КОД безопасности

Аппаратно-программный комплекс шифрования

Континент

Версия 3.9

Руководство администратора

Межсетевое экранирование

RU.88338853.501430.022 90 4

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

Список сокращений

АПКШ	Аппаратно-программный комплекс шифрования
БД	База данных
КШ	Криптографический шлюз
МЭ	Межсетевой экран
НСД	Несанкционированный доступ
ОС	Операционная система
ПО	Программное обеспечение
РМ	Рабочее место
ПУ	Программа управления
СУ	Сетевое устройство
ЦУС	Центр управления сетью
DNS	Domain Name System
DoS	Denial of Service
DSCP	Differentiated Services Code Point
FTP	File Transfer Protocol
HTTPS	HyperText Transfer Protocol Secure
ICMP	Internet Control Message Protocol
IP	Internet Protocol
IPP	IP Precedence
MIME	Multipurpose Internet Mail Extensions
NAT	Network Address Translation
POSIX	Portable operating system interface
SSH	Secure Shell
SSL	Secure Sockets Layer
TCP	Transmission Control Protocol
TLS	Transport Layer Security
ToS	Type of Service
UDP	User Datagram Protocol
URL	Uniform Resource Locator
UTC	Coordinated Universal Time — всемирное координированное время

Введение

Документ предназначен для администраторов изделия "Аппаратно-программный комплекс шифрования "Континент". Версия 3.9" (далее — комплекс, АПКШ "Континент"). В нем содержатся сведения, необходимые администраторам для настройки межсетевого экрана комплекса.

Дополнительные сведения, необходимые администратору комплекса, содержатся в [**1**], [**2**].

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

Служба технической поддержки. Связаться со службой технической поддержки можно по телефону 8 800 505-30-20 или по электронной почте support@securitycode.ru.

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

Версия — 3.9.3 от 14.02.2924.

Глава 1
Объекты ЦУС

Межсетевой экран по умолчанию работает в режиме блокировки проходящего через КШ трафика. Настройка МЭ осуществляется путем определения списков правил фильтрации и трансляции трафика согласно топологии сети и требованиям безопасности.

Правила фильтрации разрешают или запрещают продвижение IP-пакетов через КШ комплекса, т. е. определяют доступность защищаемой сети для других локальных сетей или из интернета.

Правила трансляции служат для преобразования заголовка IP-пакетов трафика при прохождении через КШ.

Правила фильтрации и трансляции (доступа) сгруппированы в списки в строгой очередности, определяющей четкий порядок действий над IP-пакетами при обработке трафика узлами комплекса. Эти списки по умолчанию пусты и пропуск всего трафика, кроме служебных пакетов комплекса, через КШ запрещен.

Прежде чем приступить к составлению списков правил доступа, необходимо создать все необходимые объекты ЦУС, выступающие в роли параметров этих правил.

Для определения IP-пакетов, к которым следует применять правило доступа, используются следующие объекты ЦУС:

Объект ЦУС		**Описание**
Значок	**Название**	
	Сетевые объекты	Отправители или получатели IP-пакета (основной характеристикой служит IP-адрес или их диапазон)
	Группы сетевых объектов	Отправители или получатели IP-пакета (основной характеристикой служит IP-адрес или их диапазон)
	Сервисы	Протокол интернет, сетевой или транспортный протокол (TCP или UDP, ICMP или IP) с возможностью указания определенного порта или их диапазона (для TCP и UDP), типа и кода ICMP-сообщения
	Пользователи	Трафик определенного пользователя
	Временные интервалы	Расписание действия правила
	Классы трафика	Трафик определенного класса
	Реакции на события	Реакции на определенные события

Примечание. Автоматически при инициализации ЦУС создаются следующие объекты ЦУС:

- набор часто используемых сервисов;
- класс трафика "Нормальный" с установленным приоритетом 5 уровня и портом 10000 внешнего интерфейса;
- временной интервал "Постоянно", определяющий ежедневное круглосуточное действие правила.

Сетевые объекты

Сетевые объекты типа Unicast привязывают к КШ. Привязка определяет КШ, на котором будут выполняться правила фильтрации с упоминанием этих сетевых объектов. Параметры привязки будут учитываться при функционировании правил фильтрации.

Внимание! Сетевой объект, относящийся к внутреннему интерфейсу КШ, должен быть обязательно привязан к этому же КШ. Обмен IP-пакетами с объектами, не имеющими привязки к данному КШ, разрешен только через внешний интерфейс.

Если сетевой объект входит в состав другого сетевого объекта, имеющего тип привязки "Защищаемый", то для дочернего объекта можно использовать только тип привязки "Внутренний".

Для сетевых объектов типа Multicast определяют перечень КШ, которые участвуют в групповой рассылке. На этих КШ будет автоматически включен режим ip multicast-routing. Адреса сетевых объектов этого типа должны принадлежать диапазону от 224.0.0.0 до 239.255.255.255.

Примечание. Мультикастовый трафик между КШ-источником и КШ-получателем, находящимися в разных защищаемых сетях, возможен только при наличии между ними парных связей (см. [1]).

Управление группами сетевых объектов описывается на стр. **11**.

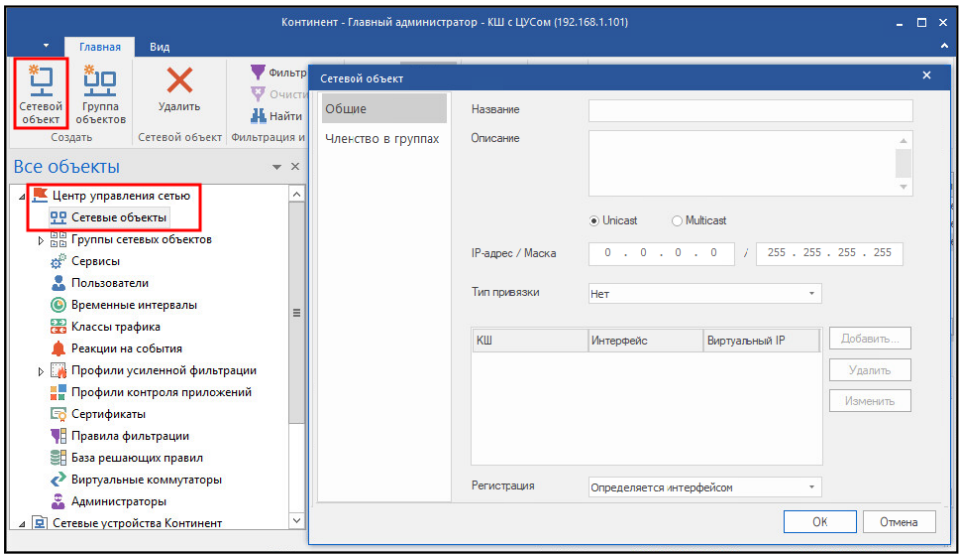
Для создания сетевого объекта:

1. Раскройте раздел "Центр управления сетью" в области объектов управления ПУ ЦУС и выберите пункт "Сетевые объекты".

   В области отображения информации появится текущий список сетевых объектов ЦУС.

2. Нажмите кнопку "Сетевой объект" на панели инструментов.

   На экране появится окно настройки параметров сетевого объекта.



3. Введите уникальное наименование сетевого объекта в поле "Название" и, при необходимости, дополнительные сведения об объекте в поле "Описание".
4. Выберите тип и задайте сетевой адрес создаваемого объекта.

5. Укажите прочие параметры сетевого объекта в соответствии с выбранным типом объекта.

Поле	Описание
Тип Unicast	
Тип привязки	Тип привязки: • Нет — привязка сетевого объекта к КШ отсутствует. • Внутренний — сетевой объект привязан к КШ. Шифрование трафика не требуется. • Защищаемый — сетевой объект привязан к КШ. Требуется шифрование трафика. **Внимание!** Шифрование трафика будет выполняться только при включении данного КШ в список связанных КШ (см. [**1**])
Привязка сетевого объекта	Привязка КШ, на котором должны выполняться правила фильтрации, с упоминанием этого сетевого объекта (только для типов привязки "Внутренний" и "Защищаемый"). Для добавления привязки нажмите кнопку "Добавить". В открывшемся окне выберите необходимые криптошлюз и интерфейс. Фильтрации будут подвергаться только те IP-пакеты, которые проходят через этот интерфейс указанного криптошлюза. При выборе значения "Любой" фильтрации будут подвергаться IP-пакеты, проходящие через любой интерфейс. **Внимание!** Если в поле "Тип привязки" указано значение "Защищаемый", не рекомендуется использовать внешний интерфейс КШ. Поле "Виртуальный IP-адрес/Маска" позволяет управлять виртуальной адресацией (см. стр. **58**). Поле доступно только в том случае, если в поле "Тип привязки" установлено значение "Защищаемый"
Тип Multicast	
Получатели	Перечень КШ, которые должны участвовать в групповой передаче (для выбора нажмите кнопку "Добавить")

6. Выберите тип регистрации событий, происходящих с этим сетевым объектом, в журнале аудита и нажмите кнопку "ОК".

   В списке объектов ЦУС появится созданный объект, а сведения о нем будут сохранены в БД.

Для редактирования параметров сетевого объекта:

1. Вызовите список сетевых объектов в области отображения информации ПУ ЦУС.
2. Вызовите контекстное меню требуемого сетевого объекта и активируйте команду "Свойства...".

   На экране появится окно настройки параметров сетевого объекта.
3. Выполните требуемые изменения и нажмите кнопку "ОК".

   В списке и в БД ЦУС параметры объекта будут заменены.

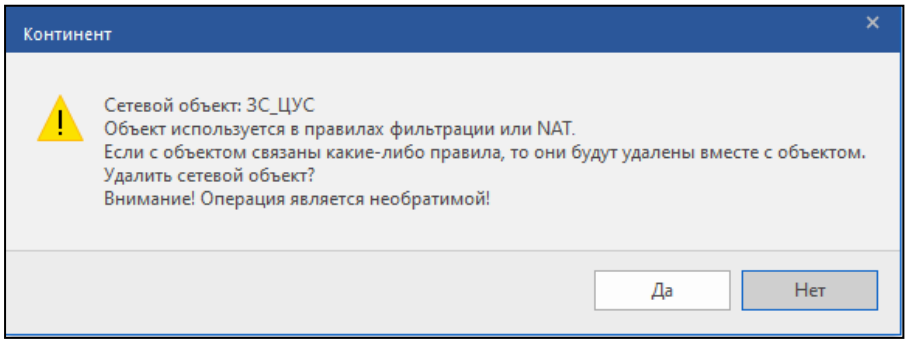
Для удаления сетевого объекта:

Внимание! Перед удалением объекта необходимо исключить его из правил фильтрации.

1. Вызовите список сетевых объектов в области отображения информации ПУ ЦУС.
2. Вызовите контекстное меню требуемого сетевого объекта и активируйте команду "Удалить выделенные...".

   На экране появится запрос на удаление объекта.
3. Нажмите кнопку "Да".

   Если удаляемый сетевой объект используется в действующих правилах фильтрации или трансляции, на экране появится предупреждающее окно о том, что соответсвующие правила будут удалены вместе с сетевым объектом без возможности восстановления.



4. Для удаления сетевого объекта и правил нажмите кнопку "Да".

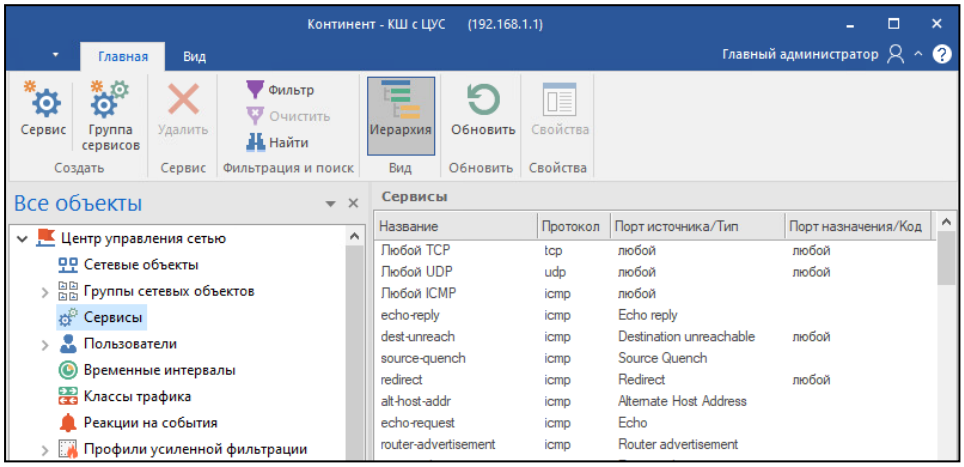
   Для отказа от удаления нажмите кнопку "Нет".

Сервисы

Для перехода к списку сервисов:

- Раскройте раздел "Центр управления сетью" в области объектов управления ПУ ЦУС и выберите пункт "Сервисы".

  В области отображения информации появится текущий список сервисов ЦУС.



Для создания сервиса:

1. Раскройте раздел "Центр управления сетью" в области объектов управления ПУ ЦУС и выберите пункт "Сервисы".

   В области отображения информации появится текущий список сервисов ЦУС.
2. Нажмите кнопку "Сервис" на панели инструментов.

   На экране появится окно настройки параметров сервиса.
3. Настройте параметры создаваемого сервиса.

Параметр	Описание
Название	Название сервиса должно быть информативным и лаконичным, так как в таблице правил фильтрации сервис представлен только названием
Протокол	Используемый протокол. Выберите его из раскрывающегося списка либо введите в это поле его номер (в соответствии с полем Protocol в заголовке IP-пакета)
Параметры протокола	Настройте параметры, специфичные для выбранного протокола: • для протоколов TCP или UDP укажите порты отправителя и получателя IP-пакетов. Для этого для каждого адресата выберите требуемый оператор из раскрывающегося списка и в появившемся поле укажите номер порта; • для протокола ICMP выберите тип ICMP-сообщения из раскрывающегося списка. Кроме этого, для ICMP-сообщений "Destination unreachable", "Redirect" и "Time exceeded", "Parameter problem" укажите код

4. Нажмите кнопку "OK".

   Список на экране и в БД ЦУС дополнится данными нового сервиса.

Для настройки параметров сервиса:

1. Вызовите список сервисов в окне отображения информации ЦУС.
2. Вызовите контекстное меню требуемого сервиса и активируйте команду "Свойства...".

   На экране появится окно настройки параметров сервиса. Перечень отображаемых полей зависит от выбора протокола.
3. Отредактируйте параметры сервиса.
4. Нажмите кнопку "OK".

   В списке на экране и в БД ЦУС параметры сервиса будут заменены.

Для удаления сервиса:

Внимание! Перед удалением сервиса необходимо исключить его из правил фильтрации.

1. Вызовите список сервисов в окне отображения информации ЦУС.
2. Вызовите контекстное меню удаляемого сервиса и активируйте команду "Удалить сервис...".

   На экране появится запрос на удаление сервиса.
3. Нажмите кнопку "Да".

   Если удаляемый сервис используется в действующих правилах фильтрации, на экране появится окно о невозможности продолжения операции со списком затронутых правил. В противном случае объект будет удален из списка, а сведения о нем — из базы данных ЦУС без возможности восстановления.

Временные интервалы

Для определения временного интервала:

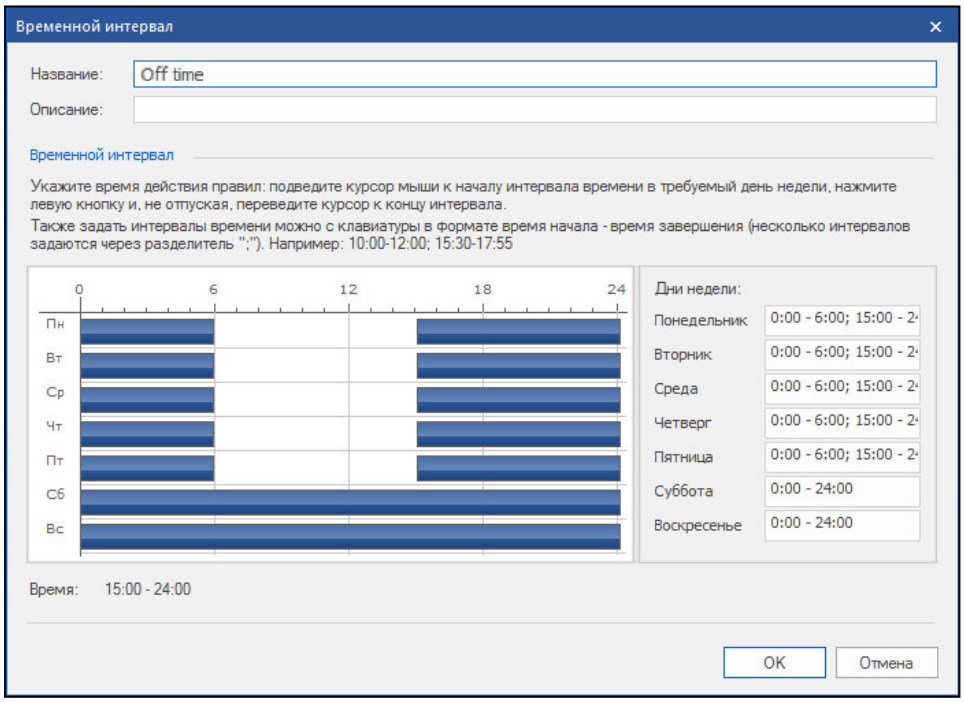
1. Раскройте раздел "Центр управления сетью" в области объектов управления ПУ ЦУС и выберите пункт "Временные интервалы".

   В области отображения информации появится текущий список временных интервалов.
2. Нажмите кнопку "Временной интервал" на панели инструментов.

   На экране появится окно настройки параметров временного интервала.
3. Укажите в поле "Название" наименование данного расписания, а в поле "Описание" — дополнительную информацию о нем.

Совет. По возможности давайте расписаниям осмысленные названия, так как при настройке параметров правил фильтрации выбор этого элемента правила осуществляется только по его названию.

4. Укажите время действия правил фильтрации: подведите курсор мыши к началу интервала времени в требуемый день недели, нажмите левую кнопку и, не отпуская, переведите курсор к концу интервала. Для задания другого интервала повторите операцию. Также задать интервалы времени можно с клавиатуры в формате время начала – время окончания, используя в качестве разграничителя между интервалами одного дня символ ";".



Примечание. Время, указанное в настройках интервалов, соответствует времени по стандарту UTC. Поэтому при настройке временных интервалов необходимо вводить поправку, учитывающую часовой пояс, в котором должны действовать правила фильтрации.

5. Нажмите кнопку "OK".

   Список временных интервалов на экране и в БД ЦУС дополнится соответствующей строкой данных.

Для настройки параметров временного интервала:

1. Вызовите список временных интервалов.
2. Вызовите контекстное меню требуемого временного интервала и активируйте команду "Свойства...".

   На экране появится окно настройки параметров временного интервала.
3. Выполните требуемые изменения и нажмите кнопку "ОК".

   Новые значения параметров временного интервала будут сохранены в базе данных ЦУС.

Для удаления временного интервала:

Внимание! Перед удалением объекта необходимо исключить его из правил фильтрации.

1. Вызовите список временных интервалов в окне объектов ЦУС.
2. Вызовите контекстное меню удаляемого временного интервала и активируйте команду "Удалить временной интервал...".

   На экране появится запрос на удаление временного интервала.
3. Нажмите кнопку "Да".

   В окне "Список объектов ЦУС" и в БД ЦУС временной интервал будет удален из списка.

Пользователи

Объекты ЦУС "Пользователи" используются в правилах фильтрации в качестве отправителя.

Предусмотрено объединение пользователей в группы. Группы также могут использоваться в правилах фильтрации в качестве отправителя.

Для просмотра списка пользователей:

- Раскройте раздел "Центр управления сетью" в области объектов управления ПУ ЦУС и выберите пункт "Пользователи".

  В области отображения информации появится текущий список пользователей и групп.

Описание работы со списком пользователей и групп приведено в [**1**].

Управление группами

Для удобства просмотра и управления объекты можно объединять в группы. Возможность группировки предусмотрена для следующих объектов:

- сетевые объекты;
- сервисы;
- пользователи.

При удалении группы объекты, входящие в нее, не удаляются.

Для создания группы объектов:

1. Раскройте раздел "Центр управления сетью" в области объектов управления ПУ ЦУС и выберите пункт объектов, группу которых требуется создать.
2. Вызовите контекстное меню в области отображения информации и выберите команду создания группы.

   На экране появится окно для создания группы.
3. Заполните поля данного диалога и нажмите кнопку "ОК".

Поле	Описание
Название	Наименование группы объектов
Описание	Дополнительные сведения (необязательный параметр)
Размещение (только для пользователей)	Сетевой объект, на хостах которого разрешен доступ для создаваемой группы пользователей
Элементы группы (сервисы, сетевые объекты, пользователи)	Перечень объектов, входящих в группу. Для формирования используйте кнопки добавления и удаления объекта
Регистрация (только для сетевых объектов)	Вариант регистрации событий в журналах

В списке появятся данные новой группы, а сведения о ней будут сохранены в базе данных ЦУС.

Для редактирования свойств группы:

1. Раскройте раздел "Центр управления сетью" в области объектов управления ПУ ЦУС, затем подраздел соответствующего сетевого объекта.
2. Вызовите контекстное меню требуемой группы и выберите команду "Свойства...".

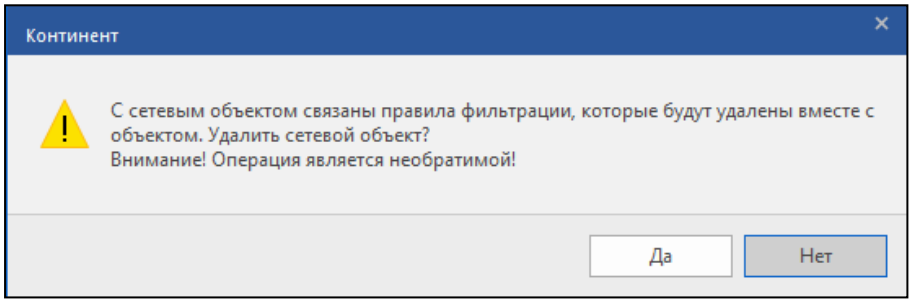
   На экране появится окно для редактирования свойств группы.
3. Внесите необходимые изменения и нажмите кнопку "ОК".

   В списке на экране и в БД ЦУС параметры группы будут заменены.

Для удаления группы:

1. Раскройте раздел "Центр управления сетью" в области объектов управления ПУ ЦУС, затем подраздел соответствующего сетевого объекта.
2. Вызовите контекстное меню требуемой группы и выберите команду "Удалить группу...".

   На экране появится окно с предупреждением, что вместе с гуппой будут удалены правила фильтрации, в которые входит данная группа.



3. Для удаления группы и правил нажмите кнопку "Да".

   Для отказа от удаления нажмите кнопку "Нет".

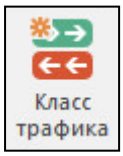
Классы трафика

Для определения класса трафика:

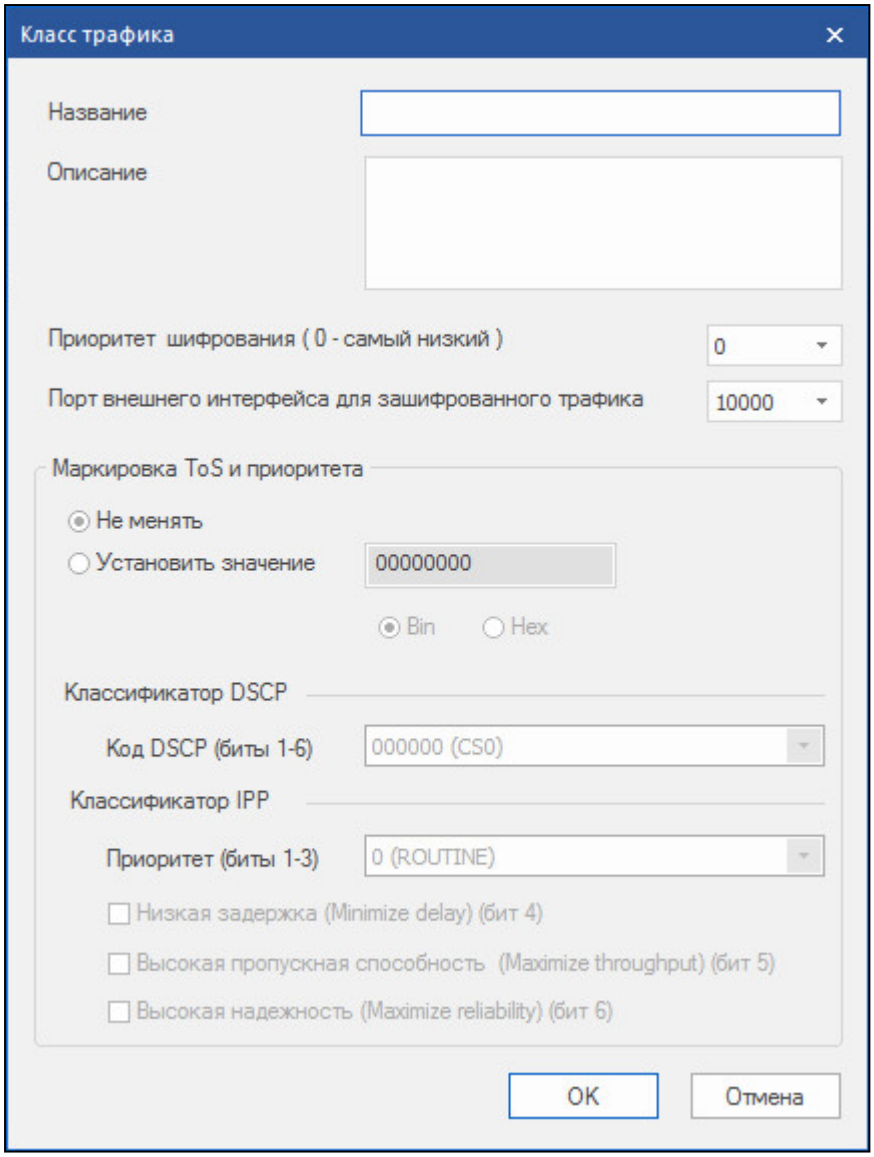
1. Раскройте раздел "Центр управления сетью" в области объектов управления ПУ ЦУС и выберите пункт "Классы трафика".

   В области отображения информации появится текущий список классов трафика.

   Примечание. Класс трафика "Нормальный" создается автоматически при инициализации ЦУС.
2. Нажмите кнопку "Класс трафика" на панели инструментов.



   На экране появится окно настройки параметров класса.



3. Заполните поля параметров и нажмите кнопку "OK".

Поле	**Описание**
Название	Наименование класса трафика
Описание	Произвольный текстовый комментарий (необязательный параметр)
Приоритет шифрования	Очередность обработки IP-пакета, отнесенного к данному классу, блоком криптографической защиты. Возможные значения 0–31. Большему значению соответствует более высокий приоритет
Порт внешнего интерфейса для зашифрованного трафика	Порт внешнего интерфейса, с которого отправляются IP-пакеты данного класса
Не менять	Сохраняет значение поля ToS у исходящего IP-пакета таким же, как у входящего
Установить значение	Назначает исходящему IP-пакету указанное значение поля ToS
Bin/Hex	Отображает назначаемое значение поля ToS в двоичном или шестнадцатеричном виде
Код DSCP (биты 1–6)	Определяет значение поля ToS по шестибитному классификатору DSCP. Возможные значения 0–63
Приоритет (биты 1–3)	Определяет первые три бита значения поля ToS по классификатору IPP. Возможные значения 0–7
Низкая задержка	Определяет четвертый бит значения поля ToS. Наличие отметки указывает режим низкой задержки

Поле	Описание
Высокая пропускная способность	Определяет пятый бит значения поля ToS. Наличие отметки указывает режим высокой пропускной способности
Высокая надежность	Определяет шестой бит значения поля ToS. Наличие отметки указывает режим высокой надежности

Для настройки параметров класса трафика:

1. Раскройте раздел "Центр управления сетью" в области объектов управления ПУ ЦУС и выберите пункт "Классы трафика".
2. Вызовите контекстное меню требуемого класса и активируйте команду "Свойства...".

   На экране появится окно настройки параметров временного интервала.
3. Осуществите требуемые изменения и нажмите кнопку "ОК".

   Новые значения параметров класса трафика будут сохранены в базе данных ЦУС.

Для удаления класса трафика:

Внимание! Перед удалением объекта необходимо исключить его из правил фильтрации.

1. Раскройте раздел "Центр управления сетью" в области объектов управления ПУ ЦУС и выберите пункт "Классы трафика".
2. Вызовите контекстное меню удаляемого класса и активируйте команду "Удалить класс трафика...".

   На экране появится запрос на удаление класса.
3. Нажмите кнопку "Да".

   В окне ПУ и в БД ЦУС класс трафика будет удален.

Примечание. Предустановленный класс трафика "Нормальный" удалению не подлежит.

Реакции на события

Агент ЦУС и СД может отслеживать определенные события и реагировать на них указанным образом. Предусмотрены следующие альтернативные реакции на события:

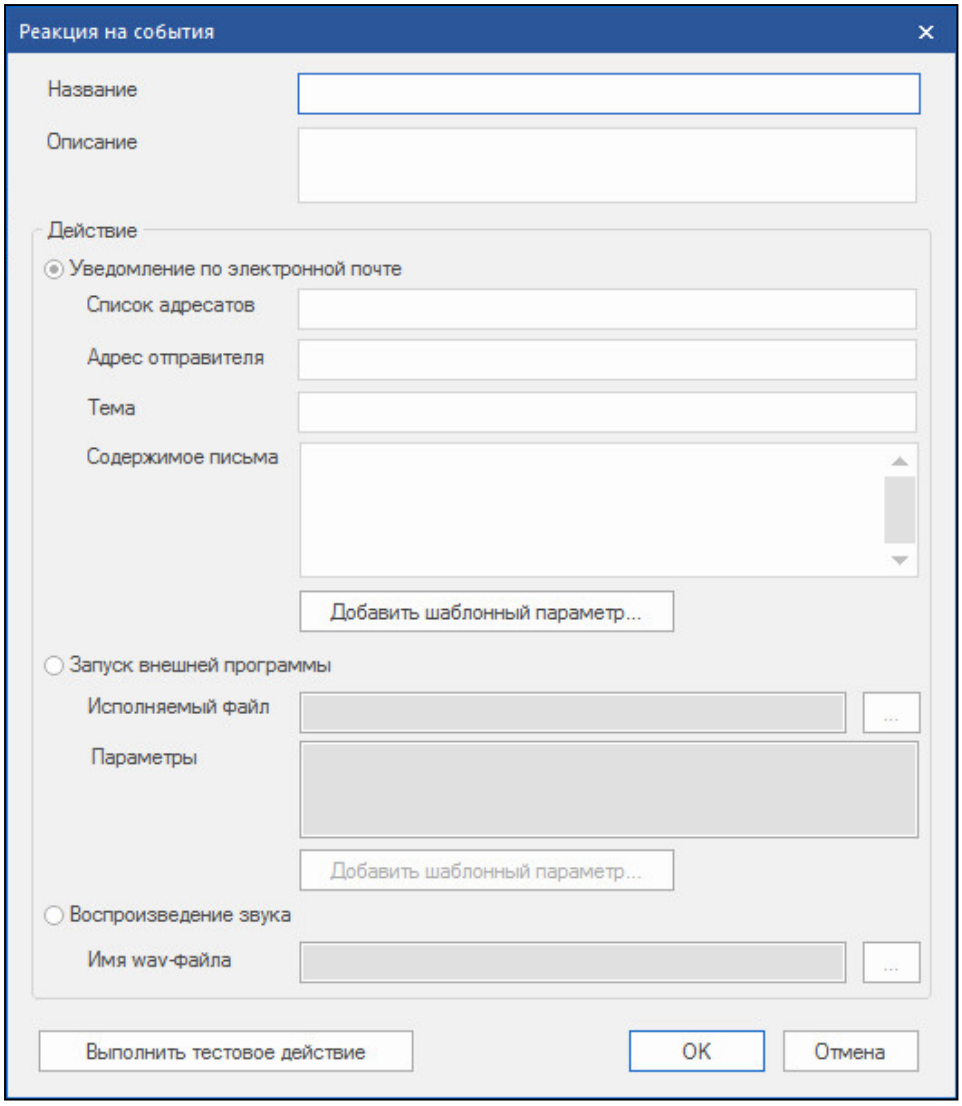
- уведомление по электронной почте;
- запуск внешней программы;
- звуковое оповещение.

Для вызова списка реакций на события:

1. Раскройте раздел "Центр управления сетью" в области объектов управления ПУ ЦУС и выберите пункт "Реакции на события".

   В области отображения информации появится текущий список реакций.
2. Нажмите кнопку "Реакция на события" на панели инструментов.

   На экране появится окно настройки параметров реакции.



3. Выберите тип действия, заполните соответствующие поля параметров и нажмите кнопку "OK".

Параметр	Описание
Название	Наименование объекта, уникальное для списка реакций на события
Описание	Произвольный текстовый комментарий (необязательный параметр)
Список адресатов	Список адресов электронной почты получателей уведомлений (через ";")
Адрес отправителя	Адрес электронной почты для отображения в поле "Отправитель" сообщения с уведомлением
Тема	Тема сообщения с уведомлением
Содержимое письма	Текст уведомления. Для вставки в текст значений параметров событий используйте кнопку "Добавить шаблонный параметр..."
Исполняемый файл	Полное имя исполняемого файла. Для выбора файла используйте кнопку "..."
Параметры	Перечень параметров запуска программы. Для вставки значений параметров событий используйте кнопку "Добавить шаблонный параметр..."
Имя wav-файла	Имя звукового файла в формате WAV. Для выбора файла в стандартном диалоге Windows используйте кнопку "..."

Примечание. Для рассылки уведомлений по электронной почте в настройках агента ЦУС и СД должен быть указан почтовый сервер, через который будут рассылаться уведомления. Описание настройки агента средствами локального управления приведено в [1].

Для настройки параметров реакции на события:

1. Раскройте раздел "Центр управления сетью" в области объектов управления ПУ ЦУС и выберите пункт "Реакции на события".
2. Вызовите контекстное меню требуемой реакции и активируйте команду "Свойства...".

   На экране появится окно настройки параметров реакции.
3. Осуществите требуемые изменения и нажмите кнопку "ОК".

   Новые значения параметров реакции на события будут сохранены в БД ЦУС.

Для удаления реакции на события:

Внимание! Перед удалением объекта необходимо исключить его из правил фильтрации.

1. Раскройте раздел "Центр управления сетью" в области объектов управления ПУ ЦУС и выберите пункт "Реакции на события".
2. Вызовите контекстное меню удаляемой реакции и активируйте команду "Удалить реакцию на события...".

   На экране появится запрос на удаление реакции.
3. Нажмите кнопку "Да".

   В окне ПУ и в БД ЦУС класс трафика будет удален.

Глава 2
Правила фильтрации

Управление правилами фильтрации

Правила фильтрации выполняются в строгом порядке — от первого до последнего. Если IP-пакет соответствует параметрам правила, над ним осуществляется действие, заданное этим правилом. Дальнейшая проверка этого IP-пакета по последующим правилам фильтрации не осуществляется.

Для управления списком правил используются команды контекстного меню или кнопки панели инструментов ПУ ЦУС.

При формировании списка правил следует учитывать, что по умолчанию прохождение трафика данных через узлы комплекса запрещено. Исключение составляют служебные пакеты комплекса.

Внимание! Мультикастовый трафик между КШ, находящимися в разных защищаемых сетях, возможен только при наличии между ними парных связей (см. [**1**]).

Для вызова списка правил фильтрации:

- В области объектов управления ПУ ЦУС выберите пункт "ЦУС | Правила фильтрации".

  В правой части окна отобразится список правил фильтрации IP-пакетов.

Список правил фильтрации отображается в форме таблицы, каждая строка которой соответствует одному правилу.

Если правило отключено, оно отображается в таблице серым цветом.

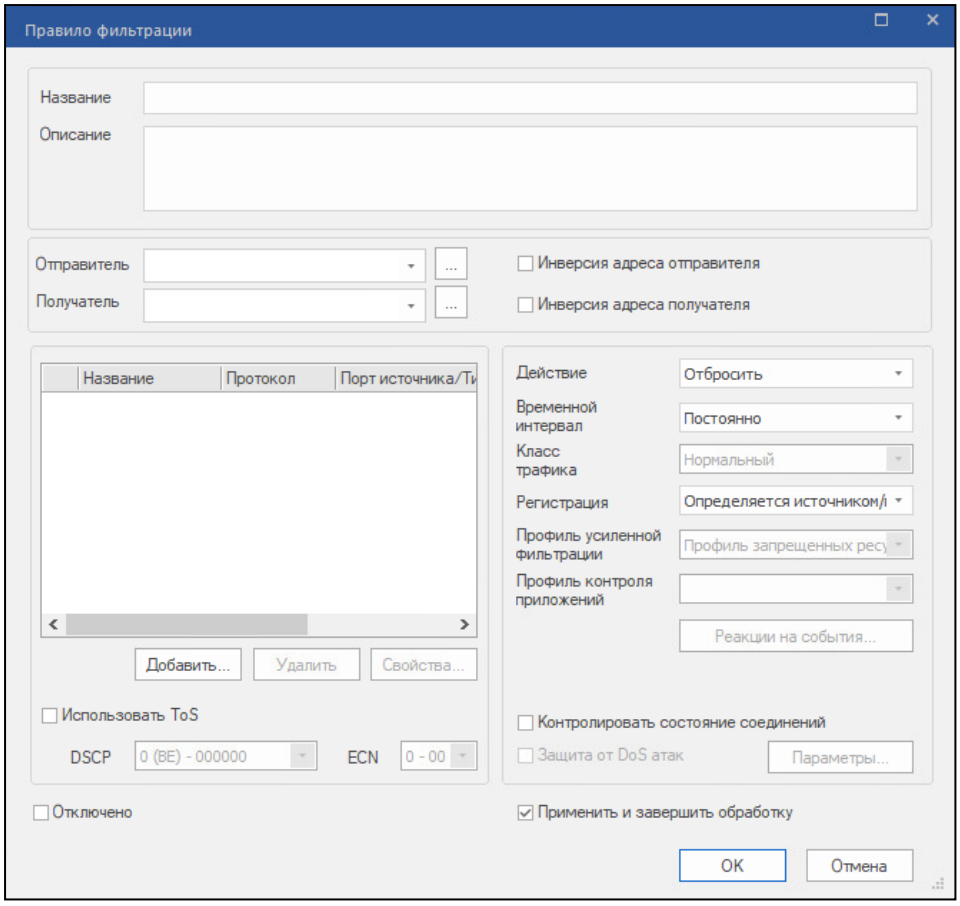
Для создания правила:

Примечание. Перед созданием правила убедитесь, что заданы все необходимые объекты ЦУС (см. стр. 6).

1. Вызовите контекстное меню в требуемом месте списка правил и активируйте команду создания правила.

   Совет. Для добавления правила в конец списка удобно воспользоваться кнопкой "Правило фильтрации" на панели инструментов.

   Откроется окно настройки параметров правила фильтрации.



2. Укажите требуемые значения параметров (см. стр. **19**) и нажмите кнопку "ОК".

Для управления правилами:

Совет. Для выбора нескольких правил используйте левую кнопку мыши и клавишу <Shift> или <Ctrl>.

1. Для редактирования правила вызовите окно его параметров, внесите необходимые изменения (см. стр. **19**) и нажмите кнопку "ОК".

   Для отмены внесенных изменений нажмите кнопку "Откатить" в панели инструментов.
2. Для удаления правила выберите одно или несколько правил в списке, нажмите кнопку "Удалить" на панели инструментов и подтвердите операцию в появившемся окне.
3. Для включения/отключения правила выберите одно или несколько правил в списке, вызовите контекстное меню и выберите пункт "Отключить правила фильтрации".
4. Для изменения местоположения правила в списке выберите его и с помощью кнопок панели инструментов "Выше" () или "Ниже" () осуществите перемещение в требуемое место.
5. Для группировки правил нажмите на панели инструментов кнопку "Группировка", выберите правило, которое будет первым в создаваемой группе, вызовите его контекстное меню, активируйте команду "Добавить разделитель..." и введите название разделителя в появившемся окне.

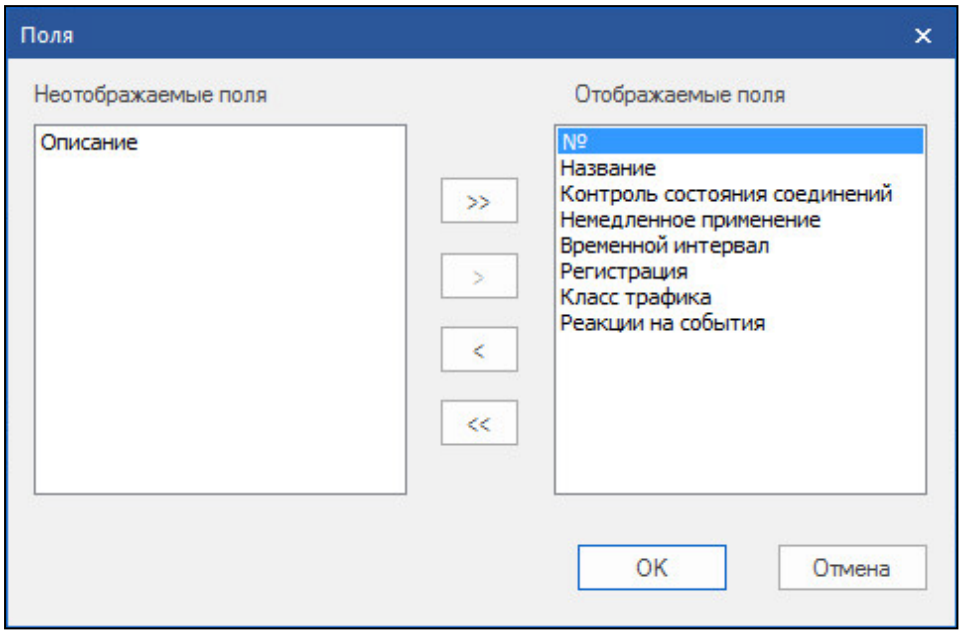
   Разделитель объединяет в группу правила под ним до следующего раздела.

   Список правил раздела можно свернуть, для этого следует нажать кнопку  слева от его названия. Аналогично проводится процедура раскрытия группы правил. На панели инструментов расположены кнопки настройки вида списка правил:

Кнопка	Описание
Свернуть все	Просмотр списка групп правил
Развернуть все	Раскрытие всех групп правил
Список	Просмотр всего списка правил без разделителей
Группировка	Просмотр всего списка правил с разделением на группы

Через контекстное меню разделителя доступны смена его имени и удаление.

6. Для настройки отображаемых параметров в таблице правил фильтрации нажмите кнопку "Поля" на панели инструментов и, используя кнопки перемещения одного или всех полей, сформируйте необходимый список, затем нажмите кнопку "ОК".



7. После выполнения всех необходимых настроек правил фильтрации сохраните изменения в конфигурации ЦУС, нажав соответствующую кнопку на панели инструментов.

Параметры правила фильтрации

Поле	Описание
Название	Наименование правила
Описание	Дополнительные сведения (необязательный параметр)
Отправитель	Имя одного из следующих объектов: • группа пользователей; • сетевой объект; • группа сетевых объектов. Определяет абонентов-отправителей, для которых будет действовать правило
Инверсия адреса отправителя*	При наличии отметки правило будет действовать для всех абонентов-отправителей, кроме указанного
Получатель	Имя одного из следующих объектов: • группа пользователей; • сетевой объект; • группа сетевых объектов. Определяет абонентов-получателей, для которых будет действовать правило
Инверсия адреса получателя*	При наличии отметки правило будет действовать для всех абонентов-получателей, кроме указанного
Сервисы	Перечень сервисов или групп сервисов. Определяет характеристики IP-пакетов, для которых будет действовать правило. Для формирования списка используйте кнопки в нижней части поля
Действие	Действие, применяемое к IP-пакету: • Пропустить — разрешить прохождение пакета. • Отбросить — запретить прохождение пакета. • Усиленная фильтрация — провести дополнительную фильтрацию в соответствии с указанным ниже профилем. • Контроль приложений — дополнительно проконтролировать принадлежность пакета трафику приложений, определенных ниже в соответствующем профиле

Поле	Описание
Временной интервал	Имя временного периода, который будет определять расписание действия правила
Класс трафика	Класс трафика, которому будут принадлежать IP-пакеты с заданными характеристиками. Класс трафика используется для формирования очереди на обработку блоком криптографической защиты, а также очереди на отправку на сетевом интерфейсе
Регистрация	Вид регистрации: • Определяется источником/получателем; • Первые 64 байта — регистрировать в журнале сетевого трафика первые 64 байта пакета; • Тело пакета — регистрировать заголовок и содержание пакета; • Первый пакет в соединении — регистрировать заголовок и содержание первого пакета, открывающего соединение. **Внимание!** Если в поле "Сервисы" указано значение "FTP", в данном поле должно быть указано одно из следующих значений: • Первые 64 байта; • Тело пакета; • Первый пакет в соединении
Профиль усиленной фильтрации	Поле доступно, если в поле "Действие" указано "Усиленная фильтрация". Выбирается из раскрывающегося списка имеющихся профилей усиленной фильтрации
Профиль контроля приложений	Поле доступно, если в поле "Действие" указано "Контроль приложений". Выбирается из раскрывающегося списка имеющихся профилей контроля приложений
Кнопка "Реакция на события…"	Вызывает на экран список зарегистрированных реакций на события. Отметьте нужные и нажмите кнопку "ОК". Кнопка доступна только при выборе в поле "Регистрация" значения "Только первый пакет соединения"
Использовать ToS	Дополнительная фильтрация по метке ToS. Если отметка установлена, пакет будет обработан данным правилом только при наличии в нем указанной метки (коды DSCP и ECN). Коды выбираются из раскрывающихся списков
Отключено	Установка отметки отключает данное правило без удаления его из списка
Контролировать состояние соединения**	Отметку устанавливают для пакетов, открывающих соединение. В этом случае автоматически создаются правила фильтрации, которые разрешают прохождение всех пакетов, относящихся к этому соединению. Автоматически созданные правила сохраняются в таблице состояния соединений и на экране не отображаются. **Внимание!** Если обратный пакет приходит на внешний интерфейс КШ, отличный от интерфейса, с которого был отправлен исходящий пакет, на КШ необходимо создать правило, разрешающее прохождение обратного пакета
Защита от DoS-атак	Включает для данного правила режим защиты от DoS-атак. Для настройки нажмите кнопку "Параметры..." (см. стр. **20**)
Применить и завершить обработку	Установка отметки присваивает данному правилу признак немедленного применения. При отсутствии отметки после совпадения правила пакетный фильтр продолжает обработку списка правил фильтрации

* Для групп сетевых объектов возможна некорректная работа в режиме инверсии адреса. Используйте инверсию адреса только для одиночных сетевых объектов.

** В таблице состояния соединений может быть зафиксировано ограниченное количество одновременно открытых соединений. При превышении этой величины для всех вновь открываемых соединений фиксируется ошибка "Connection Refused". В этом случае используйте правила без контроля состояния соединений.

Настройка режима защиты от DoS-атак

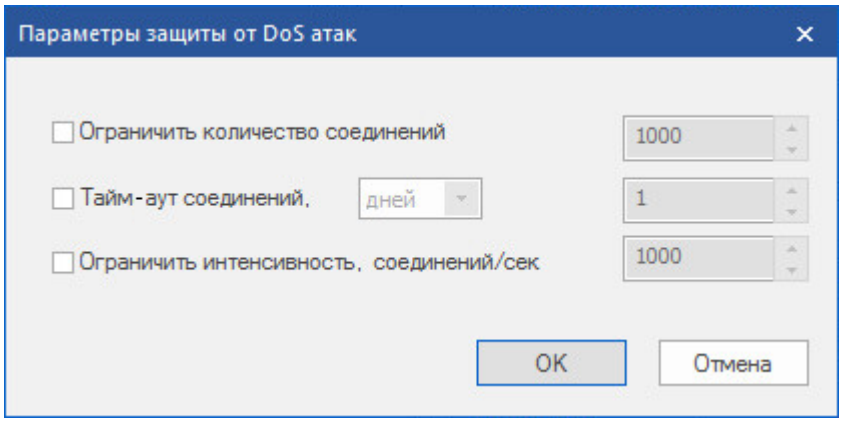
Включение и настройку режима защиты от DoS-атак выполняют в окне редактирования правила фильтрации. При этом осуществляется контроль параметров состояния соединений. Этот режим действует для данного правила при наличии следующих условий:

- поле "Действие" содержит значение "Пропустить";
- установлена отметка в поле "Контролировать состояние соединения".

Для настройки параметров правила фильтрации:

1. В окне редактирования правила фильтрации установите отметку в поле "Защита от DoS-атак" и нажмите кнопку "Параметры...".

   На экране появится диалог "Параметры защиты от DoS-атак".



2. Заполните поля диалога и нажмите кнопку "OK".

Поле	Описание
Ограничить количество соединений	Максимальное количество соединений, которое может быть установлено по указанному правилу фильтрации
Тайм-аут соединений	Время, по истечении которого неактивное соединение будет автоматически разорвано
Ограничить интенсивность соединений/сек.	Количество новых соединений, регистрируемых для данного правила, в секунду

Очистка таблицы состояния соединений

Отметку "Контролировать состояние соединений" в свойствах правила фильтрации устанавливают для пакетов, открывающих соединение. В этом случае автоматически создаются правила фильтрации, которые разрешают прохождение всех пакетов, относящихся к этому соединению. Автоматически созданные правила сохраняются в таблице состояния соединений и в списке правил фильтрации не отображаются. Таблица состояния соединений формируется на каждом КШ.

Принудительная очистка таблицы состояния соединений требуется в следующих случаях:

- редактирование правила фильтрации с контролем состояния соединения;
- изменение объектов, используемых в правиле фильтрации с контролем состояния:
  - изменение привязки сетевого объекта, используемого как индивидуально, так и в составе группы;
  - изменение состава группы сетевых объектов;
  - изменение свойств временного интервала;
- изменение списка правил фильтрации:
  - удаление правила фильтрации с контролем состояния соединения;
  - добавление или перемещение отменяющего правила ниже по списку;
  - добавление или перемещение отменяющего правила с признаком немедленного действия выше по списку;
  - перемещение правила с контролем состояния относительно отменяющего правила;
- изменение значения параметра "Автоматический исходящий NAT" в настройках Multi-WAN (режим "Обеспечение отказоустойчивости канала связи").

  Внимание! Изменение значения параметра "Автоматический исходящий NAT" на введенных в эксплуатацию КШ запрещено регулятором.

Для очистки таблицы:

1. Вызовите контекстное меню требуемого КШ и активируйте команду "Очистить таблицу состояний соединений".

Примечание. Возможен множественный выбор КШ.

На экране появится запрос на подтверждение очистки таблицы.

2. Нажмите кнопку "Да".

Контроль приложений

МЭ при фильтрации обеспечивает двухступенчатую обработку трафика. После проверки IP-адресов, портов и типа сервиса (5-tuple) трафик можно дополнительно проанализировать и обработать на уровне прикладных протоколов, в формате контроля трафика определенного приложения (см. ниже) или усиленной фильтрации (см. стр. **24**).

Для контроля трафика приложений необходимо:

1. Создать необходимые профили контроля приложений (см. ниже).
2. Включить профиль в правило фильтрации (см. стр. **24**).

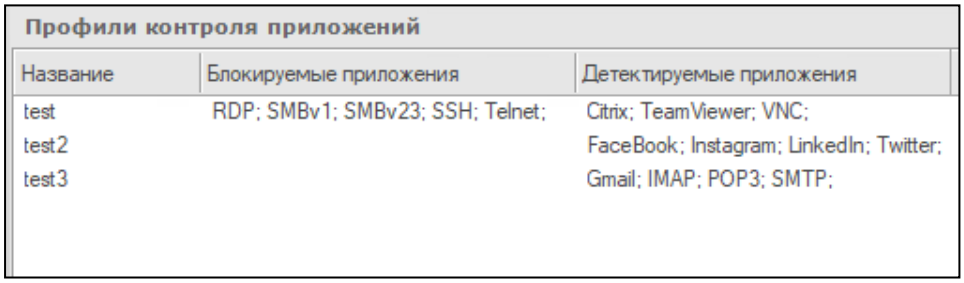
   Внимание! Инспекция приложений не может быть задана в правиле фильтрации одновременно с усиленной фильтрацией прикладных протоколов.

Профили контроля приложений

Для просмотра списка профилей:

- В главном окне ПУ ЦУС в области объектов управления раскройте раздел "Центр управления сетью" и выберите пункт "Профили контроля приложений".

  В правой части главного окна отобразится список профилей контроля приложений.

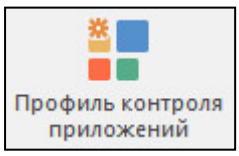


Для создания нового профиля:

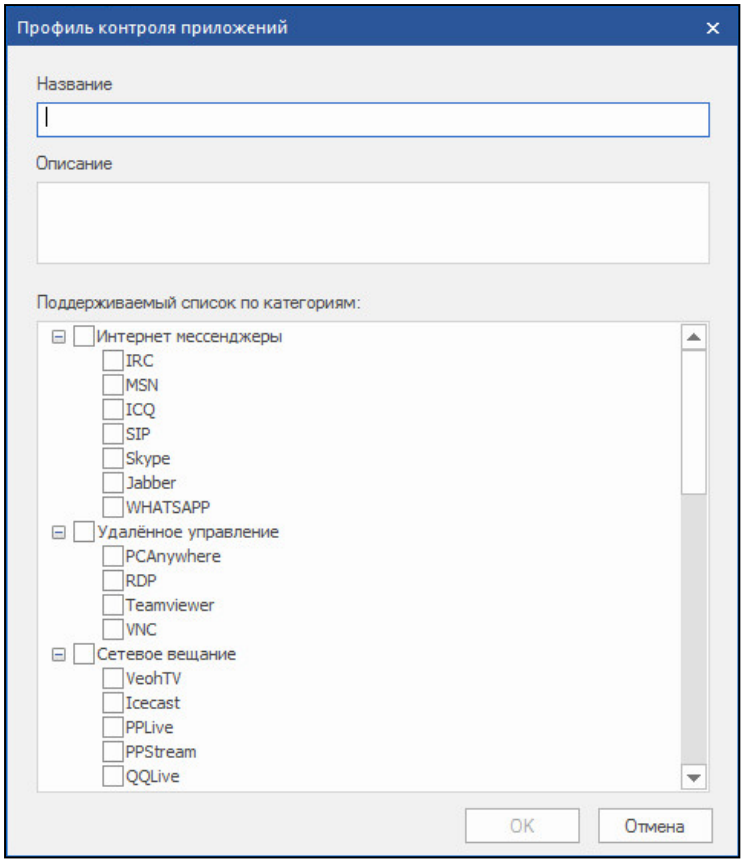
1. В главном окне ПУ ЦУС в области объектов управления раскройте раздел "Центр управления сетью" и выберите пункт "Профили контроля приложений".

   В правой части главного окна отобразится список имеющихся профилей. Предустановленных профилей нет.

2. Нажмите на панели инструментов кнопку "Профиль контроля приложений".



На экране появится окно настроек профиля.



3. Заполните поля названия профиля и, при необходимости, расширенного описания.
4. Поставьте отметки в полях приложений, трафик которых требуется контролировать. При этом вид отметки обозначает действие.

Отметка	Действие
☐	Не обрабатывать (трафик пропускается без регистрации в журнале)
⚠	Детектирование (трафик пропускается с регистрацией в журнале НСД криптошлюза)
✖	Блокировка (трафик блокируется с регистрацией в журнале НСД криптошлюза)

Совет. Для выбора одного типа действия для трафика всех приложений категории достаточно установить отметку в поле этой категории.

5. Нажмите кнопку "ОК".

   Окно "Профиль контроля приложений" закроется и в списке на экране появится новый профиль.

Для управления профилями:

1. Для просмотра списка профилей выберите в области объектов управления раздел "Профили контроля приложений".

   В правой части главного окна отобразится список имеющихся профилей.
2. Для просмотра и редактирования параметров профиля выберите его в списке и на панели инструментов нажмите кнопку "Свойства". После внесения изменений нажмите кнопку "ОК".
3. Для удаления профиля выберите его в списке и на панели инструментов нажмите кнопку "Удалить", затем нажмите кнопку "Да" в появившемся запросе на подтверждение удаления профиля.

Включение профиля в правило фильтрации

Для включения профиля контроля приложений в правило фильтрации:

1. Выберите подходящее правило фильтрации или создайте новое (работа с правилами фильтрации описывается на стр. **17**).
2. Вызовите окно редактирования параметров правила фильтрации и выберите для параметра "Действие" значение "Контроль приложений" из раскрывающегося списка.
3. В параметре "Профиль контроля приложений" выберите требуемый профиль.
4. Нажмите кнопку "OK" в нижней части диалога.

   Диалог настройки параметров правила фильтрации закроется.

Усиленная фильтрация

Средствами межсетевого экрана, входящего в состав комплекса, предусмотрена дополнительная фильтрация, которая позволяет анализировать и обрабатывать сетевой трафик на уровне некоторых прикладных протоколов (далее — усиленная фильтрация). Такими протоколами являются:

- HTTP;
- HTTPS;
- FTP.

В механизме усиленной фильтрации используются настраиваемые профили. Каждый профиль включает в себя один или несколько наборов фильтров (агентов) и описание действия, которое должно быть выполнено с пакетом, удовлетворяющим одновременно всем условиям, заданным в фильтрах.

В каждом наборе фильтров (агенте) задаются атрибуты, по которым должна выполняться фильтрация трафика:

Атрибут	Описание
Адрес	IP-адрес (IP-адреса) или DNS-имя получателя
Команды/методы	Фильтрация сетевого трафика осуществляется по FTP-командам и HTTP-методам
Контент	Фильтрация осуществляется по MIME-типам передаваемых данных. Используется стандартный список MIME-заголовков и расширений файлов. Для варианта FTP не используется
Маршруты	Фильтрация сетевого трафика осуществляется по маршрутам, описанным с помощью регулярных выражений POSIX. В описаниях маршрутов допускается использование латинских символов и символов кириллицы

Примечание. При заполнении атрибута "Адрес" следует учитывать:

- Для указания DNS-имени следует использовать латинские символы или символы кириллицы. Допускается использование символа "*" для обозначения любого домена соответствующего уровня.
- Для указания в качестве получателя любого IP-адреса необходимо ввести ".*" (без кавычек). Для протокола HTTPS для этой цели рекомендуется ввести "./ " (либо разрешать метод "CONNECT" в запрещающем профиле усиленной фильтрации).

Действия, которые могут быть выполнены с пакетом при срабатывании фильтра:

- блокирование — уничтожение сетевых пакетов сессии данного соединения с регистрацией отброшенных пакетов в журнале сетевого трафика;
- разрешение — отсутствие каких-либо действий над сетевыми пакетами и отправка их адресату без изменений;
- перенаправление — перенаправление клиента на заранее заданный адрес.

Для запуска режима усиленной фильтрации необходимо:

1. Выполнить предварительные настройки (см. ниже).
2. Создать профиль для требуемого протокола (см. стр. **28**).
3. Создать необходимые наборы фильтров (агенты) и включить их в профиль (см. стр. **30**).
4. Создать правило фильтрации и включить в него профиль (см. стр. **32**).
5. Задать список исключений — веб-ресурсов, при обращении к которым механизм усиленной фильтрации не должен срабатывать (см. стр. **32**).

Предварительные настройки

Настройки включают в себя:

1. Указание адреса DNS-сервера для работы с URL. Данную настройку выполняют для всех зарегистрированных КШ комплекса.
2. Создание корневого сертификата Удостоверяющего центра для усиленной фильтрации по HTTPS. Сертификат издают средствами ПУ ЦУС.

   Внимание! Для корректной работы https-соединений корневой сертификат Удостоверяющего центра должен быть установлен на всех компьютерах защищаемых сетей комплекса. Для этого после создания корневого сертификата необходимо выполнить процедуру экспорта сертификата в файл (см. стр. **27**) и далее передать файл для установки сертификата на компьютеры.

> **Примечание.** За 14 и 7 дней до истечения срока действия сертификата в ПУ ЦУС появляется соответствующее сообщение с указанием даты истечения срока действия.

Для указания адреса DNS-сервера:

1. В ПУ ЦУС выберите в списке КШ, вызовите контекстное меню и выберите пункт "Свойства...".

   На экране появится окно "Свойства криптошлюза".
2. Перейдите на вкладку "DNS", нажмите кнопку "Добавить", введите адрес DNS-сервера и нажмите кнопку "ОК".

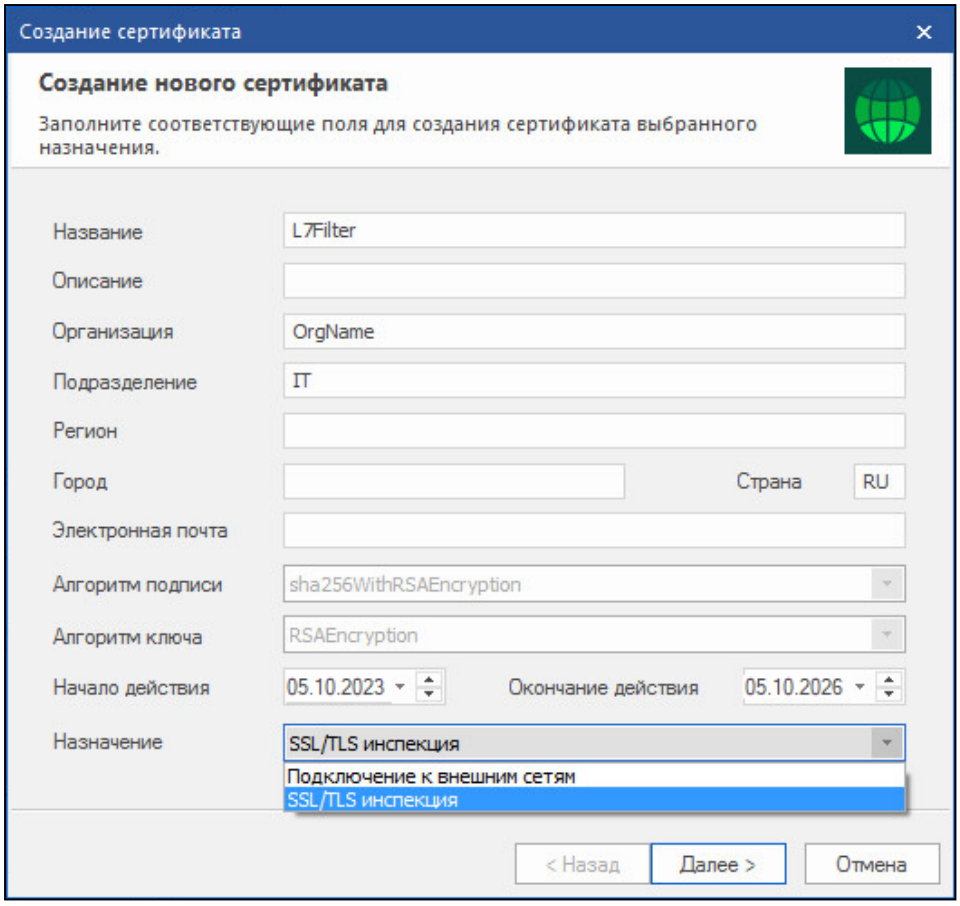
Для создания корневого сертификата:

1. В главном окне ПУ ЦУС в области объектов управления раскройте раздел "Центр управления сетью" и выберите пункт "Сертификаты".

   В правой части главного окна отобразится список зарегистрированных в ЦУС сертификатов.
2. На панели инструментов нажмите кнопку "Сертификат".

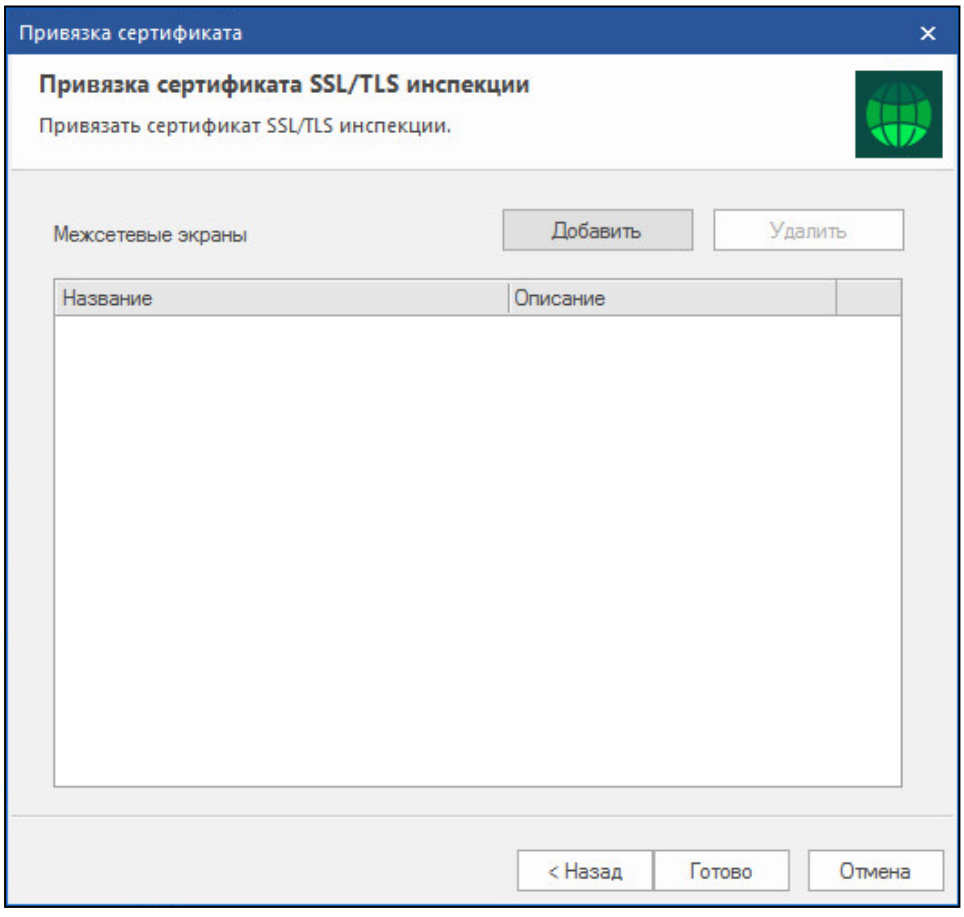
   

   На экране появится окно "Создание сертификата".
3. Заполните поля параметров сертификата. В поле "Назначение" укажите "SSL/TLS инспекция", выбрав это значение из раскрывающегося списка.



Нажмите кнопку "Далее".

На экране появится окно "Привязка сертификата".



4. Нажмите кнопку "Добавить".

   На экране появится список зарегистрированных криптошлюзов.

5. Выберите КШ, на котором должна действовать усиленная фильтрация по HTTPS, и нажмите кнопку "ОК".

   В окне "Привязка сертификата" появится строка, отображающая привязку создаваемого сертификата к криптошлюзу.

6. Выполните пп. **4**, **5** для всех КШ, на которых должна действовать усиленная фильтрация по HTTPS.

   Для удаления привязки сертификата к КШ выберите соответствующую строку в окне "Привязка сертификата" и нажмите кнопку "Удалить".

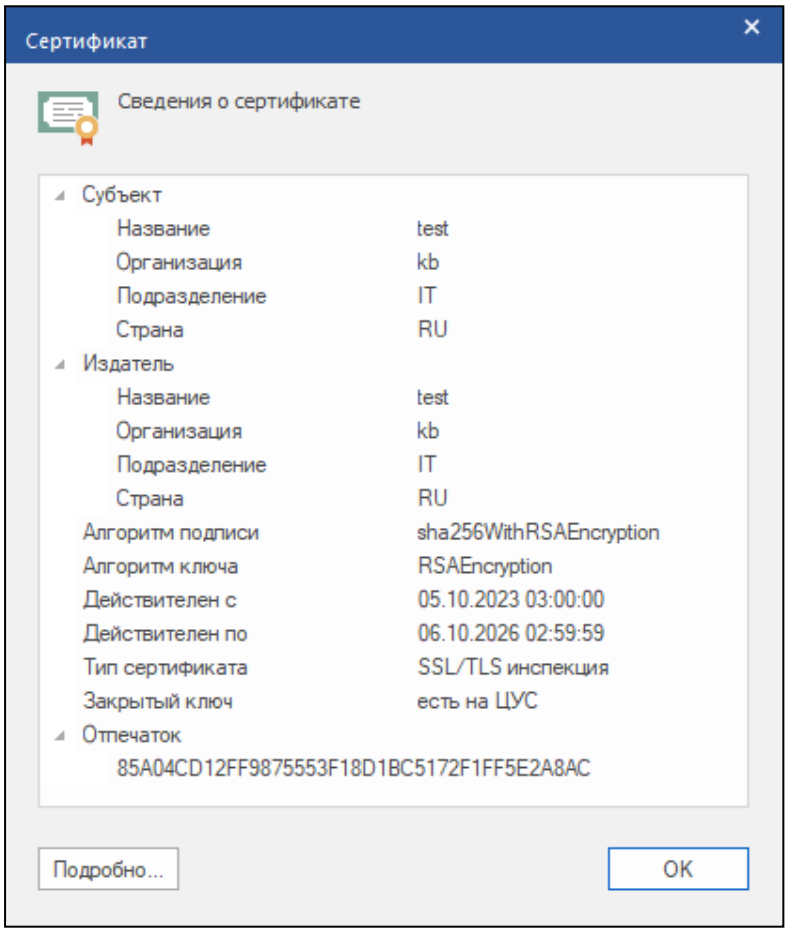
7. После привязки сертификата ко всем необходимым КШ нажмите кнопку "Готово".

   Диалог "Привязка сертификата" закроется и в списке сертификатов появится вновь созданный сертификат.

Для экспорта корневого сертификата в файл:

1. Выберите сертификат в списке, вызовите контекстное меню и выберите пункт "Свойства...".

   На экране появится окно "Сертификат".



2. Нажмите кнопку "Подробно...".

   На экране появится окно с подробными сведениями о сертификате.

3. Перейдите на вкладку "Состав" и нажмите кнопку "Копировать в файл...".

   На экране появится окно мастера экспорта сертификата.

4. Нажмите кнопку "Далее", выберите формат экспорта сертификата и нажмите кнопку "Далее".

   На экране появится стандартный диалог ОС Windows сохранения файла.

5. Укажите имя сохраняемого файла и путь и нажмите кнопку "Далее".

   На экране появится завершающий диалог мастера экспорта.

6. Нажмите кнопку "Готово".

   Диалог мастера закроется и сертификат будет сохранен в файл.

Профили усиленной фильтрации

Для просмотра списка профилей:

1. В главном окне ПУ ЦУС в области объектов управления раскройте раздел "Центр управления сетью" и выберите пункт "Профили усиленной фильтрации".

   В правой части главного окна отобразится список профилей усиленной фильтрации.

   Список содержит созданные администратором профили и два профиля, заданных по умолчанию: "Профиль запрещенных ресурсов" и "Системный".

   "Профиль запрещенных ресурсов" не подлежит редактированию и удалению и используется в правилах фильтрации для запрета доступа к ресурсам единого реестра Роскомнадзора (см. стр. **39**).

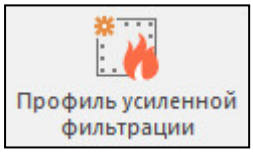
   Профиль "Системный" является служебным и в правилах фильтрации не используется. Он предназначен для хранения наборов фильтров (агентов), входивших в удаленные профили. Предусмотрено удаление агентов из данного профиля. Сам профиль "Системный" удалению не подлежит.

2. Для просмотра состава профиля раскройте в области объектов управления раздел "Профили усиленной фильтрации" и выберите требуемый профиль в списке.

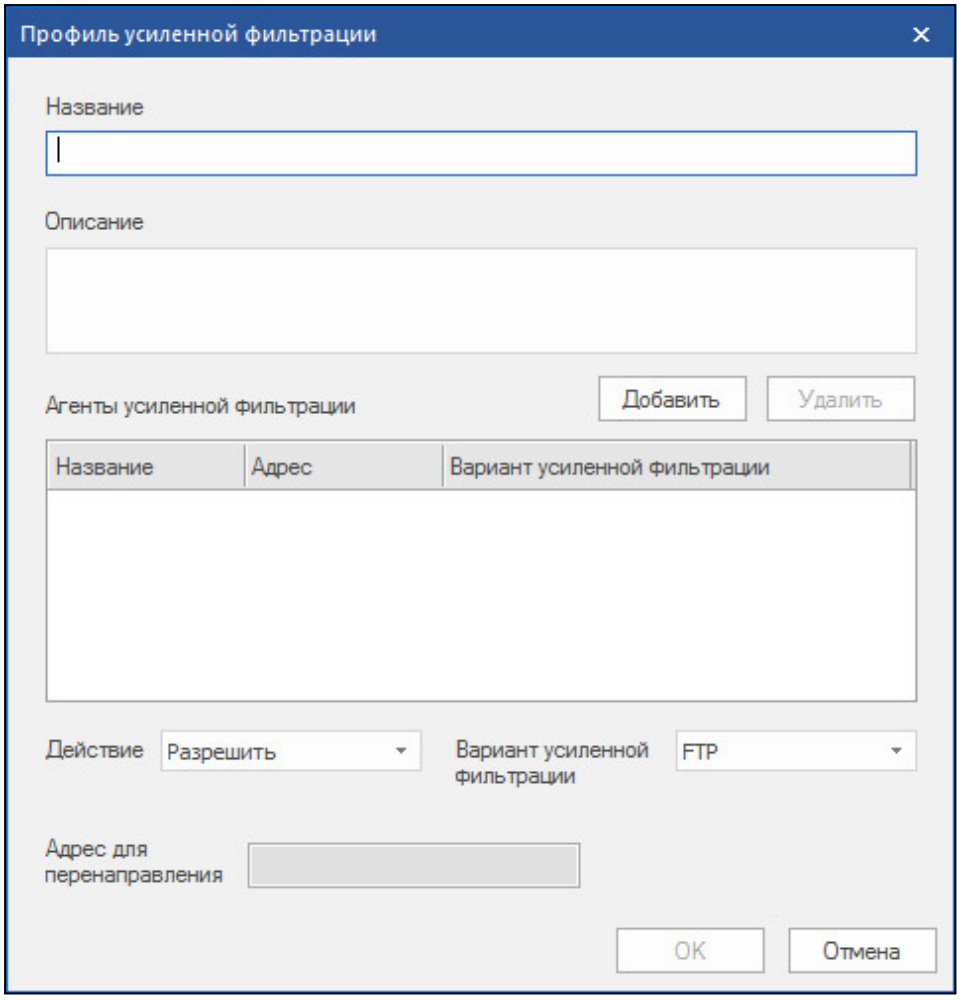
   В правой части окна отобразится список наборов фильтров (агентов), включенных в состав профиля. Для нового профиля список агентов будет пуст.

Для создания нового профиля:

1. В области объектов управления выберите пункт "Профили усиленной фильтрации" и на панели инструментов нажмите кнопку "Профиль усиленной фильтрации" .

   На экране появится окно настроек профиля.



2. Заполните поля настроек необходимой информацией.

Поле	Описание
Название	Название создаваемого профиля
Описание	Краткое описание профиля
Агенты усиленной фильтрации	Список агентов, включаемых в создаваемый профиль. Для добавления агента в список нажмите кнопку "Добавить" и выберите его из раскрывающегося списка. Если агенты не создавались, данное поле можно заполнить после создания требуемых агентов
Действие	Действие, которое должно быть выполнено при срабатывании фильтра. Для всех протоколов доступны следующие значения: • разрешить; • запретить. Для протоколов HTTP и HTTPS доступно также: • перенаправить. **Внимание!** Перенаправление с HTTP-сайтов на HTTPS-сайты и наоборот не работает
Вариант усиленной фильтрации	Используемый прикладной протокол: • HTTP; • HTTPS; • FTP
Адрес для перенаправления	Заполняется, если в поле "Действие" указано "Перенаправить". Для http-соединения достаточно ввести доменное имя. Для https-соединения адрес необходимо ввести в формате https://<доменное имя>. **Внимание!** Не допускается указывать адрес в формате https:\\<доменное имя>

3. Нажмите кнопку "OK".

Окно "Профиль усиленной фильтрации" закроется и в списке на экране появится новый профиль.

Для удаления профиля:

1. Выберите профиль в списке и на панели инструментов нажмите кнопку "Удалить".

   На экране появится запрос на подтверждение удаления профиля.

2. Выберите "Да".

   Профиль будет удален.

   Внимание! Агенты, входящие в удаляемый профиль, будут помещены в профиль "Системный". Если удаляемый профиль включен в одно или несколько правил фильтрации, на экране появится предупреждение о необходимости предварительно исключить его из правила (правил).

Для редактирования профиля:

1. Выберите профиль в списке и на панели инструментов нажмите кнопку "Свойства".

   На экране появится диалог "Профиль усиленной фильтрации".

2. Внесите необходимые изменения и нажмите кнопку "ОК".

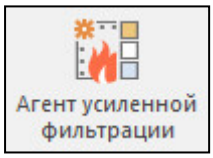
Агенты усиленной фильтрации

Для создания агента:

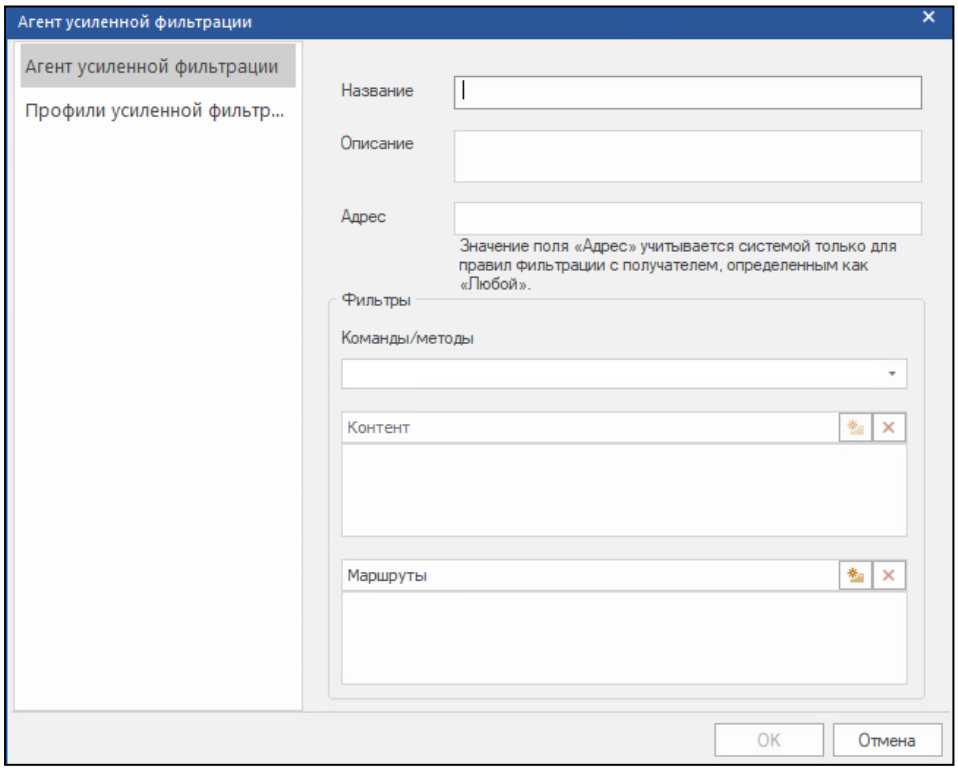
1. В области объектов управления выберите раздел "Центр управления сетью | Профили усиленной фильтрации" и выберите в нем профиль, для которого должен быть создан агент.

   В правой части главного окна отобразится список агентов усиленной фильтрации, входящих в данный профиль.

2. На панели инструментов нажмите кнопку "Агент усиленной фильтрации".



   На экране появится окно настроек агента.



3. Заполните поля на вкладке "Агент усиленной фильтрации" (см. стр. **24**).

   Обязательным для заполнения является поле "Название". Остальные поля можно заполнить позже.

4. Если необходимо добавить данный агент в другие профили, перейдите на вкладку "Профили усиленной фильтрации".

   На вкладке отображается список профилей, в которые входит данный агент.

   Внимание! Добавить агент можно только в профили усиленной фильтрации для одного прикладного протокола (HTTP, HTTPS или FTP).

5. Для включения агента в другой профиль нажмите кнопку "Добавить".

   На экране появится список профилей усиленной фильтрации соответствующего варианта (HTTP, HTTPS, FTP).

6. Выберите профиль и нажмите кнопку "OK".

   Выбранный профиль появится в списке на вкладке "Профили усиленной фильтрации".

   Примечание. Для удаления профиля выберите его в списке и нажмите кнопку "Удалить".

7. Для завершения процедуры создания агента нажмите кнопку "OK" в нижней части окна.

   В результате выполнения процедуры в списке агентов появится соответствующая строка.

Для изменения настроек агента:

1. В области объектов управления выберите раздел "Центр управления сетью | Профили усиленной фильтрации" и выберите в нем профиль, в котором используется агент.

   В правой части главного окна отобразится список агентов усиленной фильтрации, входящих в данный профиль.

2. Выберите агент для изменения настроек и на панели инструментов нажмите кнопку "Свойства".

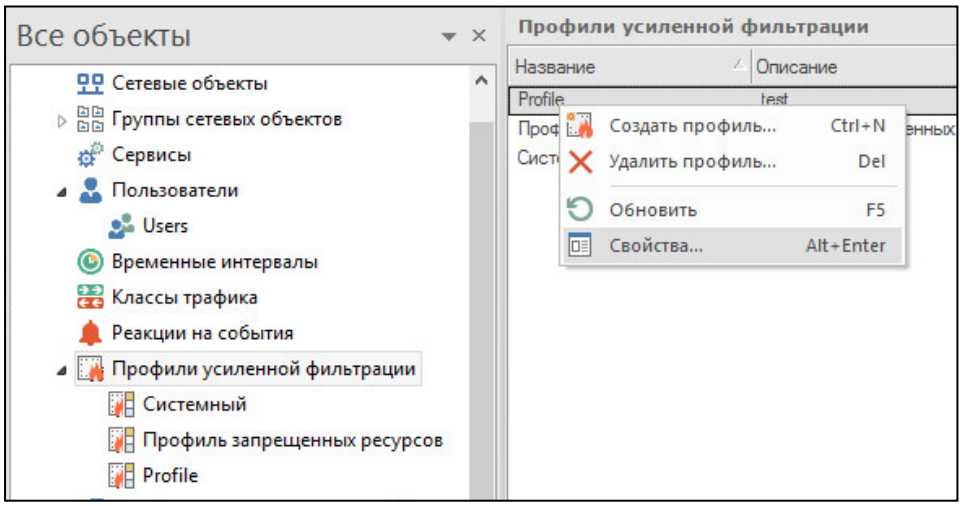
   На экране появится окно настроек агента.

3. Внесите необходимые изменения и нажмите кнопку "OK".

   Окно настроек агента закроется.

Для удаления агента из профиля:

1. В области объектов управления выберите раздел "Профили усиленной фильтрации", вызовите в области отображения информации контекстное меню профиля, из которого необходимо удалить агент, и выберите в нем пункт "Свойства...".



   На экране появится окно настроек профиля.

2. Выберите в списке агентов требуемый и нажмите кнопку "Удалить".

   Агент будет удален из профиля.

Для удаления агента из системы:

1. В разделе "Профили усиленной фильтрации" области объектов управления выберите любой профиль, в котором находится агент, затем выберите агент из списка в области отображения информации.

2. Нажмите в панели инструментов кнопку "Удалить".

   На экране появится запрос на подтверждение выполнения операции.

3. Нажмите кнопку "Да" в окне запроса.

   Агент будет удален из системы.

Включение профиля в правило фильтрации

Для включения профиля усиленной фильтрации в правило:

1. Выберите подходящее правило фильтрации или создайте новое (работа с правилами фильтрации описана на стр. **17**).
2. Вызовите окно редактирования параметров правила фильтрации и выберите для параметра "Действие" значение "Усиленная фильтрация" из раскрывающегося списка.
3. В параметре "Профиль усиленной фильтрации" выберите профиль.
4. При указании в правиле фильтрации определенного сервиса проверьте соответствие его порта назначения и используемого протокола усиленной фильтрации.

Протокол фильтрации	Порт назначения сервиса
HTTP	80
HTTPS	443
FTP	21

5. Нажмите кнопку "ОК" в нижней части диалога.

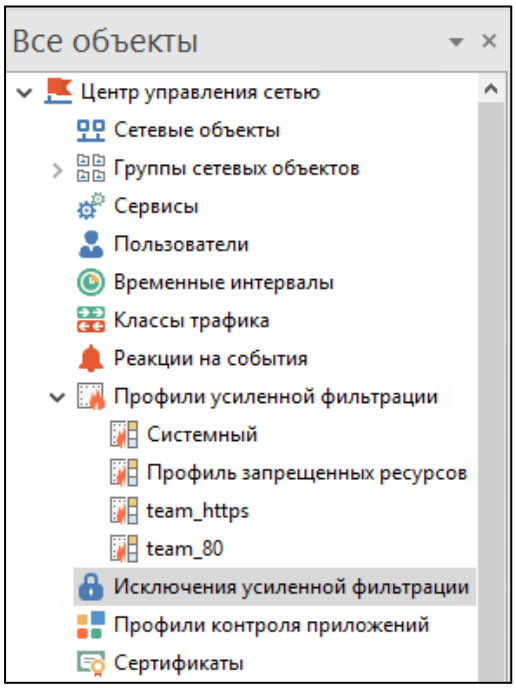
   Диалог настройки параметров правила фильтрации закроется.

Исключения усиленной фильтрации

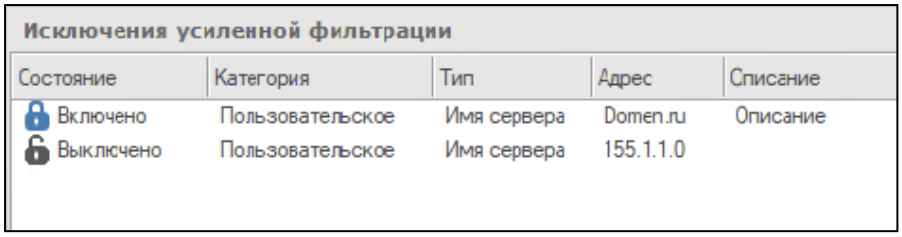
В процессе эксплуатации комплекса администратор может добавлять новые исключения. При создании нового исключения ему присваивается категория "Пользовательское". Пользовательские исключения можно редактировать и удалять.

Для просмотра списка исключений:

- В главном окне ПУ ЦУС в области объектов управления раскройте раздел "Центр управления сетью" и выберите пункт "Исключения усиленной фильтрации".



   В правой части главного окна отобразится список исключений усиленной фильтрации. Если исключения не создавались, список будет пустым.



Каждое исключение описывается следующими параметрами:

- Состояние — Включено/Выключено;
- Категория — Вендорское/Пользовательское;
- Тип — способ задания адреса ресурса (имя сервера или IP-адрес);
- Адрес — адрес (имя) сервера;
- Описание — комментарий к исключению.

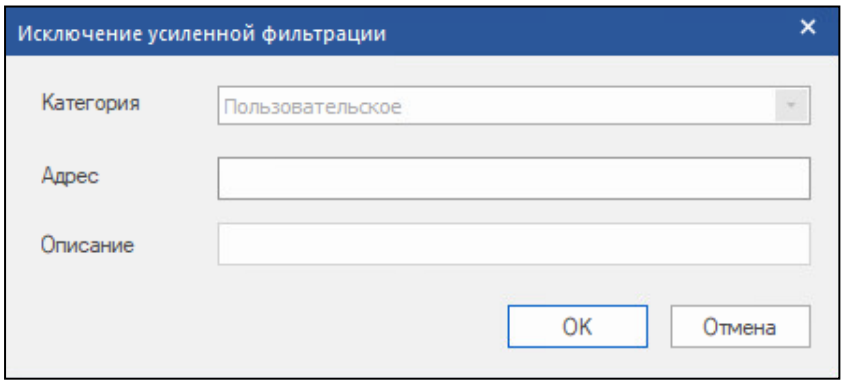
При просмотре списка исключений доступны следующие операции:

- обновление списка исключений с использованием кнопки в панели инструментов;
- сортировка списка исключений по любому параметру;
- поиск исключений в списке по значению любого параметра;
- фильтрация списка исключений;
- добавление нового исключения;
- редактирование выбранного исключения;
- копирование выбранного исключения;
- удаление выбранного исключения;
- изменение состояния выбранного исключения.

Для добавления исключения:

1. Откройте список исключений и на панели инструментов нажмите кнопку "Исключение усиленной фильтрации" или используйте соответствующую команду контекстного меню.

   На экране появится окно создания нового исключения.



   Создаваемому исключению присваивается категория "Пользовательское".

2. Введите адрес (имя) сервера и краткое описание исключения.

   Внимание! Адрес исключения не должен пересекаться с уже существующими исключениями.

3. Нажмите кнопку "OK".

   Новое исключение будет добавлено в конец списка исключений.

Для сортировки списка исключений по параметру:

1. Наведите курсор на заголовок столбца (название параметра) и нажмите левую кнопку мыши.

   Справа от названия параметра появится значок .

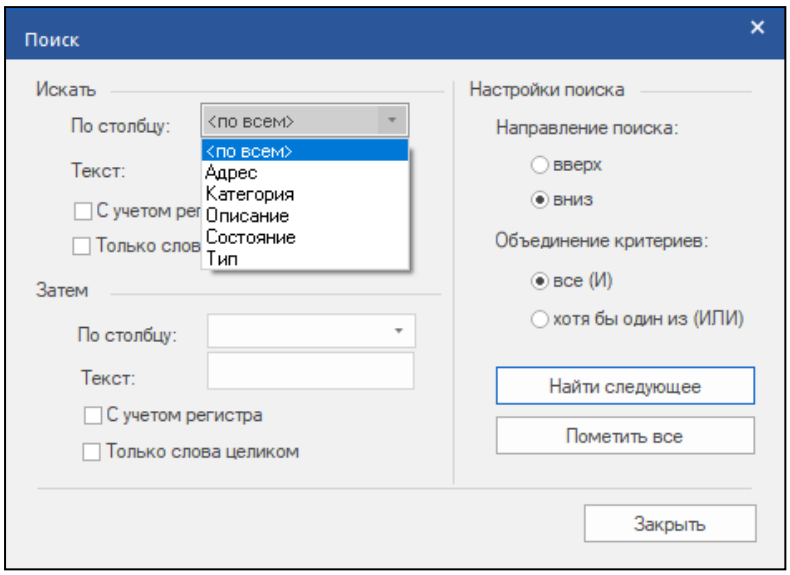
2. Нажмите на значок.

   Список будет отсортирован по данному параметру.

Для поиска исключения по значению параметра:

1. Нажмите в панели инструментов кнопку "Найти".

   Появится окно настройки параметров поиска.



2. Настройте параметры поиска. Поиск может осуществляться как по всем, так и по отдельному параметру.
3. Нажмите кнопку "Найти следующее".

Для фильтрации отображаемого списка исключений:

1. Нажмите в панели инструментов кнопку "Фильтр".

   Появится окно настройки фильтра.
2. Задайте параметры фильтра и нажмите кнопку "ОК".

   В списке отобразятся исключения, удовлетворяющие настройке фильтра.

Для редактирования исключения:

1. Выберите в списке исключение и на панели инструментов нажмите кнопку "Свойства".

   На экране появится окно с параметрами выбранного исключения.
2. Укажите новые значения параметров и нажмите кнопку "ОК".

   В общем списке исключение отобразится с новыми параметрами.

Для копирования исключения:

1. Выберите в списке исключение и на панели инструментов нажмите кнопку "Копировать" или используйте соответствующую команду контекстного меню.

   На экране появится окно с параметрами выбранного исключения.
2. Укажите новые значения параметров и нажмите кнопку "ОК".

   В общем списке исключение отобразится с новыми параметрами.

Для удаления исключения:

1. Выберите в списке исключение и на панели инструментов нажмите кнопку "Удалить" или используйте соответствующую команду контекстного меню.

   На экране появится окно подтверждения операции удаления.
2. Нажмите кнопку "Да".

   Исключение будет удалено из списка.

Для изменения состояния исключения:

- Выберите в списке исключение и на панели инструментов нажмите кнопку "Включено" или "Выключено".

  Исключение будет переведено в соответствующее состояние.

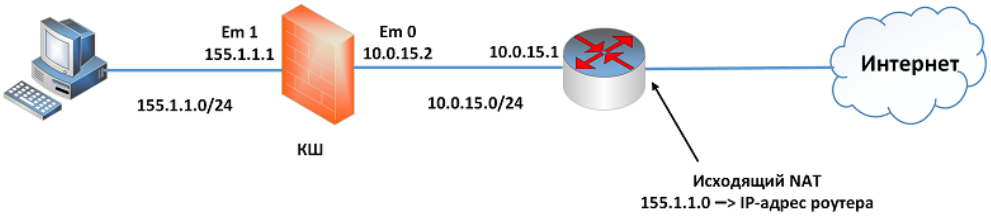
Примеры применения усиленной фильтрации

В данном подразделе приведены примеры применения правил усиленной фильтрации.

Разрешающие правила усиленной фильтрации

Ниже приведен пример применения правил усиленной фильтрации для разрешения работы в защищаемой сети с приложением TeamViewer.

На рисунке ниже показан хост, расположенный в сети 155.1.1.0/24. Сеть защищена криптошлюзом КШ, который выполняет функции межсетевого экрана.



Выход в сеть интернет осуществляется через роутер.

Интерфейсы криптошлюза:

- внешний — Em 0, IP-адрес 10.0.15.2;
- внутренний — Em 1, IP-адрес 155.1.1.1.

Требуется обеспечить работу пользователя хоста с приложением TeamViewer. Для этого необходимо на КШ задать правила усиленной фильтрации, разрешающие прохождение пакетов http и https, и правило, разрешающее доступ к DNS-серверу.

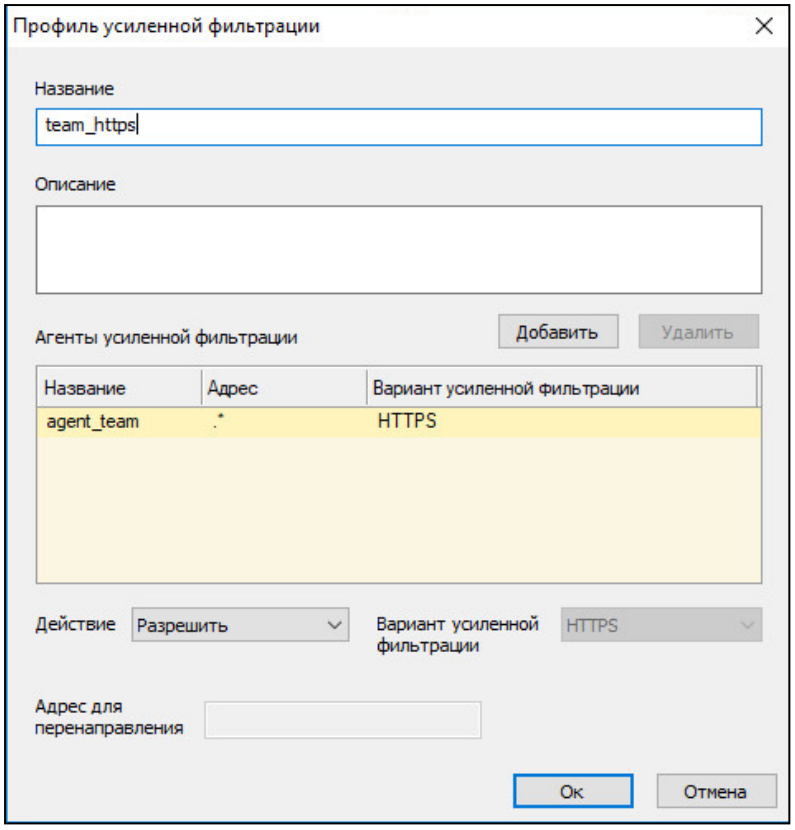
Перед началом фомирования правил фильтрации необходимо выполнить следующие настройки:

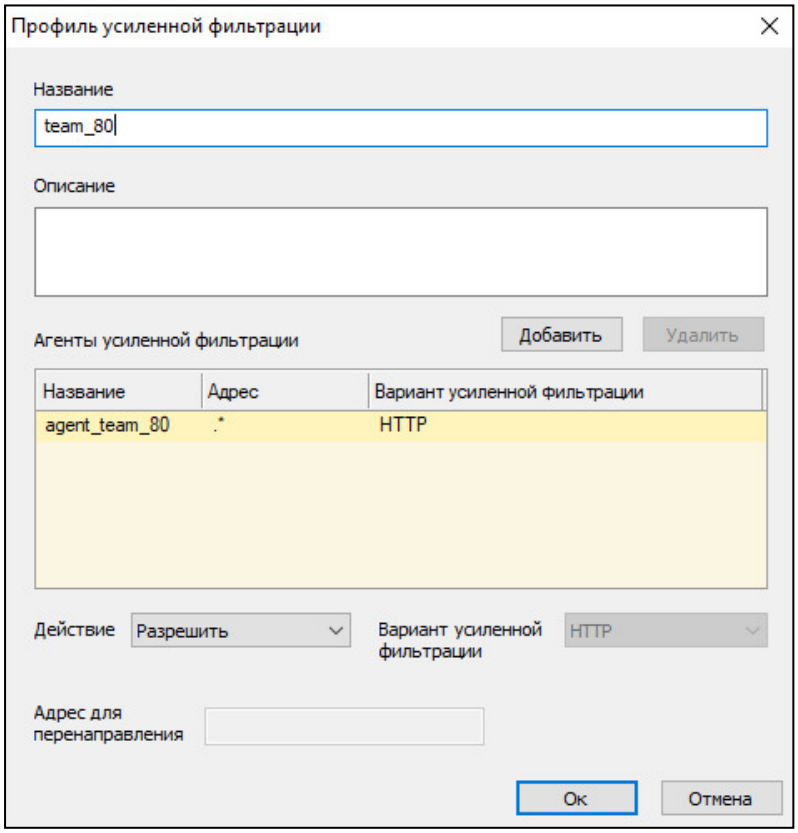
- На хосте, с которого будет осуществляться доступ в интернет, задать шлюз по умолчанию — 155.1.1.1 (внутренний интерфейс криптошлюза Em 1) и IP-адрес DNS-сервера.
- На криптошлюзе задать маршрут по умолчанию, в котором в качестве следующего узла указать IP-адрес роутера 10.0.15.1 (см. рисунок выше), и указать IP-адрес DNS-сервера.
- Создать сертификат SSL/TLS-инспекции и установить его на хост, с которого будет осуществляться доступ в интернет.

Для формирования правил фильтрации:

1. Создайте два профиля усиленной фильтрации, разрешающие https и http, с названиями team_https и team_80 соответственно. При создании профилей не включайте в них агенты.
2. Создайте два агента усиленной фильтрации с названиями agent_team и agent_team_80. При создании агентов поля "Адрес" и "Команды/методы" оставьте пустыми (фильтрация будет проводиться по всем доступным HTTP-методам).
3. Включите agent_team в профиль team_https, а agent_team_80 — в профиль team_80.

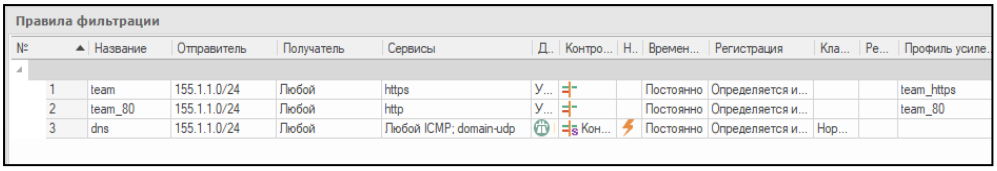
   В профиле team_https укажите вариант усиленной фильтрации — HTTPS, а в профиле team_80 — HTTP (см. рисунки ниже).





4. Составьте два разрешающих правила усиленной фильтрации для HTTPS и HTTP, используя созданные профили усиленной фильтрации (см. рисунок ниже).

В правилах удалите отметку в поле "Применить и завершить обработку".



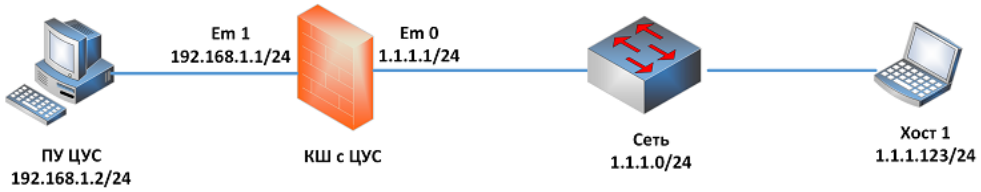
5. Составьте правило фильтрации для доступа к DNS-серверу (см. рисунок выше).

   Установите отметку в поле "Применить и завершить обработку".
6. Сохраните изменения.
7. Запустите на хосте приложение TeamViewer и проверьте его работоспособность.

Можно также использовать другой вариант описанных выше правил фильтрации — во всех трех правилах установить отметку в поле "Применить и завершить обработку".

Проверка работы правил усиленной фильтрации

Ниже на рисунке показаны компьютер с установленной ПУ ЦУС, криптошлюз с ЦУС и виртуальная машина Хост 1 с операционной системой Windows, расположенная в сети 1.1.1.0/24.



На КШ с ЦУС настроены интерфейсы:

- внешний — Em 0, IP-адрес 1.1.1.1/24;
- внутренний — Em 1, IP-адрес 192.168.1.1/24.

На компьютере с ПУ ЦУС настроены работа агента ЦУС и СД и программа просмотра журналов.

На виртуальной машине Хост 1 задан шлюз по умолчанию 1.1.1.1 и настроен http-сервер.

Требуется проверить работу правил усиленной фильтрации.

Для проверки необходимо выполнить следующие настройки:

1. Создать сетевой объект.
2. Создать профиль усиленной фильтрации.
3. Создать агент усиленной фильтрации и включить его в профиль.
4. Создать правило усиленной фильтрации.
5. Создать сертификат и установить его на компьютере с ПУ ЦУС.

Для создания сетевого объекта:

- В ПУ ЦУС создайте сетевой объект со следующими настройками:

Параметр	Значение
Название	Сеть ПУ ЦУС
IP-адрес/Маска	192.168.1.0/255.255.255.0
Тип привязки	Внутренний
Криптошлюз	КШ с ЦУС
Интерфейс	Em 1

Для создания профиля усиленной фильтрации:

- В ПУ ЦУС создайте профиль усиленной фильтрации со следующими настройками:

Параметр	Значение
Название	Profile_http
Действие	Разрешить
Вариант усиленной фильтрации	HTTP

Для создания агента усиленной фильтрации:

- В ПУ ЦУС в разделе "Профили усиленной фильтрации" выберите созданный профиль Profile_http и нажмите кнопку "Создать агент усиленной фильтрации".

  Создайте агент усиленной фильтрации со следующими параметрами:

Параметр	Значение
Название	Agent_http
Адрес	1.1.1.123

  Остальные параметры агента оставьте установленными по умолчанию.

Для создания правила усиленной фильтрации:

- В ПУ ЦУС перейдите в раздел "Правила фильтрации" и нажмите кнопку "Создать правило фильтрации".

  Создайте правило фильтрации со следующими параметрами:

Параметр	Значение
Название	ПФ с контролем приложений
Отправитель	Сеть ПУ ЦУС
Получатель	Любой
Сервисы	http
Действие	Усиленная фильтрация
Временной интервал	Постоянно
Профиль усиленной фильтрации	Profile_http

  Установите отметку "Применить и завершить обработку".

Для создания и установки сертификата:

1. В ПУ ЦУС перейдите в раздел "Сертификаты" и нажмите кнопку "Создать сертификат".

   Появится форма для заполнения полей сертификата.
2. Заполните поля:

Поле	Значение
Название	Ssl_sert
Организация	Test
Подразделение	Test
Назначение	SSL/TLS Инспекция

3. Нажмите кнопку "Далее" и в открывающемся окне нажмите кнопку "Добавить".

4. Выберите "КШ с ЦУС" и нажмите кнопку "Готово".

   Сертификат будет создан.
5. Выберите созданный сертификат и на вкладке "Состав" выберите "Копировать в файл...".
6. Установите сертификат в хранилище локального компьютера (хост с ПУ ЦУС) в Доверенные корневые центры сертификации.

   Дождитесь применения конфигурации на КШ с ЦУС.

Для проверки работы правил:

1. На хосте с ПУ с ЦУС с помощью браузера зайдите на страницу по адресу http://1.1.1.123.

   Страница успешно загрузится.
2. Закройте браузер, перейдите в раздел "Профили усиленной фильтрации", откройте созданный профиль усиленной фильтрации Profile_http и укажите действие — "Запретить".

   Дождитесь применения конфигурации на КШ с ЦУС.
3. На хосте с ПУ с ЦУС с помощью браузера зайдите на страницу по адресу http://1.1.1.123.

   Страница не загружается.
4. Откройте журнал сетевого трафика КШ с ЦУС.

   В журнале появится запись об отброшенном пакете согласно правилам усиленной фильтрации.

Запрет доступа к ресурсам единого реестра Роскомнадзора

Используя правила фильтрации, можно организовать запрет на доступ к ресурсам, включенным в состав единого реестра Роскомнадзора. При этом предусмотрено два варианта фильтрации — по IP-адресам и по URL.

Для фильтрации по IP-адресам необходимо сформировать правило (или правила), в котором в качестве источника или получателя указана группа сетевых объектов с именем "Реестр запрещенных ресурсов". Группа содержит сведения обо всех ресурсах единого реестра Роскомнадзора, в том числе IP-адреса запрещенных ресурсов. Группа "Реестр запрещенных ресурсов" создается автоматически при инициализации ЦУС и изначально не содержит объектов. Заполнение группы объектами осуществляется загрузкой в БД ЦУС сведений о запрещенных ресурсах, полученных в Роскомнадзоре (см. далее).

Для фильтрации по URL необходимо сформировать правило усиленной фильтрации, в котором используется специальный профиль — профиль запрещенных ресурсов. Профиль формируется автоматически на основании загружаемых в БД ЦУС сведений о запрещенных ресурсах. Сведения загружаются в БД ЦУС в виде xml-файла. Профиль содержит список агентов, которые также формируются автоматически. Поле "Адрес" в свойствах агента заполняется из тега domain загружаемого xml-файла. При формировании правила в поле "Действие" следует указать значение "Усиленная фильтрация", а в поле "Профиль усиленной фильтрации" — "Профиль запрещенных ресурсов" (работа с правилами фильтрации описана на стр. **17**).

Внимание! Независимо от того, что в настройках профиля запрещенных ресурсов у параметра "Вариант усиленной фильтрации" указано HTTP, профиль запрещенных ресурсов также работает с HTTPS-сервисами. При этом должно быть выполнено следующее:

- создан сертификат SSL/TLS-инспекции (см. стр. **25**);
- в настройки правила фильтрации добавлен HTTPS-сервис (см. стр. **17**).

Загрузка сведений о запрещенных ресурсах

Порядок получения сведений о запрещенных ресурсах единого реестра приведен на портале Роскомнадзора.

Сведения (выгрузка) представляют собой xml-файл, который должен быть загружен в БД ЦУС.

Загрузка файла в БД ЦУС может быть выполнена вручную средствами ПУ ЦУС или автоматически агентом Роскомнадзора (о настройке и работе агента см. [**1**]).

Для загрузки файла вручную:

1. В ПУ ЦУС выберите команду "ЦУС | Загрузить файл реестра запрещенных ресурсов".

   На экране появится стандартный диалог выбора файла.
2. Укажите файл выгрузки и нажмите в диалоге кнопку "Открыть".

   Сведения о запрещенных ресурсах будут загружены в БД ЦУС.

Для просмотра сведений о запрещенных ресурсах в БД ЦУС:

- В ПУ ЦУС в окне объектов раскройте папку "Центр Управления Сетью | Группы сетевых объектов".

  В главном окне отобразится строка со сведениями о реестре запрещенных ресурсов.

  При выделении строки в дополнительном окне отобразится список правил фильтрации, в которых используется группа сетевых объектов "Реестр запрещенных ресурсов".

  Примечание. Если такие правила фильтрации не создавались, список в дополнительном окне будет пустым.

Внимание! Группа "Реестр запрещенных ресурсов" удалению и редактированию не подлежит.

Глава 3
Правила трансляции

Общие сведения

Трансляция осуществляется для IP-пакета, который соответствует всем параметрам правила трансляции. Проверка параметров осуществляется в сформированном в ПУ ЦУС списке правил трансляции до первого полного соответствия.

По типу правила трансляции сетевых адресов в АПКШ "Континент" разделяются на:

- исходящие;
- входящие;
- 1:1.

Внимание! По VPN-каналу трансляция FTP-трафика не поддерживается, т.е. клиент не сможет подключиться к FTP-серверу, если запрос идет из защищаемой сети одного КШ на FTP-сервер, находящийся в защищаемой сети другого КШ, при наличии парной связи между этими КШ.

Общий порядок создания правила трансляции:

1. Создайте элементы правил (см. стр. **6**), которые будут использоваться в качестве параметров правил трансляции:
   - сетевые объекты;
   - сервисы.
2. Создайте правило трансляции (см. ниже) и, при необходимости, соответствующее правило фильтрации (см. стр. **17**).

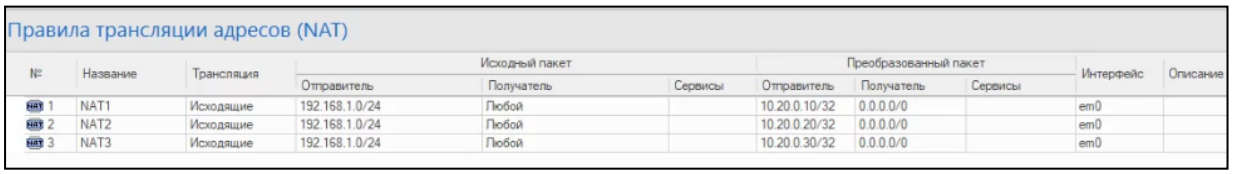
Управление правилами трансляции

Вызов списка правил трансляции

Для вызова списка правил трансляции:

1. В области объектов управления ПУ ЦУС выберите пункт "Сетевые устройства Континент | Криптошлюзы".

   В правой части окна отобразится список криптошлюзов, зарегистрированных в ЦУС.
2. Выберите в списке нужный КШ и перейдите к вкладке "Правила трансляции адресов (NAT)".


Правила трансляции адресов (NAT)

№	Название	Трансляция	Исходный пакет			Преобразованный пакет			Интерфейс	Описание
			Отправитель	Получатель	Сервисы	Отправитель	Получатель	Сервисы		
1	NAT1	Исходящие	192.168.1.0/24	Любой		10.20.0.10/32	0.0.0.0/0		em0	
2	NAT2	Исходящие	192.168.1.0/24	Любой		10.20.0.20/32	0.0.0.0/0		em0	
3	NAT3	Исходящие	192.168.1.0/24	Любой		10.20.0.30/32	0.0.0.0/0		em0	

   Список правил трансляции отображается в форме таблицы, каждая строка которой соответствует одному правилу. Поля таблицы содержат параметры правила трансляции.

   При работе правил трансляции адресов действует принцип приоритизации — стоящее в списке правило выше имеет более высокий приоритет. Наивысший приоритет имеет первое в списке правило. Изменение приоритета осуществляется перемещением правила в списке вверх или вниз с помощью мыши или кнопок в панели инструментов.

Параметры правил трансляции

Ниже в таблице приведено описание параметров правил трансляции сетевых адресов.

Параметр	Описание
№	Уникальный номер правила, используется в журналах в качестве идентификатора
Название	Название правила

Параметр	Описание
Трансляция	Тип правила трансляции (Входящие, Исходящие, 1:1)
Исходный пакет	
Отправитель	Сетевой объект. Указывается название сетевого объекта
Получатель	Сетевой объект. Указывается название сетевого объекта
Сервисы*	Перечень контролируемых сервисов или их групп
Преобразованный пакет	
Отправитель	Значения: • Адрес — фиксированный адрес; • Адрес интерфейса (только для правил типа "Исходящие") — адрес указанного интерфейса КШ
Получатель	IP-адрес получателя после трансляции
Сервисы	Порты отправителя/получателя
Интерфейс	Интерфейс КШ
Описание	Дополнительные сведения (необязательный параметр)
Регистрация	Вид регистрации • Определяется источником/получателем. • Первые 64 байта — регистрировать в журнале сетевого трафика первые 64 байта пакета. • Тело пакета — регистрировать заголовок и содержание пакета. • Первый пакет в соединении — регистрировать заголовок и содержание первого пакета, открывающего соединение
Временной интервал	Время действия правила
Класс трафика	Выбирается из зарегистрированных классов трафика (см. стр. **12**)
Реакция на события	Вид регистрации при срабатывании правила

* Для настройки входящего правила трансляции можно использовать сервисы только со следующими параметрами:

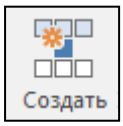
- протокол — TCP или UDP;
- порт источника — любой (определяется с помощью оператора "Любой");
- порт назначения — конкретное значение одного порта.

Процедура настройки параметров сервиса приведена на стр. **9**.

Создание правила трансляции

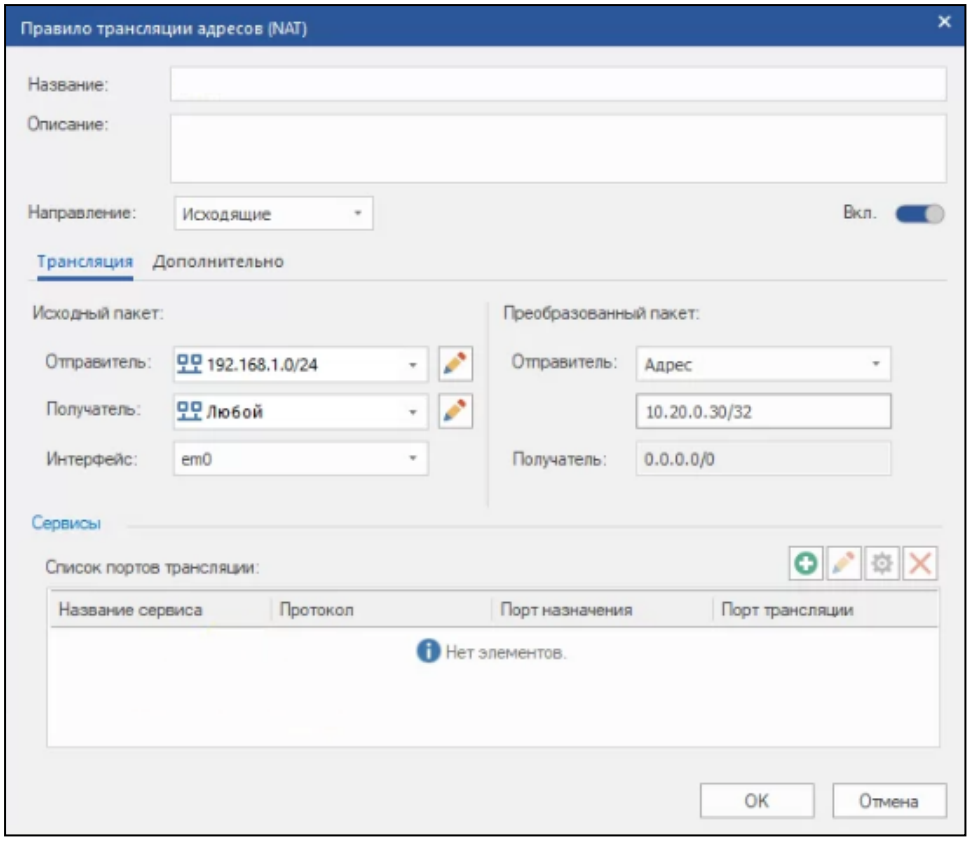
Для создания правила:

1. Вызовите список правил трансляции и нажмите кнопку "Создать" в панели инструментов.

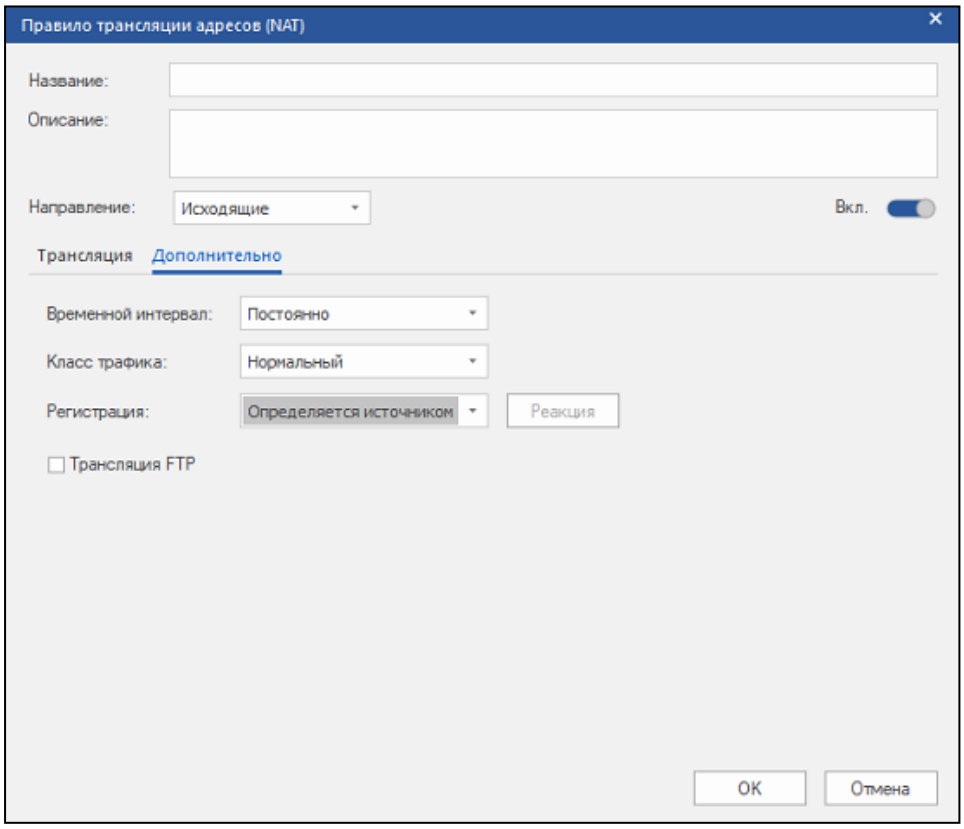


На экране появится окно "Правило трансляции адресов (NAT)".

Примечание. При наличии созданных правил трансляции можно создать новое правило трансляции на основе копии имеющегося. Для этого необходимо вызвать контекстное меню копируемого правила и активировать команду "Создать копию...". В этом случае окно "Правило трансляции адресов (NAT)" будет заполнено копируемыми параметрами, доступными для редактирования.



2. Укажите требуемые значения параметров (см. стр. **41**) и при необходимости перейдите на вкладку "Дополнительно".



На вкладке "Дополнительно" можно задать следующие параметры правила:

- Временной интервал, в течение которого должно действовать правило.

- Класс трафика, которому будут принадлежать IP-пакеты с заданными характеристиками. Класс трафика используется для формирования очереди на обработку блоком криптографической защиты, а также на отправку на сетевом интерфейсе.
- Вид регистрации при срабатывании правила.
- Кнопка "Реакция" вызывает на экран список зарегистрированных реакций на события. Отметьте нужные и нажмите кнопку "ОК". Кнопка доступна только при выборе в поле "Регистрация" значения "Первый пакет в соединении".
- Отметку в поле "Трансляция FTP" устанавливают для обеспечения корректной трансляции адресов источника для правила NAT 1:1 при передаче данных по протоколу FTP.

  Внимание!

  При добавлении правила трансляции (1:1), отличающегося от уже имеющегося только наличием отметки в поле "Трансляция FTP", работа FTP не гарантируется.

3. После настройки параметров нажмите кнопку "ОК".

   Список правил дополнится соответствующей строкой.

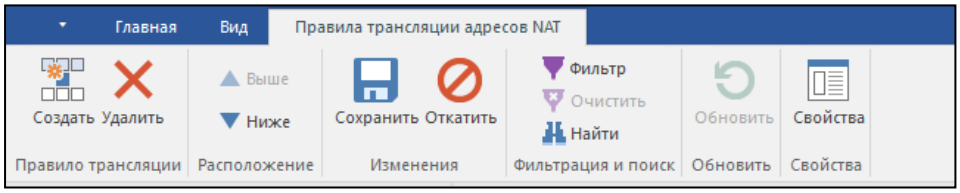
Работа с правилами трансляции

При работе с правилами предусмотрены следующие операции:

Совет. Для выбора нескольких правил используйте левую кнопку мыши и клавишу <Shift> или <Ctrl>.

1. Для редактирования правила вызовите окно его параметров, нажав кнопку "Свойства" на панели инструментов, внесите необходимые изменения в соответствии с описанием параметров(см. стр. **41**) и нажмите кнопку "ОК".

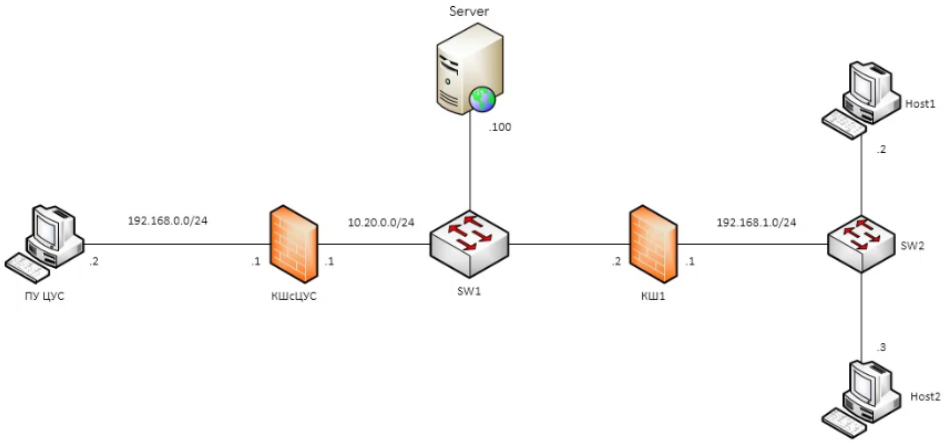
   Для отмены внесенных изменений нажмите кнопку "Откатить" в панели инструментов.



2. Для удаления правила выберите одно или несколько правил в списке, нажмите кнопку "Удалить" на панели инструментов и подтвердите операцию в появившемся окне.
3. Для включения/отключения правила выберите его в списке, вызовите окно настройки параметров и переведите переключатель "Вкл/Откл" в соответствующее положение.
4. Для фильтрации отображаемых в списке правил нажмите кнопку "Фильтр" на панели инструментов, выберите параметр фильтрации в поле "По столбцу", укажите его значение в поле "Текст", при необходимости установите отметки в дополнительных полях фильтра. Для использования сразу двух параметров фильтрации заполните поля в области "Затем" и задайте логику сочетания параметров (И/ИЛИ). Проверьте введенные параметры и нажмите кнопку "ОК".
5. Для просмотра всего списка правил без установленной фильтрации нажмите на панели инструментов кнопку "Очистить".
6. Для поиска по определенному значению параметра правила фильтрации выберите в списке правило, с которого начнется поиск, затем нажмите на панели инструментов кнопку "Найти". Настройте параметры поиска (см. п. **4**) и задайте направление поиска от выбранного правила. Нажмите кнопку "Найти следующее" для перехода к первому правилу в списке, удовлетворяющему условиям поиска. Для выделения правил, удовлетворяющих условиям поиска, нажмите кнопку "Пометить все".

Пример применения правил трансляции

В данном подразделе приводится пример применения правил трансляции сетевыхт адресов для схемы, приведенной ниже. Также приводятся примеры приоритизации правил и использование имени внешнего интерфейса в правилах NAT вместо IP-адреса.



На схеме выше показаны криптошлюзы КШ 1 и криптошлюз с ЦУС.

У КШ 1 есть своя внутренняя сеть 192.168.1.0/24, в которой расположены хосты Host1 и Host2.

У КШ с ЦУС так же есть своя внутренняя сеть 192.168.0.0/24, в которой находится ПУ ЦУС.

Также на схеме показана внешняя сеть 10.20.0.0/24, в которой находится сервер.

Пример правил трансляции приведен для следующих типов:

- исходящие;
- 1:1;
- входящие.

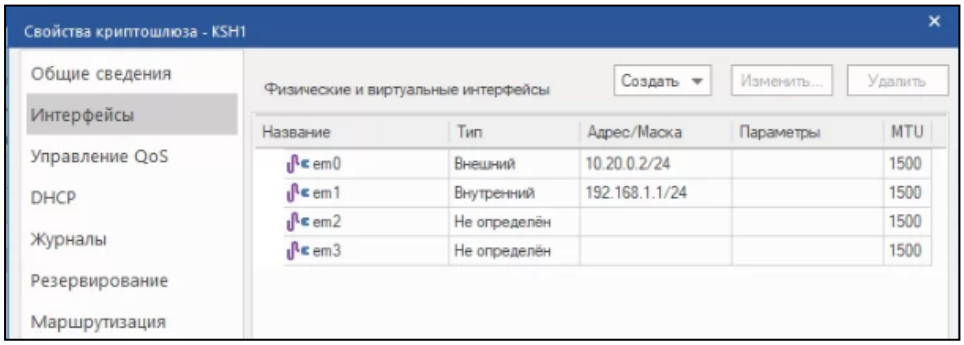
Для настройки и проверки работы правил трансляции в данном примере необходимо:

- проверить настройку интерфейсов КШ 1;
- создать сетевые объекты, используемые в правилах трансляции;
- создать правила для каждого типа (исходящие, 1:1, входящие) и проверить их работу;
- проверить работу приоритизации правил.

Настройка интерфейсов КШ 1

1. В ПУ ЦУС перейдите к списку криптошлюзов, откройте окно свойств КШ 1 и перейдите в раздел "Интерфейсы".

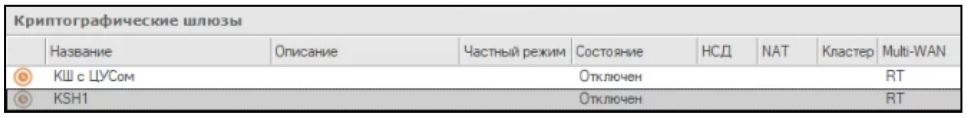
   В правой части окна отобразится список интерфейсов КШ 1.



   В данном примере на КШ 1 настроены интерфейсы em0 (внешний) и em1 (внутренний).

2. После просмотра сведений об интерфейсах закройте окно свойствКШ 1.

   Будет выполнен возврат к списку криптошлюзов.



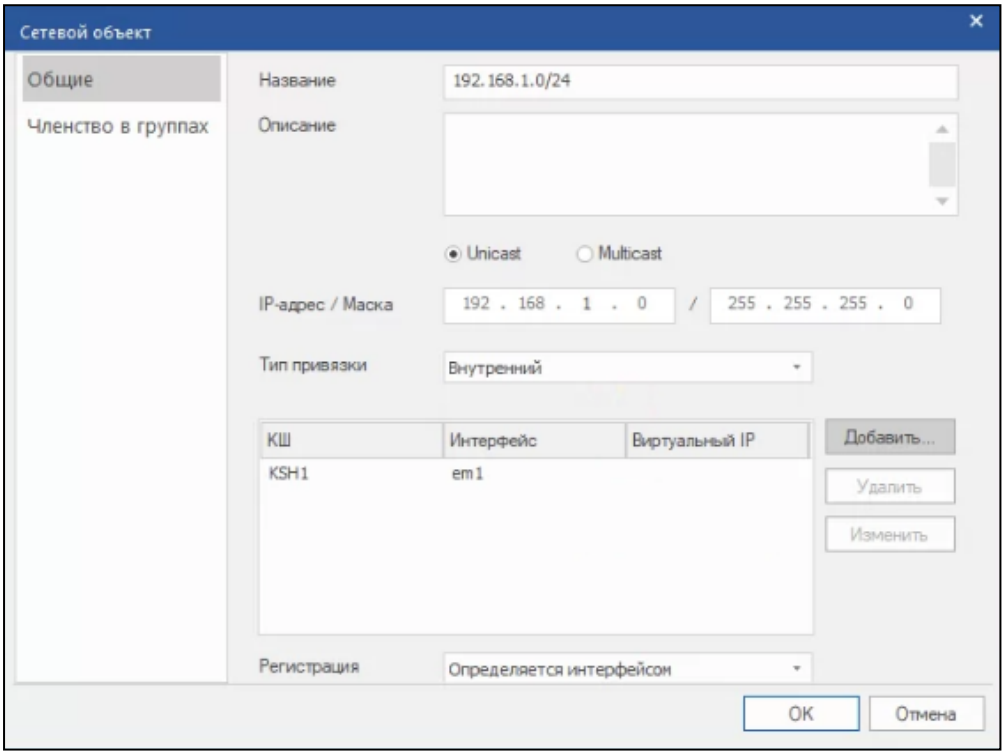
Создание сетевых объектов

В правилах трансляции будут использоваться следующие сетевые объекты:

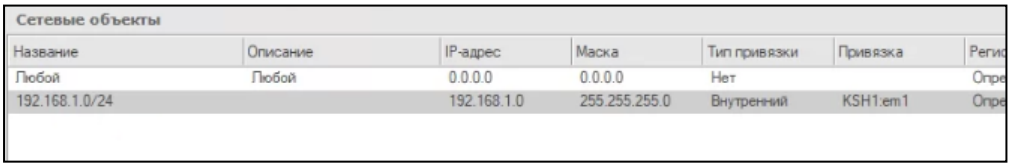
- внутренняя сеть КШ 1;
- хост 1;
- хост 2;
- сервер.

Создайте сетевые объекты (о создании и настройке сетевых объектов см. стр. **7**) и задайте их параметры, как показано на рисунках ниже.

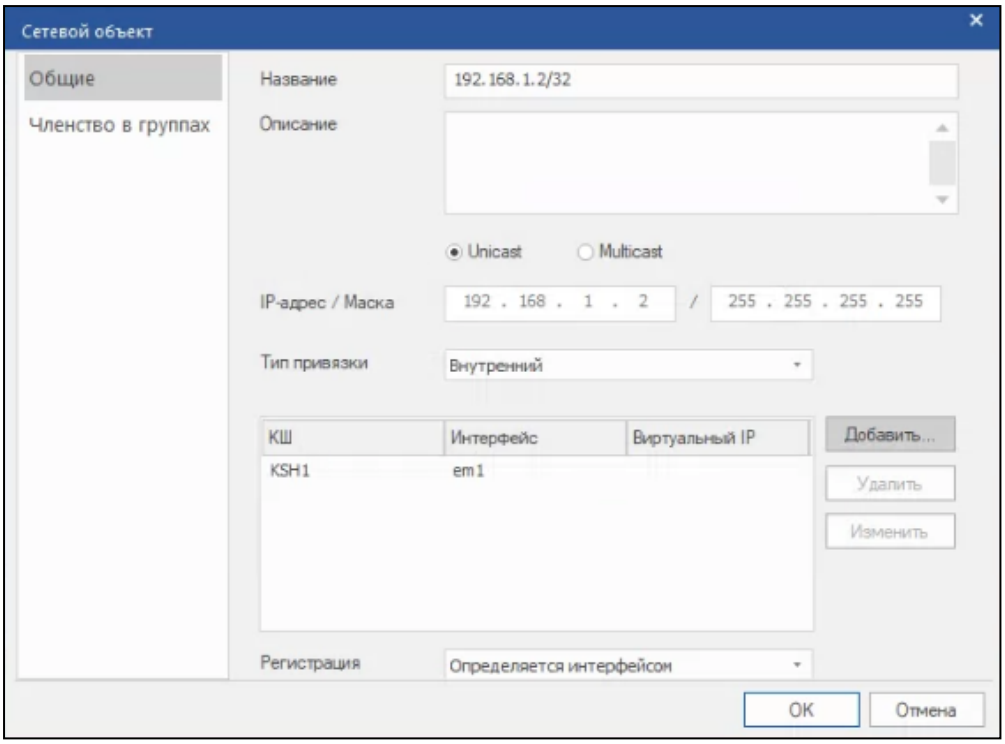
Внутренняя сеть КШ 1



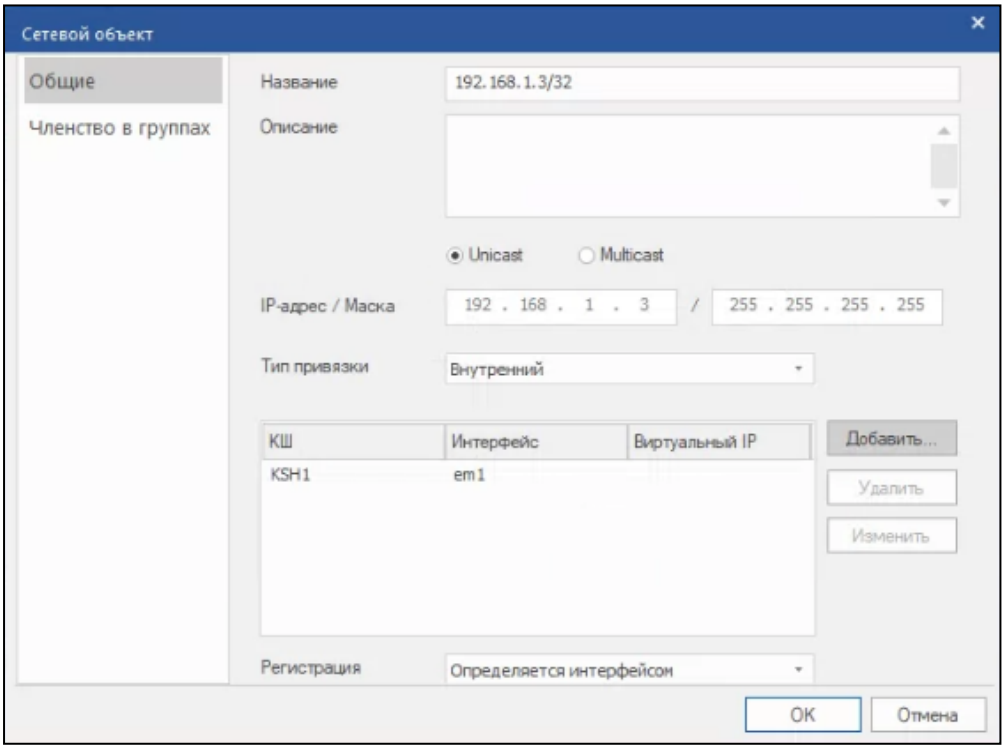
После настройки параметров как указано на рисунке выше, новый сетевой объект появится в списке.

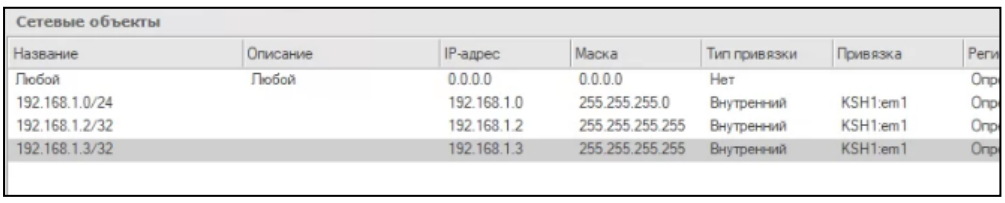


Хост 1

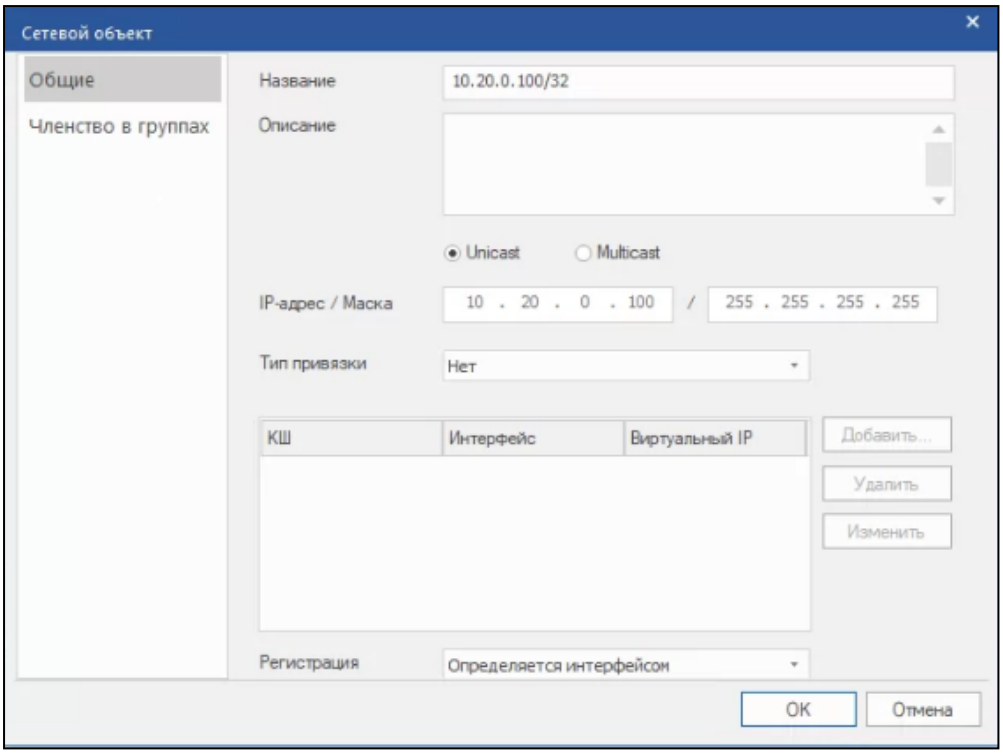

Сетевой объект
Общие
Членство в группах
Название
192.168.1.2/32
Описание
Unicast
Multicast
IP-адрес / Маска
192 . 168 . 1 . 2
/
255 . 255 . 255 . 255
Тип привязки
Внутренний
КШ
Интерфейс
Виртуальный IP
KSH1
em1
Добавить...
Удалить
Изменить
Регистрация
Определяется интерфейсом
OK
Отмена

Хост 2

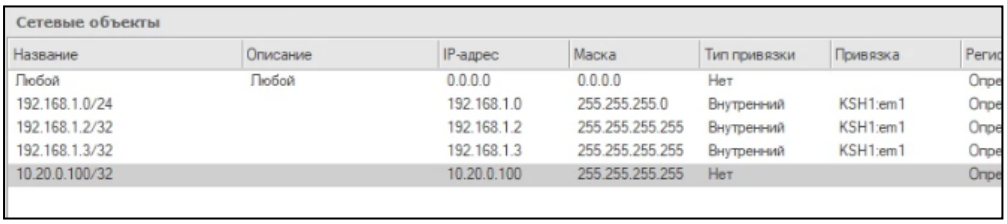

Сетевой объект
Общие
Членство в группах
Название
192.168.1.3/32
Описание
Unicast
Multicast
IP-адрес / Маска
192 . 168 . 1 . 3
/
255 . 255 . 255 . 255
Тип привязки
Внутренний
КШ
Интерфейс
Виртуальный IP
KSH1
em1
Добавить...
Удалить
Изменить
Регистрация
Определяется интерфейсом
OK
Отмена


Сетевые объекты
Название
Описание
IP-адрес
Маска
Тип привязки
Привязка
Любой
Любой
0.0.0.0
0.0.0.0
Нет
192.168.1.0/24
192.168.1.0
255.255.255.0
Внутренний
KSH1:em1
192.168.1.2/32
192.168.1.2
255.255.255.255
Внутренний
KSH1:em1
192.168.1.3/32
192.168.1.3
255.255.255.255
Внутренний
KSH1:em1

Сервер



В результате список будет содержать 4 сетевых объекта:



Исходящие правила трансляции адресов

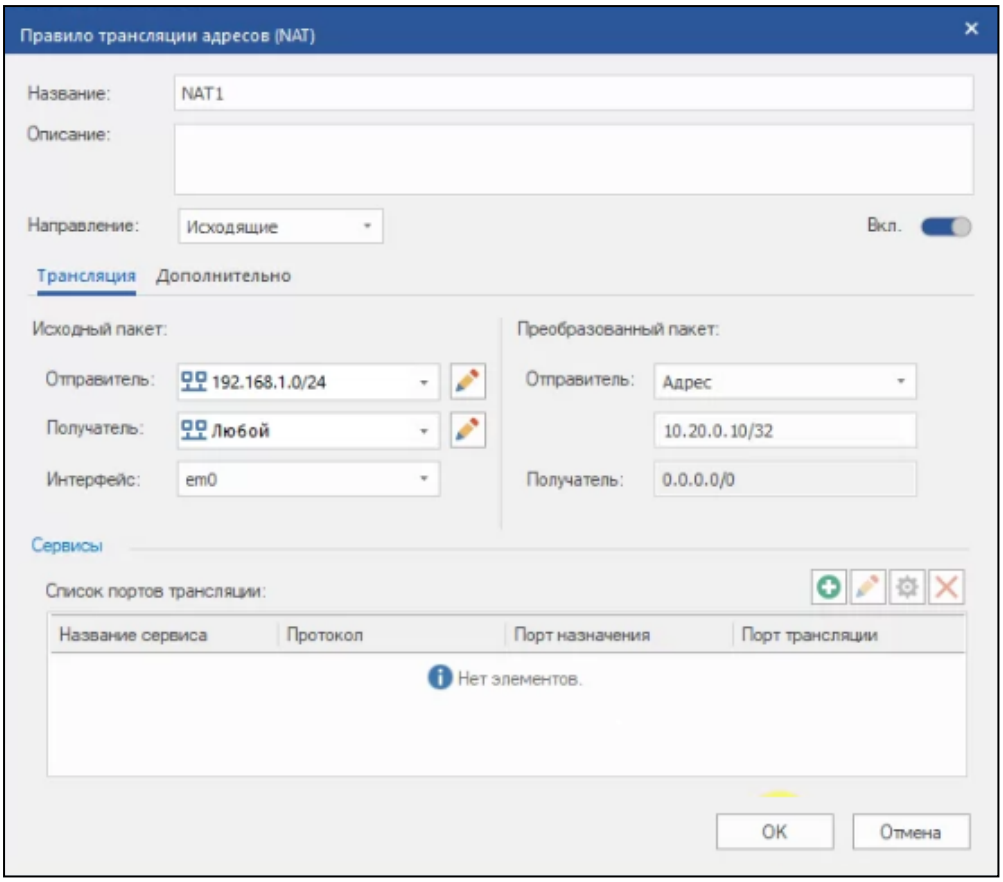
Требуется получить доступ к серверу с хостов Host1 и Host2 при помощи правил трансляции.

Для иллюстрации работы приоритизации правил будет создано 3 правила.

1. Перейдите к списку криптошлюзов, выберите КШ 1 и перейдите в раздел "Правила трансляции адресов (NAT)".
2. В панели инструментов нажмите кнопку "Создать".

   Откроется окно настройки правила трансляции.

Первое правило NAT 1



Исходный пакет:

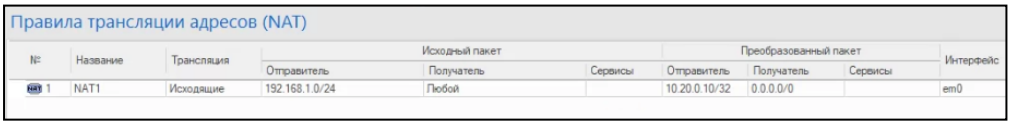
- Отправитель — сеть, в которой расположены хосты.
- Получатель — любой.

Преобразованный пакет:

- Отправитель — Адрес, произвольный (например, 10.20.0.10/32, см. рис .выше).

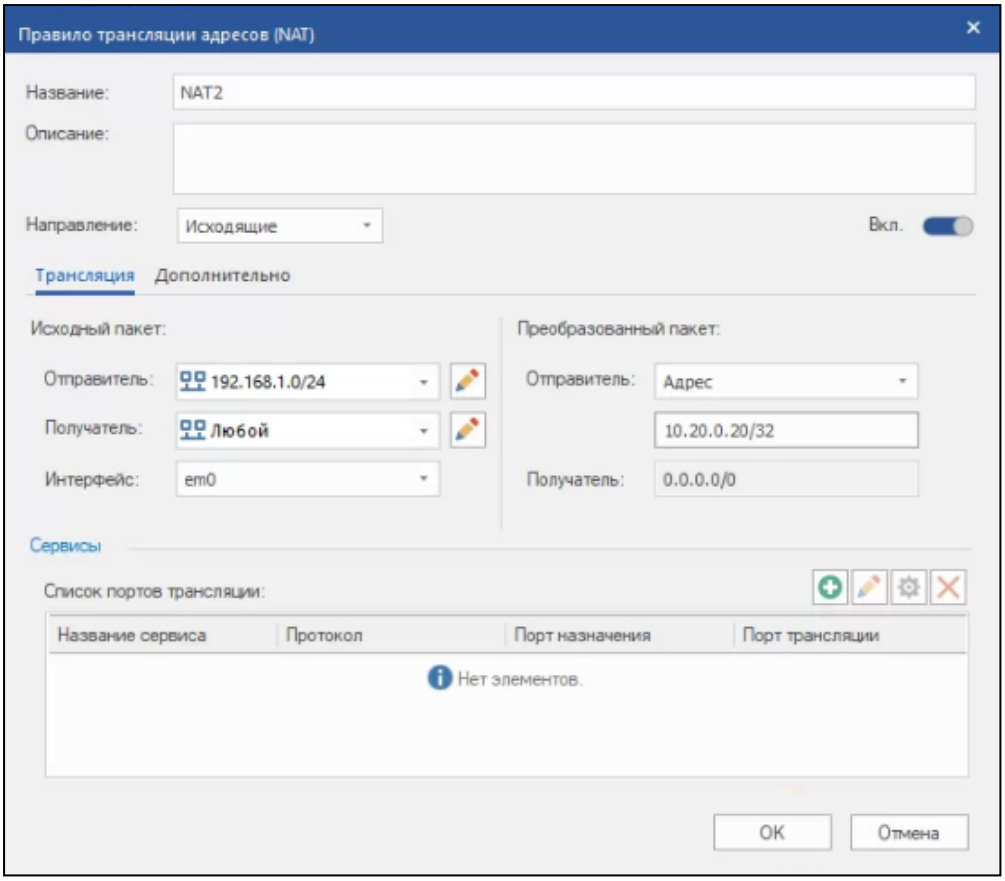
Сервисы можно не задавать. По умолчанию, если сервисы не заданы, разрешены все.

После задания параметров нажмите кнопку "OK". В списке появится первое правило.



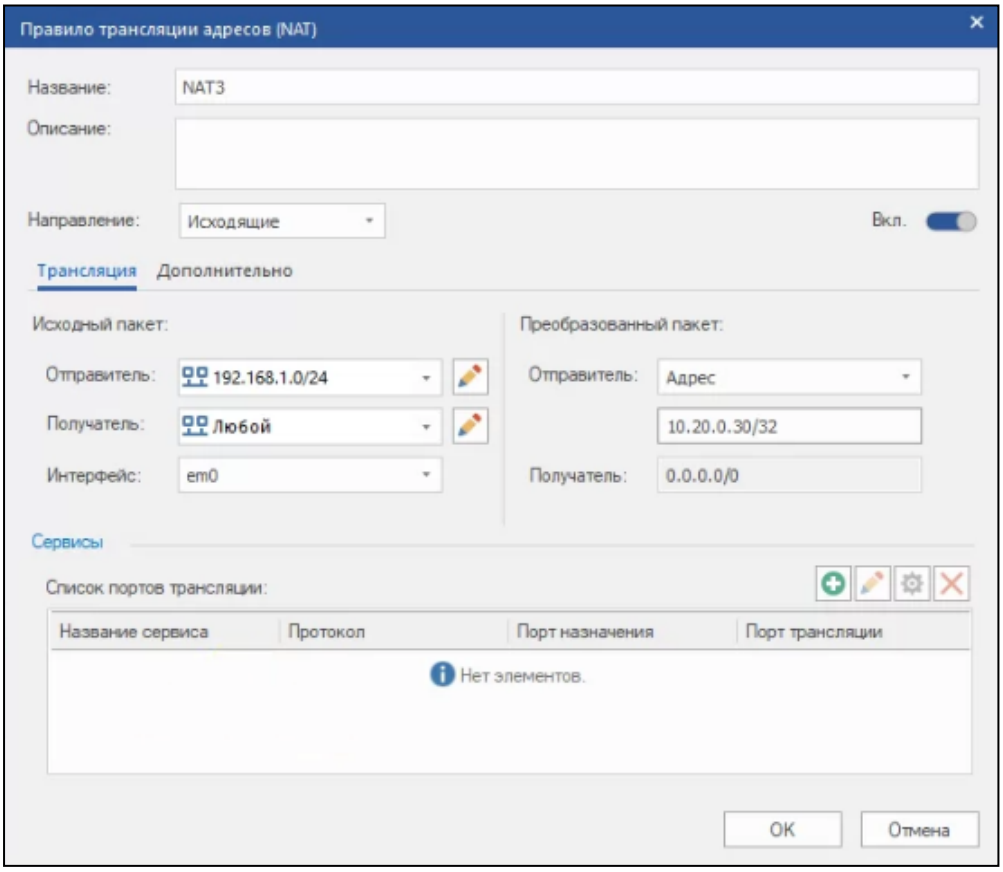
Второе правило NAT 2

Второе правило повторяет первое, за исключением адреса отправителя в преобразованном пакете (10.20.0.20/32).

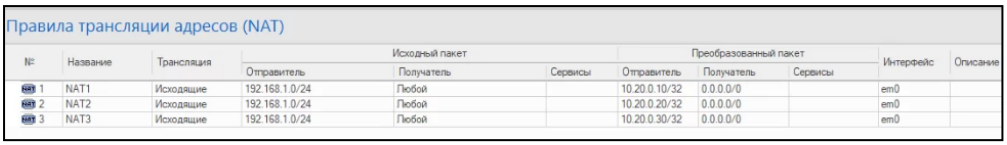


Третье правило NAT 3

Третье правило так же отличается от первых двух адресом отправителя в преобразованном пакете (10.20.0.30/32).



В результате в списке будут отображены 3 правила трансляции NAT 1 – NAT 3. Разница между этими правилами заключается только в том — на какой адрес они подменяют адреса из подсети 192.168.1.0/24.


Правила трансляции адресов (NAT)

№	Название	Трансляция	Исходный пакет			Преобразованный пакет			Интерфейс	Описание
			Отправитель	Получатель	Сервисы	Отправитель	Получатель	Сервисы		
1	NAT1	Исходящие	192.168.1.0/24	Любой		10.20.0.10/32	0.0.0.0/0		em0	
2	NAT2	Исходящие	192.168.1.0/24	Любой		10.20.0.20/32	0.0.0.0/0		em0	
3	NAT3	Исходящие	192.168.1.0/24	Любой		10.20.0.30/32	0.0.0.0/0		em0	

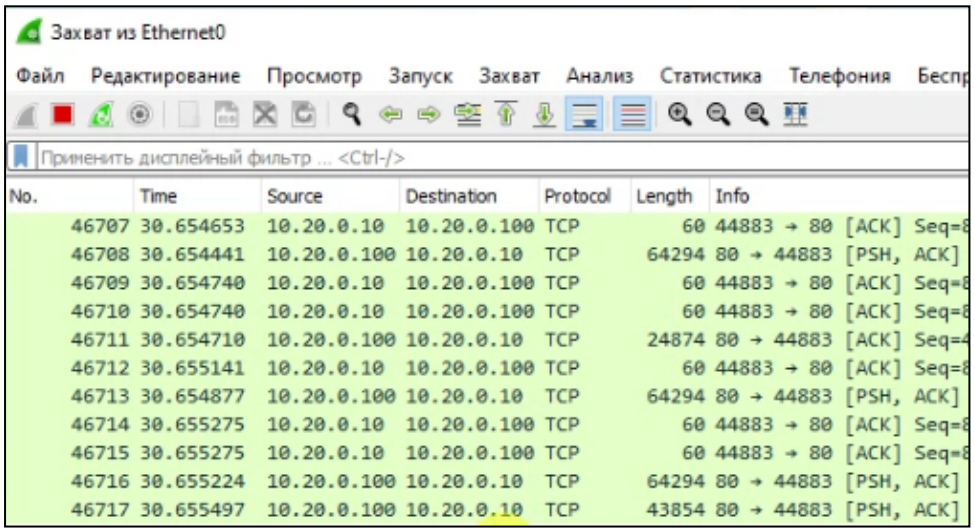
Приоритетным будет правило, которое в списке стоит выше. В данном случае приоритетным правилом является NAT 1.

Изменение приоритета правила выполняется с помощью кнопок "Выше" и "Ниже" в панели инструментов.

Нажмите в панели инструментов кнопку "Сохранить".

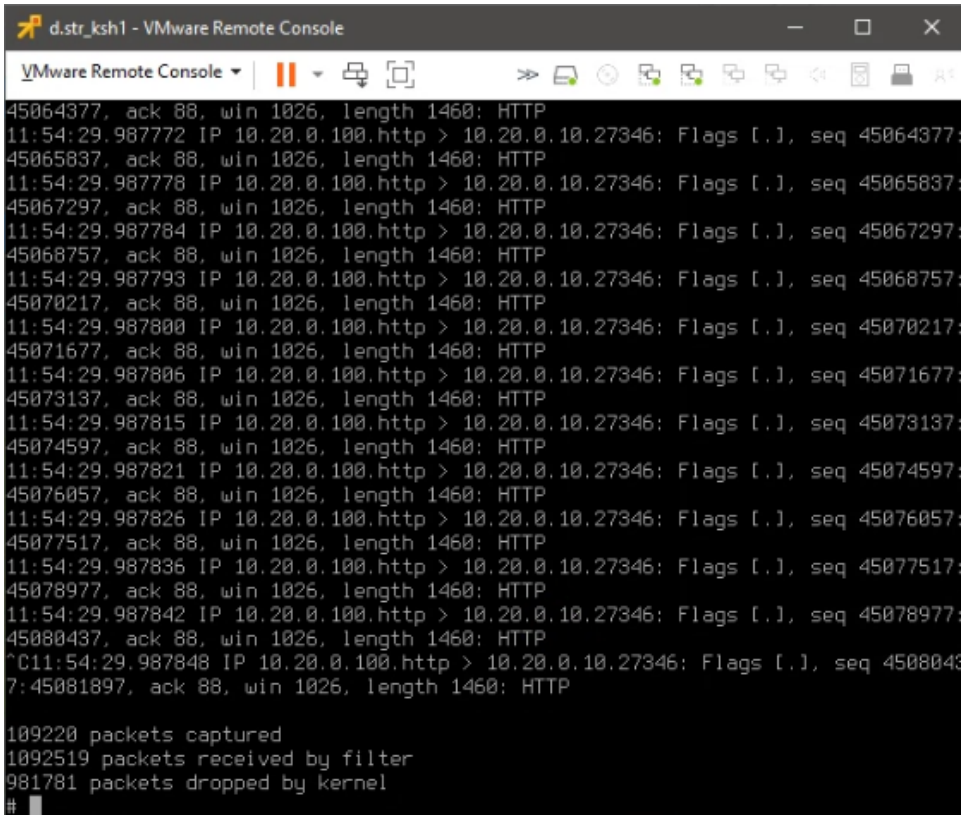
Для проверки работы исходящих правил NAT:

1. На сервере запустите http-сервер.
2. На хостах Host 1 и Host 2 запустите скачивание файла с сервера.
3. Запустите на сервере сетевой анализатор (например, Wireshark) и убедитесь, что к серверу идут обращения с адреса 10.20.0.10.



4. На КШ 1 средствами локального меню запустите на внешнем интерфейсе tcpdump.

   tcpdump -i em0 host 10.20.0.100



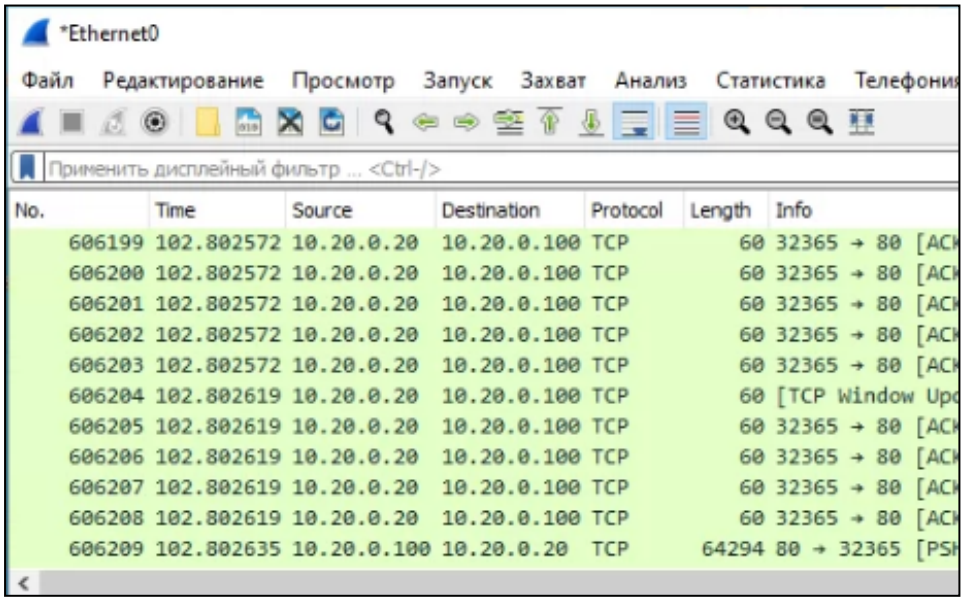
В tcpdump видно, что обращения идут с адреса 10.20.0.10 в соответствии с первым правилом NAT1.

5. Измените приоритет правила NAT 2. Для этого выделите его в списке правил трансляции и с помощью кнопки "Выше" в панели инструментов переместите правило на верхнюю строчку списка.

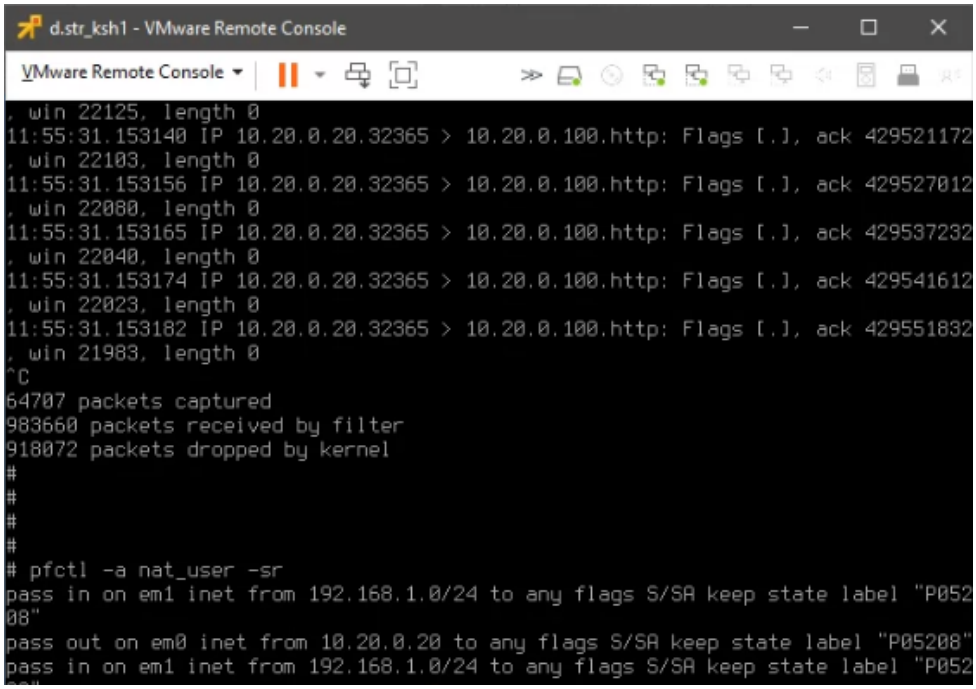
   Теперь правило NAT 2 будет иметь высший приоритет.

6. Нажмите в панели инструментов кнопку "Сохранить" и дождитесь применения настроек.

7. Запустите на сервере сетевой анализатор и убедитесь, что к серверу идут обращения с адреса 10.20.0.20.



8. На КШ 1 средствами локального меню запустите на внешнем интерфейсе tcpdump (см. п. **4**).

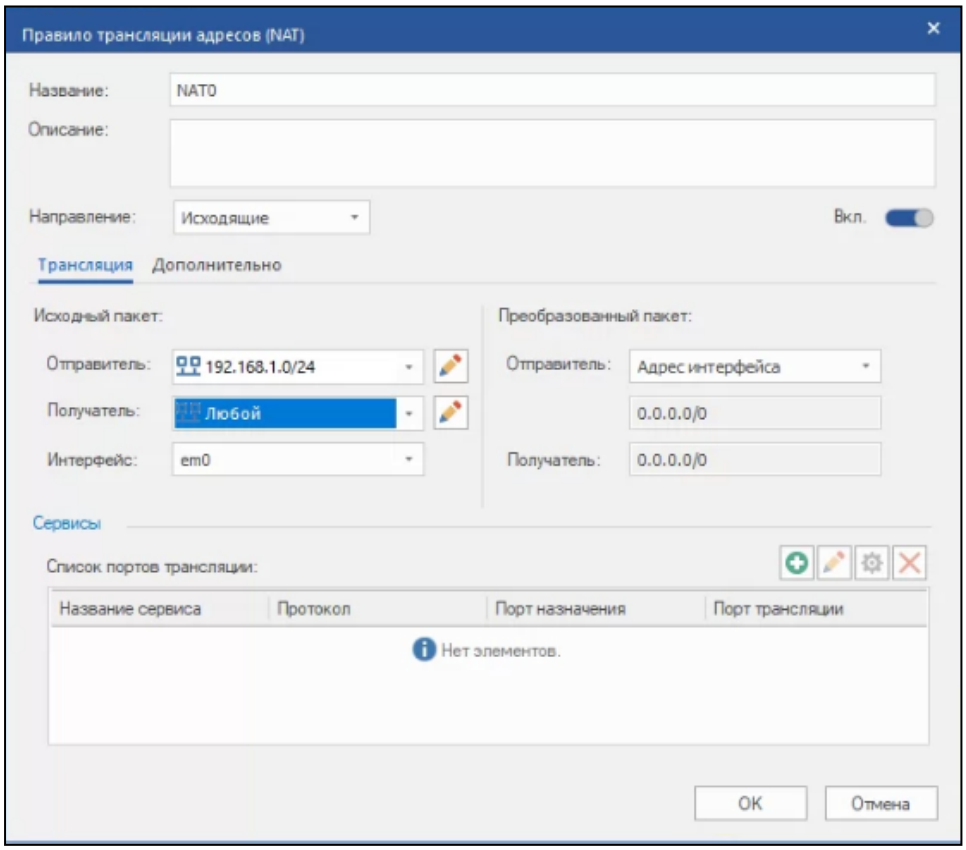


В tcpdump видно, что обращения идут с адреса 10.20.0.20 в соответствии с правилом NAT 2.

9. Выделите в списке правил трансляции правило NAT 3 и с помощью кнопки "Выше" переместите его на верхнюю строчку списка.

10. Выполните проверку, как было описано выше для правил NAT 1 и NAT 2, и убедитесь, что работает правило NAT 3.

11. В ПУ ЦУС создайте еще одно исходящее правило трансляции NAT 0. В правиле вместо указания какого-либо адреса в преобразованном пакете укажите Отправитель: Адрес интерфейса.

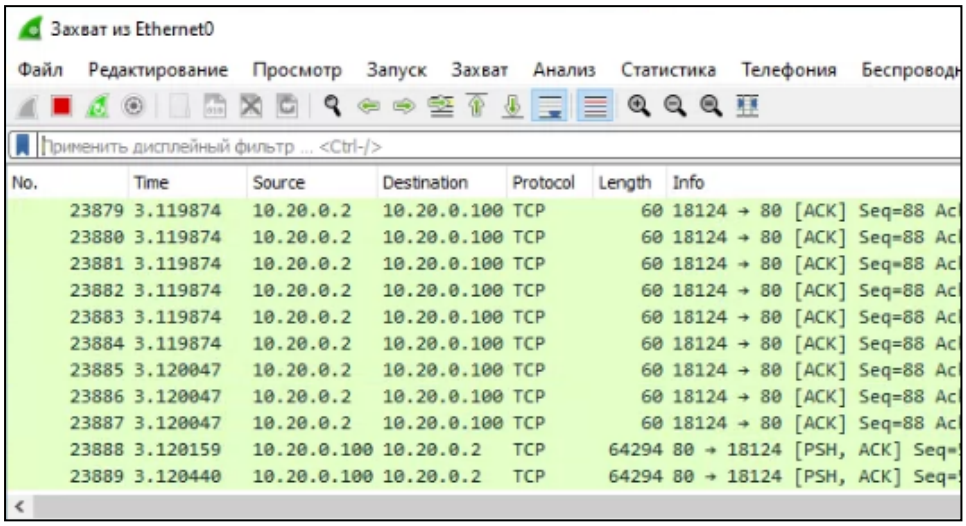


В соответствии с данным правилом внутренний адрес должен будет замениться на внешний адрес КШ 1.

12. Нажмите в панели инструментов кнопку "Сохранить" и дождитесь применения настроек.

Правило NAT 0 будет в конце списка.

13. Переместите правило NAT 0 на самый верх списка, сохраните изменения и дождитесь применения настроек.
14. Запустите на сервере сетевой анализатор и убедитесь, что к серверу идут обращения с адреса 10.20.0.2, который является внешним адресом интерфейса КШ 1.



Внимание!

Замена внутреннего адреса на внешний адрес интерфейса доступна только для исходящих правил трансляции адресов.

Правила трансляции адресов 1:1

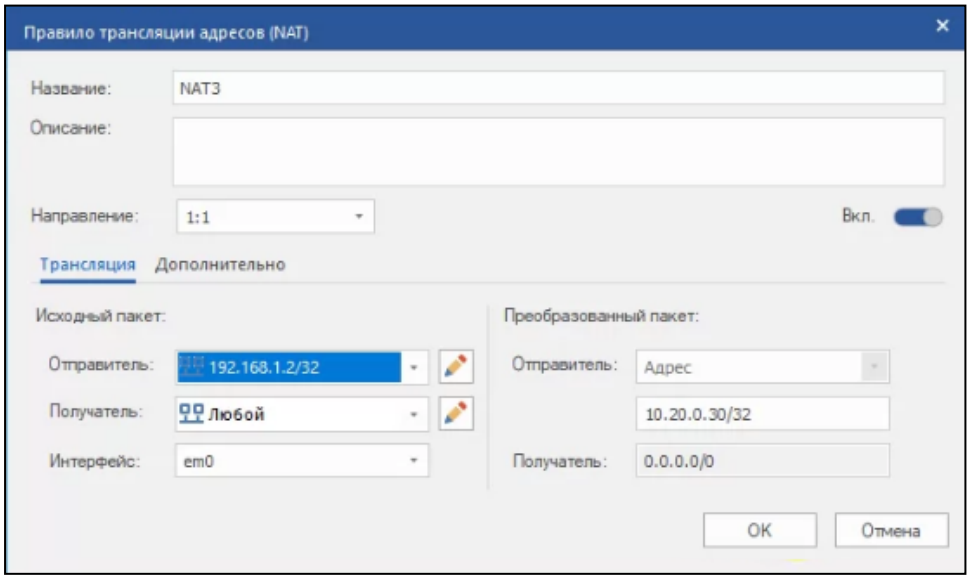
1. Удалите правило NAT 0.
2. Поменяйте в правилах NAT 1 — NAT 3 направление с "Исходящие" на "1:1".
3. В исходном пакете в качестве отправителя выберите хост 192.168.1.2/32.

   Внимание!

   Дипазон адресов отправителя в исходном пакете должен соответствовать диапазону адресов отправителя в преобразованном пакете.

   Укажите параметры правил в соответствии с приведенными ниже рисунками.

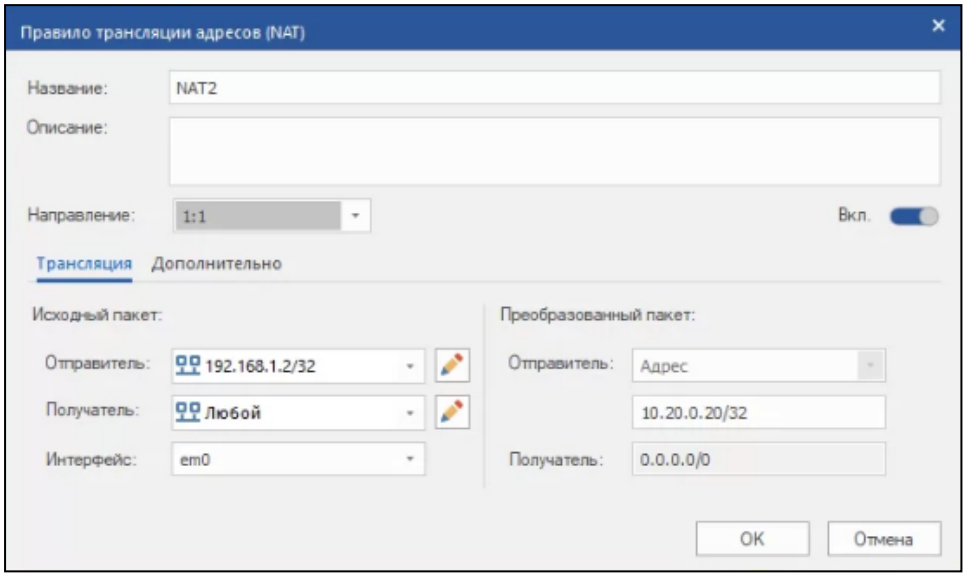
   NAT 3



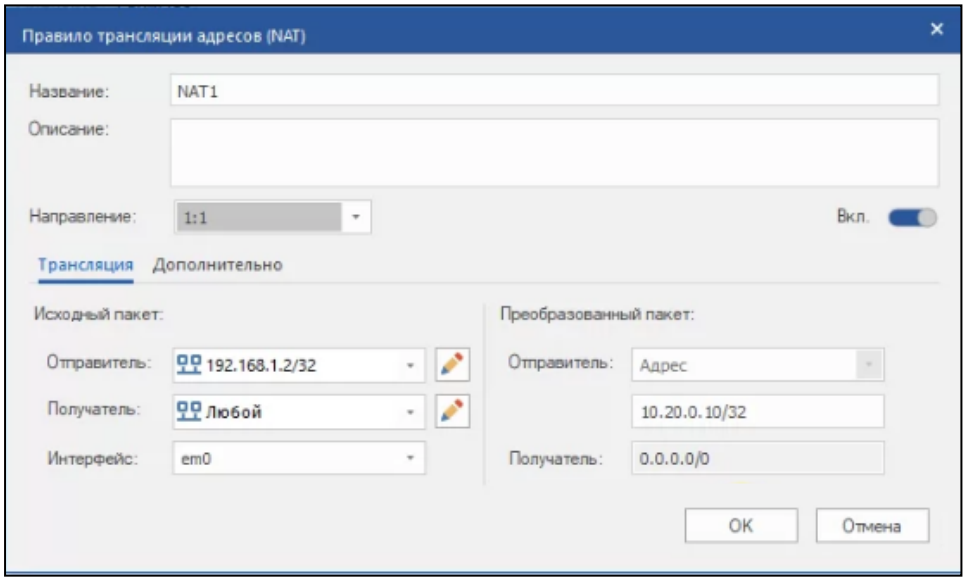
Внимание!

В диапазон адресов отправителя в преобразованном пакете не должен попадать адрес внешнего интерфейса КШ 1.

NAT 2

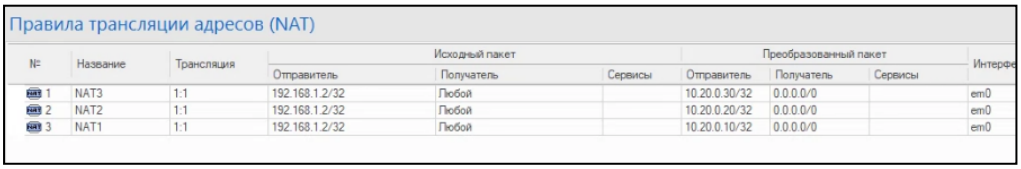


NAT 1



4. Сохраните настройки параметров правил.

   В результате в списке будут отображаться 3 правила.

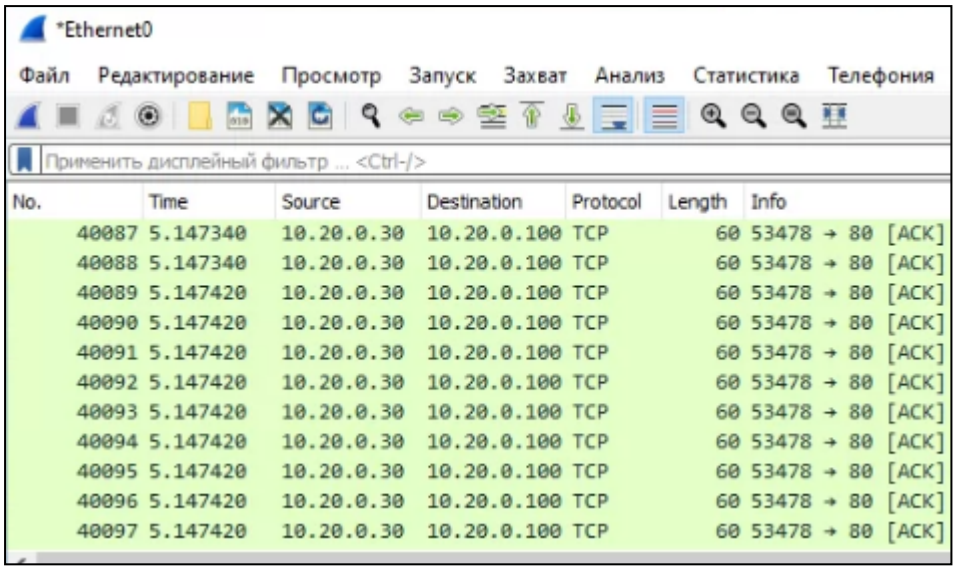


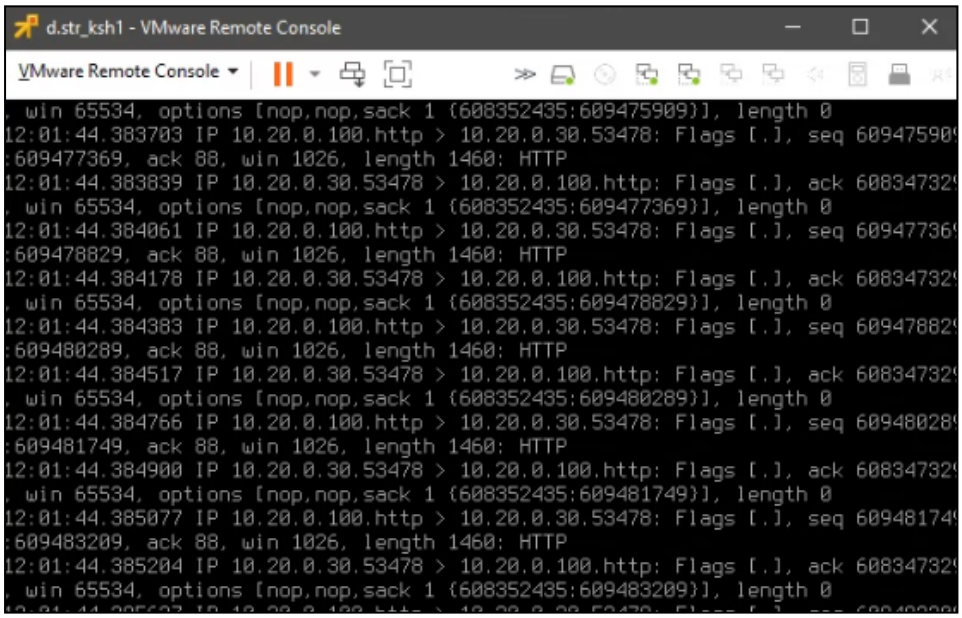
   В соответствии с правилом 1:1 адрес хоста 192.168.1.2/32 должен меняться на адрес:

   - 10.20.0.30/32 (NAT 3)
   - 10.20.0.20/32 (NAT 2).
   - 10.20.0.10/32 (NAT 1)

5. После применения конфигурации запустите на сервере сетевой анализатор, а на внешнем интерфейсе КШ 1 — tcpdump.

Так как правило NAT 3 имеет высший приоритет, адрес 192.168.1.2/32 поменялся на 10.20.0.30 (см. рисунки ниже).



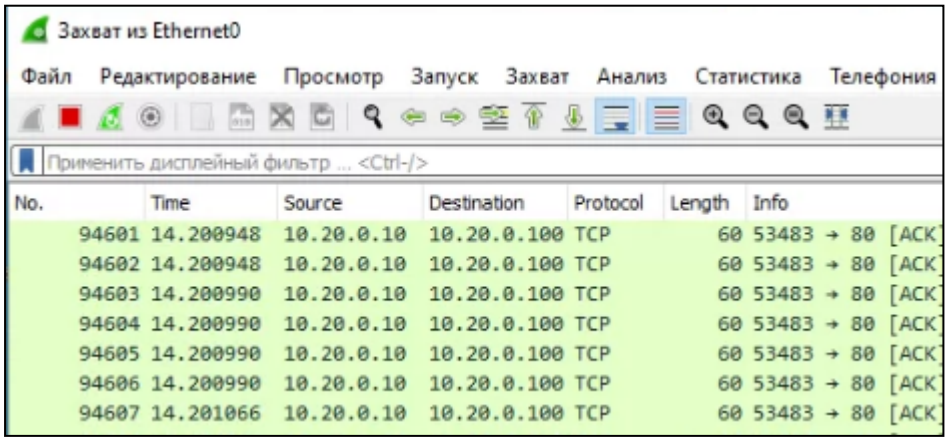


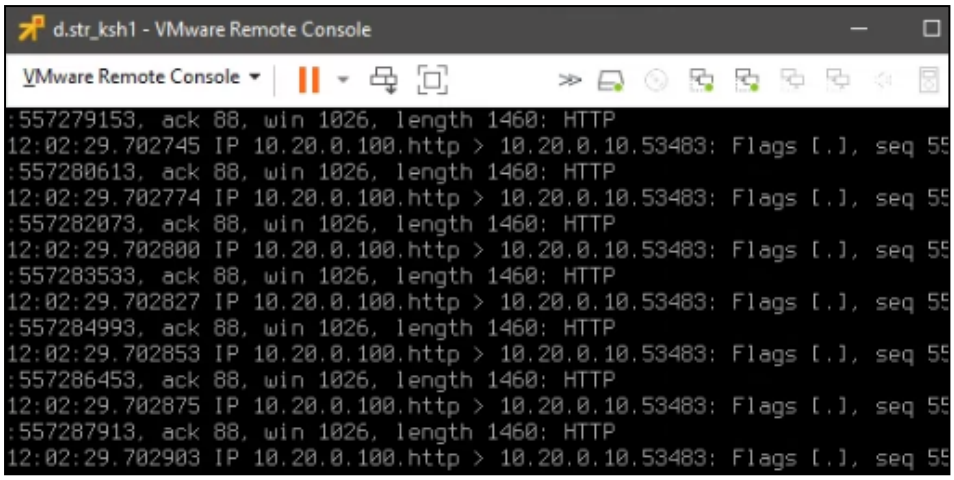
6. Измените приоритет правила NAT 1. Переместите его на первую строку списка и нажмите в панели инструментов кнопку "Сохранить".

Дождитесь применения изменений.

7. Запустите сетевой анализатор и tcpdump.

Адрес поменялся на на 10.20.0.10.





Входящие правила трансляции адресов

Оставьте в списке только правила NAT 1 и NAT 2.

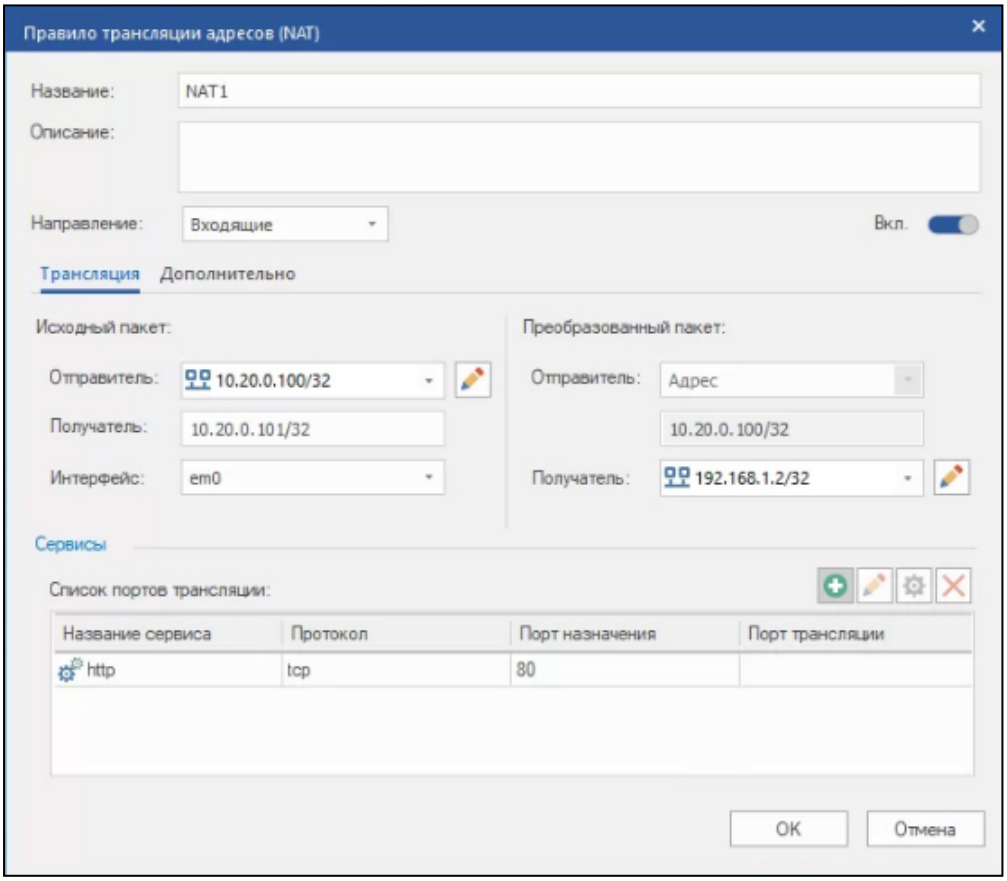
Правило NAT 1

Отправителем выберите сервер (10.20.0.100/32).

Получателем будет какой-либо случайный свободный адрес из внешней подсети (10.20.0.101/32).

Принимающим будет хост (на схеме — Host 1, 192.168.1.2/32).

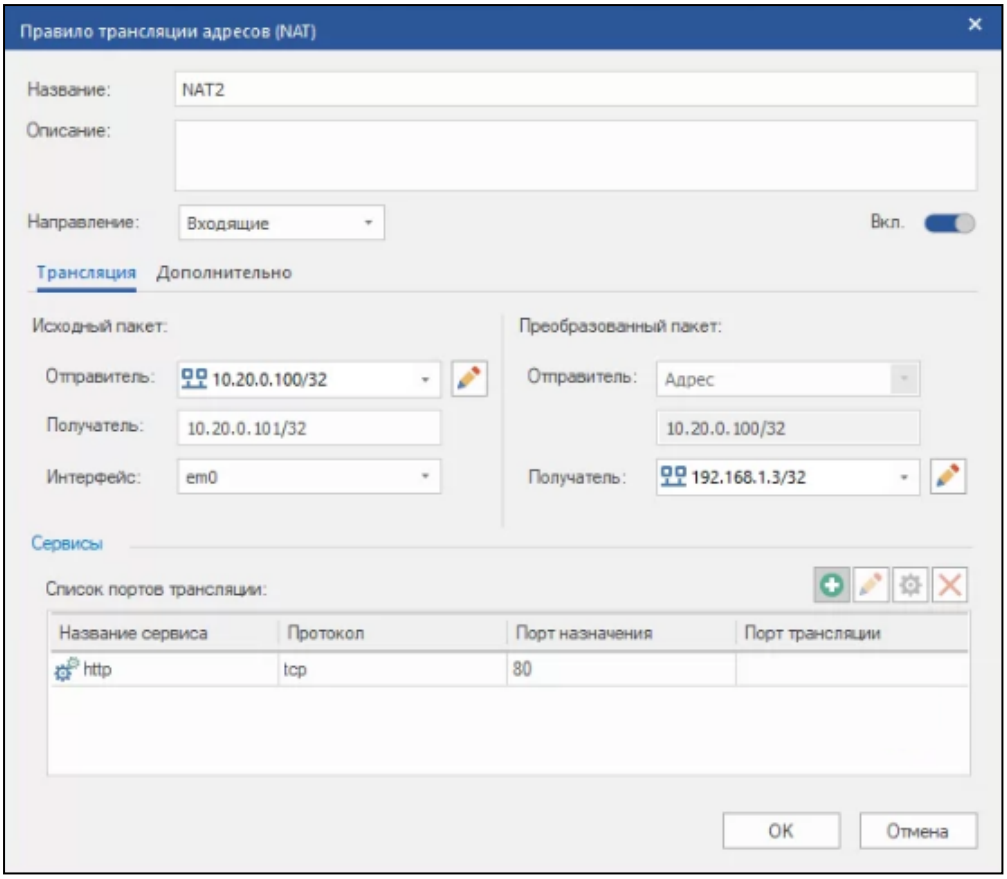
В разделе "Сервисы" укажите порт (в данном случае — 80).



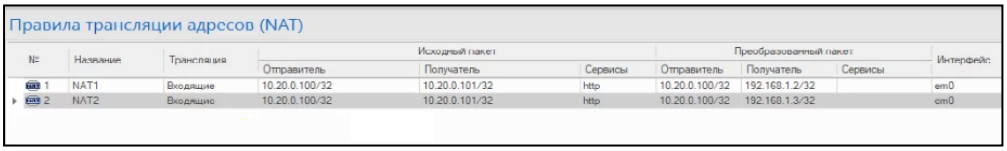
Правило NAT 2

В этом правиле принимающим будет Host 2 (192.168.1.3/32).

Остальные значения параметров такие же , как в правиле NAT 1 (см. рисунок ниже).



В результате в спике имеются два правила входящих NAT для разных хостов.



После настройки правил сохраните изменения.

Для проверки работы входящих правил NAT:

1. Запустите http-серверы на хостах Host 1 и Host 2.
2. На сервере, находящемся во внешней сети (10.20.0.100), запустите скачивание файлов с серверов, запущенных на хостах Host 1 и Host 2.

   При обращении сервера из внешней сети на адрес 10.20.0.101/32 в зависимости от действующего входящего правила NAT КШ 1 будет направлять запросы на Host 1 или Host 2.

   В данном случае правило NAT 1 имеет более высокий приоритет, поэтому скачивание будет осуществляться с сервера Host 1.
3. Для проверки работы приоритизации входящих правил NAT повысьте приоритет правила NAT 2, сохраните настройки и убедитесь что скачивание начнет осуществляться с сервера Host 2.

Виртуальная адресация

Для обеспечения возможности обмена информацией по защищенному каналу между пересекающимися подсетями, защищенными разными КШ, используется механизм виртуальной адресации.

Отправителю и получателю, находящимся в пересекающихся подсетях за разными КШ, назначаются виртуальные адреса.

Отправитель шлет пакет со своего реального адреса на виртуальный адрес получателя. При этом КШ отправителя перед шифрованием заменяет реальный адрес отправителя на виртуальный.

В зашифрованном пакете адреса отправителя и получателя — виртуальные.

КШ получателя после расшифровки заменяет адрес получателя на реальный. В результате пакет приходит на реальный адрес получателя с виртуального адреса отправителя.

Для настройки схемы с применением виртуальной адресации необходимо для каждой пары отправитель – получатель назначить виртуальные адреса. Виртуальный адрес отправителя или получателя назначается хосту или подсети, которые являются зарегистрированными сетевыми объектами.

Для назначения виртуального адреса сетевому объекту:

1. Вызовите список сетевых объектов.
2. Выберите в списке сетевой объект, для которого необходимо назначить виртуальный адрес, вызовите контекстное меню и активируйте команду "Свойства".

   На экране появится окно настройки параметров сетевого объекта.

   Описание полей окна настройки см. стр. **8**.
3. Нажмите кнопку "Изменить".

   На экране появится окно "Изменение привязки сетевого объекта".
4. Установите отметку в поле "Виртуальный IP-адрес/Маска" и введите назначаемый виртуальный адрес.

   Внимание! Поле "Виртуальный IP-адрес/Маска" доступно только в том случае, если в поле "Тип привязки" установлено значение "Защищаемый".
5. Нажмите кнопку "ОК".

   Окно изменения привязки сетевого объекта закроется.
6. Нажмите кнопку "ОК".

   Окно настройки параметров сетевого объекта закроется.

Приложение

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
TCP/22	Передача данных SSH	РМ / СУ
TCP/443	Обмен сообщениями при включенном на АП режиме защищенного соединения "Потоковое подключение (TCP)" или "Подключение через прокси-сервер"	АП / СД. СД / АП
TCP/4431, 1025-65535	Обмен сообщениями. ПУ СД и агент ЦУС и СД устанавливают подключение со случайного порта из диапазона 1025-65535 к СД на порт 4431. СД отвечает с порта 4431 на тот порт компьютера с ПУ СД или с агентом ЦУС и СД, с которого пришло подключение	ПУ СД / СД. СД / ПУ СД. Агент ЦУС и СД / СД. СД / агент ЦУС и СД
TCP/4444	Передача сообщений. ПУ ЦУС, активный и пассивный ЦУС, агент ЦУС и СД, агент обновлений БРП, агент РКН устанавливают подключение со случайного порта 1024-65535 на порт ЦУС 4444. ЦУС отвечает на тот порт, с которого было обращение	ПУ ЦУС / ЦУС. Активный ЦУС / пассивный ЦУС. Пассивный ЦУС / активный ЦУС. Агент ЦУС и СД / ЦУС. ЦУС / агент ЦУС и СД. Аент ЦУС и СД / ЦУС. Агент обновлений БРП / ЦУС. ЦУС / агент обновлений БРП. Агент РКН / ЦУС. ЦУС / агент РКН
TCP/4445	Передача обновлений ПО	ПУ ЦУС / ЦУС
	Обмен сообщениями. ПУ ЦУС устанавливает подключение со случайного порта из диапазона 1024-65535 на порт ЦУС 4445. ЦУС отвечает на тот порт, с которого было обращение	ПУ ЦУС / агент ЦУС и СД. Агент ЦУС и СД / ПУ ЦУС
TCP/4446	Аутентификация хостов 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	Клиент аутентификации / ЦУС. ЦУС / Клиент аутентификации
TCP/5100	Передача сообщений	ЦУС / КШ
	Обмен сообщениями в кластере. Узел кластера обращается к парному со случайного порта из диапазона 10000-65535 на порт 5100. Парный отвечает на тот порт, с которого было обращение	Основной КШ / резервный КШ. Резервный КШ / основной КШ
TCP/5101	Обмен сообщениями. КШ устанавливает подключение со случайного порта 10000-65535 на порт ЦУС 5101. ЦУС отвечает на тот порт, с которого было обращение	КШ / ЦУС. ЦУС / КШ
TCP/5103	Передача файлов. КШ устанавливает подключение со случайного порта 10000-65535 на порт ЦУС 5103. ЦУС отвечает на тот порт, с которого было обращение	ЦУС / КШ. КШ / ЦУС

Протокол/ порт	Описание	Источник/получатель
TCP/5109	Связь ЦУС с узлами (для узлов версии 3.9.1 и выше)	ЦУС / СУ
TCP/7500	Обмен сообщениями. Порт на клиентской стороне фиксирован (7500)	СД / АП. АП / СД
UDP/123	Передача данных синхронизации NTP	ЦУС / внешний NTP-сервер
UDP/161	Передача данных SNMP	РМ администратора / СУ
UDP/514	Отправка системных сообщений на внешний syslog-сервер	СУ / внешний syslog-сервер
UDP/5101	Передача сообщений от КШ к ЦУС. КШ обращается с порта 5100 на порт ЦУС 5101. ЦУС отвечает с порта 5101 на порт 5100	КШ / ЦУС. ЦУС / КШ
UDP/5106 UDP/5107	Поддержка работы КШ за NAT-узлом. В зависимости от используемых классов трафика, КШ отправляют пакеты с портов 10000-10031 на порты ЦУС 5106-5107	КШ / ЦУС
UDP/5109	Связь ЦУС с узлами (для узлов версии 3.9.1 и выше) КШ обращается с порта 5100 на порт ЦУС 5109. ЦУС отвечает с порта 5109 на порт 5100	ЦУС / СУ. СУ / ЦУС
UDP/5557	Обмен сообщениями об активности между КШ в кластере (с порта 5557 на порт 5557)	Основной КШ / резервный КШ. Резервный КШ / основной КШ
UDP/4433	Обмен сообщениями между СД и АП. 4433 порт установлен по умолчанию, изменяется в программе управления СД	АП / СД. СД / АП
UDP/7500	Обмен сообщениями. Порт на клиентской стороне фиксирован (7500)	СД / АП. АП /СД
UDP/10000-10031	Передача зашифрованного трафика. В зависимости от используемых классов трафика, узлы обмениваются пакетами с портов 10000-10031 на соответствующие порты 10000-10031	СУ / СУ. СУ / ЦУС. ЦУС / СУ

Документация

1. Аппаратно-программный комплекс шифрования "Континент". Версия 3.9. Руководство администратора. Управление комплексом.
2. Аппаратно-программный комплекс шифрования "Континент". Версия 3.9. Руководство администратора. Настройка VPN.