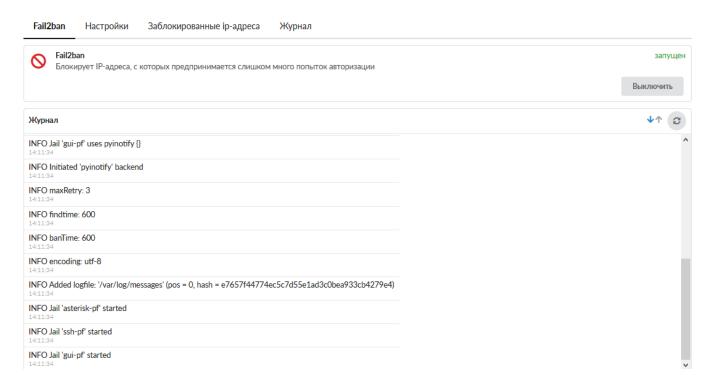
2025/12/05 16:14 1/4 Fail2ban

Fail2ban

Fail2ban - сканирует лог-файлы и блокирует IP-адреса, которые ведут себя подозрительно, к примеру, делая слишком много попыток входа с неверным паролем в попытках найти уязвимость. Данная атака часто называется брутфорсом.

Модуль «Fail2ban» расположен в Меню «Защита», и имеет четыре вкладки: «Fail2ban», «Настройки», «Заблокированные ір-адреса», и «Журнал».

Общие сведения



На данной вкладке отображается состояние модуля (включен/выключен/не настроен), кнопка «Выключить» (или «Включить» если модуль выключен) и последние сообщения в журнале модуля.

Настройки

Увеличивать время бана Количество обычных банов перед увеличением времени бана * Интервал обычных банов * Априламительный фана * Интервал обычных банов * Оприламительный фана * Интервал обычных банов * Оприламительный фана * Оприламительн	Fail2ban	Настройки	Заблоки	рованные ір-адреса	Жу	рнал	1			
Количество неудачных попыток авторизаций вторизаций вт				цитить веб-почту ▼				Защитить VPN-сервер		
авторизаций * 3	✓ SSH		FTP		✓ GU	II				
3 Увеличивать время бана Количество обычных банов перед увеличением времени бана * 10 мин. 10 мин. 10 мин. Мин. Мин. Мин. Мин. Мин. Мин. Мин. М		дачных попыток		Интервал неудачных *	попыток	авто	ризаций	Блокировать на *		
Увеличивать время бана Количество обычных банов перед увеличением времени бана * Интервал обычных банов * 10	3			10			мин.	10		мин.
3 10 10 мин 10		го времи бапа						Добавить к обычному времени блокировки *		
	Количество обы	ічных банов пере,	Д	Инторрад общинку ба	*			Добавить к обычному врем	иени бло	кировки
	Количество обы увеличением вр	ічных банов пере,	^		анов [*]		мин.	•		жировки мин.

Данная вкладка предназначена для настройки работы модуля «Fail2ban».

Флаги: «Защитить почтовый сервер», «Защитить веб-почту», «Защитить сервер телефонии», «Защитить VPN-сервер», «SSH», «FTP», «GUI« - позволяют fail2ban анализировать логи авторизации в соответствующих модулях.

Поле «**Количество неудачных попыток авторизаций**» - позволяет задать количество неудачных попыток авторизации в модуле, отмеченном флагамом, после чего ір-адресу будет заблокирован доступ к «ИКС»

Поле «**Интервал неудачных попыток авторизаций**» - время, в течении которого подсчитывается количество неудачных попыток авторизации

Поле «**Блокировать на**» - При срабатывании блокировки, доступ с ір-адреса будет прекращен на заданной количество минут

Флаг «Увеличивать время бана» - позволяет включить дополнительные настройки fail2ban («Количество обычных банов перед увеличением времени бана», «Интервал обычных банов», «Добавить к обычному времени блокировки») для способствования увеличения времени бана.

Так при срабатывании бана n-раз (указанных в поле «Количество обычных банов перед увеличением времени бана») в течении времени t (указанного в «Интервал обычных банов») доступ к «ИКС» ір-адресу будет заблокирован на n+1 бане на время = t+ «Блокировать на». Стоит отметить, что значение указанное в поле «Интервал обычных банов» должно быть больше, чем произведение значений полей «Блокировать на» и «Количество обычных банов перед увеличением времени бана».

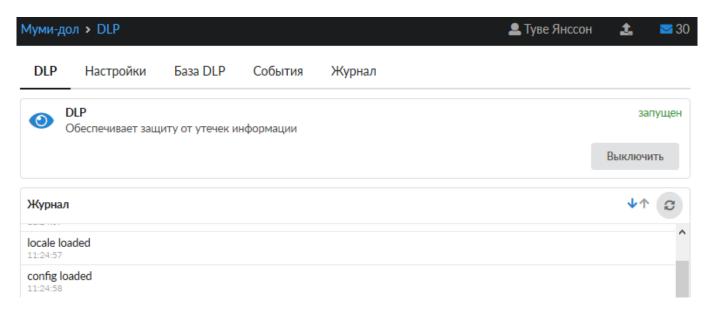
Кнопка «Белый список». При нажатии будет открыто новое диалоговое окно, в котором возможно задать соответствие ip-адреса и сервиса/всех сервисов, для которых fail2ban не

https://doc-old.a-real.ru/ Printed on 2025/12/05 16:14

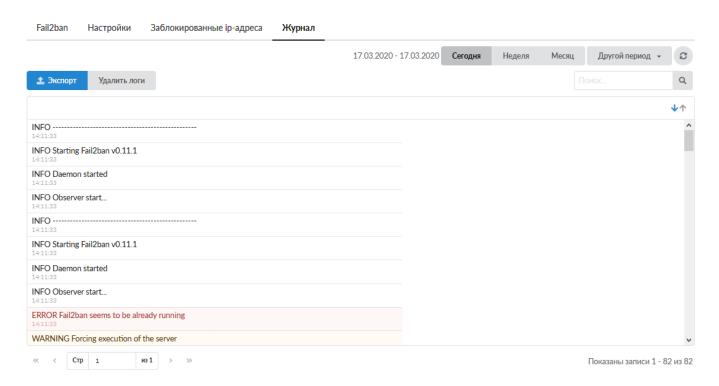
2025/12/05 16:14 3/4 Fail2ban

будет срабатывать.

Заблокированные ір-адреса



Журнал



Отображает сводку всех системных сообщений модуля «Fail2ban» с указанием даты и времени. Журнал разделен на страницы, кнопками «вперед» и «назад» возможно переходить со страницы на страницу, либо ввести номер требуемой страницы. Записи в журнале выделяются цветом в зависимости от вида сообщения. Обычные сообщения системы отмечены белым цветом, сообщения о состоянии системы (включение/выключение) - зеленым, предупреждения – желтым, ошибки - красным. В правом верхнем углу модуля находится строка поиска, а также

Last update: 2020/03/17 16:14

возможность выбора периода отображения журнала событий. По умолчанию журнал отображает события за текущую дату. При необходимости можно сохранить данные журнала в файл, нажав кнопку «Экспорт» или удалить данные журнала, за определенный период, нажав кнопку «Удалить логи».

From:

https://doc-old.a-real.ru/ - Документация

Permanent link:

https://doc-old.a-real.ru/doku.php?id=ics70:fail2ban&rev=1584450890





https://doc-old.a-real.ru/ Printed on 2025/12/05 16:14