mod_evasive – защита от DOS и DDOS атак

Опубликовано muff в Пт, 2011-02-04 06:13

Один из методов защититы web-сервера от флуд атак и слабого ddos-а - это установка модуля **mod_evasive**.

Установку выполним из портов:

```
# cd /usr/ports/www/mod_evasive/ && make install clean && rehash
```

После установки модуль автоматически добавляет себя в списки подгружаемых модулей. Остается только расскоментировать его в httpd.conf:

```
LoadModule evasive20_module   libexec/apache22/mod_evasive20.so
```

Также необходимо добавить в httpd.conf такой блок:

```
<IfModule mod_evasive20.c>
	DOSHashTableSize 3097
	DOSPageCount 4
	DOSSiteCount 15
	DOSPageInterval 3
	DOSSiteInterval 3
	DOSBlockingPeriod 600
	DOSEmailNotify ddos [at] example [dot] com
</IfModule>
```

Доступные для использования опции:

- **DOSHashTableSize**: это размер хэш-таблицы которая обрабатывает запросы к WWW-серверу.
- **DOSPageCount**: число запросов к одной странице от одного и того же IP в течение указаного интервала времени.
- **DOSSiteCount**: число запросов ко всем страницам домена, т.е если поступило более 90-ти запросов с одного ай-пи на разные страницы домена – тогда такой ай-пи будет заблокирован.
- **DOSPageInterval**: Интервал для директивы DOSPageCount (в секундах)
- **DOSSiteInterval**: Интервал для директивы DOSSiteCount (в секундах)
- **DOSBlockingPeriod**: На сколько заблокировать ай-пи (в секундах)
- **DOSEmailNotify**: может быть использован для уведомления, будет отправлять сообщение по электронной почте о том что такой-то IP был заблокирован.
- **DOSSystemCommand**: эта директива используется для выполнения какой-нибудь вашей команды когда IP блокируется. Вы можете использовать это для добавления IP-адреса в таблицу фаервола. (пример: "**/sbin/ipfw table 111 add %s**".
  В переменную "%s" передается от модуля IP-адресс атакуемого хоста)
- **DOSWhiteList**: список белых IP адресов, можно и по маскам (напр. 127.0.0.*)

После внесения изменений перезапускаем Apache:

```
# apachectl graceful
```

В результате в логах сервера можно наблюдать следующие записи:

```
# cat /var/log/messages | grep evasive
 Feb 4 05:15:28 web0 mod_evasive[49786]: Blacklisting address 193.106.56.242: possible DoS attack.
Feb 4 05:24:11 web0 mod_evasive[51080]: Blacklisting address 95.135.45.76: possible DoS attack.
```

Источник (получено *2025-03-13 23:00*):
http://muff.kiev.ua/content/modevasive-zashchita-ot-dos-i-ddos-atak