УТВЕРЖДЕНО

BY.РТНК.45007-01 34 01-ЛУ

Программный продукт «Конфигуратор Bel VPN» Руководство пользователя

BY.РТНК.45007-01 34 01

Листов 20

Инд. № подл.	Подп. и дата	Взам. инд. №	Инв. № дубл.	Подп. и дата

2022

Оглавление

1. Общие сведения, назначение

Программный продукт «Конфигуратор Bel VPN» (далее — ПП «Конфигуратор Bel VPN», конфигуратор) представляет собой псевдографический интерфейс взаимодействия пользователя с ПАК (ПК) «Шлюз безопасности Bel VPN Gate 4.5» (далее – шлюз). Предназначен для проведения первоначальной настройки шлюза, а также для внесения изменений в настройки в последствии.

2. Работа с программным продуктом «Конфигуратор Bel VPN»

2.1 Файлы необходимые для работы программного продукта «Конфигуратор Bel VPN»

Программный продукт «Конфигуратор Bel VPN» предустановлен на шлюз безопасности. Файлы продукта располагаются в директории `/opt/Configurator/`.

Также конфигуратор может дополнительно устанавливаться на шлюз Bel VPN Gate.

Для дополнительной установки поставляется в виде файла configurator_1.0.0_all.deb. Файл размещаемся в репозитории для обновления продуктов BEL VPN Gate http://updates.s-terra.by/ (например: http://updates.s-terra.by/stretch/configurator_1.0.0_all.deb).

После настройки репозитория для обновления продуктов BEL VPN Gate установка производится командой `apt install configurator`. Программный продукт устанавливается в папку `/opt/Configurator/`.

По окончании инсталляции конфигуратора необходимо перезапустить шлюз безопасности, после этого можно запустить конфигуратор.

2.2 Запуск программного продукта «Конфигуратор Bel VPN»

Запуск конфигуратора производится командой `conf` в ОС Debian.

Меню конфигуратора выполнено в виде древовидной структуры, предоставляющей доступ к настройкам различных параметров шлюза.

Навигация по меню конфигуратора осуществляется с помощью клавиш (кнопок) компьютерной клавиатуры «стрелка вверх», «стрелка вниз», «стрелка влево», «стрелка вправо», либо цифровых клавиш, соответствующих нужному пункту меню. Вход в нужный пункт меню осуществляется с помощью клавиш «Enter» или «Пробел». Возврат к предыдущей ветке меню производится либо через выбор опции <Назад>, либо с помощью клавиши «Esc». Выход из конфигуратора производится в Главном меню либо через выбор опции <Выход>, либо с помощью нажатия клавиши «Esc».

Структура меню конфигуратора представлена в Приложении.

Из Главного меню доступны настройки параметров операционной системы шлюза безопасности, настройки работы с сертификатами, настройки параметров защищенного соединения (политики ISAKMP, IPSec, настройка трафика, подлежащего шифрованию, настройка криптокарты), настройки интерфейсов и маршрутизации (Рисунок 1):

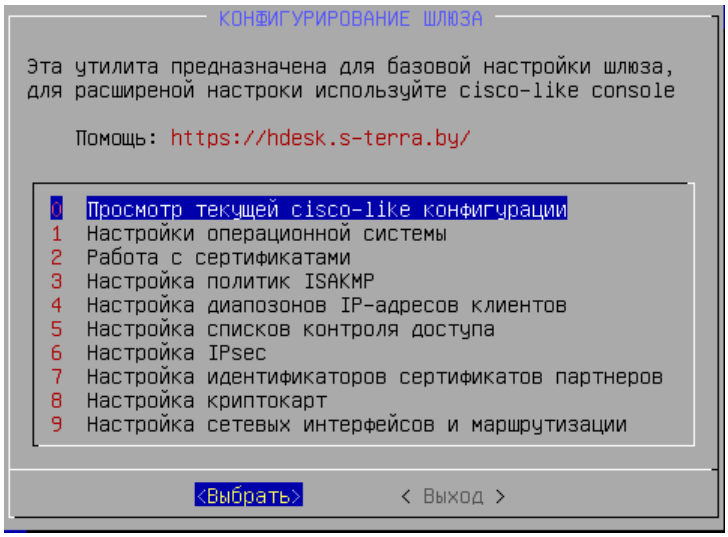

Рисунок 1

2.3 Просмотр текущей cisco-like конфигурации

Пункт меню «Просмотр текущей cisco-like конфигурации» позволяет просматривать текущую конфигурацию шлюза в cisco-like консоли (Рисунок 2):

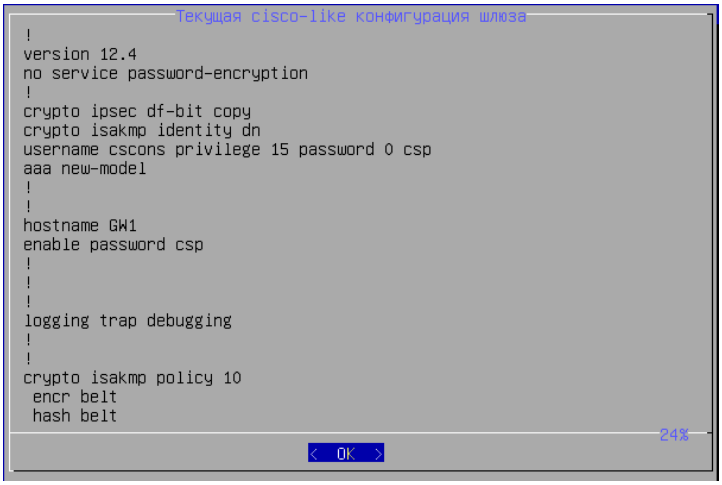

Рисунок 2

2.4 Настройки операционной системы

Пункт «Настройки операционной системы» (Рисунок 3) позволяет настроить следующие параметры:

- имя шлюза;
- дата и время;
- временная зона (часовой пояс);
- протокол NTP;
- настройки Syslog;
- доступ по SSH.

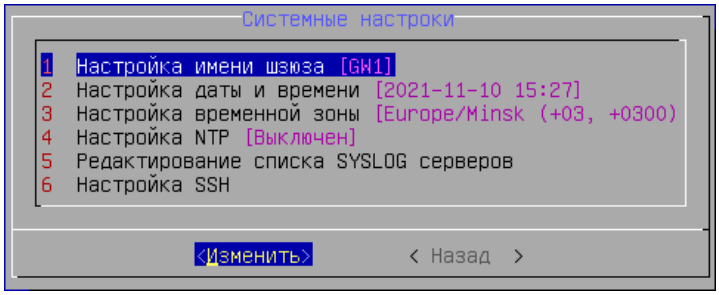

Рисунок 3

В каждом пункте подменю в квадратных скобках указывается текущее значение данной настройки.

2.4.1 Настройка имени шлюза

Для настройки имени шлюза используется пункт «1 Настройка имени шлюза» в меню «Настройки операционной системы» в котором, в соответствии с прилагаемой инструкцией, задается имя шлюза (Рисунок 4):

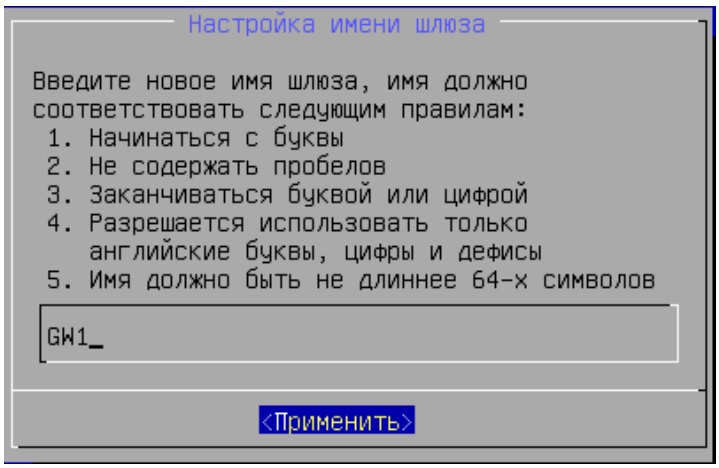

Рисунок 4

2.4.2 Настройка даты и времени

Для настройки даты и времени шлюза в меню «Настройки операционной системы» выбирается пункт «2 Настройка даты и времени» и устанавливаются необходимые значения даты и времени (Рисунок 5, Рисунок 6):

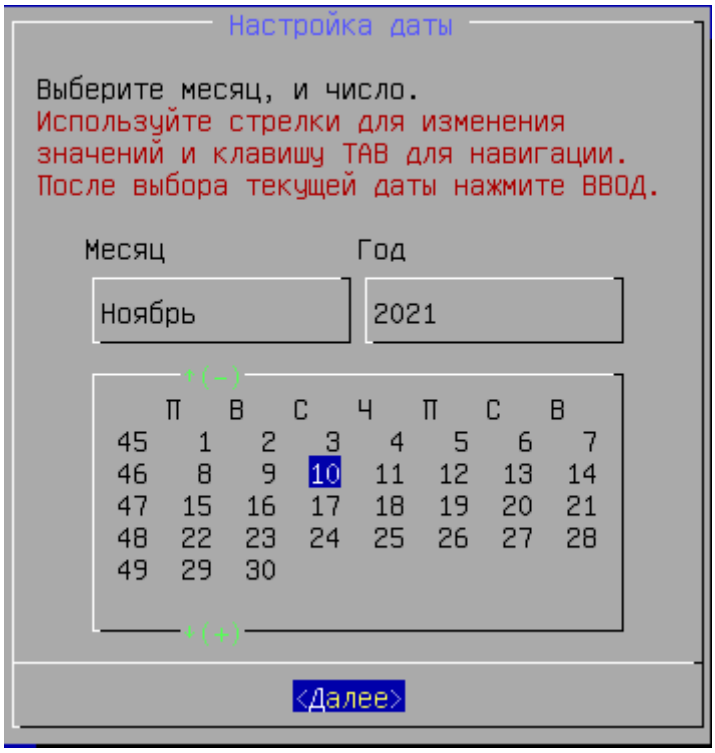

Рисунок 5

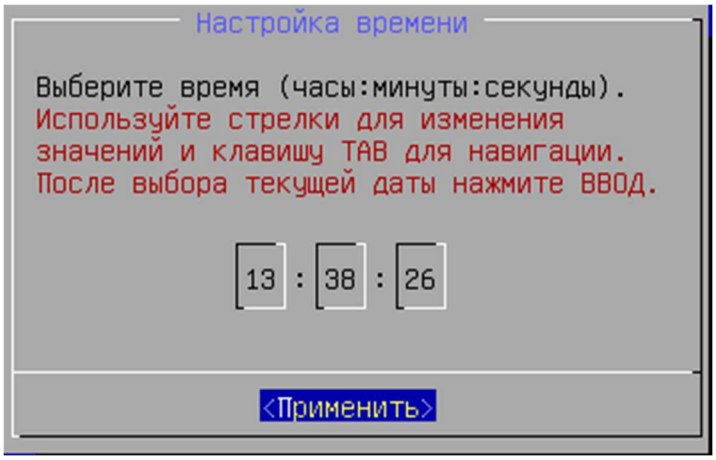

Рисунок 6

2.4.3 Настройка временной зоны

Для настройки временной зоны в меню «Настройки операционной системы» используется пункт «3 Настройка временной зоны». Далее выбирается географический район (Рисунок 7) и город (область) (Рисунок 8), соответствующий нужному часовому поясу:

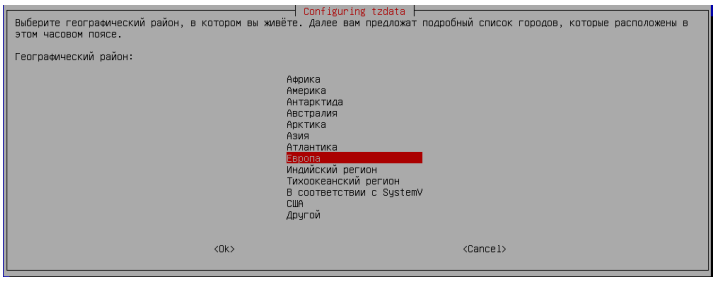

Рисунок 7

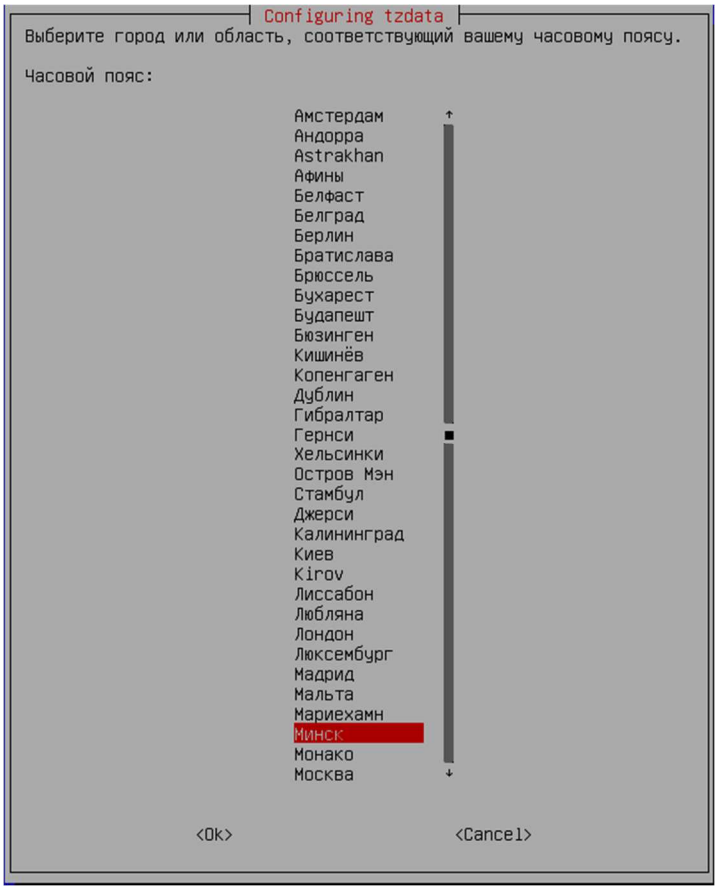

Рисунок 8

2.4.4 Настройка NT□

Для настройки синхронизации даты/времени по протоколу N□□ в меню «Настройки операционной системы» выбирается пункт «4 Настройка N□□». Далее - включается протокол N□□ (по умолчанию выключен) и задается I□-адрес N□□-сервера (или нескольких серверов), с которым будет осуществляться синхронизация даты/времени (Рисунок 9):

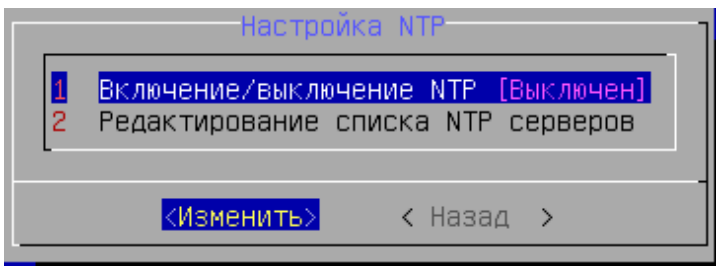

Рисунок 9

2.4.5 Редактирование списка SYSLOG серверов

Настройка отправки системных логов на SYSLOG сервера осуществляется в пункте «5 Редактирование списка SYSLOG меню «Настройки операционной системы» (Рисунок 10). В данном меню настраиваются следующие параметры: объект, сгенерировавший событие, уровень важности события, протокол, по которому осуществляется связь с SYSLOG сервером, IP-адрес или доменное имя SYSLOG сервера, TCP/UDP порт, по которому SYSLOG сервер принимает SYSLOG сообщения.

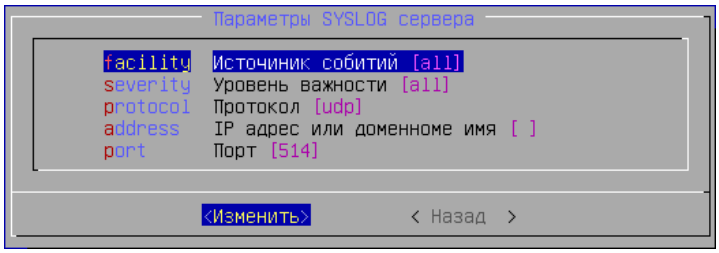

Рисунок 10

2.4.6 Настройка SSH

В пункте «6 Настройка SSH» меню «Настройки операционной системы» настраиваются параметры доступа к шлюзу по протоколу SSH для администрирования (Рисунок 11):

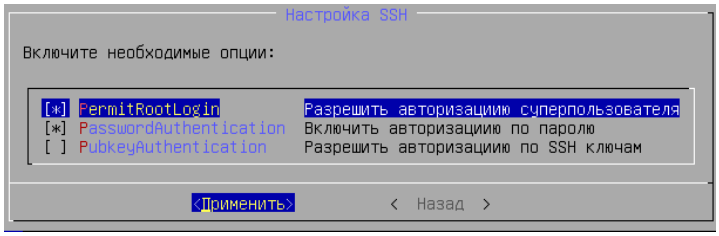

Рисунок 11

2.5 Работа с сертификатами

Пункт главного меню «Работа с сертификатами» позволяет просмотреть имеющиеся сертификаты, создать запрос на новый сертификат, осуществить импорт сертификатов в базу продукта, удалить сертификат из базы продукта, а также включить или отключить проверку списка отозванных сертификатов (Рисунок 12):

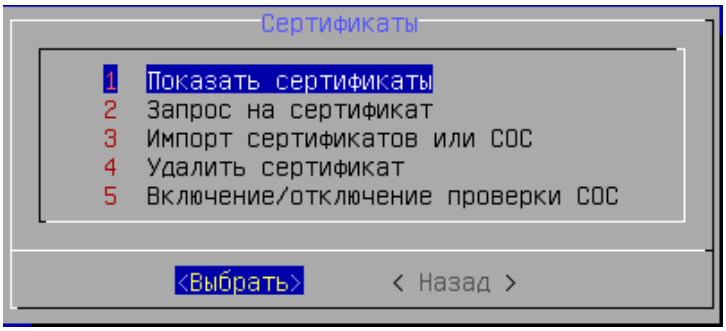

Рисунок 12

2.5.1 Просмотр сертификатов

Просмотр сертификатов, импортированных в базу шлюза, и их текущий статус осуществляется в пункте «1 Показать сертификаты» меню «Сертификаты» (Рисунок 13):

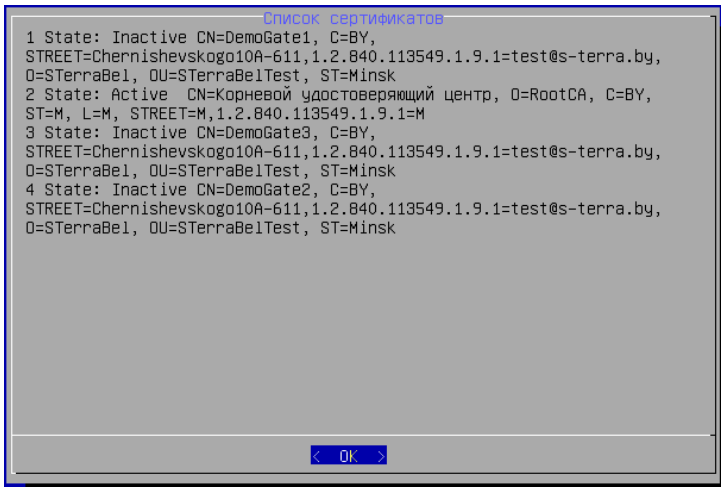

Рисунок 13

2.5.2 Создание запроса на сертификат

Формирование запроса на сертификат производится в пункт «2 Запрос на сертификат» меню «Сертификаты». Далее вводятся необходимые параметры сертификата (Рисунок 14).

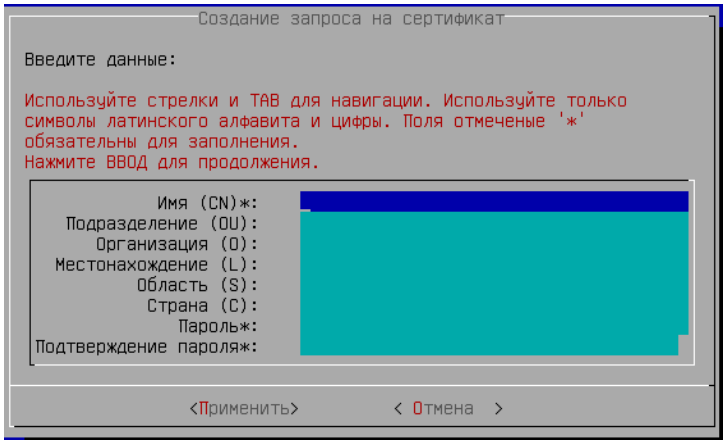

Рисунок 14

Сформированный запрос сохраняется в виде файла `*.req` в директории `/opt/certs/` на файловой системе шлюза (Рисунок 15).

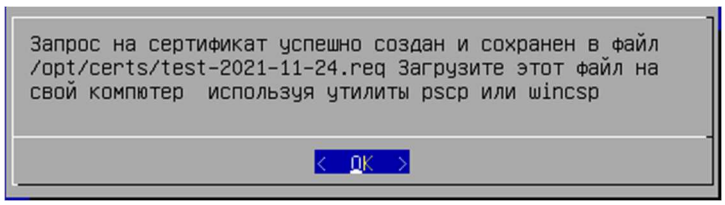

Рисунок 15

2.5.3 Импорт сертификатов или СОС

Импорт сертификатов или списка отозванных сертификатов в базу шлюза производится в меню «Сертификаты» в пункте «3 Импорт сертификатов или СОС». Данное меню позволяет произвести импорт доверенного сертификата удостоверяющего центра, личного сертификата и списка отозванных сертификатов (Рисунок 16):

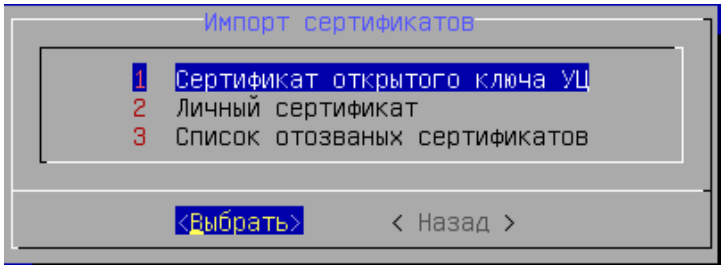

Рисунок 16

2.5.3.1 Импорт сертификата открытого ключа УЦ

Рисунок 17

В нижней строке прописывается путь к файлу сертификата. В левой панели осуществляется выбор каталога, в правой — выбор файла в соответствующем каталоге (Рисунок 17).

Далее (если сертификаты скопированы на шлюз в виде *.p7b файла) осуществляется выбор необходимого сертификата, содержащегося в *.p7b файле (Рисунок 18):

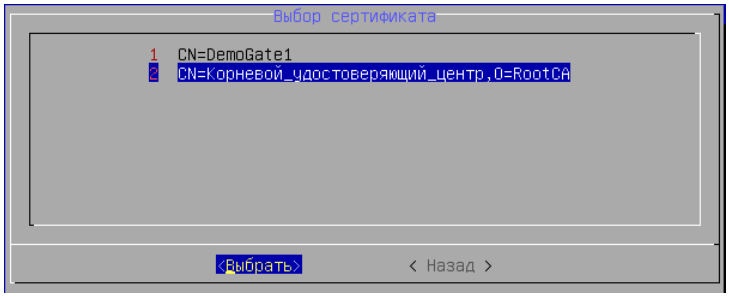

Рисунок 18

2.5.3.2 Импорт личного сертификата

Процесс импорта личного сертификата осуществляется аналогично импорту сертификата открытого ключа УЦ (п. 2.5.3.1).

2.5.3.3 Импорт списка отозванных сертификатов

Процесс импорта списка отозванных сертификатов осуществляется аналогично импорту сертификата открытого ключа УЦ (п. 2.5.3.1).

2.5.4 Удаление сертификатов

Удаление сертификата из базы шлюза осуществляется в меню «Сертификаты» в пункте «4 Удалить сертификат» путем выбора соответствующего сертификата из предлагаемого списка (Рисунок 19):

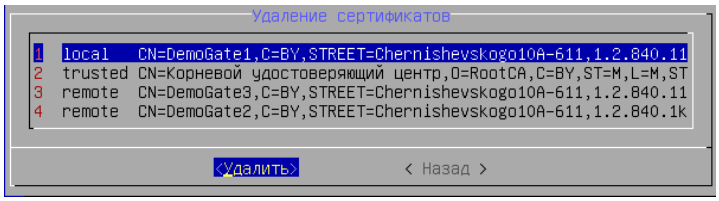

Рисунок 19

2.5.5 Включение/отключение проверки COC

Настройка проверки списка отозванных сертификатов осуществляется в меню «Сертификаты» в пункте «5 Включение/отключение проверки COC» (Рисунок 20):

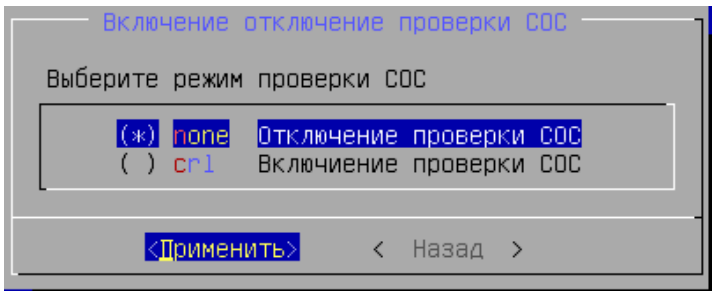

Рисунок 20

2.6 Настройка параметров ISAKMP

В пункте главного меню «Настройка параметров ISAKMP» производится настройка фрагментации ISAKMP-пакетов, типа идентификатора шлюза, предопределенных ключей и набора политик ISAKMP (Рисунок 21):

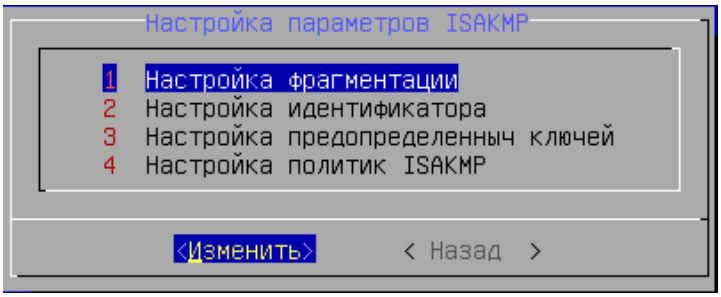

Рисунок 21

2.6.1 Настройка фрагментации

В меню «Настройка параметров ISAKMP» в пункте «1 Настройка фрагментации» производится включение либо выключение фрагментации пакетов ISAKMP (Рисунок 22):

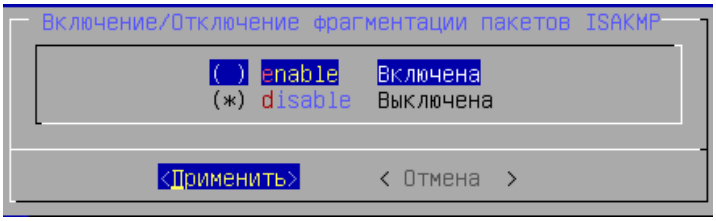

Рисунок 22

2.6.2 Настройка идентификатора

В меню «Настройка параметров ISAKMP» в пункте «2 Настройка идентификатора» осуществляется выбор типа идентификатора (Рисунок 23). В качестве идентификатора может использоваться IP-адрес, поле сертификата или имя шлюза.

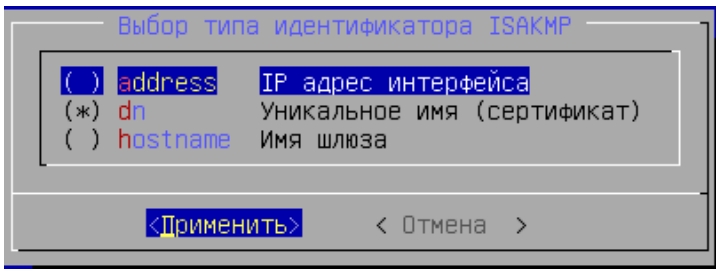

Рисунок 23

2.6.3 Настройка предопределённых ключей

В меню «Настройка параметров ISAKMP» в пункте «3 Настройка предопределённых ключей» производится настройка параметров предопределенных ключей (тип используемого идентификатора, значение идентификатора – IP-адрес или имя хоста и сам предопределенный ключ) (Рисунок 24):

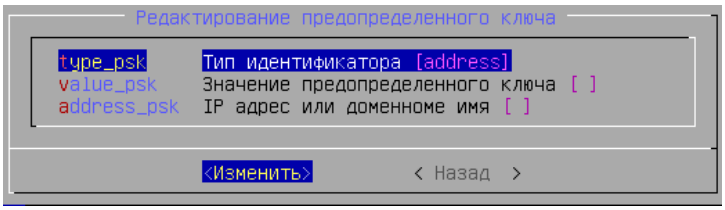

Рисунок 24

2.6.4 Настройка политик ISAKMP

В меню «Настройка параметров ISAKMP» в пункте «4 Настройка политик ISAKMP» производится настройка набора параметров для установления ISAKMP-сессии (метод аутентификации, алгоритм шифрования, алгоритм выработки общего ключа, способ проверки целостности и время жизни ISAKMP сессии) (Рисунок 25, Рисунок 26):

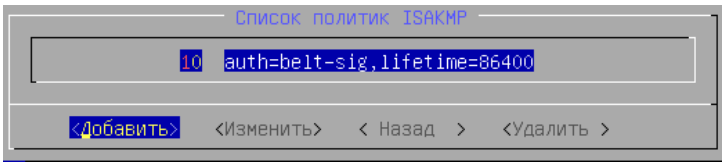

Рисунок 25

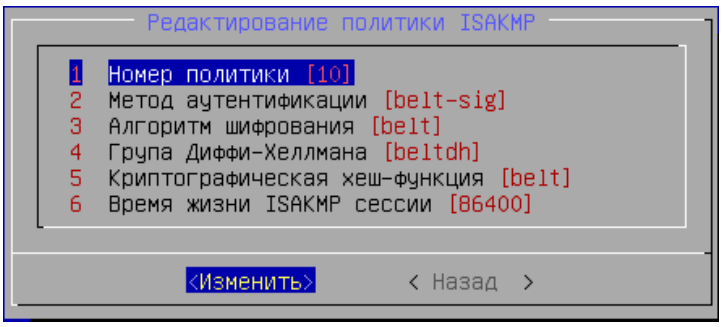

Рисунок 26

Также имеется возможность добавлять новые политики ISAKMP, либо удалять имеющиеся.

2.7 Настройка диапазонов IP-адресов клиентов

В пункте главного меню «Настройка диапазонов IP-адресов клиентов» задается пул адресов, из которого будут выдаваться IP-адреса клиентам, устанавливающим соединение со шлюзом по динамической криптокарте (Рисунок 27, Рисунок 28). Также имеется возможность редактирования имеющихся диапазонов, добавления новых диапазонов, либо удаление ранее созданных.

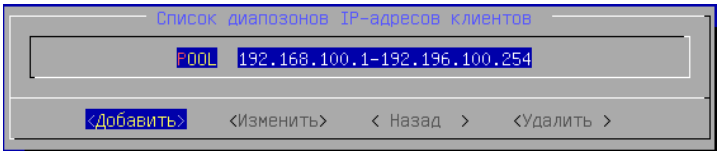

Рисунок 27

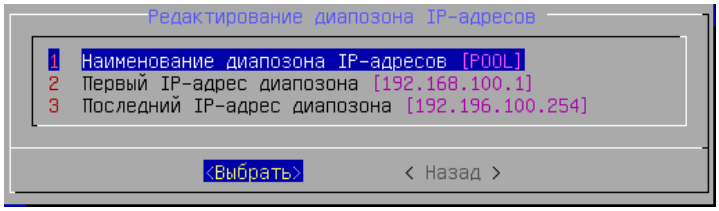

Рисунок 28

2.8 Настройка списков контроля доступа

Пункт главного меню «Настройка списков контроля доступа» позволяет создавать, редактировать и удалять именованные расширенные списки контроля доступа, используемые в том числе и для определения «интересного» трафика в процессе шифрования (Рисунок 29):

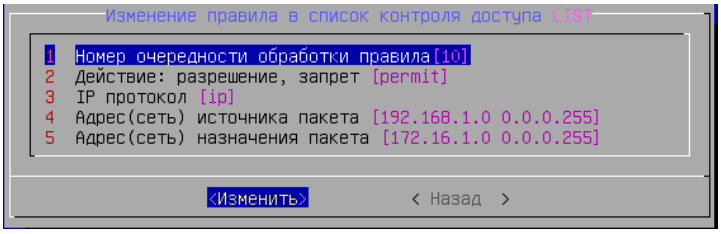

Рисунок 29

2.9 Настройка IPSec

В пункте главного меню «Настройка IPSec» настраиваются параметры IPSec-соединения: набор криптопреобразований для шифрования, интервалы перестроения туннелей, настройка обработки бита фрагментации (Рисунок 30):

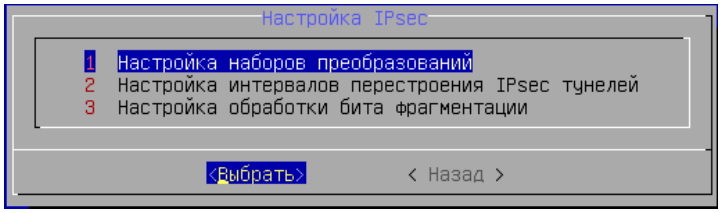

Рисунок 30

2.9.1 Настройка наборов преобразований

В меню «Настройка IPsec» в пункте «1 Настройка наборов преобразований» производится настройка параметров IPSec-соединения (протокол шифрования трафика, протокол аутентификации, режим инкапсуляции) (Рисунок 31):

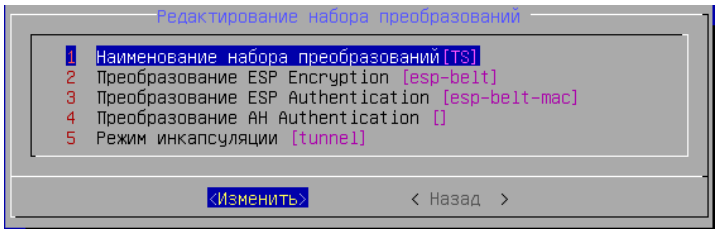

Рисунок 31

2.9.2 Настройка интервалов перестроения IPSec туннелей

В меню «Настройка IPsec» в пункте «2 Настройка интервалов перестроения IPSec туннелей» настраиваются параметры перестроения IPSec-соединений (Рисунок 32). Имеется возможность задания интервала перестроения в секундах или в килобайтах:

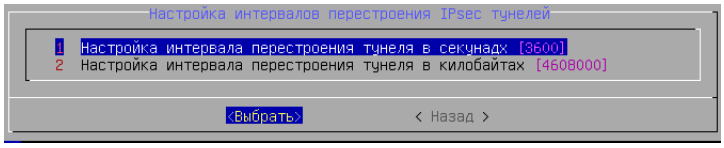

Рисунок 32

2.9.3 Настройка обработки бита фрагментации

Параметры работы с битом фрагментации в инкапсулированных пакетах устанавливаются в меню «Настройка IPsec» в пункте «3 Настройка обработки бита фрагментации» (Рисунок 33). Имеется возможность принудительной установки бита фрагментации, очистки, либо копирования значения бита фрагментации из исходного пакета:

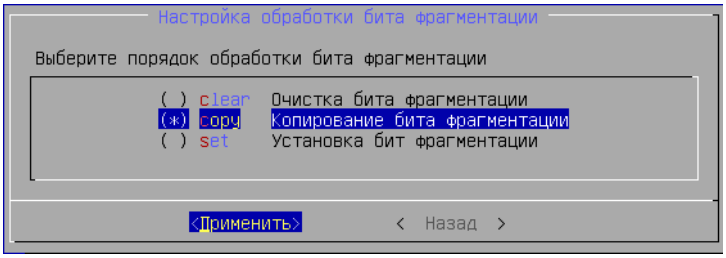

Рисунок 33

2.10 Настройка идентификаторов сертификатов партнеров

В пункте главного меню «Настройка идентификаторов сертификатов партнеров» задаются поля сертификатов, используемые для идентификации партнеров (Рисунок 34):

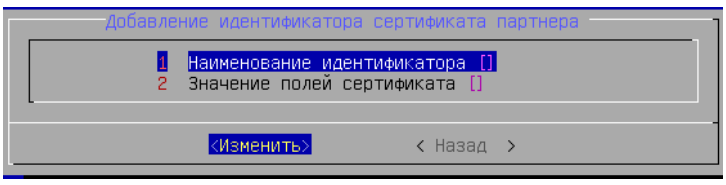

Рисунок 34

2.11 Настройка криптокарт

Настройка статических и динамических криптокарт осуществляется в пункте главного меню «Настройка криптокарт» (Рисунок 35):

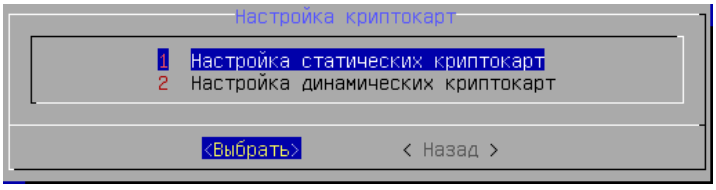

Рисунок 35

2.11.1 Настройка статических криптокарт

При настройке статической криптокарты задаются следующие параметры:

IP-адрес партнера.

- Диапазон IP-адресов, выдаваемых клиентам;
- «Интересный трафик», подлежащий шифрованию;
- Набор криптопреобразований для данного трафика;
- Группа Диффи-Хеллмана, для выработки общего ключа;
- Адреса DNS, передаваемые клиенту, Идентификатор партнера для фильтрации, а также включение/отключение обратного маршрута.

В этом же пункте меню осуществляется привязка динамической криптокарты к статической (Рисунок 36, Рисунок 37):

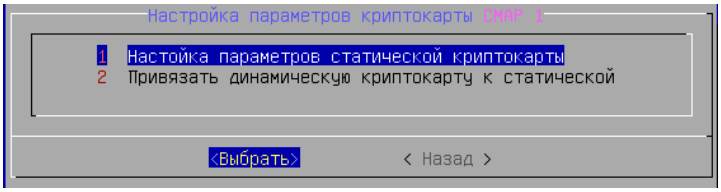

Рисунок 36

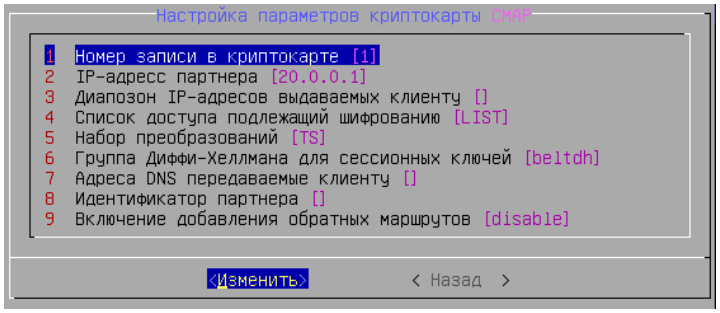

Рисунок 37

2.11.2 Настройка динамических криптокарт

Аналогично производится настройка динамической криптокарты (Рисунок 38):

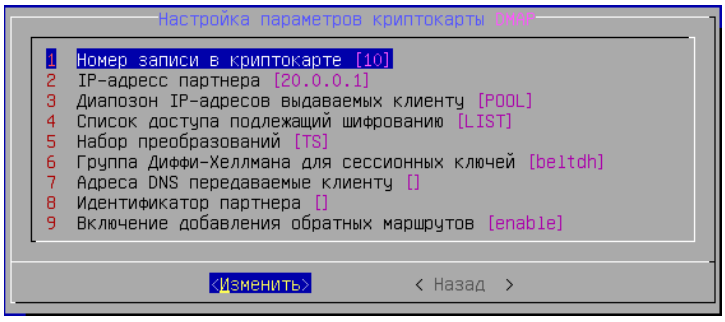

Рисунок 38

2.12 Настройка сетевых интерфейсов и маршрутизации

Пункт главного меню «Настройка сетевых интерфейсов и маршрутизации» позволяет задать IP-адреса интерфейсов, привязать к ним криптокарты и настроить статические маршруты (Рисунок 39):

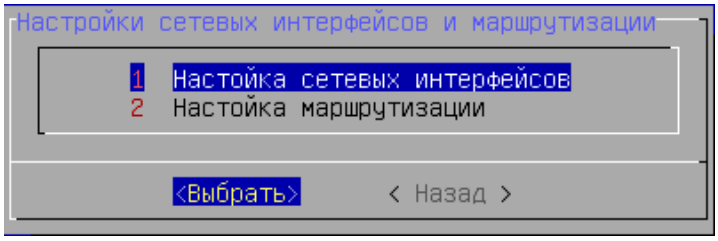

Рисунок 39

2.12.1 Настройка сетевых интерфейсов

В меню «Настройка сетевых интерфейсов и маршрутизации» в пункте «1 Настройка сетевых интерфейсов» задаются IP-адреса интерфейсов, устанавливается значение MTU, а также привязываются криптокарты к интерфейсам (Рисунок 40, Рисунок 41):

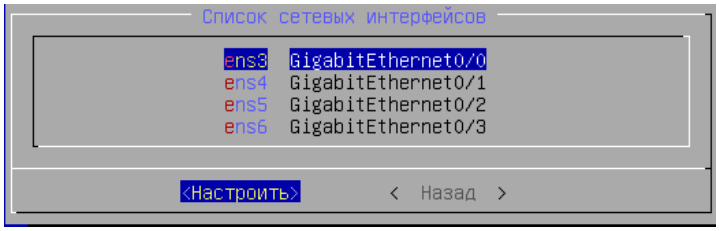

Рисунок 40

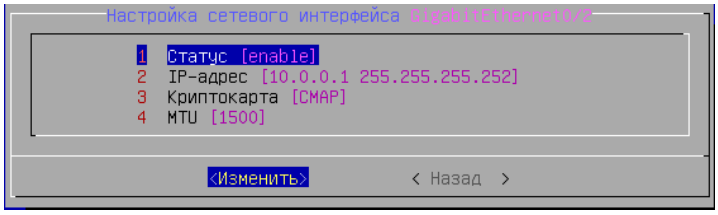

Рисунок 41

2.12.2 Настройка маршрутизации

В меню «Настройка сетевых интерфейсов и маршрутизации» в пункте «2 Настройка маршрутизации» осуществляется добавление, редактирование и удаление статических маршрутов (Рисунок 42, Рисунок 43):

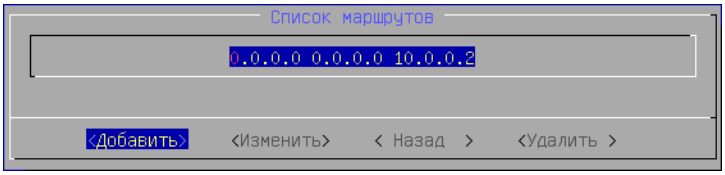

Рисунок 42

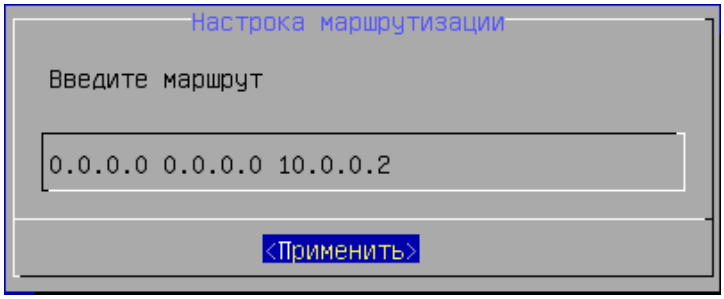

Рисунок 43

Все настройки, произведенные в конфигураторе, сохраняются в cisco-like консоли и доступны для редактирования с ее помощью.

Приложение

Структура меню конфигуратора:

– Просмотр текущей конфигурации
– Настройки операционной системы
– – Настройка имени шлюза
– – Настройка даты и времени
– – Настройка временной зоны
– – Настройка NTP
– – – Включение / выключение NTP
– – – Редактирование списка NTP серверов
– – Редактирование списка SYSLOG серверов
– – Настройка SSH
– Работа с сертификатами
– – Показать сертификаты
– – Запрос на сертификат
– – Импорт сертификатов или СОС
– – – Сертификат открытого ключа УЦ
– – – Личный сертификат
– – – Список отозванных сертификатов
– – Удалить сертификат
– – Включение / отключение проверки СОС
– Настройка параметров ISAKMP
– – Настройка фрагментации
– – Настройка идентификатора
– – Настройка предопределенных ключей
– – Настройка политик ISAKMP
– – – Номер политики
– – – Метод аутентификации
– – – Алгоритм шифрования
– – – Группа Диффи-Хеллмана
– – – Криптографическая хеш-функция
– – – Время жизни ISAKMP сессии
– Настройка диапазона IP-адресов клиентов
– – Наименование диапазона IP-адресов
– – Первый IP-адрес диапазона
– – Последний IP-адрес диапазона
– Настройка списков контроля доступа
– – Номер очередности обработки правила
– – Действие: разрешение, запрет
– –IP протокол
– – Адрес (сеть) источника пакета
– – Адрес (сеть) назначения пакета
– Настройка IPsec
– –Настройка наборов преобразований
– – – Наименование набора преобразований
– – – Преобразование ESP Encryption
– – – Преобразование ESP Authentication
– – – Преобразование AH Authentication
– – – Режим инкапсуляции
– – Настройка интервалов перестроения IPsec туннелей
– – – Настройка интервала перестроения туннеля в секундах
– – – Настройка интервала перестроения туннеля в килобайтах
– – Настройка обработки бита фрагментации
– Настройка идентификаторов сертификатов партнеров
– – Наименование идентификатора
– – Значение полей сертификата
– Настройка криптокарт
– – Настройка статических криптокарт
– – – Настройка параметров статической криптокарты
– – – – Номер записи в криптокарте
– – – – IP-адрес партнера
– – – – Диапазон IP-адресов, выдаваемых клиенту
– – – – Список доступа, подлежащий шифрованию
– – – – Набор преобразований
– – – – Группа Диффи-Хеллмана для сессионных ключей
– – – – Адреса DNS передаваемые клиенту
– – – – Идентификатор партнера
– – – – Включение добавления обратных маршрутов
– – – Привязать динамическую криптокарту к статической
– – – – Номер записи в криптокарте
– – – – Динамическая криптокарта
– – Настройка динамических криптокарт
– – – Номер записи в криптокарте
– – – IP-адрес партнера
– – – Диапазон IP-адресов, выдаваемых клиенту
– – – Список доступа, подлежащий шифрованию
– – – Набор преобразований
– – – Группа Диффи-Хеллмана для сессионных ключей
– – – Адреса DNS передаваемые клиенту
– – – Идентификатор партнера
– – – Включение добавления обратных маршрутов
– Настройка сетевых интерфейсов и маршрутизации
– – Настройка сетевых интерфейсов
– – – Статус
– – – IP-адрес
– – – Криптокарта
– – – MTU
– – Настройка маршрутизации