Form Protection

https://campus.barracuda.com/doc/96774518/

Form Protection can be found as part of App Profiles if on Datapath 12.0 or higher.

By adding URLs, you can decide which types of protection pertain to all or a portion of your application. The main panel shows the URL and the right panel displays the features that are or can be enabled for it.

Features for *Root* will apply to your entire application with the exception of any other URLs defined here. For example, adding the URL */file-upload.php* creates a new feature group. Features enabled in the right panel will apply to <*yourdomain.com/file-upload.php*>. Adding the URL */admin/** also creates a new feature group. Features enabled in the right panel will apply to all files in the <*yourdomain.com/admin/*> branch of your application.

The following features can be configured for each URL:

Only features that are licensed or made available for your application will appear in the right panel.

- **Brute force protection** – Stops attacks from making multiple automated submissions using forms in your applications. It also stops attackers from systematically trying to access pages over and over again with the intention of trying multiple username/password combinations to brute force entry in to your application. See Brute Force Attack for more information.
- **Data theft protection** – Prevents unauthorized disclosure of confidential information. Rules must be created at the Data Theft Protection component before they can be applied here.
- **File upload protection** – This 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.
  To 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.
- **Login form information** – For credential protection to work you need to specify the format and details for the login form.
- **Credential attack protection** – Protects against Credential Stuffing and/or Credential

Spraying. See Credential Attack Protection for more information about these attack vectors.

- **Privileged account protection** – Watches for signs of account takeover by evaluating session elements such as the connecting entity's geolocation, user agent, header value, and network details. Learn more at Privileged Account Protection.
- **GraphQL security** – Secures your GraphQL APIs with capabilities that include native parsing of requests and enforcement of security checks. See GraphQL Security for more information.
- **JWT validation** – Uses the received JSON Web Token (JWT) to validate the authenticity of the client sending HTTP requests and the token claims. See JSON Web Token (JWT) Validation to learn more.

Privileged account protection, GraphQL security and JWT validation are only available on datapath v12.0 and later.