Enabling Brute Force Protection

https://campus.barracuda.com/doc/4259869/

Brute Force Protection

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

Preventing Brute Force Attacks

Brute Force protection sets a maximum number of requests (all requests or only invalid requests) to a URL space from a single client, or from all sources, within a configured time interval. It blocks offending clients from making further requests. You can specify exception clients for which no maximum is enforced. Brute Force protection prevents 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.

Other Brute Force Attack Prevention options:

1. To detect brute force attacks against session management (too many sessions given out to a single IP address or range), use Session Tracking.
2. To control the rate of requests to specific resources (URL spaces), and to provide different levels of service to different sets of clients, use Rate Control Pool.

On the **BOT MITIGATION > Bot Mitigation** page, in the **Bot Mitigation Policy** section, click **Edit** in the **Options** column next to the desired URL policy. Next, configure the following values:

- **Enable Brute Force Prevention** – Set to *Yes* to enable brute force attack prevention for this URL policy.
- **Counting Criterion** – Specifies whether requests from all sources, or requests per IP address are counted. Values: *Per IP* , *All Sources* ; Default: *Per IP* .
- **Count Window** – Specifies the time interval in seconds to which **Max Allowed Accesses Per**

IP or **Max Allowed Accesses From All Sources** applies. Range: *1 - 6000*; Default: *60* (one minute).

- **Count Auth Response** - When set to *Yes*, the auth responses are considered for counting.
- **Auth Response Identifier** - Choose the auth response identifier type.
  - **Auth Failure Response Codes** - The authentication status codes 401 and 407 will be considered as invalid status codes, and not as exception. For example, when **Max Failed Accesses Per IP** is set to 10, and **Count Auth Responses** is set to **Yes**, the Barracuda Web Application Firewall allows 10 failed requests (4xx and 5xx codes including 401 and 407) for the time specified in **Count Window**, after which the brute force action policy will be applied.
  - **Response Page Text** - The text patterns that will be matched against the response page.
    - **Text to match** - Provide the text patterns that need to be matched against the response page and then click **Add**.

      You can add a maximum of 5 text patterns to match. If required, you can delete the existing patterns in order to add new ones.

- **Enable Invalid status code only** – Set to *Yes* to monitor and count only invalid requests from a single client or from all sources. If set to *No*, both valid and invalid requests from a single client or from all sources are counted. Requests exceeding the configured **Max Allowed Accesses Per IP** and **Max Allowed Accesses From All Sources** are blocked.

  When **Enable Invalid Status Code Only** is set to *Yes*, the Barracuda Web Application Firewall counts the requests with invalid status codes in the response. Status codes greater than 400 are considered invalid status codes, with the exception of 401 and 407.

Client IP Address

- **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
- **Max Bandwidth Per IP** - Specifies the maximum number of bytes to be exchanged between the client and the Barracuda Web Application Firewall for the time specified in **Count Window**, after which the requests will be blocked. This field is available only when **Counting Criterion** is set to *Per IP*. If the value is set to zero (0), it exempts the brute force policy validation.
  - **Range**: 0 - 1048576 (in KB)
  - **Default**: 0
- **Max Bandwidth From All Sources** - Specifies the maximum number of bytes to be exchanged between all clients and the Barracuda Web Application Firewall for the time specified in **Count Window**, after which the requests will be blocked. This field is available only when **Counting Criterion** is set to *All Sources*. If the value is set to zero (0), it exempts the brute force policy validation.

- **Range**: 0-10485760 (in KB)
- **Default**:0

- **Max Failed Accesses Per IP** - Specifies the maximum number of failed requests (4xx and 5xx status codes) to be allowed per IP address for the time specified in **Count Window**, after which the requests will be blocked. This field is available only when **Counting Criterion** is set to *Per IP*. If the value is set to zero (0), it exempts the brute force policy validation.
  - **Range**: 0 - 65535
  - **Default**: 10
- **Max Failed Accesses From All Sources** - Specifies the maximum number of failed requests (4xx and 5xx status codes) to be allowed from all sources for the time specified in **Count Window**, after which the requests will be blocked. This field is available only when **Counting Criterion** is set to *All Sources*. If the value is set to zero (0), it exempts the brute force policy validation.
  - **Range**: 0 - 65535
  - **Default**: 100
- **Exception Clients** – Specifies IP addresses for which no maximum number of accesses is enforced. You can enter a single IP address, a range of IP addresses, or a combination of both using a comma (,) as a delimiter. The range of IP addresses must be separated with a hyphen (-). This makes an exception list of client IP addresses (unlimited access users). This list should not have overlapping IP ranges.
  - **Values**: Suitable IP Range

Client Fingerprint

- **Max Allowed Accesses Per Client Fingerprint** - Specifies the maximum number of requests to be allowed per client fingerprint to access the web application for the time specified in **Count Window**, after which the requests will be blocked. This field is available only when **Counting Criterion** is set to *By Client*. If the value is set to zero (0), it exempts the brute force policy validation.
  - **Range**: 0 - 65535;
  - **Default**: 0
- **Max Bandwidth Per Client Fingerprint** - Specifies the maximum number of bytes to be exchanged between the client and the Barracuda Web Application Firewall for the time specified in **Count Window**, after which the requests will be blocked. This field is available only when **Counting Criterion** is set to *By Client*. If the value is set to zero (0), it exempts the brute force policy validation.
  - **Range**: 0-1048576 (in KB)
  - **Default**:0
- **Max Failed Accesses Per Client Fingerprint** - Specifies the maximum number of failed requests (4xx and 5xx status codes) to be allowed per client fingerprint for the time specified in **Count Window**, after which the requests will be blocked. This field is available only when **Counting Criterion** is set to *By Client* . If the value is set to zero (0), it exempts the brute force policy validation.
  - **Range**: 0 - 65535;
  - **Default**: 0

- **Exception Fingerprint** - Specifies client fingerprints for which no brute force validation is enforced . You can enter either a single or multiple client fingerprints separated by a comma without any space. This makes an exception list of client fingerprints (unlimited access users).

Click **Save** to save the above settings.

Client Fingerprinting Capability

The Barracuda Web Application Firewall uses the Client Fingerprinting capability to increase security. This feature collects information about the browser attributes from all the devices that the client uses during login. Cient Fingerprinting uses the collected information to identify suspicious clients (potential bots) and recognize web scraping attacks more quickly.

To enable Client Fingerprinting,

1. Navigate to **Basic > Services > Advanced Configuration** and set **Enable Client Fingerprinting** to *Yes*.
2. Navigate to the **Advanced** section of the **Advanced > System Configuration** page and set **Enable Client Fingerprinting** to *Yes*.