IR600 & IR900

IPSec VPN Guide

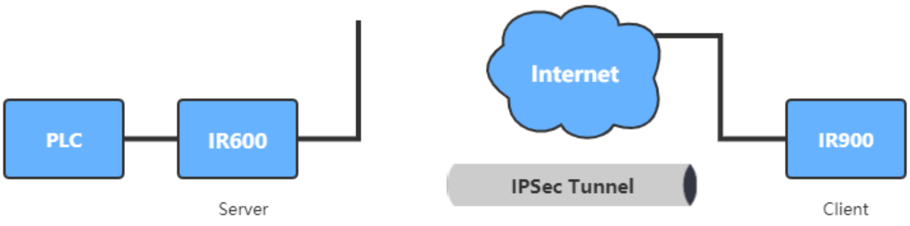
Version V1.0-EN Date: March, 2020

InHand Networks
Global Leader in Industrial IoT

Content

1. Abstract

This guide will show how to configure an IPSec VPN Tunnel between an IR600 device and an IR900 device. Here we use IR600 for the Server of IPSec VPN and IR900 for Client.



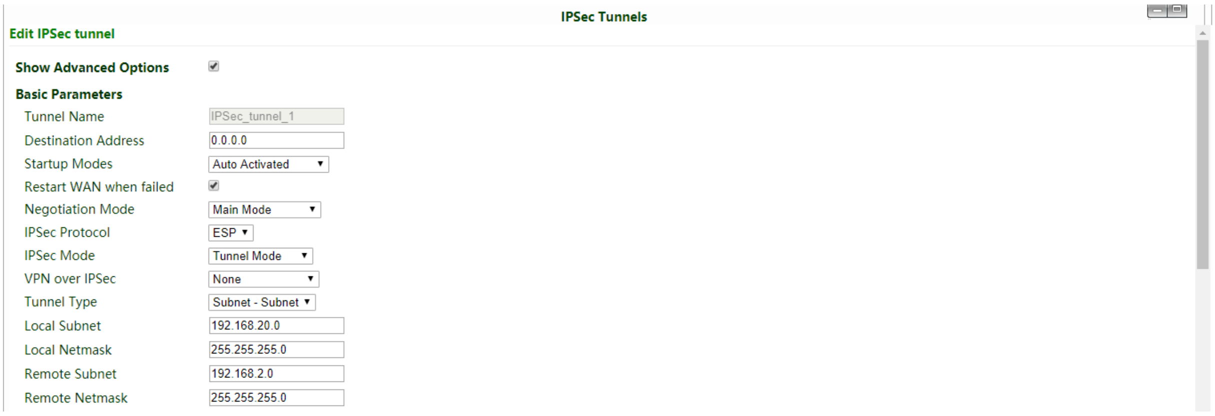
2. Configuration

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

2.1 Server Configuration

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

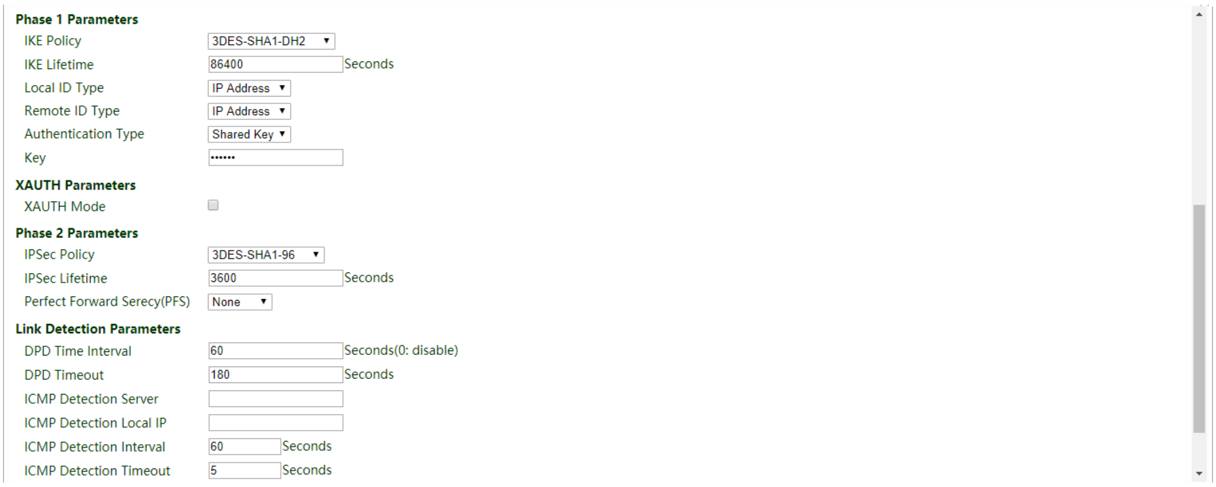
Click **“VPN >> IPSec Tunnels”,** then click “**Add**” to add the new tunnel.



IPSec Tunnels

Edit IPSec tunnel

Show Advanced Options	☑
Basic Parameters	
Tunnel Name	IPSec_tunnel_1
Destination Address	0.0.0.0
Startup Modes	Auto Activated ▾
Restart WAN when failed	☑
Negotiation Mode	Main Mode ▾
IPSec Protocol	ESP ▾
IPSec Mode	Tunnel Mode ▾
VPN over IPSec	None ▾
Tunnel Type	Subnet - Subnet ▾
Local Subnet	192.168.20.0
Local Netmask	255.255.255.0
Remote Subnet	192.168.2.0
Remote Netmask	255.255.255.0



Phase 1 Parameters

IKE Policy	3DES-SHA1-DH2 ▾	
IKE Lifetime	86400	Seconds
Local ID Type	IP Address ▾	
Remote ID Type	IP Address ▾	
Authentication Type	Shared Key ▾	
Key	••••••	

XAUTH Parameters

XAUTH Mode	□

Phase 2 Parameters

IPSec Policy	3DES-SHA1-96 ▾	
IPSec Lifetime	3600	Seconds
Perfect Forward Serecy(PFS)	None ▾	

Link Detection Parameters

DPD Time Interval	60	Seconds(0: disable)
DPD Timeout	180	Seconds
ICMP Detection Server		
ICMP Detection Local IP		
ICMP Detection Interval	60	Seconds
ICMP Detection Timeout	5	Seconds

1) Set the **Destination Address** as **0.0.0.0** for the server side.

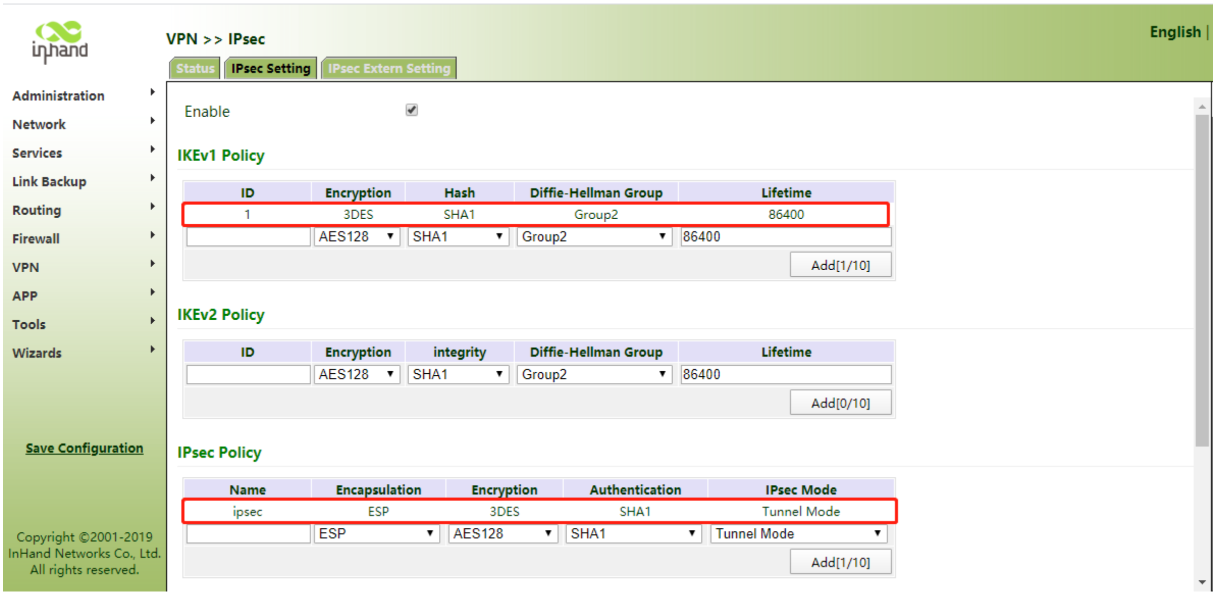
2) Fill in the **Local** and **Remote Subnet** alternatively.

3) In the "**Phase 1 Parameters**" part, because here the **Authentication Type** is **Shared Key**, so the user needs to set a **Key** for the IPSec tunnel.

4) **NEVER** forget to click "**Save**" everytime after doing any change.

2.2 Client Configuration

Step 1: Click "**VPN >> IPsec**" to enter the **IPsec Setting** page. Do the configuration of "**IKEv1 Policy**" and "**IPsec Policy**" part. Keep the corresponding parameters as same as the Server's setting.



VPN >> IPsec

Enable ☑

IKEv1 Policy

ID	Encryption	Hash	Diffie-Hellman Group	Lifetime
1	3DES	SHA1	Group2	86400
	AES128 ▾	SHA1 ▾	Group2 ▾	86400

Add[1/10]

IKEv2 Policy

ID	Encryption	integrity	Diffie-Hellman Group	Lifetime
	AES128 ▾	SHA1 ▾	Group2 ▾	86400

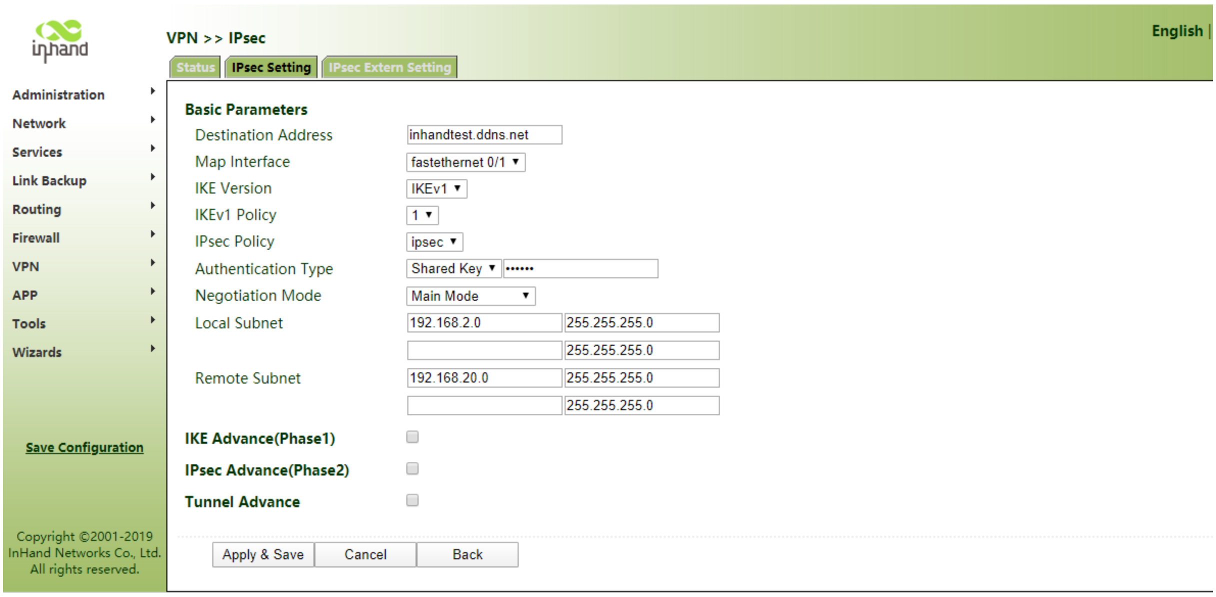
Add[0/10]

IPsec Policy

Name	Encapsulation	Encryption	Authentication	IPsec Mode
ipsec	ESP	3DES	SHA1	Tunnel Mode
	ESP ▾	AES128 ▾	SHA1 ▾	Tunnel Mode ▾

Add[1/10]

Step 2: In the bottome of the page, in the "**IPsec Tunnels**" part, click "**Add**" to add a new IPsec tunnel.



VPN >> IPsec

Basic Parameters

Destination Address	inhandtest.ddns.net	
Map Interface	fastethernet 0/1	
IKE Version	IKEv1	
IKEv1 Policy	1	
IPsec Policy	ipsec	
Authentication Type	Shared Key	••••••
Negotiation Mode	Main Mode	
Local Subnet	192.168.2.0	255.255.255.0
		255.255.255.0
Remote Subnet	192.168.20.0	255.255.255.0
		255.255.255.0

IKE Advance(Phase1) □

IPsec Advance(Phase2) □

Tunnel Advance □

1) Fill in the Destination address of the configured **IPSec VPN Server**. Both the IP address and the domain name are acceptable.

2) Select **Map Interface**. Celluar 1 for dial-up Internet accessing. When accessing Internet through WAN, select the corresponding Ethernet port name.

3) Select the same **Authentication Type** as the server's setting and fill in the same password.

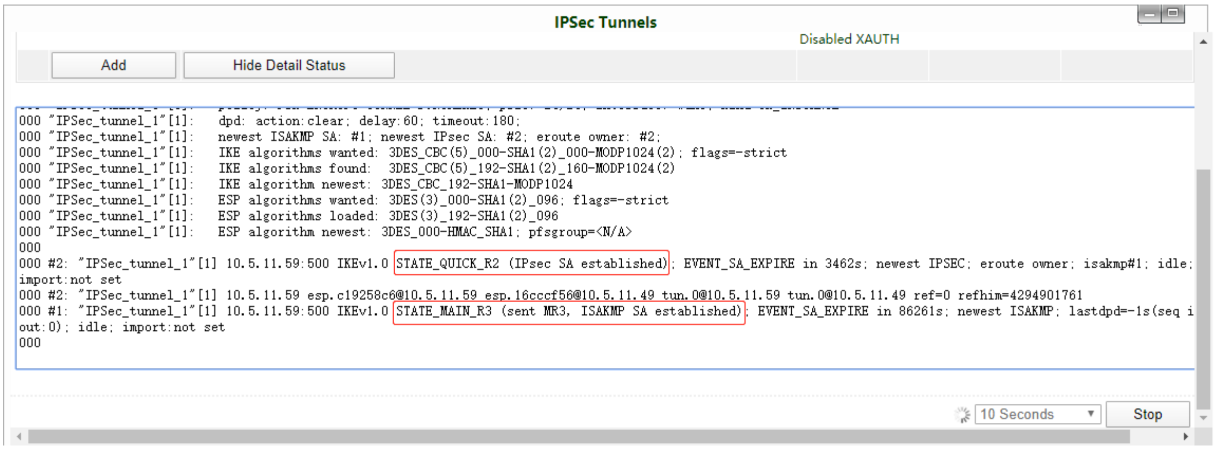
4) Fill in the Local and Remote Subnet. (Opposite to the server's setting)

3. Verify

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

3.1 Verify Server

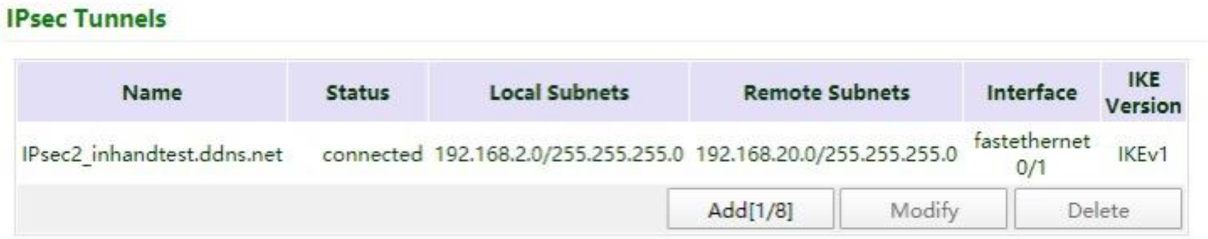
Click **"VPN >> IPSec Tunnels"**, then click the "**Show Detail Status**" button. When there shows the word like red blocks show in the following figure, the IPSec tunnel is successful configured.



```
000 "IPSec_tunnel_1"[1]:   dpd: action:clear; delay:60; timeout:180;
000 "IPSec_tunnel_1"[1]:   newest ISAKMP SA: #1; newest IPsec SA: #2; eroute owner: #2;
000 "IPSec_tunnel_1"[1]:   IKE algorithms wanted: 3DES_CBC(5)_000-SHA1(2)_000-MODP1024(2); flags=-strict
000 "IPSec_tunnel_1"[1]:   IKE algorithms found:  3DES_CBC(5)_192-SHA1(2)_160-MODP1024(2)
000 "IPSec_tunnel_1"[1]:   IKE algorithm newest: 3DES_CBC_192-SHA1-MODP1024
000 "IPSec_tunnel_1"[1]:   ESP algorithms wanted: 3DES(3)_000-SHA1(2)_096; flags=-strict
000 "IPSec_tunnel_1"[1]:   ESP algorithms loaded: 3DES(3)_192-SHA1(2)_096
000 "IPSec_tunnel_1"[1]:   ESP algorithm newest: 3DES_000-HMAC_SHA1; pfsgroup=<N/A>
000
000 #2: "IPSec_tunnel_1"[1] 10.5.11.59:500 IKEv1.0 STATE_QUICK_R2 (IPsec SA established); EVENT_SA_EXPIRE in 3462s; newest IPSEC; eroute owner; isakmp#1; idle;
import:not set
000 #2: "IPSec_tunnel_1"[1] 10.5.11.59 esp.c19258c6@10.5.11.59 esp.16cccf56@10.5.11.49 tun.0@10.5.11.59 tun.0@10.5.11.49 ref=0 refhim=4294901761
000 #1: "IPSec_tunnel_1"[1] 10.5.11.59:500 IKEv1.0 STATE_MAIN_R3 (sent MR3, ISAKMP SA established); EVENT_SA_EXPIRE in 86261s; newest ISAKMP; lastdpd=-1s(seq i
out:0); idle; import:not set
000
```

3.2 Verify Client

Click “**VPN >> IPsec”** to enter the **IPsec Setting** page. In the bottom of the page, the status of the added IPsec tunnel will show up. When the status is “connected”, the IPSec tunnel is successful configured.


IPsec Tunnels

Name	Status	Local Subnets	Remote Subnets	Interface	IKE Version
IPsec2_inhandtest.ddns.net	connected	192.168.2.0/255.255.255.0	192.168.20.0/255.255.255.0	fastethernet 0/1	IKEv1

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