How to Configure Brute Force Prevention

https://campus.barracuda.com/doc/17629553/

Brute Force Prevention

Brute Force attacks attempt unauthorized access by repeatedly bombarding the system with guessed parameters.

To enable Brute Force prevention:

1. Edit the default URL policy (**default-url-policy**) on the **SECURITY > Advanced Security** page.
2. Set **Enable Bruteforce Prevention** to **Yes**.

Preventing Brute Force Attacks

Brute Force prevention sets the maximum number of requests (all requests or only invalid requests) to a URL space from a single client, or from all sources, within the specified time interval. It blocks offending clients from making further requests. You can specify exception clients for which no maximum is enforced. Bruteforce prevention stops the following types of rate based attacks:

- Brute force attempts to gain access – Repetitive login failures in quick succession may be an attempt to gain unauthorized access using guessed credentials.
- Brute force attempts to steal session tokens – Session tokens, authentication mechanisms for requests by already authenticated users, can be guessed and stolen through repeated requests.
- Distributed Denial of Service attacks (DDoS) – Repeated requests for the same resource can impair critical functionality by exhausting server resources.
- Vulnerability scanning tools – High rates of requests can probe web applications for weaknesses. Typically these tools execute a database of commonly known and unknown (blind) attacks which are executed in quick succession.

To detect brute force attacks against session management (too many sessions given out to a single IP address or range), use session tracking.

On the **SECURITY > Advanced Security** page, locate the desired URL policy and click **Edit** in the **Options** column next to it.

To configure Brute Force prevention, modify the following settings:

- **Enable Bruteforce Prevention** – Set to **Yes** to enable bruteforce attack prevention for this URL policy.
- **Enable Invalid Status Code Only** – Set to **Yes** to monitor and count only invalid requests from a single client or all sources. If set to *No*, both valid and invalid requests from a single client or all sources are counted. Requests exceeding the configured **Max Allowed Accesses Per IP** and **Max Allowed Accesses From All Sources** are blocked.
- **Count Window** – Specifies the time interval in seconds to which the **Max Allowed Accesses Per IP** or **Max Allowed Accesses From All Sources** applies. **Range**: 1 – 6000; Default: 60 (one minute).
- **Max Allowed Accesses Per IP** – Specifies the maximum number of requests allowed to this web application per IP address. **Range**: 1 – 65535; Default: 10.
- **Max Allowed Accesses From All Sources** – Specifies the maximum number of requests allowed to this web application from all sources. **Range**: 1 – 65535; Default: 100.
- **Counting Criterion** – Specifies whether requests from all sources, or requests per IP are counted. Values: **Per IP**, **All Sources**; Default: **Per IP**.
- **Exception Clients**: Specifies IP addresses for which no maximum number of accesses is enforced. You can enter a single, or a range of IP addresses, or a combination of both with a comma (,) as a delimiter. The range of IP addresses must be separated with a hyphen (-). This makes an exception list of client IPs (unlimited access users). This list should not have any overlapping IP ranges. Values: Suitable IP Range;

Click **Save** when you have finished.

© 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.