



# Руководство администратора

СЛЕТ.10101-01 90 02

Версия 1.0. Выпуск от марта 2025

## Настройка Termidesk Connect

## ОГЛАВЛЕНИЕ

1 .	ОБЩИЕ СВЕДЕНИЯ.....	8
1.1 .	О документе.....	8
1.2 .	Типографские соглашения .....	8
2 .	КОМПОНЕНТЫ TERMIDESK CONNECT И ИХ ВЗАИМОДЕЙСТВИЕ .....	9
2.1 .	Основные компоненты и порядок их взаимодействия .....	9
3 .	НАСТРОЙКИ СИСТЕМЫ .....	11
3.1 .	Лицензия .....	11
3.2 .	Отказоустойчивость.....	11
3.2.1 .	Общие сведения по отказоустойчивости Termidesk Connect.....	11
3.2.2 .	Настройка отказоустойчивой конфигурации для первого устройства.....	12
3.2.3 .	Настройка отказоустойчивой конфигурации для второго устройства.....	14
3.2.4 .	Пример выполнения команд для отказоустойчивой конфигурации.....	15
3.2.5 .	Проверка состояний устройств в отказоустойчивой конфигурации.....	15
3.3 .	Сеть .....	16
3.3.1 .	Общие сведения по настройке сети .....	16
3.3.2 .	Настройка VRF.....	17
3.3.3 .	Настройка VLAN .....	17
3.3.4 .	Настройка IP-адресов .....	18
3.3.5 .	Настройка маршрутизации.....	19
3.3.6 .	Настройка IP-фондов.....	19
3.4 .	Диагностика.....	20
3.5 .	Аудит .....	21
3.5.1 .	Журналы Termidesk Connect .....	21
3.6 .	Резервное копирование и обновление.....	21
3.6.1 .	Общие сведения по управлению образами и резервными копиями .....	21
3.6.2 .	Управление резервными копиями через инструмент va .....	22

3.6.3 .	Управление образами через инструмент va.....	23
4 .	УПРАВЛЕНИЕ ТРАФИКОМ .....	25
4.1 .	Проверки.....	25
4.1.1 .	Общие сведения о проверках.....	25
4.1.2 .	Создание и настройка ICMP-проверки .....	25
4.1.3 .	Создание и настройка TCP-проверки.....	26
4.2 .	Реальные Серверы .....	28
4.2.1 .	Общие сведения о Реальных Серверах.....	28
4.2.2 .	Создание и настройка группы Реальных Серверов .....	28
4.3 .	Серверы Балансировки.....	29
4.3.1 .	Общие сведения о Серверах Балансировки.....	29
4.3.2 .	Создание и настройка Сервера Балансировки для протокола TCP .....	29
4.3.3 .	Создание и настройка Сервера Балансировки для протокола RAPID-TCP.....	32
4.4 .	TLS .....	34
4.4.1 .	Общие сведения о TLS .....	34
4.4.2 .	Файлы для SSL/TLS.....	35
4.4.3 .	Профили SSL/TLS.....	35
4.4.4 .	Создание и настройка серверного SSL-профиля .....	35
4.4.5 .	Создание и настройка клиентского SSL-профиля .....	37
4.5 .	Сценарии.....	40
4.5.1 .	Общие сведения о сценариях.....	40
4.5.2 .	Добавление сценария.....	42
4.5.3 .	Примеры сценариев для выбора Сервера Балансировки .....	43
4.5.4 .	Примеры сценариев для изменения содержимого запросов.....	44
4.5.5 .	Примеры сценариев для ответа на запрос .....	45
4.6 .	Виртуальные Серверы .....	46
4.6.1 .	Общие сведения о Виртуальных Серверах.....	46
4.6.2 .	Создание и настройка Виртуального Сервера для балансировки по протоколу TCP .....	48

4.6.3 .	Создание и настройка Виртуального Сервера для балансировки по протоколу RAPID-TCP .....	50
4.6.4 .	Создание и настройка виртуального сервера для балансировки по протоколу HTTP .....	52
5 .	ГЕОБАЛАНСИРОВКА .....	55
5.1 .	ADNS.....	55
5.1.1 .	Общие сведения об ADNS.....	55
5.1.2 .	Создание и настройка ADNS .....	55
5.2 .	Геолокационные IP-базы .....	55
5.2.1 .	Общие сведения о геолокационных IP-базах .....	55
5.2.2 .	Добавление геолокационных IP-баз.....	55
5.3 .	DNS View .....	57
5.3.1 .	Общие сведения о DNS View .....	57
5.3.2 .	Создание и настройка DNS View.....	57
5.4 .	Сервисы.....	58
5.4.1 .	Общие сведения о Сервисах .....	58
5.4.2 .	Создание и настройка Сервиса .....	58
5.5 .	Геобалансировка. Виртуальные Серверы .....	59
5.5.1 .	Общие сведения о Виртуальных Серверах геобалансировки.....	59
5.5.2 .	Создание и настройка Виртуальных Серверов геобалансировки .....	59
5.6 .	Зоны.....	61
5.6.1 .	Общие сведения о Зонах .....	61
5.6.2 .	Создание и настройка Зоны .....	61
6 .	ИНТЕРФЕЙС РАСШИРЕННОГО МЕНЮ TERMIDESK CONNECT .....	64
6.1 .	Общие сведения по работе с интерфейсом расширенного меню.....	64
6.2 .	Смена пароля администратора .....	64
6.3 .	Перезагрузка.....	64
6.4 .	Выключение.....	65
6.5 .	Переход в интерфейс командной строки .....	65

7 .	ИНТЕРФЕЙС CLI TERMIDESK CONNECT .....	66
7.1 .	Общие сведения по работе с CLI.....	66
7.2 .	Команда bash.....	66
7.3 .	Команда clear .....	66
7.4 .	Команда commit.....	66
7.5 .	Команда debug .....	66
7.6 .	Команда delete .....	67
7.7 .	Команда discard .....	68
7.8 .	Команда load .....	68
7.9 .	Команда mode .....	68
7.10 .	Команда quit.....	68
7.11 .	Команда save.....	69
7.12 .	Команда set .....	69
7.12.1 .	Общие сведения по команде set.....	69
7.12.2 .	Объект geolb .....	70
7.12.3 .	Объект ha .....	71
7.12.4 .	Объект health-check.....	72
7.12.5 .	Объект interfaces.....	72
7.12.6 .	Объект ip.....	73
7.12.7 .	Объект ipset.....	73
7.12.8 .	Объект lbs.....	74
7.12.9 .	Объект nasm.....	75
7.12.10 .	Объект restconf .....	76
7.12.11 .	Объект ssl-profile .....	77
7.12.12 .	Объект rs-pool.....	81
7.12.13 .	Объект system .....	81
7.12.14 .	Объект user.....	82
7.12.15 .	Объект vlan .....	82

7.12.16 . Объект vrf.....	82
7.12.17 . Объект vs.....	82
7.13 . Команда show .....	84
7.14 . Команда top.....	84
7.15 . Команда up.....	84
7.16 . Команда validate .....	84
7.17 . Команда write.....	85
8 . ВЕБ-ИНТЕРФЕЙС TERMIDESK CONNECT .....	86
8.1 . Доступ к веб-интерфейсу Termidesk Connect.....	86
8.2 . Обзор доступных функций веб-интерфейса.....	86
8.3 . Работа с панелью управления и мониторинга.....	88
8.4 . Функция «Система».....	88
8.4.1 . Лицензионное соглашение .....	88
8.4.2 . Параметры сети.....	88
8.4.2.1 . Сеть. Общие сведения .....	88
8.4.2.2 . Добавление VRF.....	89
8.4.2.3 . Просмотр списка сетевых интерфейсов .....	89
8.4.2.4 . Добавление VLAN .....	89
8.4.2.5 . Добавление IP-адресации.....	90
8.4.2.6 . Добавление параметров маршрутизации.....	91
8.4.2.7 . Добавление IP-фондов.....	91
8.4.3 . Обновление.....	92
8.5 . Функция «Управление трафиком».....	92
8.5.1 . Добавление проверки .....	92
8.5.2 . Добавление Реального Сервера .....	93
8.5.3 . Добавление Сервера Балансировки.....	94
8.5.4 . Параметры TLS .....	96
8.5.5 . Просмотр и добавление сертификата через веб-интерфейс Termidesk Connect .....	96

8.5.6 .	Профили.....	96
8.5.7 .	Добавление файлов сценария .....	99
8.5.8 .	Добавление Виртуального Сервера.....	99
8.6 .	Функция «ГеоБН» .....	101
8.6.1 .	Добавление ADNS.....	101
8.6.2 .	Добавление Площадок.....	101
8.6.3 .	Добавление DNS View .....	101
8.6.4 .	Добавление Сервисов .....	102
8.6.5 .	Добавление Виртуальных Серверов геобалансировки .....	103
8.6.6 .	Добавление Зоны .....	104
9 .	ПЕРЕЧЕНЬ ТЕРМИНОВ .....	107
10 .	ПЕРЕЧЕНЬ СОКРАЩЕНИЙ .....	109

## 1 . ОБЩИЕ СВЕДЕНИЯ

### 1.1 . О документе

Настоящий документ является второй частью руководства администратора на программу для электронной вычислительной машины «Балансировщик нагрузки Термидеск Коннект» (далее – Termidesk Connect). Документ предназначен для администраторов системы и сети.

Во второй части руководства приведена настройка Termidesk Connect, рассмотрено взаимодействие компонентов. Для того чтобы получить информацию об установке Termidesk Connect, необходимо обратиться к первой части руководства администратора – СЛЕТ.10101-01 90 01 «Руководство администратора. Установка Termidesk Connect».

### 1.2 . Типографские соглашения

В настоящем документе приняты следующие типографские соглашения:

- моноширинный шрифт – используется для выделения фрагментов текста программ, наименований файлов и папок (директорий), наименований пакетов, путей перемещения, строк комментариев, различных программных элементов (объект, класс, тип, переменная, команда, макрос и т. д.), а также вводимого и выводимого текста в режиме командной строки;
- «кавычки» – текст, заключенный в кавычки, используется для обозначения наименований документов, названий компонентов Termidesk, пунктов меню, наименований окон, вкладок, полей, других элементов графического интерфейса, а также вводимого и выводимого текста в режиме графического интерфейса;
- **[квадратные скобки]** – текст, заключенный в квадратные скобки, используется для наименования экранных кнопок;
- **<угловые скобки>** – текст, заключенный в угловые скобки, используется для наименования клавиш клавиатуры.



## 2. КОМПОНЕНТЫ TERMIDESK CONNECT И ИХ ВЗАИМОДЕЙСТВИЕ

### 2.1. Основные компоненты и порядок их взаимодействия

Termidesk Connect состоит из группы объектов (компонентов):

- Виртуальный Сервер – представляет собой абстракцию, терминирующую на себя трафик от пользователя. Для Виртуального Сервера задаются IP-адрес, порт, тип (TCP, HTTP), правила перенаправления трафика на Сервера Балансировки, правила модификации трафика и другие параметры. Помимо указанных параметров к Виртуальному Серверу привязываются:
  - SSL-профиль, представляющий собой набор настроек протокола SSL (сертификат, ключ, используемые алгоритмы);
  - TCP-профиль, представляющий собой набор настроек протокола TCP;
- Сервер Балансировки – представляет собой абстракцию, которая не имеет собственного IP-адреса и порта. Для Сервера Балансировки задаются тип, алгоритм балансировки, действия при недоступности Реальных Серверов, правила модификации трафика, а также привязываются одна или несколько групп Реальных Серверов;
- группа Реальных Серверов – объединение нескольких реальных серверов и их периодических проверок. Реальный Сервер - это узел с установленным приложением, доставку которого обеспечивает Termidesk Connect. Для включения Реального Сервера в список доставки Termidesk Connect задаются его IP-адрес, порт.

Помимо перечисленных компонентов в состав включаются следующие, если Termidesk Connect используется для геораспределенной балансировки:

- Виртуальный Сервер геобалансировки – представляет собой абстракцию, терминирующую на себя трафик. Для него задаются алгоритм балансировки, время жизни (TTL) и другие параметры;
- Сервис – это объект (абстракция) с назначенным IP-адресом, доступ к которому нужно предоставить пользователю в рамках геобалансировки. Для Сервиса задается локальный IP-адрес, отправляющийся в DNS-ответе, если пользователь подключается из внутренней сети организации, и общедоступный IP-адрес для остальных случаев.

Процесс подключения пользователя выглядит следующим образом (см. Рисунок 1):

- запрос от пользователя приходит на Виртуальный Сервер;
- Виртуальный Сервер на основе заданных настроек определяет, как будет обработан поступивший запрос;
- далее на основании правил балансировки уровней L4 или L7 запрос передается на Сервер Балансировки;

- Сервер Балансировки на основе заданных настроек балансировки обрабатывает запрос, выполняет проверку группы Реальных Серверов и направляет подключение на один из Реальных Серверов для доступа к приложению.

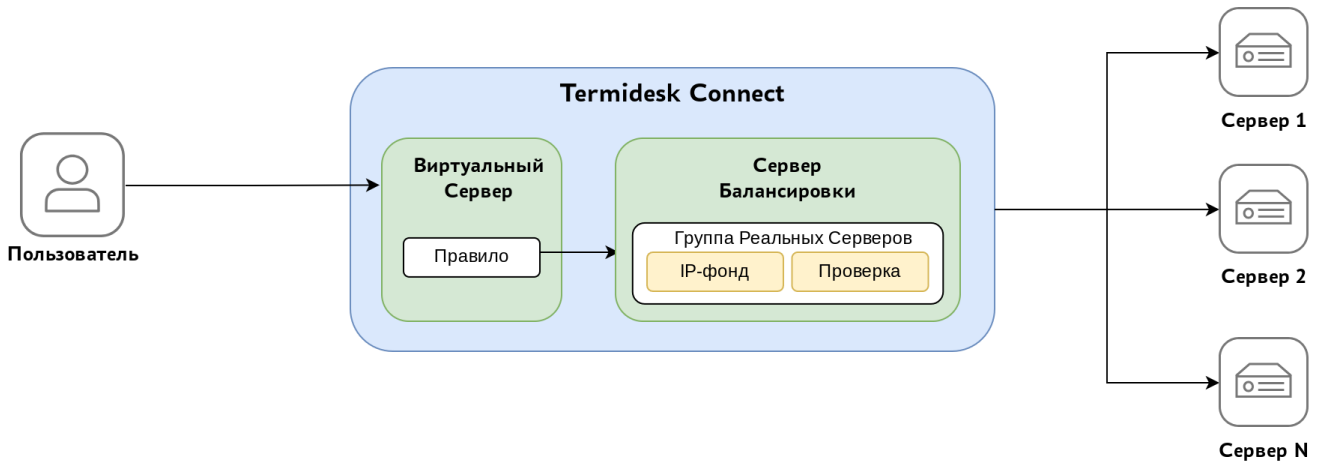


Рисунок 1 – Общий принцип взаимодействия

## 3. НАСТРОЙКИ СИСТЕМЫ

### 3.1 . Лицензия

Принятие лицензионного соглашения осуществляется при загрузке и первоначальной настройке Termidesk Connect (см. подраздел **Порядок загрузки Termidesk Connect на платформу виртуализации** документа СЛЕТ.10101-01 Руководство администратора. Установка Termidesk Connect).

### 3.2 . Отказоустойчивость

#### 3.2.1 . Общие сведения по отказоустойчивости Termidesk Connect

Для обеспечения постоянства доступа пользователя к приложениям, размещенным в инфраструктуре организации, Termidesk Connect может быть настроен в отказоустойчивой (высокодоступной) конфигурации.

**И** Для настройки отказоустойчивой (высокодоступной) конфигурации необходимо использовать два узла Termidesk Connect.

Termidesk Connect в отказоустойчивой конфигурации обеспечивает:

- синхронизацию конфигураций между двумя и более устройствами Termidesk Connect. При этом синхронизируется не вся конфигурация: часть параметров являются индивидуальной для каждого устройства;
- резервирование IP-адресов виртуальных серверов;
- переключение трафика между устройствами Termidesk Connect при выходе какого-либо из них из строя.

Для обеспечения отказоустойчивости устройства Termidesk Connect объединяются в одноранговый кластер, и имеют одинаковые права и возможности. Однако для упрощения настройки принято, что существуют следующие узлы:

- мастер-узел («Active») – устройство обрабатывает трафик пользователей в настоящий момент;
- резервный узел («Standby») – устройство в настоящий момент не обрабатывает трафик пользователей.

Параметры, синхронизирующиеся между устройствами Termidesk Connect:


- файлы сертификатов;
- Lua-файлы;
- сохраненная конфигурация.

Параметры конфигурации, не синхронизирующиеся и настраиваемые на каждом устройстве Termidesk Connect отдельно:

- IP-адреса с типом «ha-type LOCAL»;
- имя устройства (hostname);
- VLAN с типом «ha-type LOCAL»;
- VRF с типом «ha-type LOCAL»;
- маршруты, находящиеся в VRF с типом «ha-type LOCAL».

Общий алгоритм настройки отказоустойчивой (высокодоступной) конфигурации:

- убедиться, что устройства Termidesk Connect имеют сетевую доступность между собой;
- убедиться, что доступны следующие порты для взаимодействия:
  - TCP 222;
  - TCP/UDP 322. Этот порт может быть изменен на другой;
- настроить первое устройство Termidesk Connect:
  - указать локальный IP-адрес, используемый для взаимодействия. Выбранный IP-адрес должен соответствовать типу «ha-type LOCAL»;
  - указать UDP-порт, используемый для взаимодействия;
  - указать интервал периодических запросов. Такой же интервал должен быть задан при настройке второго (резервного) устройства Termidesk Connect;
  - указать приоритет устройства. Для мастер-узла указывается 0 («Active»), для резервного узла указывается 1 («Standby»);
  - указать параметры подключения ко второму устройству;
- настроить зеркально второе устройство Termidesk Connect:
  - указать локальный IP-адрес, используемый для взаимодействия. Выбранный IP-адрес должен соответствовать типу «ha-type LOCAL»;
  - указать UDP-порт, используемый для взаимодействия;
  - указать интервал периодических запросов, который был задан на первом устройстве Termidesk Connect;
  - указать приоритет устройства. Если для первого устройства ранее был задан 0 («Active»), то для второго устройства задать приоритет 1 («Standby»);

 Приоритеты обязательно должны различаться в настройках устройств!

- указать параметры подключения к первому устройству.

### 3.2.2 . Настройка отказоустойчивой конфигурации для первого устройства

Настройка отказоустойчивой конфигурации выполняется из интерфейса командной строки Termidesk Connect.

Для настройки первого устройства (мастер-узла) Termidesk Connect используются команды:

- задание приоритета первого устройства (мастер-узла):

```
set ha priority 0
```

- указание локального IP-адреса, используемого для взаимодействия:

**⚠ Выбранный IP-адрес должен соответствовать типу «ha-type LOCAL».**

```
set ha ip <IP-адрес>
```

- задание UDP-порта, используемого для взаимодействия (по умолчанию – 322):

```
set ha port <порт>
```

- задание интервала (в миллисекундах) периодических запросов (по умолчанию – 1000):

**⚠ Интервал должен быть одинаковым на всех устройствах.**

```
set ha interval <значение>
```

- задание имени второго устройства Termidesk Connect, с которым будет осуществляться взаимодействие (имя может быть любым):

```
set ha remote <имя второго устройства>
```

- задание приоритета второго устройства Termidesk Connect:

```
set ha remote <имя второго устройства> priority 1
```

- задание IP-адреса второго устройства Termidesk Connect:

```
set ha remote <имя второго устройства> ip <IP-адрес>
```

- задание UDP-порта второго устройства Termidesk Connect:

```
set ha remote <имя второго устройства> port <порт>
```

- задание пароля пользователя второго устройства Termidesk Connect:

```
set ha remote <имя второго устройства> seckey <порт>
```

- применение заданных настроек:

```
commit
```

- сохранение настроек:

```
write
```

### 3.2.3 . Настройка отказоустойчивой конфигурации для второго устройства

Настройка отказоустойчивой конфигурации выполняется из интерфейса командной строки Termidesk Connect.

Для настройки второго устройства (резервного узла) Termidesk Connect используются команды:

- задание приоритета второго устройства (резервного узла):

```
set ha priority 1
```

- указание локального IP-адреса, используемого для взаимодействия:

**⚠** Выбранный IP-адрес должен соответствовать типу «ha-type LOCAL».

```
set ha ip <IP-адрес>
```

- задание UDP-порта, используемого для взаимодействия (по умолчанию – 322):

```
set ha port <порт>
```

- задание интервала (в миллисекундах) периодических запросов (по умолчанию – 1000):

**⚠** Интервал должен быть одинаковым на всех устройствах.

```
set ha interval <значение>
```

- задание имени первого устройства Termidesk Connect, с которым будет осуществляться взаимодействие (имя может быть любым):

```
set ha remote <имя первого устройства>
```

- задание приоритета первого устройства Termidesk Connect:

```
set ha remote <имя второго устройства> priority 0
```

- задание IP-адреса первого устройства Termidesk Connect:

```
set ha remote <имя первого устройства> ip <IP-адрес>
```

- задание UDP-порта первого устройства Termidesk Connect:

```
set ha remote <имя первого устройства> port <порт>
```

- задание пароля пользователя первого устройства Termidesk Connect:

```
set ha remote <имя первого устройства> seckey <порт>
```

- применение заданных настроек:

```
commit
```

- сохранение настроек:

```
write
```

### 3.2.4 . Пример выполнения команд для отказоустойчивой конфигурации

В таблице (см. Таблица 1) приведен пример команд для первого и второго устройства Termidesk Connect.

Таблица 1 – Пример команд для отказоустойчивой конфигурации

Первое устройство NodeTDC15-1	Второе устройство NodeTDC15-2
set ha	set ha
set ha priority 0	set ha priority 1
set ha ip 192.0.2.10	set ha ip 192.0.2.11
set ha port 322	set ha port 322
set ha interval 1000	set ha interval 1000
set ha remote NodeTDC15-2	set ha remote NodeTDC15-1
set ha remote NodeTDC15-2 priority 1	set ha remote NodeTDC15-1 priority 0
set ha remote NodeTDC15-2 ip 192.0.2.11	set ha remote NodeTDC15-1 ip 192.0.2.10
set ha remote NodeTDC15-2 port 322	set ha remote NodeTDC15-1 port 322
set ha remote NodeTDC15-2 seckey P@ss	set ha remote NodeTDC15-1 seckey P@ss

### 3.2.5 . Проверка состояний устройств в отказоустойчивой конфигурации

Проверка состояний устройств в отказоустойчивой конфигурации выполняется из интерфейса командной строки Termidesk Connect.

Для проверки состояния используется команда:

```
show status ha
```

Вывод команды отобразит:

- роль устройства, на котором выполнена команда:
  - STANDBY – устройство, не обрабатывающее в настоящий момент трафик пользователей;
  - ACTIVE – устройство, обрабатывающее в настоящий момент трафик пользователей;
- состояние устройства, на котором выполнена команда:
  - OPERATING – отказоустойчивая конфигурация работает корректно;

- Hello-exchange – настройка отказоустойчивой конфигурации на устройствах не соответствует друг другу, либо у устройств отсутствует сетевое взаимодействие;
- состояние соседнего устройства, с которым настроена отказоустойчивая конфигурация:
  - имя устройства;
  - приоритет;
  - IP-адрес;
  - порт;
  - доступность;
  - роль устройства;
  - дата и время последней синхронизации.

Пример вывода команды:

```
1 #####
2 # Отказоустойчивость #
3 #####
4     Роль: STANDBY
5     Состояние: OPERATING
6     =====
7 (1)         Узел: NodeTDC15-1
8             Приоритет: 0
9             IP-адрес: 192.0.2.1
10            Порт: 322
11            Доступность: доступен
12            Роль: ACTIVE
13            Время сверки hello: 2025-03-15 12:32:57.434339
```

### 3.3 . Сеть

#### 3.3.1 . Общие сведения по настройке сети

Для интеграции Termidesk Connect в существующую сеть организации нужно выполнить настройку:

- VRF (опционально);
- VLAN;
- IP-адресов;
- маршрутизации;
- IP-фондов (опционально).

IP-фонд – это группа IP-адресов, которые может использовать Termidesk Connect для взаимодействия с Реальными Серверами. Настройка IP-фонда необходима для:

- определения перечня IP-адресов, с которых Termidesk Connect будет подключаться к Реальным Серверам;



- снятия существующих сетевых ограничений по количеству открытых TCP-сессий со стороны Termidesk Connect к Реальным Серверам.

❗ Добавление IP-фондов в общем случае помогает решить ситуацию, когда количество TCP-сессий, открываемых между Termidesk Connect (работающим в режиме Full Proxy) и Реальными Серверами, ограничивается максимально возможным их количеством (65 536) для одного IP-адреса.

### 3.3.2 . Настройка VRF

Настройка VRF является необязательной и выполняется одним из способов:

- из интерфейса командной строки Termidesk Connect;
- из веб-интерфейса Termidesk Connect (см. подраздел **Добавление VRF**).

Для создания VRF используются команды:

- создание VRF и назначение таблицы маршрутизации:

❗ Описание параметров также приведено в подразделе **Команда set**.

```
set vrf name <имя> table-id <номер таблицы>
```

❗ Номер таблицы задает идентификатор таблицы маршрутизации, которая будет ассоциирована с этим VRF. Номер таблицы должен быть уникальным.

- применение конфигурации:

```
commit
```

- сохранение конфигурации:

```
write
```

### 3.3.3 . Настройка VLAN

Настройка VLAN является необязательной и выполняется одним из способов:

- из интерфейса командной строки Termidesk Connect;
- из веб-интерфейса Termidesk Connect (см. подраздел **Добавление VLAN**).

Для создания и настройки VLAN используются команды:

- создание VLAN и назначение ему идентификатора:

❗ Описание параметров также приведено в подразделе **Команда set**.

```
set vlan name <имя> vlan-id <идентификатор>
```

- назначение VLAN сетевому интерфейсу:

 Сетевые интерфейсы определяются автоматически при загрузке Termidesk Connect.

```
set vlan name <имя> if-ethernet <имя интерфейса>
```

- (опционально) назначение VRF для VLAN:

```
set vlan name <имя> vrf <имя VRF>
```

- применение конфигурации:

```
commit
```

- сохранение конфигурации:

```
write
```


### 3.3.4. Настройка IP-адресов

Настройка IP-адресов является обязательной и выполняется одним из способов:

- из интерфейса командной строки Termidesk Connect;
- из веб-интерфейса Termidesk Connect (см. подраздел **Добавление IP-адресации**).

Для добавления и настройки IP-адресов используются команды:

- добавление IP-адреса в формате CIDR:

 Описание параметров также приведено в подразделе **Команда set**.

```
set ip address <IP-адрес> <префикс сети>
```

- назначение сетевого интерфейса для добавленного IP-адреса:

 Сетевые интерфейсы определяются автоматически при загрузке Termidesk Connect.

```
set ip address <IP-адрес> <префикс сети> if-ethernet <имя интерфейса>
```

 Пример:

```
set ip address 172.16.0.1 /16 if-ethernet eth0
```

- или назначение VLAN для добавленного IP-адреса:

⚠ VLAN должен быть предварительно создан.

```
set ip address <IP-адрес> <префикс сети> if-vlan <имя VLAN>
```

- применение конфигурации:

```
commit
```

- сохранение конфигурации:

```
write
```

### 3.3.5 . Настройка маршрутизации

Настройка маршрутизации является обязательной и выполняется одним из способов:

- из интерфейса командной строки Termidesk Connect;
- из веб-интерфейса Termidesk Connect (см. подраздел **Добавление параметров маршрутизации**).

Для добавления маршрута используются команды:

- добавление маршрута с указанием IP-адреса в формате CIDR:

📘 Описание параметров также приведено в подразделе **Команда set**.

```
set ip route <имя VRF> <IP-адрес/маска> <IP-адрес шлюза>
```

📘 Пример:

```
set ip route namevrf 0.0.0.0/8 172.16.0.1
```

- применение конфигурации:

```
commit
```

- сохранение конфигурации:

```
write
```

### 3.3.6 . Настройка IP-фондов

Настройка IP-фондов является необязательной и выполняется одним из способов:

- из интерфейса командной строки Termidesk Connect;
- из веб-интерфейса Termidesk Connect (см. подраздел **Добавление IP-фонда**).

Для создания и настройки IP-фондов используются команды:

- создание IP-фонда:

**⚠** Имя создаваемого объекта не должно содержать дефисов, нижнее подчеркивание использовать разрешено.

```
set ipset id <имя>
```

**i** Описание параметров также приведено в подразделе **Команда set**.

- добавление IP-адреса в IP-фонд:

**i** IP-адрес может быть любым: он необязательно должен быть из списка тех, что уже существуют для физических сетевых интерфейсов.

```
set ipset id <имя> ips <IP-адрес>
```

- применение конфигурации:

```
commit
```

- сохранение конфигурации:

```
write
```

- просмотр конфигурации IP-фонда (указывается формат вывода – XML, JSON и TXT):

```
show configuration xml ipset id <имя>
```

- просмотр конфигурации IP-адреса в IP-фонде:

```
show configuration <тип просмотра> ipset id <имя> ips <IP-адрес>
```

### 3.4 . Диагностика

Диагностика позволяет выявить сетевые неисправности при возникновении проблем с подключением через Termidesk Connect.

Диагностика сети в Termidesk Connect выполняется через стандартный интерфейс командной строки Linux Shell. Для перехода в интерфейс следует вызвать из CLI команду:

```
bash
```

Для диагностики сети могут использоваться команды Linux Shell:

- для проверки сетевого соединения к узлу:

```
sudo ping <IP-адрес>
```

- для анализа и фильтрации трафика:

```
sudo tcpdump -i <интерфейс>
```

- для проверки маршрута до узла:

```
sudo tcptraceroute <IP-адрес> <порт>
```

- для анализа и фильтрации трафика SSL/TLS:

```
sudo ssldump
```

## 3.5 . Аудит

### 3.5.1 . Журналы Termidesk Connect

Для просмотра журнала нужно:

- перейти в стандартный интерфейс командной строки Linux Shell из CLI:

```
bash
```

- выполнить:

```
sudo journalctl -f -u <имя службы>
```

- или выполнить:

```
sudo tail -f /var/log/syslog
```

## 3.6 . Резервное копирование и обновление

### 3.6.1 . Общие сведения по управлению образами и резервными копиями

Для управления образами Termidesk Connect и их настройкой используется инструмент `va`.

Инструмент `va` доступен при переходе в стандартный интерфейс командной строки Linux Shell, для этого:

- перейти в интерфейс командной строки Termidesk Connect;
- выполнить:

```
bash
```

Использование:

```
va <опция>
```

Для получения информации по основным опциям инструмента `va` следует выполнить:

```
va ?
```

Перечень доступных опций приведен в таблице (см. Таблица 2).

Таблица 2 – Основные опции инструмента `va`

Опция	Описание
<code>backup</code>	Управление резервными копиями
<code>image</code>	Управление образами
<code>init</code>	Инициализация служб и первичная настройка образа
<code>setup</code>	Настройка служб
<code>version</code>	Вывод версии образа

### 3.6.2 . Управление резервными копиями через инструмент `va`

Для управления резервными копиями используется опция `backup` с командами, перечисленными в таблице (см. Таблица 3).

Таблица 3 – Основные команды опции `backup`

Команда	Описание
<code>compat</code>	Вывод минимальной версии, необходимой для совместимости резервных копий
<code>create</code>	Создание новой резервной копии
<code>delete</code>	Удаление резервной копии
<code>list</code>	Вывод списка резервных копий
<code>restore</code>	Восстановление из резервной копии

Примеры использования:

- получение списка резервных копий текущего образа:

```
sudo va backup list
```

- получение списка резервных копий конкретного образа:

```
sudo va backup list <имя образа>
```

- создание резервной копии:

```
sudo va backup create
```

- удаление резервной копии текущего образа:

```
sudo va backup delete <имя резервной копии>
```

- удаление резервной копии конкретного образа:

```
sudo va backup delete <имя резервной копии> <имя образа>
```

- восстановление из резервной копии текущего образа:

```
sudo va backup restore <имя резервной копии>
```

- восстановление из резервной копии конкретного образа:

```
sudo va backup restore <имя резервной копии> <имя образа>
```

### 3.6.3 . Управление образами через инструмент va

Для управления образами используется опция `image` с командами, перечисленными в таблице (см. Таблица 4).

Таблица 4 – Основные команды опции `image`

Команда	Описание
<code>current</code>	Установка приоритета загрузки указанному образу
<code>delete</code>	Удаление образа
<code>list</code>	Вывод списка образов
<code>update</code>	Обновление существующего образа
<code>upgrade</code>	Установка нового образа

Примеры использования:

- установка нового образа:

```
sudo va image upgrade <путь к новому образу>
```

- установка нового образа с распаковкой в него резервной копии текущего образа:

```
sudo va image upgrade <путь к новому образу> <имя резервной копии>
```

- установка нового образа с распаковкой в него резервной копии конкретного образа:

```
sudo va image upgrade <путь к новому образу> <имя образа> <имя резервной копии>
```

- получение списка образов:

```
va image list
```

- получение списка всех образов:

```
va image list all
```

- установить текущий образ приоритетным для загрузки:

```
sudo va image current
```

- установить приоритетную загрузку указанному образу:

```
sudo va image current <имя образа>
```

- удаление образа:

```
sudo va image delete <имя образа>
```



## 4. УПРАВЛЕНИЕ ТРАФИКОМ

### 4.1. Проверки

#### 4.1.1. Общие сведения о проверках

Проверки являются методами тестирования и диагностики сетевых соединений и работоспособности сервисов. Termidesk Connect позволяет создать:

- ICMP-проверки, основанные на использовании протокола ICMP для определения состояния сетевого соединения. Такие проверки выполняют отправку ICMP-запросов на узел, и на основании ответов определяют, доступен он или нет;
- TCP-проверки, основанные на использовании протокола TCP. Такие проверки позволяют определить, доступен ли сервис на указанном порту.

#### 4.1.2. Создание и настройка ICMP-проверки

Создание и настройка ICMP-проверок выполняется одним из способов:

- из интерфейса командной строки Termidesk Connect;
- из веб-интерфейса Termidesk Connect (см. подраздел **Добавление проверки**).

Для создания и настройки ICMP-проверки используются команды:

- создание проверки:

```
set health-check id <имя>
```

 Описание параметров также приведено в подразделе **Команда set**.

- назначение протокола для проверки:

```
set health-check id <имя> ICMP
```

- задание интервала проверки:

```
set health-check id <имя> ICMP interval 10
```

- задание времени ожидания (в секундах) ответа на запрос:

```
set health-check id <имя> ICMP timeout 5
```

- задание количества повторных проверок в случае отсутствия ответа:

```
set health-check id <имя> ICMP try 1
```

- задание необходимого количества успешных проверок после восстановления связности:

```
set health-check id <имя> ICMP success-try 1
```

- (опционально) указание IP-адреса назначения, если он отличается от IP-адреса, указанного в настройках реального сервера:

```
set health-check id <имя> ICMP target-ip <IP-адрес>
```

- указание IP-адреса источника (Termidesk Connect), с которого будет выполнена проверка:

- i** Указание отдельных IP-адресов для проверок используется для логического разделения трафика:
- для перенаправления пользовательских подключений к Реальным Серверам Termidesk Connect будет использовать один пул IP-адресов (IP-фонд);
  - соответственно, для проверок будут использоваться другие IP-адреса, указанные непосредственно в проверках.

```
set health-check id <имя> ICMP source-ip <IP-адрес>
```

- применение заданных настроек:

```
commit
```

- сохранение настроек:

```
write
```

- просмотр заданных проверок (указывается формат вывода – XML, JSON и TXT):

```
show configuration xml health-check id <имя>
```

- просмотр выполненных команд:

```
show configuration cli health-check id <имя>
```

#### 4.1.3 . Создание и настройка ТСП-проверки

Создание и настройка ТСП-проверок выполняется одним из способов:

- из интерфейса командной строки Termidesk Connect;
- из веб-интерфейса Termidesk Connect (см. подраздел **Добавление проверки**).

Для создания и настройки ТСП-проверки используется следующий набор команд:

- создание проверки:

```
set health-check id <имя>
```

**i** Описание параметров также приведено в подразделе **Команда set**.

- назначение протокола для проверки:

```
set health-check id <имя> TCP
```

- задание интервала проверки:

```
set health-check id <имя> TCP interval 10
```

- задание времени ожидания (в секундах) ответа на запрос:

```
set health-check id <имя> TCP timeout 5
```

- задание количества повторных проверок в случае отсутствия ответа:

```
set health-check id <имя> TCP try 1
```

- задание необходимого количества успешных проверок после восстановления связности:

```
set health-check id <имя> TCP success-try 1
```

- (опционально) указание IP-адреса назначения, если он отличается от IP-адреса, указанного в настройках реального сервера:

```
set health-check id <имя> TCP target-ip <IP-адрес>
```

- указание IP-адреса источника (Termidesk Connect), с которого будет выполнена проверка:

```
set health-check id <имя> TCP source-ip <IP-адрес>
```

- (опционально) порт назначения, подлежащий проверке (по умолчанию используется порт реального сервера из группы реальных серверов):

```
set health-check id <имя> TCP target-port <порт>
```

- применение заданных настроек:

```
commit
```

- сохранение настроек:

```
write
```

- просмотр заданных проверок (указывается формат вывода – XML, JSON и TXT):

```
show configuration xml health-check id <имя>
```

- просмотр выполненных команд:

```
show configuration cli health-check id <имя>
```

## 4.2 . Реальные Серверы

### 4.2.1 . Общие сведения о Реальных Серверах

Реальный Сервер в Termidesk Connect представляет собой IP-адрес и порт узла с установленным приложением (ресурсом), доступ к которому предоставляется пользователю. Доступ пользователя к Реальным Серверам балансируется Серверами Балансировки.

Группа Реальных Серверов – объединение нескольких Реальных Серверов и их периодических проверок.


### 4.2.2 . Создание и настройка группы Реальных Серверов

Создание и настройка группы Реальных Серверов выполняется одним из способов:

- из интерфейса командной строки Termidesk Connect;
- из веб-интерфейса Termidesk Connect (см. подраздел **Добавление Реального Сервера**).

Для создания и настройки группы Реальных Серверов используются команды:

- создание группы Реальных Серверов:

 Имя создаваемого объекта не должно содержать дефисов, нижнее подчеркивание использовать разрешено.

```
set rs-pool id <имя>
```

 Описание параметров также приведено в подразделе **Команда set**.

- (опционально) указание IP-фонда (см. подраздел **Сеть**):

```
set rs-pool id <имя> ipset-id <имя>
```

- назначение Реального Сервера группе (может быть задано несколько узлов):

```
set rs-pool id <имя> rs <IP-адрес> <порт>
```

- (опционально) назначение ранее созданной проверки для группы Реальных Серверов:

```
set rs-pool id <имя> hc-id <имя>
```

- применение заданных настроек:

```
commit
```

- сохранение настроек:

```
write
```

- просмотр заданных настроек (указывается формат вывода – XML, JSON и TXT):

```
show configuration xml rs-pool id <имя>
```

- просмотр выполненных команд:

```
show configuration cli rs-pool id <имя>
```

## 4.3 . Серверы Балансировки

### 4.3.1 . Общие сведения о Серверах Балансировки

Сервер Балансировки в Termidesk Connect – это объект (абстракция), с заданным алгоритмом балансировки и другими параметрами, реализующий перенаправление подключения пользователя на один из Реальных Серверов.

### 4.3.2 . Создание и настройка Сервера Балансировки для протокола TCP


Создание и настройка Сервера Балансировки выполняется одним из способов:

- из интерфейса командной строки Termidesk Connect;
- из веб-интерфейса Termidesk Connect (см. подраздел **Добавление Сервера Балансировки**).


Для создания и настройки Сервера Балансировки используются команды:

- создание Сервера Балансировки:

```
set lbs TCP <имя>
```

 Описание параметров также приведено в подразделе **Команда set**.

- назначение группы Реальных Серверов для Сервера Балансировки:

 В текущей версии Termidesk Connect предполагается, что один Сервер Балансировки работает с одной группой Реальных Серверов.

```
set lbs TCP <имя> rs-pool-id <имя>
```

- указание минимального количества активных Реальных Серверов, при котором Сервер Балансировки также будет активен:

- ❗ Если Сервер Балансировки становится неактивным (переходит в статус «Не работает»), то в текущей версии Termidesk Connect подключение пользователя к Реальному Серверу будет сброшено.

```
set lbs TCP <имя> min-rs <значение>
```

- (опционально) задание алгоритма привязки пользователя к Реальному Серверу на время активной сессии:

- ❗ Алгоритм привязки пользователя может быть:

- IPSOURCE – привязка по IP-адресу источника запроса, т.е. IP-адресу пользователя;
- NONE – привязка не используется.

Настройка привязки пользователя используется, когда нужно сохранить соединение пользователя на определенном Реальном Сервере. Это актуально, например, в электронной коммерции – Интернет-магазинах и др., чтобы алгоритмы балансировки не перенаправили пользователя на другой Реальный Сервер.

```
set lbs TCP <имя> persistence algorithm <тип>
```

- (опционально) задание времени ожидания (в секундах), в течение которого повторное подключение пользователя будет направлено на ранее выбранный Реальный Сервер:

- ❗ Пример: пользователь запросил доступ к приложению, а Termidesk Connect направил его на Реальный Сервер N. Пользователь получил приложение, поработал с ним и отключился, но позже запросил доступ снова.

Если задано время ожидания, то:

- в течение этого времени Termidesk Connect будет «помнить» о том, что пользователь ранее подключался к Реальному Серверу N;
- если время ожидания не истекло и пользователь повторно запросил доступ, то Termidesk Connect перенаправит подключение пользователя на Реальный Сервер N.

```
set lbs TCP <имя> persistence ipsource-param timeout <значение>
```

- задание алгоритма балансировки:

```
set lbs TCP <имя> algorithm <алгоритм>
```

- ❗ Алгоритм балансировки может быть:

- ROUNDROBIN – подключения пользователей в этом случае распределяются последовательно между Реальными Серверами, что обеспечивает их равномерное распределение;
- LEASTCONN – подключения пользователей в этом случае распределяются оптимизировано, с учетом количества текущих активных соединений на каждом Реальном Сервере. Для подключения пользователя выбирается Реальный Сервер с наименьшим количеством текущих активных соединений, что обеспечивает более равномерное распределение нагрузки и помогает избежать перегрузки отдельных Реальных Серверов.

- при использовании алгоритма LEASTCONN указывается время (в секундах), на которое производится смена алгоритма на ROUNDROBIN во время изменений в группе Реальных Серверов:

**i** Параметр `starttime` указывает, на какое время после изменения группы Реальных Серверов Сервер Балансировки перейдет на работу по алгоритму ROUNDROBIN для выравнивания количества подключений между Реальными Серверами. Это позволяет исключить перегрузку Реального Сервера в случае, когда состав группы изменился (добавился новый узел), и все подключения пользователей были перенаправлены на новый Реальный Сервер.

```
set lbs TCP <имя> leastconn-param starttime <значение>
```

- (опционально) привязка клиентского SSL-профиля к Серверу Балансировки (см. подраздел **Создание и настройка клиентского SSL-профиля**):

```
set lbs TCP <имя> ssl-profile-id <имя профиля>
```

- применение заданных настроек:

```
commit
```

- сохранение настроек:

```
write
```

- просмотр заданных настроек (указывается формат вывода – XML, JSON и TXT):

```
show configuration xml lbs TCP <имя>
```

- просмотр выполненных команд:

```
show configuration cli lbs TCP <имя>
```

### 4.3.3 . Создание и настройка Сервера Балансировки для протокола RAPID-TCP

Создание и настройка Сервера Балансировки выполняется из интерфейса командной строки Termidesk Connect.

Для создания и настройки Сервера Балансировки используются команды:

- создание Сервера Балансировки:

```
set lbs RAPID-TCP <имя>
```

**i** Описание параметров также приведено в подразделе **Команда set**. Часть настроек выполняется аналогично Серверу Балансировки для протокола TCP (см. подраздел **Создание и настройка Сервера Балансировки для протокола TCP**).

- назначение группы Реальных Серверов для Сервера Балансировки:

**i** В текущей версии Termidesk Connect предполагается, что один Сервер Балансировки работает с одной группой Реальных Серверов.

```
set lbs RAPID-TCP <имя> rs-pool-id <имя>
```

- указание минимального количества активных Реальных Серверов, при котором Сервер Балансировки также будет активен:

```
set lbs RAPID-TCP <имя> min-rs <значение>
```

- задание алгоритма балансировки:

```
set lbs RAPID-TCP <имя> algorithm <алгоритм>
```

- при использовании алгоритма LEASTCONN указывается время (в секундах), на которое производится смена алгоритма на ROUNDROBIN во время изменений в группе Реальных Серверов:

```
set lbs RAPID-TCP <имя> leastconn-param starttime <значение>
```

- (опционально) задание алгоритма привязки пользователя к Реальному Серверу на время активной сессии:

```
set lbs RAPID-TCP <имя> persistence algorithm <тип>
```

- (опционально) задание времени ожидания (в секундах), в течение которого повторное подключение пользователя будет направлено на ранее выбранный Реальный Сервер:



```
set lbs RAPID-TCP <имя> persistence ipsource-param timeout <значение>
```

- активация или отключение режима сохранения IP-адреса из IP-фонда для взаимодействия с Реальным Сервером:

❗ Режим сохранения IP-адреса из IP-фонда работает следующим образом:

- если режим активирован (`true`), то Termidesk Connect будет сохранять ранее выбранный IP-адрес из пула адресов IP-фонда для взаимодействия с Реальным Сервером;
- если режим отключен (`false`), то Termidesk Connect будет выбирать случайный IP-адрес из пула адресов IP-фонда для взаимодействия с Реальным Сервером.

```
set lbs RAPID-TCP <имя> persistence ipsource-param ipset-src-persist <true/false>
```

- задание времени жизни сессии (в секундах) после получения управляющего флага FIN в заголовке пакета:

```
set lbs RAPID-TCP <имя> fin-timeout <значение>
```

- задание времени жизни сессии (в секундах) при бездействии (отсутствии пакетов):

```
set lbs RAPID-TCP <имя> connection-idle <значение>
```

- активация или отключение режима подмены IP-адреса клиента:

❗ Режим подмены IP-адреса клиента работает следующим образом:

- если режим активирован (`true`), то Termidesk Connect не будет подменять IP-адрес клиента. Следовательно, при взаимодействии с Реальным Сервером в источник запроса будет помещен IP-адрес клиента. При этом сетевой инфраструктурой должна обеспечиваться правильная обработка такого запроса: Реальный Сервер должен иметь возможность ответить на него;
- если режим отключен (`false`), то Termidesk Connect подменяет IP-адрес источника (клиента) и взаимодействует с Реальным сервером со своего IP-адреса. При этом в группе Реальных Серверов обязательно должен быть задан IP-фонд (см. подраздел **Создание и настройка группы Реальных Серверов**).

```
set lbs RAPID-TCP <имя> use-cip <false/true>
```

- применение заданных настроек:

```
commit
```

- сохранение настроек:

```
write
```

- просмотр заданных настроек (указывается формат вывода – XML, JSON и TXT):

```
show configuration xml lbs RAPID-TCP <имя>
```

- просмотр выполненных команд:

```
show configuration cli lbs RAPID-TCP <имя>
```

## 4.4 . TLS

### 4.4.1 . Общие сведения о TLS

TLS используется в Termidesk Connect для:

- настройки доступа к веб-интерфейсу по протоколу HTTPS;
- настройки SSL-соединения;
- настройки функционала SSL Offload;
- настройки взаимной аутентификации по протоколу mTLS.

**i** Подразумевается, что SSL и TLS – два неразрывно связанных протокола. Поэтому здесь и далее они равнозначны: например, SSL Offload и TLS Offload представляют один и тот же процесс, но далее будет использовано только наименование SSL Offload.

SSL Offload – это процесс, в котором преобразование трафика SSL/TLS выполняется не на серверах приложений (Реальных Серверах), а на Termidesk Connect, что также позволяет снизить нагрузку с Реальных Серверов. Процесс выглядит следующим образом:

- Termidesk Connect терминирует на себе сессию пользователя;
- в зависимости от настроек Termidesk Connect:
  - либо преобразует полученные данные к открытому виду для последующего их анализа и обработки;
  - либо не преобразует полученные данные, поскольку они уже пришли в открытом виде;
- далее, в зависимости от настроек, Termidesk Connect:
  - либо отправляет на Реальный Сервер данные без преобразования;
  - либо преобразует данные, а потом отправляет их на Реальный Сервер.

Для реализации этого функционала создаются SSL-профили.

#### 4.4.2 . Файлы для SSL/TLS

Загрузка сертификатов и ключей выполняется через веб-интерфейс (см. подраздел **Просмотр и добавление сертификата через веб-интерфейс Termidesk Connect**).

 После загрузки файлы будут расположены в каталоге `/etc/ssl/tdc/`.

#### 4.4.3 . Профили SSL/TLS

Профили определяют настройки и параметры, используемые для преобразования данных. В контексте управления трафиком важно понимать различия между серверными и клиентскими профилями:

- серверный профиль настраивается для обеспечения безопасного соединения между пользователем и Termidesk Connect;
- клиентский профиль настраивается для обеспечения безопасного соединения между Termidesk Connect и Реальным Сервером.

#### 4.4.4 . Создание и настройка серверного SSL-профиля

Для создания и настройки серверного SSL-профиля используется формат работы с командой:

```
set ssl-profile server <имя профиля> <параметр> <значение>
```

 Описание параметров также приведено в подразделе **Команда set**.

Команда настройки серверных SSL-профилей включает в себя аналогичные параметры, что и клиентский профиль, с дополнительной настройкой идентификации имени сервера и управлением режимом взаимной аутентификации (mTLS).

Пример команд настройки серверного SSL-профиля:


- создание SSL-профиля:

```
set ssl-profile server <имя профиля>
```

- указание времени ожидания (в секундах) ответа от пользователя:

```
set ssl-profile server <имя профиля> handshake-timeout <значение>
```

- (опционально) указание значения поля SNI из TLS Hello, для которого требуются особые настройки обработки:

 SNI – расширение протокола TLS, позволяющее пользователю сообщать имя узла, с которым он хочет установить соединение во время процесса «рукопожатия». Это позволяет серверу (в Termidesk Connect – Виртуальному Серверу) предоставлять несколько сертификатов на одном IP-адресе и TCP-порту, и, следовательно, позволяет работать

нескольким HTTPS-сайтам или другим сервисам поверх TLS на одном IP-адресе без использования одного и того же сертификата на всех сайтах. Имя узла передается в TLS Hello пользователя.

**⚠** Если требуется задать правила для нескольких SNI, то для каждого из них должна использоваться индивидуальная настройка.

```
set ssl-profile server <имя профиля> host <имя>
```

- указание списка центров сертификации, которые используются для проверки подлинности клиентского сертификата пользователя:

**i** Используется, если активирована взаимная аутентификация по протоколу mTLS.

```
set ssl-profile server <имя профиля> host <имя> setting ca-cert <список>
```

- указание пути к файлу сертификата сервера, который будет использоваться для аутентификации Termidesk Connect:

```
set ssl-profile server <имя профиля> host <имя> setting cert <путь>
```

- указание пути к файлу параметров Диффи-Хеллмана, используемого для безопасного обмена ключами при установлении SSL-соединения:

```
set ssl-profile server <имя профиля> host <имя> setting dh-params <путь>
```

- указание пути к файлу закрытого ключа, соответствующему серверному сертификату:

```
set ssl-profile server <имя профиля> host <имя> setting key <путь>
```

- (опционально) если ключ зашифрован, то указать пароль для расшифровки закрытого ключа:

```
set ssl-profile server <имя профиля> host <имя> setting password <пароль>
```

- активация поддержки взаимной аутентификации по протоколу mTLS:

```
set ssl-profile server <имя профиля> host <имя> setting mtls true
```

- определение набора алгоритмов, которые могут использоваться для преобразования данных между пользователем и Termidesk Connect:

**⚠** Команда позволяет за один раз добавить только один алгоритм.

После создания SSL-профиля по умолчанию уже назначены следующие алгоритмы: TLS\_AES\_256\_GCM\_SHA384, TLS\_CHACHA20\_POLY1305\_SHA25, TLS\_AES\_128\_GCM\_SHA256, ECDHE-ECDSA-AES256-GCM-SHA384, ECDHE-ECDSA-AES128-GCM-SHA256, ECDHE-ECDSA-AES256-SHA384, ECDHE-RSA-AES256-SHA384, ECDHE-ECDSA-AES128-SHA256, ECDHE-RSA-AES128-SHA256, ECDHE-ECDSA-AES256-SHA, ECDHE-RSA-AES256-SHA, ECDHE-ECDSA-AES128-SHA, ECDHE-RSA-AES128-SHA.

```
set ssl-profile server <имя профиля> host <имя> setting ciphers <алгоритм> true
```

- указание версии протокола TLS для данного серверного SSL-профиля:

```
set ssl-profile server <имя профиля> host <имя> setting versions <версия TLS> true
```

После настройки профилей необходимо применить и сохранить данные:

- применение заданных настроек:

```
commit
```

- сохранение настроек:

```
write
```

- просмотр заданных настроек серверного SSL-профиля (указывается формат вывода – XML, JSON и TXT):

```
show configuration xml ssl-profile server <имя профиля>
```

- просмотр выполненных команд:

```
show configuration cli ssl-profile server <имя профиля>
```

- ⚠ Termidesk Connect позволяет использовать особую конфигурацию серверного SSL-профиля для соединения, не попавшего в указанные правила. Если пришедший SNI пуст, либо не соответствует SNI, указанному в параметре host, то для этого соединения будет применена конфигурация setting-default.

#### 4.4.5 . Создание и настройка клиентского SSL-профиля

Для создания и настройки клиентского SSL-профиля используется формат работы с командой:

```
set ssl-profile client <имя> <параметр> <значение>
```

- 📘 Описание параметров также приведено в подразделе **Команда set**.

Пример команд настройки клиентского профиля:

- создание клиентского SSL-профиля:

```
set ssl-profile client <имя>
```

⚠ При создании клиентского SSL-профиля создается минимально необходимая конфигурация для него.  
Все настройки, приведенные далее, относятся к переопределению конфигурации по умолчанию.

- указание версии протокола TLS для данного SSL-профиля:

⚠ Команда позволяет за один раз добавить только одно значение протокола TLS.  
После создания SSL-профиля по умолчанию уже назначены следующие версии: tls-v1, tls-v11, tls-v12.

```
set ssl-profile client <имя> versions <версия TLS> true
```

- определение набора алгоритмов, которые могут использоваться для преобразования данных между Termidesk Connect и Реальным Сервером:

⚠ Команда позволяет за один раз добавить только один алгоритм.  
После создания SSL-профиля по умолчанию уже назначены следующие алгоритмы:  
TLS\_AES\_256\_GCM\_SHA384, TLS\_CHACHA20\_POLY1305\_SHA256,  
TLS\_AES\_128\_GCM\_SHA256, ECDHE-ECDSA-AES256-GCM-SHA384, ECDHE-ECDSA-AES128-GCM-SHA256, ECDHE-ECDSA-AES256-SHA384, ECDHE-RSA-AES256-SHA384,  
ECDHE-ECDSA-AES128-SHA256, ECDHE-RSA-AES128-SHA256, ECDHE-ECDSA-AES256-SHA, ECDHE-RSA-AES256-SHA, ECDHE-ECDSA-AES128-SHA, ECDHE-RSA-AES128-SHA.

```
set ssl-profile client <имя> ciphers <алгоритм> true
```

- указание имени сервера по умолчанию для расширения SNI:

ⓘ По умолчанию для соединения с Реальным Сервером используется SNI из запроса пользователя. Однако, если в запросе пользователя это поле было пустым, то Termidesk Connect при соединении с Реальным Сервером будет использовать SNI, указанный в sni-default.

```
set ssl-profile client <имя> sni-default <имя>
```

- указание времени ожидания (в секундах) установки соединения с Реальным Сервером:

```
set ssl-profile client <имя> handshake-timeout <значение>
```

- (опционально) указание списка центров сертификации, которые используются для проверки подлинности Реального Сервера (используется, если активирована взаимная аутентификация по протоколу mTLS):

```
set ssl-profile client <имя> ca-cert <список>
```

- (опционально) указание пути к файлу клиентского сертификата, который будет использоваться для аутентификации на Реальном Сервере (используется, если активирована взаимная аутентификация по протоколу mTLS):

```
set ssl-profile client <имя> cert <путь>
```

- (опционально) указание пути к файлу параметров Диффи-Хеллмана, используемому для обмена ключами и обеспечения безопасного соединения:

```
set ssl-profile client <имя> dh-params <путь>
```

- (опционально) указание пути к файлу закрытого ключа, соответствующему клиентскому сертификату (используется, если активирована взаимная аутентификация по протоколу mTLS):

```
set ssl-profile client <имя> key <путь>
```

- (опционально) если ключ зашифрован, то указать пароль для расшифровки закрытого ключа:

```
set ssl-profile client <имя> password <пароль>
```

После настройки профилей необходимо применить и сохранить данные:

- применение заданных настроек:

```
commit
```

- сохранение настроек:

```
write
```

- просмотр заданных настроек клиентского SSL-профиля (указывается формат вывода – XML, JSON и TXT):

```
show configuration xml ssl-profile client <имя>
```

- просмотр выполненных команд:

```
show configuration cli ssl-profile client <имя>
```

## 4.5 . Сценарии

### 4.5.1 . Общие сведения о сценариях

Сценарии – это Lua-файлы, являющиеся дополнением к основным параметрам конфигурации Виртуальных Серверов.

Сценарии предназначены для:

- выбора Сервера Балансировки: распределения клиентских запросов по нескольким Серверам Балансировки на основе данных в запросе;
- изменения содержимого запросов (HTTPS/HTTPS);
- ответа на запрос (HTTP/HTTPS);
- прерывания нежелательного соединения.

В сценариях можно определять условия выполнения того или иного действия логическими выражениями:

- if;
- elseif;
- else;
- end.

Условиями для логических выражений могут быть любые данные, полученные из запроса, а также комбинация эти данных, например:

- выражение для сравнения имени хоста из запроса с именем abc.ru для выполнения какого-либо действия:

```
1 If client.http_req.host == "abc.ru" then
```

- выражение для сравнения имени хоста из запроса с именем abc.ru и принадлежностью к определенному IP-адресу:

```
1 if (client.http_req.host == "abc.ru" and client.remote_p.ip == "192.0.2.1")
```

Для работы с полученными данными можно использовать возможности языка программирования Lua. Примеры выражений для обработки запроса вида qwe.123.ru/abczxc:

- выражение сравнения. Результатом будет true:

```
1 If client.http_req.path == "/abcZxc"
```

- выражение содержания определенного значения. Результатом будет true:

```
1 If (client.http_req.path:find("zx"))
```

- выражение для получения определенной части строки. Результатом будет qwe:



```
1 (client.http_req.host:match("(.*).123.ru")
```

Обработка правил сценария осуществляется через глобальную переменную `client`, которая содержит в себе ряд полей. Описание полей приведено в таблице (см. Таблица 5).

**⚠** Обработка правил сценария останавливается после выражения: `client.action = "xxx"`.

Таблица 5 – Описание полей структуры `client`

Поле	Тип поля	Описание
<code>client.remote_p</code>	Структура	Содержит поля удаленной точки подключения, где: <ul style="list-style-type: none"> <li><code>remote_p.ip</code> (строка) – возвращает IP-адрес соединения;</li> <li><code>remote_p.port</code> (целое) – возвращает порт соединения;</li> <li><code>remote_p.is_network(VAR)</code> (метод) – осуществляет проверку, является ли IP-адрес частью сети, задаваемой в переменной <code>VAR</code> вида <code>{IP}/{PREFIX}</code>:</li> </ul> <pre> 1  if    client.remote_p.is_network    ("127.0.0.1/24") then 2  ... 3  end                     </pre>
<code>client.local_p</code>	Структура	Содержит поля локальной точки подключения, аналогично <code>remote_p</code>
<code>client.http_req</code>	Структура или <code>nil</code>	<p><b>i</b> В текущей версии Termidesk Connect значение <code>nil</code> для балансировки уровня L7 вернуться не может.</p> Содержит поля HTTP-запроса или возвращает значение <code>nil</code> (HTTP-запрос отсутствует). Описание полей приведено в таблице (см. Таблица 6)
<code>client.bs</code>	Строка	Определяет имя Сервера Балансировки.                     Пример: <pre>client.bs = "lb1"</pre>
<code>client.respond.status</code>	Целое	Возвращает код ответа
<code>client.action</code>	Строка	Определяет действие: <ul style="list-style-type: none"> <li><code>client.action = "bs"</code> – возвращает Сервер Балансировки, определенный в <code>client.bs</code>;</li> <li><code>client.action = "respond"</code> – возвращает ответ клиенту, не передавая запрос на Реальный Сервер. Содержимое ответа описывается в <code>client.respond.status</code>;</li> <li><code>client.action = "drop"</code> – сбрасывает соединение</li> </ul>

Таблица 6 – Описание полей структуры http\_req

Поле	Тип поля	Описание								
http_req.version	Целое	Возвращает версию протокола HTTP: целое число, в котором младший десяток соответствует значению после точки, старший десяток - перед точкой. Поддерживаются версии: 1.0, 1.1. Пример: для HTTP/1.0 будет возвращен ответ: 10								
http_req.method	Строка	Возвращает метод запроса (GET, POST, HEAD, DELETE, PATCH, PUT, OPTIONS, CONNECT, TRACE и др.). В примере ниже: GET								
http_req.path	Строка	Возвращает путь запроса. В примере ниже: termideskconnect								
http_req.query	Строка	Возвращает запрос. В примере ниже: test=query								
http_req.path_and_query	Строка	Возвращает полный путь запроса. В примере ниже: termideskconnect?test=query								
http_req.host	Строка	Возвращает значение заголовка Host. В примере ниже: connect.termidesk.ru								
http_req.headers	Таблица (словарь)	Возвращает все заголовки со значениями. В примере ниже: <table border="1" data-bbox="901 1070 1513 1339"> <tbody> <tr> <td>1</td> <td>Host: connect.termidesk.ru</td> </tr> <tr> <td>2</td> <td>User-Agent: Mozilla Firefox /3.0.3</td> </tr> <tr> <td>3</td> <td>Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8</td> </tr> <tr> <td>4</td> <td>Cookie: sessionId=100TC</td> </tr> </tbody> </table>	1	Host: connect.termidesk.ru	2	User-Agent: Mozilla Firefox /3.0.3	3	Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8	4	Cookie: sessionId=100TC
1	Host: connect.termidesk.ru									
2	User-Agent: Mozilla Firefox /3.0.3									
3	Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8									
4	Cookie: sessionId=100TC									
http_req.body	Строка	Возвращает тело HTTP-запроса								

Примеры из таблицы (см. Таблица 6) отражены в этом ответе на запрос к узлу termideskconnect по протоколу HTTP:

```

1 GET /termideskconnect?test=query HTTP/1.0
2 Host: connect.termidesk.ru
3 User-Agent: Mozilla Firefox/3.0.3
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
5 Cookie: sessionId=100TC
  
```

#### 4.5.2 . Добавление сценария

Добавление сценария выполняется одним из способов:

- из интерфейса командной строки Termidesk Connect;
- из веб-интерфейса Termidesk Connect (см. подраздел **Добавление файлов сценария**).

Пример команды с указанием порядка исполнения и имени файла сценария:

```
set vs HTTP <имя> luarules 5 script test.lua
```

**⚠** Файл должен быть расположен в каталоге `/var/lib/tdc/lbscripts/content-switching/`. Порядковый номер определяет очередность выполнения файла сценария: например, сценарий с порядковым номером 10 будет исполнен раньше, чем сценарий с порядковым номером 15.

При этом правила в файлах сценариев также обрабатываются по порядку:

- сначала правила из файла сценария с наименьшим порядковым номером;
- затем правила из файла сценария со следующим порядковым номером, если не было совпадений.

Правила сценария могут располагаться как в одном файле, так и в нескольких.

#### 4.5.3 . Примеры сценариев для выбора Сервера Балансировки

Примеры приведены в таблице (см. Таблица 6).

Таблица 7 – Примеры сценариев для выбора Сервера Балансировки

Сценарий		Описание
1 2	<code>client.bs = "lb1"</code> <code>client.action = "bs"</code>	Передача любого запроса на Сервер Балансировки «lb1»
1 2 3 4 5 6 7	<code>if client.http_req.host == "abc"</code> <code>then</code> <code>client.bs = "lb1"</code> <code>client.action = "bs"</code> <code>else</code> <code>client.respond.status =</code> <code>403</code> <code>client.action = "respond"</code> <code>end</code>	Если имя хоста в запросе точно соответствует «abc», то направить запрос на Сервер Балансировки «lb1». В противном случае вернуть код ответа 403 (по умолчанию вернется ошибка 503)
1 2 3 4 5 6 7	<code>if (client.http_req.host:find("abc"</code> <code>) and</code> <code>client.remote_p:is_network("192.0.</code> <code>2.0/24")) then</code> <code>client.bs = "lb1"</code> <code>client.action = "bs"</code> <code>else</code> <code>client.respond.status =</code> <code>403</code> <code>client.action = "respond"</code> <code>end</code>	Если имя хоста содержит текст «abc» и запрос пришел из сети 192.0.2.0/24, то вернуть Сервер Балансировки «lb1». В противном случае вернуть код ответа 403 (по умолчанию вернется ошибка 503)

Сценарий	Описание
<pre> 1  if client.http_req.path:find("red") 2      then 3          client.bs = "lb1" 4          client.action = "bs" 5  elseif client.http_req.path:find(" 6  green") then 7          client.bs = "lb2" 8          client.action = "bs" 9  else 10         client.bs = "lb-default" 11         client.action = "bs" 12     end </pre>	<p>Если:</p> <ul style="list-style-type: none"> <li>путь содержит «red», то вернуть Сервер Балансировки «lb1»;</li> <li>путь содержит «green», то вернуть Сервер Балансировки «lb2».</li> </ul> <p>Если не сработало ни одно из условий выше, то вернуть Сервер Балансировки «lb-default»</p>

#### 4.5.4 . Примеры сценариев для изменения содержимого запросов

Примеры приведены в таблице (см. Таблица 7).

Таблица 8 – Примеры сценариев для изменения содержимого запросов

Сценарий	Описание
<pre> 1  if (client.http_req.host:find("abc 2  ") and 3  client.remote_p:is_network("192.0. 4  2.0/24")) then 5 6  client.http_req.header:field_set(" 7  XFF", client.remote_p.ip) 8  client.bs = "lb1" 9  client.action = "bs" 10 end </pre>	<p>Если имя хоста содержит текст «abc» и запрос пришел из сети 192.0.2.0/24, то добавить заголовок «XFF: &lt;IP-адрес пользователя при подключении&gt;», и перенаправить запрос на Сервер Балансировки «lb1».</p> <p>Результат:</p> <pre> 1  WEB -- 03&lt;p&gt;Method GET&lt;/p&gt;&lt;p&gt; 2  &gt;URL on server: /&lt;/p&gt;&lt;p&gt;REQ 3  Headers: &lt;/p&gt;Host: 4  abc.domain.ru 5  User-Agent: curl/7.81.0 6  Accept: */* 7  XFF: 192.0.2.5 </pre>
<pre> 1  function startswith(text, prefix) 2      return text:find(prefix, 1, true) 3      == 1 4  end 5 6  if 7      startswith(client.http_req.host, 8      "abc") then 9  client.http_req.header:field_set(" 10 Remote-port", 11 client.remote_p.port) 12 client.http_req.header:field_set(" 13 XFF", client.remote_p.ip) 14 client.bs = "lb1" 15 client.action = "bs" 16 end </pre>	<p>Если имя хоста начинается с «abc», то добавить заголовок «XFF: &lt;IP-адрес пользователя при подключении&gt;» и «Remote-port: &lt;порт-источник на клиенте&gt;», и перенаправить запрос на Сервер Балансировки «lb1»</p>

Сценарий	Описание
<pre> 1  if client.http_req.path:find("abc") 2      then 3          if 4              client.http_req.header:field_count 5                  ("X-Forwarded-For") &gt; 0 then 6                      xff, xffip = 7                      client.http_req.header:field_get(" 8                          X-Forwarded-For") 9                      client.http_req.header:field_set(" 10                         X-Forwarded-For", xffip ..", "..cl 11                         ient.remote_p.ip) 12                      else 13                          client.http_req.header:field_set(" 14                             X-Forwarded-For", 15                             client.remote_p.ip) 16                          end 17                      client.bs = "lb1" 18                      client.action = "bs" 19                  end </pre>	<p>Если:</p> <ul style="list-style-type: none"> <li>путь запроса содержит «app», то при наличии заголовка X-Forwarded-For добавить IP-адрес клиента в конец запроса;</li> <li>заголовка не было в запросе, то добавить новый.</li> </ul> <p>Перенаправить запрос на Сервер Балансировки «lb1»</p>
<pre> 1  client.http_req.host = 2  client.http_req.host:match("(.*).r 3  u") .. ".local" 4  client.http_req.path = "/external" 5  .. client.http_req.path 6  client.bs = "lb1" 7  client.action = "bs" </pre>	<p>Подменить домен «gu» на домен «local» (например, если запрос идет к app.domain.ru, то в сторону Реального Сервера должен прийти app.domain.local). В начале пути запроса добавить «/external» и перенаправить запрос на Сервер Балансировки «lb1»</p>

#### 4.5.5 . Примеры сценариев для ответа на запрос

Примеры приведены в таблице (см. Таблица 8).

Таблица 9 – Примеры сценариев для ответа на запрос

Сценарий	Описание
<pre> 1  if (client.http_req.method ~= "GET" and 2      client.http_req.method ~= "HEAD") then 3      client.action = "drop" 4  end </pre>	<p>Если метод не GET или не HEAD, то сбросить соединение</p>

Сценарий		Описание
<pre> 1 client.respond.status = 302 2 client.respond.header["Location"] =   "https://" .. client.http_req.host ..   client.http_req.path 3 client.respond.header["Connection"] =   "close" 4 client.action = "respond"                     </pre>	Перенаправить соединение с HTTP на HTTPS	
<pre> 1 <b>if</b> client.remote_p:is_network("192.0.2.   0/24") <b>then</b> 2   client.respond.header["Connection"]   = "close" 3   client.respond.header["Content-   type"] = 'text/html 4   client.respond.body = [[&lt;html&gt; 5   &lt;body&gt; 6   &lt;meta charset="UTF-8"&gt; 7   &lt;h1&gt;Lets goodbye!&lt;/h1&gt; 8   &lt;p&gt;Доступ запрещен&lt;/p&gt; 9   &lt;/body&gt; 10  &lt;/html&gt;]] .. "IP: " ..   client.remote_p.ip .. "\n TRY: " ..   client.http_req.host ..   client.http_req.path .. "\n" ..   "Vserver: " .. client.local_p.ip .. ":"   .. client.local_p.port 11 client.action = 'respond'                     </pre>	Если запрос из сети 192.0.2.0/24, то ответить HTML-страницей и параметрами запроса	

## 4.6 . Виртуальные Серверы

### 4.6.1 . Общие сведения о Виртуальных Серверах

Виртуальные Серверы в Termidesk Connect – это объект (абстракция), являющийся точкой входа для пользователей. Виртуальный Сервер принимает на себя подключение пользователя и далее через Серверы Балансировки принимается решение, на какой из Реальных Серверов будет направлено подключение.

Виртуальный Сервер может работать для балансировки протокола TCP (уровень L4 в модели OSI), RAPID TCP (уровень L4 в модели OSI) или HTTP (уровни L3-L7 в модели OSI). Выбор протокола зависит от того, какой тип балансировки требуется реализовать:

- при балансировке уровня L4 по протоколу TCP (см. Рисунок 2) клиент устанавливает соединение с Виртуальным Сервером Termidesk Connect, далее Termidesk Connect задействует алгоритмы, определенные в Сервере Балансировки, и устанавливает TCP-соединение с Реальным Сервером. В рамках установленного TCP-соединения передаются данные, которые Termidesk Connect не фильтрует;

- при балансировке уровня L4 по протоколу RAPID-TCP (см. Рисунок 3) клиент отправляет пакет SYN на Виртуальный Сервер Termidesk Connect. Уже на этом этапе Termidesk Connect задействует алгоритмы, определенные в Сервере Балансировки, и перенаправляет пакет SYN на Реальный Сервер. После установления TCP-соединения данные передаются в рамках него;
- при балансировке уровня L7 (see page 0) клиент устанавливает TCP-соединение с Виртуальным Сервером Termidesk Connect, далее Termidesk Connect ожидает от клиента HTTP-запрос. На основании переданного HTTP-запроса Termidesk Connect задействует алгоритмы, определенные в Сервере Балансировки, и устанавливает TCP-соединение с Реальным Сервером.

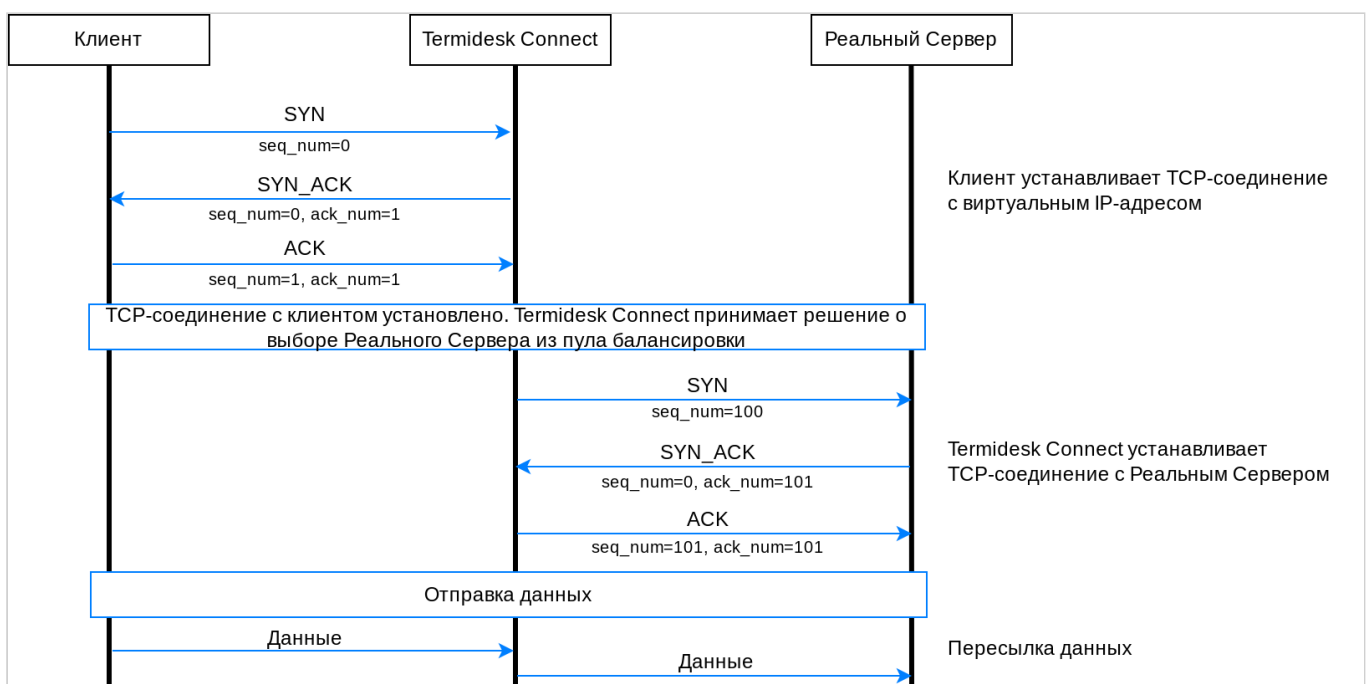


Рисунок 2 – Балансировка уровня L4 для TCP

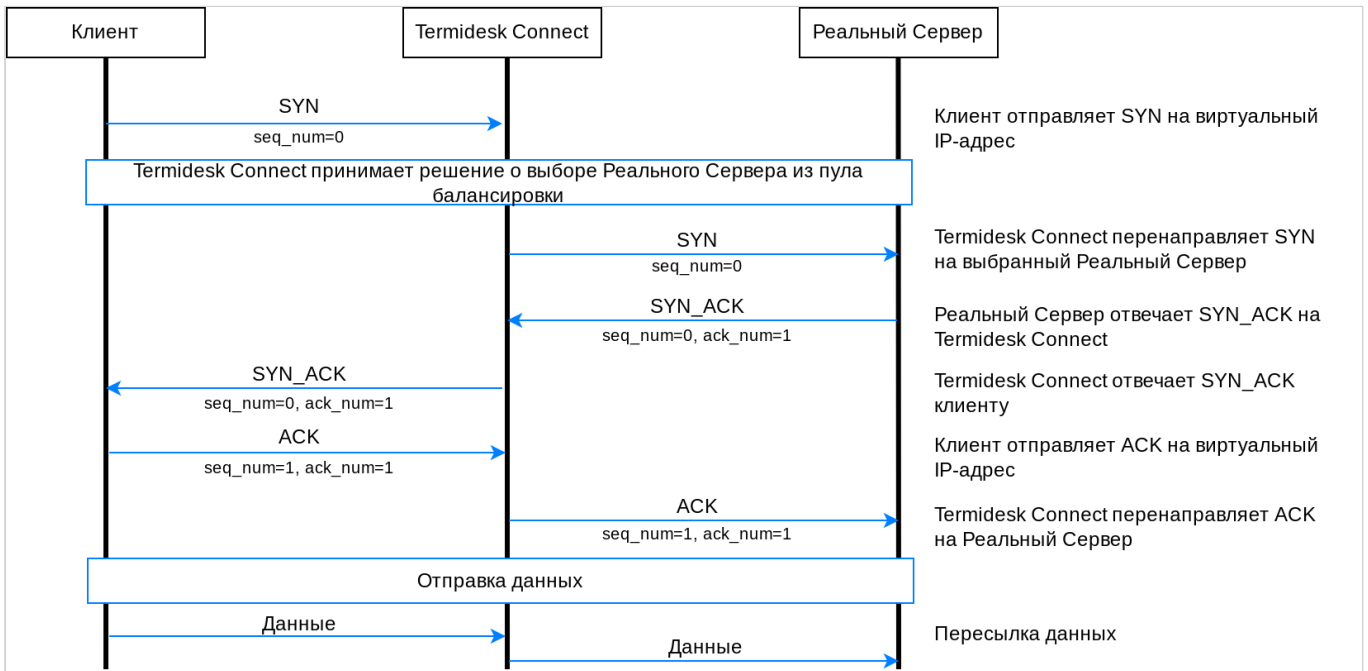


Рисунок 3 – Балансировка уровня L4 для RAPID-TCP

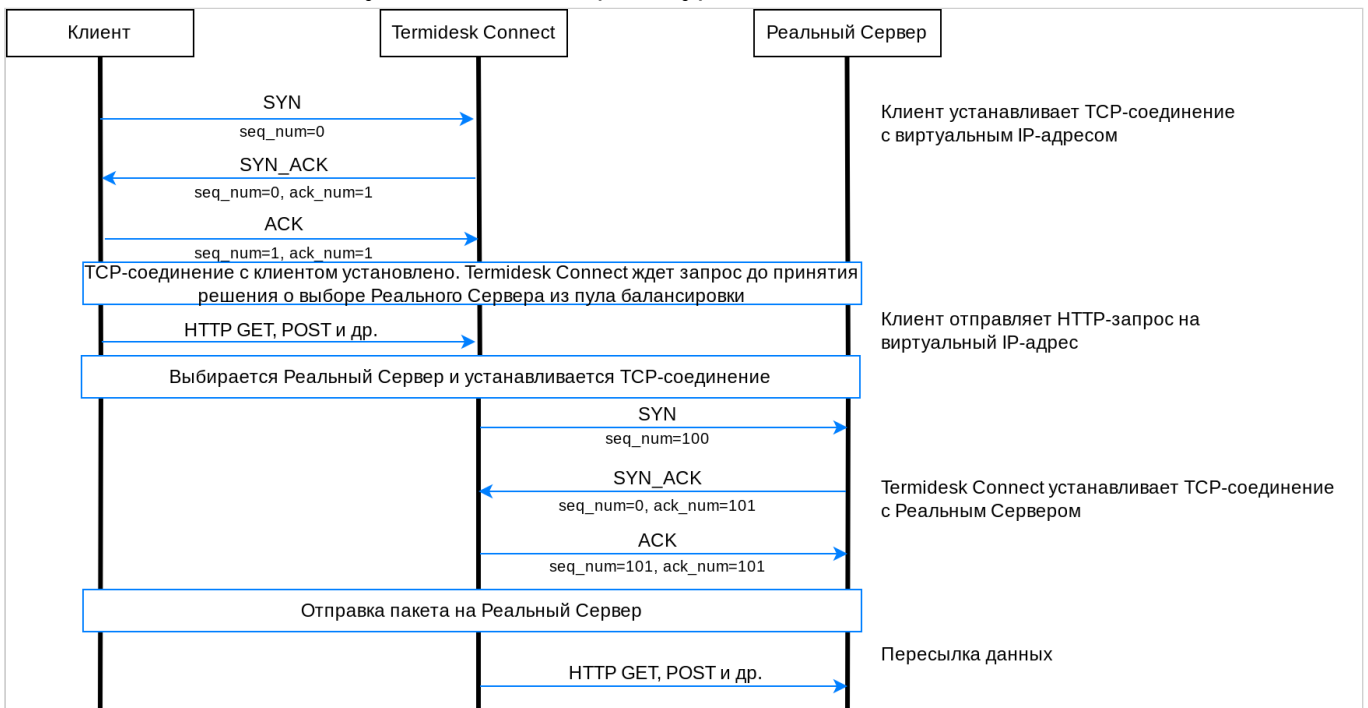


Рисунок 4 – Балансировка уровня L7

#### 4.6.2 . Создание и настройка Виртуального Сервера для балансировки по протоколу TCP

Создание и настройка Виртуального Сервера выполняется одним из способов:

- из интерфейса командной строки Termidesk Connect;
- из веб-интерфейса Termidesk Connect (см. подраздел **Добавление Виртуального Сервера**).



Для создания и настройки Виртуального Сервера для балансировки по протоколу TCP используются команды:

- создание Виртуального Сервера:

```
set vs TCP <имя>
```

**i** Описание параметров также приведено в подразделе **Команда set**.

- задание IP-адреса Виртуального Сервера:

```
set vs TCP <имя> vip ip <IP-адрес>
```

- задание порта Виртуального Сервера:

```
set vs TCP <имя> vip port <порт>
```

- задание алгоритма определения статуса Виртуального Сервера:

**i** Алгоритм определения статуса может быть:

- OR – статус Виртуального Сервера будет «В работе», если работает хотя бы один ассоциированный с ним Сервер Балансировки;
- AND – статус Виртуального Сервера будет «В работе», если работают все ассоциированные с ним Серверы Балансировки;
- NONE – не использовать никакой из алгоритмов.

```
set vs TCP <имя> check-lbs algorithm <алгоритм>
```

- задание Сервера Балансировки (можно указать несколько узлов), по состоянию которого будет определяться статус Виртуального Сервера:

**i** Статус Виртуального Сервера зависит от статуса ассоциированного с ним Сервера Балансировки. Алгоритм определения статуса задается в команде выше.

```
set vs TCP <имя> check-lbs lbs-ids <имя>
```

- задание правила выбора Сервера Балансировки:

**i** Параметр <приоритет> задает приоритет применения правила: чем ниже число, тем выше приоритет, и тем раньше правило будет обработано Виртуальным Сервером.

```
set vs TCP <имя> netrules <приоритет>
```

- задание сети источника в формате CIDR для правила:

**i** В правиле задается сеть источника запроса: в зависимости от того, из какой сети подключился пользователь, будет выбран тот или иной Сервер Балансировки.

```
set vs TCP <имя> netrules <приоритет> network <сеть/маска>
```

- задание Сервера Балансировки для правила:

```
set vs TCP <имя> netrules <приоритет> lbs-id <имя>
```

- (опционально) привязка серверного SSL-профиля к Виртуальному Серверу (см. подраздел **Создание и настройка серверного SSL-профиля**):

```
set lbs TCP <имя> ssl-profile-id <имя профиля>
```

- (опционально) привязка VRF к Виртуальному Серверу:

```
set lbs TCP <имя> vrf <имя VRF>
```

- применение заданных настроек:

```
commit
```

- сохранение настроек:

```
write
```

- просмотр заданных настроек (указывается формат вывода – XML, JSON и TXT):

```
show configuration xml vs TCP <имя>
```

- просмотр выполненных команд:

```
show configuration cli vs TCP <имя>
```

#### 4.6.3 . Создание и настройка Виртуального Сервера для балансировки по протоколу RAPID-TCP

Создание и настройка Виртуального Сервера выполняется одним из способов:

- из интерфейса командной строки Termidesk Connect;
- из веб-интерфейса Termidesk Connect (см. подраздел **Добавление Виртуального Сервера**).

Для создания и настройки Виртуального Сервера для балансировки по протоколу RAPID-TCP используются команды:

- создание Виртуального Сервера:

```
set vs RAPID-TCP <имя>
```

**i** Описание параметров также приведено в подразделе **Команда set**.

- задание IP-адреса Виртуального Сервера:

```
set vs RAPID-TCP <имя> vip ip <IP-адрес>
```

- задание порта Виртуального Сервера:

```
set vs RAPID-TCP <имя> vip port <порт>
```

- задание алгоритма определения статуса Виртуального Сервера:

**i** Алгоритм определения статуса может быть:

- OR – статус Виртуального Сервера будет «В работе», если работает хотя бы один ассоциированный с ним Сервер Балансировки;
- AND – статус Виртуального Сервера будет «В работе», если работают все ассоциированные с ним Серверы Балансировки;
- NONE – не использовать никакой из алгоритмов.

```
set vs RAPID-TCP <имя> check-lbs algorithm <алгоритм>
```

- задание Сервера Балансировки (можно указать несколько узлов), по состоянию которого будет определяться статус Виртуального Сервера:

**i** Статус Виртуального Сервера зависит от статуса ассоциированного с ним Сервера Балансировки. Алгоритм определения статуса задается в команде выше.

```
set vs RAPID-TCP <имя> check-lbs lbs-ids <имя>
```

- задание правила выбора Сервера Балансировки:

**i** Параметр <приоритет> задает приоритет применения правила: чем ниже число, тем выше приоритет, и тем раньше правило будет обработано Виртуальным Сервером.

```
set vs RAPID-TCP <имя> netrules <приоритет>
```

- задание сети источника в формате CIDR для правила:

**i** В правиле задается сеть источника запроса: в зависимости от того, из какой сети подключился пользователь, будет выбран тот или иной Сервер Балансировки.

```
set vs RAPID-TCP <имя> netrules <приоритет> network <сеть/маска>
```

- задание Сервера Балансировки для правила:

```
set vs RAPID-TCP <имя> netrules <приоритет> lbs-id <имя>
```

- (опционально) привязка VRF к Виртуальному Серверу:

```
set lbs RAPID-TCP <имя> vrf <имя VRF>
```

- применение заданных настроек:

```
commit
```

- сохранение настроек:

```
write
```

- просмотр заданных настроек (указывается формат вывода – XML, JSON и TXT):

```
show configuration xml vs RAPID-TCP <имя>
```

- просмотр выполненных команд:

```
show configuration cli vs RAPID-TCP <имя>
```

#### 4.6.4 . Создание и настройка виртуального сервера для балансировки по протоколу HTTP

Создание и настройка Виртуального Сервера выполняется одним из способов:

- из интерфейса командной строки Termidesk Connect;
- из веб-интерфейса Termidesk Connect (см. подраздел **Добавление Виртуального Сервера**).

Для создания и настройки Виртуального Сервера для балансировки по протоколу HTTP используются команды:

- создание Виртуального Сервера:

```
set vs HTTP <имя>
```

 Описание параметров также приведено в подразделе **Команда set**.

- задание IP-адреса:

```
set vs HTTP <имя> vip ip <IP-адрес>
```

- задание порта:

```
set vs HTTP <имя> vip port <порт>
```

- задание алгоритма определения статуса Виртуального Сервера:

```
set vs HTTP <имя> check-lbs algorithm <алгоритм>
```

- задание Сервера Балансировки (можно указать несколько узлов), по состоянию которого будет определяться статус Виртуального Сервера:

```
set vs HTTP <имя> check-lbs lbs-ids <имя>
```

- задание сценария исполняемого файла формата LUA:

**i** Параметр <приоритет> задает приоритет применения сценария: чем ниже число, тем выше приоритет, и тем раньше сценарий будет обработан Виртуальным Сервером.

```
set vs HTTP <имя> luarules <приоритет>
```

**i** Подробное описание работы со сценариями приведено в подразделе **Сценарии**.

- задать имя исполняемого файла формата LUA:

**!** Файл должен быть расположен в каталоге `/var/lib/tdc/lbscripts/content-switching/`.

```
set vs HTTP <имя> luarules <приоритет> script <имя файла>
```

- (опционально) привязка серверного SSL-профиля к Виртуальному Серверу (см. подраздел **Создание и настройка серверного SSL-профиля**):

```
set lbs HTTP <имя> ssl-profile-id <имя профиля>
```

- (опционально) привязка VRF к Виртуальному Серверу:

```
set lbs HTTP <имя> vrf <имя VRF>
```

- применение заданных настроек:

```
commit
```

- сохранение настроек:

```
write
```

- просмотр заданных проверок (указывается формат вывода – XML, JSON и TXT):

```
show configuration xml vs HTTP <имя>
```

- просмотр выполненных команд:

```
show configuration cli vs HTTP <имя>
```

## 5. ГЕОБАЛАНСИРОВКА

### 5.1. ADNS

#### 5.1.1. Общие сведения об ADNS

ADNS в Termidesk Connect – это объект (абстракция), позволяющий настроить Termidesk Connect в качестве авторитетного DNS-сервера. Для ADNS настраивается IP-адрес и порт для приема входящих DNS-запросов от пользователей или вышестоящих DNS-серверов.

#### 5.1.2. Создание и настройка ADNS

Создание и настройка ADNS выполняется одним из способов:

- из интерфейса командной строки Termidesk Connect;
- из веб-интерфейса Termidesk Connect (см. подраздел **ADNS**).

Для создания и настройки ADNS используются команды:

- назначение IP-адреса и порта, на котором Termidesk Connect будет принимать входящие DNS-запросы:

```
set geolb adns <IP-адрес> <порт>
```

 Описание параметров также приведено в подразделе **Команда set**.

- применение заданных настроек:

```
commit
```

- сохранение настроек:

```
write
```

### 5.2. Геолокационные IP-базы

#### 5.2.1. Общие сведения о геолокационных IP-базах

Геолокационная IP-база (GeoIP) – это база данных, содержащая информацию по пулам IP-адресов, их координатам и наименованиям локаций. Используется для определения местоположения IP-адреса пользователя: страны, города, широты, долготы и др.

В Termidesk Connect такие IP-базы используются для активации определенного алгоритма балансировки и выбора ближайшей к пользователю Площадки.

#### 5.2.2. Добавление геолокационных IP-баз

Для добавления собственной геолокационной IP-базы нужно:

- конвертировать основную геолокационную IP-базу в формат JSON, например, с помощью утилиты `mmdbctl`:

```
mmdbctl export <путь к базе .mmdb> -o <путь к новому файлу базы .json>
```

- сформировать текстовый файл (например, `geonames.txt`) для удобного поиска `geoname_id` с помощью командной строки:

```
1 jq -r '. | "(continent.geoname_id),(country.geoname_id),
(.subdivisions[0].geoname_id),(city.geoname_id),(location | "(latitude),
(longitude),(accuracy_radius))|(continent.code)|(country.names | "(ru):
(en))"|(.subdivisions[0].names | "(ru):(en))"|(.city.names | "(ru):
(en))";' exported-geoip.json | sort | uniq > geonames.txt
```

- найти необходимые географические идентификаторы в базе данных, например:

```
1 grep -i 'Тюмень' geonames.txt grep -i 'vladivos' geonames.txt sed -e '/Санкт/I!
d' -e '/rus/I!d' geonames.txt
```

**i** Идентификаторы находятся в первом столбце, если разделительный знак принять за «|». В этом же списке находятся координаты в системе WGS 84 (последние два значения), а также радиус точности местоположения в километрах. Координаты можно заменить, воспользовавшись онлайн-картой.

- сформировать файл (например, `infrastructure.txt`) с содержимым IP-адресов и их местоположений:

```
1 10.0.1.0/24,6255148,2017370,536203,498817,59.93863,30.31413,5
2 10.0.3.0/25,6255148,2017370,1488747,1488754,57.138530,65.522186,1
3 10.0.3.128/25,6255148,2017370,1488747,1488754,57.116799,65.550740,1
```

**i** Где:

- значения в столбце 1 соответствуют подсети, для которой определяется местоположение;
- далее в столбцах 2 – 5 следуют идентификаторы: континента, страны, региона, города;
- затем в столбцах 6 и 7 приводятся координаты (широта, долгота);
- в столбце 8 приводится радиус точности в километрах.

Необходимые столбцы: 1, 6, 7.

- конвертировать получившийся файл в формат MMDB с помощью исполняемого файла `writer.py`:

**!** Необходимо предварительно установить библиотеку `netaddr`:

```
sudo apt install python3-netaddr
```



```
python3 writer.py --file infrastructure.txt --output infrastructure.mmdb
```

Содержимое исполняемого файла `writer.py` приведено в справочном центре Termidesk Connect: <https://wiki.astralinux.ru/pages/viewpage.action?pageId=348179676>.

## 5.3 . DNS View

### 5.3.1 . Общие сведения о DNS View

DNS View в Termidesk Connect – это объект (абстрация), описывающий сети, при запросе из которых должен быть выдан локальный IP-адрес Сервиса (см. подраздел **Сервисы**).

DNS View может быть привязан к Виртуальному Серверу геобалансировки (см. подраздел **Геобалансировка. Виртуальные Серверы**), что позволит настроить поведение, при котором на запросы из определённой сети Сервис будет всегда отвечать локальным IP-адресом.

### 5.3.2 . Создание и настройка DNS View

Создание и настройка DNS View выполняется одним из способов:

- из интерфейса командной строки Termidesk Connect;
- из веб-интерфейса Termidesk Connect (см. подраздел **Добавление DNS View**).

Для создания и настройки DNS View используются команды:

- создание DNS View:

```
set geolb view <имя>
```

**i** Описание параметров также приведено в подразделе **Команда set**.

- задание IP-адреса сети в формате CIDR:

```
set geolb view <имя> net <сеть/маска>
```

**i** Пример команды:

```
set geolb view ViewForLocalNet net 172.16.0.0/16
```

- применение заданных настроек:

```
commit
```

- сохранение настроек:

```
write
```

## 5.4 . Сервисы

### 5.4.1 . Общие сведения о Сервисах

Сервис в Termidesk Connect – это объект (абстракция) с назначенным IP-адресом, доступ к которому нужно предоставить пользователю в рамках геобалансировки. IP-адрес, заданный в Сервисе, помещается в DNS-ответ.

Можно задать два типа IP-адреса:

- общедоступный – IP-адрес назначается Сервису всегда, соответственно в DNS-ответах он будет помещаться всегда;
- локальный – IP-адрес назначается Сервису только в тех случаях, когда нужно обеспечить его функционирование также во внутренней сети организации.

В случае, если назначены оба IP-адреса:

- если к Сервису запросил доступ внешний пользователь, то в DNS-ответ будет помещен общедоступный IP-адрес;
- если к Сервису запросил доступ внутренний пользователь, сеть которого попадает в DNS View (см. подраздел **DNS View**), то в DNS-ответ будет помещен локальный IP-адрес.

### 5.4.2 . Создание и настройка Сервиса

Создание и настройка Сервиса выполняется одним из способов:

- из интерфейса командной строки Termidesk Connect;
- из веб-интерфейса Termidesk Connect (см. подраздел **Добавление Сервисов**).

Для создания и настройки Сервиса используются команды:

- создание Сервиса:

```
set geolb service <имя>
```

**i** Описание параметров также приведено в подразделе **Команда set**.

- (опционально) задание проверки, которая будет выполняться для Сервиса:

**i** Используются те же проверки, которые были заданы для управления трафиком (см. подраздел **Проверки**).

```
set geolb service <имя> hc-id <имя>
```

- (опционально) задание локального IP-адреса Сервиса:

**i** Для работы функционала DNS View (см. подраздел **DNS View**) задание IP-адреса обязательно.

```
set geolb service <имя> local-ip <IP-адрес>
```

- задание общедоступного IP-адреса Сервиса:

```
set geolb service <имя> public-ip <IP-адрес>
```

- (опционально) задание веса Сервиса:

**i** Вес определяет приоритет Сервиса и устанавливается в диапазоне от 0 до 255, параметр необходим при балансировке с использованием алгоритма ROUNDROBIN. Чем больше вес Сервиса, тем чаще на этот Сервис идет перенаправление входящих подключений.

```
set geolb service <имя> weight <значение>
```

- применение заданных настроек:

```
commit
```

- сохранение настроек:

```
write
```

- просмотр заданных настроек (указывается формат вывода – XML, JSON и TXT):

```
show configuration xml geolb service <имя>
```

- просмотр выполненных команд:

```
show configuration cli geolb service <имя>
```

## 5.5 . Геобалансировка. Виртуальные Серверы

### 5.5.1 . Общие сведения о Виртуальных Серверах геобалансировки

Виртуальные серверы геобалансировки в Termidesk Connect – это объект (абстракция), описывающий алгоритмы балансировки, по которым будут выдаваться IP-адреса Сервисов в DNS-ответах.

### 5.5.2 . Создание и настройка Виртуальных Серверов геобалансировки

Создание и настройка Виртуального Сервера геобалансировки выполняется одним из способов:

- из интерфейса командной строки Termidesk Connect;
- из веб-интерфейса Termidesk Connect (см. подраздел **Добавление Виртуальных Серверов геобалансировки**).

Для создания и настройки Виртуального Сервера геобалансировки используются команды:

- создание Виртуального Сервера геобалансировки:

```
set geolb vs <имя>
```

**i** Описание параметров также приведено в подразделе **Команда set**.

- задание алгоритма геобалансировки:

**i** Могут быть заданы алгоритмы:

- ONLINE – Виртуальный Сервер включит в DNS-ответ все доступные (прошедшие проверку) IP-адреса;
- ROUNDROBIN – Виртуальный Сервер последовательно распределит подключения между Сервисами для их равномерного распределения;
- SOURCEIPHASH – Виртуальный Сервер будет перенаправлять подключения к Сервисам, основываясь на значении хеша IP-адреса. Это гарантирует, что подключение одного пользователя всегда будет направляться на один и тот же Сервис, снижая вероятность перегрузки;
- STATICPROXIMITY – Виртуальный Сервер перенаправит подключения на ближайшую Площадку для выдачи Сервиса. В этом случае учитывается местоположение исходного источника запроса (см. подраздел **Геолокационные IP-базы**).

```
set geolb vs <имя> algorithm <алгоритм>
```

- управление опцией `esc` (EDNS Client Subnet), может принимать значения ON (включена) или OFF (выключена):

**i** Опция `esc` используется для хранения информации о сети исходного источника запроса. Это полезно в случае, когда запрос пришел от вышестоящего DNS-сервера, местоположение которого точно неизвестно. Termidesk Connect получит информацию о сети исходного источника из входящего DNS-запроса и сохранит ее.

```
set geolb vs <имя> esc <значение>
```

- задание типа привязки входящего подключения к одному Сервису на время обработки его DNS-запросов:

**i** Параметру могут быть заданы значения:

- OFF – привязка к Сервису отключена;
- SRCIP – привязка входящего подключения к Сервису на основе его IP-адреса.

```
set geolb vs <имя> persistence <значение>
```

- задание привязки Сервиса к Виртуальному Серверу геобалансировки:

```
set geolb vs <имя> service-ids <имя>
```

- задание привязки DNS View к Виртуальному Серверу геобалансировки:

**i** Привязка DNS View к Виртуальному Серверу геобалансировки позволит настроить поведение, при котором на запросы из определённой сети Сервис будет всегда отвечать локальным IP-адресом (см. подраздел **Сервисы**).

```
set geolb vs <имя> view-id <имя>
```

- применение заданных настроек:

```
commit
```

- сохранение настроек:

```
write
```

- просмотр заданных (указывается формат вывода – XML, JSON и TXT):

```
show configuration xml geolb vs <имя>
```

- просмотр выполненных команд:

```
show configuration cli geolb vs <имя>
```

## 5.6 . Зоны

### 5.6.1 . Общие сведения о Зонах

Зоны в Termidesk Connect – это объект, описывающий доменные имена, для которых обеспечивается геобалансировка подключений.

### 5.6.2 . Создание и настройка Зоны

Создание и настройка Зоны выполняется одним из способов:

- из интерфейса командной строки Termidesk Connect;
- из веб-интерфейса Termidesk Connect (см. подраздел **Добавление Зоны**).

Для создания и настройки Зоны используются команды:

- создание Зоны:

```
set geolb zone <имя домена>
```

❗ Описание параметров также приведено в подразделе **Команда set**.

- задание поддомена для указанного домена:

❗ В командах с опцией `nodes` используется символ «.» для указания корневого домена. Для применения настроек домена третьего уровня нужно вместо точки использовать имя поддомена.

Пример задания поддомена `connect` для домена `connect.termidesk.ru`:

```
set geolb zone termidesk.ru nodes connect
```

```
set geolb zone <имя домена> nodes .
```

- задание TTL для создаваемой зоны:

```
set geolb zone <имя домена> nodes . ttl <значение>
```

- задание порядкового номера Виртуального Сервера, который будет использоваться для работы с доменом (значения указываются в порядке возрастания):

```
set geolb zone <имя домена> nodes . vs <значение>
```

- задание Виртуального Сервера для указанного порядкового номера `vs`:

❗ Можно указать несколько Виртуальных Серверов в Зоне для домена. Обработка запросов будет осуществляться в порядке возрастания порядкового номера Виртуального Сервера, указанного в параметре `vs`.

```
set geolb zone <имя домена> nodes . vs <значение> vs-id <имя>
```

- применение заданных настроек:

```
commit
```

- сохранение настроек:

```
write
```

- просмотр заданных настроек (указывается формат вывода – XML, JSON и TXT):

```
show configuration xml geolb zone <имя домена>
```

- просмотр выполненных команд:

```
show configuration cli geolb zone <имя домена>
```

## 6. ИНТЕРФЕЙС РАСШИРЕННОГО МЕНЮ TERMIDESK CONNECT

### 6.1 . Общие сведения по работе с интерфейсом расширенного меню

Интерфейс расширенного меню предназначен для настройки и управления Termidesk Connect и предоставляет базовый набор функций для работы с Termidesk Connect после его запуска.

Переход в интерфейс расширенного меню выполняется клавишей **<F2>** из главного меню Termidesk Connect. Для перехода потребуется ввести текущий пароль администратора (по умолчанию после установки – `tdadmin`).

### 6.2 . Смена пароля администратора

После установки Termidesk Connect по умолчанию используется логин `tdadmin` с паролем `tdadmin` для доступа к ряду функций управления.

Для смены пароля:

- в главном меню Termidesk Connect нажать клавишу **<F2>**, ввести текущий пароль администратора;
- далее выбрать пункт «Пароль» и нажать клавишу **<ENTER>**;
- в появившемся окне (см. Рисунок 5) ввести текущий пароль и нажать экранную кнопку **[OK]**;
- затем (см. Рисунок 6) ввести новый пароль, переключиться на строку «Повтор пароля» при помощи клавиши **<↓>** (**<СТРЕЛКА ВНИЗ>**) и повторить ввод пароля. Подтвердить данные, нажав экранную кнопку **[OK]**.

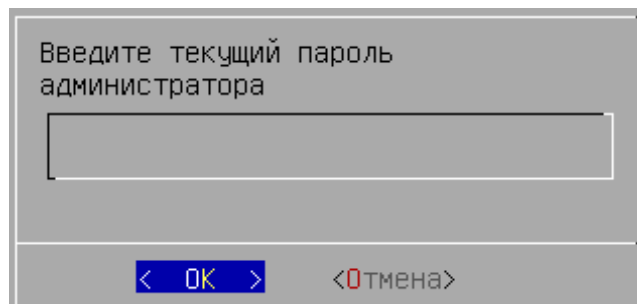


Рисунок 5 – Ввод текущего пароля администратора

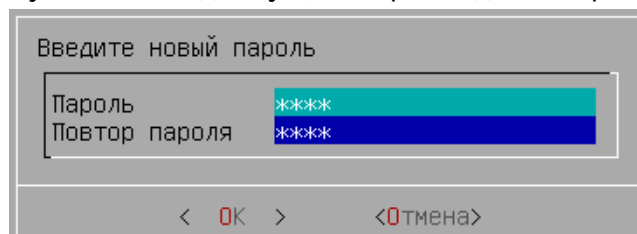


Рисунок 6 – Ввод нового пароля администратора

### 6.3 . Перезагрузка

Для перезагрузки Termidesk Connect:



- в главном меню Termidesk Connect нажать клавишу **<F2>**, ввести текущий пароль администратора;
- далее выбрать пункт «Перезагрузка» и нажать клавишу **<ENTER>**;
- подтвердить действие, нажав экранную кнопку **[Да]**.

#### 6.4 . Выключение

Для завершения работы Termidesk Connect и выключения ВМ:

- в главном меню Termidesk Connect нажать клавишу **<F2>**, ввести текущий пароль администратора;
- далее выбрать пункт «Выключение» и нажать клавишу **<ENTER>**;
- подтвердить действие (см. Рисунок 7), нажав экранную кнопку **[Да]**.

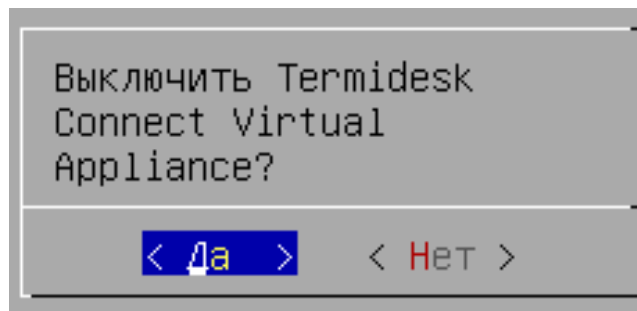


Рисунок 7 – Подтверждение выключения Termidesk Connect

#### 6.5 . Переход в интерфейс командной строки

Для перехода в интерфейс командной строки:

- в главном меню Termidesk Connect нажать клавишу **<F2>**, ввести текущий пароль администратора;
- далее выбрать пункт «CLI» и нажать клавишу **<ENTER>**;
- отобразится строка приглашения `vatc #`, свидетельствующая об успешном переходе в интерфейс командной строки.

## 7. ИНТЕРФЕЙС CLI TERMIDESK CONNECT

### 7.1 . Общие сведения по работе с CLI

CLI предназначен для настройки и управления Termidesk Connect и предоставляет набор команд с возможностью их автоматического дополнения.

 CLI является основным способом настройки Termidesk Connect.

Переход в CLI осуществляется из главного меню Termidesk (см. подраздел **Переход в интерфейс командной строки**).

Для просмотра списка доступных команд или просмотра справки по ним можно воспользоваться клавишами:

- **<ТАВ>** - выводит возможные варианты продолжения команды:
  - если вариантов больше одного, то выводит список доступных опций;
  - если вариант один, то автоматически дописывает окончание команды;
- **<?>** - выводит список доступных команд с краткой справкой к ним. Ввод клавиши не будет отображен в CLI.

### 7.2 . Команда `bash`

Выполняет переход в стандартный интерфейс командной строки Linux Shell.

Для некоторых команд, выполняемых через стандартный интерфейс командной строки Linux Shell требуется повышение привилегий. В этом случае следует вызвать команду через `sudo` и ввести текущий пароль администратора:

```
sudo <команда>
```

Для того чтобы вернуться в интерфейс CLI Termidesk Connect, нужно выполнить в Linux Shell:

```
exit
```

### 7.3 . Команда `clear`

Очищает CLI от результатов выполнения предыдущих команд.

### 7.4 . Команда `commit`

Применяет изменения, сделанные в предварительной конфигурации, в рабочую конфигурацию. Без сохранения (команда `write`) изменения сбросятся после перезагрузки Termidesk Connect.

### 7.5 . Команда `debug`

Устанавливает уровень отладки и вывода отладочной информации. Позволяет включать или отключать отладочные сообщения, что полезно для диагностики и анализа работы системы.

Формат:

```
debug <подсистема> <уровень>
```

Доступные подсистемы для отладки приведены в таблице (см. Таблица 10).

Таблица 10 – Доступные подсистемы

Подсистема	Описание
backend	Подсистема настройки и управления внутренней конфигурацией Termidesk Connect
cli	Подсистема интерфейса командной строки
restconf	Подсистема интерфейса управления, основанного на протоколе REST

Доступные уровни отладки приведены в таблице (см. Таблица 11).

Таблица 11 – Доступные уровни отладки

Уровень	Описание
0	Отладочный режим отключен. Отладочные сообщения выводиться не будут
1	Вывод минимальных отладочных сообщений
2 и выше	Чем выше уровень, тем больше подробностей отображается в отладочных сообщениях

## 7.6 . Команда delete

Удаляет существующие объекты или их параметры из конфигурации (изменения попадают в предварительную конфигурацию).

Формат:

```
delete <объект> <параметр> <значение>
```

Доступные для удаления объекты приведены в таблице.

Таблица 12 – Доступные для удаления объекты

Объект	Описание
all	Вся рабочая конфигурация. Не требует указания параметров объекта, поскольку удаляет все параметры. Пример команды: <pre>delete all</pre>
geolb	Конфигурация, описывающая настройку геораспределенной балансировки
ha	Конфигурация, описывающая настройку в отказоустойчивом (высокодоступном) исполнении Termidesk Connect
health-check	Конфигурация, описывающая настройку проверок
interfaces	Конфигурация, описывающая настройку сетевых интерфейсов
ip	Конфигурация, описывающая настройку IP-адресов
ipset	Конфигурация, описывающая настройку IP-фондов

Объект	Описание
lbs	Конфигурация, описывающая настройку Серверов Балансировки
nacm	Конфигурация, описывающая настройку протокола NETCONF
restconf	Конфигурация, описывающая настройку протокола RESTCONF
rs-pool	Конфигурация, описывающая настройку группы Реальных Серверов
ssl-profile	Конфигурация, описывающая настройку SSL-профилей для функционала SSL Offload
system	Конфигурация, описывающая системные настройки
user	Конфигурация, описывающая настройку пользователей
vlan	Конфигурация, описывающая настройку VLAN
vrf	Конфигурация, описывающая настройку VRF
vs	Конфигурация, описывающая настройку Виртуальных Серверов

### 7.7 . Команда discard

Отменяет несохраненные изменения предварительной конфигурации и возвращает ее к состоянию, соответствующему текущей рабочей конфигурации.

### 7.8 . Команда load

Загружает конфигурацию из XML-файла в предварительную конфигурацию.

Формат:

```
load <XML-файл> <действие>
```

Доступные действия приведены в таблице (см. Таблица 13).

Таблица 13 – Доступные действия для команды load

Действие	Описание
merge	Объединяет параметры из указанного файла с текущей предварительной конфигурацией. Если объекты из файла совпадают с уже существующими, то они будут обновлены. Если какие-то объекты отсутствуют, то они будут добавлены
replace	Заменяет текущую предварительную конфигурацию параметрами из указанного файла. Все существующие в конфигурации объекты и параметры будут удалены перед загрузкой новых

### 7.9 . Команда mode

Выбирает поддерево конфигурации.

### 7.10 . Команда quit

Выполняет выход из CLI и переход в расширенное меню Termidesk Connect (см. раздел **Интерфейс расширенного меню Termidesk Connect**).

### 7.11 . Команда save

Сохраняет текущую предварительную конфигурацию Termidesk Connect в XML-файл.

Формат:

```
save <XML-файл>
```

Чтобы позже загрузить сохраненную конфигурацию из файла используется команда load (см. подраздел **Команда load**).

### 7.12 . Команда set

#### 7.12.1 . Общие сведения по команде set

Устанавливает новый объект в конфигурации. Команда позволяет как создать объект без параметров, так и создать объект и назначить ему параметры одной командой.

Формат:

```
set <объект>
```

или

```
set <объект> <параметр объекта> <ключ> <значение>
```

Доступные для создания объекты приведены в таблице (см. Таблица 14).

Таблица 14 – Доступные объекты для команды set


Объект	Описание
geolb	Конфигурация, описывающая настройку геораспределенной балансировки
ha	Конфигурация, описывающая настройку в отказоустойчивом (высокодоступном) исполнении Termidesk Connect
health-check	Конфигурация, описывающая настройку проверок
interfaces	Конфигурация, описывающая настройку сетевых интерфейсов
ip	Конфигурация, описывающая настройку IP-адресов
ipset	Конфигурация, описывающая настройку IP-фондов
lbs	Конфигурация, описывающая настройку Серверов Балансировки
nacm	Конфигурация, описывающая настройку протокола NETCONF
restconf	Конфигурация, описывающая настройку протокола RESTCONF
rs-pools	Конфигурация, описывающая настройку группы Реальных Серверов
ssl-profile	Конфигурация, описывающая настройку SSL-профилей для функционала SSL Offload
system	Конфигурация, описывающая системные настройки
user	Конфигурация, описывающая настройку пользователей
vlan	Конфигурация, описывающая настройку VLAN

Объект	Описание
vrf	Конфигурация, описывающая настройку VRF
vs	Конфигурация, описывающая настройку Виртуальных Серверов

### 7.12.2 . Объект geolb

Доступные команды объекта geolb приведены в таблице (см. Таблица 15).

Таблица 15 – Доступные команды объекта geolb

Команда	Описание
set geolb adns <IP-адрес> <порт>	Создание конфигурации ADNS-сервера. Пример команды: <pre>set geolb adns ip 192.168.1.1 53</pre>
set geolb geodb <имя>	Указание файла геолокационной IP-базы
set geolb service <имя> <параметр> <значение>	Создание конфигурации Сервиса с определенными значениями параметров. Параметром может быть: <ul style="list-style-type: none"> <li>▪ hc-id – проверка, относящаяся к геораспределенной балансировке;</li> <li>▪ local-ip – внутренний IP-адрес Сервиса;</li> <li>▪ public-ip – внешний IP-адрес Сервиса;</li> <li>▪ site – Площадка;</li> <li>▪ weight – вес Сервиса</li> </ul>
set geolb site <имя>	<div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 5px;">  Функциональность команды в разработке и приведена для ознакомления.                     </div> Создание конфигурации удаленной Площадки
set geolb view <имя> <сеть>	Создание конфигурации DNS View. Параметр <сеть> задается в формате CIDR. Пример команды: <pre>set geolb view ViewForLocalNet net 172.16.0.0/16</pre>

Команда	Описание
set geolb vs <имя> <параметр> <значение>	Создание конфигурации Виртуального Сервера геобалансировки. Параметром может быть: <ul style="list-style-type: none"> <li>▪ algorithm – алгоритм выбора Виртуального Сервера;</li> <li>▪ ecs – использование опции EDNS Client Subnet;</li> <li>▪ persistence – использование привязки сессии пользователя;</li> <li>▪ service-ids – привязка Виртуального Сервера к Сервису;</li> <li>▪ view-id – привязка Виртуального Сервера к идентификатору DNS View.</li> </ul> Для параметра algorithm могут устанавливаться следующие значения: <ul style="list-style-type: none"> <li>▪ ONLINE – Виртуальный Сервер перенаправит подключения только на доступные Сервисы;</li> <li>▪ ROUNDROBIN – Виртуальный Сервер последовательно распределит подключения между Сервисами для их равномерного распределения;</li> <li>▪ SOURCEIPHASH – Виртуальный Сервер будет перенаправлять подключения к Сервисам, основываясь на значении хеша IP-адреса. Это гарантирует, что подключение одного пользователя всегда будет направляться на один и тот же Сервис, снижая вероятность перегрузки;</li> <li>▪ STATICPROXIMITY – Виртуальный Сервер перенаправит подключения на ближайшую Площадку для выдачи Сервиса. В этом случае учитывается местоположение исходного источника запроса (см. подраздел <b>Геолокационные IP-базы</b>).</li> </ul> Для параметра ecs могут устанавливаться значения ON (включен) или OFF (отключен). Опция ecs используется для хранения информации о сети исходного источника запроса. Это полезно в случае, когда запрос пришел от вышестоящего DNS-сервера, местоположение которого точно неизвестно. Termidesk Connect получит информацию о сети исходного источника из входящего DNS-запроса и сохранит ее. Для параметра persistence могут устанавливаться следующие значения: <ul style="list-style-type: none"> <li>▪ OFF – привязка входящего подключения к Сервису отключена;</li> <li>▪ SRCIP – привязка входящего подключения к Сервису на основе его IP-адреса</li> </ul>
set geolb zone <имя домена> <параметр> <значение>	Создание конфигурации сетевой зоны. Параметр может принимать значение nodes, который является частью географически распределенной балансировки нагрузки для конкретного домена

### 7.12.3. Объект ha

Доступные команды объекта ha приведены в таблице (см. Таблица 16).

Таблица 16 – Доступные команды объекта ha

Команда	Описание
set ha	Создание отказоустойчивой (высокодоступной) конфигурации со значениями по умолчанию
set ha interval <значение>	Задание интервала (в миллисекундах) периодических запросов. Интервал должен быть одинаковым на всех устройствах. Значение по умолчанию: 1000
set ha ip <IP-адрес>	Указание IP-адресов, используемых для взаимодействия. Выбранные IP-адреса должны соответствовать типу «ha-type LOCAL»
set ha port <порт>	Задание UDP-порта, используемого для взаимодействия. Значение по умолчанию: 322

Команда	Описание
<code>set ha priority 1</code>	Задание приоритета устройства. Возможные значения: <ul style="list-style-type: none"> <li>0 («Active») – устройство является мастер-узлом и обрабатывает трафик пользователей в настоящий момент;</li> <li>1 («Standby») – устройство является резервным узлом и в настоящий момент не обрабатывает трафик пользователей</li> </ul>
<code>set ha remote &lt;имя устройства&gt;</code>	Задание имени соседнего устройства, участвующему в отказоустойчивой (высокодоступной) конфигурации. Имя может быть любым
<code>set ha remote &lt;имя устройства&gt; &lt;параметр&gt; &lt;значение&gt;</code>	Задание параметров подключения к соседнему устройству, участвующему в отказоустойчивой (высокодоступной) конфигурации. Параметром может быть: <ul style="list-style-type: none"> <li><code>ip</code> – IP-адрес соседнего устройства;</li> <li><code>port</code> – порт соседнего устройства;</li> <li><code>priority</code> – приоритет соседнего устройства;</li> <li><code>seckey</code> – пароль пользователя соседнего устройства</li> </ul>

#### 7.12.4. Объект health-check

Доступные команды объекта health-check приведены в таблице (см. Таблица 17).

Таблица 17 – Доступные команды объекта health-check

Команда	Описание
<code>set health-check id &lt;имя&gt;</code>	Создание проверки
<code>set health-check id &lt;имя&gt; &lt;тип&gt; &lt;параметр&gt; &lt;значение&gt;</code>	Настройка проверки. Тип указывает на использование определенного протокола проверки, может быть: <ul style="list-style-type: none"> <li>ICMP – ICMP-проверка;</li> <li>TCP – TCP-проверка.</li> </ul> Для ICMP могут устанавливаться параметры: <ul style="list-style-type: none"> <li><code>interval</code> – время (в секундах), через которое будут отправляться запросы;</li> <li><code>source-ip</code> – IP-адрес источника, с которого отправляются запросы;</li> <li><code>success-try</code> – количество успешных попыток, необходимых для проверки;</li> <li><code>target-ip</code> – IP-адрес цели, к которой будут отправляться запросы;</li> <li><code>timeout</code> – время ожидания ответа (в секундах) ответа на запрос;</li> <li><code>try</code> – количество повторных проверок в случае отсутствия ответа.</li> </ul> Для TCP могут устанавливаться параметры, аналогичные ICMP, включая параметр <code>target-port</code> : <ul style="list-style-type: none"> <li><code>target-port</code> – порт, на который будет отправлен запрос</li> </ul>

#### 7.12.5. Объект interfaces

Доступные команды объекта interfaces приведены в таблице (см. Таблица 18).




 Объект `interfaces` определяет конфигурацию сетевых интерфейсов Termidesk Connect. Сетевой интерфейс появляется в списке доступных в объекте `interfaces` автоматически после загрузки Termidesk Connect.



Таблица 18 – Доступные команды объекта interfaces

Команда	Описание
set interfaces interface <имя интерфейса> description <описание>	Добавление текстового описания сетевому интерфейсу
set interfaces interface <имя интерфейса> ethernet arp <false/true>	<div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 5px;">  Функциональность команды в разработке и приведена для ознакомления.                 </div> Активация или отключение протокола ARP для сетевого интерфейса
set interfaces interface <имя интерфейса> type <значение>	<div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 5px;">  Тип интерфейса определяется автоматически после загрузки Termidesk Connect. Не рекомендуется вручную изменять его.                 </div> Тип интерфейса

### 7.12.6 . Объект ip

Доступные команды объекта ip приведены в таблице (см. Таблица 19).


Таблица 19 – Доступные команды объекта ip

Команда	Описание
set ip address <IP-адрес> <префикс сети>	Добавление IP-адреса в формате CIDR
set ip address <IP-адрес> <префикс сети> i f-ethernet <имя интерфейса>	Назначение IP-адреса существующему сетевому интерфейсу
set ip address <IP-адрес> <префикс сети> ha-type <тип>	Назначение режима использования IP-адреса при отказоустойчивой конфигурации, где <тип> может быть: <ul style="list-style-type: none"> <li>▪ LOCAL – IP-адрес используется в локальной конфигурации, не синхронизируется для отказоустойчивой конфигурации;</li> <li>▪ SHARED – IP-адрес синхронизируется для отказоустойчивой конфигурации</li> </ul>
set ip address <IP-адрес> <префикс сети> i f-vlan <имя>	Назначение IP-адреса существующему интерфейсу VLAN
set ip route <имя VRF> <сеть/маска> <IP-адрес шлюза>	Создание маршрута. По умолчанию существует VRF default – создание маршрута по умолчанию

### 7.12.7 . Объект ipset

Доступные команды объекта ipset приведены в таблице (см. Таблица 20).

Таблица 20 – Доступные команды объекта ipset

Команда	Описание
set ipset id <имя>	<div style="border: 1px solid #ffc107; padding: 5px; margin-bottom: 5px;">  Имя создаваемого объекта не должно содержать дефисов, нижнее подчеркивание использовать разрешено.                 </div> Создание IP-фонда с IP-адресами
set ipset id <имя> ips <IP-адреса>	Добавление в IP-фонд IP-адресов

Команда	Описание
set ipset id <имя> vrf <имя VRF>	Добавление в IP-фонд VRF. По умолчанию существует VRF default

### 7.12.8 . Объект lbs

Доступные команды объекта lbs приведены в таблице (см. Таблица 21).

Таблица 21 – Доступные команды объекта lbs

Команда	Описание
set lbs TCP <имя>	Создание Сервера Балансировки для протокола TCP
set lbs TCP <имя> <параметр> <значение>	<p>Настройка Сервера Балансировки для протокола TCP.</p> <p>Параметром может быть:</p> <ul style="list-style-type: none"> <li>▪ algorithm – алгоритм балансировки;</li> <li>▪ leastconn-param starttime– время (в секундах) смены алгоритма с LEASTCONN на ROUNDROBIN во время изменений в группе Реальных Серверов;</li> <li>▪ min-rs – минимальное количество действующих Реальных Серверов, необходимых для обработки запросов;</li> <li>▪ persistence – параметр, определяющий постоянство подключения пользователя к Реальному Серверу;</li> <li>▪ rs-pool-id – группа Реальных Серверов, к которой будет привязан Сервер Балансировки;</li> <li>▪ ssl-profile-id – клиентский SSL-профиль, который будет использоваться для функционала SSL Offload.</li> </ul> <p>Для параметра algorithm могут устанавливаться следующие значения:</p> <ul style="list-style-type: none"> <li>▪ ROUNDROBIN – подключения пользователей в этом случае распределяются последовательно между Реальными Серверами, что обеспечивает их равномерное распределение;</li> <li>▪ LEASTCONN – подключения пользователей в этом случае распределяются оптимизировано, с учетом количества текущих активных соединений на каждом Реальном Сервере. Для подключения пользователя выбирается Реальный Сервер с наименьшим количеством текущих активных соединений, что обеспечивает более равномерное распределение нагрузки и помогает избежать перегрузки отдельных Реальных Серверов.</li> </ul> <p>Для параметра persistence могут устанавливаться следующие дополнительные параметры:</p> <ul style="list-style-type: none"> <li>▪ algorithm – алгоритм привязки пользователя к Реальному Серверу. Может принимать значения:               <ul style="list-style-type: none"> <li>• IPSOURCE – привязка по IP-адресу источника запроса, т.е. IP-адресу пользователя;</li> <li>• NONE – привязка не используется;</li> </ul> </li> <li>▪ ipsource-param timeout – время ожидания (в секундах), в течение которого повторное подключение пользователя будет направлено на ранее выбранный Реальный Сервер</li> </ul>
set lbs RAPID-TCP <имя>	Создание Сервера Балансировки для протокола RAPID TCP

Команда	Описание
set lbs RAPID-TCP <имя> <параметр> <значение>	<p>Настройка Сервера Балансировки для протокола RAPID TCP.</p> <p>Параметром может быть:</p> <ul style="list-style-type: none"> <li>▪ algorithm – алгоритм балансировки;</li> <li>▪ leastconn-param starttime– время (в секундах) смены алгоритма с LEASTCONN на ROUNDROBIN во время изменений в группе Реальных Серверов;</li> <li>▪ min-rs – минимальное количество действующих Реальных Серверов, необходимых для обработки запросов;</li> <li>▪ persistence – параметр, определяющий постоянство подключения пользователя к Реальному Серверу;</li> <li>▪ rs-pool-id – группа Реальных Серверов, к которой будет привязан Сервер Балансировки;</li> <li>▪ connection-idle – время жизни сессии (в секундах) при бездействии (отсутствии пакетов);</li> <li>▪ fin-timeout – время жизни сессии (в секундах) после получения управляющего флага FIN в заголовке пакета;</li> <li>▪ use-cip – управление режимом подмены IP-адреса клиента.</li> </ul> <p>Для параметра algorithm могут устанавливаться следующие значения:</p> <ul style="list-style-type: none"> <li>▪ ROUNDROBIN – подключения пользователей в этом случае распределяются последовательно между Реальными Серверами, что обеспечивает их равномерное распределение;</li> <li>▪ LEASTCONN – подключения пользователей в этом случае распределяются оптимизировано, с учетом количества текущих активных соединений на каждом Реальном Сервере. Для подключения пользователя выбирается Реальный Сервер с наименьшим количеством текущих активных соединений, что обеспечивает более равномерное распределение нагрузки и помогает избежать перегрузки отдельных Реальных Серверов.</li> </ul> <p>Для параметра persistence могут устанавливаться следующие дополнительные параметры:</p> <ul style="list-style-type: none"> <li>▪ algorithm – алгоритм привязки пользователя к Реальному Серверу. Может принимать значения:                             <ul style="list-style-type: none"> <li>• IPSOURCE – привязка по IP-адресу источника запроса, т.е. IP-адресу пользователя;</li> <li>• NONE – привязка не используется;</li> </ul> </li> <li>▪ ipsource-param timeout – время ожидания (в секундах), в течение которого повторное подключение пользователя будет направлено на ранее выбранный Реальный Сервер;</li> <li>▪ ipsource-param ipset-src-persist – управление режимом сохранения IP-адреса из IP-фонда для взаимодействия с Реальным Сервером</li> </ul>

### 7.12.9 . Объект nasm

Доступные команды объекта nasm приведены в таблице (см. Таблица 22).

Таблица 22 – Доступные команды объекта nasm

Команда	Описание
set nasm	Создание конфигурации NETCONF со значениями по умолчанию

Команда	Описание
set nasm <параметр> <значение>	Настройка конфигурации NETCONF. Параметром может быть: <ul style="list-style-type: none"> <li>▪ enable-external-groups – управление поддержкой внешних групп пользователей;</li> <li>▪ enable-nasm – проверка активации контроля доступа;</li> <li>▪ exec-default – управлением действием по умолчанию для выполнения команд, если явное правило отсутствует;</li> <li>▪ groups – назначение списка групп пользователю;</li> <li>▪ read-default – управление доступом к чтению данных, если явное правило отсутствует;</li> <li>▪ rule-list – управление списком правил контроля доступа;</li> <li>▪ write-default – управление доступом к записи данных, если явное правило отсутствует</li> </ul>

### 7.12.10 . Объект restconf

Доступные команды объекта restconf приведены в таблице (см. Таблица 23).

Таблица 23 – Доступные команды объекта restconf

Команда	Описание
set restconf	Создание конфигурации RESTCONF со значениями по умолчанию
set restconf auth-type <тип>	Назначение типа аутентификации, где <тип> может принимать значения: <ul style="list-style-type: none"> <li>▪ client-certificate – тип аутентификации с использованием клиентского сертификата для идентификации пользователя;</li> <li>▪ none – аутентификация не используется;</li> <li>▪ user – тип аутентификации с использованием имени пользователя и пароля для доступа к API</li> </ul>
set restconf debug <значение>	Управление отладкой и мониторингом работы RESTCONF, где <debug> – уровень детализации отладочных сообщений, может принимать значения: <ul style="list-style-type: none"> <li>▪ 0 – отключение отладки (по умолчанию);</li> <li>▪ 1 – базовая информация о работе системы и основных событиях;</li> <li>▪ 2 – более подробная информация, включая некоторые внутренние события и предупреждения;</li> <li>▪ 3 – полная отладочная информация, включая детализированные логи о внутреннем состоянии, вызовах функций и т.п.</li> </ul>
set restconf enable <false/true>	Управление режимом RESTCONF
set restconf enable-core-dump <false/true>	Управление режимом создания снимка (дампа) состояния памяти ядра
set restconf log-destination <тип>	Указание формата записи журнала, где <тип> может принимать значения: <ul style="list-style-type: none"> <li>▪ syslog – запись в службу syslog;</li> <li>▪ file – запись в файл</li> </ul>
set restconf pretty <false/true>	Управление режимом форматирования заголовков в формате XML или JSON
set restconf server-ca-cert-path <путь>	Указание файла сертификата корневого удостоверяющего центра (CA)
set restconf server-cert-path	Указание файла сертификата сервера

Команда	Описание
set restconf server-key-path	Указание закрытого ключа, который соответствует сертификату сервера
set restconf socket <идентификатор> <IP-адрес> <порт>	Настройка соединения к API в программном пространстве: <ul style="list-style-type: none"> <li>▪ &lt;идентификатор&gt; – уникальный идентификатор, который определяет область применения API;</li> <li>▪ &lt;IP_адрес&gt; – IP-адрес сервера, на котором располагается API;</li> <li>▪ &lt;Порт&gt; – номер порта, через который осуществляется доступ к API на указанном сервере.</li> </ul> Пример команды: <pre style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;">set restconf socket default 127.0.0.1 8080</pre>

### 7.12.11 . Объект ssl-profile

Доступные команды объекта ssl-profile приведены в таблице (см. Таблица 24).

Таблица 24 – Доступные команды объекта ssl-profile

Команда	Описание
set ssl-profile server <имя>	Создание серверного SSL-профиля для функционала SSL Offload. Серверный SSL-профиль определяет взаимодействие между пользователем и Termidesk Connect, где Termidesk Connect является сервером

Команда	Описание
<pre>set ssl-profile server &lt;имя&gt; &lt;параметр&gt; &lt;значение&gt;</pre>	<p>Настройка серверного SSL-профиля для функционала SSL Offload.</p> <p>Параметром может быть:</p> <ul style="list-style-type: none"> <li>▪ <code>handshake-timeout</code> – время ожидания (в секундах) установления соединения;</li> <li>▪ <code>host</code> – значения поля SNI из TLS Hello, для которого требуются особые настройки обработки;</li> <li>▪ <code>setting-default</code> – конфигурация по умолчанию. Используется, если пришедший SNI пуст, либо не соответствует SNI, указанному в параметре <code>host</code>.</li> </ul> <p>Для определения конфигурации, которая должна использоваться для SNI из параметра <code>host</code>, применяются параметры:</p> <ul style="list-style-type: none"> <li>▪ <code>ca-cert</code> – список центров сертификации для проверки подлинности. Используется, если активирована взаимная аутентификация по протоколу mTLS;</li> <li>▪ <code>cert</code> – файл сертификата сервера для аутентификации;</li> <li>▪ <code>ciphers</code> – список используемых алгоритмов преобразований. Полный перечень приведен после таблицы;</li> <li>▪ <code>dh-params</code> – файл с ключами Диффи-Хеллмана;</li> <li>▪ <code>key</code> – файл закрытого ключа, соответствующий сертификату сервера;</li> <li>▪ <code>mtls</code> – управление режимом взаимной аутентификации по протоколу mTLS. Значение может быть:                         <ul style="list-style-type: none"> <li>• <code>true</code> (также можно <code>enable</code>) – взаимная аутентификация включена;</li> <li>• <code>false</code> (также можно <code>disable</code>) – взаимная аутентификация отключена;</li> </ul> </li> <li>▪ <code>password</code> – пароль к файлу закрытого ключа, если он необходим;</li> <li>▪ <code>versions</code> – версии протокола TLS, которые должны поддерживаться при установлении соединения.</li> </ul> <p>Для параметра <code>versions</code> могут устанавливаться следующие значения:</p> <ul style="list-style-type: none"> <li>▪ <code>ssl-v3</code> – не рекомендуется использовать из-за уязвимостей;</li> <li>▪ <code>tls-v1</code> – первая версия TLS, которая улучшает безопасность по сравнению с SSLv3, но также содержит некоторые уязвимости;</li> <li>▪ <code>tls-v11</code> – улучшенная версия TLS 1.0, которая исправляет некоторые недостатки, но все еще считается устаревшей;</li> <li>▪ <code>tls-v12</code> – широко используемая версия, обеспечивающая улучшенные механизмы шифрования и безопасности;</li> <li>▪ <code>tls-v13</code> – последняя версия протокола TLS, предлагающая значительные улучшения в производительности и безопасности</li> </ul>
<pre>set ssl-profile client &lt;имя&gt;</pre>	<p>Создание клиентского SSL-профиля для функционала SSL Offload. Клиентский SSL-профиль определяет взаимодействие между Termidesk Connect и Реальным Сервером, где Termidesk Connect является клиентом.</p>

Команда	Описание
<pre>set ssl-profile client &lt;имя&gt; &lt;параметр&gt; &lt;значение&gt;</pre>	<p>Настройка клиентского SSL-профиля для функционала SSL Offload.</p> <p>Параметром может быть:</p> <ul style="list-style-type: none"> <li>▪ <code>ca-cert</code> – список центров сертификации для проверки подлинности. Используется, если активирована взаимная аутентификация по протоколу mTLS;</li> <li>▪ <code>cert</code> – файл клиентского сертификата для аутентификации Termidesk Connect на Реальном Сервере. Используется, если активирована взаимная аутентификация по протоколу mTLS;</li> <li>▪ <code>ciphers</code> – список используемых алгоритмов преобразования. Полный перечень приведен после таблицы;</li> <li>▪ <code>dh-params</code> – файл с ключами Диффи-Хеллмана;</li> <li>▪ <code>handshake-timeout</code> – время ожидания (в секундах) установления соединения;</li> <li>▪ <code>key</code> – файл закрытого ключа для аутентификации Termidesk Connect и Реального Сервера. Используется, если активирована взаимная аутентификация по протоколу mTLS;</li> <li>▪ <code>password</code> – пароль к файлу закрытого ключа, если он необходим;</li> <li>▪ <code>sni-default</code> – значение по умолчанию для SNI;</li> <li>▪ <code>versions</code> – версии протокола TLS, которые должны поддерживаться при установлении соединения.</li> </ul> <p>Для параметра <code>versions</code> могут устанавливаться следующие значения:</p> <ul style="list-style-type: none"> <li>▪ <code>ssl-v3</code> – не рекомендуется использовать из-за уязвимостей;</li> <li>▪ <code>tls-v1</code> – первая версия TLS, которая улучшает безопасность по сравнению с SSLv3, но также содержит некоторые уязвимости;</li> <li>▪ <code>tls-v11</code> – улучшенная версия TLS 1.0, которая исправляет некоторые недостатки, но все еще считается устаревшей;</li> <li>▪ <code>tls-v12</code> – широко используемая версия, обеспечивающая улучшенные механизмы шифрования и безопасности;</li> <li>▪ <code>tls-v13</code> – последняя версия протокола TLS, предлагающая значительные улучшения в производительности и безопасности</li> </ul>

**❗** Список поддерживаемых алгоритмов преобразования для параметра `ciphers`:

- AES128-GCM-SHA256;
- AES256-GCM-SHA384;
- AES128-SHA AES256-SHA;
- AES128-SHA256;
- AES256-SHA256;
- DHE-PSK-AES128-CBC-SHA;
- DHE-PSK-AES128-CBC-SHA256;
- DHE-PSK-AES128-GCM-SHA256;
- DHE-PSK-AES256-CBC-SHA;
- DHE-PSK-AES256-CBC-SHA384;
- DHE-PSK-AES256-GCM-SHA384;
- DHE-PSK-CHACHA20-POLY1305;
- DHE-RSA-AES128-GCM-SHA256;

- DHE-RSA-AES128-SHA;
- DHE-RSA-AES128-SHA256;
- DHE-RSA-AES256-GCM-SHA384;
- DHE-RSA-AES256-SHA;
- DHE-RSA-AES256-SHA256;
- DHE-RSA-CHACHA20-POLY1305;
- ECDHE-ECDSA-AES128-GCM-SHA256;
- ECDHE-ECDSA-AES128-SHA;
- ECDHE-ECDSA-AES128-SHA256;
- ECDHE-ECDSA-AES256-GCM-SHA384;
- ECDHE-ECDSA-AES256-SHA;
- ECDHE-ECDSA-AES256-SHA384;
- ECDHE-ECDSA-CHACHA20-POLY1305;
- ECDHE-PSK-AES128-CBC-SHA;
- ECDHE-PSK-AES128-CBC-SHA256;
- ECDHE-PSK-AES256-CBC-SHA;
- ECDHE-PSK-AES256-CBC-SHA384;
- ECDHE-PSK-CHACHA20-POLY1305;
- ECDHE-RSA-AES128-GCM-SHA256;
- ECDHE-RSA-AES128-SHA;
- ECDHE-RSA-AES128-SHA256;
- ECDHE-RSA-AES256-GCM-SHA384;
- ECDHE-RSA-AES256-SHA;
- ECDHE-RSA-AES256-SHA384;
- ECDHE-RSA-CHACHA20-POLY1305;
- GOST2001-GOST89-GOST89;
- GOST2012-GOST8912-GOST8912;
- PSK-AES128-CBC-SHA;
- PSK-AES128-CBC-SHA256;
- PSK-AES128-GCM-SHA256;
- PSK-AES256-CBC-SHA;
- PSK-AES256-CBC-SHA384;
- PSK-AES256-GCM-SHA384;
- PSK-CHACHA20-POLY1305;
- RSA-PSK-AES128-CBC-SHA;
- RSA-PSK-AES128-CBC-SHA256;




- RSA-PSK-AES128-GCM-SHA256;
- RSA-PSK-AES256-CBC-SHA;
- RSA-PSK-CHACHA20-POLY1305;
- SRP-RSA-AES-128-CBC-SHA;
- TLS\_AES\_256\_GCM\_SHA384;
- SRP-RSA-AES-256-CBC-SHA;
- TLS\_CHACHA20\_POLY1305\_SHA256;
- SRP-AES-256-CBC-SHA;
- RSA-PSK-AES256-CBC-SHA384;
- SRP-AES-128-CBC-SHA;
- RSA-PSK-AES256-GCM-SHA384;
- TLS\_AES\_128\_GCM\_SHA256.

### 7.12.12 . Объект rs-pool

Доступные команды объекта rs-pool приведены в таблице (см. Таблица 25).

Таблица 25 – Доступные команды объекта rs-pool

Команда	Описание
set rs-pool id <имя>	<div style="border: 1px solid yellow; padding: 5px; margin-bottom: 5px;">  Имя создаваемого объекта не должно содержать дефисов, нижнее подчеркивание использовать разрешено.                 </div> Создание группы Реальных Серверов
set rs-pool id <имя> <параметр> <значение>	Настройка группы Реальных Серверов. Параметром может быть: <ul style="list-style-type: none"> <li>▪ hc-id – проверка, которая будет использоваться для группы Реальных Серверов;</li> <li>▪ ipset-id – IP-фонд;</li> <li>▪ rs – узел Реального Сервера (с его IP-адресом и портом), для привязки к группе Реальных Серверов. Может быть задано несколько узлов</li> </ul>

### 7.12.13 . Объект system

Доступные команды объекта system приведены в таблице (см. Таблица 26).

Таблица 26 – Доступные команды объекта system

Команда	Описание
set system hostname <имя>	Назначение имени хоста
set system mgmt ip <IP-адрес>	Назначение IP-адреса из списка заданных адресов, на котором будет доступен интерфейс управления
set system mgmt ip webui-port <порт>	Назначение порта, на котором будет доступен веб-интерфейс Termidesk Connect
set system timezone <часовой пояс>	Назначение часового пояса из списка доступных

### 7.12.14 . Объект user

Доступные команды объекта user приведены в таблице (см. Таблица 27).

Таблица 27 – Доступные команды объекта user

Команда	Описание
set user <имя>	Создание пользователя
set user <имя> <параметр> <значение>	Настройка пользователя. Параметром может быть: <ul style="list-style-type: none"> <li>▪ password – пароль пользователя;</li> <li>▪ role – функция пользователя. Может быть:                             <ul style="list-style-type: none"> <li>• user (по умолчанию);</li> <li>• admin</li> </ul> </li> </ul>

### 7.12.15 . Объект vlan

Доступные команды объекта vlan приведены в таблице (см. Таблица 28).

Таблица 28 – Доступные команды объекта vlan

Команда	Описание
set vlan name <имя>	Создание VLAN
set vlan name <имя> vlan-id <идентификатор>	Назначение идентификатора VLAN
set vlan name <имя> if-ethernet <имя интерфейса>	Назначение VLAN сетевому интерфейсу (физическому)
set vlan name <имя> vrf <имя VRF>	Назначение VRF для VLAN
set vlan name <имя> ha-type <тип>	Назначение режима использования VLAN при отказоустойчивой конфигурации, где <тип> может быть: <ul style="list-style-type: none"> <li>▪ LOCAL – VLAN используется в локальной конфигурации, не синхронизируется для отказоустойчивой конфигурации;</li> <li>▪ SHARED – VLAN синхронизируется для отказоустойчивой конфигурации</li> </ul>

### 7.12.16 . Объект vrf

Доступные команды объекта vrf приведены в таблице (см. Таблица 29).


Таблица 29 – Доступные команды объекта vrf

Команда	Описание
set vrf name <имя>	Создание VRF
set vrf name <имя> table-id <номер таблицы>	Назначение идентификатора таблицы маршрутизации, которая будет ассоциирована с этим VRF. Номер таблицы должен быть уникальным
set vrf name <имя> ha-type <тип>	Назначение режима использования VRF при отказоустойчивой конфигурации, где <тип> может быть: <ul style="list-style-type: none"> <li>▪ LOCAL – VRF используется в локальной конфигурации, не синхронизируется для отказоустойчивой конфигурации;</li> <li>▪ SHARED – VRF синхронизируется для отказоустойчивой конфигурации</li> </ul>

### 7.12.17 . Объект vs

Доступные команды объекта vs приведены в таблице (см. Таблица 30).

Таблица 30 – Доступные команды объекта vs

Команда	Описание
set vs HTTP <имя>	Создание Виртуального Сервера для балансировки по протоколу HTTP
set vs HTTP <имя> <параметр> <значение>	<p>Настройка Виртуального Сервера для балансировки по протоколу HTTP.</p> <p>Параметром может быть:</p> <ul style="list-style-type: none"> <li>▪ check-lbs – настройка проверки доступности Серверов Балансировки;</li> <li>▪ luarules – настройка применения исполняемых файлов формата LUA, которые определяют правила обработки трафика, проходящего через Виртуальный Сервер;</li> </ul> <div style="border: 1px solid #ccc; padding: 5px; margin: 10px 0;"> <p> Описание работы со сценариями приведено в подразделе <b>Сценарии</b>.</p> </div> <ul style="list-style-type: none"> <li>▪ ssl-profile-id – серверный SSL-профиль, который будет использоваться для соединений;</li> <li>▪ vip – IP-адрес и порт, который будет присвоен Виртуальному Серверу;</li> <li>▪ vrf – имя VRF для привязки к Виртуальному Серверу.</li> </ul> <p>Для параметра check-lbs устанавливаются следующие дополнительные параметры:</p> <ul style="list-style-type: none"> <li>▪ algorithm – алгоритм определения статуса Виртуального Сервера. Может принимать значения:                             <ul style="list-style-type: none"> <li>• OR – статус Виртуального Сервера будет «В работе», если работает хотя бы один ассоциированный с ним Сервер Балансировки;</li> <li>• AND – статус Виртуального Сервера будет «В работе», если работают все ассоциированные с ним Серверы Балансировки;</li> <li>• NONE – не использовать никакой из алгоритмов;</li> </ul> </li> <li>▪ lbs-ids – Серверы Балансировки, влияющие на статус Виртуального Сервера. Статус Виртуального Сервера зависит от статуса ассоциированного с ним Сервера Балансировки</li> </ul>
set vs TCP <имя>	Создание Виртуального Сервера для балансировки по протоколу TCP
set vs TCP <имя> <параметр> <значение>	<p>Настройка Виртуального Сервера для балансировки по протоколу TCP.</p> <p>Параметры идентичны команде выше, за исключением luarules (не применимо для Виртуального Сервера уровня L4).</p> <p>Вместо него задается параметр netrules – настройки применения правил на основе сети источника. Для параметра указывается:</p> <ul style="list-style-type: none"> <li>▪ &lt;приоритет&gt; – приоритет применения правила: чем ниже число, тем выше приоритет, и тем раньше правило будет обработано Виртуальным Сервером;</li> <li>▪ &lt;сеть/маска&gt; – сеть источника запроса. В зависимости от того, из какой сети подключился пользователь, будет выбран тот или иной Сервер Балансировки;</li> <li>▪ lbs-id – Сервер Балансировки для правила.</li> </ul> <p>Пример команды для параметра netrules:</p> <div style="border: 1px solid #ccc; padding: 5px; margin: 10px 0;"> <pre>set vs TCP VSName netrules 10 network 0.0.0.0/0</pre> </div>

Команда	Описание
set vs RAPID-TCP <имя>	Настройка Виртуального Сервера для балансировки по протоколу RAPID TCP
set vs RAPID-TCP <имя> <параметр> <значение>	Настройка Виртуального Сервера для балансировки по протоколу RAPID TCP. Параметры идентичны команде выше, за исключением ssl-profile-id (не задается для RAPID TCP)

### 7.13 . Команда show

Отображает различные параметры Termidesk Connect: конфигурацию, состояние, версию и др.

Формат:

```
show <опция> <параметры>
```

Доступные опции приведены в таблице (см. Таблица 31).

Таблица 31 – Доступные объекты команды show

Опция	Описание
configuration	Вывод рабочей конфигурации Termidesk Connect. Может также использоваться вывод конкретного элемента или параметра рабочей конфигурации в определенном формате: <pre>show configuration &lt;формат&gt; &lt;параметр&gt;</pre> Формат может быть: <ul style="list-style-type: none"> <li>▪ cli – вывод будет представлен командами CLI;</li> <li>▪ json – вывод будет представлен в формате JSON;</li> <li>▪ netconf – вывод будет представлен в формате операций протокола управления конфигурациями сетевых устройств NETCONF;</li> <li>▪ text – вывод будет представлен простым текстом;</li> <li>▪ xml – вывод будет представлен в формате XML</li> </ul>
difference	Вывод различий между предварительной и рабочей конфигурациями
status	Вывод состояния объектов
version	Вывод информации о версии Termidesk Connect

### 7.14 . Команда top

Возвращает в корень дерева конфигурации. Обычно используется, если конфигурация редактируется через команду mode (см. подраздел **Команда mode**), для удобства навигации по элементам конфигурации.

### 7.15 . Команда up

Возвращает на уровень выше в дереве конфигурации. Обычно используется, если конфигурация редактируется через команду mode (см. подраздел **Команда mode**), для удобства навигации по элементам конфигурации.

### 7.16 . Команда validate

Проверяет корректность изменений в предварительной конфигурации.

**7.17 . Команда write**

Сохраняет сделанные изменения конфигурации. Команда необходима для сохранения изменений после перезагрузки Termidesk Connect.

## 8. ВЕБ-ИНТЕРФЕЙС TERMIDESK CONNECT

### 8.1 . Доступ к веб-интерфейсу Termidesk Connect

Доступ к веб-интерфейсу управления Termidesk Connect осуществляется из веб-браузера по протоколу HTTPS с указанием URL-адреса: `https://<IP-адрес>:<порт>`.

Для доступа к веб-интерфейсу по протоколу HTTPS на этапе установки в автоматически генерируется самоподписанный сертификат и закрытый ключ к нему. IP-адрес и порт, на котором будет доступен веб-интерфейс, задается при первоначальной настройке Termidesk Connect (см. подраздел **Первоначальная настройка Termidesk Connect**).

Для подключения должны использоваться веб-браузеры с поддержкой спецификации W3C HTML5: Яндекс.Браузер версии 15.9 и выше, Google Chrome версии 46 и выше, Mozilla Firefox версии 41 и выше.

Минимально необходимое разрешение экрана монитора для работы с веб-интерфейсом - 1366x768 пикселей.

На странице подключения нужно заполнить экранные поля:

- «Логин» - идентификатор субъекта с ролью «Администратор»;
- «Пароль» - набор символов, подтверждающий назначение полномочий.

По умолчанию после установки используется логин `tdadmin` с паролем `tdadmin`.

### 8.2 . Обзор доступных функций веб-интерфейса

Веб-интерфейс Termidesk Connect позволяет администратору выполнить ряд задач по настройке и управлению, а именно:

- отслеживать статистику производительности, доступности узлов и сетевой активности Termidesk Connect;
- выполнять настройки системы, управлять трафиком, балансировкой запросов, задавать сценарии работы узлов.

Сразу после авторизации в левой части веб-интерфейса администратору доступна панель, содержащая список основных функций, перечисленных в таблице (см. Таблица 32).

В правой верхней части веб-интерфейса доступна возможность сохранить текущую конфигурацию Termidesk Connect. Для этого следует нажать экранную кнопку **[Сохранить]**.

Параметры конфигурации будут сохранены в БД Termidesk Connect. Для применения параметров конфигурации следует выполнить перезапуск Termidesk Connect.

Таблица 32 – Описание разделов веб-интерфейса

Наименование раздела или функции	Описание
«Главная»	Предоставляет сведения о нагрузке на узел, пропускной способности узла, сетевой активности и доступности узлов сетевой инфраструктуры
«Настройки»	Предоставляет доступ к параметрам конфигурирования Termidesk Connect
«Система»	Предоставляет доступ к настройкам системных параметров
«Лицензия»	Предоставляет возможность ознакомления с лицензионным соглашением
«Сеть»	Задаёт параметры для маршрутизации и взаимодействия узлов в IP-сетях для интеграции Termidesk Connect в существующую сеть организации
«Обновление»	Позволяет выполнить обновление Termidesk Connect на новую версию
«Управление трафиком»	Предоставляет доступ к настройкам локальной балансировки подключений, управления доступом и проверки доступности реальных серверов
«Проверки»	Задаёт параметры периодических проверок доступности реальных серверов для балансировки подключений
«Реальные серверы»	Задаёт адреса и порты узлов с опубликованными приложениями, а также параметры проверки их доступности
«Серверы балансировки»	Определяет логику распределения подключений между группой реальных серверов
«TLS»	Позволяет настроить параметры для функционала SSL Offload
«Файлы»	Позволяет загружать файлы закрытого ключа и публичного сертификата для защищенного соединения по протоколу TLS
«Профили»	Позволяет задавать настройки SSL-профилей для управления параметрами обработки TLS-соединений
«Сценарии»	Задаёт параметры обработки запросов с использованием файлов сценария, которые определяют логику взаимодействия с реальными серверами и маршрутизации трафика
«Виртуальные серверы»	Определяет правила обработки пользовательских запросов и их последующую передачу на сервер балансировки в соответствии с заданными настройками
«ГеоБН»	Предоставляет доступ к настройкам геораспределенной балансировки подключений, позволяющим перенаправлять пользовательские запросы на наиболее подходящий ЦОД с учетом текущих параметров доступности и производительности узлов на основе DNS-запросов
«ADNS»	Задаёт настройку Termidesk Connect в качестве ADNS-сервера
«Площадки»	Задаёт имена логических групп серверов или ЦОД, которые используются в геораспределенной балансировке
«DNS View»	Задаёт настройку сетей, для запросов из которых будет выдаваться локальный IP-адрес, настроенный в сервисах
«Сервисы»	Задаёт настройку общедоступного и локального IP-адреса, который будет помещаться в DNS-ответы

Наименование раздела или функции	Описание
«Виртуальные серверы»	Определяет правила балансировки, по которым в DNS-ответах будут выдаваться IP-адреса сервисов
«Зоны»	Задаёт настройку DNS-зоны, для которой будет применяться балансировка
«Документация»	Содержит ссылку на актуальную документацию Termidesk Connect
«Настройка языка»	Определяет язык отображения элементов веб-интерфейса
«Выход из системы»	Завершает текущую сессию пользователя в веб-интерфейсе и возвращает экран авторизации

### 8.3 . Работа с панелью управления и мониторинга

Для просмотра панели управления и мониторинга в левой части веб-интерфейса нужно нажать экранную кнопку **[Главная]**.

В графических блоках панели управления и мониторинга визуализируется краткое представление следующей статистики:

- «Uptime» – отображает время непрерывной работы Termidesk Connect с момента последнего запуска или перезагрузки;
- «Доступность» – отображает сведения о количестве и статусе доступности следующих узлов:
  - «Виртуальные серверы» – количество и статус доступности виртуальных серверов;
- «Ресурсы» – отображает сведения о нагрузке на аппаратные компоненты узла:
  - «ЦП» – процент загруженности центрального процессора;
  - «ОЗУ» – процент загруженности оперативной памяти.

### 8.4 . Функция «Система»

#### 8.4.1 . Лицензионное соглашение

Для просмотра Лицензионного соглашения следует перейти «Настройки – Система – Лицензия».

#### 8.4.2 . Параметры сети

##### 8.4.2.1 . Сеть. Общие сведения

Раздел «Сеть» предназначен для настройки сетевых параметров, обеспечивающих корректную маршрутизацию и взаимодействие узлов в IP-сетях.

Раздел предоставляет доступ к настройке следующих сетевых параметров:

- «VRF» – позволяет создавать виртуальные таблицы маршрутизации для изоляции сетевого трафика и разделения маршрутов между различными сетевыми сегментами;
- «Интерфейсы» – позволяет управлять физическими и виртуальными сетевыми интерфейсами, включая их параметры и привязку к VLAN;
- «VLAN» – позволяет сегментировать сеть на виртуальные локальные сети для изоляции трафика между группами устройств, подключенными к одной физической сети;



- «IP» – позволяет управлять IP-адресами, связанными с интерфейсами;
- «Маршруты» – позволяет задавать статические маршруты для управления передачей данных между сетевыми сегментами;
- «Фонды IP» – используется для управления пулами IP-адресов, которые могут быть назначены устройствам или интерфейсам.

#### 8.4.2.2 . Добавление VRF

Для отображения списка VRF следует перейти «Настройки – Система – Сеть – VRF».

По умолчанию записи представлены в табличном виде и упорядочены согласно столбцу «Имя».

Основные параметры списка приведены в таблице (см. Таблица 33).

Таблица 33 – Основные параметры списка VRF

Параметр	Описание
«Имя»	Наименование VRF
«Номер таблицы»	Идентификатор VRF

Для добавления VRF следует перейти «Настройки – Система – Сеть – VRF» и нажать экранную кнопку **[Добавить]**.

Затем заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. Таблица 34).

Таблица 34 – Данные для добавления VRF

Параметр	Описание
«Имя»	Наименование VRF
«Номер таблицы»	Идентификатор VRF
«Локальный»	Определяет режим использования VRF в отказоустойчивой конфигурации. При активации параметра используется только локальная конфигурация. Отключение параметра позволяет синхронизировать конфигурацию между устройствами

#### 8.4.2.3 . Просмотр списка сетевых интерфейсов

Для отображения списка сетевых интерфейсов следует перейти «Настройки – Система – Сеть – Интерфейсы».

По умолчанию записи представлены в табличном виде и упорядочены согласно столбцу «Имя».

Основные параметры списка приведены в таблице (см. Таблица 35).

Таблица 35 – Основные параметры списка сетевых интерфейсов

Параметр	Описание
«Имя»	Наименование сетевого интерфейса

#### 8.4.2.4 . Добавление VLAN

Для отображения списка VLAN следует перейти «Настройки – Система – Сеть – VLAN».

По умолчанию записи представлены в табличном виде и упорядочены согласно столбцу «ID».

Основные параметры списка приведены в таблице (см. Таблица 36).

Таблица 36 – Основные параметры списка VLAN

Параметр	Описание
«ID»	Идентификатор VLAN
«Имя»	Наименование VLAN
«Интерфейс»	Наименование сетевого интерфейса, которому назначен VLAN
«VRF»	Наименование VRF, которой назначен VLAN

Для добавления VLAN следует перейти «Настройки – Система – Сеть – VLAN» и нажать экранную кнопку **[Добавить]**.

Затем заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. Таблица 37).

Таблица 37 – Данные для добавления VLAN

Параметр	Описание
«Имя»	Наименование VLAN
«ID»	Идентификатор VLAN
«Интерфейс»	Выбор сетевого интерфейса, которому будет назначен VLAN
«Локальный»	Определяет режим использования VLAN в отказоустойчивой конфигурации. При активации параметра используется только локальная конфигурация. Отключение параметра позволяет синхронизировать конфигурацию между устройствами
«VRF»	Выбор VRF, которой будет назначен VLAN

#### 8.4.2.5 . Добавление IP-адресации

Для отображения списка IP-адресов следует перейти «Настройки – Система – Сеть – IP».

По умолчанию записи представлены табличном виде и упорядочены согласно столбцу «Адрес».

Основные параметры списка приведены в таблице (см. Таблица 38).

Таблица 38 – Основные параметры списка IP-адресов

Параметр	Описание
«Адрес»	IP-адрес, который назначен интерфейсу
«Префикс»	Размер подсети в формате CIDR
«Интерфейс»	Сетевой интерфейс, которому назначен IP-адрес

Для добавления IP-адреса следует перейти «Настройки – Система – Сеть – IP» и нажать экранную кнопку **[Добавить]**.

Затем заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. Таблица 39).

Таблица 39 – Данные для добавления IP-адреса

Параметр	Описание
«Адрес»	IP-адрес, который будет назначен интерфейсу

Параметр	Описание
«Префикс»	Размер подсети в формате CIDR
«Интерфейс»	Выбор сетевого интерфейса, которому будет назначен IP-адрес
«Локальный»	Определяет режим использования IP-адреса в отказоустойчивой конфигурации. При активации параметра используется только локальная конфигурация. Отключение параметра позволяет синхронизировать конфигурацию между устройствами

#### 8.4.2.6 . Добавление параметров маршрутизации

Для отображения списка параметров маршрутизации следует перейти «Настройки – Система – Сеть – Маршруты».

По умолчанию записи представлены в табличном виде и упорядочены согласно столбцу «Сеть». Основные параметры списка приведены в таблице (см. Таблица 40).

Таблица 40 – Основные параметры списка параметров маршрутизации

Параметр	Описание
«Сеть»	Адрес и маска сети назначения в формате CIDR
«Адрес шлюза»	IP-адрес шлюза, через который будет выполнена маршрутизация
«VRF»	Наименование VRF, назначенного маршруту

Для добавления параметров маршрутизации следует перейти «Настройки – Система – Сеть – Маршруты» и нажать экранную кнопку **[Добавить]**.

Затем заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. Таблица 41).

Таблица 41 – Данные для добавления параметров маршрутизации

Параметр	Описание
«Сеть»	Адрес и маска сети назначения в формате CIDR
«Адрес шлюза»	IP-адрес шлюза, через который будет выполнена маршрутизация
«VRF»	Выбор VRF для добавления маршрута

#### 8.4.2.7 . Добавление IP-фондов

Для отображения списка IP-фондов следует перейти «Настройки – Система – Сеть – Фонды IP».

По умолчанию записи представлены в табличном виде и упорядочены согласно столбцу «Имя». Основные параметры списка приведены в таблице (см. Таблица 42).

Таблица 42 – Основные параметры списка IP-фондов

Параметр	Описание
«Имя»	Наименование IP-фонда

Для добавления IP-фонда следует перейти «Настройки – Система – Сеть – Фонды IP» и нажать экранную кнопку **[Добавить]**.

Затем заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. Таблица 43).

Таблица 43 – Данные для добавления IP-фонда

Параметр	Описание
«Имя»	Наименование IP-фонда
«VRF»	Выбор VRF для добавления списка IP-адресов
«IP адреса»	Список IP-адресов, которым будет разрешено устанавливать соединение с Реальным Сервером. Над списком IP-адресов можно выполнять следующие действия: <ul style="list-style-type: none"> <li>▪ добавить, для этого нажать экранную кнопку <b>[+]</b> и указать соответствующий IP-адрес в открывшемся поле;</li> <li>▪ удалить, для этого выбрать нужные IP-адреса в списке и нажать экранную кнопку <b>[-]</b></li> </ul>

### 8.4.3 . Обновление

Для обновления Termidesk Connect следует перейти «Настройки – Система – Обновление», нажать экранную кнопку **[Загрузить]** и указать путь к файлу обновления в формате .img.

## 8.5 . Функция «Управление трафиком»

### 8.5.1 . Добавление проверки

Для отображения списка проверок следует перейти «Настройки – Управление трафиком – Проверки».

По умолчанию записи представлены табличном виде и упорядочены согласно столбцу «Имя».

Основные параметры списка приведены в таблице (см. Таблица 44).

Таблица 44 – Основные параметры списка проверок

Параметр	Описание
«Имя»	Наименование проверки
«Тип»	Метод проверки доступности узла. Возможные значения: <ul style="list-style-type: none"> <li>▪ «TCP»;</li> <li>▪ «ICMP»</li> </ul>

Для добавления проверки следует перейти «Настройки – Управление трафиком – Проверки» и нажать экранную кнопку **[Добавить]**.

Затем заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. Таблица 45).

Таблица 45 – Данные для добавления проверки доступности сервера

Параметр	Описание
«Имя»	Наименование проверки

Параметр	Описание
«Тип»	Выбор метода проверки доступности узла. Возможные значения: <ul style="list-style-type: none"> <li>▪ «ТСР» – проверяет доступность узла, выполняя попытку подключения к указанному ТСР-порту;</li> <li>▪ «ICMP» – выполняет проверку доступности узла с помощью ICMP-запросов (ping)</li> </ul>
«Интервал, с»	Период (в секундах) между проверками доступности узла. Значение по умолчанию: «10»
«Время ожидания ответа, с»	Время (в секундах) ожидания ответа от узла при проверке его доступности. Значение по умолчанию: «5»
«Кол-во попыток, шт»	Максимальное количество проверок состояния узла, необходимых для признания его недоступным. Значение по умолчанию: «1»
«Успешное кол-во попыток, шт»	Минимальное количество успешных проверок состояния узла, необходимых для признания его доступным. Значение по умолчанию: «1»
«IP источника запроса»	IP-адрес, с которого инициируется запрос или устанавливается соединение
«IP назначения»	IP-адрес назначения, к которому будет направлен запрос или установлено соединение. Если сервис на указанном IP-адресе недоступен, этот адрес исключается из списка балансировки
«Порт»	Порт назначения, к которому будет направлен запрос или установлено соединение. Если служба на указанном порту недоступна, то узел будет исключен из списка балансировки. Параметр доступен при добавлении проверки с типом «ТСР»

### 8.5.2 . Добавление Реального Сервера

Для отображения списка Реальных Серверов следует перейти «Настройки – Управление трафиком – Реальные серверы».

По умолчанию записи представлены табличном виде и упорядочены согласно столбцу «Имя».

Основные параметры списка приведены в таблице (см. Таблица 46).

Таблица 46 – Основные параметры списка Реальных Серверов

Параметр	Описание
«Имя»	Наименование Реального Сервера
«Состояние»	Статус Реального Сервера

Для добавления группы Реальных Серверов следует перейти «Настройки – Управление трафиком – Реальные серверы» и нажать экранную кнопку **[Добавить]**.

Затем заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. Таблица 47).

Таблица 47 – Данные для добавления группы Реальных Серверов

Параметр	Описание
«Имя»	Наименование группы Реальных Серверов
«Используемая проверка»	Выбор заданного метода проверки доступности узла
«Фонд IP»	Выбор IP-фонда, которому будет разрешено устанавливать соединение со списком Реальных Серверов
«Список реальных серверов»	Над списком Реальных Серверов можно выполнять следующие действия: <ul style="list-style-type: none"> <li>▪ добавить, для этого нажать экранную кнопку <b>[Добавить]</b>;</li> <li>▪ удалить, для этого выбрать нужные серверы в списке и нажать экранную кнопку <b>[Удалить]</b></li> </ul>

Форма «Список реальных серверов» позволяет задать список Реальных Серверов.

Доступные параметры для добавления Реального Сервера перечислены в столбце «Параметр» следующей таблицы (см. Таблица 48).

Таблица 48 – Данные для добавления Реального Сервера

Параметр	Описание
«IP»	IP-адрес Реального Сервера
«Порт»	Порт Реального Сервера

### 8.5.3 . Добавление Сервера Балансировки

Для отображения списка Серверов Балансировки следует перейти «Настройки – Управление трафиком – Серверы балансировки».

По умолчанию записи представлены табличном виде и упорядочены согласно столбцу «Имя».

Основные параметры списка приведены в таблице (см. Таблица 49).




Таблица 49 – Основные параметры списка Серверов Балансировки

Параметр	Описание
«Имя»	Наименование Сервера Балансировки
«Тип»	Используемый протокол для балансировки входящих подключений
«Состояние»	Статус Сервера Балансировки
«Алгоритм»	Используемый алгоритм балансировки
«TLS Профиль»	Используемый клиентский TLS-профиль для аутентификации на Реальном Сервере

Для добавления Сервера Балансировки следует перейти «Настройки – Управление трафиком – Серверы балансировки» и нажать экранную кнопку **[Добавить]**.

Затем заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. Таблица 50).

Таблица 50 – Данные для добавления Сервера Балансировки

Параметр	Описание
«Имя»	Наименование Сервера Балансировки
«Тип»	Выбор протокола, который будет использован для балансировки подключений. Возможные значения: <ul style="list-style-type: none"> <li>▪ «TCP»;</li> <li>▪ «RAPID-TCP»</li> </ul>
«Группа РС»	<div style="border: 1px solid orange; padding: 5px; margin-bottom: 5px;">  В текущей версии Termidesk Connect доступна возможность выбора только одной группы Реальных Серверов.                     </div> Выбор группы Реальных Серверов
«Минимальное количество РС, шт»	Минимально необходимое количество доступных Реальных Серверов в группе для перевода Сервера Балансировки в статус «В работе»
«Алгоритм»	Выбор алгоритма, который будет использован для балансировки подключений. Возможные значения: <ul style="list-style-type: none"> <li>▪ «ROUNDROBIN» – поочередное распределение запросов между серверами в группе;</li> <li>▪ «LEASTCONNECTION» – запрос направляется на наименее загруженный сервер</li> </ul>
«Время старта, с»	<div style="border: 1px solid orange; padding: 5px; margin-bottom: 5px;">  В текущей версии Termidesk Connect параметр не влияет на работу Termidesk Connect. Приведена справочная информация.                     </div> Период (в секундах), в течение которого будет запущено выполнение алгоритма «ROUNDROBIN». Параметр позволяет выполнить равномерное распределение запросов между Реальными Серверами с момента, когда один или несколько серверов станут доступны. Параметр доступен только при выборе алгоритма «LEASTCONNECTION»
«Постоянство выбора РС (persistence)»	<div style="border: 1px solid orange; padding: 5px; margin-bottom: 5px;">  В текущей версии Termidesk Connect доступна возможность выбора только привязки с типом «IPSOURCE».                     </div> Выбор типа привязки пользователя к одному Реальному Серверу на время активной сессии
«Время жизни, с»	Период (в секундах), в течение которого сохраняется привязка пользователя к Реальному Серверу при активированном параметре «Постоянство выбора РС (persistence)». Таймер параметра сбрасывается к заданному значению при каждом новом действии пользователя

Параметр	Описание
«Сохранять SRC IP»	<p>Параметр позволяет управлять подменой IP-адреса источника запроса при активированном параметре «Постоянство выбора РС (persistence)».</p> <p>Активация параметра сохраняет исходный IP-адрес источника запроса при подключении к Реальному Серверу. Отключение параметра подменяет IP-адрес источника запроса при подключении к Реальному Серверу.</p> <p>Параметр доступен только при выборе протокола типа «RAPID-TCP»</p>
«Таймаут закрытия по FIN, с»	<p>Период (в секундах) времени хранения записи о сессии после получения FIN-пакета.</p> <p>Параметр доступен только при выборе протокола типа «RAPID-TCP»</p>
«Сохранять клиентский IP»	<p>Параметр позволяет управлять подменой IP-адреса клиента.</p> <p>Активация параметра сохраняет исходный IP-адрес клиента при подключении к Реальному Серверу. Отключение параметра подменяет IP-адрес клиента при подключении к Реальному Серверу.</p> <p>Параметр доступен только при выборе протокола типа «RAPID-TCP».</p>
«Продолжительность неактивной сессии, с»	<p>Период (в секундах), в течение которого соединение остается открытым при отсутствии активной сессии.</p> <p>Параметр доступен только при выборе протокола типа «RAPID-TCP»</p>
«Клиентский TLS профиль»	<p>Выбор клиентского TLS-профиля для аутентификации на Реальном Сервере.</p> <p>Параметр доступен только при выборе типа балансировки «TCP»</p>

#### 8.5.4 . Параметры TLS

#### 8.5.5 . Просмотр и добавление сертификата через веб-интерфейс Termidesk Connect

Для доступа к веб-интерфейсу Termidesk Connect по протоколу HTTPS, а также для других подключений, требующих защищенного соединения, на этапе первичной настройки генерируется самоподписанный сертификат.

Для просмотра списка сертификатов следует перейти «Настройки – Управление трафиком – TLS – Файлы». Файлы располагаются в каталоге `/etc/ssl/tdc/`.

Для загрузки сертификата нужно нажать экранную кнопку **[Загрузить]** и выбрать соответствующий файл:

- файл сертификата. Поддерживаются форматы: `.pem`, `.crt`, `.cer`;
- файл закрытого ключа. Поддерживаются форматы: `.pem`, `.key`;
- файл проверки цепочки сертификатов (необязательно). Поддерживаются форматы: `.pfx`, `.pem`, `.crt`, `.cer`.

#### 8.5.6 . Профили

Для отображения списка профилей следует перейти «Настройки – Управление трафиком – TLS – Профили».



По умолчанию записи представлены в табличном виде и упорядочены согласно столбцу «Имя». Основные параметры списка приведены в таблице (см. Таблица 51).

Таблица 51 – Основные параметры списка Профилей

Параметр	Описание
«Имя»	Наименование профиля
«Тип»	Тип профиля

Для добавления профиля следует перейти «Настройки – Управление трафиком – TLS – Профили» и нажать экранную кнопку **[Добавить]**.

Затем заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. Таблица 52).

Таблица 52 – Данные для добавления Профиля

Параметр	Описание
«Имя»	Наименование профиля
«Timeout»	Время ожидания (в секундах) установки соединения
«Тип»	Выбор типа профиля. Возможные значения: <ul style="list-style-type: none"> <li>▪ «Клиентский»;</li> <li>▪ «Серверный»</li> </ul>
«Конфигурация по-умолчанию»	Форма настройки защищенного SSL-соединения для профиля типа «Серверный». Для настройки защищенного SSL-соединения нужно раскрыть форму «Конфигурация по-умолчанию» и нажать экранную кнопку <b>[Создать]</b> . Конфигурация используется, когда пришедший SNI не соответствует ни одному заданному значению. Статус «Активна» свидетельствует об использовании заданных параметров защищенного SSL-соединения
«Файл сертификата»	Выбор файла клиентского сертификата для аутентификации на Реальном Сервере
«mTLS»	Активация использования протокола mTLS. Параметр доступен только при настройке конфигурации по умолчанию для профиля типа «Серверный»
«Файл ключа»	Выбор файла закрытого ключа, соответствующего клиентскому сертификату
«SNI по-умолчанию»	Наименование сервера по умолчанию для расширения SNI Параметр доступен только для профиля типа «Клиентский»
«Файл сертификата УЦ»	Выбор файла со списком центров сертификации, которые используются для проверки подлинности Реального Сервера
«Файл параметров Diffie-Hellman KE»	Выбор файла с ключами Диффи-Хеллмана для обеспечения безопасного соединения
«Пароль»	Пароль для расшифровки файла закрытого ключа, если ключ зашифрован

Параметр	Описание
«Поддерживаемые версии TLS (SSL)»	Выбор поддерживаемых версий протокола TLS для установления соединения. Для использования защищенного соединения нужно отметить галочкой соответствующую версию протокола в списке. Для выбора всех версий протокола следует нажать экранную кнопку <b>[Выбрать всё]</b> . Для очистки списка нужно нажать экранную кнопку <b>[Clear]</b>
«Наборы криптографических алгоритмов»	Выбор поддерживаемых алгоритмов преобразования данных. Для использования преобразования данных нужно отметить галочкой соответствующий алгоритм в списке. Для выбора всех алгоритмов следует нажать экранную кнопку <b>[Выбрать всё]</b> . Для очистки списка нужно нажать экранную кнопку <b>[Clear]</b>
«Сервера»	Список SNI. Параметр доступен только для профиля типа «Серверный» Над списком можно выполнять следующие действия: <ul style="list-style-type: none"> <li>▪ добавить, для этого нажать экранную кнопку <b>[Добавить]</b>;</li> <li>▪ изменить приоритет, для этого выбрать нужное правило в списке и нажать экранную кнопку <b>[Изменить приоритет]</b>;</li> <li>▪ удалить, для этого выбрать нужные правила в списке и нажать экранную кнопку <b>[Удалить]</b></li> </ul>

Доступные параметры для добавления SNI перечислены в столбце «Параметр» следующей таблицы (см. Таблица 53).

Таблица 53 – Данные для добавления SNI

Параметр	Описание
«SNI»	Имя (hostname) узла, полученное во время установки соединения
«Конфигурация»	Форма настройки защищенного SSL-соединения с SNI. Для настройки защищенного SSL-соединения нужно раскрыть форму «Конфигурация» и нажать экранную кнопку <b>[Создать]</b> . Статус «Активна» свидетельствует об использовании заданных параметров защищенного SSL-соединения
«Файл сертификата»	Выбор файла серверного сертификата, который будет передан для заданного SNI
«mTLS»	Активация использования протокола mTLS
«Файл ключа»	Выбор файла закрытого ключа, соответствующего серверному сертификату
«Файл сертификата УЦ»	Выбор файла со списком центров сертификации, которые используются для проверки подлинности
«Файл параметров Diffie-Hellman KE»	Выбор файла с ключами Диффи-Хеллмана для обеспечения безопасного соединения
«Пароль»	Пароль для расшифровки файла закрытого ключа, если ключ зашифрован

Параметр	Описание
«Поддерживаемые версии TLS (SSL)»	Выбор поддерживаемых версий протокола TLS для установления соединения. Для использования защищенного соединения нужно отметить галочкой соответствующую версию протокола в списке. Для выбора всех версий протокола следует нажать экранную кнопку <b>[Выбрать всё]</b> . Для очистки списка нужно нажать экранную кнопку <b>[Clear]</b>
«Наборы криптографических алгоритмов»	Выбор поддерживаемых алгоритмов преобразования данных. Для использования преобразования данных нужно отметить галочкой соответствующий алгоритм в списке. Для выбора всех алгоритмов следует нажать экранную кнопку <b>[Выбрать всё]</b> . Для очистки списка нужно нажать экранную кнопку <b>[Clear]</b>

### 8.5.7 . Добавление файлов сценария

Для загрузки файла следует перейти «Настройки – Управление трафиком – Сценарии» и нажать экранную кнопку **[Загрузить]**.

Допускается загрузка только файлов сценариев в формате .lua.

### 8.5.8 . Добавление Виртуального Сервера

Для отображения списка Виртуальных Серверов следует перейти «Настройки – Управление трафиком – Виртуальные серверы».

По умолчанию записи представлены в табличном виде и упорядочены согласно столбцу «Имя».

Основные параметры списка приведены в таблице (см. Таблица 54).

Таблица 54 – Основные параметры списка Виртуальных Серверов

Параметр	Описание
«Имя»	Наименование Виртуального Сервера
«IP Адрес»	IP-адрес Виртуального Сервера
«Порт»	Порт Виртуального Сервера
«Тип»	Тип протокола для балансировки подключения
«Состояние»	Статус Виртуального Сервера
«TLS Профиль»	Используемый серверный TLS-профиль

Над Виртуальными Серверами можно выполнять следующие действия:

- включить, для этого выбрать нужные серверы в списке и нажать экранную кнопку **[Включить]**;
- выключить, для этого выбрать нужные серверы в списке и нажать экранную кнопку **[Выключить]**.

Для добавления Виртуального Сервера следует перейти «Настройки – Управление трафиком – Виртуальные серверы» и нажать экранную кнопку **[Добавить]**.

Затем заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. Таблица 55).

Таблица 55 – Данные для добавления Виртуального Сервера

Параметр	Описание
«Имя»	Наименование Виртуального Сервера
«Тип»	Выбор типа протокола для балансировки подключения. Возможные значения: <ul style="list-style-type: none"> <li>▪ «TCP»;</li> <li>▪ «HTTP»;</li> <li>▪ «RAPID-TCP»</li> </ul>
«IP Адрес»	IP-адрес Виртуального Сервера
«Порт»	Порт Виртуального Сервера
«Зависимость состояния»	Параметр позволяет задать правило изменения статуса Виртуального Сервера в зависимости от состояния Серверов Балансировки в списке. Для добавления Сервера Балансировки нужно нажать экранную кнопку <b>[Добавить]</b> и выбрать нужный сервер в списке. Возможные значения: <ul style="list-style-type: none"> <li>▪ «NONE» – Виртуальный Сервер всегда находится в статусе «В работе»;</li> <li>▪ «OR» – Виртуальный Сервер находится в статусе «В работе», если хотя бы один Сервер Балансировки доступен;</li> <li>▪ «AND» – Виртуальный Сервер переходит в статус «Отключен», если хотя бы один Сервер Балансировки становится недоступным</li> </ul>
«VRF»	Выбор VRF для добавления Виртуального Сервера
«Серверный TLS профиль»	Выбор серверного TLS-профиля
«Правила»	Список правил для балансировки подключений. Над списком правил можно выполнять следующие действия: <ul style="list-style-type: none"> <li>▪ добавить, для этого нажать экранную кнопку <b>[Добавить]</b>;</li> <li>▪ изменить приоритет, для этого выбрать нужное правило в списке и нажать экранную кнопку <b>[Изменить приоритет]</b>;</li> <li>▪ удалить, для этого выбрать нужные правила в списке и нажать экранную кнопку <b>[Удалить]</b></li> </ul>

Доступные правила балансировки подключений по протоколу TCP перечислены в столбце «Параметр» следующей таблицы (см. Таблица 56).

Таблица 56 – Данные для добавления правил балансировки подключений по протоколу TCP

Параметр	Описание
«Приоритет»	Приоритет обработки правила
«Сервер балансировки»	Выбор Сервера Балансировки
«Сеть источника запроса»	IP-адрес сети в формате CIDR

Доступные правила балансировки подключений по протоколу HTTP перечислены в столбце «Параметр» следующей таблицы (см. Таблица 57).

Таблица 57 – Данные для добавления правил балансировки подключений по протоколу HTTP

Параметр	Описание
«Приоритет»	Приоритет обработки правила
«Сценарий»	Выбор исполняемого файла в раскрывающемся списке

## 8.6 . Функция «ГеоБН»

### 8.6.1 . Добавление ADNS

Для отображения списка ADNS следует перейти «Настройки – ГеоБН – ADNS».

По умолчанию записи представлены табличном виде и упорядочены согласно столбцу «IP Адрес».

Основные параметры списка приведены в таблице (см. Таблица 58).

Таблица 58 – Основные параметры списка ADNS

Параметр	Описание
«IP Адрес»	IP-адрес Termidesk Connect для обработки DNS-запросов
«Порт»	Порт для обработки DNS-запросов

Для добавления ADNS следует перейти «Настройки – ГеоБН – ADNS» и нажать экранную кнопку **[Добавить]**.

Затем заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. Таблица 59).

Таблица 59 – Данные для добавления ADNS

Параметр	Описание
«IP Адрес»	IP-адрес Termidesk Connect для обработки DNS-запросов
«Порт»	Порт для обработки DNS-запросов

### 8.6.2 . Добавление Площадок

Для отображения списка Площадок следует перейти «Настройки – ГеоБН – Площадки».

По умолчанию записи представлены табличном виде и упорядочены согласно столбцу «Имя».

Основные параметры списка приведены в таблице (см. Таблица 60).

Таблица 60 – Основные параметры списка Площадок

Параметр	Описание
«Имя»	Наименование Площадки

Для добавления Площадки следует перейти «Настройки – ГеоБН – Площадки» и нажать экранную кнопку **[Добавить]**.

Затем заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. Таблица 61).

Таблица 61 – Данные для добавления Площадки

Параметр	Описание
«Имя»	Наименование группы серверов или ЦОД геораспределенной балансировки

### 8.6.3 . Добавление DNS View

Для отображения списка DNS View следует перейти «Настройки – ГеоБН – DNS View».

По умолчанию записи представлены табличном виде и упорядочены согласно столбцу «Имя».

Основные параметры списка приведены в таблице (см. Таблица 62).

Таблица 62 – Основные параметры списка DNS View

Параметр	Описание
«Имя»	Наименование DNS View

Для добавления DNS View следует перейти «Настройки – ГеоБН – DNS View» и нажать экранную кнопку **[Добавить]**.

Затем заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. Таблица 63).

Таблица 63 – Данные для добавления DNS View

Параметр	Описание
«Имя»	Наименование DNS View
«Сети»	Список сетей, при запросе из которых Termidesk Connect будет выдавать локальные IP-адреса Сервисов. Над списком сетей можно выполнять следующие действия: <ul style="list-style-type: none"> <li>▪ добавить, для этого нажать экранную кнопку <b>[Добавить]</b> и указать IP-адрес сети в формате CIDR в открывшемся поле;</li> <li>▪ удалить, для этого выбрать нужные сети в списке и нажать экранную кнопку <b>[Удалить]</b></li> </ul>

#### 8.6.4 . Добавление Сервисов

Для отображения списка сервисов следует перейти «Настройки – ГеоБН – Сервисы».

По умолчанию записи представлены табличном виде и упорядочены согласно столбцу «Имя».

Основные параметры списка приведены в таблице (см. Таблица 64).

Таблица 64 – Основные параметры списка Сервисов

Параметр	Описание
«Имя»	Наименование Сервиса
«Состояние»	Статус Сервиса
«Публичный IP»	IP-адрес Сервиса, используемый для доступа из внешних сетей
«Внутренний IP»	IP-адрес Сервиса, используемый для доступа внутри локальной сети


Над Сервисами можно выполнять следующие действия:

- включить, для этого выбрать нужные Сервисы в списке и нажать экранную кнопку **[Включить]**;
- выключить, для этого выбрать нужные Сервисы в списке и нажать экранную кнопку **[Выключить]**.

Для добавления Сервиса следует перейти «Настройки – ГеоБН – Сервисы» и нажать экранную кнопку **[Добавить]**.

Затем заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. Таблица 65).

Таблица 65 – Данные для добавления Сервиса

Параметр	Описание
«Имя»	Наименование Сервиса
«Вес»	Определяет приоритет распределения запросов на Сервис. Распределение запросов на Сервис выполняется при активации алгоритма «ROUNDROBIN» на Виртуальном Сервере геобалансировки (см. подраздел <b>Виртуальные Серверы геобалансировки</b> )
«Публичный IP»	IP-адрес Сервиса, используемый для доступа из внешних сетей
«Внутренний IP»	IP-адрес Сервиса, используемый для доступа внутри локальной сети
«Проверка»	Выбор типа проверки доступности Сервиса
«Площадка»	 В текущей версии Termidesk Connect параметр представлен в демонстрационном режиме.


### 8.6.5 . Добавление Виртуальных Серверов геобалансировки

Для отображения списка Виртуальных Серверов геобалансировки следует перейти «Настройки – ГеоБН – Виртуальные серверы».

По умолчанию записи представлены в табличном виде и упорядочены согласно столбцу «Имя».

Основные параметры списка приведены в таблице (см. Таблица 66).

Таблица 66 – Основные параметры списка Виртуальных Серверов геобалансировки

Параметр	Описание
«Имя»	Наименование Виртуального Сервера геобалансировки
«Состояние DNS View»	 В текущей версии Termidesk Connect состояние отображается в демонстрационном режиме. Статус DNS View
«Алгоритм»	Используемый алгоритм балансировки

Над Виртуальными Серверами геобалансировки можно выполнять следующие действия:

- включить, для этого выбрать нужные серверы в списке и нажать экранную кнопку **[Включить]**;
- выключить, для этого выбрать нужные серверы в списке и нажать экранную кнопку **[Выключить]**.

Для добавления Виртуального Сервера геобалансировки следует перейти «Настройки – ГеоБН – Виртуальные серверы» и нажать экранную кнопку **[Добавить]**.

Затем заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. Таблица 67).


Таблица 67 – Данные для добавления Виртуального Сервера геобалансировки

Параметр	Описание
«Имя»	Наименование Виртуального Сервера геобалансировки
«ECS»	Активация перенаправления запросов на ближайший Сервис на основе информации о подсети источника запроса
«Алгоритм»	Выбор метода балансировки подключений. Возможные значения: <ul style="list-style-type: none"> <li>▪ «ONLINE» - перенаправление запросов только на доступные Сервисы в списке балансировки;</li> <li>▪ «ROUNDROBIN» - поочередное распределение запросов между Сервисами в списке балансировки;</li> <li>▪ «SOURCEIPHASH» - привязка запросов к Сервисам на основе хеша IP-адреса;</li> <li>▪ «STATICPROXIMITY» - перенаправление запросов на ближайшую Площадку для выдачи Сервиса</li> </ul>
«Постоянство выбора сервиса (persistence)»	Выбор типа привязки источника запроса к одному Сервису на время обработки его DNS-запросов. Возможные значения: <ul style="list-style-type: none"> <li>▪ «OFF» - привязка к Сервису отключена;</li> <li>▪ «SRCIP» - привязка источника запроса к Сервису на основе его IP-адреса</li> </ul>
«DNS View»	Выбор DNS View
«Сервисы»	Список Сервисов для балансировки подключений. Над списком Сервисов можно выполнять следующие действия: <ul style="list-style-type: none"> <li>▪ добавить, для этого нажать экранную кнопку <b>[Добавить]</b>;</li> <li>▪ удалить, для этого выбрать нужные правила в списке и нажать экранную кнопку <b>[Удалить]</b></li> </ul>

По умолчанию список Сервисов представлен табличном виде и упорядочен согласно столбцу «Имя».

Основные параметры списка приведены в таблице (см. Таблица 64).

Таблица 68 – Основные параметры списка Сервисов

Параметр	Описание
«Имя»	Наименование Сервиса
«Состояние»	<div style="border: 1px solid yellow; padding: 5px; margin-bottom: 5px;">  В текущей версии Termidesk Connect состояние сервиса отображается в демонстрационном режиме.                 </div> Статус Сервиса
«Вес»	Приоритет распределения запросов на Сервис

### 8.6.6 . Добавление Зоны

Для отображения списка Зон следует перейти «Настройки – ГеоБН – Зоны».

По умолчанию записи представлены табличном виде и упорядочены согласно столбцу «Имя».

Основные параметры списка приведены в таблице (см. Таблица 69).



Таблица 69 – Основные параметры списка Зон

Параметр	Описание
«Имя»	Наименование Зоны

Для добавления Зоны следует перейти «Настройки – ГеоБН – Зоны» и нажать экранную кнопку **[Добавить]**.

Затем заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. Таблица 70).

Таблица 70 – Данные для добавления Зоны

Параметр	Описание
«Имя»	Наименование Зоны
«Поддомены»	Список поддоменов, для которых задаются параметры обработки запросов. Над списком поддоменов можно выполнять следующие действия: <ul style="list-style-type: none"> <li>▪ добавить, для этого нажать экранную кнопку <b>[Добавить]</b>;</li> <li>▪ изменить, для этого выбрать нужные поддомены в списке и нажать экранную кнопку <b>[Изменить]</b>;</li> <li>▪ удалить, для этого выбрать нужные поддомены в списке и нажать экранную кнопку <b>[Удалить]</b></li> </ul>

По умолчанию список поддоменов представлен табличном виде и упорядочен согласно столбцу «Имена».

Основные параметры списка приведены в таблице (см. Таблица 71).

Таблица 71 – Основные параметры списка поддоменов

Параметр	Описание
«Имена»	Наименование поддомена
«TTL»	Время жизни DNS-записи (в секундах)
«Виртуальные серверы»	Список назначенных Виртуальных Серверов для обработки запросов

Данные, необходимые для добавления поддомена, перечислены в столбце «Параметр» следующей таблицы (см. Таблица 72).

Таблица 72 – Данные для добавления поддомена

Параметр	Описание
«Поддомен»	Наименование поддомена
«TTL»	Время жизни DNS-записи (в секундах)
«Виртуальные серверы»	Список назначенных Виртуальных Серверов для обработки запросов. Над списком Виртуальных Серверов можно выполнять следующие действия: <ul style="list-style-type: none"> <li>▪ добавить, для этого нажать экранную кнопку <b>[Добавить]</b>;</li> <li>▪ удалить, для этого выбрать нужные серверы в списке и нажать экранную кнопку <b>[Удалить]</b></li> </ul>

Данные, необходимые для добавления списка виртуальных серверов перечислены в столбце «Параметр» следующей таблицы (см. Таблица 73).

Таблица 73 – Данные для добавления списка Виртуальных Серверов

Параметр	Описание
«Порядковый номер»	Приоритет обработки запросов Виртуальным Сервером. Обработка запросов осуществляется в порядке возрастания порядкового номера Виртуального Сервера. В случае недоступности Виртуального Сервера, запросы будут обработаны следующим по порядку Виртуальным Сервером
«Виртуальный сервер»	Выбор Виртуального Сервера в списке

## 9. ПЕРЕЧЕНЬ ТЕРМИНОВ

Термин	Определение
DNS View	Объект (абстракция), описывающий сети, при запросе из которых должен быть выдан локальный IP-адрес Сервиса
Full Proxy	Режим, при котором Termidesk Connect является посредником между клиентом и Реальным Сервером и полностью обрабатывает входящие и исходящие соединения
Linux Shell	Программный интерфейс для взаимодействия пользователя с ОС
SSL Offload	Процесс, в котором преобразование трафика SSL/TLS выполняется не на серверах приложений (Реальных Серверах), а на Termidesk Connect
Termidesk Connect	Программа для электронной вычислительной машины «Балансировщик нагрузки Термидеск Коннект»
TLS Hello	Начальный этап установки соединения по протоколу TLS
Виртуальный Сервер	Объект (абстракция), терминирующий на себя трафик от пользователя
Виртуальный Сервер геобалансировки	Объект (абстракция) в рамках геобалансировки, терминирующий на себя трафик от пользователя
Группа Реальных Серверов	Объединение нескольких Реальных Серверов и их периодических проверок
Закрытый ключ	Сохраняемый в тайне ключ из ключевой пары, принадлежащий владельцу и не подлежащий распространению
Зона	Объект, описывающий доменные имена, для которых обеспечивается геобалансировка подключений
Клиентский SSL-профиль	Профиль для обеспечения безопасного соединения между Termidesk Connect и Реальным Сервером
Ключ	Параметр в виде последовательности псевдослучайных чисел
Ключевая пара	Упорядоченная пара математически однозначно связанных ключей, определяющих взаимосвязанные защитные преобразования
Мастер-узел («Active»)	Устройство в рамках отказоустойчивой (высокодоступной) конфигурации, обрабатывающее трафик пользователей в настоящий момент
Открытый ключ	Ключ из ключевой пары, который может быть сделан общедоступным
Предварительная конфигурация («candidate»)	Представляет собой временное хранилище конфигурации, где вносятся изменения перед их применением. Изменения в такой конфигурации можно редактировать, проверять и отменять без влияния на рабочую конфигурацию Termidesk Connect. Чтобы изменения вступили в силу, их нужно записать командой <code>commit</code>

Термин	Определение
Рабочая конфигурация («running»)	<p>Представляет собой конфигурацию, в данный момент используемую Termidesk Connect.</p> <p>Рабочая конфигурация будет обновлена, если для предварительной конфигурации выполнить команду <code>commit</code>.</p> <p>Если Termidesk Connect перезагрузится, то изменения в рабочей конфигурации будут сброшены, если не выполнена команда <code>write</code></p>
Реальный Сервер	Узел с установленным приложением, доставку которого обеспечивает Termidesk Connect
Резервный узел	Устройство в рамках отказоустойчивой (высокодоступной) конфигурации, не обрабатывающее трафик пользователей в настоящий момент
Сервер Балансировки	Объект (абстракция), с заданным алгоритмом балансировки и другими параметрами, реализующий перенаправление подключения пользователя на один из Реальных Серверов
Серверный SSL-профиль	Профиль для обеспечения безопасного соединения между пользователем и Termidesk Connect
Сервис	Объект (абстракция), представляющий собой IP-адрес, который может быть в DNS-ответе
Сертификат	Артефакт, содержащий открытый ключ, информацию о владельце ключа и подтверждающий принадлежность открытого ключа владельцу, защищенный с применением закрытого ключа
Сохраненная конфигурация («startup»)	<p>Представляет собой конфигурацию, загружаемую при старте Termidesk Connect.</p> <p>После перезагрузки Termidesk Connect сохраненная конфигурация копируется в рабочую.</p> <p>Чтобы рабочая конфигурация была загружена при следующем запуске (стала сохраненной конфигурацией), нужно выполнить команду <code>write</code></p>
Хеш	Строка бит, являющаяся выходным результатом функции хеширования
Центр сертификации	Программный компонент, реализующий возможность подтверждения подлинности ключей с помощью сертификатов

## 10 . ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

Сокращение	Пояснение
ADNS	Authoritative Domain Name System (авторитетная система доменных имен)
API	Application Programming Interface (программный интерфейс приложения)
ARP	Address Resolution Protocol (протокол разрешения адресов)
CIDR	Classless Inter-Domain Routing (бесклассовая адресация)
CLI	Command Line Interface (интерфейс командной строки)
DNS	Domain Name System (система доменных имен)
EDNS	Extension Mechanisms for DNS (спецификация расширения DNS)
FIN	Finish (флаг протокола TCP для завершения соединения)
FQDN	Fully Qualified Domain Name (полностью определенное имя домена)
HTTP	HyperText Transfer Protocol (протокол передачи гипертекста)
HTTPS	Hypertext Transfer Protocol Secure (расширение протокола HTTP для поддержки шифрования)
ICMP	Internet Control Message Protocol (протокол межсетевых управляющих сообщений)
IP	Internet Protocol (межсетевой протокол)
JSON	JavaScript Object Notation (стандартный текстовый формат для структурированных данных)
L3	Третий (сетевой) уровень сетевой модели OSI
L4	Четвертый (транспортный) уровень сетевой модели OSI
L7	Седьмой (транспортный) уровень сетевой модели OSI
mTLS	Multiplexed Transport Layer Security (протокол, основанный на TLS с усиленной безопасностью)
NETCONF	Протокол конфигурации сетевых устройств
OSI	The Open Systems Interconnection model (модель стека сетевых протоколов)
RAPID-TCP	Rapid Transmission Control Protocol (оптимизированный протокол управления передачей)
RESTCONF	Протокол, предоставляющий программный интерфейс для доступа к данным, определенным в моделях YANG
SNI	Server Name Indication (расширение протокола TLS для идентификации имени сервера)
SSL	Secure Sockets Layer (криптографический протокол)
SYN	Запрос на подключение по протоколу TCP
TCP	Transmission Control Protocol (протокол управления передачей)
TLS	Transport Layer Security (протокол защиты транспортного уровня)

Сокращение	Пояснение
TTL	Time To Live (время жизни IP-пакета)
TXT	Формат текстового представления
UDP	User Datagram Protocol (протокол пользовательских дейтаграмм)
VLAN	Virtual Local Area Network (виртуальная локальная сеть)
VRF	Virtual Routing and Forwarding (технология реализации нескольких виртуальных маршрутизаторов на базе одного физического)
XML	Xtensible Markup Language (расширяемый язык разметки)
YANG	Yet Another Next Generation (язык моделирования данных)



© ООО «УВЕОН»

119571, г. Москва, Ленинский проспект,  
д. 119А, помещ. 9Н  
<https://termidesk.ru/>  
Телефон: +7 (495) 975-1-975

Общий e-mail: [info@uveon.ru](mailto:info@uveon.ru)  
Отдел продаж: [sales@uveon.ru](mailto:sales@uveon.ru)  
Техническая поддержка: [support@uveon.ru](mailto:support@uveon.ru)