КОД безопасности

Аппаратно-программный комплекс шифрования

Континент

Версия 3.9 (исполнение 3.М3)

Руководство администратора

Настройка VPN

RU.88338853.501430.022 03 90 5

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
КК	Криптографический коммутатор (криптокоммутатор)
КШ	Криптографический шлюз (криптошлюз)
ЛВС	Локальная вычислительная сеть
НСД	Несанкционированный доступ
ОС	Операционная система
ПО	Программное обеспечение
ПУ	Программа управления
РМ	Рабочее место
ЦУС	Центр управления сетью
ICMP	Internet Control Message Protocol
IP	Internet Protocol
MTU	Maximum Transmission Unit
NAT	Network Address Translation
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
USB	Universal Serial Bus
VPN	Virtual Private Network

Введение

Документ предназначен для администраторов изделия " Аппаратно- программный комплекс шифрования "Континент". Версия 3.9 (исполнение 3.М3)" (далее — комплекс, АПКШ "Континент"). В нем содержатся общие сведения о принципах построения и порядке настройки VPN "Континент".

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.

Глава 1
Принципы построения VPN

Компоненты VPN

В АПКШ "Континент" для построения сетей VPN используются следующие компоненты:

- криптошлюзы (L3VPN);
- криптокоммутаторы (L2VPN);
- ЦУС;
- программа управления ЦУС (далее — программа управления).

Криптошлюз

Криптошлюз — программное средство, предварительно устанавливаемое на специализированную аппаратную платформу с архитектурой x64 и предназначенное для выполнения следующих функций в сетях L3VPN:

- организация защищенных каналов на сетевом уровне с заданной топологией;
- обеспечение передачи данных на канальном и сетевом уровне;
- трансляция сетевых адресов;
- пакетная фильтрация;
- регистрация событий безопасности, управления и системных событий.

Криптографический коммутатор

Криптографический коммутатор представляет собой программное средство, предварительно устанавливаемое на специализированную аппаратную платформу с архитектурой x64.

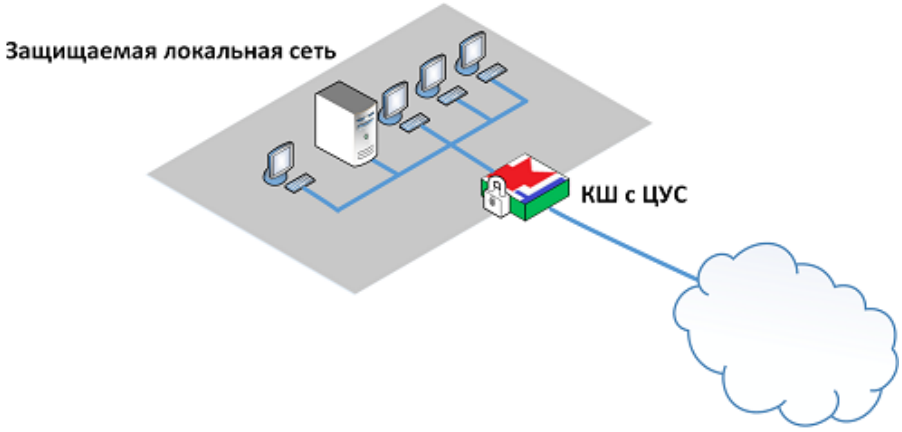
Криптографический коммутатор обеспечивает защищенную передачу Ethernet-кадров (L2) через сети общего пользования между территориально разделенными сегментами сети предприятия с использованием шифрованных (L3) VPN-туннелей "Континент" (L2VPN).

Центр управления сетью

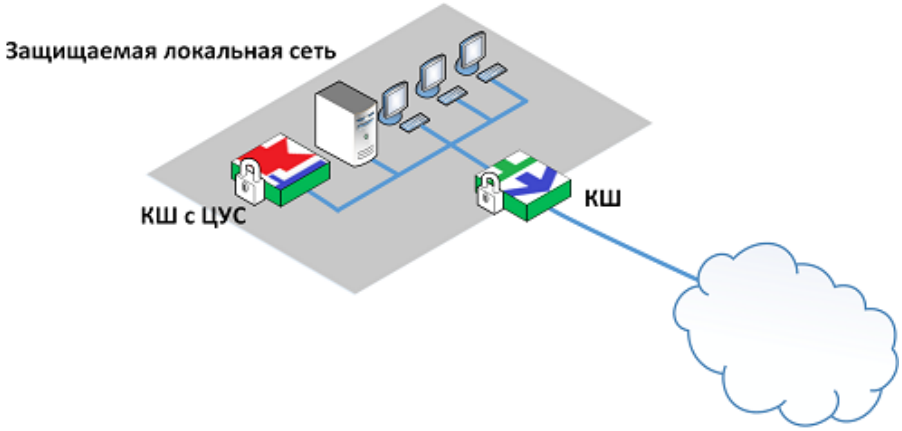
ЦУС — программное средство, предназначенное для настройки и централизованного управления работой сетевых устройств комплекса, участвующих в работе VPN. В функции ЦУС входит также контроль работы и состояния сетевых устройств, включая передачу необходимых сведений в систему мониторинга и аудита АПКШ "Континент".

ЦУС устанавливают на один из криптошлюзов сети VPN. При этом возможны два варианта расположения ЦУС:

- ЦУС устанавливают на КШ, защищающий локальную вычислительную сеть и играющий роль шлюза.



- ЦУС устанавливают на КШ, расположенный внутри защищаемой сети.



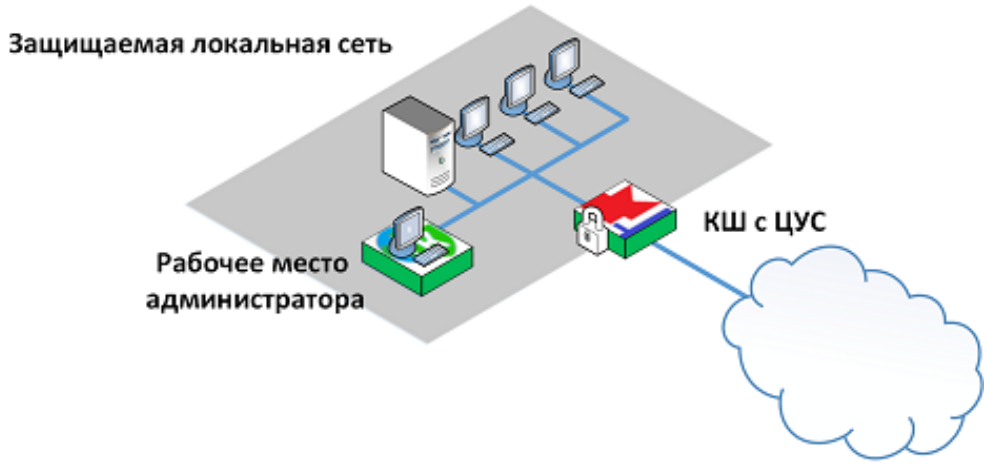
Второй вариант является предпочтительным, так как снимает с КШ, работающего как шлюз, нагрузку, связанную с выполнением функций ЦУС.

ЦУС имеет в своем составе базу данных, в которой хранятся все настройки АПКШ "Континент", в том числе настройки VPN. В эту же базу данных поступают сведения о состоянии криптошлюзов.

Программа управления ЦУС

Программа управления ЦУС — программа, устанавливаемая на рабочем месте администратора комплекса и предназначенная для централизованной настройки сети VPN и межсетевого экрана.

Как правило, рабочее место администратора располагается в сети, защищенной КШ с ЦУС.



В программе управления администратором задаются и настраиваются все элементы создаваемой сети VPN и связи между ними. Настройки хранятся в базе данных ЦУС.

Программу управления устанавливают при вводе комплекса в эксплуатацию после инициализации ЦУС.

Для работы с программой управления необходимо предъявить идентификатор администратора.

Объекты ЦУС

Для построения маршрутов и составления правил фильтрации, действующих в рамках VPN, используются элементы, называемые объектами ЦУС. Такими объектами являются:

- сетевые объекты и группы сетевых объектов;
- сервисы;
- временные интервалы.

Сетевой объект — логический элемент, идентифицирующий какой-либо из элементов локальной сети, а именно: хост (рабочая станция), подсеть, диапазон адресов. Сетевые объекты используются при построении маршрутов, а также в правилах фильтрации и трансляции для определения отправителя или получателя IP-пакетов.

Сервис — логический элемент, идентифицирующий какой-либо из шаблонов характеристик соединений в локальной сети. Используется в правилах фильтрации и трансляции для определения характеристик IP- пакетов, к которым следует применять правило. К этим характеристикам относятся протокол (TCP, UDP, ICMP или номер протокола), диапазоны портов отправителя и получателя (для TCP и UDP), тип и код ICMP-сообщения.

Временной интервал — расписание или интервал времени, в течение которого должно действовать правило фильтрации или трансляции.

Создание объектов ЦУС и настройку их параметров выполняет главный администратор комплекса в программе управления ЦУС.

Более подробные сведения об объектах ЦУС приводятся в [**4**].

Межсетевой экран

В АПКШ "Континент" криптошлюзы помимо функций шифрования выполняют функции межсетевого экранирования.

Политика межсетевого экранирования в VPN описывает:

- интерфейсы, направленные в интернет;
- интерфейсы, направленные во внутренние (локальные) сети;
- расписание, ограничивающее время работы VPN;
- типы данных, которые могут передаваться.

Политика межсетевого экранирования для каждого криптошлюза задается в виде списка правил фильтрации. Поэтому для прохождения трафика в туннеле необходимо, чтобы настройки, выполненные для криптошлюза в рамках VPN, соответствовали политике межсетевого экранирования.

Зашифрование и расшифрование данных криптошлюзом начинается автоматически после проверки первого пакета на соответствие всем условиям политики межсетевого экранирования.

Планирование построения VPN

Чтобы сэкономить время и правильно настроить VPN, рекомендуется заранее спланировать конфигурацию VPN. Конфигурация VPN включает в себя ряд обязательных и дополнительных параметров. Предварительно необходимо определить:

- источники и получатели IP-трафика;
- хосты, серверы и локальные сети, которые должны быть включены в VPN;
- сетевые устройства, включаемые в конфигурацию;
- интерфейсы, через которые подключаются сетевые устройства;
- интерфейсы, через которые локальные сети получают доступ к VPN-шлюзам.

После сбора приведенной выше информации можно выбрать наиболее подходящую топологию сети VPN.

Конфигурация VPN определяет взаимодействие между криптошлюзами и хостами, серверами или локальными сетями, которые образуют сеть VPN. Для конфигурирования VPN необходимо определить:

- Частные IP-адреса для трафика, генерируемого сетевыми объектами (хостами, серверами и подсетями). Эти адреса представляют собой адреса источников, которым разрешена передача трафика в VPN. IP-адресом источника может быть индивидуальный адрес, диапазон адресов или адрес подсети.
- IP-адреса внешних интерфейсов криптошлюзов. Криптошлюзы устанавливают туннели между собой по этим интерфейсам.
- IP-адреса внутренних интерфейсов криптошлюзов. Сетевые объекты в защищаемых сетях будут соединяться со своими криптошлюзами этими интерфейсами.

Лицензии

Для функционирования VPN необходимо наличие зарегистрированной лицензии на все криптошлюзы комплекса, входящие в VPN, включая КШ с ЦУС.

Лицензии на введенные в эксплуатацию криптошлюзы являются накопительными. Общее количество разрешенных к использованию объектов определяется суммой объектов, указанных в каждой лицензии.

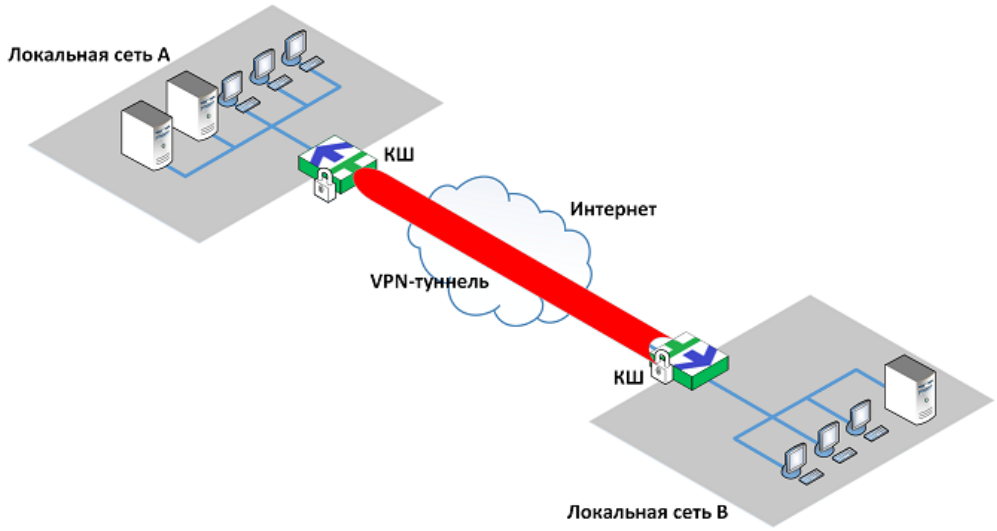
Подробные сведения об управлении лицензиями приводятся в [**3**].

VPN-туннель

В АПКШ "Континент" технология VPN подразумевает создание защищенных каналов (туннелей) между двумя сетевыми устройствами — криптошлюзами. За каждым из сетевых устройств расположена локальная сеть или сегмент сети. При передаче трафика из одной защищаемой сети в другую сетевые устройства выполняют зашифрование данных до того, как они попадут в туннель, и расшифрование этих данных после того, как они туннель покинут.

В АПКШ "Континент" используется симметричная криптографическая система. Криптографическое соединение между двумя КШ в сети осуществляется на ключах парной связи. Зашифрование каждого IP-пакета производится на индивидуальном ключе — ключе шифрования пакета, который формируется из ключа парной связи. Для зашифрования данных используется алгоритм ГОСТ 28147-89 в режиме гаммирования с обратной связью. Имитозащита данных осуществляется с использованием алгоритма ГОСТ 28147-89 в режиме имитовставки.

На рисунке ниже показаны две локальные сети. На периметре каждой из них установлен криптошлюз. Связь между сетями осуществляется по общедоступным каналам (например, по сети интернет).



Хосты локальной сети A и хосты локальной сети B обмениваются данными, используя туннель между криптошлюзами:

- хост из локальной сети A посылает пакеты хосту, расположенному в сети B;
- криптошлюзы соединяются друг с другом и создают туннель;
- КШ сети A зашифровывает передаваемые пакеты и отправляет их по туннелю;
- КШ сети B расшифровывает данные и передает их хосту-получателю;
- хост получателя в сети B получает расшифрованные данные.

Аналогично происходит передача пакетов в обратном направлении, когда какой-либо из хостов локальной сети B инициирует обмен данными с хостом сети A.

Зашифрование пакетов данных предотвращает доступ к данным при перехвате пакетов третьей стороной.

IP-адрес криптошлюза — это, как правило, IP-адрес сетевого интерфейса, направленного в интернет.

Несмотря на то что IP-трафик в действительности проходит через различные маршрутизаторы, расположенные в интернете, можно говорить о том, что VPN-туннель — это просто безопасное соединение между двумя криптошлюзами.

Для пользователей локальных сетей A и B наличие VPN-туннеля не предъявляет никаких дополнительных требований. Приложения на их компьютерах так же, как и обычно, генерируют пакеты с соответствующими адресами отправителя и получателя. Все функции, связанные с зашифрованием, инкапсулированием и отправкой пакетов, выполняют криптошлюзы.

Зашифрованные данные передаются только внутри туннеля между двумя криптошлюзами. Между компьютером пользователя и криптошлюзом данные передаются в незашифрованном виде.

Один криптошлюз может поддерживать создание одновременно нескольких туннелей, а каждый туннель может обеспечивать одновременно более чем одно соединение.

Глава 2
Развертывание L3VPN

Предварительные замечания

Перед началом настройки и ввода VPN в эксплуатацию необходимо убедиться в выполнении следующих условий:

- Выполнена инициализация ЦУС.

  Инициализацию ЦУС выполняют в полном соответствии с указаниями, приведенными в [**3**].
- На рабочем месте администратора установлена ПУ ЦУС и настроено соединение с ЦУС.

  Описание программы управления и ее настройка описаны в [**2**] и [**3**].
- Криптошлюзы, входящие в состав VPN, зарегистрированы в программе управления, проинициализированы и введены в эксплуатацию.

  Регистрацию, инициализацию и ввод криптошлюзов в эксплуатацию выполняют в соответствии с общим порядком развертывания сетевых устройств (см. [**3**]).

Примечание. Общее количество криптошлюзов, введенных в эксплуатацию, включая КШ с ЦУС, должно соответствовать требованиям политики лицензирования.

Порядок развертывания L3VPN

Развертывание защищенной корпоративной сети включает в себя последовательное выполнение следующих этапов:

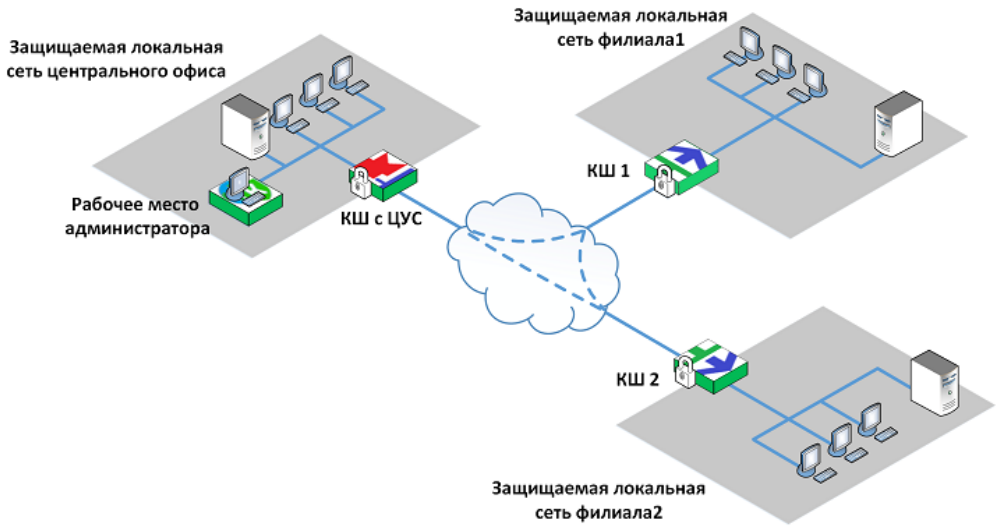
1. Настройка интерфейсов криптошлюзов и ЦУС (см. следующий подраздел).
2. Создание объектов ЦУС (см. стр. **16**).
3. Установление парных связей между криптошлюзами (см. стр. **27**).
4. Настройка параметров маршрутизации (см. стр. **32**).
5. Создание правил фильтрации (см. стр. **37**).
6. Проверка работоспособности настроенных VPN-каналов (см. стр. **39**).

Настройка интерфейсов

Рассмотрим построение L3VPN для корпоративной сети предприятия, объединяющей локальные сети центрального офиса и двух филиалов.

Для построения VPN будут использованы следующие компоненты, входящие в состав комплекса:

- криптошлюзы (на рисунке ниже — КШ 1 и КШ 2);
- центр управления сетью, установленный на КШ, защищающем локальную сеть центрального офиса;
- программа управления ЦУС, установленная на рабочем месте администратора в защищенной сети центрального офиса.

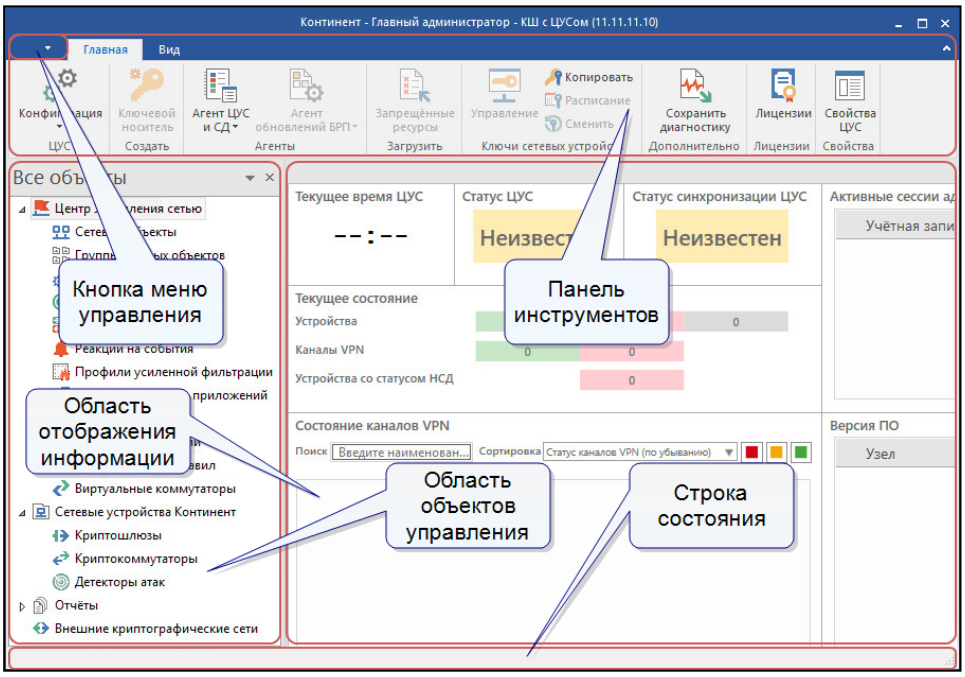


Настройка интерфейсов выполняется в программе управления ЦУС для каждого зарегистрированного криптошлюза.

Для настройки интерфейсов:

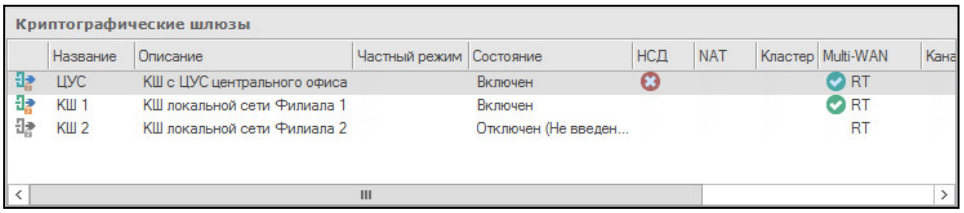
1. Запустите программу управления ЦУС.

   На экране появится главное окно ПУ ЦУС.



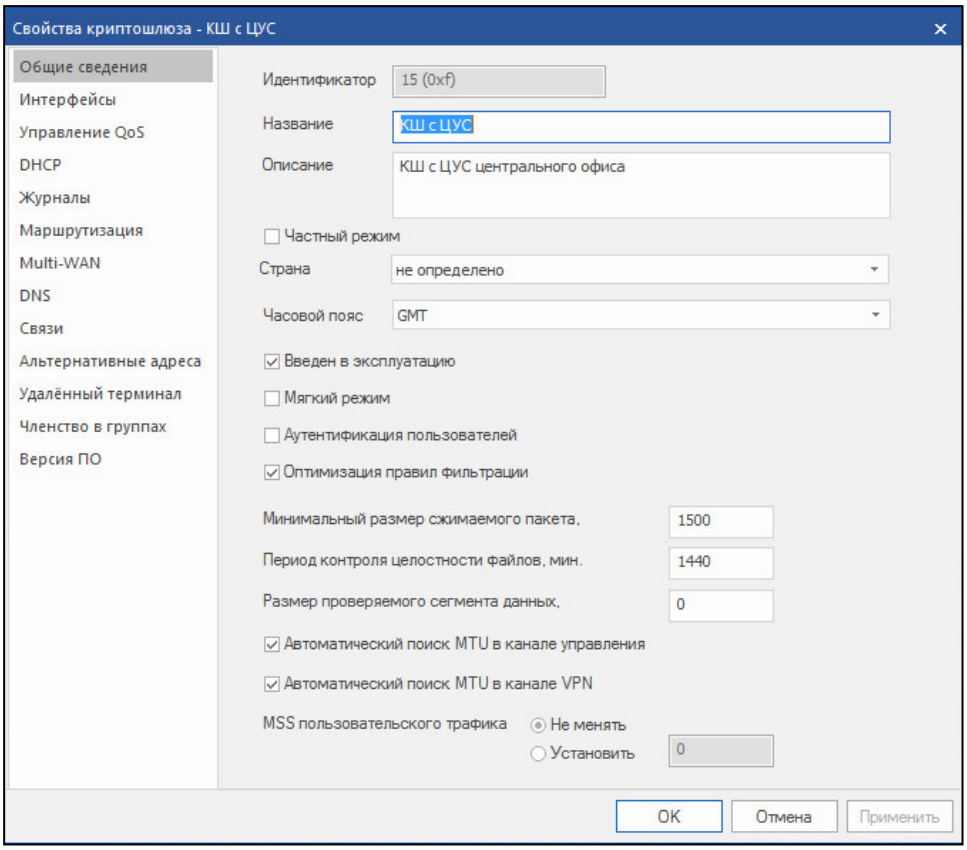
2. Выберите в левой части окна раздел "Сетевые устройства Континент" и в нем — пункт "Криптошлюзы".

   В области отображения информации появится список зарегистрированных криптошлюзов. Ниже представлен список криптошлюзов, соответствующий схеме на стр. **13**.



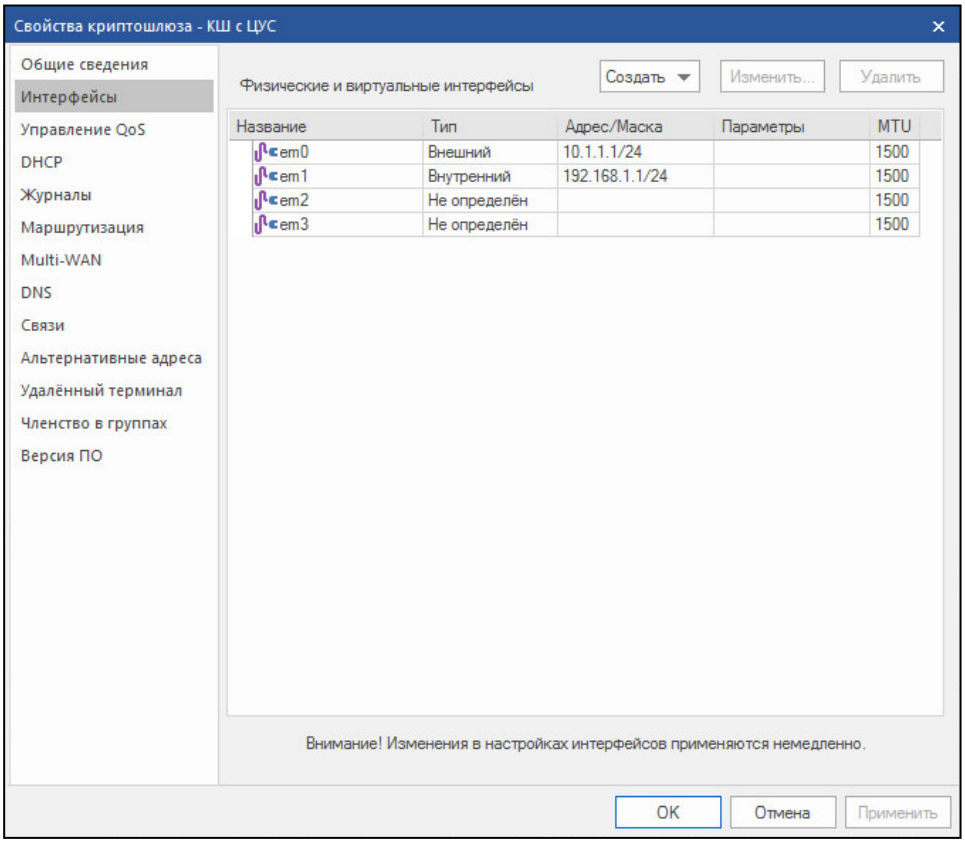
3. Выберите в списке криптошлюз и в панели инструментов нажмите кнопку "Свойства". В качестве примера выбран КШ с ЦУС.

На экране появится окно "Свойства криптошлюза".



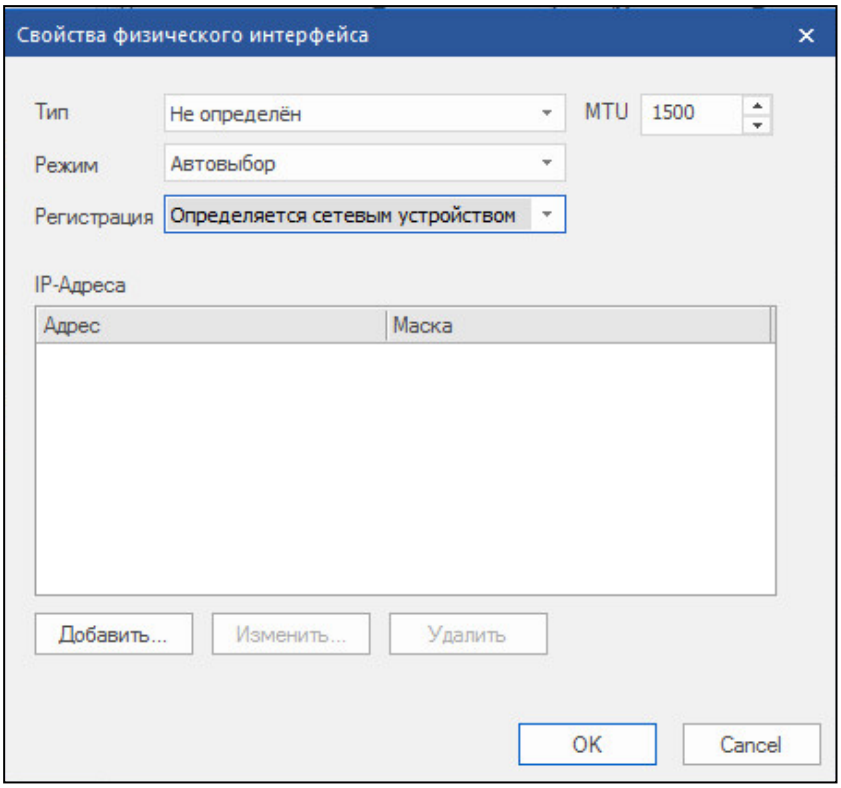
4. В левой части окна выберите вкладку "Интерфейсы".

В правой части окна появится список интерфейсов криптошлюза.



5. Настройте параметры используемых интерфейсов. Для этого выберите интерфейс в списке и нажмите кнопку "Изменить...".

   На экране появится окно "Свойства физического интерфейса".



6. Укажите значения параметров интерфейса.

Параметр	Описание
Тип	Тип интерфейса (внешний или внутренний): • Внешний — интерфейс, подключаемый к сетям общего пользования. • Внутренний — интерфейс, подключаемый к защищаемой сети
MTU	Максимальная единица передачи данных (в байтах). Допустимые значения: • для КШ (внутренние и внешние интерфейсы) 576–9000; • для КК (внешний интерфейс) 576–9100
Режим	Режим работы сетевой карты
Регистрация	Задание правила регистрации событий в журналах. Значения: • Определяется сетевым устройством (правило наследуется из свойств сетевого устройства); • Первые 64 байта; • Тело пакета
IP-адреса	Список IP-адресов интерфейса. Для добавления нового адреса нажмите кнопку "Добавить", укажите IP-протокол (IPv4 или IPv6; IPv6 используется только для внешних интерфейсов) и далее введите адрес и маску (префикс для IPv6). Для удаления выбранного IP-адреса используйте кнопку "Удалить"

7. Для сохранения заданных параметров нажмите кнопку "OK" в нижней части окна "Свойства физического интерфейса".

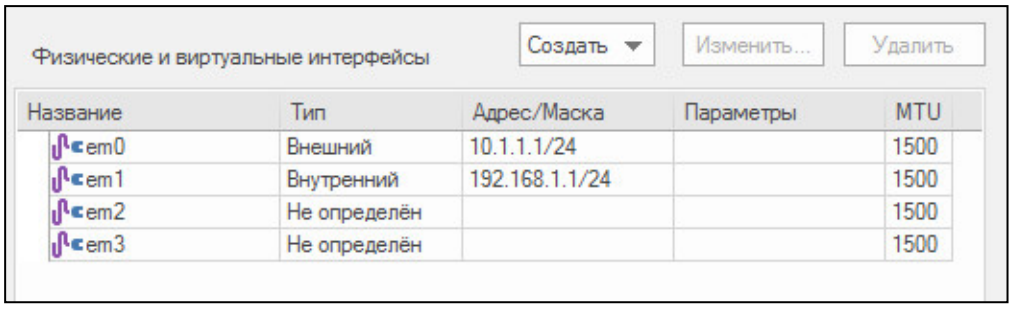
   Окно закроется и заданные значения параметров отобразятся в списке интерфейсов криптошлюза.

8. Выберите следующий интерфейс и настройте его параметры (см. пп. **4–6**).

9. После настройки всех интерфейсов нажмите кнопку "OK" или "Применить" в нижней части окна "Свойства криптошлюза".

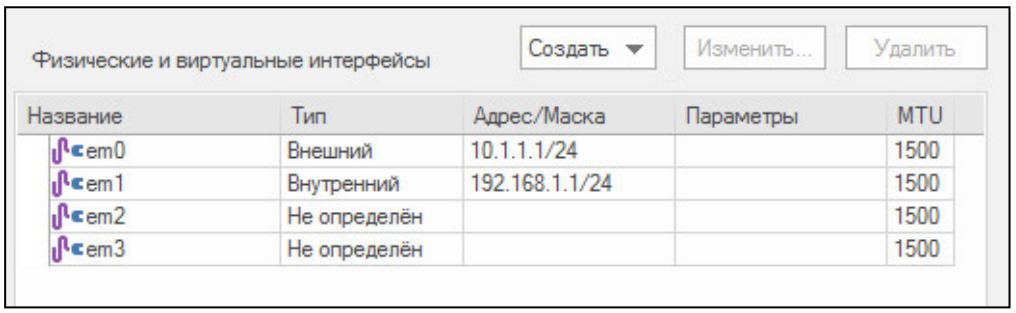
Ниже приведены настройки интерфейсов криптошлюзов для схемы, приведенной на стр. **13**.

КШ с ЦУС:



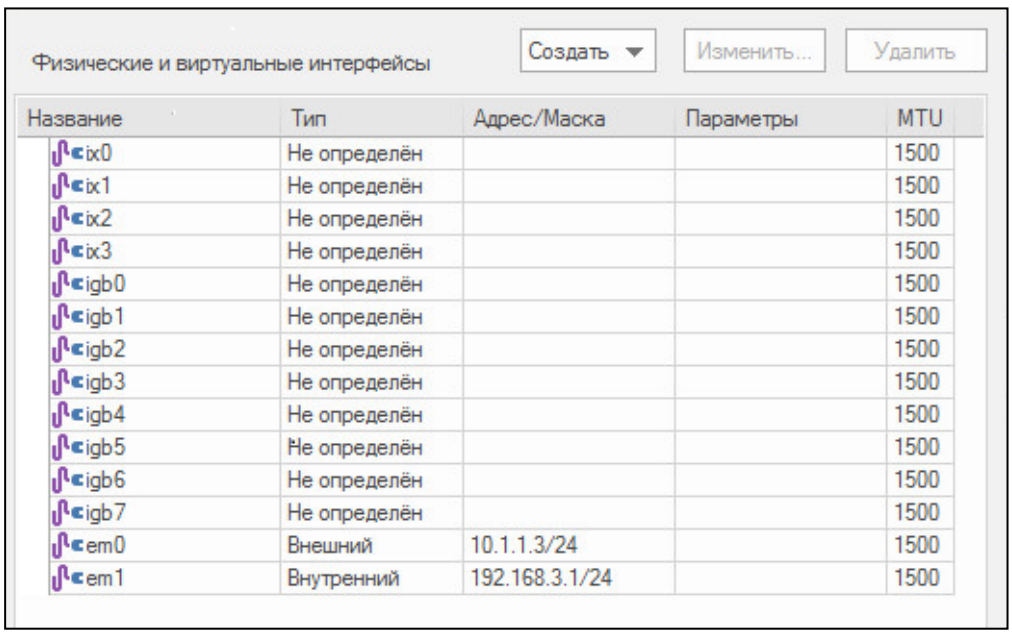
Название	Тип	Адрес/Маска	Параметры	MTU
em0	Внешний	10.1.1.1/24		1500
em1	Внутренний	192.168.1.1/24		1500
em2	Не определён			1500
em3	Не определён			1500

КШ 1:



Название	Тип	Адрес/Маска	Параметры	MTU
em0	Внешний	10.1.1.1/24		1500
em1	Внутренний	192.168.1.1/24		1500
em2	Не определён			1500
em3	Не определён			1500

КШ 2:



Название	Тип	Адрес/Маска	Параметры	MTU
ix0	Не определён			1500
ix1	Не определён			1500
ix2	Не определён			1500
ix3	Не определён			1500
igb0	Не определён			1500
igb1	Не определён			1500
igb2	Не определён			1500
igb3	Не определён			1500
igb4	Не определён			1500
igb5	Не определён			1500
igb6	Не определён			1500
igb7	Не определён			1500
em0	Внешний	10.1.1.3/24		1500
em1	Внутренний	192.168.3.1/24		1500

Создание объектов ЦУС

В данном подразделе приводится описание процедур создания сетевых объектов, сервисов и временных интервалов, которые будут использоваться в правилах фильтрации и при создании маршрутов в VPN "Континент".

Сетевые объекты

Для вызова списка сетевых объектов:

- В левой части окна ПУ ЦУС (см. стр. **13**) выберите пункт "Центр управления сетью | Сетевые объекты".

  В правой части окна отобразится перечень сетевых объектов.

Создание и удаление сетевых объектов, а также настройка их параметров осуществляются в этом окне.

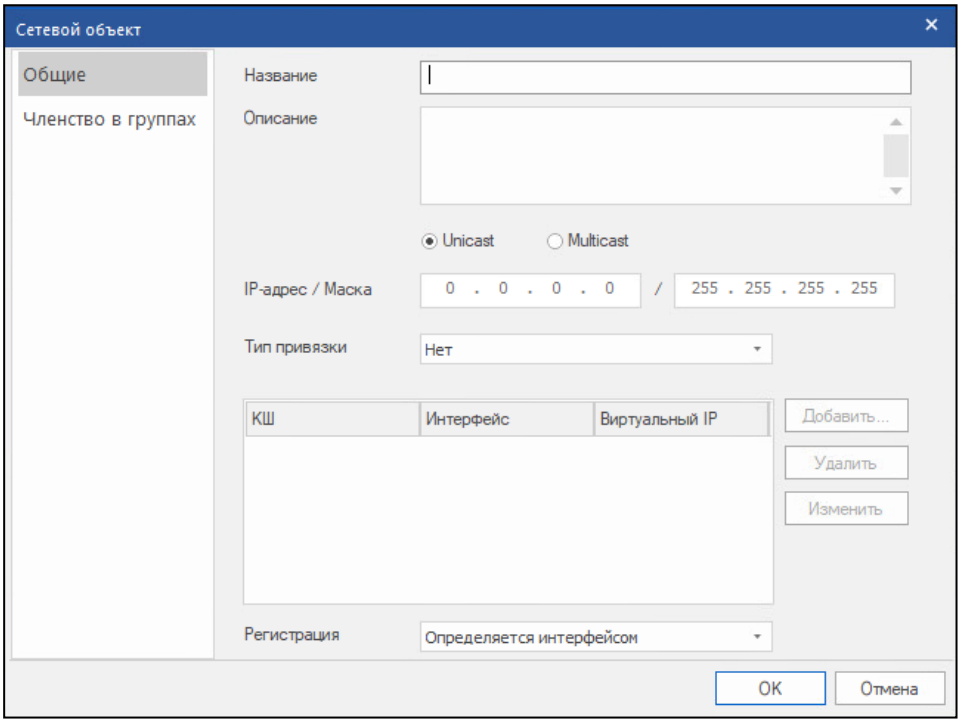
Объект "Любой", имеющий IP-адрес "0.0.0.0" и определяющий сеть в диапазоне всех известных IP-адресов, создается автоматически при инициализации ЦУС.

Для создания сетевого объекта:

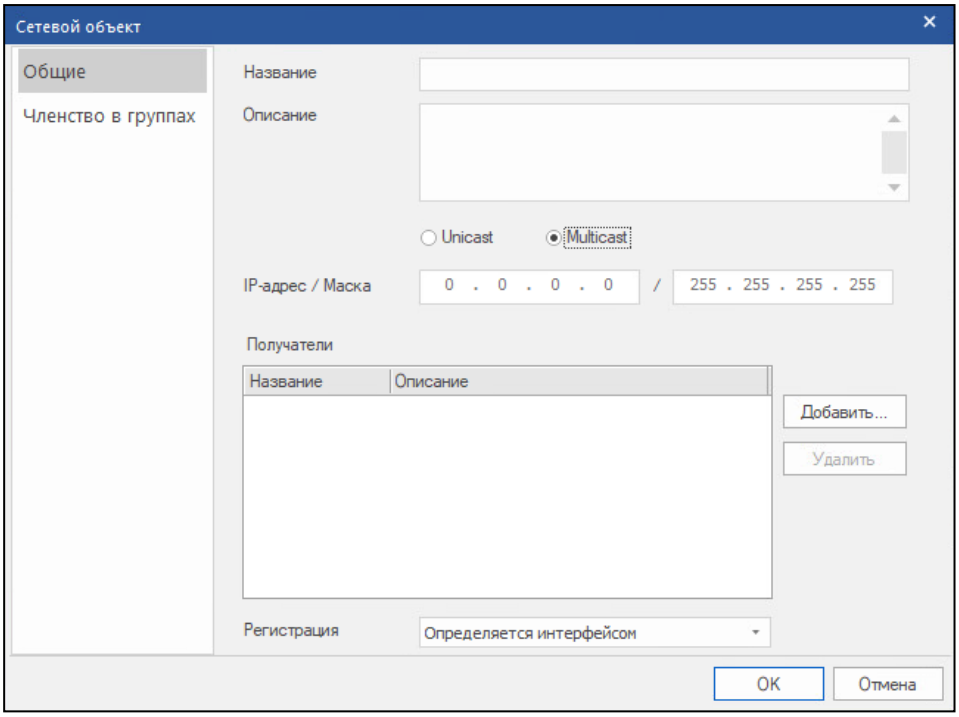
1. Вызовите список сетевых объектов.
2. В панели инструментов нажмите кнопку "Создать сетевой объект".

   На экране появится окно настройки параметров сетевого объекта.

Примечание. Окно настройки можно вызвать с помощью контекстного меню. Для этого установите курсор в свободное место списка и нажмите правую кнопку мыши.



На рисунке выше показано окно настройки для сетевого объекта типа Unicast. Для объекта типа Multicast окно настройки показано на рисунке ниже.



3. Заполните поля на вкладке "Общие".

Поле	Описание
Название	Уникальное наименование сетевого объекта
Описание	Дополнительные сведения (необязательный параметр)
Unicast	Однонаправленная передача данных (сетевой пакет направляется одному адресату)
Multicast	Групповая передача данных (сетевой пакет одновременно направляется определенной группе адресатов)
IP-адрес	IP-адрес сегмента сети или отдельного компьютера
Маска	Маска сети. Все значимые биты адреса должны покрываться маской. Например, если поле "IP-адрес" содержит значение "134.17.11.0", то значение маски может равняться "255.255.255.0", но не может быть равно "255.255.0.0". Если указано значение "255.255.255.255" — задана сеть из одного компьютера, IP-адрес которого определяется значением поля "IP-адрес"

4. Если тип создаваемого сетевого объекта Unicast, перейдите к п. **5**.

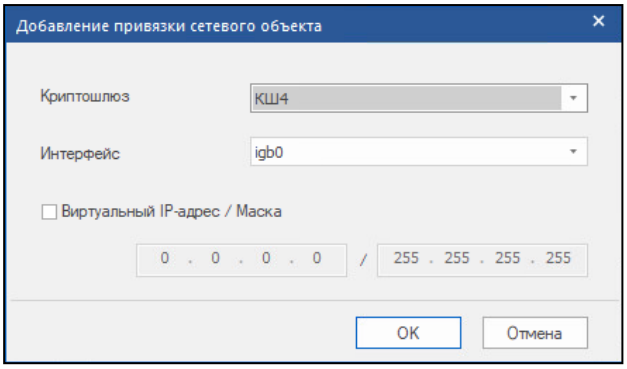
Если тип создаваемого сетевого объекта Multicast, перейдите к п.**11**.

5. Выполните привязку создаваемого сетевого объекта к криптошлюзу. Для этого выберите 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.

6. Нажмите кнопку "Добавить". Кнопка доступна только для типов привязки "Внутренний" и "Защищаемый".

Появится окно для задания параметров привязки.



7. Выберите из раскрывающегося списка криптошлюз, на котором должны выполняться правила фильтрации с упоминанием данного сетевого объекта (список содержит все зарегистрированные в БД ЦУС криптошлюзы).

   Внимание! Шифрование трафика будет выполняться только при включении данного КШ в список связанных КШ (см. стр. **27**).

8. Выберите из раскрывающегося списка интерфейс указанного КШ.

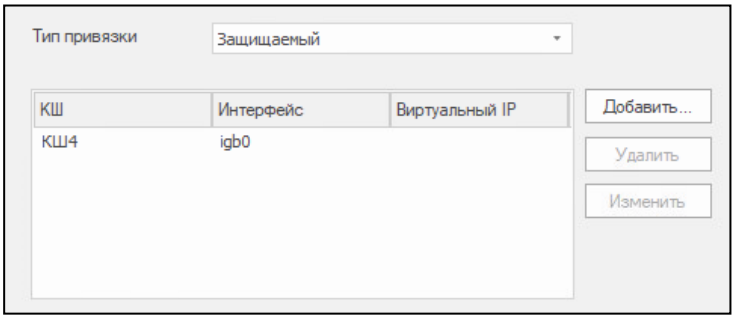
   Фильтрации будут подлежать только те IP-пакеты, которые проходят через этот интерфейс указанного криптошлюза (только для типов привязки "Внутренний" и "Защищаемый"). При выборе значения "Любой" фильтрации будут подвергаться IP-пакеты, проходящие через любой интерфейс.

   Внимание! Если в поле "Тип привязки" указано значение "Защищаемый", не рекомендуется использовать внешний интерфейс КШ.

9. Если необходимо использовать виртуальный IP-адрес, присвоенный данному интерфейсу, установите соответствующую отметку и введите IP-адрес и маску (только для типа привязки "Защищаемый").

   Далее нажмите кнопку "OK".

   Привязка отобразится в окне настройки параметров создаваемого сетевого устройства.



10. Если необходимо выполнить привязку данного сетевого объекта к другим КШ, повторите выполнение пп. **6**–**9** и далее перейдите к п. **12**.
11. Для создаваемого сетевого объекта типа Multicast укажите получателей — перечень КШ, которые должны участвовать в групповой передаче. Для этого нажмите кнопку "Добавить" и выберите КШ из общего списка криптошлюзов.
12. Задайте правило регистрации событий в журналах. Доступные значения:
    - Определяется интерфейсом;
    - Первые 64 байта;
    - Тело пакета.
13. Если необходимо включить данный сетевой объект в группу/группы, перейдите к вкладке "Членство в группах" и сформируйте список групп, членом которых будет являться данный объект (о создании групп см. стр. **20**).

Используйте кнопки:

Добавить	Вызывает на экран перечень зарегистрированных групп сетевых объектов
Удалить	Удаляет выбранную в списке группу

14. Нажмите кнопку "ОК".

Для удаления сетевого объекта:

1. Вызовите список сетевых объектов.
2. Вызовите контекстное меню удаляемого сетевого объекта и активируйте команду "Удалить выделенные...".

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

   На экране появится предупреждение об удалении правил фильтрации для этого объекта.

   Примечание. При подтверждении удаления будут удалены только те правила фильтрации и правила трансляции, которые используют этот объект непосредственно. Правила фильтрации для групп, содержащих удаляемый объект, удалены не будут.
4. Нажмите кнопку "Да".

   Объект будет удален из списка немедленно, а сведения о нем — из базы данных ЦУС без возможности восстановления.

Группы сетевых объектов

Для создания группы сетевых объектов:

1. В левой части окна программы управления выберите пункт "Центр управления сетью | Группы сетевых объектов".

   В правой части окна отобразится список групп сетевых объектов. Если группы не создавались, в списке будет представлена только группа "Реестр запрещенных ресурсов", созданная по умолчанию.
2. В панели инструментов нажмите кнопку "Создать группу сетевых объектов".

   На экране появится окно настройки параметров создаваемой группы.
3. Введите название и краткое описание создаваемой группы.
4. Сформируйте список входящих в группу сетевых объектов. Для этого используйте кнопки "Добавить" и "Удалить".
5. Укажите правило регистрации событий в журналах. Доступные значения:
   - Определяется интерфейсом;
   - Первые 64 байта;
   - Тело пакета.
6. Для завершения настройки параметров группы нажмите кнопку "ОК".

   Окно настройки параметров закроется и в списке появится новая группа.

Для редактирования свойств группы:

1. Вызовите в окне объектов контекстное меню нужной группы и выберите команду "Свойства...".

   На экране появится окно настройки параметров группы.
2. Внесите необходимые изменения и нажмите кнопку "ОК".

Для удаления группы:

1. Вызовите в окне объектов контекстное меню нужной группы и выберите команду "Удалить выделенные...".

   На экране появится запрос на удаление.
2. Нажмите кнопку "Да".

Примечание. При удалении группы сетевых объектов, которые используются в правилах фильтрации или трансляции, на экране появится предупреждение об удалении правил для этой группы. Нажмите кнопку "Да" для удаления группы вместе с правилами. Кнопка "Нет" отменяет удаление группы.

Группа будет удалена из списка немедленно, а сведения о ней — из базы данных ЦУС без возможности восстановления. При этом объекты, которые входили в эту группу, не будут удалены.

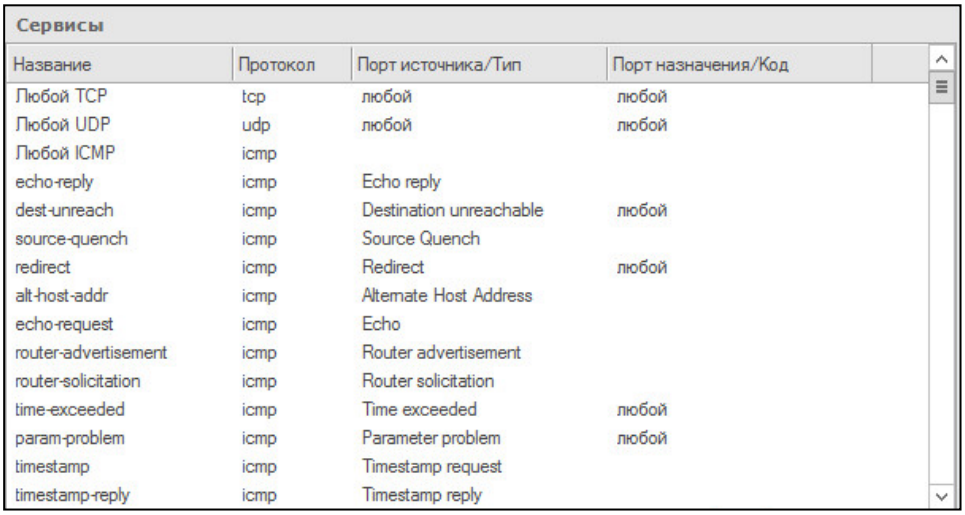
Сервисы

При установке ПО ЦУС в базе данных автоматически создается список наиболее часто используемых сервисов. При необходимости можно создавать новые сервисы и добавлять их в список. Сервисы можно объединять в группы.

Для вызова списка сервисов:

- В левой части окна программы управления выберите пункт "Центр управления сетью | Сервисы".

  В правой части окна отобразится список сервисов.

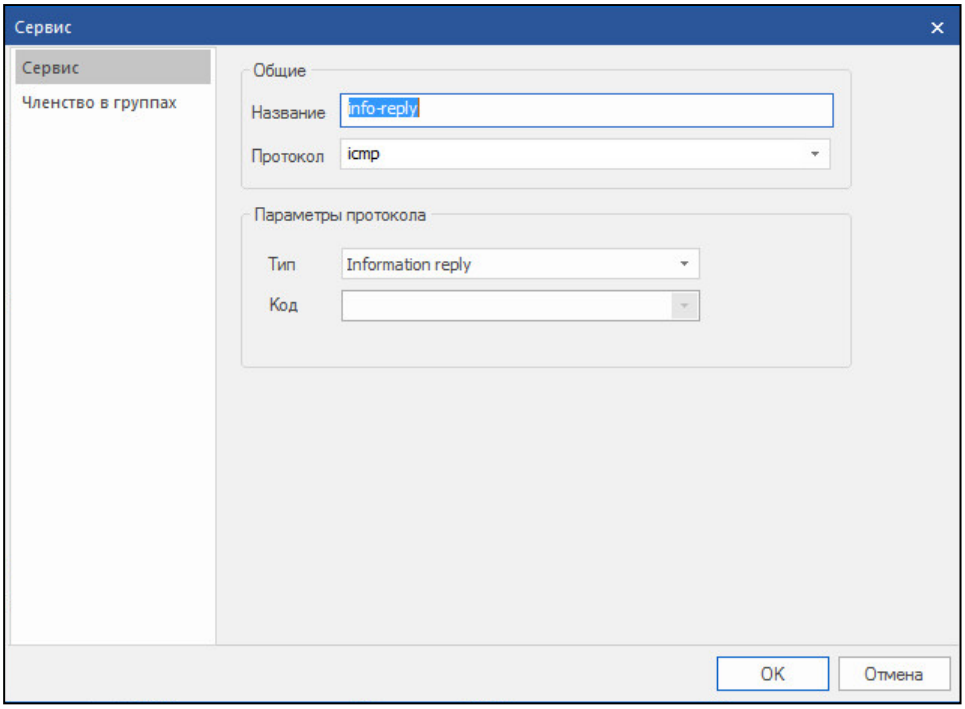

Сервисы

Название	Протокол	Порт источника/Тип	Порт назначения/Код
Любой TCP	tcp	любой	любой
Любой UDP	udp	любой	любой
Любой ICMP	icmp		
echo-reply	icmp	Echo reply	
dest-unreach	icmp	Destination unreachable	любой
source-quench	icmp	Source Quench	
redirect	icmp	Redirect	любой
alt-host-addr	icmp	Alternate Host Address	
echo-request	icmp	Echo	
router-advertisement	icmp	Router advertisement	
router-solicitation	icmp	Router solicitation	
time-exceeded	icmp	Time exceeded	любой
param-problem	icmp	Parameter problem	любой
timestamp	icmp	Timestamp request	
timestamp-reply	icmp	Timestamp reply	

Для просмотра параметров сервиса:

- Выберите сервис в списке и нажмите в панели инструментов кнопку "Свойства" (или используйте одноименную команду контекстного меню).

  На экране появится окно настройки параметров сервиса.



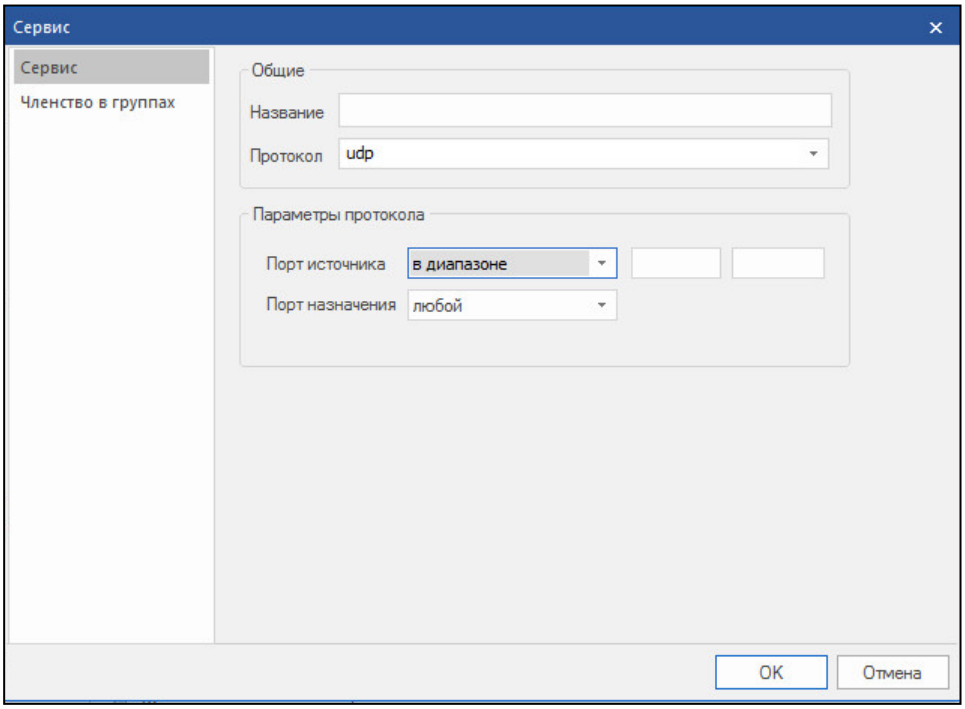
Окно содержит две вкладки: "Сервис" и "Членство в группах".

- Вкладка "Сервис" предназначена для отображения и настройки параметров.
- Вкладка "Членство в группах" предназначена для отображения групп, в которые входит данный сервис, а также для включения сервиса в группу/ исключения сервиса из группы.

Для создания нового сервиса:

1. Вызовите список сервисов и в панели инструментов нажмите кнопку "Создать сервис".

   На экране появится окно настройки параметров сервиса.



2. Введите название создаваемого сервиса и укажите протокол, выбрав его из списка.

3. В зависимости от выбранного протокола укажите его параметры:
   - для протоколов tcp и udp укажите порт источника и порт назначения;
   - для протокола icmp укажите тип и код (в зависимости от типа).
4. Если необходимо включить сервис в группу, перейдите на вкладку "Членство в группах" и добавьте группу или группы, в которые должен входить данный сервис. Для этого используйте кнопки "Добавить" и "Удалить".
5. Для завершения настройки нажмите кнопку "ОК".

   Окно настройки параметров закроется, и в списке появится новый сервис.

Для создания новой группы сервисов:

1. Вызовите список сервисов и в панели инструментов нажмите кнопку "Создать группу сервисов".

   На экране появится окно "Группа сервисов".
2. Введите название группы и с помощью кнопок "Добавить" и "Удалить" сформируйте список сервисов, которые должны входить в данную группу.
3. После завершения формирования списка нажмите кнопку "ОК".

   Новая группа отобразится в левой части главного окна в пункте "Центр управления сетью | Сервисы". При выделении группы в правой части окна отобразится список сервисов, входящих в данную группу.

Для изменения параметров сервиса/группы сервисов:

1. Выберите объект в списке и в панели инструментов нажмите кнопку "Свойства" (или используйте одноименную команду контекстного меню).

   На экране появится окно настройки параметров сервиса.
2. Внесите необходимые изменения и нажмите кнопку "Применить".

Для удаления сервиса/группы сервисов:

1. Для удаления сервиса выберите его в списке и в панели инструментов нажмите кнопку "Удалить сервис" (или используйте команду контекстного меню).

   Для удаления группы выберите ее в пункте "Центр управления сетью | Сервисы", вызовите контекстное меню и выберите команду "Удалить группу сервисов".

   На экране появится запрос на удаление.
2. Нажмите кнопку "Да".

   Примечание. При удалении группы сетевых объектов, которые используются в правилах фильтрации или трансляции, на экране появится предупреждение об удалении правил для этой группы. Нажмите кнопку "Да" для удаления группы вместе с правилами. Кнопка "Нет" отменяет удаление группы.

   Группа будет удалена из списка немедленно, а сведения о ней — из базы данных ЦУС без возможности восстановления. При этом объекты, которые входили в эту группу, не будут удалены.

Временные интервалы

Для вызова списка временных интервалов:

- В левой части окна программы управления выберите пункт "Центр управления сетью | Временные интервалы".

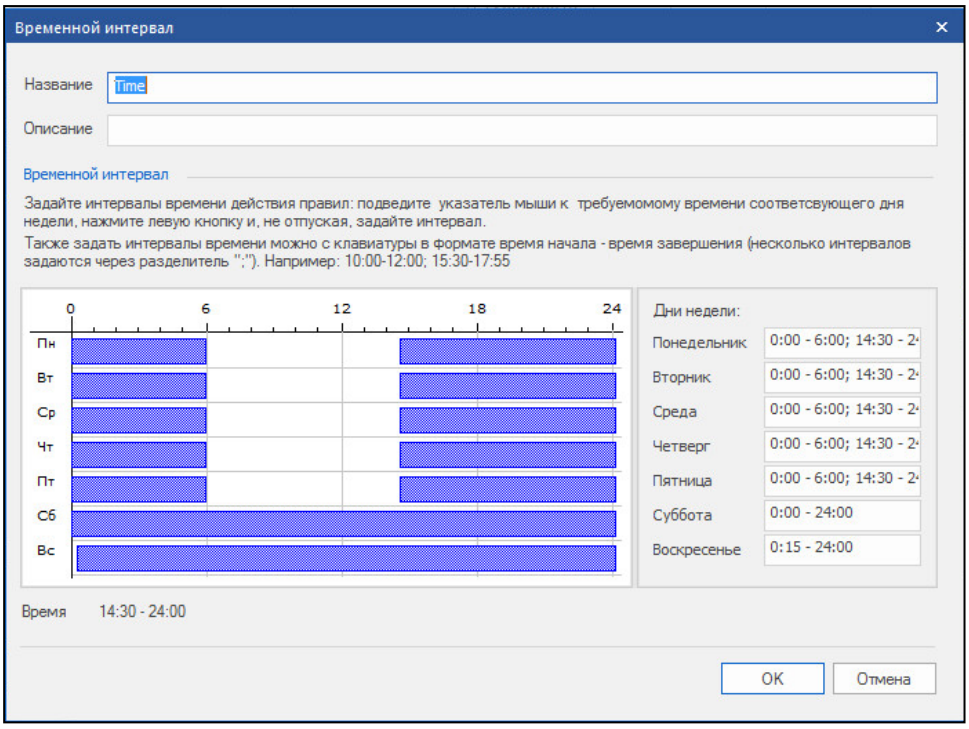
  В правой части окна отобразится перечень временных интервалов.

  Примечание. Если временные интервалы не создавались, по умолчанию присутствует интервал "Постоянно".

Для создания временного интервала:

1. Вызовите список временных интервалов.
2. В панели инструментов нажмите кнопку "Создать временной интервал".

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 правила — 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 ";".

   Внимание! Время, указанное в настройках интервалов, соответствует времени по Гринвичу (GMT). Поэтому при настройке временных интервалов необходимо вводить поправку, учитывающую часовой пояс, в котором должны действовать правила фильтрации.

5. Нажмите кнопку "OK".

   В списке появится имя нового временного интервала.

Для изменения параметров временного интервала:

1. Вызовите список временных интервалов.
2. Выделите в списке требуемый временной интервал и в панели инструментов нажмите кнопку "Свойства".

   На экране появится окно настройки параметров временного интервала.
3. Введите необходимые изменения в соответствии с описанной выше процедурой и нажмите кнопку "OK".

Для удаления временного интервала:

Внимание! Перед удалением временного интервала его необходимо исключить из правил фильтрации и трансляции.

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

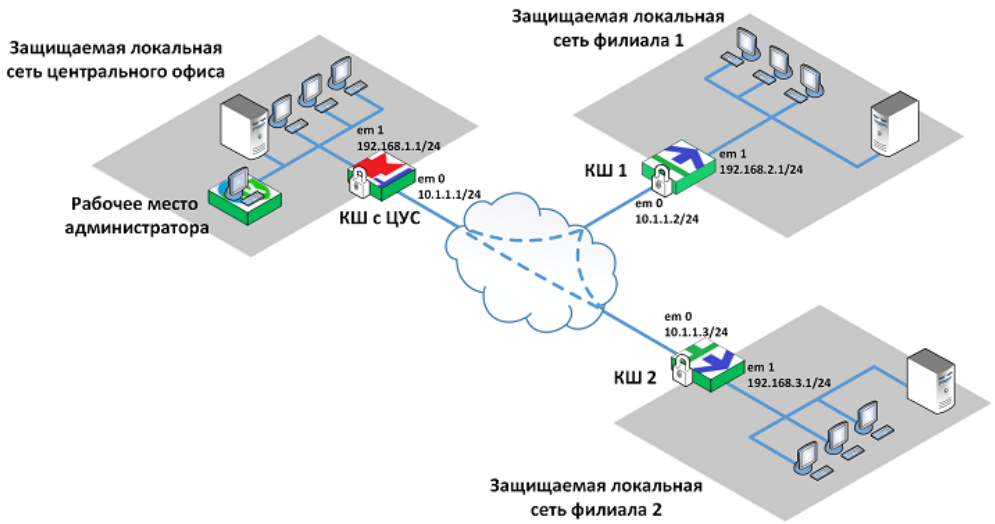
   На экране появится запрос на удаление временного интервала.

3. Нажмите кнопку "Да".

   Временной интервал будет удален из списка немедленно, а сведения о нем — из базы данных ЦУС без возможности восстановления.

Примеры сетевых объектов

В данном подразделе приведены примеры сетевых объектов для схемы, показанной на рисунке ниже.



На схеме для каждого криптошлюза указаны его внешний и внутренний интерфейсы.

КШ с ЦУС

Внешний	em 0	10.1.1.1/24
Внутренний	em 1	192.168.1.1/24

КШ 1

Внешний	em 0	10.1.1.2/24
Внутренний	em 1	192.168.2.1/24

КШ 2

Внешний	em 0	10.1.1.3/24
Внутренний	Em 1	192.168.3.1/24

Для создания объектов используйте процедуру, описанную на стр. **17**.

Сеть

Создайте три объекта: защищаемая сеть центрального офиса, защищаемая сеть филиала 1 и защищаемая сеть филиала 2.

Центральный офис

Параметр	Значение
Название	Центральный офис
Описание	Защищаемая сеть центрального офиса
Unicast	Unicast
IP-адрес	192.168.1.0
Маска	255.255.255.0
Тип привязки	Защищаемый

Параметр	Значение
Криптошлюз	КШ с ЦУС
Интерфейс	em1

Филиал 1

Параметр	Значение
Название	Филиал 1
Описание	Защищаемая сеть филиала 1
Unicast	Unicast
IP-адрес	192.168.2.0
Маска	255.255.255.0
Тип привязки	Защищаемый
Криптошлюз	КШ 1
Интерфейс	em1

Филиал 2

Параметр	Значение
Название	Филиал 2
Описание	Защищаемая сеть филиала 2
Unicast	Unicast
IP-адрес	192.168.3.0
Маска	255.255.255.0
Тип привязки	Защищаемый
Криптошлюз	КШ 2
Интерфейс	em1

Хост

Создайте три объекта: хост в защищаемой сети центрального офиса, хост в защищаемой сети филиала 1 и хост в защищаемой сети филиала 2.

Хост 1

Параметр	Значение
Название	Хост 1
Описание	Хост в сети центрального офиса
Unicast	Unicast
IP-адрес	192.168.1.1
Маска	255.255.255.255
Тип привязки	Внутренний
Криптошлюз	КШ с ЦУС
Интерфейс	em1

Хост 1.1

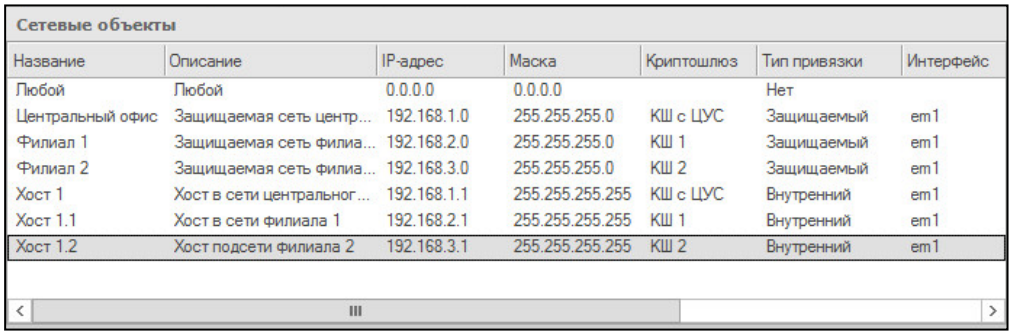
Параметр	Значение
Название	Хост 1.1
Описание	Хост в сети филиала 1

Параметр	Значение
Unicast	Unicast
IP-адрес	192.168.2.1
Маска	255.255.255.255
Тип привязки	Внутренний
Криптошлюз	КШ 1
Интерфейс	em1

Хост 1.2

Параметр	Значение
Название	Хост 1.2
Описание	Хост в сети филиала 2
Unicast	Unicast
IP-адрес	192.168.3.1
Маска	255.255.255.255
Тип привязки	Внутренний
Криптошлюз	КШ 2
Интерфейс	em1

Созданные с указанными параметрами объекты отобразятся в списке сетевых объектов.


Сетевые объекты

Название	Описание	IP-адрес	Маска	Криптошлюз	Тип привязки	Интерфейс
Любой	Любой	0.0.0.0	0.0.0.0		Нет	
Центральный офис	Защищаемая сеть центр...	192.168.1.0	255.255.255.0	КШ с ЦУС	Защищаемый	em1
Филиал 1	Защищаемая сеть филиа...	192.168.2.0	255.255.255.0	КШ 1	Защищаемый	em1
Филиал 2	Защищаемая сеть филиа...	192.168.3.0	255.255.255.0	КШ 2	Защищаемый	em1
Хост 1	Хост в сети центральног...	192.168.1.1	255.255.255.255	КШ с ЦУС	Внутренний	em1
Хост 1.1	Хост в сети филиала 1	192.168.2.1	255.255.255.255	КШ 1	Внутренний	em1
Хост 1.2	Хост подсети филиала 2	192.168.3.1	255.255.255.255	КШ 2	Внутренний	em1

Установление парных связей между криптошлюзами

Парная связь — это связь между двумя криптошлюзами, которая означает, что трафик, передаваемый между ними, должен быть зашифрованным. При построении VPN "Континент" необходимо задать парные связи для всех криптошлюзов, между которыми должны устанавливаться защищенные соединения.

Для установления парных связей в свойствах криптошлюза формируют список тех криптошлюзов, с которыми должны быть установлены такие связи.

Количество защищенных соединений (VPN-каналов) для каждой пары связанных сетевых устройств соответствует количеству зарегистрированных в системе классов трафика (сведения о классах трафика приводятся в [**2**]).

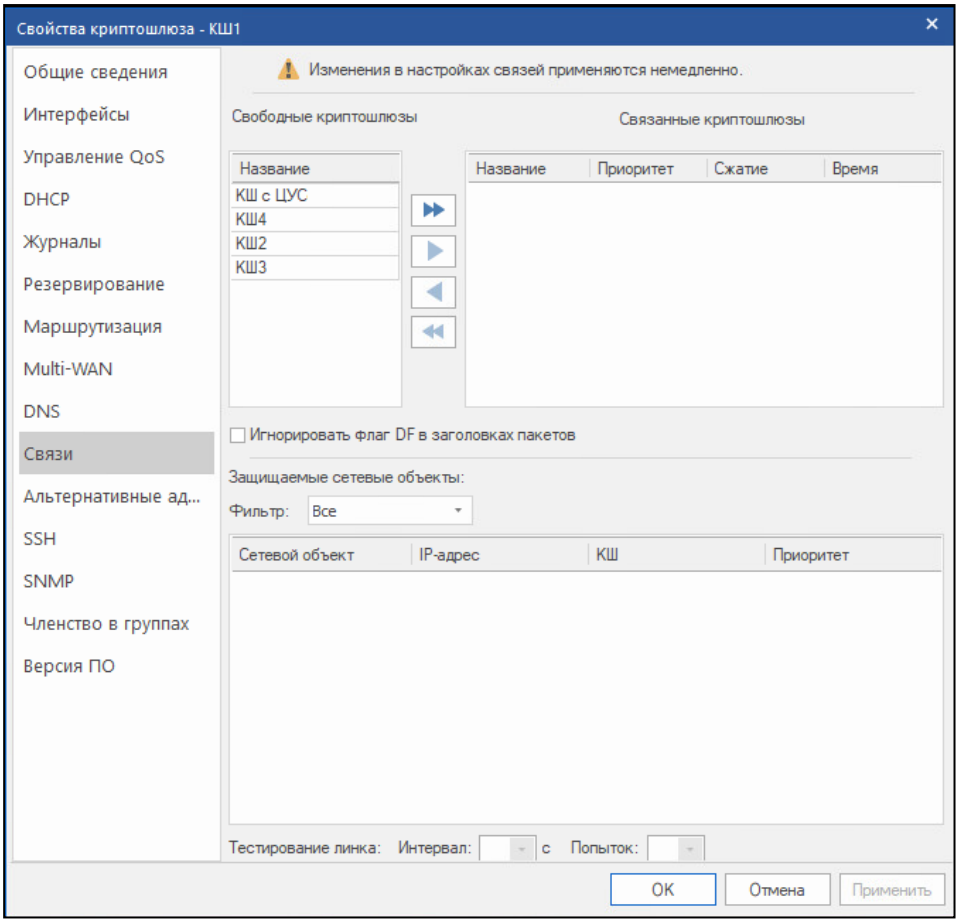
Для формирования списка связанных криптошлюзов:

1. Вызовите контекстное меню криптошлюза, для которого необходимо сформировать парные связи, и активируйте команду "Свойства…".

   На экране появится окно настройки свойств данного криптошлюза.

2. Перейдите на вкладку "Связи".

   На вкладке отображаются два списка: "Свободные криптошлюзы" и "Связанные криптошлюзы".

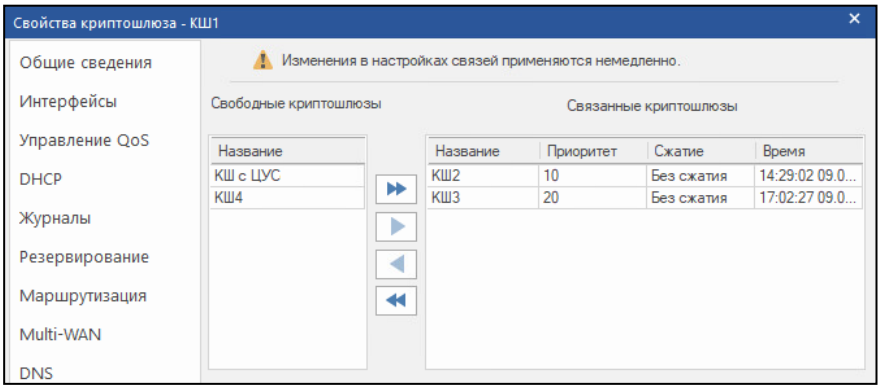


Если парные связи между криптошлюзами не создавались, список связанных криптошлюзов будет пустым.

3. Сформируйте список связанных сетевых устройств. Для этого переместите криптошлюзы, с которыми должна быть установлена парная связь данного криптошлюза, в список "Связанные криптошлюзы".

   Перемещайте выбранные элементы из списка в список с помощью кнопок "<", "<<" и ">", ">>".

4. Если данный КШ (на рисунке ниже КШ 1) имеет парные связи с двумя другими КШ (КШ 2 и КШ 3), к которым имеет привязку один и тот же защищаемый сетевой объект, необходимо для каждой связи (КШ 1—КШ 2 и КШ 1—КШ 3) указать приоритеты, в соответствии с которыми КШ 1 будет отправлять зашифрованные пакеты защищаемому сетевому объекту. Для этого выделите поле "Приоритет", раскройте список и выберите в нем нужное значение. Допустимые значения: 1–255, где значение "1" — самый высокий приоритет.



5. При необходимости для каждого КШ из списка "Связанные криптошлюзы" укажите нужный режим сжатия передаваемых IP-пакетов. Для этого выделите поле "Сжатие", раскройте список и выберите в нем нужное значение.

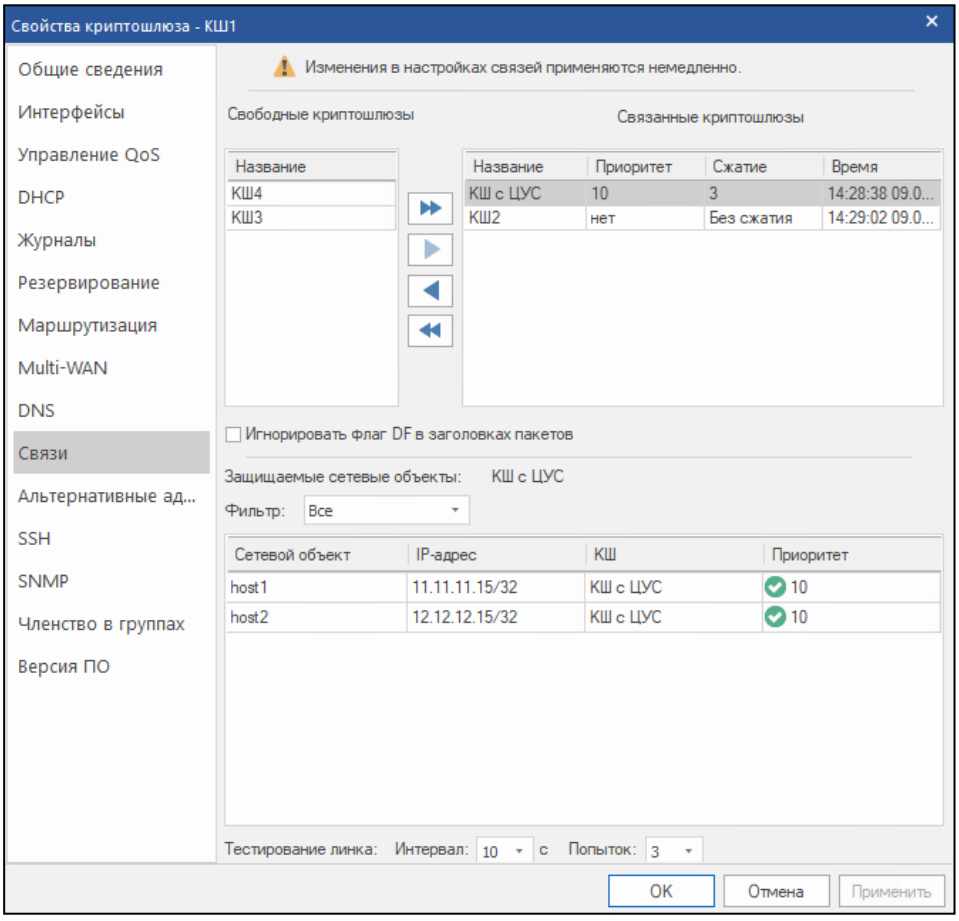
   Список содержит значения от "1" до "9" и "Без сжатия". При переходе от режима "1" к режиму "9" степень сжатия IP-пакетов увеличивается и, соответственно, увеличивается время сжатия. При выборе значения "Без сжатия" сжатие IP-пакетов не осуществляется.

6. Если при обработке IP-пакетов необходимо игнорировать флаг DF в заголовках, установите соответствующую отметку.

7. Для каждой парной связи данного КШ (на рисунке выше — КШ 1) задайте параметры проверки работоспособности канала. Для этого выделите в списке "Связанные криптошлюзы" строку парной связи.

   В нижней части окна отобразится список защищаемых сетевых объектов.

   На рисунке ниже выбрана парная связь КШ 1 — КШ с ЦУС. При этом в списке защищаемых сетевых объектов отобразятся привязанные к КШ с ЦУС сетевые объекты host 1 и host 2.



Внимание! Для просмотра списка защищаемых сетевых объектов можно использовать фильтр. Варианты использования фильтра:

- Все — в списке отображаются все сетевые объекты, привязанные в рамках выбранной парной связи;
- Много связей — отображаются сетевые объекты, привязанные к более чем одному КШ;
- Одна связь — отображаются сетевые объекты, привязанные только к одному КШ.

8. В поле "Интервал" выберите интервал времени между проверками работоспособности канала. Доступные значения: 1–60 секунд.

В поле "Попыток" выберите количество проверок, на основании которых принимается решение о неработоспособности канала. Доступные значения: 1–10.

Примечание. Введенные значения будут применены к каждому КШ парной связи.

9. Нажмите кнопку "ОК" для сохранения изменений.

   Изменения в данном диалоге вступают в силу сразу после их внесения.

   С этого момента данные сетевые устройства могут устанавливать между собой защищенное соединение.

Внимание! Параметры сжатия IP-пакетов каждого из двух криптошлюзов, составляющих пару взаимодействующих КШ, настраиваются отдельно и могут не совпадать.

Групповые операции с парными связями

Для установления парных связей между криптошлюзами или криптокоммутаторами можно использовать групповые операции. Они позволяют выбрать в списке сразу несколько сетевых устройств (КШ или КК) и создать для них парные связи с другими сетевыми устройствами из списка.

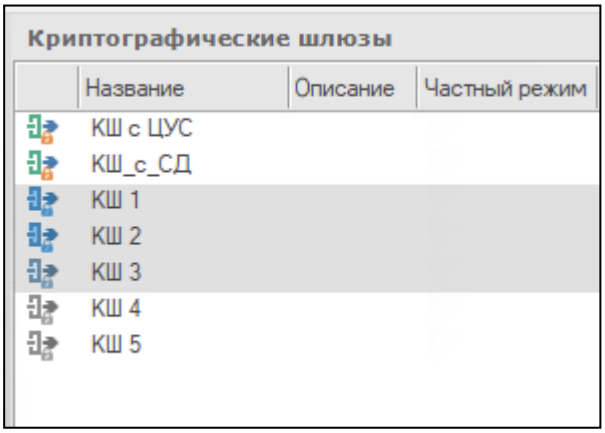
С помощью групповых операций можно:

- создать полносвязную матрицу для группы сетевых устройств;
- добавить для группы сетевых устройств парные связи с другими сетевыми устройствами;
- удалить все парные связи между сетевыми устройствами выбранной группы;
- удалить парные связи у всех сетевых устройств группы.

Для выполнения групповых операций:

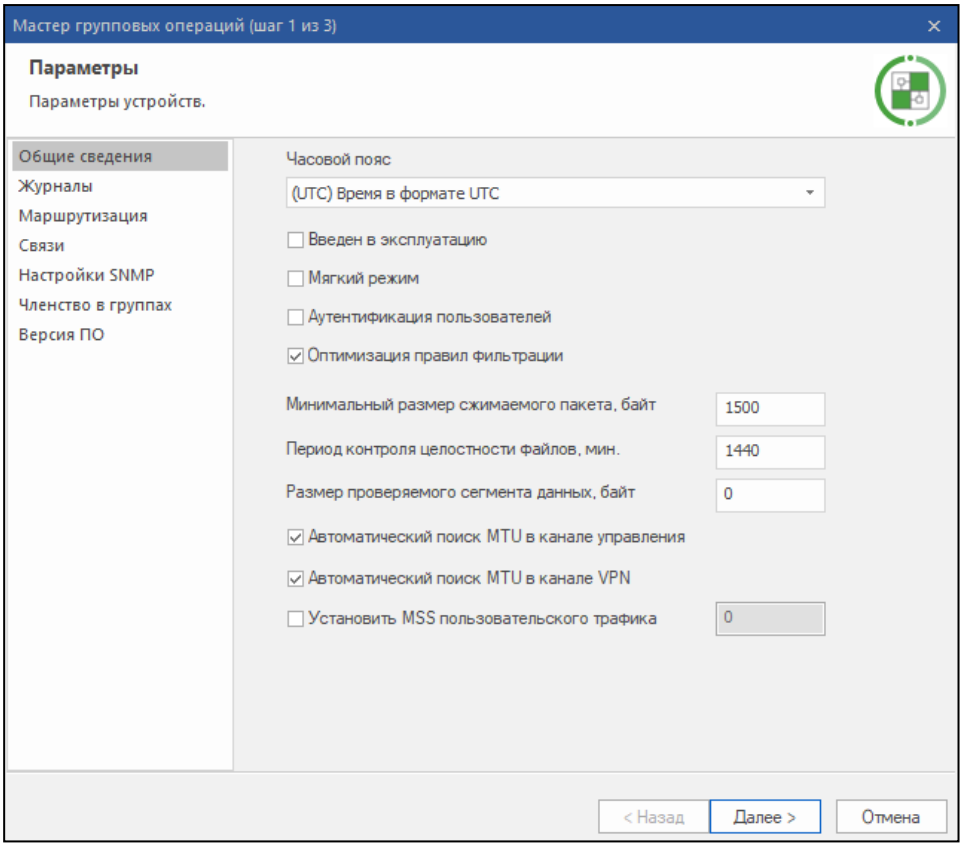
1. Перейдите к списку сетевых устройств (криптошлюзов или криптокоммутаторов) и выделите с помощью клавиши <Ctrl> группу устройств, для которых необходимо выполнить групповую операцию.

   На рисунке ниже показан список криптошлюзов, в который входят КШ с ЦУС, КШ с СД и КШ 1 — КШ 5. Выбрана группа КШ 1 — КШ 3.

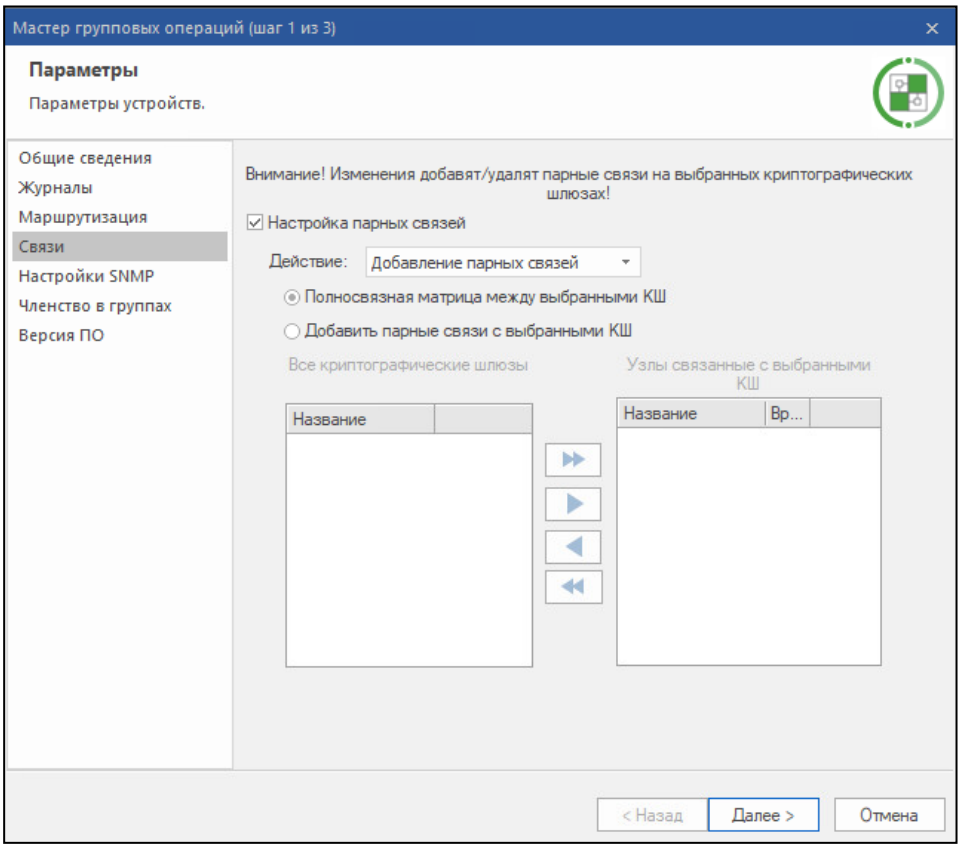


2. Нажмите на панели инструментов кнопку "Групповые операции".

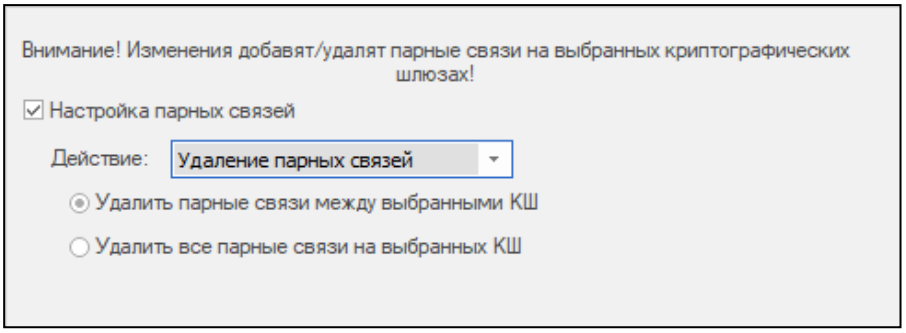
   На экране появится окно мастера групповых операций.



3. Перейдите в раздел "Связи", установите отметку "Настройка парных связей" и в поле "Действие" выберите "Добавление парных связей" или "Удаление парных связей".



- Если выбрано удаление парных связей, выберите "Удалить парные связи между выбранными КШ" или "Удалить все парные связи на выбранных КШ".

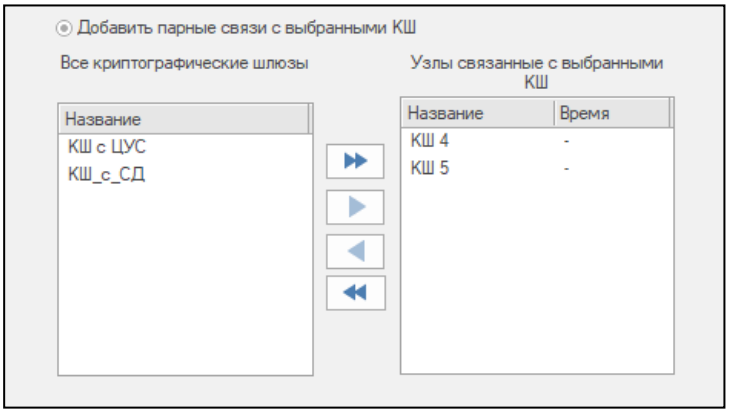


  Перейдите к п.**5**.

- Если требуется создать полносвязную матрицу для группы выбранных устройств (КШ 1 — КШ 3), установите переключатель в соответствующее положение и перейдите к п.**5**.
- Если требуется добавить для группы выбранных сетевых устройств (КШ 1 — КШ 3) парные связи с другими сетевыми устройствами, установите переключатель в соответствующее положение.

  В левом списке отобразятся все зарегистрированные сетевые устройства, за исключением выбранных устройств (КШ 1 — КШ 3).

4. Переместите из левого списка в правый те устройства, с которыми должны быть установлены парные связи каждого устройства группы (КШ 1 — КШ 3). Например, КШ 4 и КШ 5.



5. Нажмите кнопку "Далее".

   На экране появится следующее окно мастера с предупреждением о выполняемой операции.

6. Нажмите кнопку "Применить".

   Операция будет выполнена, и на экране появится следующее окно мастера, отображающее результаты выполненной операции. В нижней части окна расположена ссылка "Посмотреть отчет", по которой можно вызвать детализированные результаты операции в виде текстового файла.

7. Нажмите кнопку "Готово" для завершения операции.

Настройка параметров маршрутизации

Внимание! В данном подразделе описана настройка статической маршрутизации в VPN. Настройка динамической маршрутизации описана в [**5**].

Правила маршрутизации разделяются на два типа:

- правила, сформированные комплексом автоматически;
- правила, заданные администратором.

Правила, сформированные автоматически, предусматривают взаимодействие только между сегментами сети, подключенными непосредственно к интерфейсам криптошлюза. Формирование таких правил происходит при добавлении очередного адреса сетевого интерфейса. Правила этого типа действуют постоянно и не могут быть удалены или изменены администратором.

На основе правил маршрутизации постоянного действия комплекс автоматически формирует временные правила. Временное правило формируется при поступлении на криптошлюз IP-пакета, адресованного одному из абонентов защищаемой сети. Такое правило имеет ограниченное время действия, и если за это время на данный адрес не поступает новый пакет, правило уничтожается. Если пакет поступает, отсчет времени действия правила начинается заново. Кроме приведенного примера временные правила создаются также при наличии на пути прохождения IP-пакета сетей, характеризующихся значением MTU меньшим, чем у интерфейса криптошлюза. Правила этого типа не могут быть удалены или изменены администратором. Они не отображаются на экране.

Если защищаемая сеть подсоединена к криптошлюзу через маршрутизатор, правила маршрутизации для абонентов этой сети задаются администратором. Эти правила действуют постоянно.

Для просмотра и редактирования правил маршрутизации:

1. В главном окне ПУ ЦУС выберите раздел "Сетевые устройства Континент" и в нем — "Криптошлюзы".

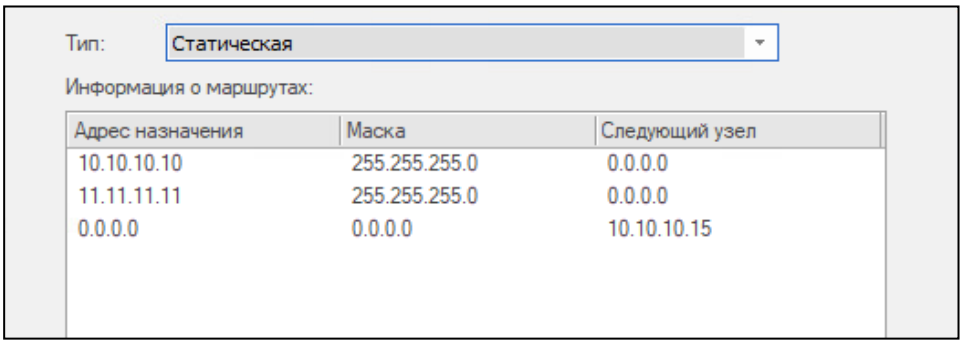
   В окне отображения информации появится список криптошлюзов.

2. Выберите криптошлюз, вызовите контекстное меню и далее выберите пункт "Свойства".

   На экране появится окно "Свойства криптошлюза".

3. Перейдите на вкладку "Маршрутизация".

   На вкладке отобразятся настройки правил маршрутизации.



   Внимание! Не изменяйте настройки в диалоге "Маршрутизация" без крайней необходимости. При некорректном вводе правил маршрутизации криптошлюз работать не будет.

Список правил маршрутизации отображается в виде таблицы, каждая строка которой соответствует одному правилу. Перечень полей таблицы правил маршрутизации и их описание представлены в таблице ниже.

Табл.1 Поля таблицы правил маршрутизации

Поле	Описание
Адрес назначения	IP-адрес подсети абонента-получателя
Маска	Маска подсети абонента-получателя
Следующий узел	IP-адрес следующего узла, через который должны проходить IP-пакеты для абонента-получателя

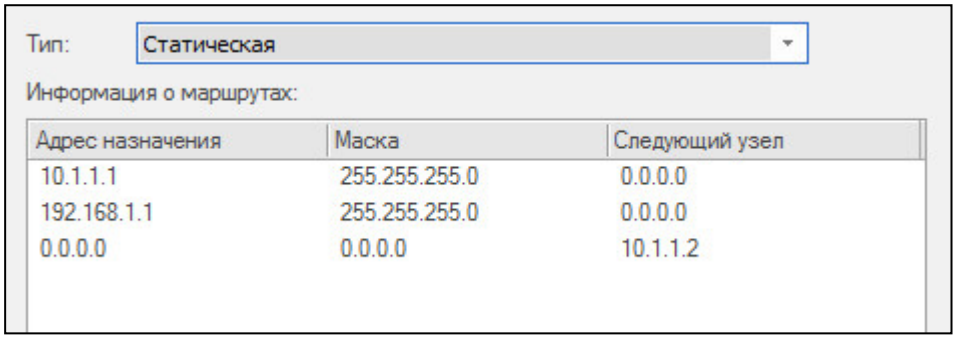
Правило маршрутизации с нулевыми маской и адресом назначения отображает маршрут по умолчанию.

Внимание! Если маршрут по умолчанию связывает сетевое устройство с ЦУС, то после его изменения соединение устройства с ЦУС становится невозможным. В этом случае требуется запись новой конфигурации на носитель и повторная инициализация сетевого устройства.

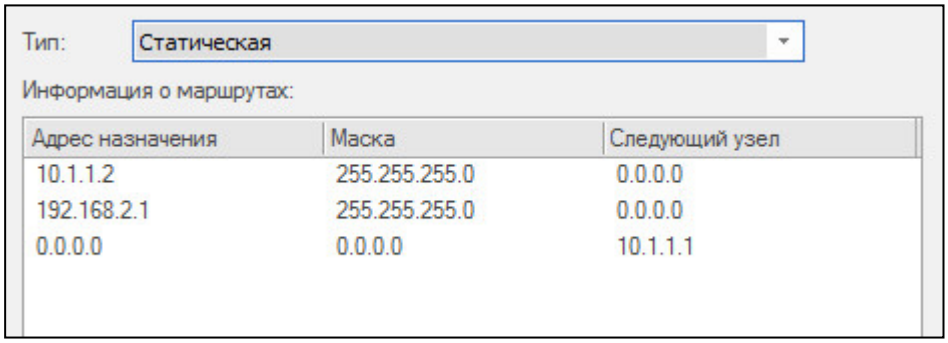
Нулевой адрес в столбце "Следующий узел" указывает, что данная подсеть доступна напрямую через интерфейс, без промежуточных маршрутизаторов.

Например, для схемы, приведенной на стр. **25**, у КШ с ЦУС и КШ 1 будут автоматически сформированы следующие правила:

КШ с ЦУС



КШ 1



В рассматриваемом примере созданные маршруты поддерживают функционирование парных связей и дополнительные маршруты для туннелей между КШ с ЦУС, КШ 1 и КШ 2 не требуются.

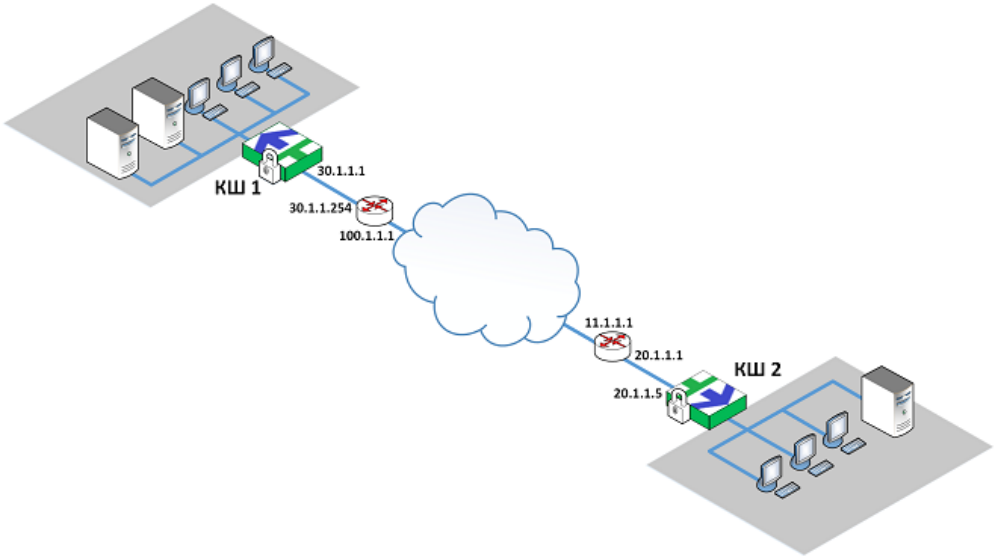
Однако на практике кроме компонентов, входящих в состав комплекса "Континент", используется сетевое оборудование сторонних производителей (например, маршрутизаторы провайдеров и пр.), что приводит к необходимости вводить дополнительные маршруты.

Подключение криптошлюза к маршрутизатору провайдера

Рассмотрим пример, в котором для подключения криптошлюза к сетям общего пользования используется маршрутизатор.

На рисунке ниже показаны криптошлюзы КШ 1 и КШ 2. КШ 1, имеющий IP-адрес 30.1.1.1, подключается к сетям общего пользования через маршрутизатор с "белым" IP-адресом 100.1.1.1, направленным в интернет, и "серым" IP-адресом 30.1.1.254 для соединения с КШ 1.

КШ 2, имеющий IP-адрес 20.1.1.5, подключается к сетям общего пользования через маршрутизатор с "белым" IP- адресом 11.1.1.1, направленным в интернет, и "серым" IP-адресом 20.1.1.1 для соединения с КШ 2.



Для обеспечения парной связи между КШ 1 и КШ 2 необходимо на каждом из них сформировать дополнительное правило маршрутизации. Ниже приводится пример процедуры формирования правила для КШ 1.

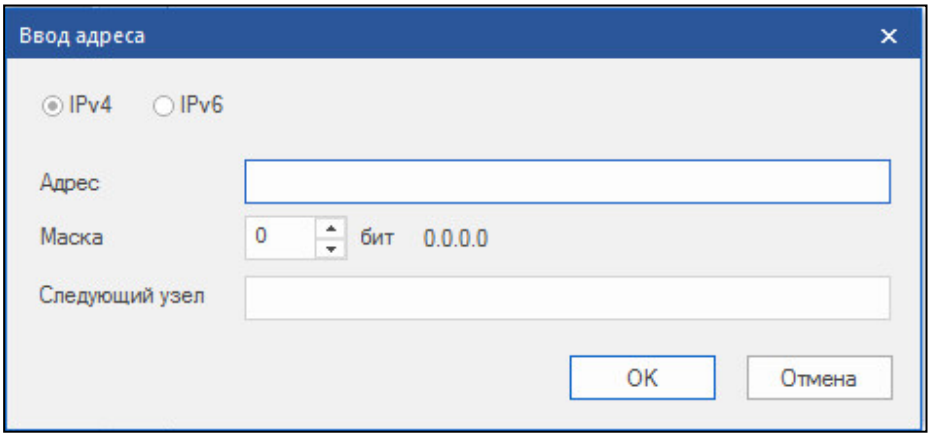
Для формирования правила КШ 1:

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

   На экране появится окно "Свойства КШ".
2. Перейдите на вкладку "Маршрутизация".

   На вкладке отобразятся правила маршрутизации.
3. Нажмите кнопку "Добавить".

   На экране появится окно "Ввод адреса".



4. Введите значения, как указано ниже, и нажмите кнопку "OK".

Поле	Значение
Адрес назначения	20.1.1.5
Маска	255.255.255.255
Следующий узел	30.1.1.254

   Маршрут с указанными параметрами появится в таблице "Информация о маршрутах".
5. Для завершения настройки нажмите в окне "Свойства криптошлюза" кнопку "Применить" или "OK".

Для формирования правила КШ 2:

- Выполните описанную выше процедуру применительно к КШ 2. Укажите следующие значения параметров:

Поле	Значение
Адрес назначения	30.1.1.1
Маска	255.255.255.255
Следующий узел	20.1.1.1

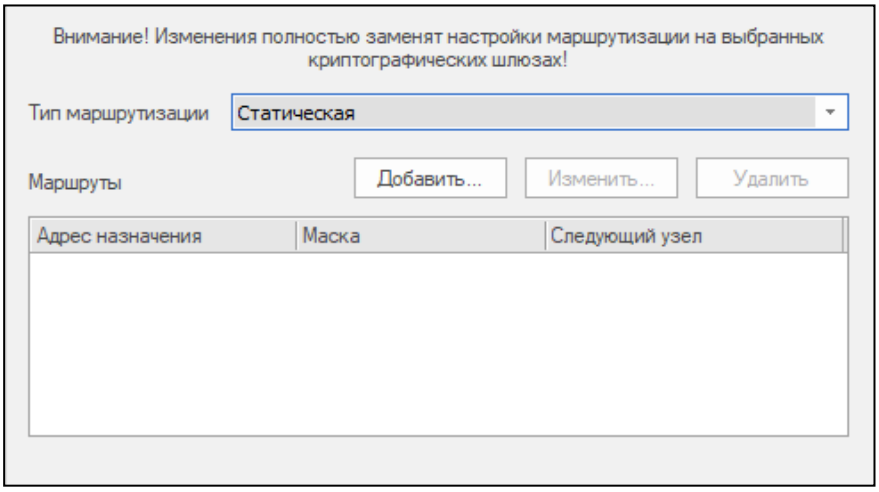
Групповые операции с параметрами маршрутизации

Правило маршрутизации можно задать сразу нескольким сетевым устройствам. Например, когда требуется одно и то же правило задать нескольким устройствам (группе сетевых устройств). Для этого необходимо выбрать несколько сетевых устройств, которым должно быть назначено правило, и далее с помощью групповых операций задать требуемое правило.

Для задания правила:

1. Перейдите к списку сетевых устройств и выделите с помощью клавиши <Ctrl> группу устройств, для которых необходимо задать правило маршрутизации.
2. Нажмите на панели инструментов кнопку "Групповые операции".

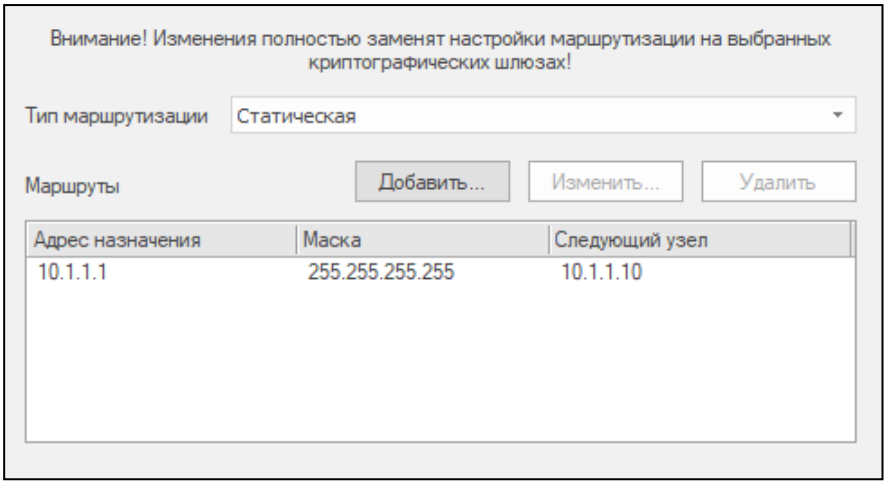
   На экране появится окно мастера групповых операций (см. рисунок на стр. **31**).
3. Перейдите в раздел "Маршрутизация" и выберите тип маршрутизации — "Статическая".



4. Нажмите кнопку "Добавить".

   На экране появится форма для ввода параметров правила маршрутизации (см. рисунок на стр. **35**).
5. Укажите параметры правила маршрутизации и нажмите кнопку "ОК".

   Параметры правила отобразятся в таблице "Маршруты".



6. При необходимости добавьте другие правила.

   Для редактирования таблицы "Маршруты" используйте кнопки "Добавить", "Изменить" и "Удалить".

7. Нажмите кнопку "Далее".

   На экране появится следующее окно мастера с предупреждением о выполняемой операции.

8. Нажмите кнопку "Применить".

   Операция будет выполнена, и на экране появится следующее окно мастера, отображающее результаты выполненной операции. В нижней части окна расположена ссылка "Посмотреть отчет", по которой можно вызвать детализированные результаты операции в виде текстового файла.

9. Нажмите кнопку "Готово" для завершения операции.

Правила фильтрации

Для прохождения трафика между защищаемыми локальными сетями VPN должны быть сформированы соответствующие правила фильтрации. Правила формирует администратор средствами программы управления. Сформированные правила хранятся в БД ЦУС в виде единого списка. Работа с правилами фильтрации подробно описана в настройках межсетевого экрана (см. [**4**]).

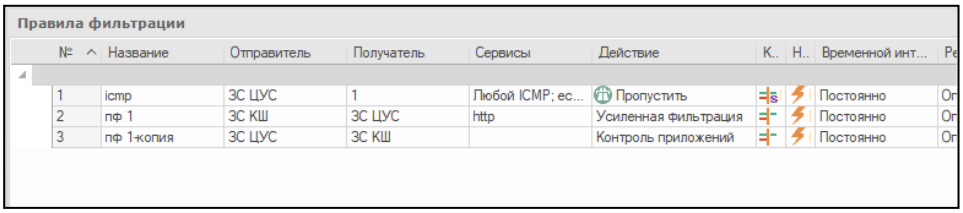
От ЦУС правила фильтрации автоматически передаются на указанные в них криптошлюзы и устанавливают порядок действий над IP-пакетами с заданными характеристиками при их обработке фильтром IP-пакетов шлюза. Поэтому для обеспечения работы туннеля между криптошлюзами следует учитывать действующие на них правила фильтрации и при необходимости изменять их или добавлять новые.

Примечание. У новых криптошлюзов, входящих в поставку, список правил фильтрации пуст и прохождение любых IP-пакетов через данный криптошлюз запрещено.

Для перехода к списку правил фильтрации:

- В главном окне программы управления выберите раздел "Центр управления сетью" и в нем — "Правила фильтрации".

  В панели отображения информации появится список всех сформированных правил фильтрации (если правила не создавались, список будет пустым).



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

Для настройки VPN первоначально необходимо создать правила фильтрации, обеспечивающие прохождение трафика между защищаемыми локальными сетями.

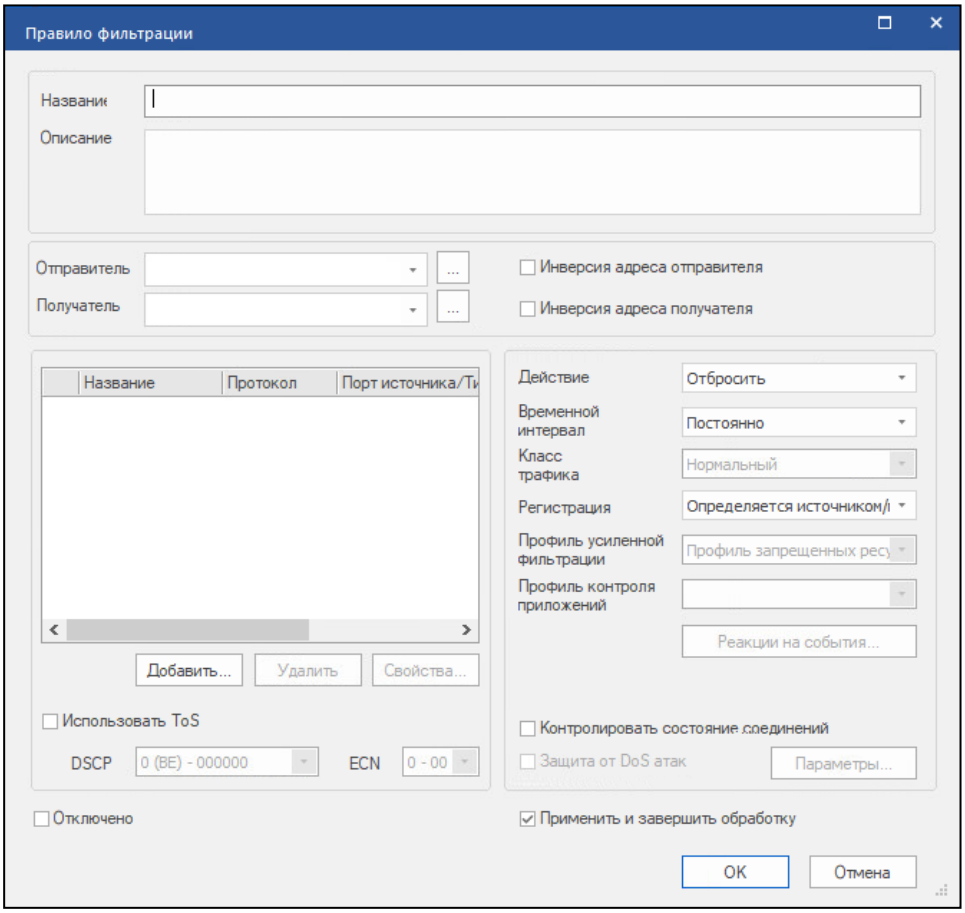
Чтобы обеспечить взаимодействие хостов защищаемых сетей центрального офиса и филиалов (см. рисунок на стр. **25**), необходимо на каждом криптошлюзе (КШ с ЦУС, КШ 1 и КШ 2) установить правило, разрешающее прохождение IP-пакетов.

Ниже приведен пример одного из вариантов создания правила, разрешающего прохождение трафика. В данном примере в качестве отправителя и получателя используется группа All_Net, включающая в себя сетевые объекты — Центральный офис, Филиал 1 и Филиал 2 (см. рисунок ниже).

Для создания разрешающего правила:

1. В главном окне программы управления перейдите к списку правил фильтрации и на панели инструментов нажмите кнопку "Создать правило фильтрации".

   На экране появится окно "Правило фильтрации".



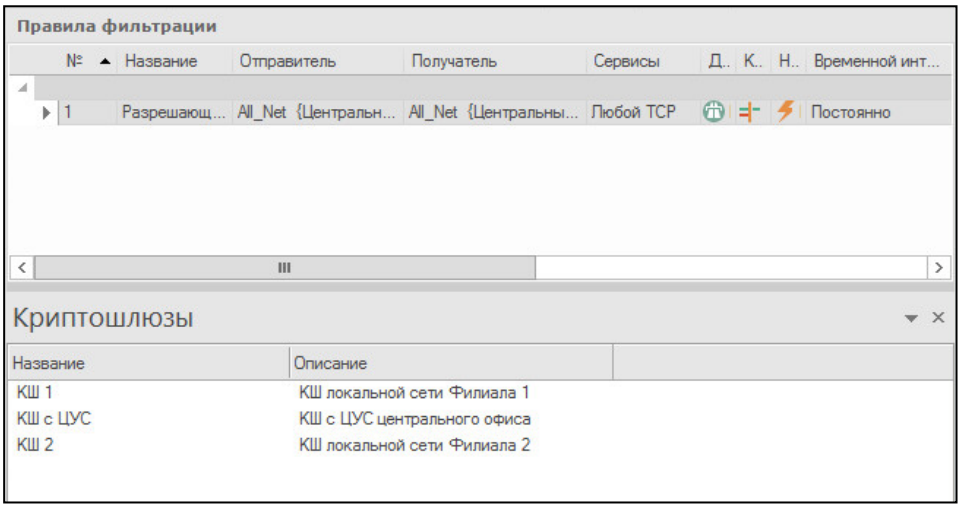
2. Заполните поля "Название" и "Описание" и далее укажите следующие значения параметров создаваемого правила:

Поле	Значение
Отправитель	All_Net
Получатель	All_Net
Действие	Пропустить
Сервис	Любой tcp

Значения других параметров можно не изменять или установить по усмотрению.

3. Нажмите кнопку "OK".

Окно "Правило фильтрации" закроется, и в списке появится новое правило.



4. Сохраните созданное правило в БД ЦУС. Для этого в главном окне ПУ ЦУС на панели инструментов нажмите кнопку "Сохранить изменения".

Внимание! Данное правило приведено в качестве примера, иллюстрирующего разрешение прохождения IP-пакетов между хостами защищаемых сетей, и может быть использовано только в совокупности с другими правилами фильтрации, учитывающими корпоративные требования политики безопасности.

Проверка работы VPN-каналов

После установления парных связей и задания правил фильтрации для криптошлюзов можно выполнить проверку настроек каналов VPN.

Для проверки настроек:

1. Запустите утилиту ping от хоста защищаемой сети центрального офиса к какому-либо хосту в защищаемой сети филиала 1.
2. На КШ с ЦУС средствами локального управления откройте дополнительное меню, используя комбинацию клавиш <ALT>+<F2>.

Примечание. Для вызова дополнительного меню необходимо предъявить персональный идентификатор администратора.

3. В дополнительном меню выберите пункт "Диагностика" и в меню "Диагностика" выберите пункт "Просмотр дампа сетевого трафика".

   На экране появится запрос на ввод имени интерфейса.
4. Введите имя внешнего интерфейса (для КШ с ЦУС — em0) и нажмите клавишу <Enter>.

   Появится запрос на задание фильтра.

5. Если необходимо отфильтровать результаты по какому-либо из сетевых протоколов, задайте фильтр в формате tcpdump, например:

```
# tcpdump -i em0 udp and port 10000 and host 199.199.1.17
```

и нажмите клавишу <Enter>.

Если применение фильтра не требуется, нажмите клавишу <Enter>.

На экране появится запрос на ограничение количества анализируемых пакетов (от 1 до 10000).

6. Введите требуемое значение и нажмите клавишу <Enter>.

На экран будут выведены сведения о прохождении зашифрованного трафика.

```
vv for full protocol decode
capture size 262144 bytes
:2d:0a, ethertype IPv4 (0x0800), length 92: 199.199.1.11.10000 > 199.199.1.12.0: UDP, leng
:ff:ff, ethertype ARP (0x0806), length 60: Request who-has 199.199.1.199 tell 199.199.1.20
:70:51, ethertype IPv4 (0x0800), length 66: 199.199.1.7.10000 > 199.199.1.10.10000: UDP, l
:94:33, ethertype IPv4 (0x0800), length 66: 199.199.1.7.10000 > 199.199.1.20.10000: UDP, l
:94:33, ethertype IPv4 (0x0800), length 150: 199.199.1.10.10000 > 199.199.1.20.10000: UDP,
:94:33, ethertype IPv4 (0x0800), length 66: 199.199.1.10.10000 > 199.199.1.20.10000: UDP,
:2f:4d, ethertype IPv4 (0x0800), length 66: 199.199.1.10.10000 > 199.199.1.7.10000: UDP, l
:2f:4d, ethertype IPv4 (0x0800), length 472: 199.199.1.11.5100 > 199.199.1.7.5101: UDP, le
:2f:4d, ethertype IPv4 (0x0800), length 74: 199.199.1.11.54963 > 199.199.1.7.5101: Flags [
:e1:b5, ethertype IPv4 (0x0800), length 74: 199.199.1.7.5101 > 199.199.1.11.54963: Flags [
```

Настройка параметров шифратора

Для шифратора сетевого устройства (КШ и КК) в меню управления предусмотрены следующие настройки:

- Включение и отключение режима шифрования трафика на основе адреса источника.

  Включение или отключение режима шифрования трафика к парному сетевому устройству зависит от принадлежности адреса источника — входит он в диапазон адресов глобальной сети интернет ("белый" адрес) или в диапазон адресов, назначаемых для внутренних сетей ("серый" адрес). При включенном режиме, если адрес источника "белый", трафик, передаваемый в защищаемую сеть парного сетевого устройства, зашифровываться не будет. При отключенном режиме такой трафик будет зашифровываться.

- Разрешение или запрет дефрагментации пакетов до фильтра.

  Дефрагментация пакетов в КШ и КК может выполняться на входе или на выходе фильтра. Для предупреждения перегрузки фильтра в случае длительного поступления на его вход фрагментированных пакетов рекомендуется установить режим, в котором дефрагментация пакетов будет выполняться до применения фильтра. Такой режим устанавливают командой "Разрешить дефрагментацию пакетов до пакетного фильтра".

  Для переключения в режим, в котором дефрагментация выполняется после фильтра, необходимо использовать команду "Запретить дефрагментацию пакетов до пакетного фильтра".

  По умолчанию установлен режим дефрагментации пакетов после фильтра.

- Разрешение или запрет распределения пакетов с учетом соединений.

  Данная настройка позволяет распределять пакеты между ядрами: пакеты с одинаковыми значениями MAC- адресов источника/получателя обрабатываются одними и теми же ядрами. Такой режим позволяет повысить производительность в тех случаях, когда трафик содержит большое количество пакетов с разными адресами источника/получателя.

  По умолчанию для КШ распределение пакетов разрешено, для КК — запрещено.

- Задание числа потоков шифрования.

На КШ и КК трафик при шифровании распределяется по потокам. При наличии свободных ресурсов процессора целесообразно повысить количество потоков для повышения производительности шифрования. Данная настройка актуальна для платформ IPC-1000 и выше.

По умолчанию число потоков определяется шифратором автоматически.

Для настройки шифратора:

Внимание! Если сетевое устройство находится в кластере, описанные ниже настройки должны быть выполнены на каждом устройстве, входящем в состав кластера.

1. Перейдите к меню управления сетевого устройства (см. стр. **61**).
2. Введите в строке ввода номер команды "Настройка шифрования" и нажмите клавишу <Enter>.

   На экране появится меню:

```
1: Включение/Отключение режима шифрования трафика на
основе адреса источника
2: Разрешение/Запрет дефрагментации пакетов до пакетного
фильтра
3: Запрет/Разрешение распределения пакетов с учетом
соединений
4: Задание числа потоков шифрования
0: Выход
Выберите пункт меню (0 – 4):
```

3. Введите номер нужной команды и нажмите клавишу <Enter>.

   Для первых трех команд статус параметра в меню на экране изменится.

   При выборе задания числа потоков шифрования на экране появится запрос:

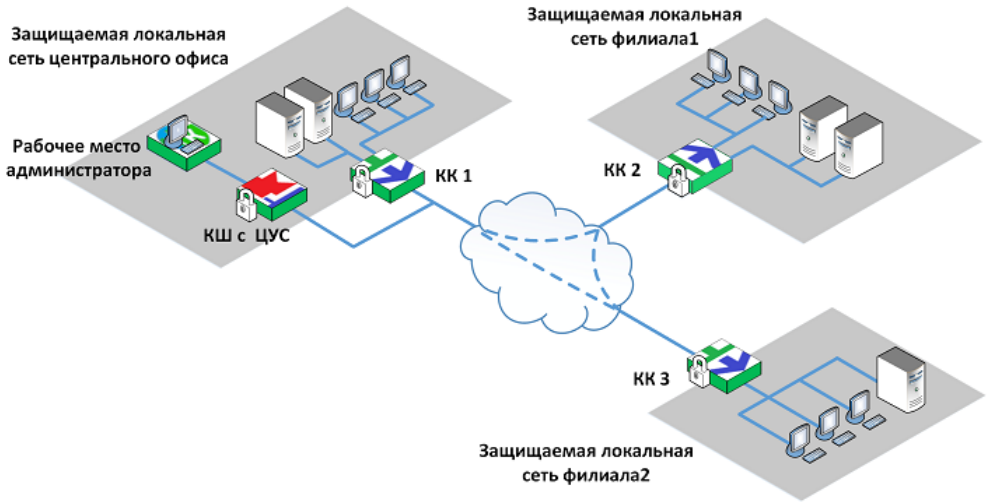
```
Задайте число потоков шифрования (1-32):
```

4. Введите нужное значение и нажмите клавишу <Enter>.

Глава 3
Развертывание L2VPN

Общие сведения

Для построения сетей L2VPN в АПКШ "Континент" используют криптографические коммутаторы. По аналогии с сетями L3VPN криптокоммутаторы размещают на периметре защищаемых ЛВС.



Внешний интерфейс криптокоммутатора направлен в сети общего доступа. К внутренним интерфейсам подключаются хосты защищаемых подсетей. Внутренние интерфейсы используются как порты коммутации в составе так называемого виртуального коммутатора.

Виртуальный коммутатор объединяет распределенные фрагменты одной сети с помощью защищенных каналов с использованием VPN-туннелей для передачи между криптокоммутаторами зашифрованного трафика.

Предусмотрено агрегирование интерфейсов криптокоммутатора. Описание агрегации интерфейсов приведено в [**2**].

Криптокоммутатор повышенной производительнсти

Криптографический коммутатор в зависимости от используемой платформы может иметь повышенную производительность. Такие криптокоммутаторы выполняют следующие функции:

- зашифрование — прием пакетов с внутреннего защищенного сетевого интерфейса, зашифрование содержимого пакета, подсчет имитовставки, инкапсуляция и отправка пакетов через защищенный сетевой интерфейс;
- расшифрование — прием пакетов с открытого сетевого интерфейса, деинкапсуляция, расшифрование, проверка имитовставки, проверка порядка следования и отправка пакетов через защищенный сетевой интерфейс.

Криптокоммутатор повышенной производительнсти имеет дополнительные интерфейсы, обозначаемые как ca0 – ca3, которые могут быть использованы в качестве внешнего и внутренних интерфейсов и могут быть агрегированы. Эти интерфейсы не используются для связи с ЦУС.

На работу криптокоммутатора повышенной производительности накладываются следующие ограничения:

- Криптокоммутатор работает только в режиме Pseudo Wire. Данные поступают на внутренний порт одного криптокоммутатора и выходят из внутреннего порта парного криптокоммутатора. В одном виртуальном коммутаторе можно использовать только два физических интерфейса от двух разных криптокоммутаторов.
- Криптокоммутатор не выполняет функции фрагментации и дефрагментации трафика. Вся фрагментация и дефрагментация должна выполняться сетевым оборудованием до попадания пакета в криптокоммутатор.
- Криптокоммутатор, пропустив через себя кадр, добавляет служебную информацию и увеличивает размер кадра на 70 байт. Таким образом, если в криптокоммутатор поступает кадр размером 1500 байт (стандартный MTU), на выходе образуется пакет размером 1570 байт, что превышает стандартный MTU. В этом случае оборудование интернет-провайдера должно поддерживать MTU 1600 байт. Или в защищенной сети должно стоять сетевое оборудование, которое фрагментирует пакеты до их попадания в криптокоммутатор, снижая размер до 1430 байт, чтобы после прохождения через криптокоммутатор размер пакета составил 1500 байт и уложился в стандартный MTU.
- Максимальный прирост производительности криптокоммутатора возможен на MTU 1500 байт. Использование Jumbo frame (MTU>1500) не приводит к значительному увеличению производительности. При маленькой длине пакета (например, при MTU 64 байт) будет наблюдаться снижение производительности. Максимально возможный MTU, поддерживаемый криптокоммутатором, — 9000 байт (с учетом добавленной служебной информации).
- Канал управления ЦУС — криптокоммутатор должен быть организован через выделенный интерфейс платформы криптокоммутатора — igb0-igb8, ixl0-ixl3.
- При применении настроек на криптокоммутаторе в него загружается ключевая информация, что приводит к перерыву связи от 2 до 8 секунд. Рекомендуется либо применять настройки во время технического окна, либо настроить отказоустойчивую схему с резервированием по LACP (см. сценарий 4 на стр. **54**) и применять настройки на разных КК по очереди, выжидая не менее 15–20 секунд до окончательного применения настроек.

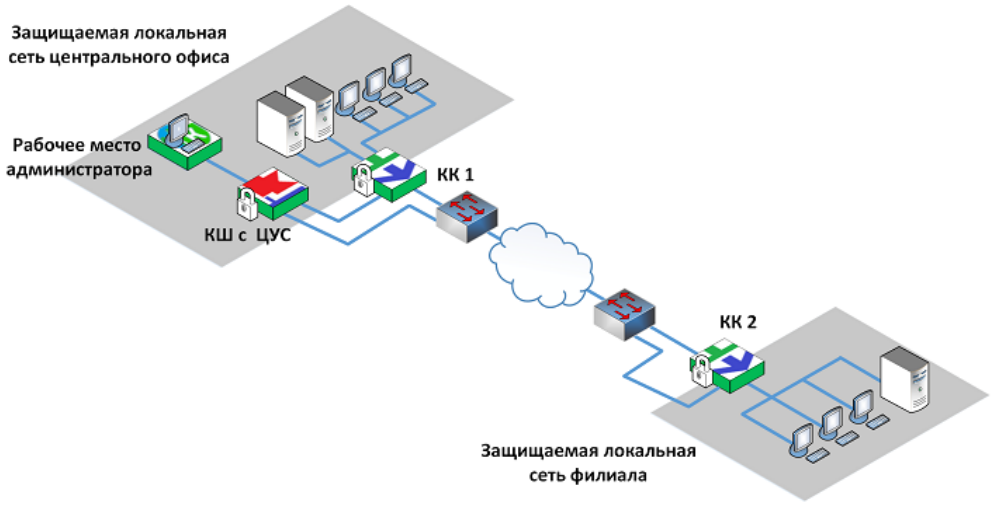
  В случае использования отказоустойчивой схемы (сценарий 4) настройки применяются по парам коммутаторов. Например (согласно рисунку): сначала КК1, за ним КК2, дождаться пока поднимется канал. Далее КК3, затем КК4, дождаться поднятия канала.
- Обновление ПО криптокоммутаторов с криптоускорителями должно осуществляться только локально с загрузочного USB-носителя. После установки ПО на платформу и ее успешного запуска необходимо штатно выключить и затем обесточить на несколько секунд отключением силовых кабелей.
- Ограничение на назначение IP-адресов интерфейсам криптокоммутатора. Динамические MAC-адреса агрегированного интерфейса генерируются в соответствии с правилом: первый из IP-адреса агрегированного интерфейса, следующий – из следующего по порядку IP-адреса.

  Например (см. сценарий 4 на стр. **54**), у КК1 IP-адрес агрегированного интерфейса lagg1 – 2.2.2.1. Для интерфейса ca0 MAC-адрес генерируется из 2.2.2.1, а для ca1 — из 2.2.2.2. При этом адрес 2.2.2.2 был назначен, например, адресом интерфейса lagg1 КК2. В этом случае MAC-адрес для интерфейса ca0 КК2 будет генерироваться из IP-адреса 2.2.2.2. В итоге интерфейсы ca1 КК1 и ca0 КК2 будут иметь одинаковые MAC-адреса, что приведет к конфликту.

Так как максимальное количество дополнительных интерфейсов — 4 (ca0 - ca4), необходимо выбирать IP-адреса агрегированных интерфейсов с шагом 4. Например, lagg1 КК1 имеет адрес 10.10.10.1, значит — MAC-адреса для ca0, ca1, ca2 и ca3 будут генерироваться соответственно из 10.10.10.1, 10.10.10.2, 10.10.10.3 и 10.10.10.4. Следующий IP-адрес, который можно использовать для другого интерфейса lagg — 10.10.10.5. При этом также не должны использоваться промежуточные адреса (в нашем случае — 10.10.10.2, 10.10.10.3 и 10.10.10.4).

- При использовании VPN-туннеля с криптокоммутаторами повышенной производительности, находящимися за маршрутизаторами, необходимо, чтобы первые октеты внешних интерфейсов этих криптокоммутаторов различались между собой.

На рисунке ниже приведен пример криптографической коммутируемой сети L2VPN для центрального офиса и филиала с применением криптокоммутаторов повышенной производительности КК 1 и КК 2.



Для построения сети в программе управления ЦУС необходимо создать виртуальный коммутатор и включить в него внутренние интерфейсы КК 1 и КК 2. Эти внутренние интерфейсы в виртуальном коммутаторе выполняют роль портов коммутации.

Порядок развертывания L2VPN

Развертывание криптографической коммутируемой сети L2VPN включает в себя последовательное выполнение следующих этапов:

1. Настройка криптокоммутаторов (см. ниже).
2. Создание виртуального коммутатора (см. стр. **48**).

Настройка криптокоммутатора

Настройку выполняют после регистрации криптокоммутатора в ПУ ЦУС и последующей его инициализации.

Настройка заключается в задании IP-адресов внешних интерфейсов криптокоммутатора.

Прочие настройки, связанные с работой криптокоммутатора как сетевого устройства, в данном руководстве не рассматриваются.

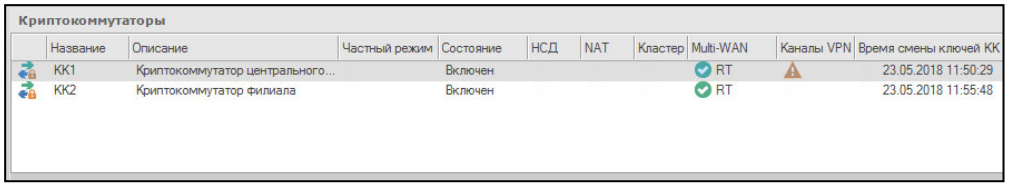
Список криптокоммутаторов

Зарегистрированные криптокоммутаторы заносятся в список сетевых устройств АПКШ "Континент".

Для перехода к списку криптокоммутаторов:

- В главном окне ПУ ЦУС в списке объектов выберите пункт "Сетевые устройства Континент | Криптокоммутаторы".

  В области отображения информации появится список зарегистрированных криптокоммутаторов.



В списке для каждого криптокоммутатора приводится следующая информация:

- название;
- краткое описание;
- частный режим — включен/выключен;
- состояние — включен/выключен;
- отметка о зарегистрированных событиях НСД;
- наличие неработоспособных каналов VPN;
- время следующей смены ключей.

В дополнительном окне приводится более подробная информация о выбранном в списке криптокоммутаторе. Дополнительное окно содержит три вкладки.

Вкладка	Описание
Состояние КК	Сведения о состоянии КК: • включен/выключен; • введен в эксплуатацию/выведен из эксплуатации. Сведения о ключах: • срок действия; • время смены ключей. Наличие зарегистрированных событий НСД. Режим работы пакетного фильтра. Статус автозагрузки. Список VPN-каналов с указанием неработоспособных и времени отказа. Статистика по трафику для каждого интерфейса КК
Виртуальные коммутаторы	Список виртуальных коммутаторов, в которые входит данный КК, с указанием количества портов виртуального коммутатора и статуса парных связей
Очередь заданий	Список текущих заданий, которые сформированы для данного КК, но еще не выполнены. Приводятся наименование задания и время ожидания — интервал времени, прошедший с момента формирования задания

При просмотре списка криптокоммутаторов доступны все основные операции, выполняемые применительно к сетевым устройствам "Континент": создание нового криптокоммутатора, настройка параметров работы, удаление криптокоммутатора, выключение, перезагрузка и т. д. Для выполнения этих операций используются кнопки панели инструментов или команды контекстного меню.

Настройка интерфейсов криптокоммутатора

Для настройки интерфейсов криптокоммутатора необходимо задать внешний интерфейс и интерфейс, выполняющий роль порта коммутации.

Интерфейс для связи с ЦУС задается при регистрации криптокоммутатора (см. [**3**]). Этот интерфейс не должен являться интерфейсом криптоускорителя.

Для настройки интерфейсов криптокоммутатора:

1. В главном окне программы управления ЦУС перейдите к списку криптокоммутаторов, выберите в списке устройство и вызовите окно "Свойства".

   На экране появится окно настройки свойств криптокоммутатора.

2. В левой части окна выберите вкладку "Интерфейсы".

   В правой части окна появится список всех имеющихся интерфейсов данного устройства:

   igb0 - igb8, ixl0 - ixl3 — интерфейсы криптокоммутатора;

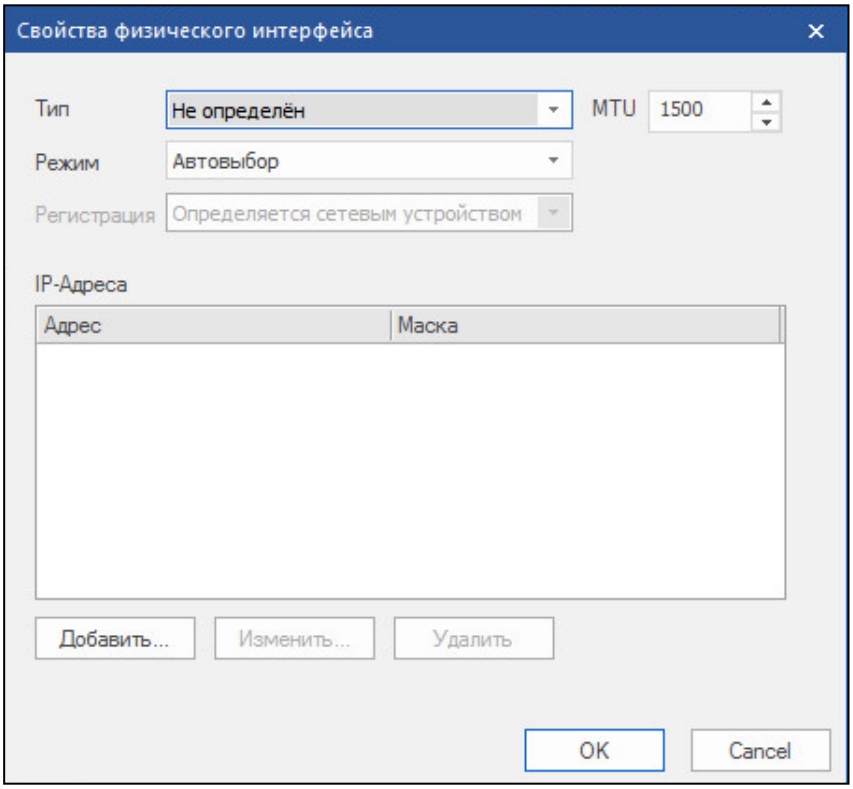
   ca0 - ca3 — интерфейсы платы криптоускорителя (только для криптокоммутатора с криптоускорителем).

3. Для задания внешнего интерфейса криптокоммутатора выберите один из интерфейсов:

   - igb0 - igb8, ixl0 - ixl3 — для криптокоммутатора без криптоускорителя;
   - ca0 - ca3 — для криптокоммутатора с криптоускорителем (например, ca0).

   Нажмите кнопку "Изменить".

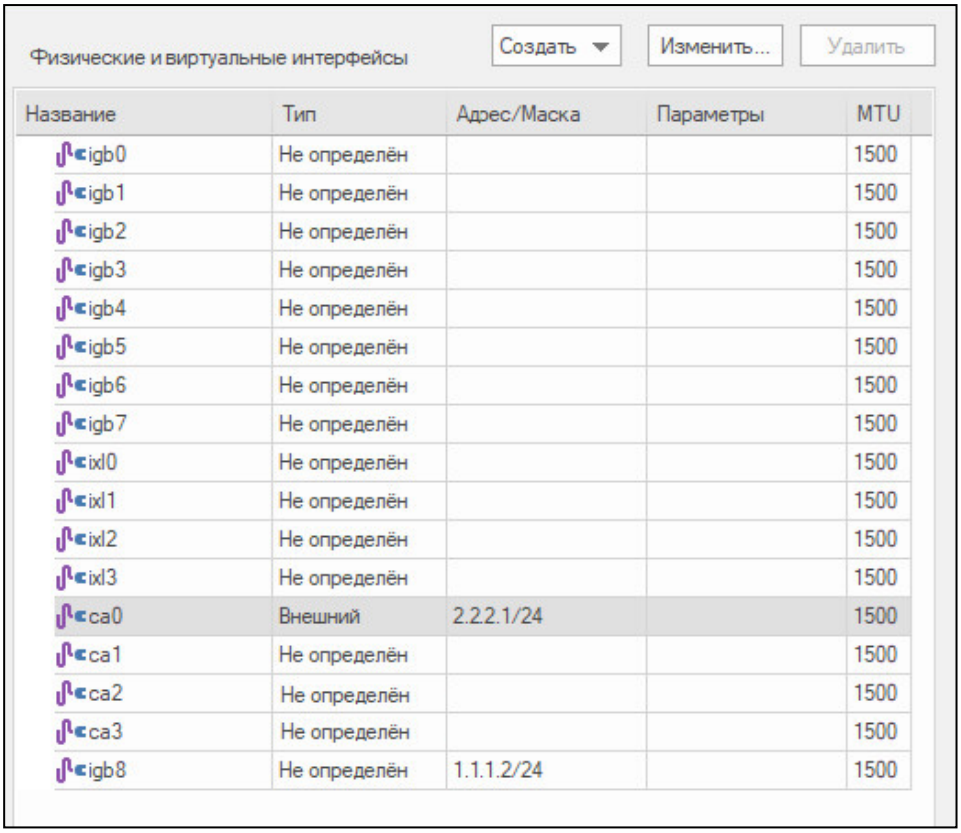
   На экране появится окно "Свойства физического интерфейса".



4. В поле "Тип" из раскрывающегося списка выберите значение "Внешний" и далее в поле "IP-адреса" введите IP-адрес и маску внешнего интерфейса криптокоммутатора.

   Нажмите кнопку "OK" в нижней части окна.

   Окно закроется, и в списке интерфейс ca0 отобразится как внешний интерфейс криптокоммутатора.



Название	Тип	Адрес/Маска	Параметры	MTU
igb0	Не определён			1500
igb1	Не определён			1500
igb2	Не определён			1500
igb3	Не определён			1500
igb4	Не определён			1500
igb5	Не определён			1500
igb6	Не определён			1500
igb7	Не определён			1500
ixl0	Не определён			1500
ixl1	Не определён			1500
ixl2	Не определён			1500
ixl3	Не определён			1500
ca0	Внешний	2.2.2.1/24		1500
ca1	Не определён			1500
ca2	Не определён			1500
ca3	Не определён			1500
igb8	Не определён	1.1.1.2/24		1500

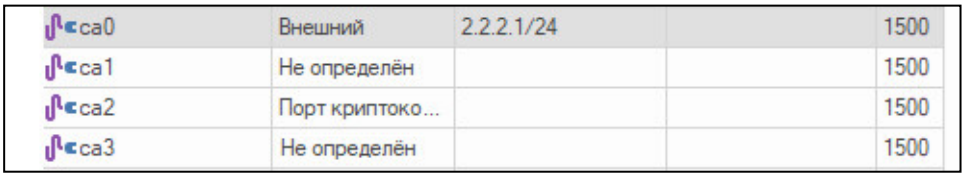
Внимание! Интерфейс igb8, предназначенный для связи с ЦУС, был задан при регистрации криптокоммутатора. Значение в поле "Тип" должно быть "Не определен".

5. Выберите один из свободных интерфейсов (igb0 - igb7, ixl0 - ixl3 — для криптокоммутатора без криптоускорителя, ca1 – ca3 — для криптокоммутатора с криптоускорителем), который должен выполнять роль порта коммутации (например, ca2), и нажмите кнопку "Изменить".

   На экране появится окно "Свойства физического интерфейса" (см. рисунок выше).

6. В поле "Тип" из раскрывающегося списка выберите значение "Порт криптокоммутатора" и нажмите кнопку "ОК" в нижней части окна.

   Окно "Свойства физического интерфейса" закроется, и в списке интерфейсов ca2 будет определен как порт криптокоммутатора.



ca0	Внешний	2.2.2.1/24		1500
ca1	Не определён			1500
ca2	Порт криптоко...			1500
ca3	Не определён			1500

7. Если необходимо задать еще один или несколько портов коммутации, выберите свободный интерфейс криптоускорителя, нажмите кнопку "Изменить" и повторите п. **6**.
8. После задания всех необходимых портов коммутации нажмите кнопку "ОК" или "Применить" в нижней части окна "Свойства криптокоммутатора".

Фильтрация протоколов на криптокоммутаторе

Приведенные ниже настройки предназначены для запрета или разрешения прохождения через криптокоммутатор пакетов следующих протоколов:

- LACP;
- STP;
- 802.1X для Port-based access control;
- Pause-пакеты.

По умолчанию после ввода криптокоммутатора в эксплуатацию прохождение пакетов указанных протоколов запрещено.

Примечание. Данная настройка не влияет на криптокоммутатор с криптоускорителем.

Для просмотра текущих настроек коммутации:

1. Перейдите к меню управления сетевым устройством (см. стр. **61**).
2. Введите в строке ввода номер команды "Настройка коммутации" и нажмите клавишу <Enter>.

   На экране появится меню настроек коммутации.

```
1: Показать текущие настройки коммутации
2: Разрешить прохождение LACP-пакетов
3: Разрешить прохождение STP-пакетов
4; Разрешить прохождение пакетов Port-Based access control
по 802.1x
5; Разрешить прохождение Pause-пакетов для flow control
0: Выход
Выберите пункт меню (0 – 5):
```

3. Введите в строке ввода номер команды "Показать текущие настройки коммутации" и нажмите клавишу <Enter>.

   На экране отобразятся текущие настройки.

```
Прохождение пакетов LACP запрещено
Прохождение пакетов STP запрещено
Прохождение пакетов 802.1 запрещено
Прохождение Pause пакетов запрещено
```

Для разрешения/запрета прохождения пакетов:

- В меню настроек коммутации введите в строке ввода номер команды для нужного протокола и нажмите клавишу <Enter>.

  Содержание команды в меню изменится на противоположное ("запретить" на "разрешить" и — наоборот).

Виртуальные коммутаторы

Описание виртуального коммутатора

Виртуальный коммутатор объединяет порты криптокоммутаторов, предназначенные для работы L2VPN. В составе виртуального коммутатора такие порты называются портами коммутации. Если в состав криптокоммутатора входит криптоускоритель, в качестве портов коммутации используются интерфейсы криптоускорителя. В этом случае в виртуальном коммутаторе можно использовать только два физических интерфейса (порта коммутации) с двух разных криптокоммутаторов.

Парные связи между криптокоммутаторами устанавливаются автоматически при создании виртуального коммутатора. При необходимости парные связи можно устанавливать и удалять вручную. Установление парных связей вы-

полняют в полном соответствии с процедурой установления парных связей для криптошлюзов (см. стр. **27**).

Процедура создания виртуального коммутатора включает в себя настройку механизма port security (задание MAC-адресов, запрет/разрешение динамической адресации, ограничение размера таблицы коммутации).

Список виртуальных коммутаторов

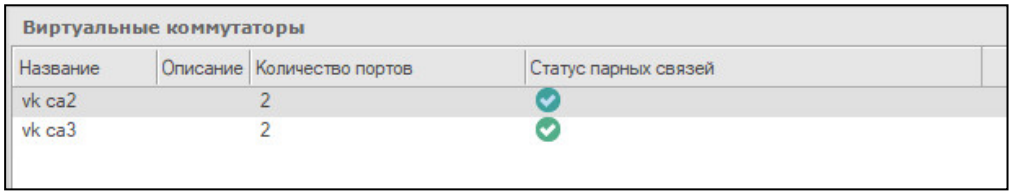
Созданные администратором виртуальные коммутаторы заносятся в список.

Для перехода к списку виртуальных коммутаторов:

- В главном окне ПУ ЦУС в списке объектов в разделе "Центр управления сетью" выберите пункт "Виртуальные коммутаторы".

  В области отображения информации появится список зарегистрированных виртуальных коммутаторов.

На рисунке ниже представлен список, включающий в себя два виртуальных коммутатора — vk ca2 и vk ca3.



В списке для каждого виртуального коммутатора приводится следующая информация:

- название;
- краткое описание;
- количество портов коммутации;
- статус парных связей.

В списке с виртуальными коммутаторами предусмотрено выполнение следующих операций:

- создание нового виртуального коммутатора и добавление его в список;
- удаление из списка;
- управление MAC-адресами;
- просмотр и изменение параметров, заданных при создании виртуального коммутатора.

Для выполнения перечисленных выше операций используются кнопки панели инструментов или команды контекстного меню.

Создание нового виртуального коммутатора

Для создания виртуального коммутатора:

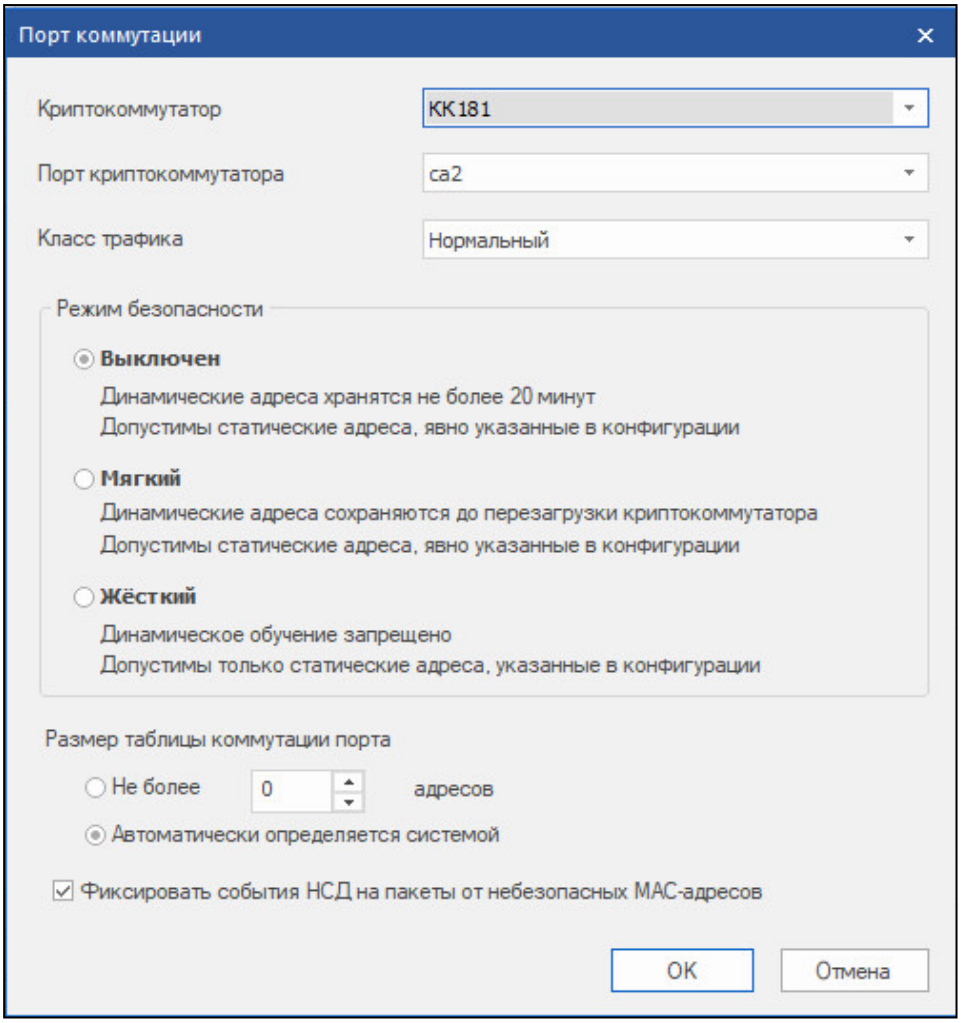
1. Перейдите к списку виртуальных коммутаторов и нажмите на панели инструментов кнопку "Создать виртуальный коммутатор" (или активируйте соответствующую команду контекстного меню).

   На экране появится окно "Виртуальный коммутатор", предназначенное для настройки параметров создаваемого виртуального коммутатора.

2. Введите название и краткое описание создаваемого виртуального коммутатора.

3. Добавьте в состав создаваемого виртуального коммутатора порты коммутации. Для этого нажмите кнопку "Добавить", расположенную справа.

   На экране появится окно "Порт коммутации".



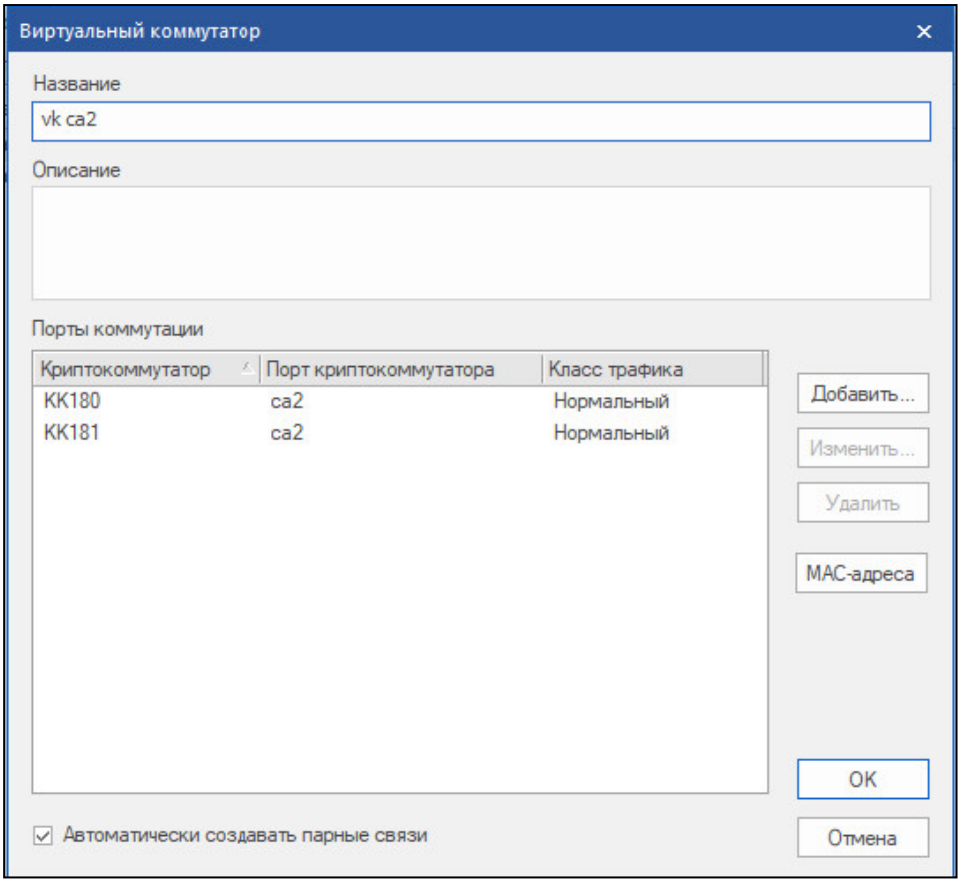
4. Укажите параметры создаваемого порта коммутации.

Поле	Описание
Криптокоммутатор	Выберите из раскрывающегося списка криптокоммутатор, порт которого должен войти в состав виртуального коммутатора
Порт криптокоммутатора	Укажите порт криптокоммутатора, выбрав его из раскрывающегося списка интерфейсов
Класс трафика	Выберите класс трафика из раскрывающегося списка
Режим безопасности	Укажите режим безопасности, в котором должен работать данный порт коммутации
Размер таблицы коммутации порта	Задайте размер таблицы коммутации порта. Максимальное количество адресов для одного порта зависит от используемой аппаратной платформы и приведено в Приложении (см. стр. **67**)
Фиксировать события НСД...	Если не требуется фиксировать события НСД на пакеты от небезопасных MAC-адресов, удалите соответствующую отметку, установленную по умолчанию

5. Нажмите кнопку "OK".

   Окно "Порт коммутации" закроется, и в окне "Виртуальный коммутатор" в списке появится добавленный порт коммутации.

6. Нажмите кнопку "Добавить..." и добавьте в список второй порт коммутации (см. пп. **4**, **5**).



Для изменения списка портов и их параметров используйте кнопки "Добавить...", "Изменить..." и "Удалить" (см. рисунок выше).

Внимание! По умолчанию в создаваемом виртуальном коммутаторе будут автоматически созданы парные связи между криптокоммутаторами, чьи порты входят в его состав. Если необходимо изменить парные связи, удалите соответствующую отметку в нижней части окна (см. рисунок выше) и установите парные связи вручную (об установлении парных связей вручную см. стр. **27**).

7. При необходимости задать статические MAC-адреса нажмите кнопку "MAC-адреса", расположенную справа (см. рисунок выше).

   На экране появится окно "Управление MAC-адресами".

   В левой части окна расположен список портов коммутации виртуального коммутатора. В правой части окна — списки MAC-адресов, назначенных портам коммутации.

8. Для назначения MAC-адреса выберите в списке порт коммутации и нажмите в панели инструментов кнопку "Добавить статический адрес".

   На экране появится окно, предназначенное для ввода MAC-адреса.

9. Введите MAC-адрес и нажмите кнопку "OK".

   Введенный адрес будет добавлен в список MAC-адресов выбранного порта коммутации.

10. Задайте все необходимые статические адреса (см. пп. **8**, **9**) и нажмите кнопку "Закрыть".

    Окно "Управление MAC-адресами" закроется.

11. Для сохранения настроек нажмите в окне "Виртуальный коммутатор" кнопку "OK".

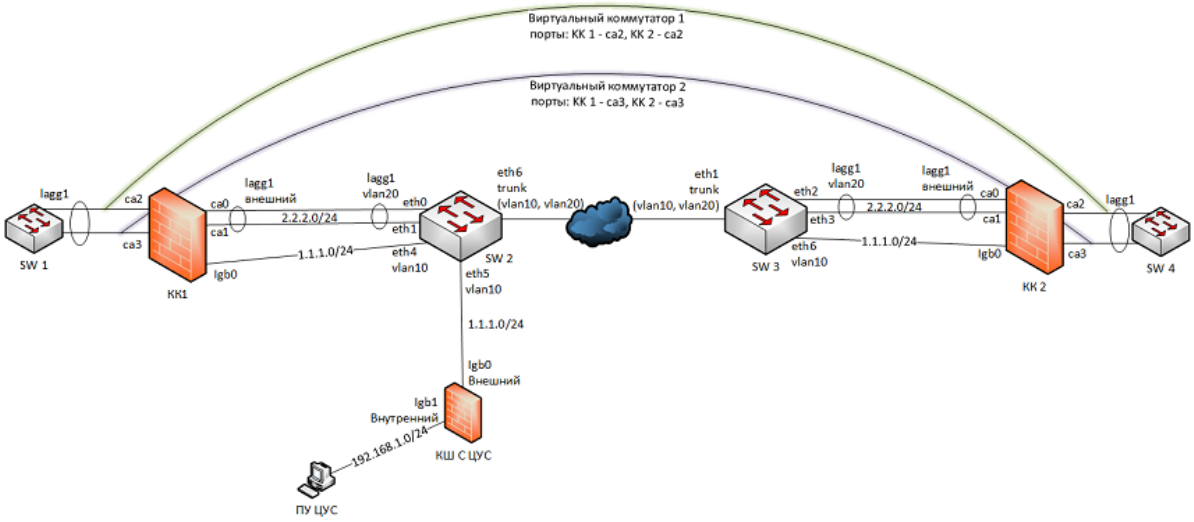
    Окно "Виртуальный коммутатор" закроется, и в списке виртуальных коммутаторов появится новый объект.

Сценарии применения криптокоммутаторов повышенной производительности

В данном подразделе приведены сценарии применения криптокоммутаторов в сетях L2VPN.

Сценарий 1

На рисунке ниже представлена схема подключения криптокоммутаторов КК 1 и КК 2 к стороннему оборудованию с агрегированными интерфейсами.



Криптокоммутаторы КК 1 и КК 2 внутренними интерфейсами подключены соответственно к коммутаторам SW 1 и SW 4 с агрегированными интерфейсами lagg1.

Внутренними интерфейсами КК 1 и КК 2 являются порты криптоускорителей ca2 и ca3. При настройке интерфейсов криптокоммутаторов тип ca2 и ca3 должен быть задан как "Порт криптокоммутатора".

В качестве внешних интерфейсов криптокоммутаторов КК 1 и КК 2 используются порты криптоускорителей ca0 и ca1, агрегированные в логические интерфейсы lagg1.

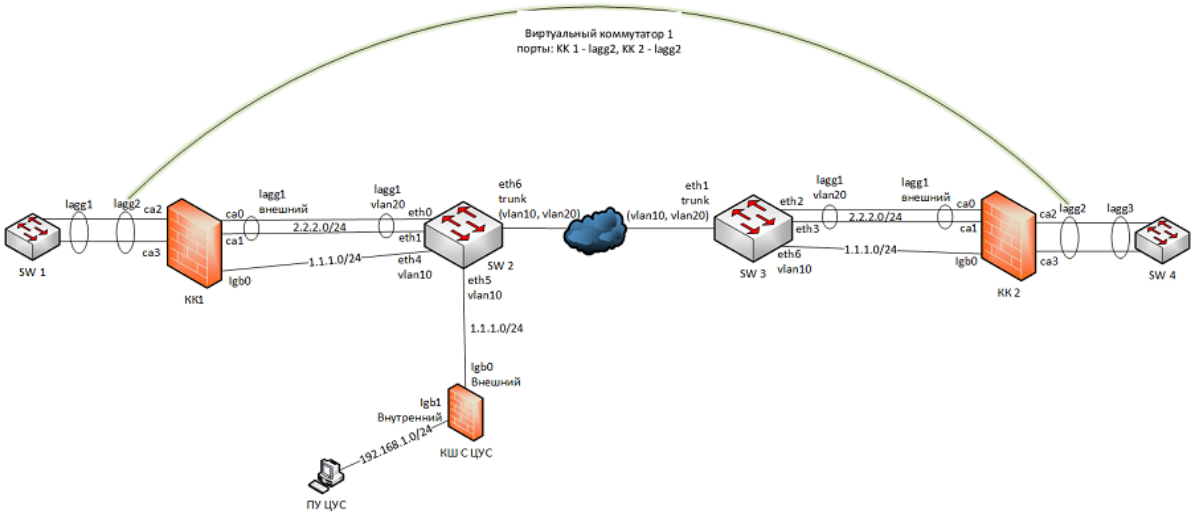
Для связи с ЦУС в криптокоммутаторах используются порты lgb0. Тип интерфейса у этих портов должен иметь значение "Не определен".

Рабочее место администратора (ПУ ЦУС) расположено в подсети, защищаемой КШ с ЦУС.

Для работы L2VPN необходимо создать два виртуальных коммутатора. В первый виртуальный коммутатор необходимо включить порты ca2 криптокоммутаторов КК 1 и КК 2, во второй — порты ca3.

Сценарий 2

Данный сценарий отличается от сценария 1 агрегированием внутренних интерфейсов криптокоммутаторов КК 1 и КК 2 (см. рисунок ниже).



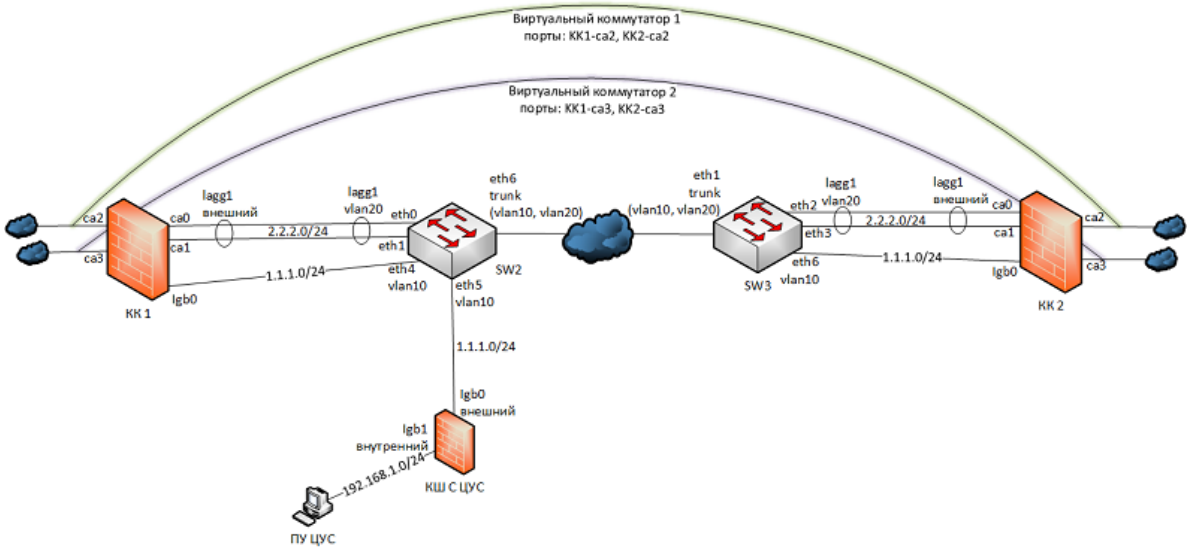
Интерфейсы ca2 и ca3 криптокоммутаторов КК 1 и КК 2 объединены в логический интерфейс lagg2.

При настройке интерфейсов криптокоммутаторов тип логического интерфейса lagg2 должен быть задан как "Порт криптокоммутатора".

Для работы L2VPN необходимо создать виртуальный коммутатор, включающий в себя порты lagg2 криптокоммутаторов КК 1 и КК 2.

Сценарий 3

На рисунке ниже показано подключение стороннего оборудования к внутренним интерфейсам ca2 и ca3 криптокоммутаторов КК 1 и КК 2. Сторонним оборудованием может быть, например, коммутатор, маршрутизатор, хост и т. п.



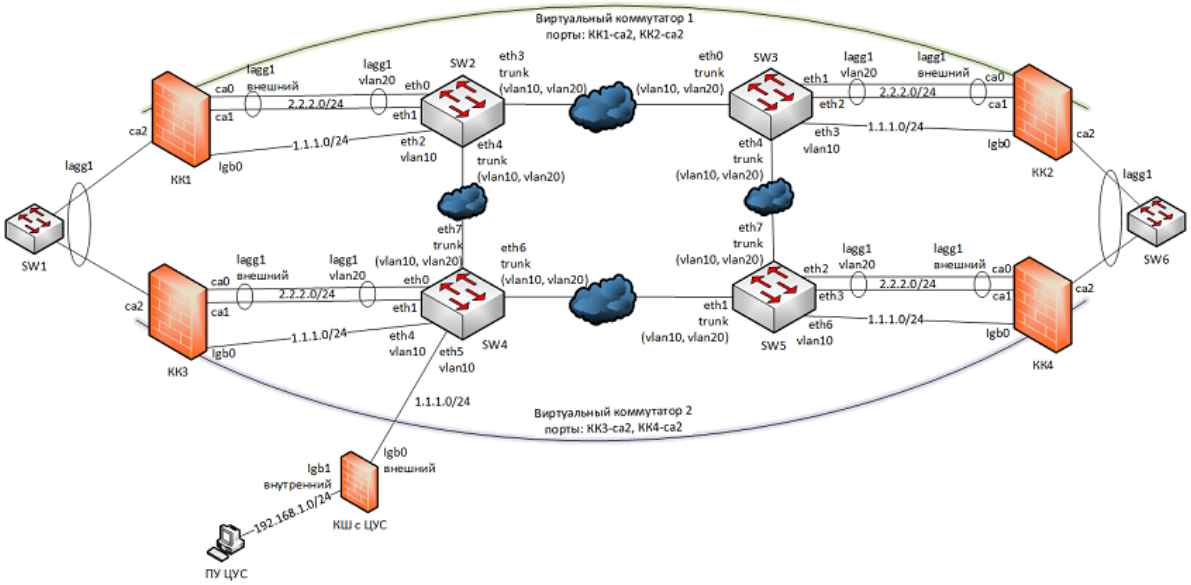
При настройке криптокоммутаторов КК 1 и КК 2 интерфейсам ca2 и ca3 необходимо задать тип "Порт криптокоммутатора".

Порты ca2 входят в состав виртуального коммутатора 1, а порты ca3 — в состав виртуального коммутатора 2.

Подключение криптокоммутаторов к коммутаторам SW2 и SW3 такое же, как и в предыдущих сценариях.

Сценарий 4

На рисунке ниже представлена схема подключения криптокоммутаторов к стороннему оборудованию, поддерживающая работоспособность L2VPN в случае выхода из строя какого-либо сетевого устройства, участвующего в передаче трафика между SW1 и SW6.



Криптокоммутаторы КК 1 и КК 3 внутренними интерфейсами ca2 подключены к агрегированному интерфейсу lagg1 устройства SW1. Аналогично криптокоммутаторы КК 2 и КК 4 подключены к SW6.

Тип интерфейсов ca2 криптокоммутаторов — "Порт криптокоммутатора".

Интерфейсы ca0 и ca1 криптокоммутаторов агрегированы во внешний интерфейс lagg1 и подключены к агрегированным интерфейсам устройств SW2–SW5.

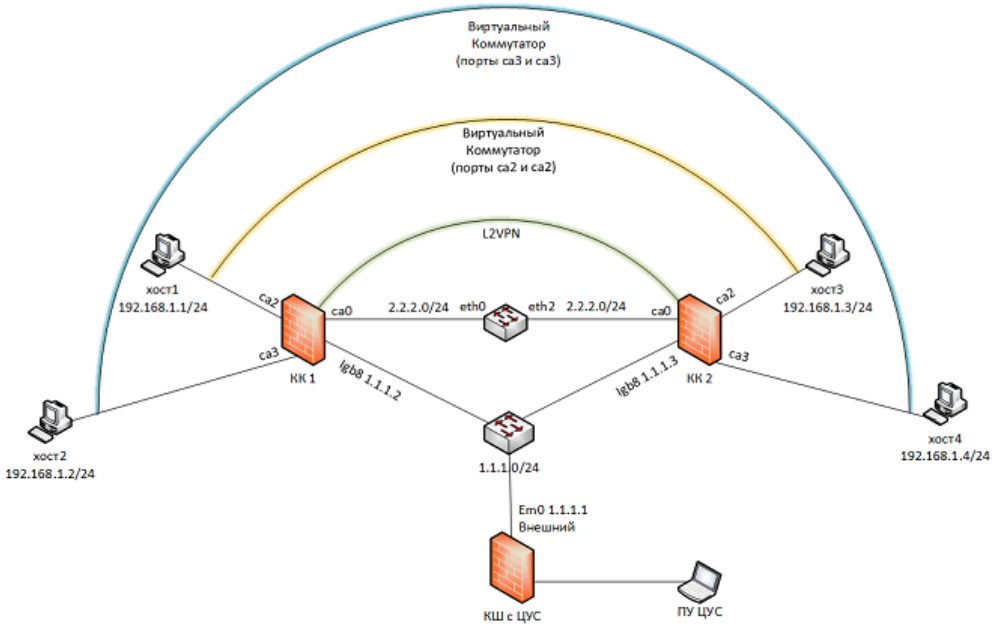
Порты ca2 криптокоммутаторов КК 1 и КК 2 входят в состав виртуального коммутатора 1. Порты ca2 криптокоммутаторов КК 3 и КК4 входят в состав виртуального коммутатора 2.

При выходе из строя какого-либо из устройств, относящихся к виртуальному коммутатору, весь трафик между SW1 и SW6 перенаправляется на устройства, относящиеся к другому виртуальному коммутатору.

Сценарий 5

Ниже приведена схема включения криптокоммутаторов, обеспечивающая прохождение трафика между хостами:

- хост 1 <—> хост 3;
- хост 2 <—> хост 4.

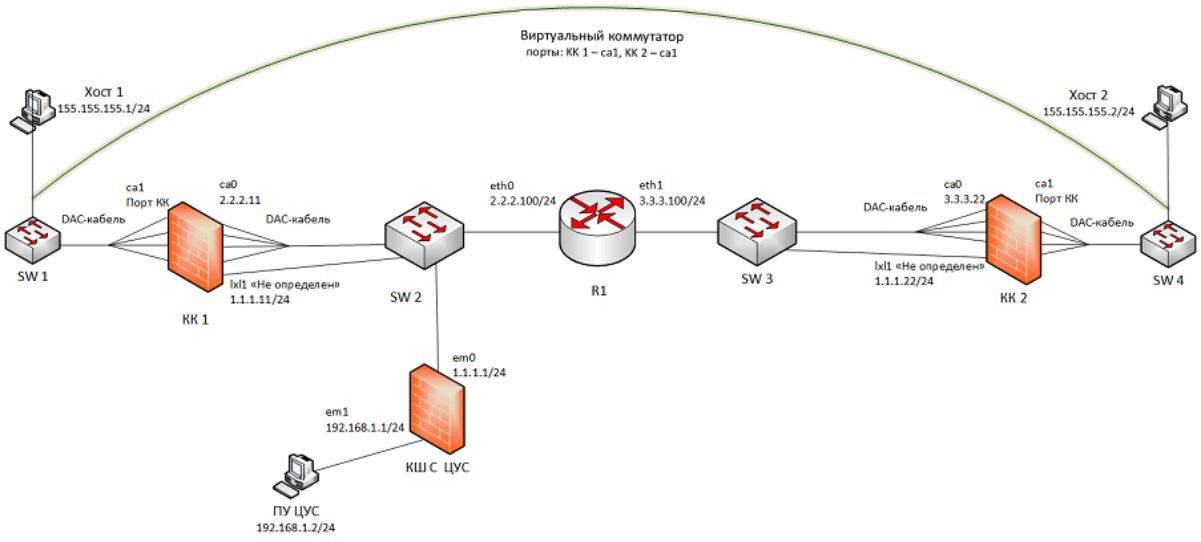


В схеме используются два виртуальных коммутатора.

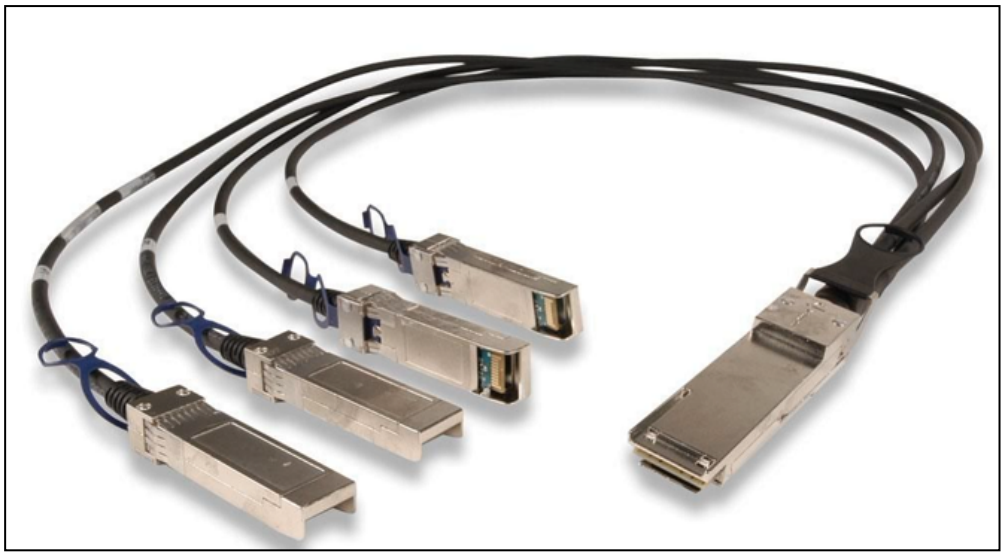
Между внешними интерфейсами размещен коммутатор стороннего производителя. Если на коммутаторе применяется агрегация интерфейсов, на криптокоммутаторах КК 1 и КК 2 также следует объединить интерфейсы ca0 и ca1 в логический интерфейс и задать его тип как внешний.

Сценарий 6

На рисунке ниже представлена схема подключения криптокоммутаторов с использованием DAC-кабеля.



DAC-кабель имеет следующий вид:



4 разъема по 10 Гб подключаются к плате криптокоммутатора, другой конец, пропускной способностью 40 Гб/с, подключается к коммутатору. При работе по данной схеме первые 4 порта — это один интерфейс ca0, а вторые 4 порта — ca1 (см. рисунок ниже).

При использовании DAC-кабеля на криптокоммутаторах КК 1 и КК 2 в ПУ ЦУС настраиваются только два интерфейса: ca0 — внешний и ca1 — порт криптокоммутатора.

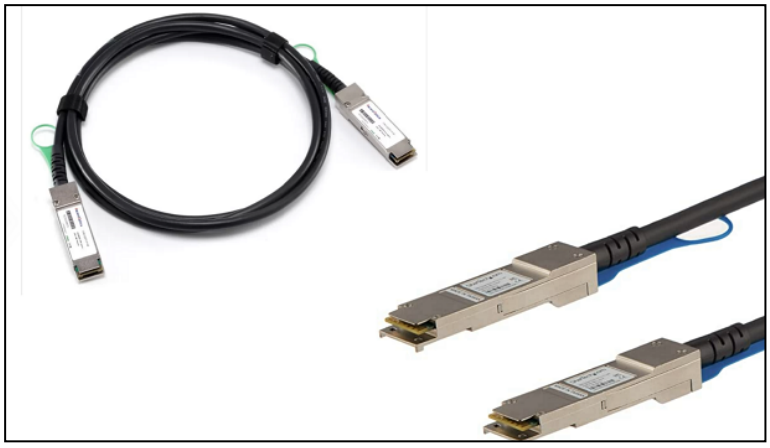
Для связи с ЦУС в криптокоммутаторах КК 1 и КК 2 используются интерфейсы lxl1 с типом "Не определен".

Для работы L2VPN и передачи шифрованного трафика между хостами (на схеме —Хост 1 и Хост 2) необходимо создать виртуальный коммутатор и включить в него порты ca1 криптокоммутаторов КК 1 и КК 2.

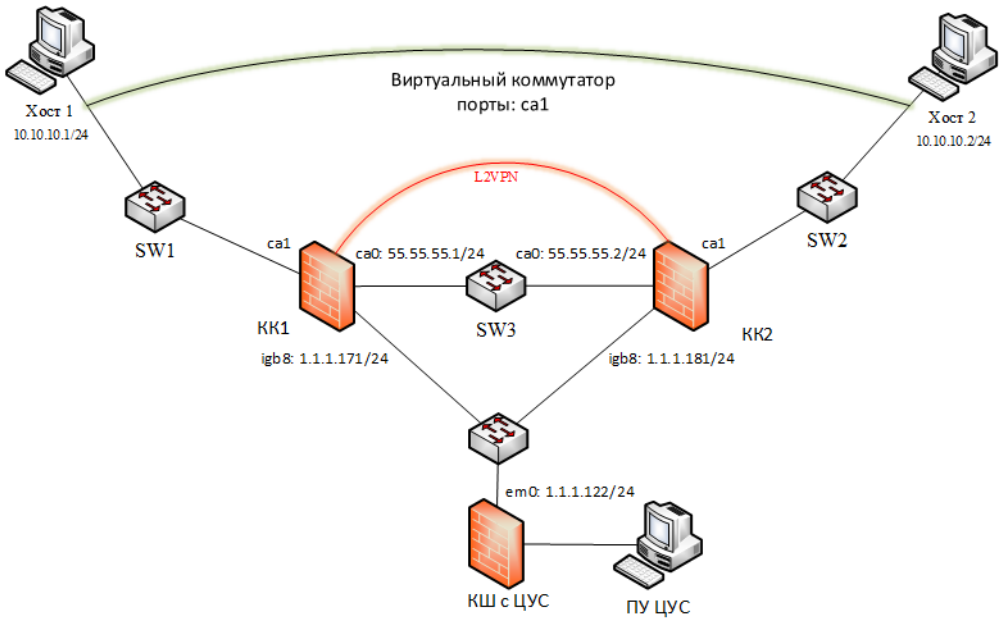
Сценарий 7

Криптокоммутатор повышенной производительности имеет в своем составе два интерфейса, пропускная способность каждого из которых составляет 40 Гб/с.

Для подключения криптокоммутатора используется специальный кабель с повышенной пропускной способностью (см. рисунок ниже).



На рисунке ниже показано применение криптокоммутаторов с повышенной производительностью для шифрования трафика между хостами, находящимися в одной подсети.



Между внешними интерфейсами ca0 криптокоммутаторов КК 1 и КК 2 размещен коммутатор SW3, а интерфейсы ca1, имеющие тип "Порт криптокоммутатора", подключены соответственно к коммутаторам SW1 и SW2.

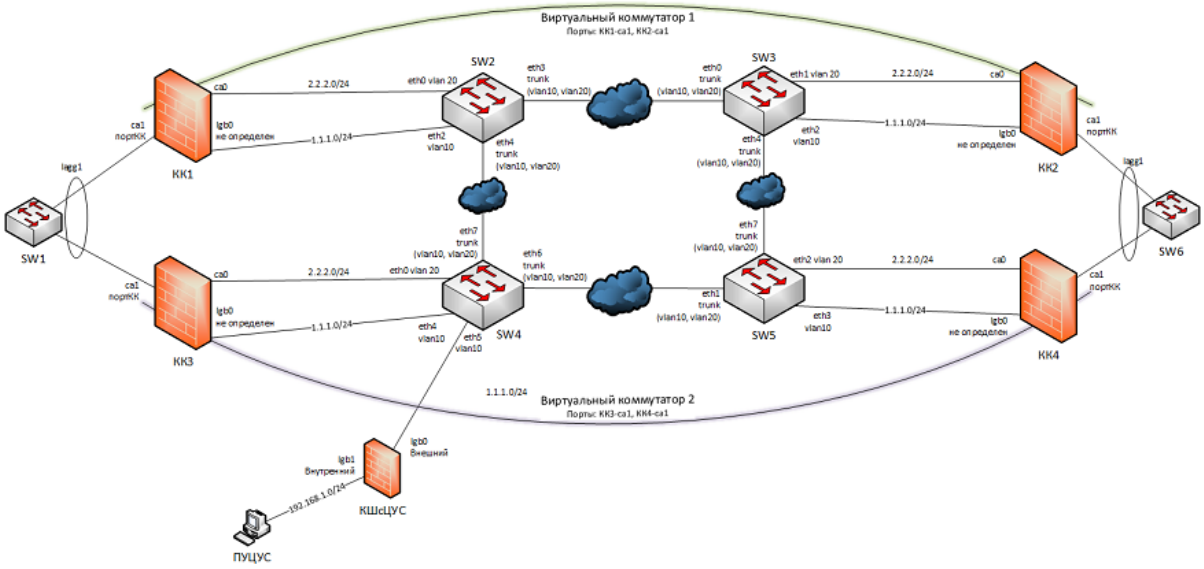
Внимание! Для подключения криптокоммутаторов в настройках интерфейсов используются только порты ca0 и ca1. При этом порт ca0 задается как внешний, а порт ca1 — как порт крипрокоммутатора.

Интерфейсы igb8 КК 1 и КК 2 предназначены для связи с ЦУС и должны иметь тип "Не определен".

Портами коммутации в виртуальном коммутаторе являются порты ca1 криптокоммутаторов КК 1 и КК 2.

Сценарий 8

На рисунке ниже представлена схема подключения криптокоммутаторов к стороннему оборудованию, поддерживающая работоспособность L2VPN в случае выхода из строя какого-либо сетевого устройства, участвующего в передаче трафика между SW1 и SW6.



Сторонним оборудованием являются коммутаторы SW1 и SW6.

Для шифрования трафика между хостами (Хост1 и Хост2, расположенные соответственно за SW1 и SW6, на схеме не показаны) используются криптокоммутаторы КК 1 – КК 4.

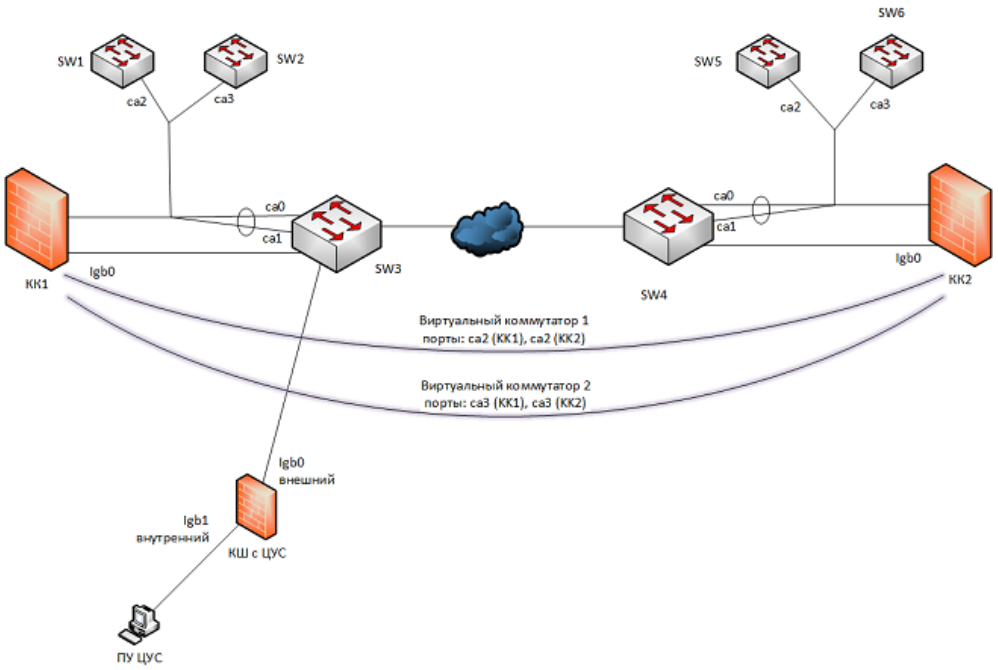
Пары криптокоммутаторов КК 1 – КК 2 и КК 3 – КК 4 расположены в разных подсетях. В каждой паре криптокоммутаторы связаны между собой внешними интерфейсами ca0.

Внутренними интерфейсами криптокоммутаторов являются порты ca1, которые подключаются к агрегированным интерфейсам коммутаторов SW1 и SW6 и выполняют роль портов коммутации в виртуальных коммутаторах ВК1 и ВК2 (см. рисунок выше).

Для связи с ЦУС в криптокоммутаторах используется интерфейс igb0, имеющий тип "Не определен".

Сценарий 9

На рисунке ниже показано подключение криптокоммутаторов повышенной производительности с использованием breakout-кабеля и агрегацией интерфейсов.



Один конец кабеля с пропускной способностью 40 Гб/с подключается к интерфейсу криптокоммутатора КК1 (QSFP).

Агрегированные интерфейсы ca0 и ca1 по 10 Гб/с подключаются к коммутатору SW3 (SFP+). Два других интерфейса ca2 и ca3 (по 10 Гб/с) подкючаются к коммутаторам соответственно SW1 и SW2.

Точно так же осуществляется подключение криптокоммутатора КК2 к коммутаторам SW4 — SW6.

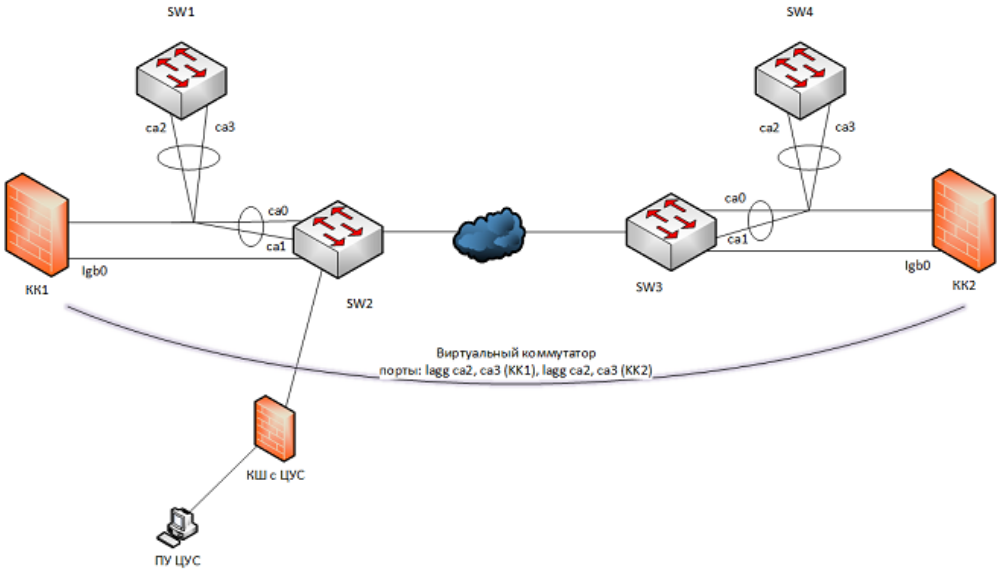
Для связи с ЦУС в криптокоммутаторах используются интерфейсы lgb0.

Таким образом имеются два виртуальных коммутатора:

- ВК 1 с портами коммутации ca2(КК1) и ca2 (КК2);
- ВК 2 с портами коммутации ca3(КК1) и ca3 (КК2).

Сценарий 10

На рисунке ниже криптокоммутатор КК1 подключен breakout-кабелем к коммутаторам SW1 и SW2, а криптокоммутатор КК2 — к коммутаторам SW3 и SW4. При подключении к коммутаторам используется агрегация интерфейсов (см. рисунок).



В виртуальном коммутаторе портами коммутации являются порт с агрегированными интерфейсами ca2 и ca3 КК1 и порт с агрегированными интерфейсами ca2 и ca3 КК2.

Приложение

Переход к меню локальной настройки параметров сетевого устройства

Для перехода к меню:

1. Откройте главное окно локального управления сетевым устройством. Для этого необходимо нажать клавишу <Enter> в короткий промежуток времени после перезагрузки узла.

```
1: Завершение работы
2: Перезагрузка
3: Управление конфигурацией
4: Настройка безопасности
5: Настройка СД <функция недоступна>
6: Тестирование
0: Выход
Выберите пункт меню (0–6):
```

2. Введите номер команды "Управление конфигурацией" и нажмите клавишу <Enter>.

   На экране появится меню локальной настройки параметров сетевого устройства.

```
1: Сохранение конфигурации
2: Загрузка конфигурации
3: Изменение адреса активного ЦУС
4: Настройка PPPoE-соединений
5: Настройка шифрования
6: Настройка фрагментации
7: Настройка коммутации
8: Настройка отладочного журнала
9: Настройка доступа удаленного терминала
10: Настройка режима ретранслятора DHCP (replace)
11: Выключение Agent relay information (опции 82) на DHCP-
ретрансляторе
12: Установить ПО криптоускорителя
0: Выход
Выберите пункт меню (0 - 12):
```

Просмотр сведений о состоянии каналов

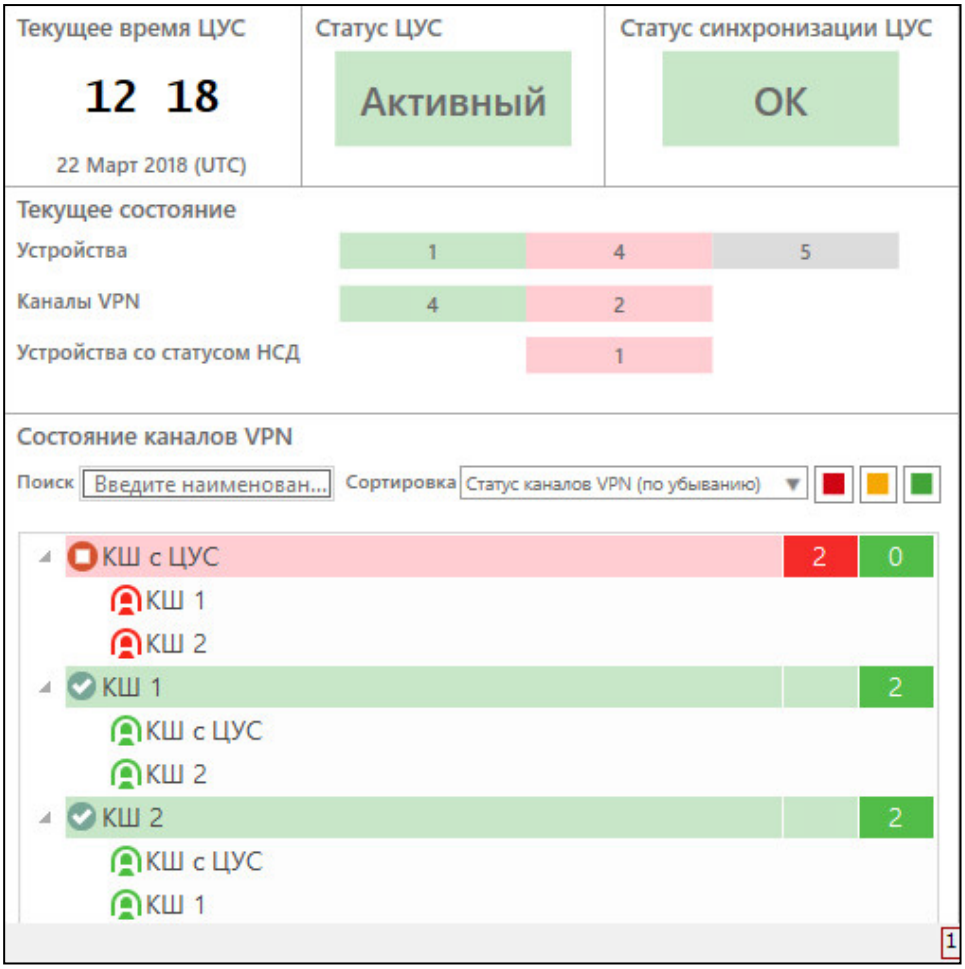
В главном окне программы управления можно просмотреть текущее состояние VPN- каналов комплекса, а также состояние каналов определенного криптошлюза.

Для просмотра сведений о каналах комплекса:

- В главном окне программы управления в панели навигации выберите раздел "Центр управления сетью".

  В области отображения информации появятся сведения о состоянии VPN-каналов:

  - общее количество рабочих и нерабочих каналов;
  - список криптошлюзов с указанием для каждого из них парных связей, а также рабочих и нерабочих каналов.



Работающие и неработающие криптошлюзы и каналы помечаются пиктограммами зеленого и красного цвета соответственно. Криптошлюзы с рабочими и нерабочими каналами помечаются пиктограммой желтого цвета.

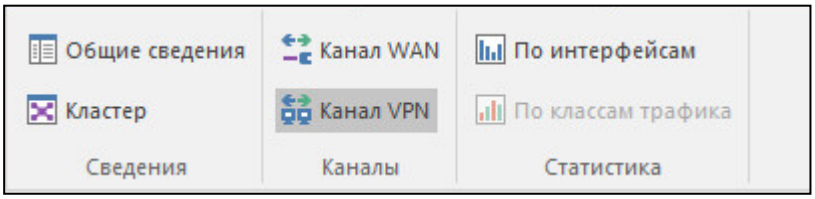
В списке криптошлюзов предусмотрены поиск по наименованию и сортировка по убыванию или возрастанию статуса. Под статусом в данном случае понимается количество нерабочих каналов.

Для просмотра сведений о каналах криптошлюза:

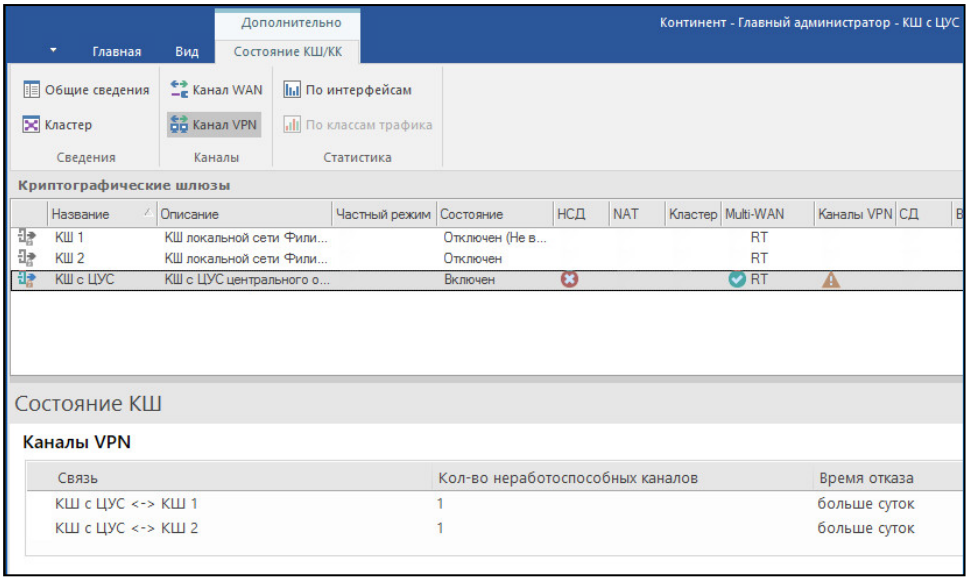
1. В списке криптошлюзов выберите устройство.

   В дополнительном окне отобразятся сведения о выбранном устройстве (состав сведений зависит от настроек интерфейса программы управления).

2. В дополнительном окне перейдите на вкладку "Состояние КШ" и при необходимости нажмите кнопку "Канал VPN" в панели инструментов.



В дополнительном окне появятся сведения о каналах VPN.



Примечание. Кроме сведений о каналах в дополнительном окне могут отображаться другие сведения в зависимости от нажатых кнопок в панели инструментов.

В разделе "Каналы VPN" отображается список парных связей данного КШ с указанием количества неработоспособных каналов для каждой из них и времени отказа.

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 отсылает пакет со своего реального адреса на виртуальный адрес получателя. При этом КШ отправителя перед зашифрованием заменяет реальный адрес отправителя на виртуальный.

В зашифрованном пакете адреса отправителя и получателя – виртуальные.

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

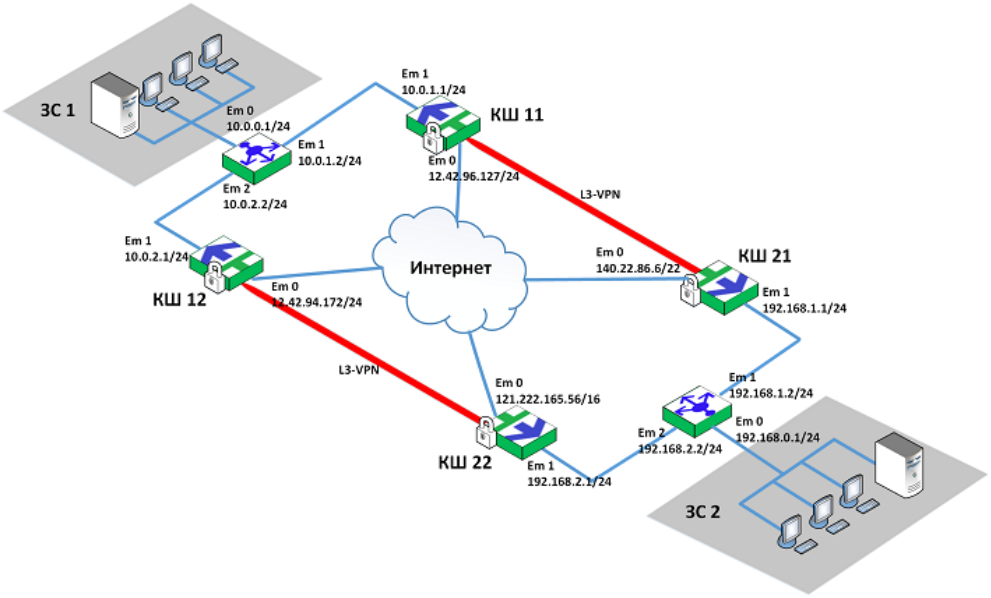
Для настройки схемы с применением виртуальной адресации необходимо для каждой пары отправитель – получатель назначить виртуальные адреса. Виртуальный адрес отправителя или получателя назначается хосту или подсети, которые являются зарегистрированными сетевыми объектами.

Назначение виртуального адреса сетевому объекту описано в процедуре создания сетевого объекта (см. стр. **17**).

Увеличение пропускной способности VPN-канала

В данном разделе приведен пример использования фермы КШ для увеличения пропускной способности VPN-канала по схеме "точка-точка".

На рисунке ниже показаны две защищаемые сети ЗС 1 и ЗС 2.



В каждой защищаемой сети устанавливают по одинаковой ферме. Нагрузка распределяется между КШ в ферме. Ферма состоит из нескольких КШ и балансировщика, распределяющего пакеты из защищенной сети между данными КШ по алгоритму Round Robin. Количество КШ определяется требуемой пропускной способностью VPN-канала.

На рисунке в защищаемой сети ЗС 1 установлены КШ 11 и КШ 12, в ЗС 2 — соответственно КШ 21 и КШ 22.

В качестве балансировщика может быть использован дополнительный КШ в режиме Multi-WAN "Балансировка трафика" (см. [**5**], "Балансировка трафика между внешними интерфейсами сетевого устройства"). Также возможно использование балансировщиков типа RR-DNS, L3/L4.

КШ из разных сетей поддерживают связь попарно по непересекающимся каналам.

Используются следующие интерфейсы:

КШ 11

Внешний	Em 0	12.42.96.127/24
Внутренний	Em 1	10.0.1.1/24

КШ 12

Внешний	Em 0	12.42.94.172/24
Внутренний	Em 1	10.0.2.1/24

КШ 21

Внешний	Em 0	140.22.86.6/22
Внутренний	Em 1	192.168.1.1/24

КШ 22

Внешний	Em 0	121.222.165.56/16
Внутренний	Em 1	192.168.2.1/24

Балансировщик ЗС 1

Em 0	10.0.0.1/24
Em 1	10.0.1.2/24

Em 2	10.0.2.2/24

Балансировщик ЗС 2

Em 0	192.168.0.1/24
Em 1	192.168.1.2/24
Em 2	192.168.2.2/24

Для настройки фермы шлюзов:

1. Создайте следующие сетевые объекты:

   Сетевые объекты с виртуальными адресами

Параметр	Сет. объект 1	Сет. объект 2	Сет. объект 3	Сет. объект 4
Название	ЗС КШ11	ЗС КШ12	ЗС КШ21	ЗС КШ22
Тип передачи данных	Unicast			
Описание	Защищаемая сеть КШ11	Защищаемая сеть КШ12	Защищаемая сеть КШ21	Защищаемая сеть КШ22
IP-адрес	10.0.0.0		192.168.0.0	
Маска	255.255.255.0			
Тип привязки	Защищаемый			
Криптошлюз	КШ11	КШ12	КШ21	КШ22
Интерфейс	Em1			
Трансляция адреса внутри VPN	Да			
Виртуальный адрес	173.17.2.0	173.17.3.0	173.17.0.0	173.17.1.0
Маска	255.255.255.0			
Регистрация	Определяется интерфейсом			

   Сетевые объекты с реальными адресами

Параметр	Сет. объект 5	Сет. объект 6	Сет. объект 7	Сет. объект 8
Название	ВС КШ11	ВС КШ21	ВС КШ12	ВС КШ22
Тип передачи данных	Unicast			
Описание	Внутренняя сеть КШ11	Внутренняя сеть КШ21	Внутренняя сеть КШ12	Внутренняя сеть КШ22
IP-адрес	173.17.2.0	173.17.0.0	173.17.3.0	173.17.1.0
Маска	255.255.255.0			
Тип привязки	Внутренний			
Криптошлюз	КШ11	КШ21	КШ12	КШ21
Интерфейс	Em1			
Трансляция адреса внутри VPN	Нет			
Регистрация	Определяется интерфейсом			

2. Создайте следующие правила фильтрации:

Параметр	Прав. фильт.1	Прав. фильт. 2	Прав. фильт. 3	Прав. фильт. 4
Название	ПФ11>21	ПФ21>11	ПФ12>22	ПФ22>12
Описание	Правило фильтрации 11>21	Правило фильтрации 21>11	Правило фильтрации 12>22	Правило фильтрации 22>12
Отправитель	ЗС КШ11	ЗС КШ21	ЗС КШ12	ЗС КШ22
Инверсия адреса отправителя	Нет			
Получатель	ЗС КШ21	ЗС КШ11	ЗС КШ22	ЗС КШ12
Инверсия адреса получателя	Нет			
Сервисы	Любой TCP, Любой UDP, Любой ICMP			
Действие	Пропустить			
Временной интервал	Постоянно			
Класс трафика	Нормальный			
Регистрация	Определяется источником/получателем			
Контролировать состояние соединения	Да			
Защита от DoS-атак	Нет			
Применить и завершить обработку	Да			
Отключено	Нет			

3. Создайте следующие правила трансляции:

Параметр	Прав. транс. 1	Прав. транс. 2	Прав. транс. 3	Прав. транс. 4
Устройство	КШ11	КШ21	КШ12	КШ22
Название	ПТ11	ПТ21	ПТ12	ПТ22
Описание	Правило трансляции 1:1			
Направление	1:1			
Источник	ВС КШ11	ВС КШ21	ВС КШ12	ВС КШ22
Получатель	ЗС КШ11	ЗС КШ21	ЗС КШ12	ЗС КШ22
Интерфейс	Em1			
Временной интервал	Постоянно			
Класс трафика	Нормальный			
Регистрация	Определяется источником/получателем			
Трансляция адреса источника… изменить на	192.168.0.0 255.255.255.0	10.0.0.0 255.255.255.0	192.168.0.0 255.255.255.0	10.0.0.0 255.255.255.0
Отключено	Нет			

4. Установите парные связи КШ11 -- КШ21 и КШ12 -- КШ22.

Максимальный размер таблицы коммутации порта

Ниже в таблице приведено максимальное количество адресов для одного порта в зависимости от используемой в АПКШ "Континент" аппаратной платформы.

Аппаратная платформа	Максимальное количество адресов
IPC-10 (LN-010A) IPC-10 (S088) IPC-10 (S185) IPC-50 (LN-010C)	10
IPC-25 (92D9) IPC-25 (9830) IPC-25 (GA6309iGN1-B2) IPC-25 (GA630iB1-B2) IPC-25 (S115) IPC-R10	25
IPC-100 (92E3) IPC-100 (G560) IPC-100 (ND_S102) IPC-100 (NM_S102) IPC-100 (S102) IPC-R50	100
IPC-400 (9297) IPC-400 (S021) IPC-400 (Small Custom) IPC-500F (LN-015C) IPC-500 (LN-015B) IPC-600 (DV-030A) IPC-800F (DV-030B) IPC-R300 IPC-R550 IPC-R800	400
IPC-1000 (9297) IPC-1000 (DV-031A) IPC-1000F2 (9297) IPC-1000F2 (DV-031C) IPC-1000F2 (S021) IPC-1000F (9297) IPC-1000F (DV-031B) IPC-1000F (S021) IPC-1000 (IBM x3650M2) IPC-1000 (Medium Custom) IPC-1000 (NDF_S021) IPC-1000NF2 (DV-031F) IPC-1000 (NMF_S021) IPC-1000 (S021) IPC-1010 (9297) IPC-2000F (S021) IPC-R1000 IPC-VM	1000

Аппаратная платформа	Максимальное количество адресов
IPC-3000 (Enterprise Custom) IPC-3000F40 (LN-021) IPC-3000FC-40G (LN-021A) IPC-3000FC (LN-021A) IPC-3000F LE (LN-021) IPC-3000F (LN-021) IPC-3000F (S021) IPC-3000 (LN-021D) IPC-3000 (NBF_S021) IPC-3000 (NDF_S021) IPC-3000NF2 LE (LN-021) IPC-3000NF2 (LN-021E) IPC-3000 (NMF_S021) IPC-3020 (S021) IPC-3034F (LN-021C) IPC-3034F (S021) IPC-3034 (S021) IPC-5000F (MS-145) IPC-R3000	3000

Документация

1. Аппаратно-программный комплекс шифрования "Континент". Версия 3.9 (исполнение 3.М3). Руководство администратора. Принципы функционирования комплекса.
2. Аппаратно-программный комплекс шифрования "Континент". Версия 3.9 (исполнение 3.М3). Руководство администратора. Управление комплексом.
3. Аппаратно-программный комплекс шифрования "Континент". Версия 3.9 (исполнение 3.М3). Руководство администратора. Ввод в эксплуатацию.
4. Аппаратно-программный комплекс шифрования "Континент". Версия 3.9 (исполнение 3.М3). Руководство администратора. Межсетевое экранирование.
5. Аппаратно-программный комплекс шифрования "Континент". Версия 3.9 (исполнение 3.М3). Руководство администратора. Сетевые функции.