Preface

Thanks for choosing UrsalinkVPN. As a web-based VPN monitoring and management platform, UrsalinkVPN establishes a virtual private network for communications between users and devices to offer a highly reliable, efficient and secure solution for connecting to machines remotely.

This guide teaches you how to configure and operate the UrsalinkVPN. You can refer to it for detailed functionality and configuration.

© 2017-2020 Xiamen Ursalink Technology Co., Ltd.

All rights reserved.

All information in this user guide is protected by copyright law. Whereby, no organization or individual shall copy or reproduce the whole or part of this user guide by any means without written authorization from Xiamen Ursalink Technology Co., Ltd.

Related Documents

<table>
<thead>
<tr>
<th>Document</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>UrsalinkVPN Datasheet</td>
<td>Datasheet for the UrsalinkVPN.</td>
</tr>
</tbody>
</table>

For assistance, please contact

Ursalink technical support:

Email: support@ursalink.com

Tel.: 86-592-5023060

Fax: 86-592-5023065

Revision History

<table>
<thead>
<tr>
<th>Date</th>
<th>Doc Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Aug. 29, 2018</td>
<td>V.1.0.0</td>
<td>Initial version</td>
</tr>
<tr>
<td>Mar. 25, 2020</td>
<td>V.1.2.0</td>
<td>Optimize the installation step according to version 1.0.17 of Ursalink VPN</td>
</tr>
</tbody>
</table>
Content

Chapter 1 Product Introduction

1.1 Overview

1.2 Advantage

Chapter 2 Installation

2.1 Pre-installation Checklist

2.2 Installation Steps

Chapter 3 Configuration

3.1 Device

3.2 Control

3.3 VPN

3.4 Certificate

3.5 Account

3.6 Tool

Chapter 4 Application Example

4.1 System Topology

4.2 Connecting Router with UrsalinkVPN

4.2.1 Network Access

4.2.2 Router Configuration

4.3 Connecting Control Station with UrsalinkVPN

4.3.1 Install OpenVPN on Windows

4.3.2 Generate Certificate from UrsalinkVPN

4.3.3 Running OpenVPN On Windows

4.3.4 Communication Test
Chapter 1 Product Introduction

1.1 Overview

UrsalinkVPN, based on WEB service design, addresses the increasing demand for bandwidth and wireless remote data access and establishes a secure and reliable VPN tunnel for users and remote devices to ensure the security of data transmission. It also solves the problem of the lack of public network IP for routers in mobile cellular network, and implements local direct access to remote devices.

1.2 Advantage

Benefits

- Fast VPN Connection
- Security and Remote Access
- Support Multiple Control Stations Connection
- Real-time Connection Status
- Real-time Remote Configuration
- Up to 1000 Devices Connection
- Visualized Page Management
Chapter 2 Installation

2.1 Pre-installation Checklist

Ubuntu 16.04 Server (64bit)

Supported browsers: Chrome, Firefox

2.2 Installation Steps

1. You can try this command to install it automatically: “

```
wget http://resource.ursalink.com/software/UrsalinkVPN/ursalinkvpn_install.sh && chmod +x ursalinkvpn_install.sh && /ursalinkvpn_install.sh
```

Or install it manual step by step. Try to download the scripts “ursalinkvpn_install.sh” to install through this link:

http://resource.ursalink.com/software/UrsalinkVPN/ursalinkvpn_install.sh, or download the package from https://www.ursalink.com/en/software-download containing “ursalink_vpn_md5” and “ursalink_vpn_amd64.deb”. Then upload these two files to Ubuntu server.

```
root@Base:~ ls
dump.rdb  ursalink_vpn_amd64.deb  ursalinkvpn_install.sh  ursalink_vpn_md5
root@Base:~
root@Base:~
root@Base:~
root@Base:~
```

2. Access the folder where you upload the two files, and execute the shell commands

```
# chmod +x ursalinkvpn_install.sh

#.ursalinkvpn_install.sh
```

```
root@Base:~# chmod +x ursalinkvpn_install.sh
root@Base:~# ./ursalinkvpn_install.sh
```

3. Execute dpkg scripts

```
# dpkg -i ursalinkvpn_install.sh
```
It might take about 10 minutes to complete the installation

4. Log in VPN Server through this link: [https://ip:18443](https://ip:18443) or [http://ip:18080](http://ip:18080)

   Default username: admin

   Default password: password
Chapter 3 Configuration

3.1 Device

Display the information about devices connected to UrsalinkVPN. You can modify the Name and Remote Subnet when the subnet allocation method is manual.

![Figure 3-1-1](image)

### Device Information

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Show the name of device</td>
</tr>
<tr>
<td>Status</td>
<td>Show the status of device</td>
</tr>
<tr>
<td>Serial Number</td>
<td>Show the serial number of device</td>
</tr>
<tr>
<td>Virtual IP</td>
<td>Show the virtual IP of device</td>
</tr>
<tr>
<td>Real IP</td>
<td>Show the IP address of device’s WAN port</td>
</tr>
<tr>
<td>Remote subnet</td>
<td>Show the segment and mask of the virtual IP addresses</td>
</tr>
</tbody>
</table>

Table 3-1-1 Device Information
### 3.2 Control

![URSALINK Control Interface]

**Figure 3-2-1**

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Show the name of control station</td>
</tr>
<tr>
<td>Status</td>
<td>Show the status of control station</td>
</tr>
<tr>
<td>Virtual IP</td>
<td>Show the virtual IP of control station</td>
</tr>
<tr>
<td>Real IP</td>
<td>Show the IP address of control station’s WAN port</td>
</tr>
<tr>
<td>Time</td>
<td>Show the connect time of the control station.</td>
</tr>
</tbody>
</table>

*Table 3-2-1 Control Information*
3.3 VPN

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Listen</td>
<td>Enter the IP address of the UrsalinkVPN.</td>
<td>Null</td>
</tr>
<tr>
<td>Protocol</td>
<td>Select communication protocol (TCP/UDP).</td>
<td>UDP</td>
</tr>
<tr>
<td>Port</td>
<td>Service port</td>
<td>1194</td>
</tr>
<tr>
<td>Client Subnet</td>
<td>Set the segment and the mask of the virtual addresses pool.</td>
<td>10.8.0.0/16</td>
</tr>
<tr>
<td>Subnet Allocation</td>
<td>Select from Manual or Auto options</td>
<td>Null</td>
</tr>
</tbody>
</table>
### Table 3-3-1 Control Information

| Method               | Manual: Modify remote subnet manually from the device menu  
| Auto: Configure router’s IP address via “Subnet Behind Client” |
|----------------------|-------------------------------------------------------------|
| Subnet Behind Client | Configure router’s DHCP Server                              
| Ping Interval        | Set the Ping interval (in second)                           
| Ping Restart         | Reconnection interval (in second)                           
| Compression          | Select from: “None”and”LZO”.  
|                      | LZO: Lempel-Ziv-Oberhumer (or LZO) is a lossless algorithm that compresses data to ensure high decompression speed |
| Encryption           | Select from “NONE”, “BF-CBC”, “DES-EDE3-CBC”, “AES-128-CBC”, “AES-192-CBC” and “AES-256-CBC” |
| Authorization Code   | Input the Authorization Code for routers (5 to 31 alphanumeric combinations) |

**3.4 Certificate**

You can create and download a certification on this page.

![Certificate Page](image)

**Figure 3-4-1**
Note that always use a unique certificate name for each client.

3.5 Account

You can edit the information about user account on this page.

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Certificate Name</td>
<td>Generate a certificate for the control station</td>
<td>Null</td>
</tr>
</tbody>
</table>

Table 3-4-1 Certificate Information

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Username</td>
<td>Enter a new username. You can use characters such as a-z, 0-9, &quot;_&quot;, &quot;,&quot;, &quot;$&quot;. The first character can't be a number.</td>
</tr>
<tr>
<td>Old Password</td>
<td>Enter the old password.</td>
</tr>
<tr>
<td>New Password</td>
<td>Enter a new password.</td>
</tr>
<tr>
<td>Confirm New Password</td>
<td>Enter the new password again.</td>
</tr>
</tbody>
</table>

Table 3-5-1 Account Information
3.6 Tool

Detective tool of Ping to detect the connections between the VPN Server, routers and control stations.

![Tool Image](image.png)

**Figure 3-6-1**

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ping IP Address</td>
<td>Destination address</td>
</tr>
</tbody>
</table>

Table 3-6-1 Tool Information

---

### Chapter 4 Application Example

#### 4.1 System Topology

![Diagram](image.png)

1. UrsalinkVPN works as OpenVPN server.
**Note** that OpenVPN server needs to have Public IP or uses DDNS.

2. The routers work as OpenVPN client and connect with UrsalinkVPN. And routers should be able to access the network.

3. The control station can be a laptop or other devices work as OpenVPN clients. After establishing connection with the UrsalinkVPN, control station can remote access to the devices that connected with the routers.

### 4.2 Connecting Router with UrsalinkVPN

Routers can connect to the UrsalinkVPN platform via cellular network, Wi-Fi, or Ethernet. This example mainly introduces the connection of router to the UrsalinkVPN platform via cellular network.

#### 4.2.1 Network Access

1. Install antennas and SIM card, and then power on the router.

2. Log in to the Web GUI.

   Ursalink router provides web-based configuration interface for device management. If this is the first time you configure the router, please use the default settings below:

   **IP Address:** 192.168.1.1

   **Username:** admin

   **Password:** password
3. Go to “Status->Overview”. Check the current firmware version of the router.
   Note that the firmware version should be higher than x.2.0.6.

4. Go to “Network > Interface > Cellular > Cellular Setting” and configure the APN information.

5. Go to “Status/Cellular” to check the cellular network status, also you can use the network detective tool “Ping” under the menu “Maintenance/tools/Ping”
   For more details, you can refer to our online video tutorial from the below link
   https://www.ursalink.com/academy-ursalink-course.lesson-1

4.2.2 Router Configuration

1. Go to “System->Device Management -> UrsalinkVPN - > UrsalinkVPN Setting”. Input the IP address or Domain Name of UrsalinkVPN.

   ![Router Configuration Image]

2. Input service port.
   Note that service port should be the same as the one configured on UrsalinkVPN.

3. Input the authorization code generated by UrsalinkVPN.

4. Input the device name, then click the Connect button.

5. Check the Connection Status of UrsalinkVPN, and go to “System->Device Management -> Ursalink VPN - > UrsalinkVPN Status”
Note that time synchronization is needed between UrsalinkVPN and routers.

4.3 Connecting Control Station with UrsalinkVPN

4.3.1 Install OpenVPN on Windows

1. OpenVPN source code and Windows installers can be downloaded from the below link:
   
2. License Agreement.

3. Make sure “OpenVPN RSA Certificate Management Scripts” has been checked.

4. Choose install location and click Install. Wait for the Installation to complete.
5. Click "Finish" to complete installation.

4.3.2 Generate Certificate from UrsalinkVPN

1. Log in UrsalinkVPN

2. Go to “Certificate”, input certificate name, and then click to Create&Download x.509 certificate.

   Note that always use a unique certificate name for each client.
4.3.3 Running OpenVPN On Windows

1. Copy Certificate to the machine if needed and place the certificate under “OpenVPN/config” as show below.

2. Running OpenVPN

4.3.4 Communication Test

1. Router connection status
   
   Virtual IP : 10.8.0.10
   
   Subnet : 192.168.1.0

2. Control station connection status
3. Testing the communication between Control station and router

-End-