

How to Configure UTM and Apple iPhone and iPad for IPSec VPN

Let's say you have an Apple iPhone or iPad and would like to use its built-in VPN client to VPN into your UTM. Here is how you would do this.

This document is a reference for UTM administrators to configure a mode-config policy to accept Apple iPhone's native VPN client connections. This is applicable for Apple iPhone 2G, 3G, 3GS, and 4 and iPad.

NOTE: AT&T US has VPN restrictions which may prohibit the iPhone from being able to see other devices on the remote VPN network when going through the AT&T data network. To bypass this restriction, use a wifi connection when trying to VPN.

1. UTM VPN Configuration

The IPSec VPN client policy required on the UTM to accept Apple iPhone VPN connections consists of a mode config record and a corresponding IKE policy. It is not required to know the IP address of the iPhone in advance in order to create a client policy on the UTM that will allow the VPN client to be authenticated.

1.1. Mode Config Record

Use mode config to create a pool of IP addresses to assign the remote iPhone VPN clients. Note that one or more IKE policies may use the same mode config record; a unique record for iPhone VPN clients is not required. **Note:** if you wish to access the Internet after the VPN is connected be sure to add the UTM LAN IP address (or another valid DNS server) as the DNS Server.

After defining the IP address range, use the default encryption and integrity for security the traffic tunnel. One key configuration requirement for the iPhone VPN client is that the Local IP Address and Local Subnet Mask must not specify an address or network. By settings these fields to 0, the associated policy will be anonymous.

The required security settings for the mode config record are as follow:

Encryption Algorithm	AES-128
Integrity Algorithm	SHA-1
Local IP Address	0.0.0.0
Local Subnet Mask	0.0.0.0
PFS Key Group	DH Group2
SA lifetime	3600

Edit Mode Config Record

Operation succeeded.

Client Pool

Record Name:

First Pool: Starting IP . . . Ending IP . . .

Second Pool: Starting IP . . . Ending IP . . .

Third Pool: Starting IP . . . Ending IP . . .

WINS Server: Primary . . . Secondary . . .

DNS Server: Primary . . . Secondary . . .

Traffic Tunnel Security Level

PFS Key Group:

SA Lifetime:

Encryption Algorithm:

Integrity Algorithm:

Local IP Address: . . .

Local Subnet Mask: . . .

Apply **Reset**

1.2. IKE Policy

Once the mode config record for the VPN client is created, create an IKE policy with the following parameters:

Exchange Mode	Main
Remote Identifier Type	FQDN
Remote Identifier data	0.0.0.0
Encryption Algorithm	AES-128
Authentication Algorithm	SHA-1
Authentication Method	Pre-shared key
Diffie-Hellman (DH) Group	DH Group2
XAUTH Configuration	Edge Device

Note that "Aggressive" exchange mode is not supported by the iPhone VPN client. As well the Remote Identifier data must be 0.0.0.0 as the iPhone VPN client's IP address is typically not known by the UTM admin or consistent.

Mode Config Record

Do you want to use Mode Config Record?

Yes No

Select Mode Config:

Record:

General

Policy Name:

Direction / Type:

Exchange Mode:

Local

Select Local Gateway: WAN1 WAN2

Identifier Type:

Identifier:

Remote

Identifier Type:

Identifier:

IKE SA Parameters

Encryption Algorithm:

Authentication Algorithm:

Authentication Method: Pre-shared key RSA-Signature

Pre-shared key: (Key Length 8 - 49 Char)

Diffie-Hellman (DH) Group:

SA-Lifetime (sec):

Enable Dead Peer Detection: Yes No

Detection Period: (Seconds)

Reconnect after failure count:

Extended Authentication

XAUTH Configuration

None

Edge Device

IPSec Host

Authentication Type:

Username:

Password:

1.3. Create an IPsec VPN User on the UTM

Next, create an IPsec VPN User on the UTM. To do this, go to **Users** and click on the **Add** button.

The screenshot shows the 'Add User' configuration page in the UTM interface. The navigation bar at the top includes 'Network Config', 'Network Security', 'Application Security', 'VPN', 'Users', 'Administration', 'Monitoring', 'Support', and 'Wizards'. The 'Users' section is active, showing a breadcrumb trail: ':: Users :: Groups :: Domains ::'. The 'Add User' form contains the following fields:

- User Name:
- User Type:
- Select Group:
- Password:
- Confirm Password:
- Idle Timeout: Minutes

At the bottom of the form, there are two buttons: **Apply** and **Reset**.

2. Apple iPhone VPN Client Configuration

The Apple iPhone VPN client will require the IKE policy settings to match on the client side.

Server	UTM's WAN IP address
Account	Username in the local User Database
Password	Password to authenticate Username
Use Certificate	Off
Group Name	Group for Username if configured
Secret	Pre-shared key from the IKE SA
Proxy	Off



And you're done!