firewall

To use the content filter policies, you must create an access rule matching your HTTP, HTTPS, FTP, SMTP, and/or SMTPS traffic and enable Application Control, File Content Scan, and, optionally, SSL Inspection. The content policy objects are added to the application rule. The file content policy is evaluated only when the application rule matches and a file transfer is detected. If the QoS band is adjusted in the file content policy rule, the change is active only for the duration of the file transfer.

For more information, see How to Configure File Content Filtering in the Firewall.

Figures