

Configuration Guide



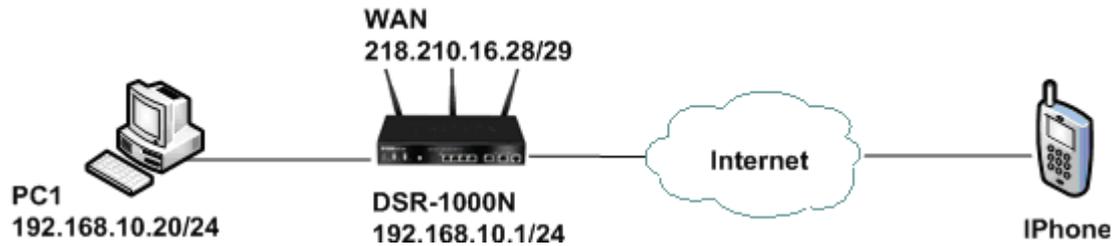
How to establish IPsec VPN Tunnel
between D-Link DSR Router and
iPhone iOS

Overview

The iPhone is a line of smartphones designed and marketed by Apple Inc. It runs Apple's iOS mobile operation system, known as the "iPhone OS". Here we are going to use the built-in IPsec client of iPhone for VPN tunnel connection. Compared to PPTP and L2TP, IPsec VPN can deliver better security by extended authentication (XAUTH) that will authenticate user credential again via iPhone interface while tunnel establishment. With this extra protection, it will effectively avoid any unauthorized users to access critical and sensitive business information through the tunnel. This document describes how to configure both DSR router and iPhone to establish a secure IPsec VPN tunnel between two devices. All screenshots in this document is captured from firmware v1.06B53 of DSR-1000N. If you are not using this version of firmware, the screenshots may not be identically the same as what you see in your D-Link DSR device.

Situation note

IPsec VPN allows road warriors to establish a safe connection to office to access enterprise internal resources or share business documents/plans/information. Since IPsec client had been embedded in many operation system including Windows and Apple IOS, road warriors can easily utilize it without any extra software or APPs installation. This document shows how road warriors connecting to internal PC/Server with full tunnel scenario using iPhone with few easy steps.



Configuration Step

1. Setup Internet Connection:

Please go to [Setup > Internet Settings > WAN1 settings > WAN1 Setup](#)

ISP Connection Type	
ISP Connection Type:	Static IP
Enable VLAN Tag:	<input type="checkbox"/>
VLAN ID:	0
IP Address:	218.210.16.28
IP Subnet Mask:	255.255.255.248
Gateway IP Address:	218.210.16.25

Domain Name System (DNS) Servers	
Primary DNS Server:	8.8.8.8
Secondary DNS Server:	168.95.1.1

MAC Address	
MAC Address Source:	Use Default Address
MAC Address:	00:00:00:00:00:00

ISP Connection Type: please select your ISP connections. In this example, it's Static IP. ISP Configuration type will probably be different depends on your environment.

2. Create a user group for IPsec extended authentication

Please go to [Advanced > Users > Groups](#)

Group Configuration	
Group Name:	<input type="text" value="XAUTH"/>
Description:	<input type="text" value="For_iphone_IPsec"/>

User Type	
PPTP User:	<input type="checkbox"/>
L2TP User:	<input type="checkbox"/>
Xauth User:	<input checked="" type="checkbox"/>
SSLVPN User:	<input type="checkbox"/>
Admin:	<input type="checkbox"/>
Guest User (readonly):	<input type="checkbox"/>
Captive Portal User:	<input type="checkbox"/>

Group Name: please provide a name for the group.

Description: please provide proper description for the group.

User Type: Enable Xauth User

3. Create a user account belong to XAUTH user group

Please go to [Advanced > Users > Users](#)

Users Configuration	
User Name:	<input type="text" value="john"/>
First Name:	<input type="text" value="john"/>
Last Name:	<input type="text" value="smith"/>
Select Group:	<input type="text" value="XAUTH"/>
Password:	<input type="password" value="••••••••"/>
Confirm Password:	<input type="password" value="••••••••"/>
Idle Time Out:	<input type="text" value="10"/> (Minutes)

User Name: this is actually user account for authentication, it's case sensitive. Here we use john for example.

First Name/Last Name: please provide proper description for user identification.

Select Group: please select XAUTH that we just created in previous step.

Password: Please configure password for the user.

Confirm Password: Input password again for confirmation.

Idle Time Out: here we configure 10 minutes for idle time out.

4. Create a policy for iPhone IPsec client:

Please go to [SETUP > VPN Settings > IPsec > IPsec Policies](#)

4.1 General Setting

General	
Policy Name:	IPsec_for_iPhone
Policy Type:	Auto Policy
IKE Version:	<input checked="" type="radio"/> IPv4 <input type="radio"/> IPv6
IKE Version:	<input checked="" type="radio"/> IKEv1 <input type="radio"/> IKEv2
IPsec Mode:	Tunnel Mode
Select Local Gateway:	Dedicated WAN
Remote Endpoint:	FQDN
	0.0.0.0
Enable Mode Config:	<input checked="" type="checkbox"/>
Enable NetBIOS:	<input type="checkbox"/>
Enable RollOver:	<input type="checkbox"/>
Protocol:	ESP
Enable DHCP:	<input type="checkbox"/>
Local IP:	Subnet
Local Start IP Address:	192.168.10.0
Local End IP Address:	
Local Subnet Mask:	255.255.255.0
Local Prefix Length:	
Remote IP:	Any
Remote Start IP Address:	

Policy Name: please configure a name for policy management purpose.

Policy type: Default setting is **Auto Policy**, please leave this option as default setting.

IP Protocol Version: Please configure to **IPv4** (default setting).

IKE Version: Please configure to **IKEv1** (default setting).

IPsec Mode: Default is **Tunnel Mode**, please keep this option as default setting.

Select Local Gateway: Please keep this setting as **Dedicated WAN**.

Remote Endpoint: Please select **FQDN** with **0.0.0.0** configuration.

Enable Mode Config: Please **Enable** this check box.

Protocol: Please configure **ESP** to IPsec protocol.

Local IP: Here is to define local network scope for IPsec connectivity. Please select **Subnet** in this example.

Local Start IP Address: Please configure **192.168.10.0** in this example for network address of DSR LAN network.

Local Subnet Mask: Please configure **255.255.255.0** in this example for Subnet Mask of DSR LAN networks.

Remote IP: Please configure to **Any** in this option. The Remote IP means iPhone's IP address which usually assigned by ISP for road warriors scenario.

4.2 Phase 1 (IKE SA Parameters) settings

Phase1 (IKE SA Parameters)	
Exchange Mode:	Main ▾
Direction / Type:	Responder ▾
Nat Traversal:	
On:	<input checked="" type="radio"/>
Off:	<input type="radio"/>
NAT Keep Alive Frequency (in seconds):	20
Local Identifier Type:	FQDN ▾
Local Identifier:	192.168.10.0
Remote Identifier Type:	FQDN ▾
Remote Identifier:	0.0.0.0
Encryption Algorithm:	
DES:	<input type="checkbox"/>
3DES:	<input type="checkbox"/>
AES-128:	<input checked="" type="checkbox"/>
AES-192:	<input type="checkbox"/>
AES-256:	<input type="checkbox"/>
BLOWFISH:	<input type="checkbox"/> [Redacted]
CAST128:	<input type="checkbox"/> [Redacted]
Authentication Algorithm:	
MD5:	<input type="checkbox"/>
SHA-1:	<input checked="" type="checkbox"/>
SHA2-256:	<input type="checkbox"/>
SHA2-384:	<input type="checkbox"/>
SHA2-512:	<input type="checkbox"/>
Authentication Method:	Pre-shared key ▾
Pre-shared key:	1234567890
Diffie-Hellman (DH) Group:	Group 2 (1024 bit) ▾
SA-Lifetime (sec):	28800
Enable Dead Peer Detection:	<input type="checkbox"/>
Detection Period:	10
Reconnect after failure count:	3
Extended Authentication:	Edge Device ▾
Authentication Type:	User Database ▾
User Name:	[Redacted]
Password:	[Redacted]

Exchange Mode: *Main mode*

Direction/Type: *Responder*

NAT Traversal: *ON*

Local Identifier Type: *FQDN*

Local Identifier: *192.168.10.0*

Remote Identifier Type: *FQDN*

Remote Identifier: *0.0.0.0*

Encryption Algorithm: *AES-128*

Authentication Algorithm: *SHA-1*

Authentication Method: *Pre-shared Key*

Pre-shared Key: Please configure a proper pre-shared key and this setting will be used on iPhone setting. In this case, the Pre-Shared Key is 1234567890 for example.

Diffie-Hellman (DH) Group: *Group 2 (1024 bit)*

SA-Lifetime (sec): *28800*

Extended Authentication: *Edge Device*

Authentication Type: *User Database*

4.3 Phase 2 (Auto Policy Parameters) settings

Phase2-(Auto Policy Parameters)

SA Lifetime: **seconds** ▼

Encryption Algorithm:

DES:

NONE:

3DES:

AES-128:

AES-192:

AES-256:

TWOFISH (128):

TWOFISH (192):

TWOFISH (256):

BLOWFISH:

CAST128:

Integrity Algorithm:

MD5:

SHA-1:

SHA2-224:

SHA2-256:

SHA2-384:

SHA2-512:

PFS Key Group: **DH Group 2 (1024 bit)** ▼

SA Lifetime (sec): 3600 seconds

Encryption Algorithm: AES-128

Integrity Algorithm: SHA-1

5. Configure IPsec Mode Config

Please go to [Setup > VPN Settings > IPsec > IPsec Mode Config](#)

IPsec Mode Config Configuration	
Tunnel Mode:	Full Tunnel ▾
Start IP Address:	192.168.12.100
End IP Address:	192.168.12.254
Primary DNS(Optional):	8.8.8.8
Secondary DNS(Optional):	168.95.192.1
Primary WINServer(Optional):	
Secondary WINServer (Optional):	

Tunnel Mode: Full Tunnel

Start IP Address: 192.168.12.100

End IP Address: 192.168.12.254

Primary DNS (Optional): 8.8.8.8 (This setting will assign DNS Server information to iPhone.)

Secondary DNS (Optional): 168.95.192.1 (Please assign a secondary DNS server to ensure name resolution still works properly if Primary DNS Server is down).

iPhone Setup

1. Create a IPsec VPN profile

Please go to [Settings > General > Network > VPN > Add VPN Configuration...](#)

The screenshot shows the 'Add Configuration' screen in an iPhone settings app. At the top, there are 'Cancel' and 'Save' buttons. Below them are three tabs: 'L2TP', 'PPTP', and 'IPSec', with 'IPSec' selected. The main configuration area includes the following fields:

- Description:** DSR-1000N
- Server:** DSR_WAN_IP
- Account:** XAUTH User Account
- Password:** Ask Every Time
- Use Certificate:** A toggle switch set to 'OFF'.
- Group Name:** An empty text field.
- Secret:** A field with ten blue dots representing a masked password.

At the bottom, there is a 'Proxy' section with three buttons: 'Off' (selected), 'Manual', and 'Auto'.

Description: A profile name for this IPsec VPN connection.

Server: Please enter an IP address of DSR WAN interface. In this example, it should be 218.210.16.28.

Account: Please fill-out your user account belong to XAUTH group. In this example, it should be "john" that we just created in the step 3.

Password: Not Required. iPhone will automatically pop up a window to request password authentication while IPsec tunnel establishment.

Group Name: Not Required.

Secret: Please fill in the Pre-shared key information that you have configured in step 4.2. In this case, the pre-shared key is 1234567890.

Proxy: Off

2. Launch IPsec VPN tunnel connection to DSR router.

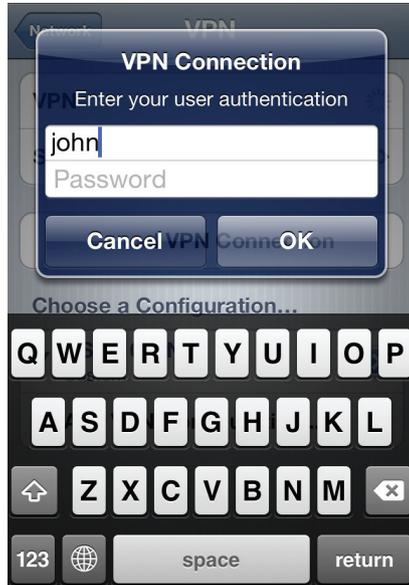
Please go to [Settings > General > Network > VPN](#):



Choose a Configuration: Please ensure that selected profile is correct since iPhone allows creating multiple profiles. In this case, please select “DSR-1000N” that we just created in the step 1.

VPN: please switch to “ON” to launch IPsec VPN tunnel connecting to DSR router.

3. Input user password in pop-up window of iPhone



Password: Please fill in password you have created in DSR configuration step 3.

D-Link[®]

Visit our website for more information
www.dlink.com

D-Link, D-Link logo, D-Link sub brand logos and D-Link product trademarks are trademarks or registered trademarks of D-Link Corporation and its subsidiaries.
All other third party marks mentioned herein are trademarks of the respective owners.

Copyright © 2011 D-Link Corporation. All Rights Reserved.