

645M-4 IPSec Server/Client setup

The following application note demonstrates the configuration of the ELPRO 645M-4 cellular modem utilizing IPSec Tunnelling. Internet Protocol Security (IPSec) is a secure networking protocol that authenticates and encrypts data packets that are sent over the Internet. When using a Public Cellular network, it is recommended that some form of security be used to protect the data from eavesdropping.

Network Example - Overview

Typical network applications that IPSec can be used for are Point to Point or Point to Multipoint applications as seen below. This application note will cover configuration for both examples.

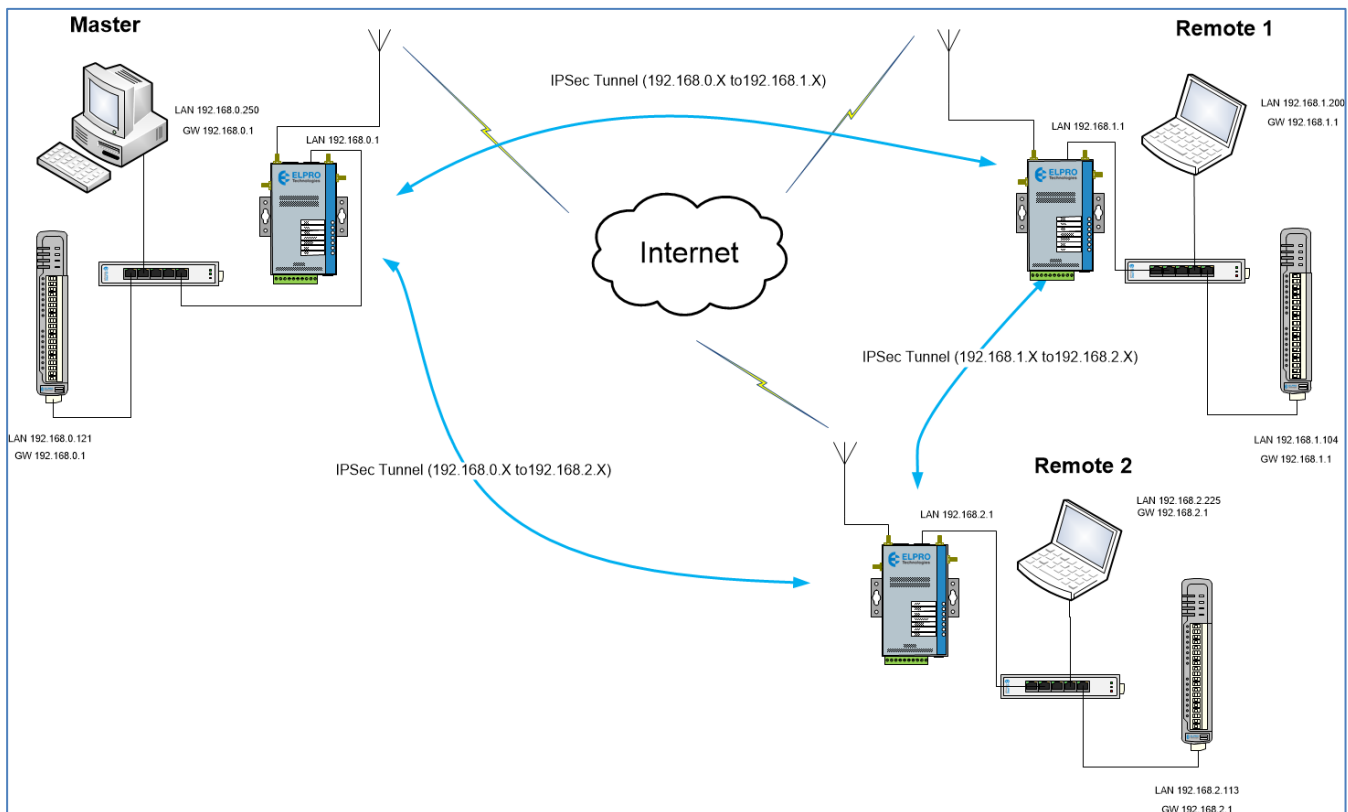


Figure 1 – Example System

To establish an IPSec communication link, we need to first setup a Server and then setup Clients to connect to this Server. This application can be setup to use Static Private Cellular IP addresses or Dynamic Public IP addresses, however if using Dynamic IP's you will need to implement DDNS service.

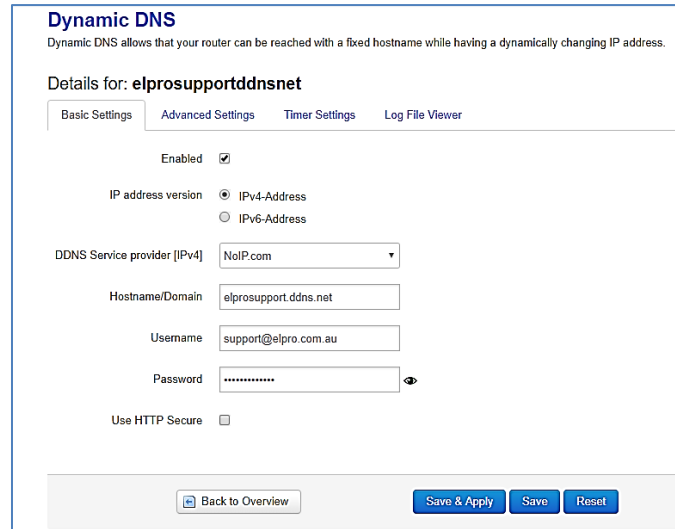
Dynamic DNS

The Public PPP IP Address assigned by cellular providers will be either a Fixed or a Dynamic IP address. Dynamic assigned IP addresses can change upon differing conditions set by the cellular carrier, when this occurs inactivity will occur until the new IP address is known, which typically requires connecting to it locally and viewing the unit status page.

The use of Dynamic DNS assigns a DNS name to the modem which then allows the modem to be accessed regardless of the assigned PPP IP address. There are a number of providers that offer Dynamic DNS "DDNS" services for example, a free service provided by "No-IP" allows users to setup between one to three host names on a domain name provided by No-IP.

In this example we are using a dynamic public IP addresses provided by "No-IP" and we have setup a Dynamic DNS address on the Server and each Clients cellular IP Address.

If you were using a Private Network with fixed IP addresses, you would just need to setup the IPsec Communications using the fixed cellular IP Addresses instead of the DDNS names.



Dynamic DNS
Dynamic DNS allows that your router can be reached with a fixed hostname while having a dynamically changing IP address.

Details for: **elprosupportddnsnet**

Basic Settings | **Advanced Settings** | Timer Settings | Log File Viewer

Enabled

IP address version IPv4-Address IPv6-Address

DDNS Service provider (IPv4)

Hostname/Domain

Username

Password

Use HTTP Secure

[Back to Overview](#) [Save & Apply](#) [Save](#) [Reset](#)

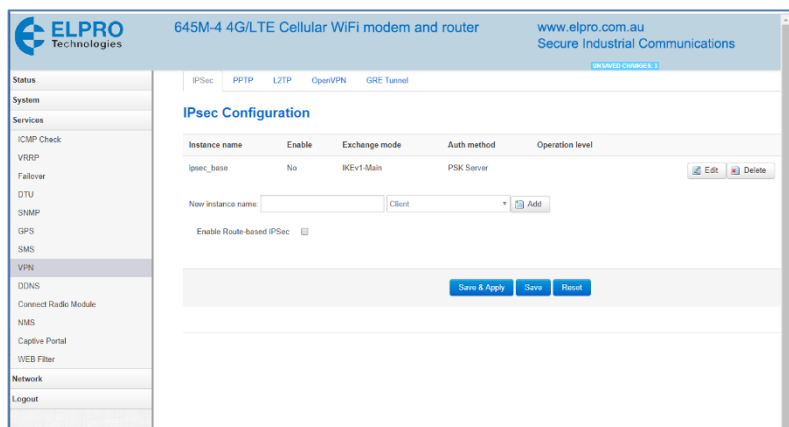
Application Example

In the Example System shown in Figure 1 above we are connecting a Master Computer and an Ethernet I/O device (115E-2) to the Server Cellular modem. The Server Modem LAN IP address is on 192.168.0.1 and the computer and the I/O device connected to the Modem will need to be in the same 192.168.0.X subnet and have a Gateway IP address of 192.168.0.1. At each of the remote locations we are also connecting a Computer/Laptop and another Ethernet I/O device (115E-2) and likewise the Client modems have a LAN IP of 192.168.1.1 (Client #1) & 192.168.2.1 (Client #2) and the I/O devices and computers connected to these modems have their IP addresses in the same subnet as the modem and have their Gateway IP address configured for the connected Cellular modems LAN IP.

IPSec Setup

The ELPRO 645M-4 IPSec configuration is located under the **Services – VPN – IPSec** webpage link.

Either edit one of the existing instance examples or create a new Server or Client one by giving it a "Name", selecting Server or Client and then selecting "Add"



ELPRO Technologies 645M-4 4G/LTE Cellular WiFi modem and router www.elpro.com.au Secure Industrial Communications

IPSec | PPTP | L2TP | OpenVPN | GRE Tunnel

IPsec Configuration

Instance name	Enable	Exchange mode	Auth method	Operation level
ipsec_base	No	IKEV1-Main	PSK Server	Edit Delete

New Instance name: Client [Add](#)

Enable Route-based IPSec

[Save & Apply](#) [Save](#) [Reset](#)

645M-4 Server Configuration

Setup the Server with the parameters as shown in the screen shots below.

Enable	<input checked="" type="checkbox"/>
Exchange mode	IKEv1-Main
Operation Level	Main
Authentication method	PSK Server
Remote VPN endpoint	elprotech.ddns.net
Local endpoint	elprosupport.ddns.net
Local IKE identifier	elprosupport.ddns.net
Remote IKE identifier	elprotech.ddns.net
Preshared Keys
Perfect Forward Secrecy	Enable
DPD action	None
DPD delay	600 seconds
DPD timeout	1400 seconds
NAT Traversal	Enable
Local source ip	
Remote source ip	

Local LAN bypass	<input type="checkbox"/>
Local subnet	192.168.0.0/24
Remote subnet	192.168.1.0/24
Phase 1 Proposal	
Enable	<input checked="" type="checkbox"/>
Encryption algorithm	3DES
Hash algorithm	HMAC_SHA1
DH group	MODP1024/2
Life time	10800 seconds
Phase 2 Proposal	
Enable	<input checked="" type="checkbox"/>
Encryption algorithm	AES 128
PFS group	MODP1024/2
Authentication	HMAC_SHA1
Life time	3600 seconds

The Main changes that will need to be made will be

- Authentication Method will be “PSK Server”
- Remote VPN endpoint will be the Dynamic DNS address setup for the Client or the Cellular IP address if using Fixed IP SIMS.
- Local Endpoint is the Dynamic DNS address setup for the Server or fixed IP address.
- Local IKE Identifier will be the same address as the Local Endpoint and the Remote IKE identifier will be the same as the Remote VPN endpoint.
- Pre-shared keys can be any password just make sure it is configured the same on each Client.
- DPD delay and Timeout is a method used to detect the aliveness of the IPSec tunnel. “DPD Delay” is the time the DPD exchange messages are sent to the peer and the “DPD Timeout” determines the timeout interval before the connection to a peer is dropped if there is no connection activity.

The rest of the parameters can be default except Local LAN Bypass needs to be deselected and the Local and the Remote Subnets will need to match that of the Server and Client’s LAN subnets, in this case the Server is on 192.168.0.X and the Client is on 192.168.1.X subnets.

When all the parameters have been entered select “Save & Apply” button.

645M-4 Client#1 Configuration

Connect to the first Clients webpage and navigate to **Services – VPN – IPSec**.

Setup the first Client with the following parameters as shown in the screen shots below.

Enable	<input checked="" type="checkbox"/>
Exchange mode	IKEv1-Main
Operation Level	Main
Authentication method	PSK Client
Remote VPN endpoint	elprosupport.ddns.net
Local endpoint	elprotech.ddns.net
Local IKE identifier	elprotech.ddns.net
Remote IKE identifier	elprosupport.ddns.net
Preshared Keys
Perfect Forward Secrecy	Enable
DPD action	None
DPD delay	600 seconds
DPD timeout	1400 seconds
NAT Traversal	Enable
Local source ip	
Remote source ip	

Local LAN bypass	<input type="checkbox"/>
Local subnet	192.168.1.0/24
Remote subnet	192.168.0.0/24
Phase 1 Proposal	
Enable	<input checked="" type="checkbox"/>
Encryption algorithm	3DES
Hash algorithm	HMAC_SHA1
DH group	MODP1024/2
Life time	10800 seconds
Phase 2 Proposal	
Enable	<input checked="" type="checkbox"/>
Encryption algorithm	AES 128
PFS group	MODP1024/2
Authentication	HMAC_SHA1
Life time	3600 seconds

When complete press “Save & Apply” and ensure the devices that are connected to the Modems and need to communicate through the tunnel are on the same Subnet as the modem and have their Gateway IP address’s set to the LAN IP address of the modem.

Also make sure the Computers do not have another Network adaptor configured, i.e. PC/Laptop with another LAN or Wi-Fi as this may interfere with the communications, etc.

645M-4 Client#2 Configuration

Configuration of the second Client should be very similar to Client1 only it will be setup with a different DDNS name and so a different Local endpoint and Local IKE identifier.

Setup the second Client with the following parameters as shown in the screen shots below.

Enable	<input checked="" type="checkbox"/>
Exchange mode	IKEv1-Main
Operation Level	Main
Authentication method	PSK Client
Remote VPN endpoint	elprosupport.ddns.net
Local endpoint	elprosales.ddns.net
Local IKE identifier	elprosales.ddns.net
Remote IKE identifier	elprosupport.ddns.net
Preshared Keys
Perfect Forward Secrecy	Enable
DPD action	None
DPD delay	600 seconds
DPD timeout	1400 seconds
NAT Traversal	Enable
Local source ip	
Remote source ip	

Local LAN bypass	<input type="checkbox"/>
Local subnet	192.168.2.0/24
Remote subnet	192.168.0.0/24
Phase 1 Proposal	
Enable	<input checked="" type="checkbox"/>
Encryption algorithm	3DES
Hash algorithm	HMAC_SHA1
DH group	MODP1024/2
Life time	10800 seconds
Phase 2 Proposal	
Enable	<input checked="" type="checkbox"/>
Encryption algorithm	AES 128
PFS group	MODP1024/2
Authentication	HMAC_SHA1
Life time	3600 seconds

When complete press “Save & Apply” and ensure the devices that are connected to the Modems and need to communicate through the tunnel are on the same Subnet as the modem and have their Gateway IP address’s set to the LAN IP address of the modem.

Also, the Devices or computers connected to the Modem must have their Gateway IP address’s set to the LAN IP address of the modem

Connection Parameters

Check the 645M-4 modem Network / Firewall page and under the “Security” tab that the “Ping from WAN to LAN” is set to “Allow”.

General Settings	Port Forwards	Traffic Rules	Source NAT	DMZ	Security	MAC Filter
System Security Configuration						
SSH access from WAN	Deny					
Ping from WAN to LAN	Allow					
Enable telnet	<input type="checkbox"/>					

Also, under the “Network / Firewall – Traffic Rules” that the “Allow All LAN Ports” rule is enabled

Firewall - Traffic Rules

Traffic rules define policies for packets traveling between different zones, for example to reject traffic between certain hosts or to open WAN ports on the router.

Traffic Rules

Name	Match	Action	Enable	Sort
DTU server	Any TCP, UDP From any host in wan To any router IP at port 5000 on this device	Accept input	<input type="checkbox"/>	<input type="button" value="+"/> <input type="button" value="+"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/>
Allow-All-LAN-Ports	Any traffic From any host in wan To any host, ports 1-65535 in lan	Accept forward	<input checked="" type="checkbox"/>	<input type="button" value="+"/> <input type="button" value="+"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/>
Allow-DHCP-Renew	IPv4-UDP From any host in wan To any router IP at port 68 on this device	Accept input	<input checked="" type="checkbox"/>	<input type="button" value="+"/> <input type="button" value="+"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/>

Checking Tunnel connection

When the Server and Clients have all been configured and the configurations applied you should be able to check the tunnel connection status at each modem by navigating to **Status – VPN – IPsec** and confirm the connections have been established in the log.

Status

- Overview
- Network
- Firewall
- Routes
- System Log
- Kernel Log
- Reboot Log
- Realtime Graphs
- VPN**
- System
- Services
- Network
- Logout

IPSec
IPSec Log
OpenVPN
PPTP tunnel
L2TP tunnel

IPSec Status

```

Status of IKE charon daemon (weakSwan 5.6.3, Linux 3.18.29, mips):
uptime: 2 hours, since Jul 31 09:17:30 2019
malloc: sbrk 139264, mmap 0, used 127568, free 11696
worker threads: 11 of 16 idle, 5/0/0/0 working, job queue: 0/0/0/0, scheduled: 8
loaded plugins: charon random nonce aes des sha1 sha2 md5 pem pkcs1 gmp x509 revocation hmac stroke kernel-netlink socket-default updown xauth-generic
Listening IP addresses:
192.168.0.1
fd0:ad7:2ee0::1
120.157.71.70
Connections:
2Network: elprosupport.ddns.net,0.0.0.0/0:::0...elprosales.ddns.net,0.0.0.0/0:::0 IKEv1
2Network: local: [elprosupport.ddns.net] uses pre-shared key authentication
2Network: remote: [elprosales.ddns.net] uses pre-shared key authentication
2Network: child: 192.168.0.0/24 === 192.168.2.0/24 TUNNEL
1Network: elprosupport.ddns.net,0.0.0.0/0:::0...elprotech.ddns.net,0.0.0.0/0:::0 IKEv1
1Network: local: [elprosupport.ddns.net] uses pre-shared key authentication
1Network: remote: [elprotech.ddns.net] uses pre-shared key authentication
1Network: child: 192.168.0.0/24 === 192.168.1.0/24 TUNNEL
Security Associations (2 up, 0 connecting):
1Network[4]: ESTABLISHED 83 minutes ago, 120.157.71.70[elprosupport.ddns.net]_123.209.233.22[elprotech.ddns.net]
1Network[4]: IKEv1 SPIs: 2e36b2f14213d3e9_181c088624ab3b082_r*, pre-shared key reauthentication in 85 minutes
1Network[4]: IKE proposal: 3DES_CBC/HMAC_SHA1_96/PRF_HMAC_SHA1/MODP_1024
1Network[8]: INSTALLED, TUNNEL, reqid 4, ESP SPIs: c72025ad_i c0d8f1b8_o
1Network[8]: AES_CBC_128/HMAC_SHA1_96/MODP_1024, 8237 bytes_i (75 pkts, 0s ago), 57120 bytes_o (88 pkts, 2s ago), rekeying in 5 minutes
1Network[8]: 192.168.0.0/24 === 192.168.1.0/24
2Network[3]: ESTABLISHED 92 minutes ago, 120.157.71.70[elprosupport.ddns.net]_123.209.124.251[elprosales.ddns.net]
2Network[3]: IKEv1 SPIs: cfb8b2f96fde548_i 7f5b7512c4ae4563_r*, pre-shared key reauthentication in 71 minutes
2Network[3]: IKE proposal: 3DES_CBC/HMAC_SHA1_96/PRF_HMAC_SHA1/MODP_1024
2Network[7]: REKEYED, TUNNEL, reqid 3, expires in 10 minutes
2Network[7]: 192.168.0.0/24 === 192.168.2.0/24
2Network[9]: INSTALLED, TUNNEL, reqid 3, ESP SPIs: c002cc04_i c4601b3c_o
2Network[9]: AES_CBC_128/HMAC_SHA1_96/MODP_1024, 35814 bytes_i (202 pkts, 0s ago), 20593 bytes_o (195 pkts, 0s ago), rekeying in 40 minutes
2Network[9]: 192.168.0.0/24 === 192.168.2.0/24

```

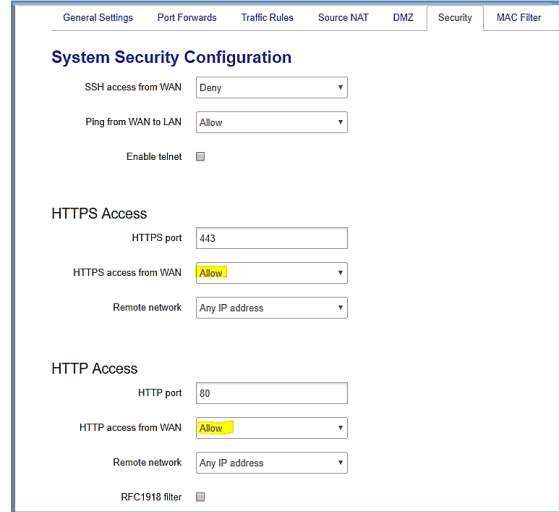
Next we should be able to check if we have connectivity between Subnets.

Open a Command window on each PC and confirm that you can Ping the other Cellular modems LAN IP address.

If you can successfully Ping, the LAN IP addresses of the other modems than you should be able to open the Web page on the Remote modems provided you have enabled HTTP/HTTPS access (see Note below)

Also, you should be able to open the Web interface of the Remote Ethernet I/O (115E-2) device that are connected to the Modems and in this case be able to pass I/O between the Ethernet I/O devices.

Note: If you wish to open the remote modems web interface via the IPsec tunnel you will need to have “Allow” HTTP and HTTPS access enabled on the Remote Modems **Network – Firewall – Security** pages.



The screenshot shows the 'System Security Configuration' page with the following settings:

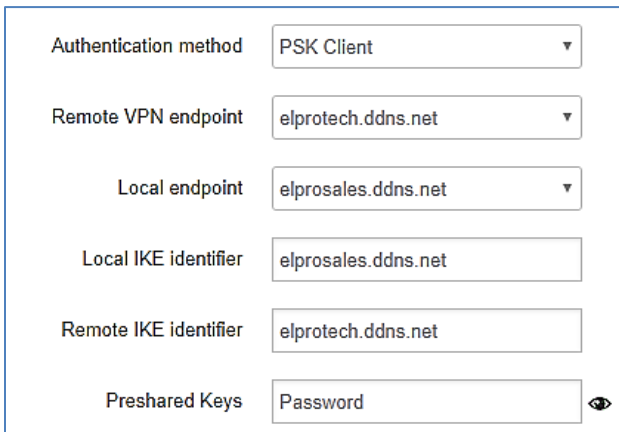
- SSH access from WAN: Deny
- Ping from WAN to LAN: Allow
- Enable telnet:
- HTTPS Access:
 - HTTPS port: 443
 - HTTPS access from WAN: Allow
 - Remote network: Any IP address
- HTTP Access:
 - HTTP port: 80
 - HTTP access from WAN: Allow
 - Remote network: Any IP address
- RFC1918 filter:

Client to Client connection.

The above system configuration will allow connectivity between the Master location LAN and each of the Remote LANs. If Remote Client to Remote Client communications is needed, then a separate IPsec tunnel will need to be configured on the remotes.

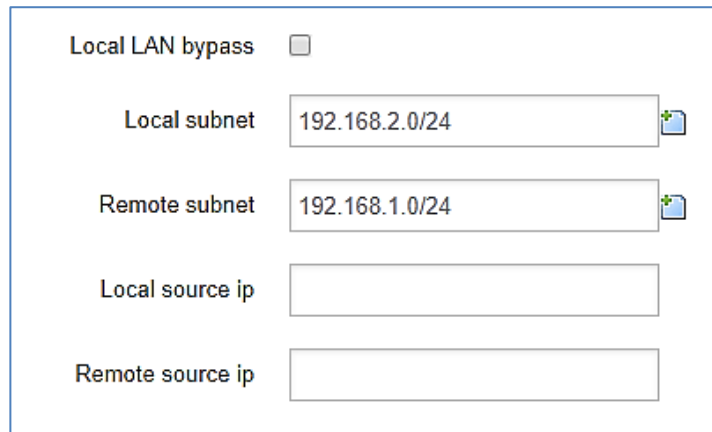
One Remote will need to be setup with a Server Configuration and the other a Client.

Configuration will essentially be the same as the above Server/Client example but with the Authentication Method, Remote VPN endpoint, Local endpoint, Local IKE Identifier and Remote IKE identifier reflecting the appropriate Server/Client configurations, see screen shot below for differences on the Client end of the link.



The screenshot shows the VPN Client configuration page with the following settings:

- Authentication method: PSK Client
- Remote VPN endpoint: elprotech.ddns.net
- Local endpoint: elprosales.ddns.net
- Local IKE identifier: elprosales.ddns.net
- Remote IKE identifier: elprotech.ddns.net
- Preshared Keys: Password



The screenshot shows the Network configuration section of the VPN Client configuration page with the following settings:

- Local LAN bypass:
- Local subnet: 192.168.2.0/24
- Remote subnet: 192.168.1.0/24
- Local source ip: [Empty field]
- Remote source ip: [Empty field]

Below screenshots show the differences for the Server end of the Link.

Authentication method	PSK Server
Remote VPN endpoint	elprosales.ddns.net
Local endpoint	elprotech.ddns.net
Local IKE identifier	elprotech.ddns.net
Remote IKE identifier	elprosales.ddns.net
Preshared Keys	Password

Local LAN bypass	<input type="checkbox"/>
Local subnet	192.168.1.0/24
Remote subnet	192.168.2.0/24
Local source ip	
Remote source ip	

Amendment Register:

Issue No.	Date	Details of Amendment
1.0	31/07/19	Draft Issue
1.1	17/12/19	Added other connection parameters & DPD times adjusted