Chapter 1. Overview .................................................................................... 1

Chapter 2. Before Configuration .............................................................. 2

Chapter 3. Configuration.............................................................................. 5

3.1 Configure IPsec VPN on TL-WR842ND (Router A) ................................................................. 5

3.2 Configure IPsec VPN on TL-ER6120 (Router B) ................................................................. 10

3.3 Check IPsec Security Alliance ......................................................................................... 16
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.

**Typical Topology**

* Here we use TL-WR842ND (Router A) and TL-ER6120 (Router B) for example.
Chapter 2. Before Configuration

Before setting up an IPsec VPN, you need to

- Ensure that the two routers are connected to the Internet, actively.
- 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 TL-WR842ND’s management webpage, then check on the Status page.
2. Log in TL-ER6120’s management webpage, then check on the Network -> Status page.
Before Configuration

TL-WR842ND's Status Page:

- This is Router A's Local Subnet.

- This will be Router B's Remote Gateway IP.
Before Configuration

TL-ER6120's Status Page:

**System Status**
- Firmware Version: 1.0.0 Build 20111114 Rel.52532
- 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**
- WAN 1 Link Up
  - Primary Connection: Dynamic
  - Status: Connected
  - IP Address: 10.10.10.117
  - Subnet Mask: 255.255.255.0
  - Gateway: 10.10.10.1
  - MAC Address: 00-19-60-60-5f-31
- WAN 2 Link Up
  - Primary Connection: Static IP
  - Status: Connected
  - IP Address: 116.19.20.28
  - Subnet Mask: 255.255.255.0
  - Gateway: 116.10.20.1
  - MAC Address: 00-19-60-60-5f-32

**LAN/DMZ**
- LAN
  - IP Address: 192.168.0.1
  - Subnet Mask: 255.255.255.0
  - DHCP Server: Enabled
  - MAC Address: 00-00-01-02-03-05

**CPU Usage**
- Core 0
  - Usage: 1%
Chapter 3. Configuration

3.1 Configure IPsec VPN on TL-WR842ND (Router A)

Step 1. Log in the management webpage of 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.

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.
### IPsec Policy Settings

- **Policy Name:** `IPsec1`
- **Local Subnet:** `192.168.1.0 / 24`
- **Peer Subnet:** `192.168.0.0 / 24`
- **Peer Gateway:** `10.10.10.117`
- **Negotiation Mode:** `IKE negotiation`
- **Security Protocol:** `ESP`
- **Authentication Algorithm:** `MD5`
- **Encryption Algorithm:** `3DES`
- **IKE Security Policy:** `Test 1`
- **PFS Group:** `NONE`
- **Lifetime:** `28800 seconds (60-604800)`
- **Enable:** `Enable`

**Actions:**
- **Create:**
- **Enter:**
- **Select:**
- **Click to add IKE list:**
- **Select:**
- **Click:**
Step 6. Check **Enable** and then click **Save** to activate the IPsec.
3.2 Configure IPsec VPN on TL-ER6120 (Router B)

Step 1. Log in the management webpage of 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.
Step 4. Go to VPN -> IKE -> IKE Policy.

Step 5. 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.
### IKE Policy

**Policy Name:** Test 2

**Exchange Mode:** Main

**Local ID Type:** IP Address

**Local ID:** Local WAN IP

**Remote ID Type:** IP Address

**Remote ID:** Remote Gateway IP

**IKE Proposal 1:** Test 2

**Pre-shared Key:** secret

**SA Lifetime:** 28800 Sec (60-604800)

**DPD:** Enable

**DPD Interval:** 10 Sec (1-300)

### List of IKE Policy

<table>
<thead>
<tr>
<th>No.</th>
<th>Name</th>
<th>Mode</th>
<th>Proposal 1</th>
<th>Proposal 2</th>
<th>Proposal 3</th>
<th>Proposal 4</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Test 2</td>
<td>Main</td>
<td>Test 2</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Step 7. 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**.

Step 9. Create a Policy Name (here take **IPsec 2** for example). Select **LAN-to-LAN** as the Mode.

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).

Select **IKE** as Policy Mode, **Test 2** as IKE Policy, **IPsec 2** as IPsec Proposal.

Select **NONE** as PFS, and enter **28800** for SA Lifetime, which are the same as Router A's.

Check **Activate** for the Status.

Click **Add**.

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

![List of Security Alliance](image)

<table>
<thead>
<tr>
<th>Index</th>
<th>Name</th>
<th>SPI</th>
<th>Tunnel Initiator</th>
<th>Tunnel Receiver</th>
<th>Security Protocol</th>
<th>AH Auth</th>
<th>ESP Auth</th>
<th>ESP Encr</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>IPsec1</td>
<td>05514210</td>
<td>10.10.10.117</td>
<td>10.10.10.101</td>
<td>ESP</td>
<td>--</td>
<td>MD5</td>
<td>3DES</td>
</tr>
<tr>
<td>2</td>
<td>IPsec2</td>
<td>125577805</td>
<td>10.10.10.101</td>
<td>10.10.10.117</td>
<td>ESP</td>
<td>--</td>
<td>MD5</td>
<td>3DES</td>
</tr>
</tbody>
</table>
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].

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.