

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



inhand	VPN >> OpenVPN Status OpenVPN Client OpenV	PN Server
Administration	Epoble	
Network	Config Mode	Manual Capita
Services 🕨	Coning Mode	
Link Backup	Authentication Type	x509-cert T
Routing	Virtual Network	172.10.10.0
Firewall •	Virtual Netmask	255.255.255.0
VPN •	Description	
APP	Show Advanced Options	v
Tools	Source Interface	fastethernet 0/1 🔻
Wizards •	Interface Type	tun 🔻
	Network Type	net30 🔻
	Protocol Type	udp 🔻
	Port	1194
Save Configuration	Cipher	Default •
	HMAC	sha1 ▼
	Client-to-Client	
Copyright ©2001-2019	Compression LZO	

- 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**. Celluar 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.



ertificate Management RO	OT 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. No file selected.		Browse	Import Public Key Certificate Import Private Key Certificate	Export Public Key Certificate Export Private Key Certificate
No file selected. No file selected. No file selected.		Browse Browse	Import Public Key Certificate Import Private Key Certificate Import CA Certificate	Export Public Key Certificate Export Private Key Certificate Export CA Certificate
No file selected. No file selected. No file selected. No file selected.		Browse Browse Browse	Import Public Key Certificate Import Private Key Certificate Import CA Certificate Import CRL	Export Public Key Certificate Export Private Key Certificate Export CA Certificate Export CRL

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.



OpenVPN	Tunnels

Edit OPENVPN Tunnel		
Tunnel name	OpenVPN_T_1	
Enable	•	
Mode	Client •	
Protocol	UDP V	
Port	1194	
OPENVPN Server	inhandserver.ddns.net	
Authentication Type	X.509 Cert	
Pre-shared Key		11
Local IP Address	172.10.10.2]
Remote IP Address	172.10.10.1]
Remote Subnet	192.168.2.0]
Remote Netmask	255.255.255.0]
Link Detection Interval	60	Seconds
Link Detection Timeout	300	Seconds
Renegotiate Interval	86400	Seconds
Enable NAT	*	
Enable LZO		
Update DNS		
Encryption Algorithms	Blowfish(128) ▼	
HMAC	SHA1 V	_
MTU	1500	
Max Fragment Size		
Debug Level	Warn 🔻	
Interface Type	TUN V	
Expert Options(Expert Only)		
Save Cancel	Delete	

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.

inhand	 Verif	ý	
Certificate Management		Certificate Manageme	nt
Enable SCEP (Simple Certificate Enrollment Protocol)			
Protect Key			
Protect Key Confirm			
C:\fakepath\ca (1).crt	Browse	Import CA Certificate	Export CA Certificate
No file selected.	Browse	Import CRL	Export CRL
C:\fakepath\public.crt	Browse	Import Public Key Certificate	Export Public Key Certificate
C:\fakepath\private.key	Browse	Import Private Key Certificate	Export Private Key Certificate
No file selected.	Browse	Import PKCS12	Export PKCS12

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.

۷	/PN >> OpenVPN									
	Status OpenVPN Client OpenVPN Server									
Γ										
	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 172.10.10.2172.10.10.1	Connected		
	Add	Show Detail Status			

Contact Us

Add: 3900 Jermantown Rd., Suite 150, Fairfax, VA 22030 USA E-mail: support@inhandneworks.com T: +1 (703) 348-2988 URL: www.inhandnetworks.com



InHand Website

© 2019 InHand Networks Inc. All rights reserved.InHand Networks Inc. reserves the right to update or modify, this document at any time without prior notice.