GUIDE TO CONFIGURING MOD_EVASIVE FOR APACHE 2.4

This guide details how to configure `mod_evasive`, a popular Apache module designed to help mitigate denial-of-service (DoS) and brute-force attacks. It works by tracking the number of requests from individual IP addresses and blocking those that exceed defined thresholds within specified time intervals.

INSTALLATION AND ENABLING

Before configuring, ensure `mod_evasive` is installed and enabled on your Apache 2.4 server. The installation method can vary depending on your operating system and how Apache was installed.

- **Debian/Ubuntu:** Use the package manager:
  ```
  sudo apt-get update
  sudo apt-get install libapache2-mod-evasive
  ```
  Then, enable the module:
  ```
  sudo a2enmod evasive
  ```
- **RHEL/CentOS/Fedora:** If not available via yum/dnf, you might need to compile it from source or find a third-party repository.
- **After installation/enabling, restart Apache:**
  `sudo systemctl restart apache2` (or `httpd`)

CONFIGURATION DIRECTIVES

`mod_evasive` directives are typically added to your main Apache configuration file (e.g., `apache2.conf` or `httpd.conf`) or in a dedicated configuration file within a directory like `conf.d/` or `mods-enabled/`.

Here are the key directives and their functions:

`DOSHashTableSize`

Default: 30000
Sets the size of the hash table used to store IP address and request counts. A larger size can handle more concurrent IP addresses but consumes more memory. You

generally don't need to change this unless dealing with an extremely high number of unique IP addresses accessing your server concurrently.

`DOSPageCount`

Default: 2
Specifies the maximum number of requests allowed from a single IP address to a *specific page* (e.g., `/index.html`) within the interval defined by `DOSPageInterval`. If this limit is exceeded, the IP may be temporarily blocked.

`DOSSiteCount`

Default: 100
Sets the maximum number of total requests allowed from a single IP address to *any page on the entire website* within the interval defined by `DOSSiteInterval`. This is a broader limit than `DOSPageCount`.

`DOSPageInterval`

Default: 1 (second)
Defines the time window (in seconds) during which the `DOSPageCount` is measured. For example, if `DOSPageCount` is 2 and `DOSPageInterval` is 1, an IP making 3 requests to the same page within 1 second will trigger a block.

`DOSSiteInterval`

Default: 1 (second)
Defines the time window (in seconds) during which the `DOSSiteCount` is measured. If `DOSSiteCount` is 100 and `DOSSiteInterval` is 1, an IP making 101 requests to any page within 1 second will be blocked.

`DOSBlockingPeriod`

Default: 10 (seconds)
Determines how long an IP address will be blocked (in seconds) after it has exceeded the configured request limits.

`DOSEmailNotify`

Default: `root@localhost`
Specifies an email address where notifications will be sent when an IP address is blocked. Set to an empty string (`''`) to disable email notifications. Ensure your server is configured to send emails.

`DOSSystemCommand`

Default: (empty)
Allows you to specify a command to execute when an IP address is blocked. This is powerful for integrating with firewall tools (e.g., `iptables`, `firewalld`) to permanently ban offending IPs. For example: `DOSSystemCommand "/sbin/iptables -I INPUT -s %s -j DROP"` (the `%s` will be replaced by the offending IP).

`DOSLogDir`

Default: `/var/log/apache2` (or `/var/log/httpd`)
This directory is used by `mod_evasive` to store temporary files, such as lock files for blocked IPs. Ensure that the Apache user (e.g., `www-data`, `apache`) has write permissions to this directory.

TUNING RECOMMENDATIONS AND STARTING POINTS

Tuning `mod_evasive` is crucial to balance security with legitimate user access. Overly aggressive settings can block normal users, while weak settings offer little protection.

General Approach

- **Start Conservatively:** Begin with the default settings or slightly adjusted values.
- **Monitor Logs:** Regularly check your Apache error logs (e.g., `/var/log/apache2/error.log`) for `mod_evasive` messages. Look for frequent blocking of IPs that appear to be legitimate.
- **Understand Your Traffic:** Know what normal traffic patterns look like for your site. How many requests per second do typical users make? How many pages does a user usually visit in a short period?
- **Gradual Adjustments:** If you see legitimate users being blocked, gradually increase the counts (`DOSPageCount`, `DOSSiteCount`) or the intervals (`DOSPageInterval`, `DOSSiteInterval`). If you are under a sustained attack, you might decrease these values.
- **Blocking Period:** A longer `DOSBlockingPeriod` (e.g., 60-300 seconds) is often more effective than a very short one.
- **Email Notifications:** Enable `DOSEmailNotify` to be alerted to potential issues.

- **System Commands:** If you have a dedicated security setup, consider using `DOSSystemCommand` to automatically block IPs at the firewall level for longer durations.

Example Starting Points for Tuning

These are general suggestions and should be adapted based on your server's performance and typical user behavior.

- **Low-Traffic Site / Personal Blog:**
  ```
  DOSPageCount 5
  DOSSiteCount 150
  DOSPageInterval 1
  DOSSiteInterval 1
  DOSBlockingPeriod 60
  ```
- **Medium-Traffic Website / Small Business:**
  ```
  DOSPageCount 10
  DOSSiteCount 200
  DOSPageInterval 1
  DOSSiteInterval 1
  DOSBlockingPeriod 120
  ```
- **High-Traffic Website / API Endpoint:**
  (Requires careful monitoring and potentially higher values or specialized solutions)
  ```
  DOSPageCount 20
  DOSSiteCount 300
  DOSPageInterval 1
  DOSSiteInterval 1
  DOSBlockingPeriod 300
  ```
  Note: For very high-traffic sites or APIs where legitimate traffic can be bursty, you might need to increase intervals or counts significantly, or consider other layers of protection.

Important Considerations:

- **Shared Hosting:** If you are on shared hosting, be cautious as aggressive settings can affect other users on the same IP address. Consult your hosting provider.
- **Load Balancers / Proxies:** If Apache is behind a load balancer or reverse proxy, ensure that Apache is configured to correctly identify the client's real IP address (e.g., using `mod_remoteip`). Otherwise, `mod_evasive` might block the proxy's IP.

- **Bots and Crawlers:** Legitimate search engine crawlers might trigger these rules. You might need to whitelist their IPs or adjust thresholds to accommodate them.

By carefully configuring and monitoring `mod_evasive`, you can significantly enhance the resilience of your Apache web server against various types of denial-of-service attacks.

David Keith Jr "mrdj" ✓