Инструкция по подключению услуги «Бизнес рассылки» по протоколу SMPP

Оглавление

[Построение Site-to-Site IPSec туннеля 3](#_Toc442185099)

[Построение Host-to-Site IPSec туннеля 5](#_Toc442185100)

[Настройка SMPP подключения 13](#_Toc442185101)

[SMPP параметры 14](#_Toc442185102)

[1. Команды протокола SMPP 14](#_Toc442185103)

[2. Длинные SMS-сообщения 14](#_Toc442185104)

[3. Кодировка SMS‑сообщений 15](#_Toc442185105)

[4. Время жизни сообщения 15](#_Toc442185106)

[5. Отчеты о доставке 15](#_Toc442185107)

[6. Правила представления номеров: 16](#_Toc442185108)

По протоколу SMPP возможно подключение Sit-to-Site и Host-to-Site:

* Схема подключения IPSec Site-to-Site VPN возможна при наличии у Клиента оборудования, поддерживающего данную технологию.
* При наличии у Клиента одного терминала рекомендованная схема подключения - Host-to-Site IPSec VPN.

# Построение Site-to-Site IPSec туннеля

1. **Для выполнения настроек VPN подключения Клиенту предоставляется таблица вида:**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | | | | XXXXX | | | |
| VPN gateway NATed (YES/NO)? | | | | | NO | | | |
| Public IP address of VPN gateway (Peer IP) | | | | | XX.XXX.XX.XX | | | |
| Key | | | | | XXXXX | | | |
| **IKE Phase1** | | | | | | | | |
| Authentication: | | | | | pre-share key | | | |
| Hash: (SHA-1 или MD5) | | | | | SHA-1 | | | |
| Encryption: (AES (256 Bits), AES (128 Bits), 3DES) | | | | | 3DES | | | |
| Diffie-Hellman group: | | | | | Group 2 (1024) | | | |
| IKE mode: | | | | | main | | | |
| Lifetime: | | | | | 86400 sec | | | |
| **IKE Phase2 (transform-set)** | | | | | | | | |
| IPSec Mode: | | | | | Tunnel | | | |
| Encryption: (AES (256 Bits), AES (128 Bits), 3DES) | | | | | AES-128 | | | |
| Perfect Forward Secrecy (PFS):  (NO или YES, DH group) | | | | | No | | | |
| Hash: | | | | | SHA-1 | | | |
| Lifetime: | | | | | 3600 (can be different, tunnel just reestablishes from time to time. Possible to set per ipsec policy) | | | |
| Lifetime kilobytes: | | | | | 1843200 (can be different, tunnel just reestablishes from time to time. Possible to set per ipsec policy) | | | |
| **List of hosts, involved in VPN-connection.** | | | | | | | | |
| №№ | Client name | | | | |  | | |
| Original IP | | Translated IP | | | Translated IP | | Original IP |
| 11 | Client IP | | 172.25.XXX.XXX | | | 172.25.60.131 | | SMPP server |
| 22 |  | |  | | |  | |  |
| **ACL** | | | | | | | | |
| №№ | | Source | | Destination | | | Service (Port) | |
| 11 | | 172.25.60.131 | | 172.25.XXX.XXX | | | 8313 | |
| 22 | |  | |  | | |  | |

Логин и пароль для подключения по SMPP будет отправлен Заказчику по SMS/E-mail.

«Уважаемый пользователь, cервис "Процессинговые рассылки" активирован. Для его использования воспользуйтесь параметрами: Логин: 00XXXX, Пароль: XXXXXX»

1. **Схема построения IPSec туннеля между сетью Клиента и сетью Оператора**



1. Клиенту выделяется приватный IP-адрес, который будет использован для связи терминалов Клиента и сервера Оператора. Данный IP-адрес является уникальный и гарантирует, что IP-адрес клиента не будет пересекаются с IP-адресом другого клиента или уже существующими IP-адресами в сети Оператора.
2. Все IP-адреса терминалов, которые будут осуществлять обмен данными с сервером Оператора, должны быть транслированы в этот один адрес при помощи технологии NAPT.
3. Далее, туннель устанавливается таким образом, чтобы шифровать данные между выделенным IP-адресом Клиента и IP-адресом сервера Оператора.
4. Если в сети Клиента уже существует сетевой диапазон, включающий IP-адрес сервера Оператора, на сетевом оборудовании Клиента необходимо настроить маршрут на сервер Оператора. Этот маршрут должен указывать на роутер, ведущий в Интернет.
5. Если в сети Клиента уже существует сетевое устройство с таким же IP-адресом, как у сервера Оператора, Клиент должен осуществлять SNAT для IP-адреса сервера Оператора на интерфейсе файервола, смотрящего в сторону сервера Оператора.

# Построение Host-to-Site IPSec туннеля

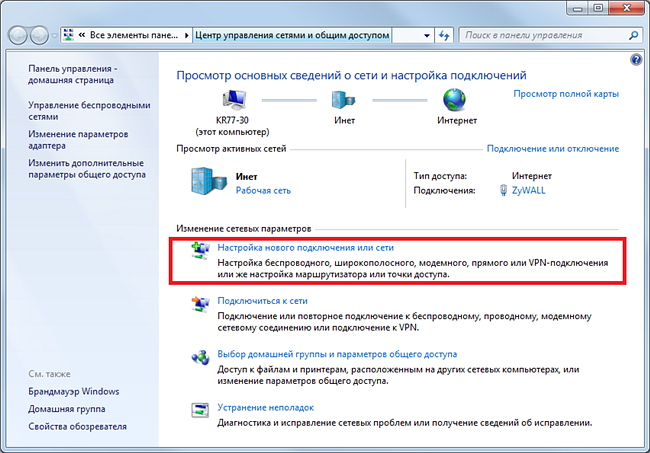
1. **Для выполнения настроек VPN подключения Клиенту предоставляется таблица вида**:

|  |  |
| --- | --- |
| L2TP VPN | |
| IP-адрес VPN-сервера |  |
| Ключ проверки подлинности |  |
| Протокол аутентификации |  |
| Имя пользователя |  |
| Пароль |  |

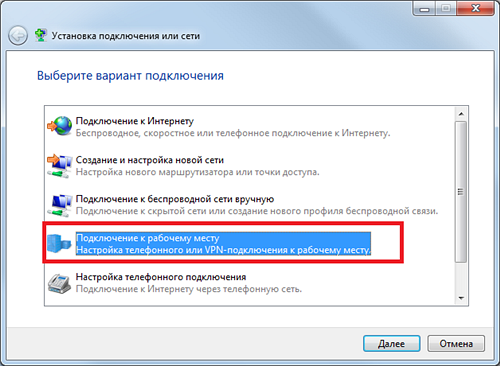
1. **Построение IPSec туннеля между хостом Клиента и сетью Оператора**

Пример настройки хоста Клиента на примере операционной системы Windows 7:

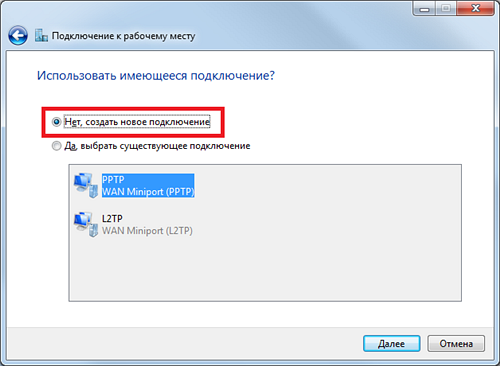
Шаг 1. Откройте **Панель управления**, затем **Центр управления** **сетями** **и общим доступом**. Выберите **Настройка нового подключения или сети**.

[](http://zyxel.ru/sites/default/files/kb/KB-2085/KB-2085-1-1.png)

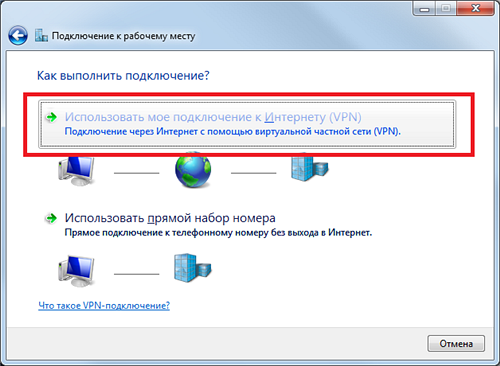
Шаг 2. Выберите **Подключение к рабочему месту**.

[](http://zyxel.ru/sites/default/files/kb/KB-2085/KB-2085-2-2.png)

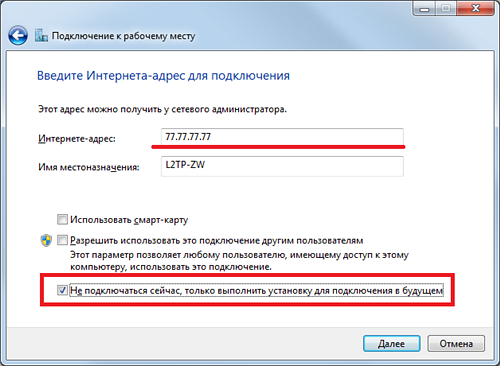
Шаг 3. Выберите **Нет, создать новое подключение**.

[](http://zyxel.ru/sites/default/files/kb/KB-2085/KB-2085-3-3.png)

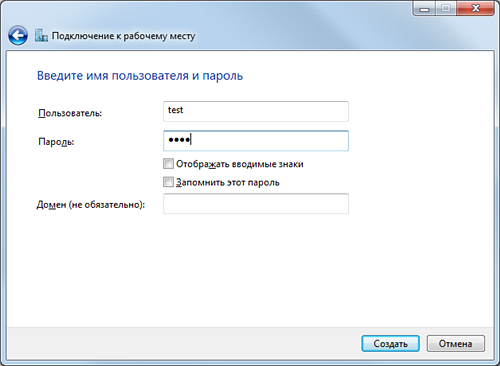
Шаг 4. Выберите **Использовать мое подключение к Интернету**.

[](http://zyxel.ru/sites/default/files/kb/KB-2085/KB-2085-4-4.png)

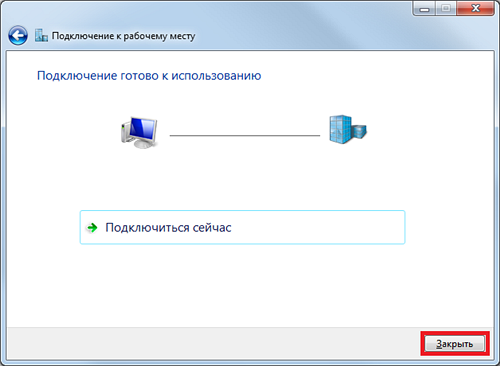
Шаг 5. Введите IP-адрес VPN-сервера из таблицы. В качестве значения поля **Имя местоназначения** укажите MTS IM. Затем выберите **Не подключаться сейчас**.

[](http://zyxel.ru/sites/default/files/kb/KB-2085/KB-2085-5-5.png)

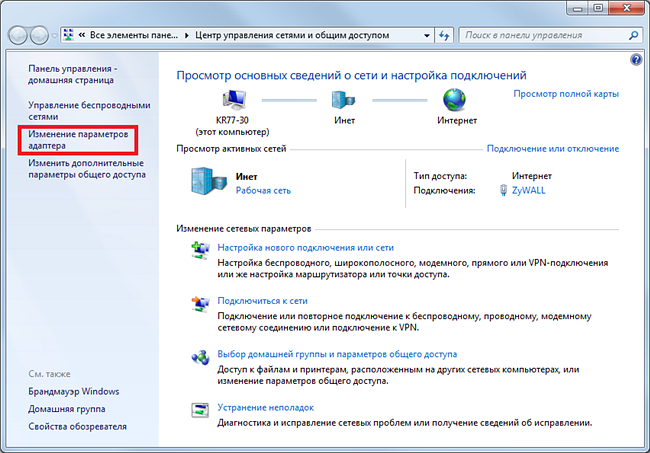
Шаг 6. Введите имя пользователя и пароль учетной записи для L2TP из таблицы.

[](http://zyxel.ru/sites/default/files/kb/KB-2085/KB-2085-6-6.png)

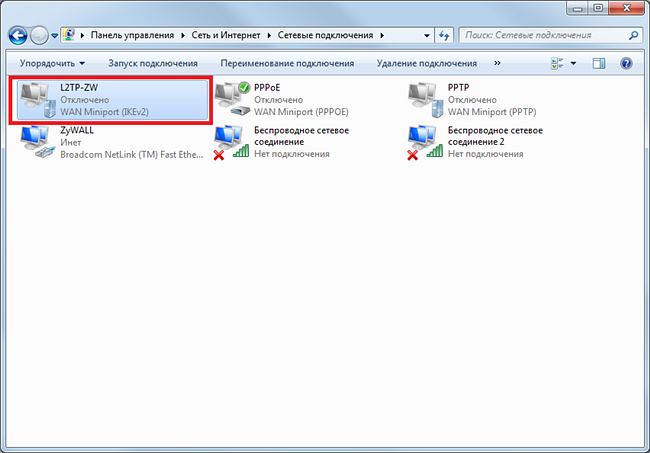
Шаг 7. Нажмите **Закрыть**.

[](http://zyxel.ru/sites/default/files/kb/KB-2085/KB-2085-7-7.png)

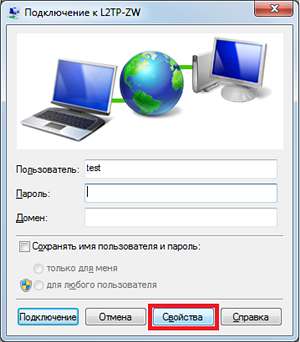
Шаг 8. Нажмите **Изменение параметров адаптера**.

[](http://zyxel.ru/sites/default/files/kb/KB-2085/KB-2085-8-8.png)

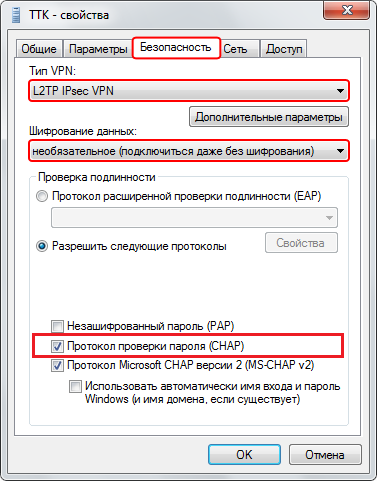
Шаг 9. Выполните двойной щелчок мышкой по созданному подключению.

[](http://zyxel.ru/sites/default/files/kb/KB-2085/KB-2085-9-9.png)

Шаг 10. Нажмите **Свойства.**

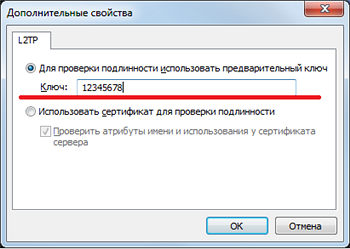
[](http://zyxel.ru/sites/default/files/kb/KB-2085/KB-2085-10-10.png)

Шаг 11. Выберите опции как на скриншоте.

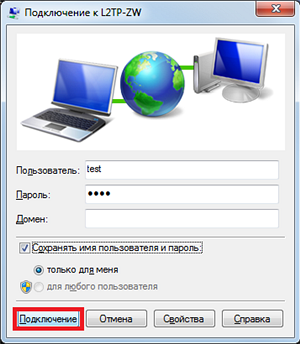


Шаг 12. Нажмите **Дополнительные параметры**.

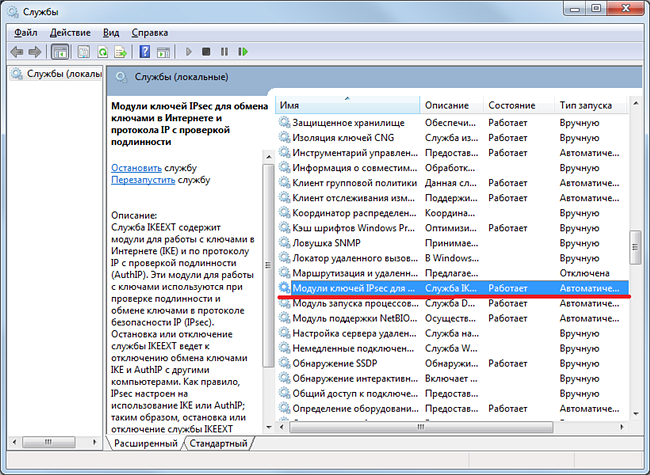
Шаг 13. Введите ключ проверки подлинности (pre-shared key) из таблицы. Нажимте **ОК**.

[](http://zyxel.ru/sites/default/files/kb/KB-2085/KB-2085-13-13.png)

Шаг 14. Введите пароль и нажмите кнопку **Подключение**.

[](http://zyxel.ru/sites/default/files/kb/KB-2085/KB-2085-14-14.png)

Шаг 15. На этом настройка будет завершена. Проверьте, что на компьютере запущена служба **Модули ключей IPSec для обмена ключами в интернете и протокола IP с проверкой подлинности** (Пуск — Панель управления — Администрирование — Службы).

[](http://zyxel.ru/sites/default/files/kb/KB-2085/KB-2085-15-15.png)

# Настройка SMPP подключения

1. Клиенту будет отправлен логин/пароль на e-mail/телефон.
2. После того как VPN соединение установлено – по SMPP необходимо подключаться к IP адресу 172.25.60.131 по порту 8313

# SMPP параметры

## **Команды протокола SMPP**

SMS-G Оператора поддерживает следующие типы команд для SMPP v3.4:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Command** | **Code** | **TX** | **RX** | **TRX** |
| bind\_transceiver | 0x00000009 | | | |
| bind\_transceiver\_resp | 0x80000009 | | | |
| enquire\_link | 0x00000015 | Y | Y | Y |
| enquire\_link\_resp | 0x80000015 | Y | Y | Y |
| deliver\_sm | 0x00000005 | N | Y | Y |
| deliver\_sm\_resp | 0x80000005 | N | Y | Y |
| submit\_sm | 0x00000004 | Y | N | Y |
| submit\_sm\_resp | 0x80000004 | Y | N | Y |
| Unbind | 0x00000006 | Y | Y | Y |
| unbind\_resp | 0x80000006 | Y | Y | Y |
| generic\_nack | 0x80000000 | Y | Y | Y |

Все другие команды или сообщения не будут обработаны, с возвращением кода ошибки ESME\_RINVCMDID.

## **Длинные SMS-сообщения**

Признак длинного SMS-сообщения должен быть передан параметром User-Data-Header или Message\_payload.

На уровне протокола SMPP v.3.4. параметры передачи длинных SMS-сообщений должны быть выражены следующим образом (согласно спецификации протокола):

* параметр *esm\_class* = 0 1 x x x x x x (Bits: 7 6 5 4 3 2 1 0)

UDHI Indicator (only relevant for MT short messages)

* параметр *short\_message* должен содержать в себе заголовок UDH

Message payload - optional SMPP 3.4 TLV (tag-length-value)

* параметр *message length = 0*
* *Optional parameter* должен содержать в себе message\_payload (0x0424)

## **Кодировка SMS‑сообщений**

|  |  |  |  |
| --- | --- | --- | --- |
| Схема кодирования | Длина текста короткого SMS-сообщения в сегменте SMS-сообщения | Длина текста длинного SMS-сообщения в сегменте SMS-сообщения |  |
| GSM 7-bit default alphabet (GSM 03.38)\* | 160 символов | 153 символа | Data coding 0 |
| UCS2 (ISO/IEC-10646) 16-bit | 70 символов | 67 символов | Data coding 8 |

\*Длина сегментов SMS-сообщения приведена с учетом использования символов основной таблицы GSM 7-bit default alphabet. При этом следует помнить, что при использовании символов расширенной таблицы GSM 7-bit default alphabet длина сегментов сообщения будет уменьшаться, поскольку каждый символ расширенной таблицы передается двумя октетами и учитывается как два символа.

## **Время жизни сообщения**

На уровне протокола SMPP v.3.4 время жизни SMS-сообщения должно быть передано параметром validity\_period (согласно спецификации протокола).

Если Клиент указывает время жизни SMS-сообщения в явном виде, согласно спецификации протокола SMPP v.3.4, то будет применен параметр validity\_period, который определен Клиентом. Но следует учитывать, что значение этого параметра не может превышать значение по умолчанию на SMSC Оператора, указанного ниже.

Если Клиент не указывает время жизни сообщения, то время жизни определяется значением по умолчанию на SMSC Оператора:

|  |  |
| --- | --- |
|  | Значение параметра Validity-Period по умолчанию на SMSC Опреатора |
| Оператор | 24 hour |

## **Отчеты о доставке**

Если Клиента желает получать отчеты о доставке SMS-сообщений, параметр registered\_delivery на уровне протокола SMPP v.3.4. должен иметь значение x x x x x x 0 1 (Bits: 7 6 5 4 3 2 1 0). При этом отчет о доставке будет передан командой deliver\_sm согласно спецификации протокола.

## **Правила представления номеров:**

1.      Для номеров абонентов МТС Украина/Водафон используются:

* dest\_addr\_ton (source\_addr\_ton) = 1
* dest\_addr\_npi (source\_addr\_npi) = 1
* dest\_addr (source\_addr) = <12-digits\_MSISDN>

2.      Для цифровых сервисных номеров, выделенных для Клиента, используются:

* dest\_addr\_ton (source\_addr\_ton) = 0
* dest\_addr\_npi (source\_addr\_npi) = 1
* dest\_addr (source\_addr) = <digital\_short\_code>

3.      Для символьных сервисных номеров, выделенных для Клиента (только для MT сообщений), используются:

* source\_addr\_ton = 5
* source\_addr\_npi = 0
* source\_addr = <alpha-numeric\_code>