

База вредоносных сигнатур

DosGate ведет собственную обновляющуюся базу вредоносных сигнатур которая поддерживается внутренней командой аналитики ServicePipe и обновляется каждый час. База вредоносных сигнатур применяется на решении в автоматическом или полу-автоматическом режиме

Содержимое Базы Данных

- Настроенные профили и контрмеры (пресеты)
- Вредоносные TLS-отпечатки
- IPv4/IPv6-адреса участвующие в ДДоС-атаках
- IPv4/IPv6-адреса участвующие в вредоносной автоматизации (парсинг, взлом)

Доставка обновлений

- API
- Через веб-интерфейс DosGate
- JSON-файлы
- Через приватный репозиторий

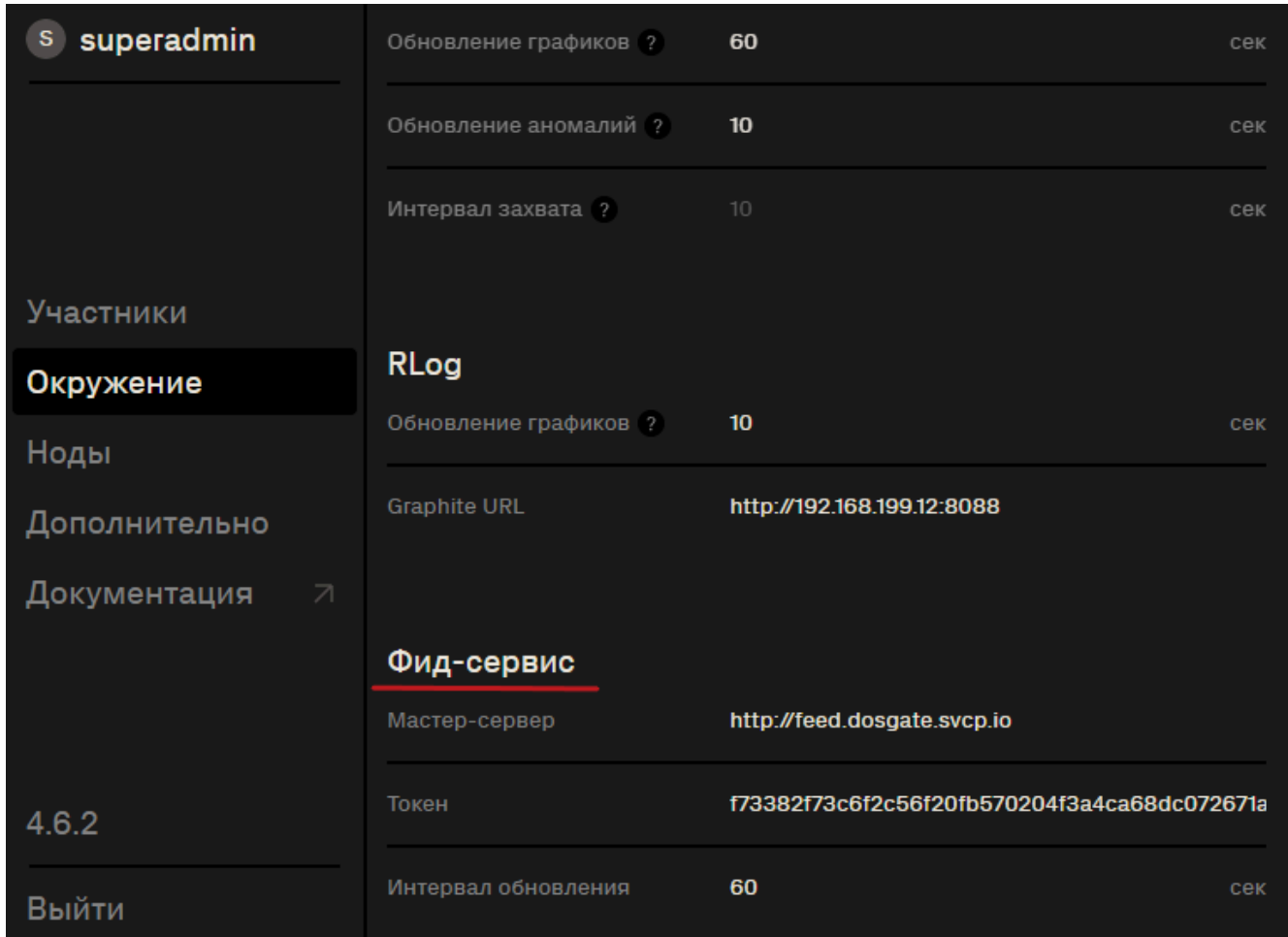
Подключение базы вредоносных сигнатур

- База вредоносных сигнатур распространяет компоненты-пресеты (готовые легитимные и вредоносные сигнатуры) для защиты сетевых сегментов и сервисов, а также вредоносные IP-списки. Она подключается и настраивается к веб-интерфейсу Spider через настройки окружения
- Содержимое базы вредоносных сигнатур уникально для каждого заказчика
- База вредоносных сигнатур поддерживается в Spider с версии 3.9.7

Шаг 1

Получите от вендора ссылку на мастер-сервер базы вредоносных сигнатур и ключ

Шаг 2

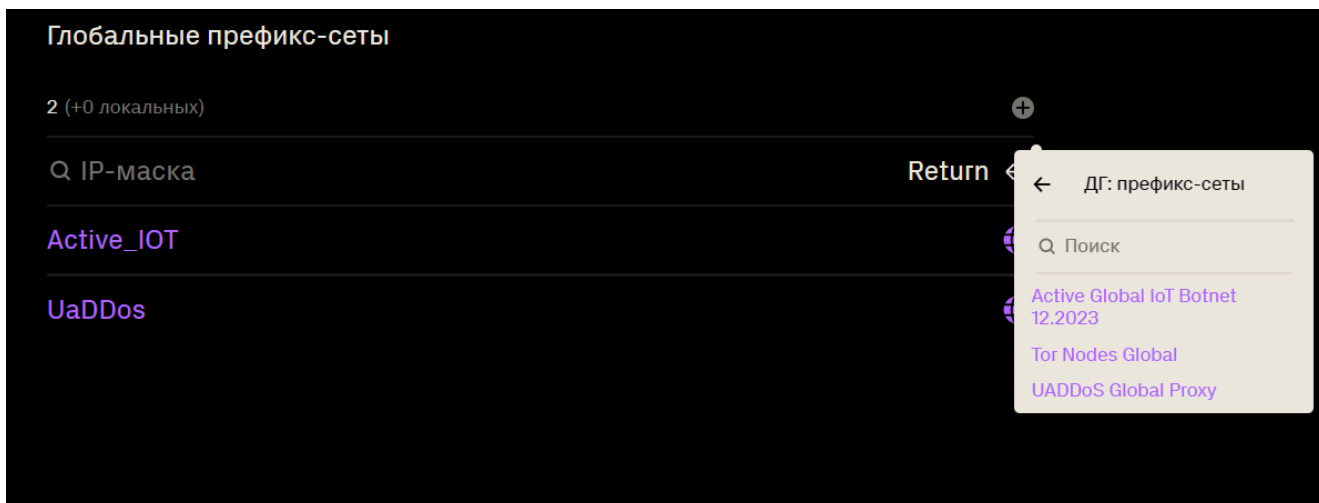


The screenshot shows the Spider admin interface. On the left is a sidebar with the user 'superadmin' and navigation links: 'Участники', 'Окружение' (highlighted), 'Ноды', 'Дополнительно', 'Документация', '4.6.2', and 'Выйти'. The main content area is divided into two sections: 'RLog' and 'Фид-сервис'.

Настройка	Значение	Единица
Обновление графиков	60	сек
Обновление аномалий	10	сек
Интервал захвата	10	сек
RLog		
Обновление графиков	10	сек
Graphite URL	http://192.168.199.12:8088	
Фид-сервис		
Мастер-сервер	http://feed.dosgate.svcp.io	
Токен	f73382f73c6f2c56f20fb570204f3a4ca68dc072671a	
Интервал обновления	60	сек

Укажите ссылку и ключ в настройках окружения Spider. Также, укажите интервал обновления в секундах

Шаг 3



Компоненты-пресеты сразу появятся в вкладке пресетов. IP-списки нужно будет создать в глобальных префикс-сетях. После создания IP-списки будут обновляться сразу в уже созданном префикс-сети и создавать их повторно не потребуется

Все синхронизируемые с базой вредоносных сигнатур сущности помечаются фиолетовым цветом. Их нельзя изменить, но можно дублировать для дальнейшего изменения