КОД БЕЗОПАСНОСТИ

Аппаратно-программный комплекс шифрования

Континент
Версия 3.M2

Руководство администратора

Тестирование каналов связи

RU.88338853.501430.006

Почтовый адрес:	**115127, Россия, Москва, а/я 66** **ООО "Код Безопасности"**
Телефон:	**8 495 982-30-20**
E-mail:	**info@securitycode.ru**
Web:	**https://www.securitycode.ru**

Оглавление

Введение

Данный документ предназначен для администраторов изделия "Аппаратно-программный комплекс шифрования «Континент». Версия 3.М2" (далее — комплекс). В документе приводится общий порядок применения сервисной программы PortChecker (далее — программа).

Приступая к изучению данного руководства, необходимо предварительно ознакомиться с документами [**1**] и [**2**].

Сайт в Интернете. Информация о продуктах компании "Код Безопасности" представлена на сайте https://www.securitycode.ru/products/.

Служба технической поддержки. Связаться со службой технической поддержки можно по телефону 8- 800-505- 30-20 или по электронной почте support@securitycode.ru. Страница службы технической поддержки на сайте компании "Код Безопасности": https://www.securitycode.ru/services/techsupport/.

Учебные курсы. Освоить аппаратные и программные продукты компании "Код Безопасности" можно в авторизованных учебных центрах. Перечень учебных центров и условия обучения представлены на сайте компании https://www.securitycode.ru/company/education/training- courses/ . Связаться с представителем компании по вопросам организации обучения можно по электронной почте (education@securitycode.ru).

Общие сведения

Назначение программы

Программа предназначена для тестирования действующих настроек межсетевых экранов, находящихся на пути зашифрованного трафика между компонентами комплекса.

Программа предназначена для решения следующих задач:

1. Имитация сетевого взаимодействия компонентов комплекса.
2. Проверка возможности обмена данными между компонентами комплекса.

Основные функции программы

Для решения перечисленных выше задач программа обеспечивает выполнение следующих основных функций:

1. Импорт схемы каналов связи комплекса из файла формата XML.
2. Экспорт схемы каналов связи комплекса в файл формата XML.
3. Создание и редактирование схемы каналов связи комплекса.
4. Проверка доступности каналов связи, указанных в схеме.
5. Проверка соединения с помощью команды ping.
6. Построение маршрутов с помощью программы traceroute.

Принципы функционирования программы

Для передачи зашифрованного трафика комплекс использует определенные протоколы и порты (см. стр. 17). Если на пути зашифрованного трафика находятся межсетевые экраны или другое оборудование, осуществляющее фильтрацию IP-пакетов, необходимо создать для них правила, разрешающие прохождение служебных пакетов комплекса по указанным протоколам и портам.

Данная сервисная программа имитирует взаимодействие процессов (программ) различных компонентов комплекса и проверяет возможность обмена данными между ними. Результаты проверки отображаются в окне программы.

Программу устанавливают на компьютеры, находящиеся в локальных сетях, в которых предполагается установка компонентов комплекса.

После запуска процесса проверки каналов связи, программа начинает обмен тестовыми IP- пакетами с другими компьютерами- имитаторами. Перечень протоколов и портов, по которым устанавливается соединение между компьютерами-имитаторами, хранится в схеме каналов связи комплекса.

Исходная схема каналов связи поставляется совместно с программой. Имеется возможность редактирования этой схемы средствами программы, а также ее экспорт в файл и импорт из файла формата XML.

Программа предоставляет возможность выполнения команд ping и traceroute, а также просмотра результатов выполнения этих команд.

Требования к оборудованию и программному обеспечению

Программа работает на любом компьютере с двухъядерным процессором и установленной ОС Windows XP или более поздней версией.

Установка программы

Для установки программы скопируйте с установочного диска на компьютер директорию \Tools\Код Безопасности\ServiceTools\.

Подготовка к тестированию

Перед проведением тестирования каналов связи между локальными сетями, в которых устанавливаются (или уже установлены) компоненты комплекса, необходимо выполнить подготовительные действия.

Для подготовки к тестированию:

1. В локальных сетях определите компьютеры, которые будут имитировать компоненты комплекса.
2. Имитирующим компьютерам установите IP-адреса, предусмотренные для компонентов Комплекса.
3. С установочного диска скопируйте директорию \Tools\Код Безопасности\ServiceTools\ на компьютеры, имитирующие компоненты комплекса.
4. На компьютерах-имитаторах запустите на исполнение файл PortChecker.exe.

Проверка каналов связи

Переход к режиму проверки каналов связи

Для перехода к режиму проверки каналов связи:

- Выберите на ленте вкладку "Каналы связи".

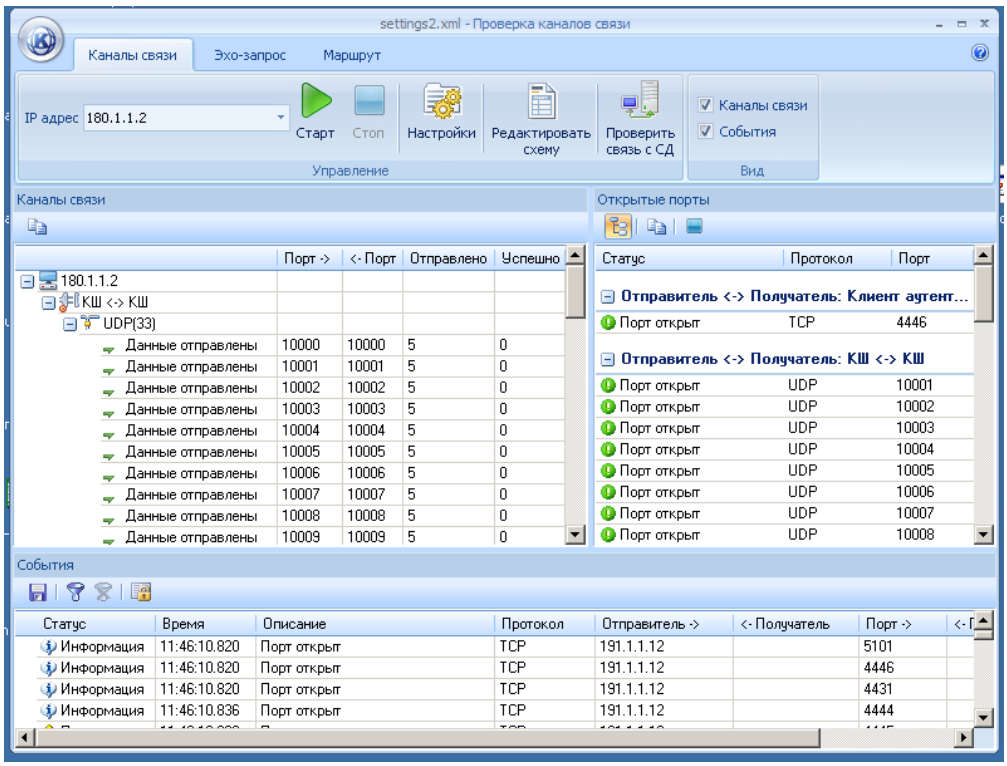


Табл.1 Окна вкладки "Каналы связи"

Окно	Описание
Каналы связи	Перечень проверяемых портов и сообщения о текущем этапе проверки и ее окончательных результатах
Открытые порты	Перечень и статус проверяемых портов на компьютере с установленной программой
События	Перечень зарегистрированных событий при проверке каналов связи

Табл.2 Инструменты вкладки "Каналы связи"

Значок	Элемент	Описание
	IP-адрес	Перечень IP-адресов, по которым будет выполнена проверка. Разделитель между введенными значениями — пробел
	Старт	Запускает процедуру проверки каналов связи
	Стоп	Останавливает процедуру проверки каналов связи
	Настройки	Вызывает диалог "Настройки" для определения параметров процесса проверки каналов связи
	Редактировать схему	Вызывает окно "Редактор схем"

Значок	Элемент	Описание
	Проверить связь с СД	Запускает процедуру проверки канала связи абонентского пункта с сервером доступа
	Каналы связи	При наличии отметки отображается окно "Каналы связи"
	События	При наличии отметки отображается окно "События"

Табл.3 Команды меню и инструменты окна "Каналы связи"

Значок	Команда	Описание
	Скопировать значения в буфер обмена	Копирует содержимое окна в буфер обмена
	Отфильтровать события	Отображает в окне "События" записи, отфильтрованные по выбранному получателю, группе портов или протоколу
	Эхо-запрос	Выполняет переход к вкладке "Эхо-запрос" для проверки соединения с выбранным получателем
	Маршрут	Выполняет переход к вкладке "Маршрут" для построения маршрута к выбранному получателю

Табл.4 Инструменты окна "Открытые порты"

Значок	Команда	Описание
	Группировать значения по отправителю и получателю	Отображает перечень портов, сгруппированных по полю "Отправитель-Получатель"
	Скопировать значения в буфер обмена	Копирует содержимое окна в буфер обмена
	Остановить сервер	Отключает прослушивание портов при отправке пакетов

Табл.5 Инструменты окна "События"

Значок	Команда	Описание
	Сохранить данные в файл	Вызывает стандартный диалог Windows для сохранения содержимого окна в файл *.csv
	Фильтровать	Вызывает диалог для определения параметров фильтрации содержимого окна
	Убрать фильтр	Выполняет очистку фильтра
	Автопрокрутка	Включает автоматический режим отображения последней записи

Настройка режима проверки каналов связи

Для настройки режима:

1. На ленте нажмите кнопку "Настройка".
   На экране появится диалог "Настройки".
2. Заполните поля диалога и нажмите кнопку "Применить":

Тайм-аут	Время ожидания, миллисекунд
Количество попыток	Количество попыток проверки канала связи

Размер сообщения (байт)	Размер тестового сообщения для проверки канала связи, байт
Интервал между попытками (с)	Период времени между попытками проверки канала связи, секунд

Управление схемой каналов связи комплекса

Создание схемы каналов связи

Для создания схемы:

1. На панели быстрого доступа нажмите кнопку "Создать".

   На экране появится пустое окно "Редактор схемы".

2. Сформируйте перечень проверяемых каналов связи. Для этого используйте следующие кнопки:

Добавить	Открывает диалог для добавления в таблицу новой записи (см. стр.**11**)
Удалить	Удаляет из таблицы выбранную запись
Редактировать	Открывает диалог для редактирования выбранной записи (см. стр.**11**)

3. Нажмите кнопку "Применить":

Импорт и экспорт схемы каналов связи

Для импорта/экспорта схемы:

- Используйте следующие кнопки панели быстрого доступа:

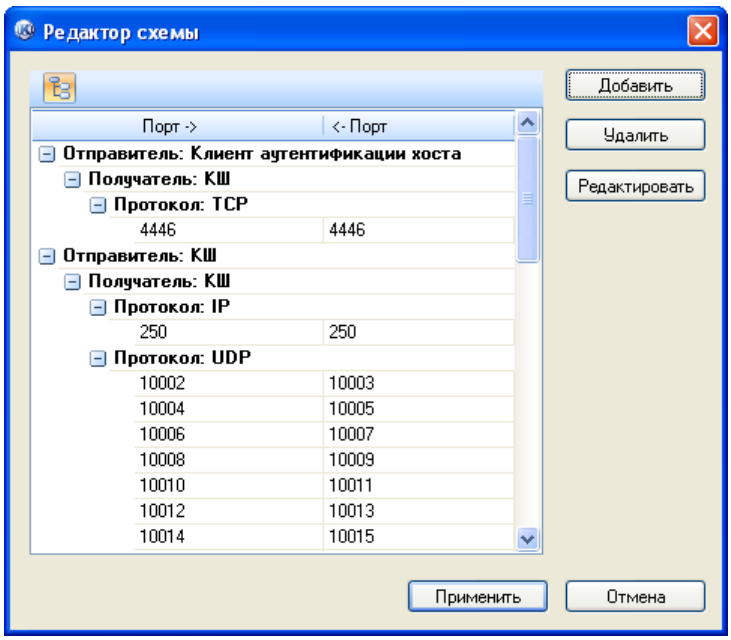
Открыть	Открывает стандартный диалог Windows для выбора файла
Сохранить	Открывает стандартный диалог Windows для сохранения файла

Редактирование схемы каналов связи

Для редактирования схемы:

1. На ленте нажмите кнопку "Редактировать".

   На экране появится окно "Редактор схемы" с имеющейся схемой каналов связи комплекса.



2. Сформируйте перечень проверяемых каналов связи. Для этого используйте следующие кнопки:

Добавить	Открывает диалог для добавления в таблицу новой записи (см. стр.**11**)
Удалить	Удаляет из таблицы выбранную запись
Редактировать	Открывает диалог для редактирования выбранной записи (см. стр.**11**)

3. Нажмите кнопку "Применить":

Создание и редактирование канала связи

Для создания и редактирования канала связи:

1. В окне "Редактор схемы" нажмите нужную кнопку:
   - "Добавить" — для добавления в таблицу новой записи;
   - "Редактировать" — для редактирования выбранной записи.

   На экране появится диалог "Канал связи".
2. Заполните поля диалога и нажмите кнопку "Применить":

Протокол	Наименование протокола
Отправитель/ Имя отправителя	Наименование компонента комплекса — отправителя IP-пакетов
Отправитель/ Порт	Порт отправителя IP-пакетов
Получатель/ Имя получателя	Наименование компонента комплекса — получателя IP-пакетов
Получатель/ Порт	Порт получателя IP-пакетов

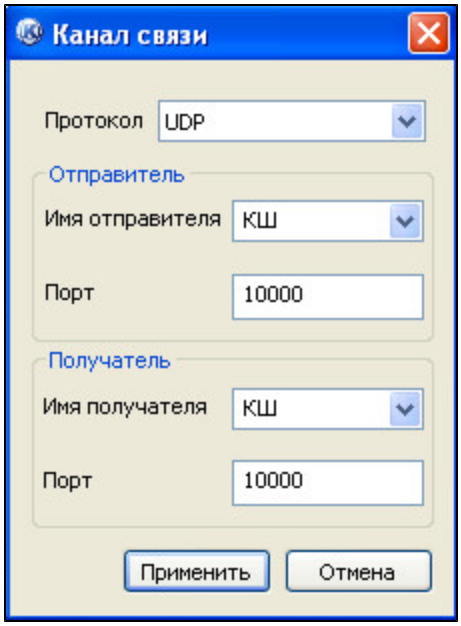
Выполнение проверки каналов связи

Для выполнения проверки:

1. На одном из компьютеров с запущенной программой остановите сервер. Для этого на вкладке "Каналы связи" в окне "Открытые порты" нажмите кнопку "Остановить сервер".
2. В инструментах вкладки "Каналы связи" нажмите кнопку "Редактировать схему".

   На экране появится окно "Редактор схемы" с имеющейся схемой каналов связи комплекса.
3. Выделите в списке порт, предназначенный для прохождения трафика, и нажмите кнопку "Редактировать".

   На экране появится окно "Канал связи".



4. Укажите одинаковые значения в полях "Порт" отправителя и получателя и нажмите кнопку "Применить".

   Окно "Канал связи" закроется.

5. В окне "Редактор схемы" нажмите кнопку "Применить".

   Окно "Редактор схемы" закроется.

6. Перейдите на второй компьютер с запущенной программой и выполните **пп. 2-5**.

7. Перейдите на первый компьютер, с которого был остановлен сервер.

8. На вкладке "Каналы связи" в поле "IP-адрес" укажите IP-адрес сервера и нажмите кнопку "Старт".

   Программа приступит к процедуре установки соединения по указанным адресам. В окне "Каналы связи" будут отображаться сообщения о состоянии процесса установки соединения для каждого порта:

Попытка подключения	Выполняется процедура подключения к указанному компьютеру
Данные отправлены	Подключение к указанному компьютеру выполнено. Выполняется проверка указанного канала связи
Не удалось подключиться	Подключение к указанному компьютеру отсутствует
Не удалось получить данные	Результат проверки указанного канала связи отрицательный
Данные получены	Результат проверки указанного канала связи положительный

9. Для ручного завершения тестирования нажмите кнопку "Стоп".

Проверка соединения

Переход к режиму проверки соединения

Для перехода к режиму:

- Выберите на ленте вкладку "Эхо-запрос".

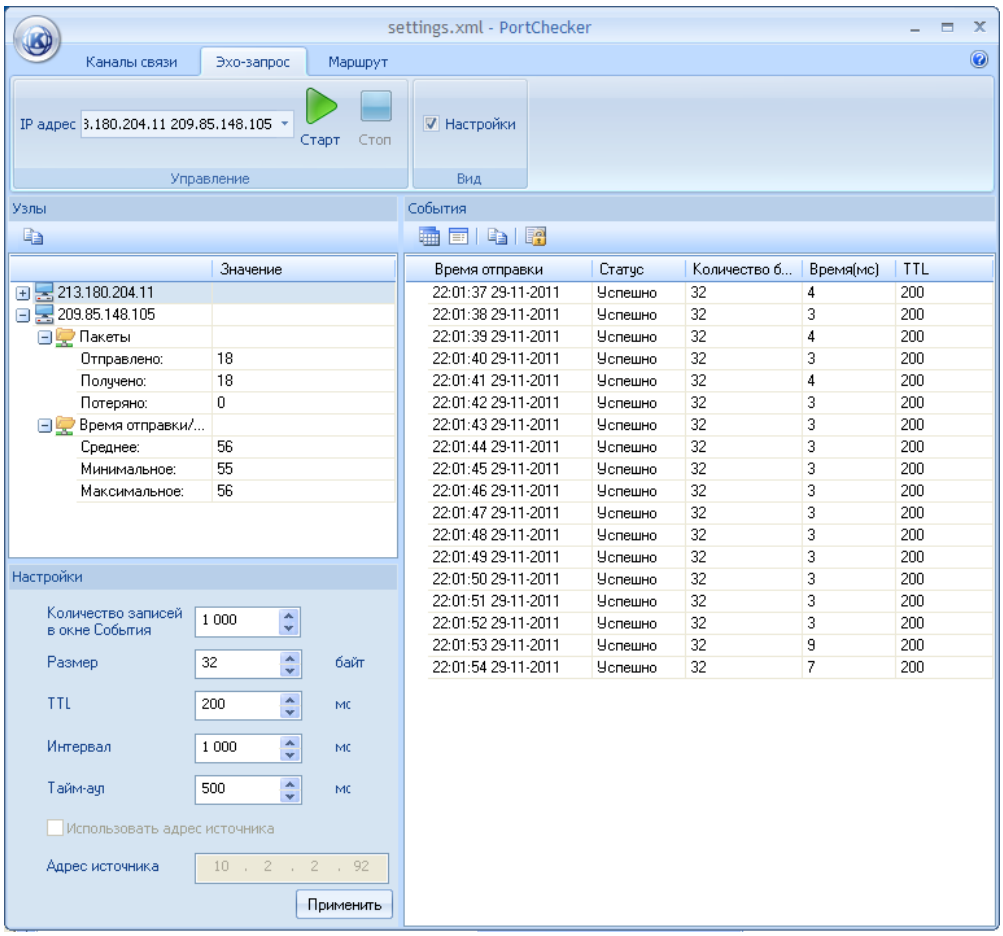


Табл.6 Окна вкладки "Эхо-запрос"

Окно	Описание
Узлы	Результаты выполнения команды ping
Настройки	Настройки команды ping
События	Перечень зарегистрированных событий

Табл.7 Инструменты вкладки "Эхо-запрос"

Значок	Элемент	Описание
	IP-адрес	Перечень IP-адресов, по которым будет выполнена проверка. Разделитель между введенными значениями — пробел
	Старт	Запускает выполнение команды ping
	Стоп	Останавливает выполнение команды ping
	Настройки	При наличии отметки отображается окно "Настройки"

Табл.8 Инструменты окна "Узлы"

Значок	Команда	Описание
	Скопировать значения в буфер обмена	Копирует содержимое окна в буфер обмена

Табл.9 Инструменты окна "События"

Значок	Команда	Описание
	Отобразить в виде таблицы	Отображает содержимое окна в виде таблицы
	Отобразить в виде списка	Отображает содержимое окна в виде списка
	Скопировать значения в буфер обмена	Копирует содержимое окна в буфер обмена
	Автопрокрутка	Включает автоматический режим отображения последней записи

Настройка режима проверки соединения

Для настройки режима:

- Заполните поля окна "Настройки" и нажмите кнопку "Применить":

Количество записей в окне "События"	Максимальное количество записей, отображаемых в окне "События". При достижении указанной величины старые записи замещаются новыми
Размер	Размер ICMP-пакета, посылаемого командой ping, байт
TTL	Время жизни ICMP-пакета, посылаемого командой ping, мс
Интервал	Период времени между отправкой ICMP-пакетов
Тайм-аут	Время ожидания сообщения с эхо-ответом, мс
Использовать адрес источника	Режим выбора сетевой карты на компьютере-отправителе (для ОС Windows Server 2008 и более новых)
Адрес источника	IP-адрес сетевой карты

Выполнение проверки соединения

Для выполнения проверки:

1. В поле "IP-адрес" укажите проверяемые IP-адреса и нажмите кнопку "Старт".

   Программа приступит к проверке соединений по указанным адресам. В окне "Узлы" будут отображаться статистические характеристики процесса.
2. Для завершения процесса нажмите кнопку "Стоп".

Построение маршрута следования данных

Переход к режиму построения маршрута

Для перехода к режиму построения маршрута:

- Выберите на ленте вкладку "Маршрут".

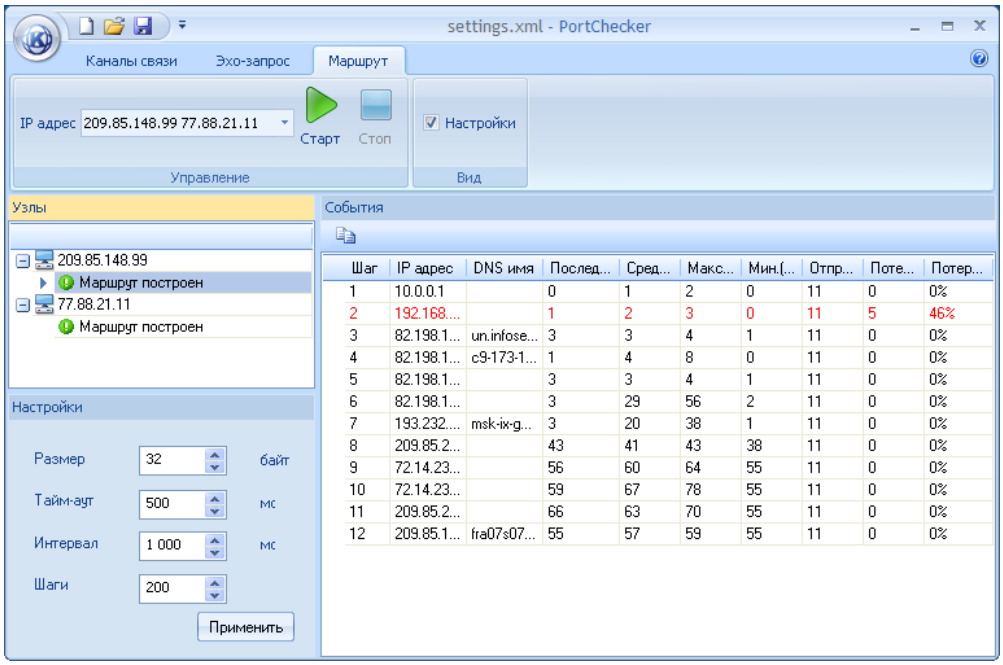


Табл.10 Окна вкладки "Маршрут"

Окно	Описание
Узлы	Результаты выполнения команды traceroute
Настройки	Настройки команды traceroute
События	Перечень зарегистрированных событий

Табл.11 Инструменты вкладки "Маршрут"

Значок	Элемент	Описание
	IP-адрес	Перечень IP-адресов, по которым будет выполнена проверка. Разделитель между введенными значениями — пробел
	Старт	Запускает выполнение команды traceroute
	Стоп	Останавливает выполнение команды traceroute
	Настройки	При наличии отметки отображается окно "Настройки"

Табл.12 Инструменты окна "События"

Значок	Команда	Описание
	Скопировать значения в буфер обмена	Копирует содержимое окна в буфер обмена

Настройка режима построения маршрута

Для настройки режима:

- Заполните поля окна "Настройки" и нажмите кнопку "Применить":

Размер пакета	Размер пакета, посылаемого командой traceroute, байт
Тайм-аут	Время ожидания ответа, миллисекунд
Интервал	Период времени между отправкой IP-пакетов, миллисекунд
Шаги	Максимальное количество маршрутизаторов на пути следования IP-пакета (TTL)

Построение маршрута

Для построения маршрута:

1. В поле "IP-адрес" укажите проверяемые IP-адреса и нажмите кнопку "Старт".

   Программа приступит к процедуре построения маршрутов для указанных IP-адресов. В окне "Узлы" будут отображаться сообщения о состоянии процесса построения маршрута для каждого IP-адреса:

Маршрут строится	Выполняется процедура построения маршрута для указанного IP-адреса
Маршрут построен	Результат построения маршрута для указанного IP-адреса положительный

2. Для завершения процесса нажмите кнопу "Стоп".

Приложение

Компоненты комплекса

Обозначение	Описание
КШ	Криптографический шлюз
Клиент аутентификации пользователя	Клиент аутентификации пользователя
ПУ ЦУС	Программа управления ЦУС
ЦУС	Центр управления сетью

Протоколы и порты

В данном разделе представлены сведения о протоколах и портах, используемых для связи между компонентами комплекса.

Если на пути зашифрованного трафика находятся межсетевые экраны или другое оборудование, осуществляющее фильтрацию IP-пакетов, необходимо создать для них правила, разрешающие прохождение служебных пакетов комплекса по протоколам и портам, указанным в таблице.

Протокол/порт	Описание	Источник/получатель	Примечание
TCP/4444	Передача сообщений от ПУ ЦУС к ЦУС; обмен сообщениями между ЦУС и агентом ЦУС. ПУ ЦУС, агент ЦУС устанавливают подключение со случайного порта 1024-65535 на порт ЦУС 4444. ЦУС отвечает на тот порт, с которого было обращение	ПУ ЦУС / ЦУС. Агент ЦУС / ЦУС	
TCP/4445	Передача обновлений ПО от ПУ ЦУС к ЦУС и обмен сообщениями между ПУ ЦУС и агентом ЦУС. ПУ ЦУС устанавливает подключение со случайного порта 1024-65535 на порт ЦУС 4445. ЦУС отвечает на тот порт, с которого было обращение	ПУ ЦУС / ЦУС. ПУ ЦУС / агент ЦУС. Агент ЦУС / ПУ ЦУС	
TCP/4446	Аутентификация пользователей в защищенном сегменте сети. Клиент аутентификации устанавливает подключение со случайного порта 1024-65535 на порт ЦУС 4446. ЦУС отвечает на тот порт, с которого было обращение	Компьютер с установленной программой "Клиент аутентификации пользователя" / КШ	

Протокол/порт	Описание	Источник/получатель	Примечание
TCP/5100	Передача сообщений от ЦУС к КШ и обмен сообщениями между КШ в кластере. Узел кластера обращается к парному с порта 10000-65535 на порт 5100. Парный отвечает на тот порт, с которого было обращение	ЦУС / КШ. Основной КШ / резервный КШ. Резервный КШ / основной КШ	
TCP/5101	Передача сообщений от КШ к ЦУС. Узел устанавливает подключение со случайного порта 10000-65535 на порт ЦУС 5101. ЦУС отвечает на тот порт, с которого было обращение	КШ / ЦУС	
TCP/5102	Передача файлов от ЦУС к КШ. Узел устанавливает подключение со случайного порта 10000-65535 на порт ЦУС 5102. ЦУС отвечает на тот порт, с которого было обращение	ЦУС / КШ	
TCP/5103	Передача файлов от ЦУС к КШ. Узел устанавливает подключение со случайного порта 10000-65535 на порт ЦУС 5103. ЦУС отвечает на тот порт, с которого было обращение	ЦУС / КШ	
UDP/5101	Передача сообщений от КШ к ЦУС. Узел обращается с порта 5100 на порт ЦУС 5101. ЦУС отвечает с порта 5101 на порт 5100	КШ (исходящий порт 5100) / ЦУС	
UDP/5106 UDP/5107	Поддержка работы КШ за NAT. В зависимости от используемых классов трафика, узлы отправляют пакеты с портов 10000-10031 на порты ЦУС 5106-5107	КШ / ЦУС	
UDP/10000	Передача зашифрованного трафика. Узлы обмениваются пакетами с порта 10000 на порт 10000	КШ / КШ. КШ / ЦУС	

Протокол/ порт	Описание	Источник/получатель	Примечание
UDP/10000-10031	Передача зашифрованного трафика. В зависимости от используемых классов трафика, узлы обмениваются пакетами с портов 10000-31 на соответствующие порты 10000-31	КШ / КШ. КШ / ЦУС	

Документация

1.	Аппаратно-программный комплекс шифрования "Континент". Руководство администратора. Централизованное управление комплексом
2.	Аппаратно-программный комплекс шифрования "Континент". Руководство администратора. Локальное управление сетевыми устройствами
3.	Аппаратно-программный комплекс шифрования "Континент". Руководство администратора. Аудит
4.	Аппаратно-программный комплекс шифрования "Континент". Руководство администратора. Аутентификация пользователя