Enabling Data Theft Protection

https://campus.barracuda.com/doc/4259947/

Data Theft Protection prevents unauthorized disclosure of confidential information. Configuring Data Theft Protection requires two steps:

- Specify any at-risk data elements handled by the web application using Security Policy.
- Enable protection of these elements where needed, using URL Policy.

Sensitive data elements may require masking to prevent their unauthorized disclosure, or requests containing sensitive data may be blocked altogether. Using Security Policy, you can configure any sensitive data elements that may need protection, along with the desired way to handle them. These settings can then be used by any service associated with the security policy. URL policies applied to narrowly defined URL spaces requiring this protection can individually enable it as needed. Other URL spaces operate without unnecessarily incurring the processing hit. To optimize performance, enable Data Theft Protection only for parts of the site known to carry sensitive information.

The **SECURITY POLICIES > Data Theft Protection** page allows configuration of identity theft data types for a security policy. You can enable protection for specific URLs using the **BOT MITIGATION > Bot Mitigation** page, **Bot Mitigation Policy** section. Security Policy Data Theft settings are then enforced only for configured URLs. Barracuda Energize Updates already provides a set of default protected patterns, such as credit card and social security numbers; however, these can also be expanded or customized, using **ADVANCED > Libraries**, to include other web application-specific data patterns needing protection from disclosure. Any configured pattern can be masked, or the response blocked altogether, if a protected pattern occurs in the server response.

When Data Theft Protection is enabled, the Barracuda Web Application Firewall intercepts the response from the server and compares it to the pattern listed in the **ADVANCED > View Internal Patterns** page and **ADVANCED > Libraries** page (if any custom identity theft patterns). If the response matches any of the defined patterns, it is blocked or cloaked based on the action (Block or Cloak) set. If the action is set to **Block**, the response sent by the server is blocked. If set to **Cloak**, a part of the data is cloaked, that is, it is overwritten with "X"s.

> When set to **Block**, the response is blocked according to the configured action for “Identity-theft-pattern-matched-in-response” in **SECURITY POLICIES > Action Policy**.

The default identity theft elements provided by the Barracuda Web Application Firewall are:

- Credit cards
- Directory indexing
- Social security numbers (SSN)

Credit Cards and SSN

To prevent exposure of personal data, such as credit card numbers and your social security number (SSN), select **Block** to block the response from the server, or **Cloak** to overwrite the characters based on values defined in the parameters **Initial Characters to Keep** and **Trailing Characters to Keep**. By default, credit card and SSN are set to **Cloak**.

Directory Indexing

If a web server is configured to display the list of all files within a requested directory, it may expose sensitive information. The Barracuda Web Application Firewall prevents exposure of valuable data by blocking the response from the server. By default, directory indexing is set to **Block**.

Configure Data Theft Protection

1. From the **SECURITY POLICIES > Data Theft Protection** page, select the policy you want to enable Data Theft Protection for.
2. In the **Configure Data Theft Protection** section, specify values for the following fields:
    1. **Data Theft Element Name** – Enter a name for the data theft element.
    2. **Enabled** – Select **Yes** to use this data element to be matched in the server response pages. This data element is used for matching server response pages only when **Enable Data Theft Protection** is also set to **Yes** on the **BOT MITIGATION > Bot Mitigation** page.
    3. **Identity Theft Type** – Select the data type from the drop-down list that the element mentioned in Data Theft Element Name belongs to. The default identity theft patterns (Credit Card, SSN, and Directory Indexing) are associated to data types defined under **ADVANCED > View Internal Patterns > Identity Theft Patterns**. If you want to associate a custom identity theft pattern created on the **ADVANCED > Libraries** page, select **<CUSTOM>** from the drop-down list and then select customized identity theft type from the **Custom Identity Theft Type** field below.
    4. **Custom Identity Theft Type** – Select the customized identity theft type to be used from the drop-down list.
    5. **Action** – If set to **Block**, the response sent by the server containing this data type is blocked. The **Block** mode should be used if the server should never expose this information. In **Cloak** mode, a part of the data is cloaked, that is, it is overwritten with X's based on **Initial Characters to Keep** and **Trailing Characters to Keep**.
    6. **Initial Characters to Keep** – Enter the number of initial characters to be displayed to the user when the data of this data type is identified in a server page. For example, an online shopping service displays a user's credit card number 1234 0000 0000 5678. If **Initial Characters to Keep** is set to *4*, the credit card number is displayed as 1234 XXXX XXXX XXXX.
    7. **Trailing Characters to Keep** – Enter the number of trailing characters to be displayed to the user when the data of this data type is identified in a server page. For example, an

online shopping service displays a user's credit card number as 1234 0000 0000 5678. If **Trailing Characters to Keep** is set to *4*, the credit card number is displayed as XXXX XXXX XXXX 5678.

3. Click **Add** to add the above configuration settings.

Custom Identity Theft Patterns

The default data theft types are displayed under **Protected Data Types** on the **SECURITY POLICIES > Data Theft Protection** page. You can also create custom identity theft data types on the **ADVANCED > Libraries** page to use.

Create a Custom Identity Theft Pattern

1. Go to the **ADVANCED > Libraries** page, **Identity Theft** section, enter a name in the **New Group** field and click **Add**.
2. Click **Add Pattern** next to the created identify theft pattern group. The **Identity Theft Patterns** window opens. Specify values for the following fields:
    1. **Pattern Name** – Enter a name to identify the pattern.
    2. **Status** – Set to **On** if you wish to use this pattern for pattern matching in the responses.
    3. **Pattern Regex** – Define the regular expression of the pattern or click the Edit icon to select and insert the pattern.
    4. **Pattern Algorithm** – Select the algorithm to associate with the pattern from the drop-down list.
    5. **Case Sensitive** – Select **Yes** if you wish the pattern defined to be treated as case sensitive.
    6. **Pattern Description** – (Optional) Enter the description for the pattern defined. Example, `Visa credit card pattern`. This indicates the pattern used here is the Visa credit card pattern.
3. Click **Add**.

Use a Custom Identity Theft Pattern

1. Go to the **SECURITY POLICIES > Data Theft Protection** page.
2. Select a policy from the **Policy Name** drop-down list.
3. In the **Configure Data Theft Protection** section, enter a name in the **Data Theft Element Name** text field.
4. Set **Enabled** to **Yes** to use this data element to be matched in the server response pages. This data element is used for matching server response pages only when **Enable Data Theft Protection** is also set to **Yes** on the **BOT MITIGATION > Bot Mitigation** page.
5. Select **CUSTOM** from the **Identity Theft Type** drop-down list.
6. Select the Identity theft pattern you created from the **Custom Identity Theft Type** drop-down list.
7. Set the **Action** to **Block** or **Cloak**. If set to **Block**, the response sent by the server containing this data type is blocked. **Block** mode should be used if the server is never expected to expose

such information. In **Cloak** mode, a part of the data is cloaked, that is, it is overwritten with X's based on **Initial Characters to Keep** and **Trailing Characters to Keep**.
8. If required, change the values of **Initial Characters to Keep** and **Trailing Characters to Keep** and click **Add**.
9. You should now bind this policy to a service, so that any request coming to that service is matched with the pattern and then processed.

Turning on Data Theft Protection Using URL Policy

To use Data Theft Protection for a requested URL, from the **BOT MITIGATION > Bot Mitigation** page, **Bot Mitigation Policy** section, you must set **Enable Data Theft Protection** to **Yes**. When **Enable Data Theft Protection** is set to **Yes** for a requested URL, the **Data Theft Protection** settings from the service's security policy will be enforced for this request.

© Barracuda Networks Inc., 2024 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.