File Upload Protection

https://campus.barracuda.com/doc/98216239/

File upload protection incorporates both Advanced Threat Protection (BATP) and Virus Scanning. The Advanced Threat Protection licensing must be enabled for your application before it can be applied here.
Virus Scanning checks files uploaded to your application and if a virus is found, that request is denied before it reaches your server.

About Advanced Threat Protection

Files uploaded to your application might contain advanced threats. Barracuda Advanced Threat Protection (BATP) scans files uploaded to your application to detect such threats.

Enabling Barracuda Advanced Threat Protection will apply an available BATP license to this application. You will then need to enable BATP within the Form Protections. You can apply it to all or just specific URLs in your application where files are uploaded.

The Barracuda Advanced Threat Protection is a cloud-based service that provides in-depth defense against ransomware, malware, and advanced cyber attacks. The Barracuda WAF-as-a-Service integrates with the Barracuda Advanced Threat Protection (BATP) to scan all files uploaded using POST method requests with encoding type multipart/form-data. BATP scans the files with multiple malware scanners that utilize different types of detection techniques to check for anomalies in the uploaded files and provides defense against zero day attacks. When a file is uploaded, Barracuda WAF-as-a-Service processes the request and uploads the file to the server, while the BATP performs the scan and logs the details. To view BATP log for a specific application, navigate to Firewall Logs in the left menu.

Note that Barracuda Advanced Threat Protection:

- Can scan files with a maximum size of 10MB.
- Is a separate license that must be purchased from Barracuda Networks.

BATP processes the following MIME types:

- application/pdf
- application/msword
- application/vnd.ms-powerpoint
- application/vnd.ms-excel

- application/x-msaccess
- application/vnd.openxmlformats-officedocument.presentationml.presentation
- application/vnd.openxmlformats-officedocument.spreadsheetml.sheet
- application/vnd.ms-cab-compressed
- application/vnd.microsoft.portable-executable
- application/vnd.openxmlformats-officedocument.wordprocessingml.document
- application/rtf

For additional details, refer to Advanced Threat Protection Configuration in the Barracuda Web Application Firewall documentation.

View Virus Scanning activity

1. At the top of the left navigation panel, select Logs.
2. Select the Firewall Logs tab.
3. Click Filter. Select Attack Type filter. For the condition, select in. For the value, select either Virus Found, Virus Scan, or both. Click Apply.
   You can specify both selections in the same line.
   Virus scanning activity appears in the table.

Enable File Upload Protection

To apply File Upload Protection to all or a portion of your application:

1. From App Profiles, add Form Protection to the desired URL.
2. In the right side panel find File Upload Protection and click on it.
3. If you see the notice "'BATP Scan' requires Advanced Threat Protection to be enabled on the application" you can click the link to enable it.
4. **Enable virus scan** – Set to **Enable**.
5. **Enable BAPT scan** – Set to **Enable**.