

# Руководство по настройке IPsec VPN-туннеля

# ОГЛАВЛЕНИЕ

<b>Глава 1.</b>	<b>Обзор.....</b>	<b>2</b>
<b>Глава 2.</b>	<b>Перед настройкой .....</b>	<b>3</b>
<b>Глава 3.</b>	<b>Настройка.....</b>	<b>5</b>
3.1	Настройка IPsec VPN-туннеля на TL-WR842ND (Маршрутизатор А) .....	5
3.2	Настройка IPsec VPN-туннеля на TL-ER6120 (Маршрутизатор В) .....	11
3.3	Проверка установленных IPsec-соединений .....	17

# Глава 1. Обзор

**IPsec VPN-туннель** используется для объединения через сеть Интернет двух или более удалённых сетей LAN, чтобы пользователи в различных удалённых сетях LAN могли взаимодействовать друг с другом, как если бы они находились в одной локальной сети.

## Типичная схема сети



\* В данном руководстве в качестве примера используются маршрутизаторы TL-WR842ND (Маршрутизатор А) и TL-ER6120 (Маршрутизатор В)

## Глава 2. Перед настройкой

Перед настройкой IPsec VPN-туннеля вам потребуется:

- Убедиться, что два маршрутизатора подключены к сети Интернет и работают.
- Проверить настройки для создания IPsec VPN-туннеля на обоих маршрутизаторах.

### Проверить настройки для создания IPsec VPN-туннеля на обоих маршрутизаторах:

1. Зайдите в веб-утилиту настройки устройства TL-WR842ND и перейдите на страницу **Status** (*Состояние*).
2. Зайдите в веб-утилиту настройки устройства TL-ER6120 и перейдите на страницу **Network** (*Сеть*) -> **Status** (*Состояние*).

Страница **Status** (Состояние) устройства TL-WR842ND:

**TP-LINK®** 300M Multi-Function Wireless N Router  
Model No. TL-WR842N / TL-WR842ND

**Status**

- Quick Setup
- WPS
- Network
- Wireless
- Guest Network
- DHCP
- VPN
- USB Settings
- Forwarding
- Security
- Parental Control
- Access Control
- Advanced Routing
- Bandwidth Control
- IP & MAC Binding
- Dynamic DNS
- System Tools

**LAN**

MAC Address: 00-0A-EB-13-09-19

**IP Address:** 192.168.1.1

Subnet Mask: 255.255.255.0

Локальная подсеть маршрутизатора А

**Wireless**

Wireless Radio: Enable

Name (SSID): TP-LINK\_130919

Mode: 11bgn mixed

Channel Width: Automatic

Channel: Auto (Current channel 2)

Max Tx Rate: 300Mbps

MAC Address: 00-0A-EB-13-09-19

WDS Status: Disable

**WAN**

MAC Address: 00-0A-EB-13-09-1A

**IP Address:** 10.10.10.101

Subnet Mask: 255.255.255.0

Default Gateway: 10.10.10.101

DNS Server: 8.8.8.8 , 172.31.1.1

Dynamic IP

Release

Страница **Status** (Состояние) устройства TL-ER6120:

**TP-LINK**

TL-ER6120

System Status

**Device Info**

Firmware Version: 1.0.0 Build 20111114 Rel.52682  
Hardware Version: TL-ER6120 v1.0

**System Time**

System Time: 2009-05-26 01:04:03 Tuesday  
Running Time: 3 Day, 2 Hour, 4 Min, 2 Sec

**WAN**

WAN1	Link Up	IP-адрес удалённого шлюза для маршрутизатора А	WAN2	Link Up
Primary Connection:	Dynamic		Primary Connection:	Static IP
Status:	Connected		Status:	Connected
IP Address:	10.10.10.117		IP Address:	116.10.20.28
Subnet Mask:	255.255.255.0		Subnet Mask:	255.255.255.0
Gateway:	10.10.10.1		Gateway:	116.10.20.1
MAC Address:	00-19-60-80-5F-31		MAC Address:	00-19-60-80-5F-32
Secondary Connection:	---		Secondary Connection:	Static IP
Status:	-		Status:	Connected
IP Address:	116.10.20.28		IP Address:	116.10.20.28
Subnet Mask:	255.255.255.0		Subnet Mask:	255.255.255.0

**LAN/DMZ**

Interface	IP Address	Subnet Mask	DHCP Server	MAC Address
LAN	192.168.0.1	255.255.255.0	Enabled	00-00-01-02-03-05

**CPU Usage**

Core	Usage
Core0	1%

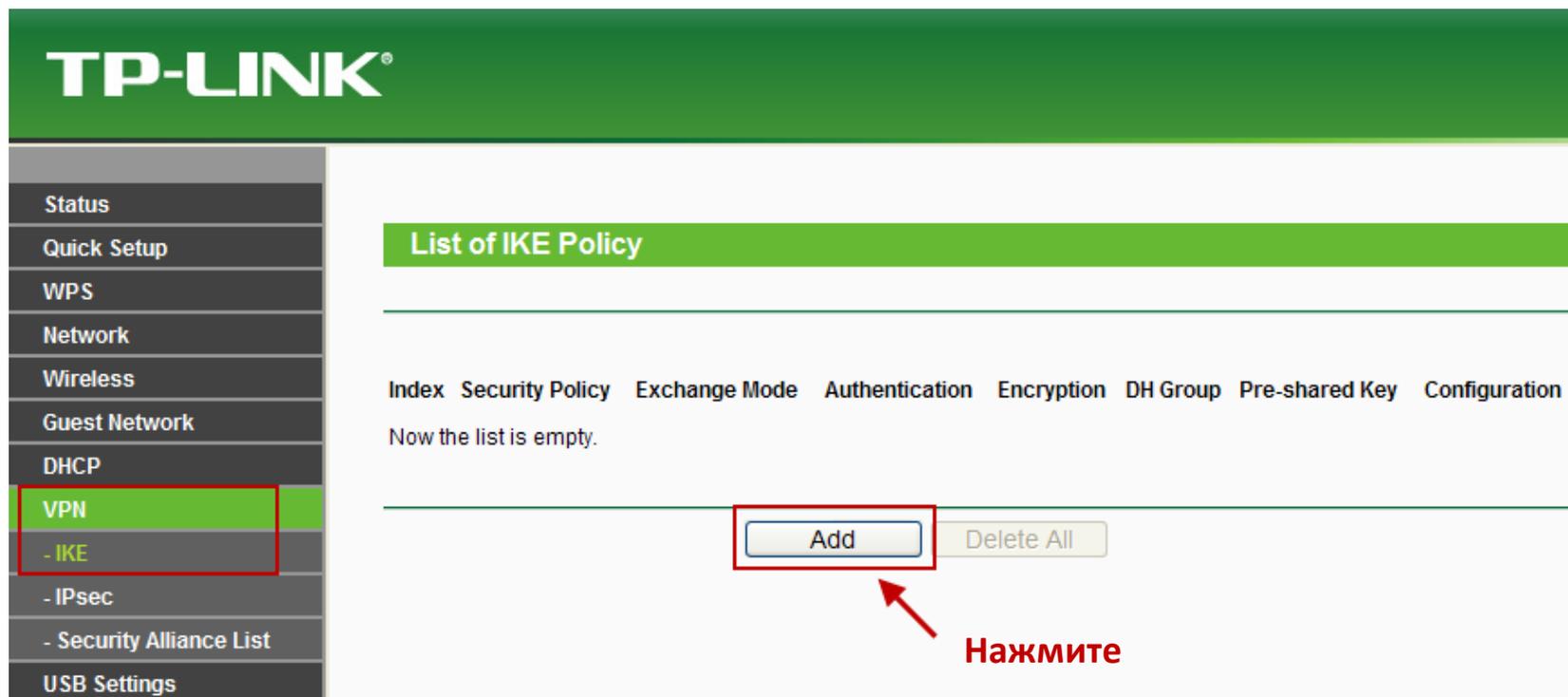
Copyright © 2011 TP-LINK TECHNOLOGIES CO., LTD. All Rights Reserved.

## Глава 3. Настройка

### 3.1 Настройка IPsec VPN-туннеля на устройстве TL-WR842ND (Маршрутизатор А)

**Шаг 1.** Перейдите в веб-утилиту управления устройством TL-WR842ND.

**Шаг 2.** Перейдите на страницу **VPN -> IKE** и нажмите **Add** (Добавить).



**Шаг 3.** Введите **Policy name** (Имя политики) (в данном примере - **Test 1**); выберите **Main mode** (Основной режим), выберите **MD5** в качестве **Authentication Algorithm** (Алгоритм аутентификации), **3DES** в качестве **Encryption Algorithm** (Алгоритм шифрования), **DH2** в качестве **DH Group** (Группа DH); и укажите значение **Pre-shared Key** (Общий ключ) (в данном случае в качестве примера используется слово **secret**). Далее нажмите **Save** (Сохранить).

**TP-LINK®**

**VPN**

- Status
- Quick Setup
- WPS
- Network
- Wireless
- Guest Network
- DHCP
- VPN**
- IKE
- IPsec
- Security Alliance List
- USB Settings
- Forwarding
- Security
- Parental Control

**IKE Policy Settings**

Policy Name:  **Введите**

Exchange Mode:  Main mode  Aggressive mode

Authentication Algorithm:  **Выберите**

Encryption Algorithm:  **Выберите**

DH Group:  **Выберите**

Pre-shared Key:  **Введите**

Lifetime:  seconds(60-604800)

DPD:  enable  disable

**Нажмите**

Шаг 4. Перейдите на страницу **VPN -> IPsec**, затем нажмите **Add** (Добавить).

The screenshot shows the TP-LINK web interface. On the left is a navigation menu with the following items: Status, Quick Setup, WPS, Network, Wireless, Guest Network, DHCP, VPN (highlighted in green), - IKE, - IPsec (highlighted with a red box), - Security Alliance List, USB Settings, Forwarding, Security, and Parental Control. The main content area is titled 'List of IPsec Policy'. Below the title, there are radio buttons for 'IPsec: Enable' and 'Disable' (selected), followed by a 'Save' button. Below this is a table with columns: Index, Name, Local Subnet, Peer Subnet, Negotiation Mode, Status, and Configuration. The table content is 'Now the list is empty.' At the bottom of the table area, there are two buttons: 'Add' (highlighted with a red box) and 'Delete All'. A red arrow points from the 'Add' button to the text 'Нажмите' (Click) written in red.

**Шаг 5.** Введите **Policy name** (Имя политики) (в данном примере - **IPsec 1**). Введите **192.168.1.0 / 24** в поле *Local Subnet* (Локальная подсеть), введите **192.168.0.0 / 24** в поле *Peer Subnet* (Удалённая сеть) (данное значение является локальной подсетью маршрутизатора B), введите **10.10.10.117** в поле *Peer Gateway* (Удалённый шлюз) (данное значение является WAN IP-адресом маршрутизатора B). Выберите **IKE negotiation** (Режим согласования IKE) в поле *Negotiation mode* (Режим согласования), выберите **ESP** в поле *Security Protocol* (Протокол безопасности), выберите **MD5** в поле *Authentication Algorithm* (Алгоритм аутентификации), выберите **3DES** в поле *Encryption Algorithm* (Алгоритм шифрования), выберите **Test 1** в поле *IKE Security Policy* (Политика безопасности IKE), выберите **NONE** (НЕТ) в качестве *PFS Group* (Группа PFS), выберите **Enable** (Включить) в качестве рабочего состояния. Далее нажмите **Save** (Сохранить).

- Status
- Quick Setup
- WPS
- Network
- Wireless
- Guest Network
- DHCP
- VPN**
- IKE
- IPsec
- Security Alliance List
- USB Settings
- Forwarding
- Security
- Parental Control
- Access Control
- Advanced Routing
- Bandwidth Control
- IP & MAC Binding
- Dynamic DNS

**IPsec Policy Settings**

**Введите**

Policy Name: IPsec1

Local Subnet: 192.168.1.0 / 24

Peer Subnet: 192.168.0.0 / 24 **Укажите**

Peer Gateway: 10.10.10.117 (IP or domain name)

Negotiation Mode:  IKE negotiation  Manual mode

Security Protocol: ESP

Authentication Algorithm: MD5 **Выберите**

Encryption Algorithm: 3DES

IKE Security Policy: Test 1 [Click here to add IKE list](#)

PFS Group: NONE

Lifetime: 28800 seconds (60-604800)

Enable: Enable **Выберите**

**Нажмите**

Save Back

**Шаг 6.** Выберите **Enable** (Включить) и нажмите **Save** (Сохранить), чтобы включить IPsec.

**TP-LINK®**

Status  
Quick Setup  
WPS  
Network  
Wireless  
Guest Network  
DHCP  
**VPN**  
- IKE  
- IPsec  
- Security Alliance List  
USB Settings  
Forwarding

**List of IPsec Policy**

Выберите

IPsec:  Enable  Disable  Нажмите

Index	Name	Local Subnet	Peer Subnet	Negotiation Mode	Status	Configuration
1	IPsec 1	192.168.1.0/24	192.168.0.0/24	IKE mode	<input checked="" type="checkbox"/> enable	<a href="#">modify</a> <a href="#">delete</a>

## 3.2 Настройка IPsec VPN-туннеля на TL-ER6120 (Маршрутизатор В)

**Шаг 1.** Перейдите в веб-утилиту настройки устройства TL-ER6120.

**Шаг 2.** Перейдите на страницу **VPN -> IKE -> IKE Proposal** (Предложение IPsec).

**Шаг 3.** Введите *Proposal Name* (Имя предложения) (в данном примере - **Test 2**). Выберите **MD5** в качестве *Authentication Algorithm* (Алгоритм аутентификации), **3DES** в качестве *Encryption Algorithm* (Алгоритм шифрования), **DH2** в качестве *DH Group* (Группа DH). Значения должны совпадать со значениями, указанными для маршрутизатора А. Затем нажмите **Add** (Добавить).

TP-LINK®

TL-ER6120

IKE Policy **IKE Proposal**

**IKE Proposal**

Proposal Name:  ← **Введите**

Authentication:  ← **Выберите (такие же значения, как и для маршрутизатора A)**

Encryption:

DH Group:

**Нажмите**

**List of IKE Proposal**

No.	Name	Auth	Encr	DH	Action
No entries.					

**Шаг 4.** Перейдите на страницу **VPN -> IKE -> IKE Policy** (Политика IKE).

**Шаг 5.** Введите *Policy name* (Имя политики) (в данном примере - **Test 2**). Выберите **Main** (Основной) в качестве *Exchange Mode* (Режим обмена), **IP-адрес** в качестве *Local ID Type* (Тип идентификатора локального узла) и *Remote ID Type* (Тип идентификатора удалённого узла), укажите **Test 2** в качестве *IKE Proposal 1* (IKE Предложение 1); введите **secret** в поле *Pre-shared Key* (Общий ключ) и **28800** в качестве *SA Lifetime* (Период действия SA); значения должны совпадать со значениями маршрутизатора A. Затем нажмите **Add** (Добавить).

- Network
- User Group
- Advanced
- Firewall
- VPN**
  - IKE
  - IPsec
  - L2TP/PPTP
- Services
- Maintenance
- Logout

**IKE Policy**

Policy Name:  **Введите**

Exchange Mode:  Main  Aggressive **Нажмите**

Local ID Type:  IP Address  FQDN **Выберите**

Local ID:

Remote ID Type:  IP Address  FQDN **Выберите**

Remote ID:

IKE Proposal 1:  **Укажите (такие же значения, как и для маршрутизатора A)**

IKE Proposal 2:

IKE Proposal 3:

IKE Proposal 4:

Pre-shared Key:

SA Lifetime:  Sec (60-604800)

DPD:  Enable  Disable

DPD Interval:  Sec (1-300)

**List of IKE Policy**

	No.	Name	Mode	Proposal 1	Proposal 2	Proposal 3	Proposal 4	Action
<input type="checkbox"/>	1	Test 2	Main	Test 2	----	----	----	 

**Шаг 6.** Перейдите на страницу **VPN -> IPsec -> IPsec Proposal** (Предложение IPsec).

**Шаг 7.** Введите *Proposal Name* (Имя предложения) (в данном примере - **IPsec 2**). Выберите **ESP** в поле *Security Protocol* (Протокол безопасности), **MD5** в качестве *ESP Authentication* (ESP Аутентификация), **3DES** в качестве *ESP Encryption* (ESP Шифрование); значения должны совпадать со значениями маршрутизатора А. Затем нажмите **Add** (Добавить).

**TP-LINK®**

TL-ER6120

IPsec Policy **IPsec Proposal** IPsec SA

**Network**

User Group

Advanced

Firewall

**VPN**

- IKE
- IPsec**
- L2TP/PPTP

Services

Maintenance

Logout

**IPsec Proposal**

Proposal Name:

Security Protocol:

ESP Authentication:

ESP Encryption:

**Нажмите**

**Введите**

**Укажите (такие же значения, как и для маршрутизатора А)**

Add

Clear

Help

**List of IPsec Proposal**

No.	Name	Protocol	AH Auth	ESP Auth	ESP Encr	Action
<input type="button" value="Select All"/> <input type="button" value="Delete"/> <input type="button" value="Search"/>						

**Шаг 8.** Перейдите на страницу **VPN -> IPsec -> IPsec Proposal** (Предложение IPsec).

**Шаг 9.** Введите *Policy name* (Имя политики) (в данном примере - **IPsec 2**). Выберите **LAN-to-LAN** в качестве режима.

Введите **192.168.0.0 / 24** в поле *Local Subnet* (Локальная подсеть), **192.168.1.0 / 24** в поле *Remote Subnet* (Удалённая подсеть) (данное значение является локальной подсетью маршрутизатора A), введите **10.10.10.101** в поле *Remote Gateway* (Удалённый шлюз) (данное значение является WAN IP-адресом маршрутизатора A).

Выберите **IKE** в поле *Policy Mode* (Режим политики), **Test 2** в поле *IKE Policy* (Политика IKE), **IPsec 2** в поле *IPsec Proposal* (Предложение IPsec).

Выберите **NONE** (НЕТ) в поле PFS, укажите **28800** в поле *SA Lifetime* (Период действия SA); значения должны совпадать со значениями маршрутизатора A.

Выберите **Activate** (Включить) в поле *Status* (Состояние).

Нажмите **Add** (Добавить).

**TP-LINK®**

TL-ER6120

IPsec Policy | IPsec Proposal | IPsec SA

**Выберите**

IPsec:  Enable  Disable **Нажмите** →

**IPsec Policy**

Policy Name:  **← Введите**

Mode:  **← Выберите**

Local Subnet:  / 24

Remote Subnet:  / 24 **← Укажите**

WAN:

Remote Gateway:  (IP Address/Domain Name) **← Укажите**

Policy Mode:  IKE  Manual **← Выберите**

IKE Policy:  **← Выберите**

IPsec Proposal 1:

IPsec Proposal 2:

IPsec Proposal 3:

IPsec Proposal 4:

PFS:  **← Выберите/укажите (такие же значения, как и для маршрутизатора A)**

SA Lifetime:  Sec (120-604800)

Status:  Activate  Inactivate

**Нажмите** →

**List of IPsec Policy**

No.	Name	Mode	Local Subnet	Remote Subnet	Policy Mode	Status	Action

**Выберите**

### 3.3 Проверка установленных IPsec-соединений

Шаг 1. Перейдите на страницу **VPN -> Security Alliance List** (Список установленных соединений) веб-утилиты настройки устройства TL-WR842ND, а также на страницу **VPN -> IPsec -> IPsec SA** веб-утилиты настройки устройства TL-ER6120.

**TP-LINK®** 300M Multi-Function Wireless N Router  
Model No. TL-WR842N / TL-WR842ND

**List of Security Alliance**

Index	Name	SPI	Tunnel Initiator	Tunnel Receiver	Security Protocol	AH Auth	ESP Auth	ESP Encr
1	IPsec 1	95514210	10.10.10.117	10.10.10.101	ESP	--	MD5	3DES
2	IPsec 1	125577895	10.10.10.101	10.10.10.117	ESP	--	MD5	3DES

Refresh

TP-LINK®

TL-ER6120

IPsec Policy IPsec Proposal **IPsec SA**

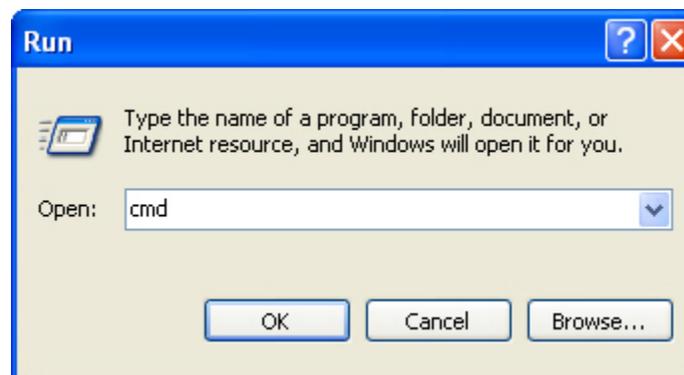
**List of IPsec SA**

No.	Name	SPI	Tunnel	Data Flow	Protocol	AH Auth	ESP Auth	ESP Encr	Status
1	IPsec2	95514210<-> 125577895	10.10.10.117 <-> 10.10.10.101	192.168.0.0/24<-> 192.168.1.0/24	ESP	---	MD5	3DES	Connected

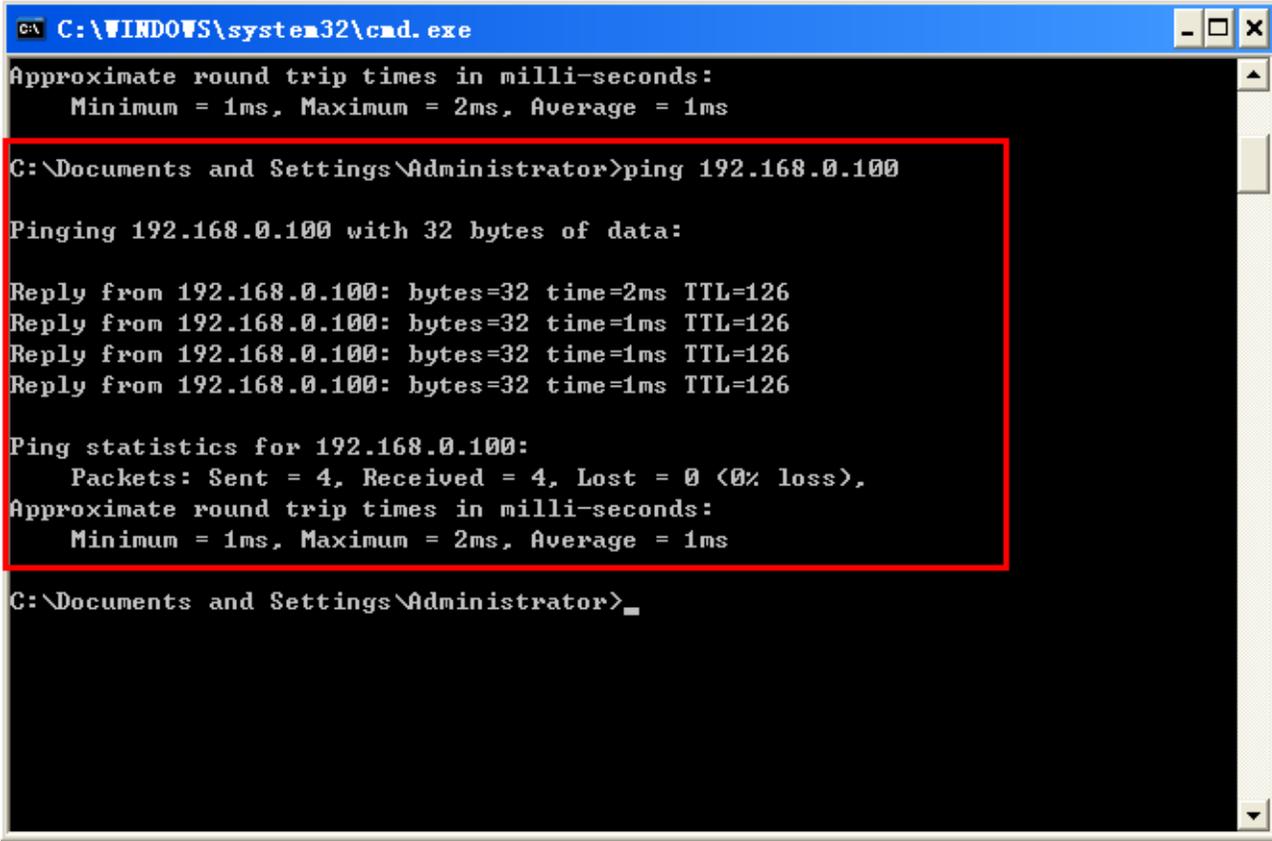
Refresh Search Help

Network  
User Group  
Advanced  
Firewall  
VPN  
• IKE  
• IPsec  
• L2TP/PPTP  
Services  
Maintenance

**Шаг 2.** На компьютере, подключённом к устройству TL-WR842ND, нажмите комбинацию клавиш [Windows] + [R], чтобы запустить окно **Выполнить**, введите **cmd** и нажмите **OK**.



**Шаг 3.** В окне командной строки введите **ping 192.168.0.x** (192.168.0.x может быть IP-адресом любого компьютера, подключённого к TL-ER6120) и затем нажмите клавишу Enter.

A screenshot of a Windows command prompt window. The title bar reads "C:\WINDOWS\system32\cmd.exe". The window content shows the execution of a ping command. The prompt is "C:\Documents and Settings\Administrator>ping 192.168.0.100". The output is: "Pinging 192.168.0.100 with 32 bytes of data: Reply from 192.168.0.100: bytes=32 time=2ms TTL=126 Reply from 192.168.0.100: bytes=32 time=1ms TTL=126 Reply from 192.168.0.100: bytes=32 time=1ms TTL=126 Reply from 192.168.0.100: bytes=32 time=1ms TTL=126 Ping statistics for 192.168.0.100: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 1ms, Maximum = 2ms, Average = 1ms". The prompt ends with "C:\Documents and Settings\Administrator>". A red rectangular box highlights the command and its output.

```
C:\WINDOWS\system32\cmd.exe
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 2ms, Average = 1ms

C:\Documents and Settings\Administrator>ping 192.168.0.100

Pinging 192.168.0.100 with 32 bytes of data:

Reply from 192.168.0.100: bytes=32 time=2ms TTL=126
Reply from 192.168.0.100: bytes=32 time=1ms TTL=126
Reply from 192.168.0.100: bytes=32 time=1ms TTL=126
Reply from 192.168.0.100: bytes=32 time=1ms TTL=126

Ping statistics for 192.168.0.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 2ms, Average = 1ms

C:\Documents and Settings\Administrator>
```

Если программа Ping работает успешно и получит ответ от устройства, подключённого к TL-ER6120, то IPsec соединение работает должным образом.

При возникновении каких-либо проблем при подключении вы можете обратиться в службу технической поддержки компании TP-LINK.