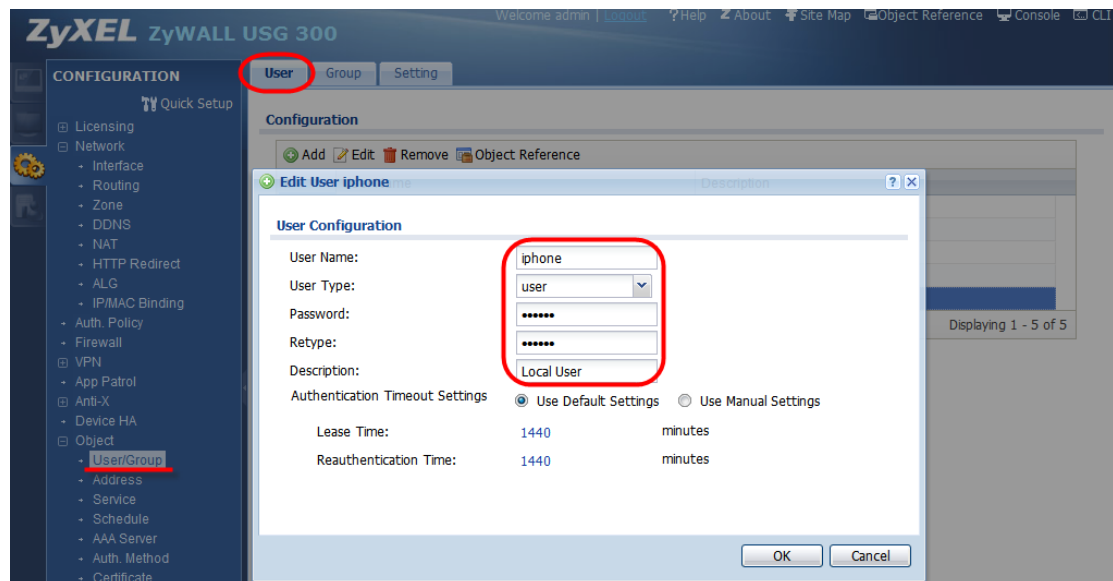


L2TP over IPSec connection between the ZyWALL USG and iPhone

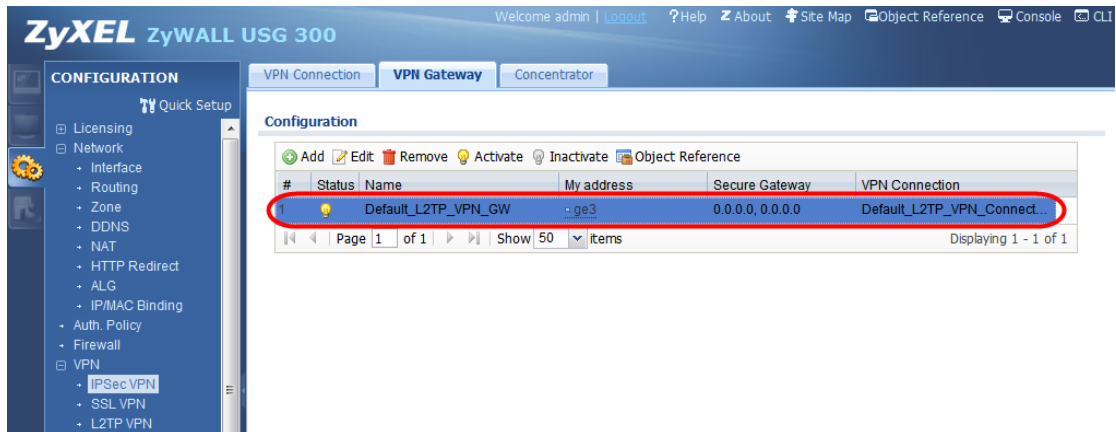
iPhone 3G is now a very popular handheld device worldwide. It not only allows mobile users to surf Internet, delivering push email, but also provides secure access to corporate resources by supporting a variety of virtual private network (VPN) technologies. This document provides step-by-step instructions for setting up a VPN connection between ZyWALL USG and an iPhone.

ZyWALL USG configuration:

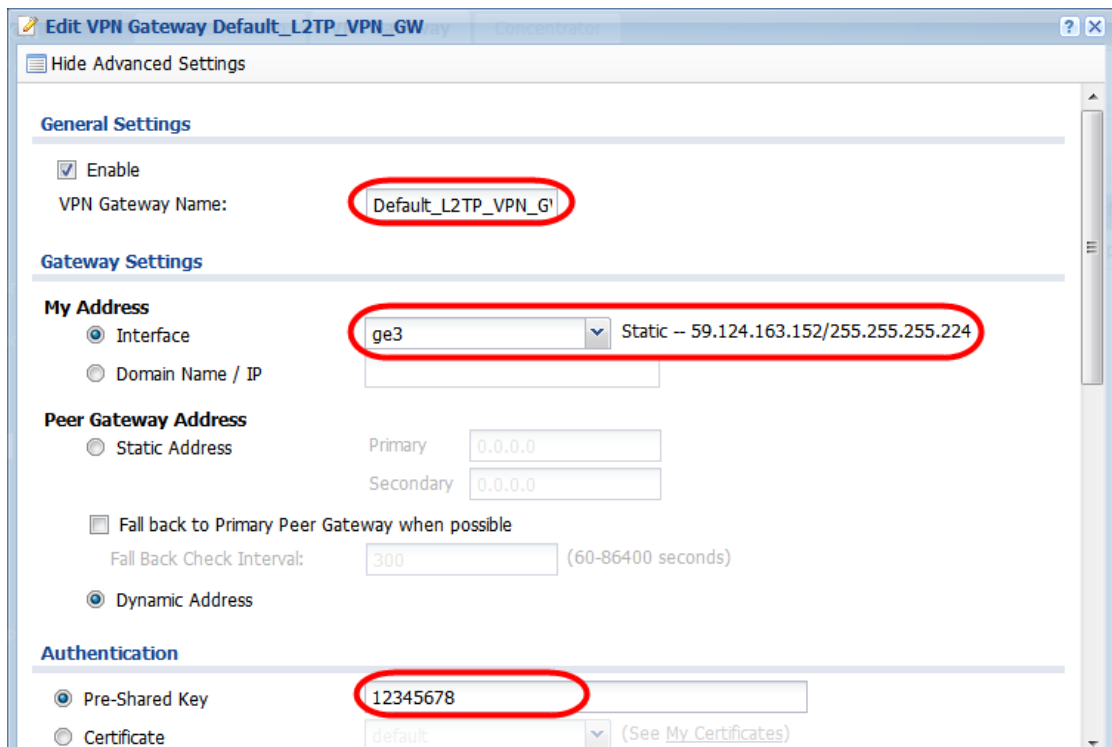
1. Configure a user account for the iPhone use when connecting. Click the **CONFIGURATION > Object > User/Group > User** page to create it. This user will be stored in "Local database".



2. To build up the L2TP over IPSec connection, we have to create the IPSec rule first. Click **CONFIGURATION > VPN > IPSec VPN > VPN Gateway** page to create it. There is one pre-configured default rule for L2TP usage.



3. Edit the default rule by filling in the following information: (click “Show Advanced Settings” first)
- VPN Gateway Name
 - Gateway setting: select the local interface as My Address and set the peer side to use Dynamic Address (Peer Gateway Address)
 - Pre-shared Key; this parameter will also be needed when configuring the iPhone connection.



- Configure the Phase 1 proposal. There is a specific combination that is supported by the iPhone (depending on iOS version). Users can check the Appendix for more details.

Local ID Type: IP
 Content: 0.0.0.0
 Peer ID Type: Any
 Content:

Phase 1 Settings

SA Life Time: 86400 (180 - 3000000 Seconds)
 Negotiation Mode: Main
 Proposal:

#	Encryption	Authentication
1	3DES	SHA1

Key Group: DH2

NAT Traversal
 Dead Peer Detection (DPD)

Extended Authentication

Enable Extended Authentication

Server Mode default
 Client Mode

User Name:
 Password:

Apply Reset OK Cancel

- After the VPN gateway setting is done, click the **CONFIGURATION > VPN > IPSec VPN > VPN Connection** page to create it. There is one pre-configured default rule for L2TP usage.

ZyXEL ZyWALL USG 300

Welcome admin | Logout ? Help About Site Map Object Reference Console CLI

CONFIGURATION

VPN Connection VPN Gateway Concentrator

Global Setting

Use Policy Route to control dynamic IPSec rules
 Ignore "Don't Fragment" setting in packet header

Configuration

#	Status	Name	VPN Gateway	Encapsula...	Algorithm	Policy
1		Default_L2TP_VPN...	Default_L2TP_VPN_GW	TRANSPO...	3DESMD5	USG_300_WAN3/...

Page 1 of 1 Show 50 items Displaying 1 - 1 of 1

6. Edit the default rule by filling in the following information: (click “Show Advanced Settings” first)
 - Connection Name
 - Select the application scenario as **Remote Access (Server Role)** and select the pre-configured VPN Gateway rule.

The screenshot shows the configuration interface for a VPN connection. The window title is "Edit VPN Connection Default_L2TP_VPN_Connection". The interface is divided into two main sections: "General Settings" and "VPN Gateway".

General Settings:

- Enable
- Connection Name: Default_L2TP_VPN_Connection
- Nailed-Up
- Enable Replay Detection
- Enable NetBIOS broadcast over IPSec

VPN Gateway:

- Application Scenario:
 - Site-to-site
 - Site-to-site with Dynamic Peer
 - Remote Access (Server Role)
 - Remote Access (Client Role)
- VPN Gateway: Default_L2TP_VPN_GW | ge3 0.0.0.0 0.0.0.0
- Manual Key:
 - Manual Key
 - My Address:
 - Secure Gateway Address:
 - SPI: (256 - 4095)
 - Encapsulation Mode:

7. For L2TP over IPSec, we must use the Transport mode scenario, the VPN is configured as a Peer-to-Peer tunnel. Thus we have to select the WAN IP address as the Local Policy.

- Configure the Phase 2 proposal. There is a specific combination that is supported by the iPhone (depending on iOS version). Users can check the Appendix for more details.

Active Protocol: ESP
 Encryption Algorithm: DES
 Authentication Algorithm: SHA1
 Encryption Key:
 Authentication Key:

Policy

Local policy: USG_300_WAN3 INTERFACE IP, 59.124.163.152
 Policy Enforcement

Phase 2 Settings

SA Life Time: 86400 (180 - 3000000 Seconds)
 Active Protocol: ESP
 Encapsulation: Transport
 Proposal

#	Encryption	Authentication
1	3DES	MD5

Perfect Forward Secrecy (PFS): none

Connectivity Check

- After the VPN connection setting is done, click **CONFIGURATION > VPN > L2TP VPN > L2TP VPN** page to create it.
 - Select the VPN connection rule
 - Assign the IP address pool
 - Select the Allowed user

ZyXEL ZyWall USG 300

Welcome admin | Logout | ? Help | About | Site Map | Object Reference

CONFIGURATION

Quick Setup

Create new Object

L2TP VPN

General Settings

Enable L2TP Over IPsec

VPN Connection: Default_L2TP_VPN_Conn
 IP Address Pool: LAN_SUBNET
 Authentication Method: default
 Allowed User: iphone
 Keep Alive Timer: 60 (1-180 seconds)
 First DNS Server (Optional): Custom Defined
 Second DNS Server (Optional): Custom Defined
 First WINS Server (Optional):
 Second WINS Server (Optional):

iPhone configuration :

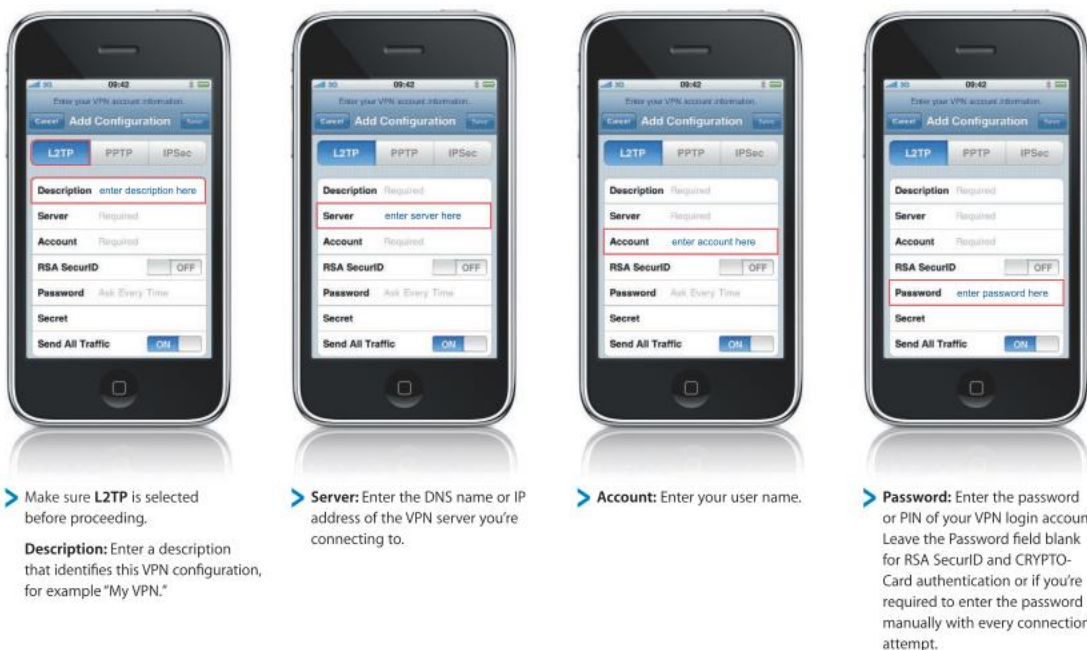
(The description is quoted from Apple iPhone instruction guide,

http://images.apple.com/iphone/business/docs/How_To_Setup_Guide.pdf)

1. Go to the network setup screen by clicking **Settings > General > Network > VPN**.



2. Click the L2TP tab and start to configure it. We need to fill in rule **Description** (e.g. iPhone_L2TP), **Server** address (e.g. www.securityusg.com), **Account** and **Password** that is configured in the USG L2TP allowed user setting.



3. The **RSA SecurID** option is not used. **Secret** must match the Pre-Shared Key from the IPsec Phase-1 rule of the ZyWALL USG. Click **Save** to save the L2TP configuration.

4. Back to the VPN page, the tunnel can be activated via the on / off icon



> **RSA SecurID:** Turn on this option if you're using a RSA SecurID token. Once enabled, the password field is hidden.



> **Secret:** Enter the group's shared secret.



> **Send All Traffic:** Turn off this option to enable split tunneling.



> Tap **Save** once you've entered all your information and settings.

5. If the iPhone "Send all traffic" option is ON, user needs to create a policy route to do SNAT for iPhone to forward traffic to Internet via the L2TP tunnel.

#	Status	User	Schedule	Incoming	Source	Destination	DSCP Code	Service	Next-Hop	DSCP Marking	SNAT	BWM
1		any	none	Default_L2TP_VPN_Connection	any	any	any	any	auto	preserve	outgoing-interface 0	

Page 1 of 1 | Show 50 items | Displaying 1 - 1 of 1

Appendix. iPhone L2TP over IPSec test note

The iPhone L2TP over IPSec VPN has some limitations.

1. For iPhone with iOS 3.x

IKE phase 1—3DES encryption with SHA1 hash method (no md5 support).

DH2 is required when using a pre-shared key.

IPSec phase 2—3DES or AES128 encryption with MD5 or SHA1 hash method.

2. For iPhone with iOS 4.x

IKE phase 1—3DES encryption with SHA1 hash method (no md5 support).

DH2 is required when using a pre-shared key.

IPSec phase 2— AES128 encryption with MD5 or SHA1 hash method.

3DES encryption will not work.

Summary of supported proposal:

	Phase 1	Phase 2
iOS 3.X	3DES-SHA1-DH2	3DES-MD5-none 3DES-SHA1-none AES128-MD5-none AES128-SHA1-none
iOS 4.X	3DES-SHA1-DH2	AES128-SHA1-none