

IPsec VPN Application Guide

CONTENTS

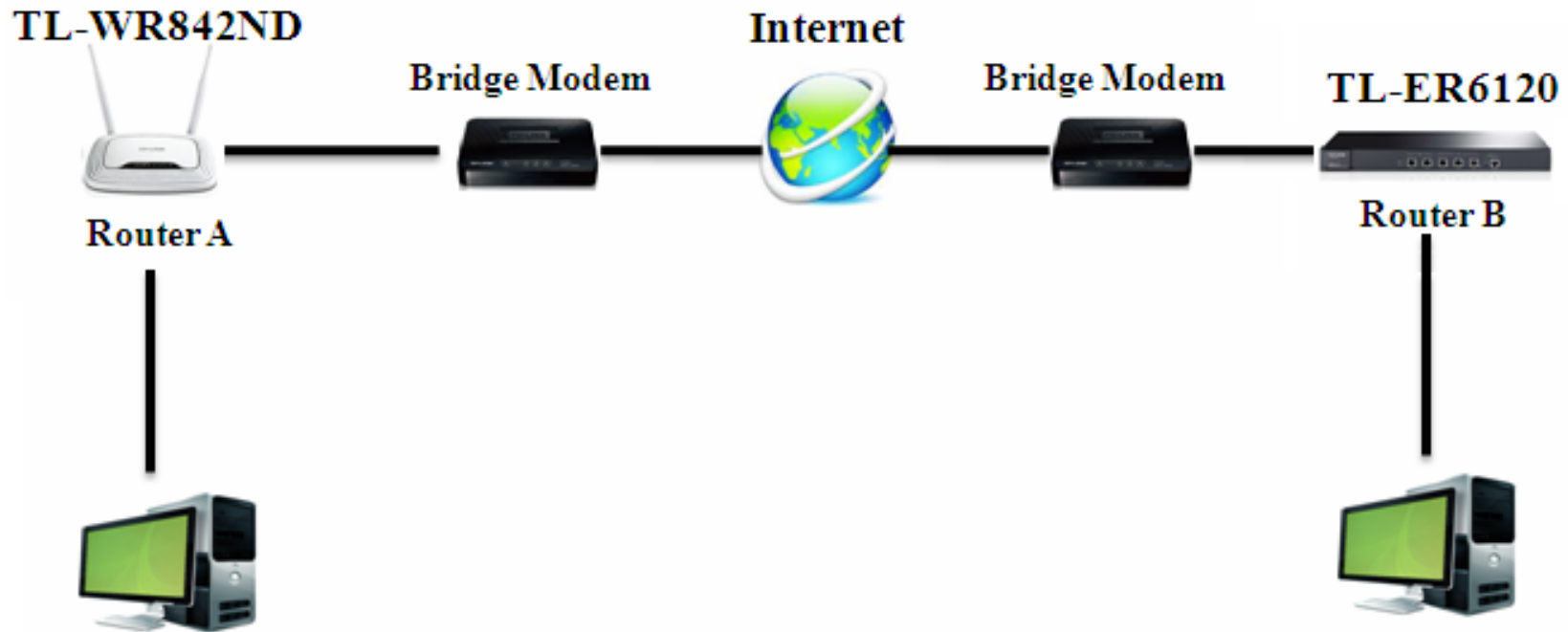
Chapter 1. Overview	1
Chapter 2. Before Configuration	2
Chapter 3. Configuration.....	5
3.1 Configure IPsec VPN on Router A.....	5
3.2 Configure IPsec VPN on Router B.....	10
3.3 Check IPsec Security Alliance	15

Chapter 1. Overview

IPsec VPN is usually built to connect two or more remote LANs via Internet so that hosts in different remote LANs are able to communicate with each other as if they are all in the same LAN.

Note: TL-WR842ND (Router A) and TL-ER6120 (Router B) are used for demonstration in this Guide.

Typical Topology



Chapter 2. Before Configuration

Before setting up an IPsec VPN, you need to:

- Ensure that the two routers are connected to the Internet.
- Verify the settings needed for IPsec VPN on the two routers.

Verify the settings needed for IPsec VPN on the two routers:

1. Log in the management webpage of Router A (TL-WR842ND), then check the Status page.
2. Log in the management webpage of Router B (TL-ER6120), then check the Network -> Status page.

TL-WR842ND's Status Page:

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

Wireless

Wireless Radio:	Enable
Name (SSID):	TP-LINK_0919
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

This is Router A's Local Subnet.

This will be Router B's Remote Gateway IP.

TL-ER6120's Status Page:

The screenshot displays the status page for a TP-LINK TL-ER6120 router. The left sidebar contains navigation links for Network, User Group, Advanced, Firewall, VPN, Services, Maintenance, and Logout. The main content area is divided into several sections:

- System Status:** Includes Device Info (Firmware Version: 1.0.0 Build 20111114 Rel.52682, Hardware Version: TL-ER6120 v1.0) and System Time (2009-05-26 01:04:03 Tuesday, Running Time: 3 Day, 2 Hour, 4 Min, 2 Sec).
- WAN:** Shows two WAN interfaces. WAN1 is configured with a dynamic primary connection, IP 10.10.10.117, and is connected. WAN2 is configured with a static primary connection, IP 116.10.20.28, and is connected. A callout bubble points to the WAN1 IP address, stating "This will be Router A's Remote Gateway IP." Another callout bubble points to the WAN2 IP address, stating "This is Router B's Local Subnet."
- LAN/DMZ:** A table showing LAN interface details:

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:** Shows a bar chart for Core0 with a usage of 1%.

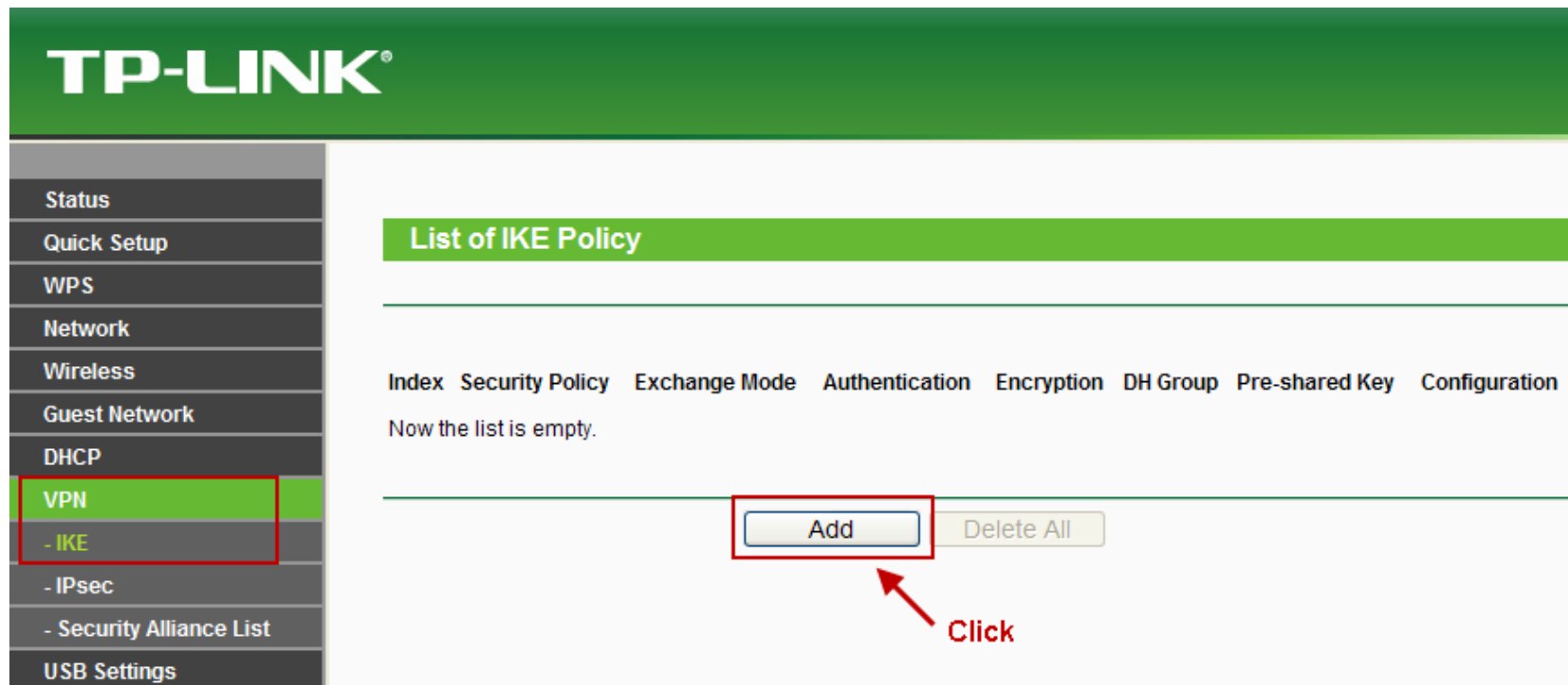
Copyright © 2011 TP-LINK TECHNOLOGIES CO., LTD. All Rights Reserved.

Chapter 3. Configuration

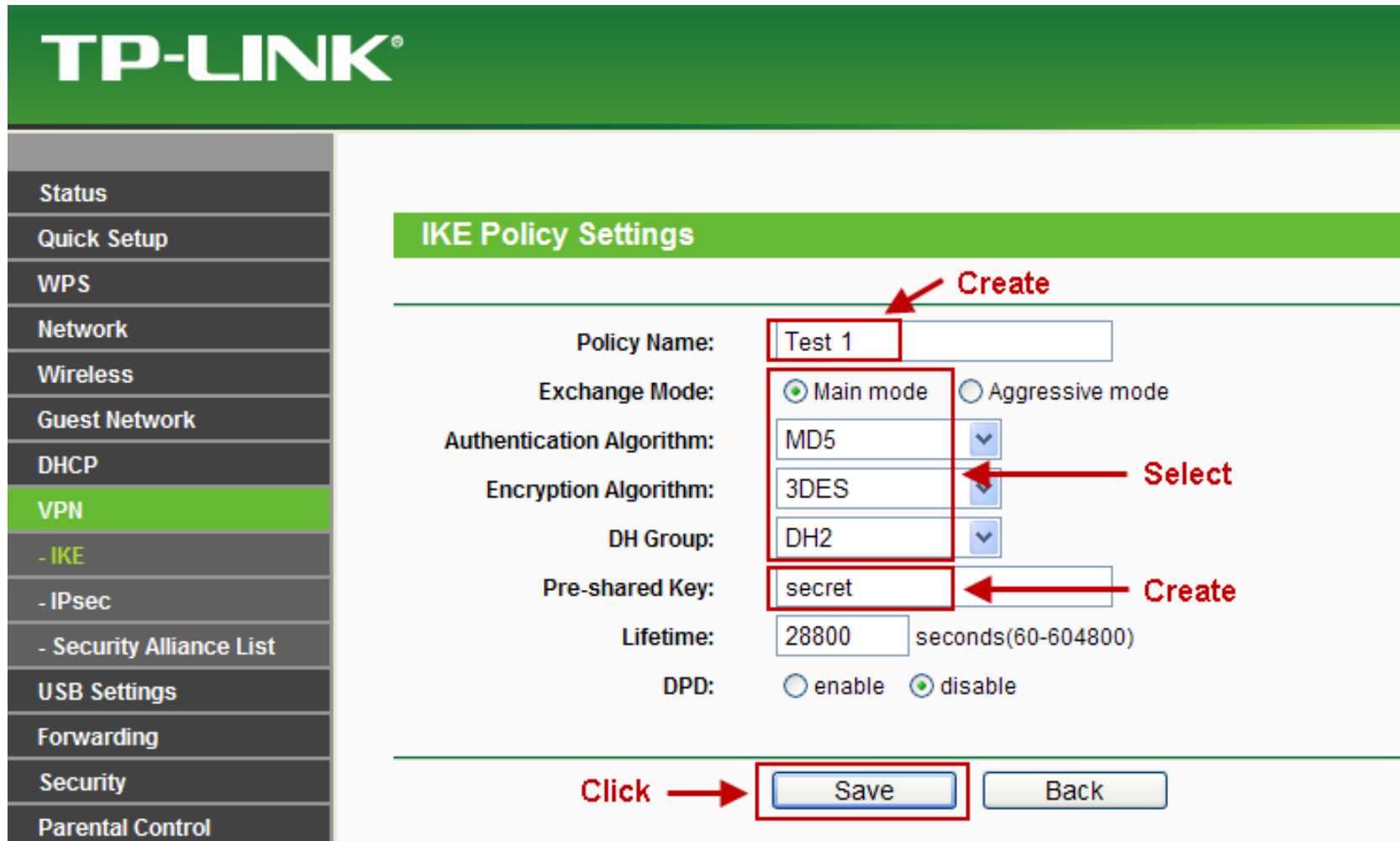
3.1 Configure IPsec VPN on Router A

Step 1. Log in the management webpage of router A (TL-WR842ND).

Step 2. Go to **VPN -> IKE**, click **Add**.



Step 3. Create a Policy Name (here take **Test 1** for example); select **Main mode** as Exchange Mode, **MD5** as Authentication Algorithm, **3DES** as Encryption Algorithm, **DH2** as DH Group; and create a Pre-shared Key (here take **secret** for example). Then click **Save**.



Step 4. Go to VPN -> IPsec, click **Add**.

TP-LINK

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

List of IPsec Policy

IPsec: Enable Disable

Index	Name	Local Subnet	Peer Subnet	Negotiation Mode	Status	Configuration
Now the list is empty.						

Click

Step 5. Create a Policy Name (here take **IPsec 1** for example). Enter **192.168.1.0 / 24** as the Local Subnet, **192.168.0.0 / 24** as the Peer Subnet (it is Router B's Local Subnet), **10.10.10.117** as the Peer Gateway (it is Router B's WAN IP). Select **IKE negotiation** as Negotiation Mode, **ESP** as Security Protocol, **MD5** as Authentication Algorithm, **3DES** as Encryption Algorithm, **Test 1** as IKE Security Policy, **NONE** as PFS Group, **Enable** as the Status. Then click **Save**.

TP-LINK®

IPsec Policy Settings

Create

Policy Name: IPsec1

Local Subnet: 192.168.1.0 / 24

Peer Subnet: 192.168.0.0 / 24 **Enter**

Peer Gateway: 10.10.10.117 (IP or domain name)

Negotiation Mode: IKE negotiation Manual mode

Security Protocol: ESP **Select**

Authentication Algorithm: MD5 **Select**

Encryption Algorithm: 3DES **Select**

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

PFS Group: NONE

Lifetime: 28800 seconds (60-604800)

Enable: Enable **Select**

Save **Back**

Click

Step 6. Check **Enable** and then click **Save** to activate the IPsec.

The screenshot shows the TP-LINK web interface for VPN configuration. On the left is a navigation menu with options: Status, Quick Setup, WPS, Network, Wireless, Guest Network, DHCP, **VPN**, - IKE, - IPsec, - Security Alliance List, USB Settings, and Forwarding. The main content area is titled "List of IPsec Policy". Below the title, there are radio buttons for "IPsec: Enable" and "Disable". The "Enable" radio button is selected and highlighted with a red box and a red arrow labeled "Check". To the right of the radio buttons is a "Save" button, also highlighted with a red box and a red arrow labeled "Click". Below these controls is a table with the following data:

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	modify delete

At the bottom of the table area, there are two buttons: "Add" and "Delete All".

3.2 Configure IPsec VPN on Router B

- Step 1.** Log in the management webpage of router B (TL-ER6120).
- Step 2.** Go to **VPN -> IKE -> IKE Proposal**.
- Step 3.** Create a Proposal Name (here take **Test 2** for example). Select **MD5** as Authentication Algorithm, **3DES** as Encryption Algorithm, **DH2** as DH Group, the same as Router A's. Then click **Add**.

The screenshot displays the TP-LINK management interface for router TL-ER6120. The 'VPN' menu item is highlighted in the left sidebar. The 'IKE Proposal' configuration page is active, showing the following fields:

- Proposal Name: (Annotated with 'Create')
- Authentication: (Annotated with 'Select')
- Encryption: (Annotated with 'Select')
- DH Group: (Annotated with '(the same as Router A's)')

On the right side, there are three buttons: (Annotated with 'Click'), , and .

Below the configuration form is a table titled 'List of IKE Proposal':

No.	Name	Auth	Encr	DH	Action
No entries.					

At the bottom of the table, there are three buttons: , , and .

Step 4. Go to **VPN -> IKE -> IKE Policy**. Create a Policy Name (here take **Test 2** for example). Select **Main** as Exchange Mode, **IP Address** as Local ID Type and Remote ID Type, **Test 2** as IKE Proposal 1; enter **secret** as Pre-shared Key, and **28800** as SA Lifetime, the same as Router A's. Then click **Add**.

TP-LINK
TL-ER6120

IKE Policy | IKE Proposal

IKE Policy

Policy Name: ← **Create**

Exchange Mode: Main Aggressive ← **Select**

Local ID Type: IP Address FQDN ← **Select**

Local ID:

Remote ID Type: IP Address FQDN ← **Select**

Remote ID:

IKE Proposal 1: ← **Select**

IKE Proposal 2:

IKE Proposal 3:

IKE Proposal 4:

Pre-shared Key: ← **Enter (the same as Router A's)**

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	----	----	----	

Select All | Delete | Search

Step 5. Go to **VPN -> IPsec -> IPsec Proposal**.

Step 6. Create a Proposal Name (here take **IPsec 2** for example). Select **ESP** as Security Protocol, **MD5** as ESP Authentication, **3DES** as ESP Encryption, the same as Router A's. Then click **Add**.

The screenshot shows the TP-LINK web interface for configuring an IPsec Proposal. The 'IPsec Proposal' tab is active. The configuration fields are as follows:

- Proposal Name: IPsec 2
- Security Protocol: ESP
- ESP Authentication: MD5
- ESP Encryption: 3DES

The 'Add' button is highlighted with a red box and an arrow pointing to it with the text "Click". A red arrow points to the "IPsec 2" field with the text "Create". Another red arrow points to the dropdown menus with the text "Select (the same as Router A's)".

Below the configuration is a table titled "List of IPsec Proposal" with the following columns: No., Name, Protocol, AH Auth, ESP Auth, ESP Encr, and Action. At the bottom of the table are buttons for "Select All", "Delete", and "Search".

Step 7. Go to **VPN -> IPsec -> IPsec Proposal**.

Step 8. Create a Policy Name (here take **IPsec 2** for example). Select **LAN-to-LAN** as the Mode.

- 1) Enter **192.168.0.0 / 24** as the Local Subnet, **192.168.1.0 / 24** as the Remote Subnet (it is Router A's Local Subnet),

10.10.10.101 as the Remote Gateway (it is Router A's WAN IP).

- 2) Select **IKE** as Policy Mode, **Test 2** as IKE Policy, **IPsec 2** as IPsec Proposal.
- 3) Select **NONE** as PFS, and enter **28800** for SA Lifetime, which are the same as Router A's.
- 4) Check **Activate** for the Status.
- 5) Click **Add**.
- 6) Check **Enable** and then click **Save** to activate the IPsec.

TP-LINK

TL-ER6120

IPsec Policy
IPsec Proposal
IPsec SA

General

 Enable Disable
 Click → Save

IPsec Policy

Policy Name: IPsec 2 ← Create
Click → Add

Mode: LAN-to-LAN ← Select
Clear

Local Subnet: 192.168.0.0 / 24

Remote Subnet: 192.168.1.0 / 24

WAN: WAN1

Remote Gateway: 10.10.10.101 (IP Address/Domain Name) ← Enter

Policy Mode: IKE Manual ← Select

IKE Policy: Test 2

IPsec Proposal 1: IPsec 2

IPsec Proposal 2: ----

IPsec Proposal 3: ----

IPsec Proposal 4: ----

PFS: NONE ← Select / Enter (the same as Router A's)

SA Lifetime: 28800 Sec (120-604800)

Status: Activate Inactivate

List of IPsec Policy

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

Select All
Activate
Inactivate
Delete
Search

3.3 Check IPsec Security Alliance

Step 1. Check the **VPN -> Security Alliance List** page of TL-WR842ND as well as the **VPN -> IPsec -> IPsec SA** page of TL-ER6120.

The screenshot shows the configuration interface of a TP-LINK 300M Multi-Function Wireless N Router. The left sidebar contains a menu with options: Status, Quick Setup, WPS, Network, Wireless, DHCP, VPN (highlighted), - IKE, - IPsec, - Security Alliance List, USB Settings, Forwarding, Security, and Parental Control. The main content area is titled 'List of Security Alliance' and displays a table with the following data:

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

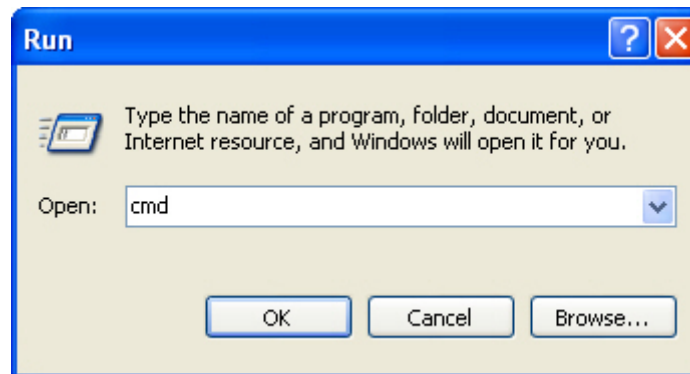
Below the table is a 'Refresh' button.

The screenshot shows the TP-LINK web interface for device TL-ER6120. The 'IPsec SA' tab is selected. A table titled 'List of IPsec SA' displays the following data:

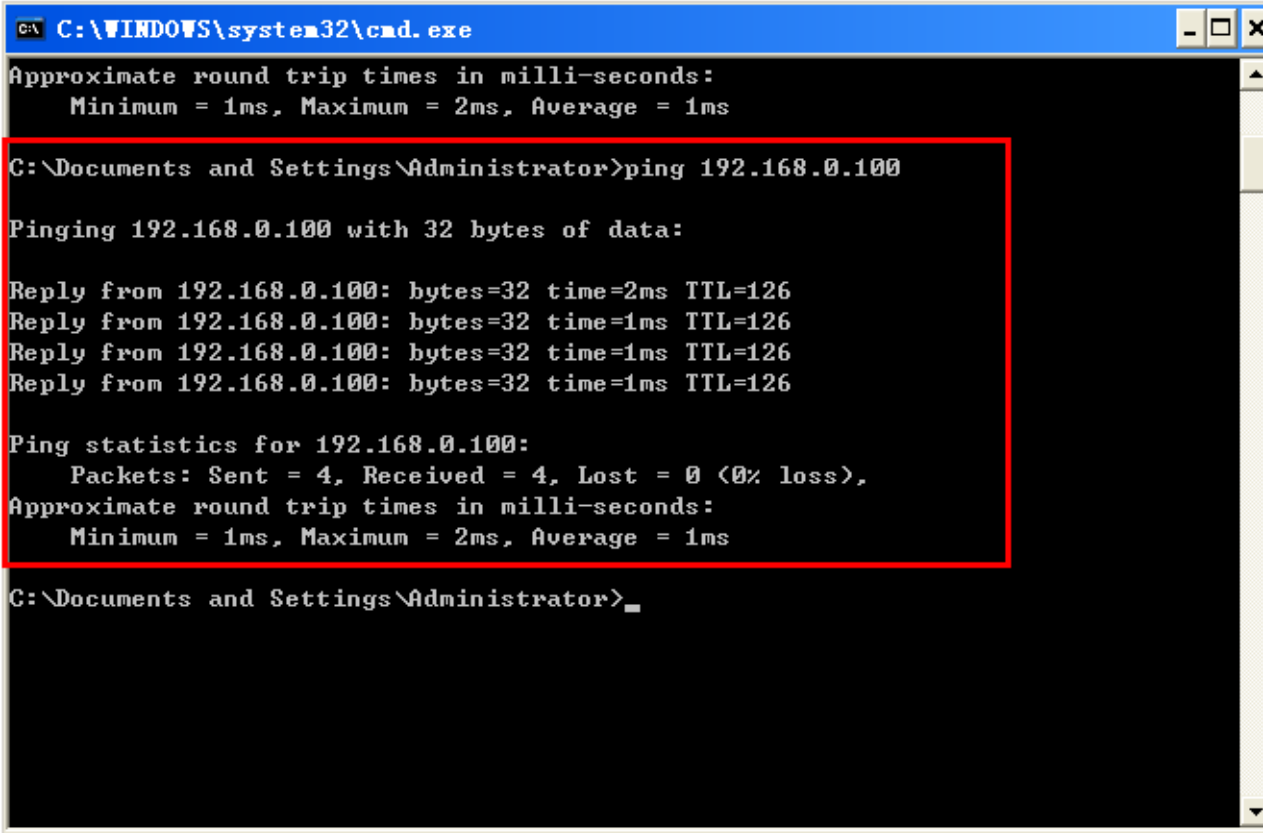
No.	Name	SPI	Tunnel	Data Flow	Protocol	AH Auth	ESP Auth	ESP Encr	Status
1	IPsec2	95514210<-> 125577895	10.10.10.117 <-> 10.10.10.101	192.168.0.0/24<-> 192.168.1.0/24	ESP	---	MD5	3DES	Connected

Below the table are buttons for 'Refresh', 'Search', and 'Help'. A left-hand navigation menu includes options like Network, User Group, Advanced, Firewall, VPN (with sub-items IKE and IPsec), L2TP/PPTP, Services, and Maintenance.

Step 2. On a host under TL-WR842ND, press [Windows Logo] + [R] to open **Run** dialog, input **cmd** and click **OK**.



Step 3. In the CLI window, type in **ping 192.168.0.x** (192.168.0.x can be IP address of any host in TL-ER6120), and then press [Enter].



```
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>_
```

If Ping proceeds successfully and gets replies from the host in TL-ER6120, the IPsec connection must be working properly now. If there are any further problems, please feel free to contact our TP-LINK technical support.