



IR600 & IR900

OpenVPN Guide

Version V1.0-EN Date: March, 2020



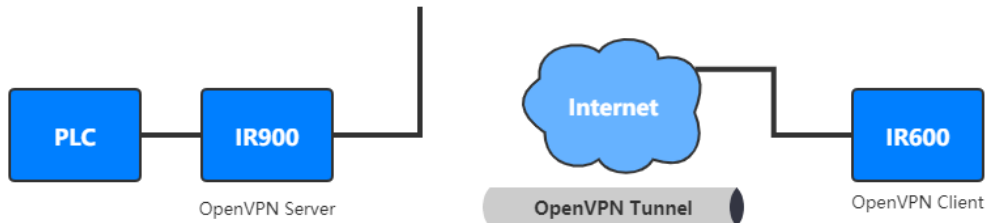
InHand Networks
Global Leader in Industrial IoT

Content

1. Abstract	1
2. Configuration	1
2.1 Server Configuration	1
2.2 Client Configuration	3
3. Verify	5
3.1 Verify OpenVPN Server	5
3.2 Verify OpenVPN Client.....	5

1. Abstract

This guide will show how to configure an OpenVPN Tunnel between an IR600 device and an IR900 device. Here we use IR600 for the OpenVPN Client and IR900 for OpenVPN Server. The authentication of the OpenVPN tunnel is selected as X.509.



2. Configuration

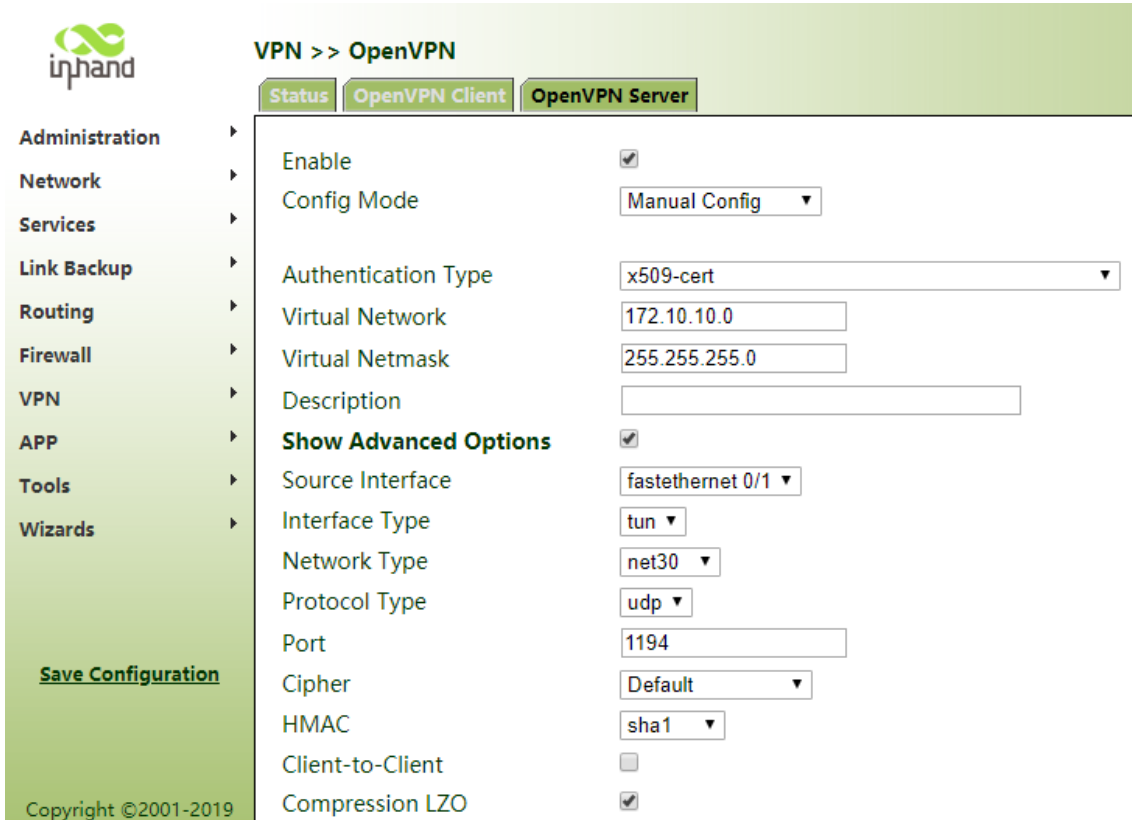
Before doing the server configuration, please make sure the both the server and the client for OpenVPN can access public network.

2.1 Server Configuration

For the OpenVPN Server, you need to make sure the server has a fixed IP address or a fixed DNS.

Step 1: Add a new OpenVPN server tunnel.

Click **"VPN >> OpenVPN"** to enter the **OpenVPN Server** page.



- 1) Select **Config Mode** as **Manual Config**.
- 2) Select **Authentication Type** as **X.509 Cert**.
- 3) Set the **Virtual Network** alternatively.
- 4) Select the **Source Interface**. Cellular 1 for dial-up Internet accessing. When accessing Internet through WAN, select the corresponding Ethernet port name.
- 5) NEVER forget to click "**Save**" everytime after doing any change.

Step 3: Import CA files.

To create the CA files, please refer to document "[Quick Guide for Creating OpenVPN CA files Base on Windows](#)".

Click "**VPN >> Certificate Management**" to import CA files.

VPN >> Certificate Management

Certificate Management **ROOT CA**

Certificate Management

Enable SCEP (Simple Certificate Enrollment Protocol)

Protect Key

Protect Key Confirm

Revocation

No file selected.	Browse...	Import Public Key Certificate	Export Public Key Certificate
No file selected.	Browse...	Import Private Key Certificate	Export Private Key Certificate
No file selected.	Browse...	Import CA Certificate	Export CA Certificate
No file selected.	Browse...	Import CRL	Export CRL
No file selected.	Browse...	Import PKCS12 Certificate	Export PKCS12 Certificate

Apply & Save Cancel

Click **“Browse”** to select the corresponding CA file, then click **“Import Certificate”**.

2.2 Client Configuration

Step 1: Add a new OpenVPN client Tunnel.

Click **VPN >> OpenVPN Tunnel**, then click **“Add”** to add the new tunnel.

Edit OPENVPN Tunnel

Tunnel name	<input type="text" value="OpenVPN_T_1"/>
Enable	<input checked="" type="checkbox"/>
Mode	<input type="text" value="Client"/>
Protocol	<input type="text" value="UDP"/>
Port	<input type="text" value="1194"/>
OPENVPN Server	<input type="text" value="inhandserver.ddns.net"/>
Authentication Type	<input type="text" value="X.509 Cert"/>
Pre-shared Key	<input type="text"/>
Local IP Address	<input type="text" value="172.10.10.2"/>
Remote IP Address	<input type="text" value="172.10.10.1"/>
Remote Subnet	<input type="text" value="192.168.2.0"/>
Remote Netmask	<input type="text" value="255.255.255.0"/>
Link Detection Interval	<input type="text" value="60"/> Seconds
Link Detection Timeout	<input type="text" value="300"/> Seconds
Renegotiate Interval	<input type="text" value="86400"/> Seconds
Enable NAT	<input checked="" type="checkbox"/>
Enable LZO	<input checked="" type="checkbox"/>
Update DNS	<input type="checkbox"/>
Encryption Algorithms	<input type="text" value="Blowfish(128)"/>
HMAC	<input type="text" value="SHA1"/>
MTU	<input type="text" value="1500"/>
Max Fragment Size	<input type="text"/>
Debug Level	<input type="text" value="Warn"/>
Interface Type	<input type="text" value="TUN"/>
Expert Options(Expert Only)	<input type="text"/>

- 1) Fill in the IP address of the configured **OpenVPN Server**. Make sure the **Protocol Type** is same as the server's setting.
- 2) Select **Authentication Type** as **x.509-cert**.
- 3) Fill in the Local and Remote IP address. (Opposite to the server's setting)

Step 2: Import CA files.

Click **VPN >> Certificate Management** to import CA files.

Certificate Management

Enable SCEP (Simple Certificate Enrollment Protocol)

Protect Key

Protect Key Confirm

C:\fakepath\ca (1).cert

No file selected.

C:\fakepath\public.crt

C:\fakepath\private.key

No file selected.

Click **“Browse”** to select the corresponding CA file, then click **“Import Certificate”**.

3. Verify

Before doing the verify, please make sure both the devices can access to the Internet.

3.1 Verify OpenVPN Server

Click **“VPN >> OpenVPN”** to enter the **Status** page. When the **Status** shows **“Connected”**, the OpenVPN Server is successfully configured.

VPN >> OpenVPN

Status | OpenVPN Client | OpenVPN Server

Tunnel Name	OpenVPN Server	Interface Type	Status	Local IP Address	Remote IP Address	Description
openvpn server	-	tun	connected (0 day, 00:27:37s)	172.10.10.1	172.10.10.2	

3.2 Verify OpenVPN Client

Click **“VPN >> OpenVPN Tunnel”**. When the **Tunnel Status** shows **“Connected”**, the OpenVPN Client is successfully configured.

OpenVPN Tunnels

Enable	Name	Tunnel Description	Tunnel Status	Conneted Time
Yes	OpenVPN_T_1	[router]==[10.5.11.47] Mode: Client Protocol: UDP; Port: 1194 172.10.10.2---172.10.10.1	Connected	

Contact Us

Add: 3900 Jermantown Rd., Suite 150, Fairfax, VA 22030 USA

E-mail: support@inhandnetworks.com

T: +1 (703) 348-2988

URL: www.inhandnetworks.com



InHand Website