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
Before Configuration

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.
Before Configuration

TL-WR842ND’s Status Page:

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

This is Router A’s Local Subnet.

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

TL-ER6120's Status Page:

**WAN**

**WAN1**
- **Link Up**: 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**: 00-19-60-80-5F-31
- **Secondary Connection**: ---
- **Status**: 
- **IP Address**: 116.10.20.23
- **Subnet Mask**: 255.255.255.0

**WAN2**
- **Link Up**: Up
- **Primary Connection**: Static IP
- **Status**: Connected
- **IP Address**: 116.10.20.28
- **Subnet Mask**: 255.255.255.0
- **Gateway**: 116.10.20.1
- **MAC Address**: 00-19-60-80-5F-32
- **Secondary Connection**: Static IP
- **Status**: Connected
- **IP Address**: 116.10.20.28
- **Subnet Mask**: 255.255.255.0

**LAN/DMZ**

<table>
<thead>
<tr>
<th>Interface</th>
<th>IP Address</th>
<th>Subnet Mask</th>
<th>DHCP Server</th>
<th>MAC Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>LAN</td>
<td>192.168.0.1</td>
<td>255.255.255.0</td>
<td>Enabled</td>
<td>00-00-01-02-03-05</td>
</tr>
</tbody>
</table>

**CPU Usage**

<table>
<thead>
<tr>
<th>Core</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1%</td>
</tr>
</tbody>
</table>
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.
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.
Step 6. Check **Enable** and then click **Save** to activate the IPsec.
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.
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.
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.

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.
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>IPSec</td>
<td>95514210</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>IPSec</td>
<td>125577395</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.