УТВЕРЖДАЮ
Генеральный директор
ООО «Кейсистемс»
_____ А. А. Матросов
«___» _____ 2023 г.

ПРОГРАММНЫЙ КОМПЛЕКС «БЮДЖЕТ-СМАРТ»

ВЕРСИЯ 23.01

Руководство администратора

Фильтрация IP адресов

ЛИСТ УТВЕРЖДЕНИЯ

Р.КС.02120-01 32 06-ЛУ

Подп. и дата	
Инв. N дубл.	
Взам. инв. N	
Подп. и дата	
Инв. N подл.	

СОГЛАСОВАНО
Заместитель генерального директора
ООО «Кейсистемс»
_____ Е. В. Фёдоров
«___» _____ 2023 г.
Руководитель ДПиРСИБ

_____ Д. В. Галкин
«___» _____ 2023 г.

2023

Литера А

УТВЕРЖДЕНО
Р.КС.02120-01 32 06-ЛУ

информационные технологии
КЕЙСИСТЕМС

ПРОГРАММНЫЙ КОМПЛЕКС «БЮДЖЕТ-СМАРТ»

ВЕРСИЯ 23.01

Руководство пользователя

Фильтрация IP адресов

Р.КС.02120-01 32 06

Листов 11

Инв. N подл	Подп. и дата	Взам. инв. N	Инв. N дубл	Подп. и дата

2023

Литера А

АННОТАЦИЯ

Настоящий документ является частью руководства администратора блока задач «Импортозамещение», объектом которого является, в том числе, программный комплекс «Бюджет-СМАРТ» (далее – «программный комплекс») версии 23.01 по автоматизации процесса проектирования, исполнения и анализа бюджетов субъектов Российской Федерации, закрытых автономно-территориальных образований и муниципальных образований.

Документ содержит описание процедуры фильтрации IP адресов для обеспечения безопасности подключения к БД.

Руководство актуально для указанной версии и для последующих версий вплоть до выпуска обновления руководства.

Порядок выпуска обновлений руководства

Выход новой версии программного комплекса сопровождается обновлением руководства пользователя только в случае наличия в версии значительных изменений режимов, описанных в руководстве, добавления новых режимов или изменения общей схемы работы. Если таких изменений версия не содержит, то остается актуальным руководство пользователя от предыдущей версии с учетом изменений, содержащихся в новой версии.

Перечень изменений версии программного комплекса содержится в сопроводительных документах к версии. Информация об изменениях руководства пользователя публикуется на сайте разработчика в разделе «Документация».

Информация о разработчике ПК «Бюджет-СМАРТ»

ООО «Кейсистемс»

Адрес: 428000, Чебоксары, Главпочтамт, а/я 172

Телефон: (8352) 323-323

Факс: (8352) 571-033

http://www.keysystems.ru

E-mail: info@keysystems.ru

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Настоящее руководство пользователя содержит описание процедуры фильтрации IP адресов, целью которой является обеспечение безопасности подключения к БД программных комплексов в финансовых органах, органах государственной и муниципальной власти, государственных и муниципальных учреждениях.

Функциональные возможности

Фильтрация IP-пакетов и преобразование сетевых адресов выполняют роль брандмауэра, защищая внутренние системы, подключенные к защищенной сети, от несанкционированного доступа. Фильтрация IP-пакетов позволяет контролировать входящие и исходящие IP-потоки сети. Служба фильтрации пропускает или отбрасывает пакеты на основе заданных правил. Применение фильтрации позволяет скрыть незарегистрированные частные IP-адреса за набором зарегистрированных IP-адресов. Это дает возможность защитить внутреннюю сеть от внешней. Кроме того, фильтрация решает проблему нехватки IP-адресов, поскольку большое число адресов может быть представлено в виде ограниченного множества зарегистрированных адресов.

Уровень подготовки пользователя

Для успешного освоения материала, изложенного в данном руководстве к пользователю предъявляются следующие требования:

- наличие опыта работы Знание TCP/IP;
- умение работать с веб-серверами (Apache, Ngninx, IIS);
- знание операционных систем Unix/Linux, Windows;
- навык и опыт работы управления, администрирования баз данных MySQL и PostgreeSQL, и знание их синтаксиса;
- умение свободно осуществлять базовые операции в стандартных приложениях операционных систем.

Перечень эксплуатационной документации

В *таблице 1* представлен список пользовательской документации в части описания блока задач «Импортозамещение».

Таблица 1. Перечень эксплуатационной документации

№ п/п	Код документа	Наименование документа
1	2	3
1	Р.КС.00000-XX 32 01-01	Установка и настройка PostgreSQL
	Р.КС.00000-XX 32 01-02	Установка и настройка СУБД на базе PostgreSQL
2	Р.КС.00000-XX 32 02	Установка и настройка СУБД-КС Docker
3	Р.КС.00000-XX 32 03	Установка WEB-Сервер-КС(Docker&Podman)
4	Р.КС.00000-XX 32 04	Резервное копирование баз СУБД-КС
5	Р.КС.03210-XX 32 04	Миграция БД MSSQL на Postgree
6*	Р.КС.02120-01 32 06	Фильтрация IP адресов
* настоящее руководство		

Условные обозначения

В документе используются следующие условные обозначения:

 Уведомление _ Важные сведения о влиянии текущих действий пользователя на выполнение других функций, задач программного комплекса.

 Предупреждение _ Важные сведения о возможных негативных последствиях действий пользователя.

 Предостережение _ Критически важные сведения, пренебрежение которыми может привести к ошибкам.

 Замечание _ Полезные дополнительные сведения, советы, общеизвестные факты и выводы.

[Выполнить] _ Функциональные экранные кнопки.

<F1> _ Клавиши клавиатуры.

«Чек» _ Наименования объектов обработки (режимов).

Статус _ Названия элементов пользовательского интерфейса.

ОКНА => НАВИГАТОР _ Навигация по пунктам меню и режимам.

п. 2.1.1
рисунок 5 _ Ссылки на структурные элементы, рисунки, таблицы текущего документа.
[1] _ Ссылки на документы из перечня ссылочных документов.

1. ПАКЕТ ФИЛЬТРАЦИИ IP-АДРЕСОВ

1.1. Поиск ближайшего неприватного адреса клиента

IP-адрес клиента выбирается из IP-адреса, взятого из HTTP-запроса и из заголовка X-Forwarded-For. Объединяя эти IP-адреса, выполняется поиск ближайшего неприватного адреса. Если такой адрес не найден, за клиентский IP берется первый адрес из заголовка X-Forwarded-For.

1.2. Фильтрация IP-адресов на сервере приложений

Под фильтрации IP-адресов понимается разрешение или запрет подключения к БД ПК через сервер приложений.

Пакет фильтрации IP-адресов включает в себя:

– глобальную фильтрацию (SafeListMiddleware - промежуточное ПО, регистрируемое в Startup.cs, разрешенные адреса берутся из секции в конфигурации сервера приложений);

– пользовательская фильтрация (по пользовательской настройке из БД - «Меню Настройки: НАСТРОЙКИ \ Доступ \ Параметры подключения - Список надежных IP-адресов клиента»)

– для авторизованных пользователей через OpenID используется фильтр действия SafeListIpFilter накладываемый на методы ServiceController, направленные на выполнение;

– для пользователей не авторизующихся через OpenID, при каждом выполнении фильтруется IP-адрес через методы SafeListService.

В конфигурации сервера приложений есть секция SafeListSettings:

```
"SafeListSettings":
  {
    "SafeListEnabled": true, //<!-- label="Включение/отключение фильтра IP-адресов"
x/>-->
    "SafeList": "" //<!-- label="<Список разрешенных IP-адресов>" x/>-->
  },
```

В SafeListEnabled устанавливается значение:

– true, если необходима фильтрация IP-адресов,

– false – если фильтрация не требуется.

Разрешение распространяется как на глобальную фильтрацию, так и на определяемую настройкой.

SafeList (как и настройка из БД) содержит список адресов IPv4 или IPv6, разделенных запятой или точкой с запятой, с которых разрешено подключение. Если необходимо запретить подключение с какого-либо адреса, поставьте перед нужным адресом спецсимвол ~.

Если список пуст, то подключение разрешено со всех адресов. Если в списке единственный символ ~, то подключение запрещено со всех адресов.

1.3. Список разрешенных адресов

SafeList (как и настройка из БД) содержит список адресов IPv4 или IPv6, разделенных запятой или точкой с запятой, с которых разрешено подключение. Если необходимо запретить адрес, то необходимо перед нужным адресом поставить спецсимвол ~.

Если список пуст, то подключение разрешено со всех адресов. Если в списке единственный символ ~, то подключение запрещено со всех адресов.

Возможно использование сетевого префикса / для указания адреса разрешенной подсети.

Примеры разрешенных и запрещенных подключений приведены в таблице (*Таблица 2*).

Таблица 2. Примеры разрешений и запретов для подключений

№	Настройка	Значение
1	2	3
1	10.38.46.0/8	разрешено подключение с IP-адресов из подсети 10.38.46.0/8
2	10.38.46.0/8, ~10.38.46.5	разрешено подключение с IP-адресов из подсети 10.38.46.0/8, кроме IP-адреса 10.38.46.5
3	~10.38.46.0/8	разрешено подключения со всех IP-адресов, кроме IP-адресов, принадлежащих к подсети 10.38.46.0/8
4	~10.38.46.0/8, 192.168.0.20	разрешено подключение с адреса 192.168.0.20, для всех остальных адресов подключение запрещено
5	10.38.46.0/8, 192.168.0.20	разрешено подключение с адреса 192.168.0.20 и адресов, принадлежащих подсети 10.38.46.0/8
6	~10.38.46.0/8, 10.38.46.5	разрешено подключение с адреса 10.38.46.5 и других адресов, не принадлежащих подсети 10.38.46.0/8
7	~10.38.46.5, 10.38.46.5	разрешено подключение со всех адресов
8	10.38.46.5, ~10.38.46.5	запрещено подключение с адреса 10.38.46.5, для всех остальных адресов подключение разрешено

ГЛОССАРИЙ

Приватный IP-адрес - IP-адрес, который существует только в рамках локальной сети. Для компьютеров с приватным адресом невозможен обмен информацией или выход в Интернет без участия посредника – сервера или роутера.

Неприватный (публичный) IP-адрес - IP-адрес, который используется в сети Интернет (его также называют «белым»).

Импортозамещение – переход к использованию отечественного ПО. Постановление правительства и последовавший за ним НПА [2] предписывает запрет на допуск в целях осуществления закупок для муниципальных и государственных нужд программного обеспечения, не включённого в Единый реестр российских программ для электронных вычислительных машин и баз данных. Кроме того, в соответствии с [1] с 1 января 2025 года органам государственной власти, заказчикам запрещается использовать иностранное программное обеспечение на принадлежащих им значимых объектах критической информационной инфраструктуры

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

Сокращение	Термин
1	2
БД	База данных
ПК	Программный комплекс

ПЕРЕЧЕНЬ ССЫЛОЧНЫХ ДОКУМЕНТОВ

1. Указ Президента Российской Федерации от 30.03.2022 № 166 «О мерах по обеспечению технологической независимости и безопасности критической информационной инфраструктуры Российской Федерации».
2. Приказ Министерства связи «Об утверждении плана по импортозамещению программного обеспечения» от 01.02.2015 № 96.

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ

Номер версии	Примечание	Дата	ФИО исполнителя
01	Начальная версия	06.07.2023	Микашкин А.Г., Котова И.В.