УТВЕРЖДЕНО
BY.PTHK.47001-01 34 02-ЛУ

Комплекс программно-аппаратный «Шлюз BelVPN 4.7»

РУКОВОДСТВО ОПЕРАТОРА CLI

BY.PTHK.47001-01 34 03

Листов 8

2025

Руководство оператора CLI

1. Назначение

Данный документ описывает функциональные возможности для существующей роли «Оператора CLI» в продукте «Комплекс программно-аппаратный Шлюз BelVPN 4.7». Помимо этого, ниже описаны рекомендации по эксплуатации и важные замечания с точки зрения безопасности, касающиеся соответствия продукта стандартам и нормативно-правовым актам Республики Беларусь.

2. Описание роли

Роль Оператора CLI необходима для выполнения общих сервисов СКЗИ, в том числе криптографические: генерация ключей, установление защищённого соединения, посредством интерпретатора команд в консоли (далее – cisco-like console).

Оператор CLI ограничен использованием команд, разрешенных внутри cisco-like console. Оператор CLI имеет максимальный уровень привилегий в рамках cisco-like console, может настраивать узел шифрования, локальные политики безопасности и имеет доступ ко всем командам в оболочке cisco-like console. Команды приведены в Приложении А.

В СКЗИ также выделена роль Оператора СКЗИ. Роли Оператора СКЗИ и Оператора CLI предлагается возложить на одно физическое лицо (на одного юридического представителя).

3. Аутентификация

Оператор CLI может авторизоваться только локально, как через отвечающий за это сервис (systemd-logind), так через cisco-like console из-под сеанса Оператора СКЗИ. Оператор СКЗИ вводит команду **cs_console**:

```
login: enable
password: Cisc_04321
```

Через сервис systemd-logind:

```
Логин: cscons
Пароль: Cisc_01234
```

После первого логина необходимо поменять стандартный пароль. На пароль введены следующие ограничения:

– минимальная длина составляет 10 символов;

– использовать минимум 1 цифру, 1 строчную букву, 1 прописную букву, 1 спецсимвол.

4. Функции

Функции доступные Оператору CLI, а также общий порядок работы с СКЗИ, изложено ниже:

1. настройка интерфейсов системы;
2. настройка плавил маршрутизации;
3. создание политики безопасности.

Приложение А

Настройка ipsec соединения

Для настройки соединения ipsec необходимо перейти в режим конфигурации оборудования командой:

```
conf t
```

Рекомендуем при первом запуске смените пароль по умолчанию:

```
username cscons password ПАРОЛЬ
```

Смените название шлюза:

```
hostname ИМЯ_ШЛЮЗА
```

Далее задайте тип идентификации удаленного пользователя:

```
crypto isakmp identity address / hostname / dn
```

со следующими параметрами:
`address` – устанавливает идентификатор адрес партнёра;
`hostname` – устанавливает идентификатор hostname партнера;
`dn` – устанавливает идентификатор в виде сертификата открытого ключа, созданного на белорусских алгоритмах).

Задайте параметры для ISAKMP командой:

```
crypto isakmp policy НОМЕР_ПОЛИТИКИ
```

Далее для данной политики задаются следующие параметры:
`hash belt`
указание хэш-алгоритма, используемого для контроля целостности сообщений в рамках ISAKMP SA на белорусских алгоритмах шифрования;
`encryption belt`
указание алгоритма шифрования сообщений белорусскими алгоритмами шифрования;
`authentication belt-sig`
аутентификация осуществляется с использованием цифровых сертификатов, созданных по алгоритму СТБ 34.101.45, pre-share аутентификация осуществляется с использованием предопределенных ключей;
Примечание: при создании предопределенного ключа необходимо чтобы он соответствовал требованиям безопасности и имел высокую энтропию. Поэтому рекомендуем использовать скрип для создания пароля, внедренный в систему.

```
group beltdh
```

указание группы Диффи-Хеллмана, используемого в рамках протокола IKE для выработки ключевого материала с белорусскими алгоритмами шифрования.

Создайте набор преобразований для IPsec:

crypto ipsec transform-set ***ИМЯ_НАБОРА_ПРЕОБРАЗОВАНИЙ*** *esp-belt esp-belt-mac*

со следующими параметрами:
mode tunnel
параметр, устанавливающий туннельный режим.

Опишите трафик, который планируется защищать. Для этого создайте расширенный список доступа:

ip access-list extended ***ИМЯ_АКСЕССЛИСТА***

Далее необходимо добавить правила в список доступа:

permit ip ***АДРЕСА_СЕТИ_ИСТОЧНИКА АДРЕСА_СЕТИ_НАЗНАЧЕНИЯ***

После всех настроек необходимо создать крипто-карту командой:

crypto map ***ИМЯ_КРИПТОКАРТЫ НОМЕР*** *ipsec-isakmp*

И задать в ней параметры, определенные ниже.
match address ***ИМЯ_АКСЕССЛИСТА***
осуществляет привязку списка доступа к записи криптографической карты;
set transform-set ***ИМЯ_НАБОРА_ПРЕОБРАЗОВАНИЙ***
указывает, какие наборы преобразований (transform set) могут использоваться с данной записью криптографической карты;
set pfs beltdh
указывает, что на стадии согласования параметров IPsec для данной записи криптографической карты должна быть затребована опция PFS, в которой будут использованы белорусские алгоритмы группы Диффи-Хеллмана;
set peer ***АДРЕС_ПАРТНЕРА***
указывает IPsec партнера для записи криптографической карты.

Настройка интерфейсов

Зайдите в настройки интерфейса:

```
interface GigabitEthernet НОМЕР_ИНТЕРФЕЙСА
```

Включите:

```
no shutdown
```

И добавьте на него адрес:

```
ip address 192.168.2.1 255.255.255.0
```

Для привязки крипто-карты к интерфейсу напишите команду:

```
crypto map ИМЯ_КРИПТОКАРТЫ
```

Для создания vrrp на интерфейсе необходимо выполнить следящий набор команд:

`vrrp authentication`

задает пароль для аутентификации пакетов протокола VRRP;

`vrrp ip`

настраивает IP-адрес виртуального маршрутизатора;

`vrrp ip route`

настраивает маршрутизацию виртуального роутера;

`vrrp preempt`

разрешает маршрутизатору переходить в состояние master, если его приоритет будет выше, чем у текущего master;

`vrrp priority`

устанавливает приоритет для маршрутизатора;

`vrrp sync-group`

синхронизирует состояние виртуальных маршрутизоторов в группе;

`vrrp timers advertise`

устанавливает интервал между отправкой VRRP-объявлений;

`vrrp timers garp`

устанавливает периодический интервал, с которым маршрутизатор, находящийся в состоянии master отправляет gratuitous ARP сообщения;

`vrrp state`

устанавливает начальное состояние виртуального маршрутизатора;

`vrrp track interface`

проверяет состояние интерфейса;

`vrrp track process`

включает отслеживание состояния процесса и меняет состояние VRRP-маршрутизатора в зависимости от статуса процессов.

Для настройки VLAN на нужном интерфейсе необходимо ввести:

interface GigabitEthernet ***НОМЕР_ИНТЕРФЕЙСА***

И далее команду:
encapsulation dot1Q
устанавливает VLAN ID на выбранном интерфейсе.

Если необходимо создать GRE интерфейс тогда пишем команду:

interface tunnel ***НОМЕР_ИНТЕРФЕЙСА***

И далее настраиваем необходимые параметры:
tunnel destination
устанавливает адрес назначения для туннельного интерфейса GRE;
tunnel source
устанавливает адрес источника для туннельного интерфейса GRE.

После всех настроек выйдите из режима конфигурации командой:
end
Примечание: Список всех команд с описанием можно посмотреть в «Руководство пользователя Cisco-like команды» расположенной на нашем сайте.

Лист регистрации изменений									
	Номера листов (страниц)				Всего листов (страниц) в докум.	№ документа	Входящий № сопроводительного докум. и дата	Подп.	Дата
Изм.	измененных	замененных	новых	аннулированных					