Application Notes

How to Configure UTM with Apple OSX and iOS Devices for IPsec VPN

Table of Contents

Concepts

NETGEAR® ProSecure® and ProSafe® security appliances are non-compromising network security solutions for midsized IT environments. They are tailored to deliver reliable, affordable, and simple network protection that businesses demand.

Secure connectivity is essential for today's business environment. With today's growing remote workforce, the need to connect back to the central office from a remote location is greater than ever. The NETGEAR UTM supports both IPsec and SSL VPN.

In this application note, we will go over the steps on how to setup IPsec VPN with the UTM and the native Mac/iOS VPN client.

This document is a reference for UTM administrators to configure a mode-config policy to accept VPN client connections from the built-in VPN client of Apple Mac OSX and Apple iOS devices. The following guide was written for OSX but is also applicable for other iOS based devices such as iPhone, iPad, and iPod Touch.

NOTE: AT&T US and some other carriers have 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.

Components

The following requirements are needed when using this guide for implementation:

Product	Model/Release	Version
NETGEAR ProSecure UTM Series	All UTM models	Firmware version 1.3.7-0 and above
Apple Mac running OSX	OSX	Version 10.6.8 and above
Apple iOS compatible device	iPhone, iPad, iPod Touch	iOS version 4.0 and above

Configuration Steps

UTM VPN Configuration

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

Mode Config Record

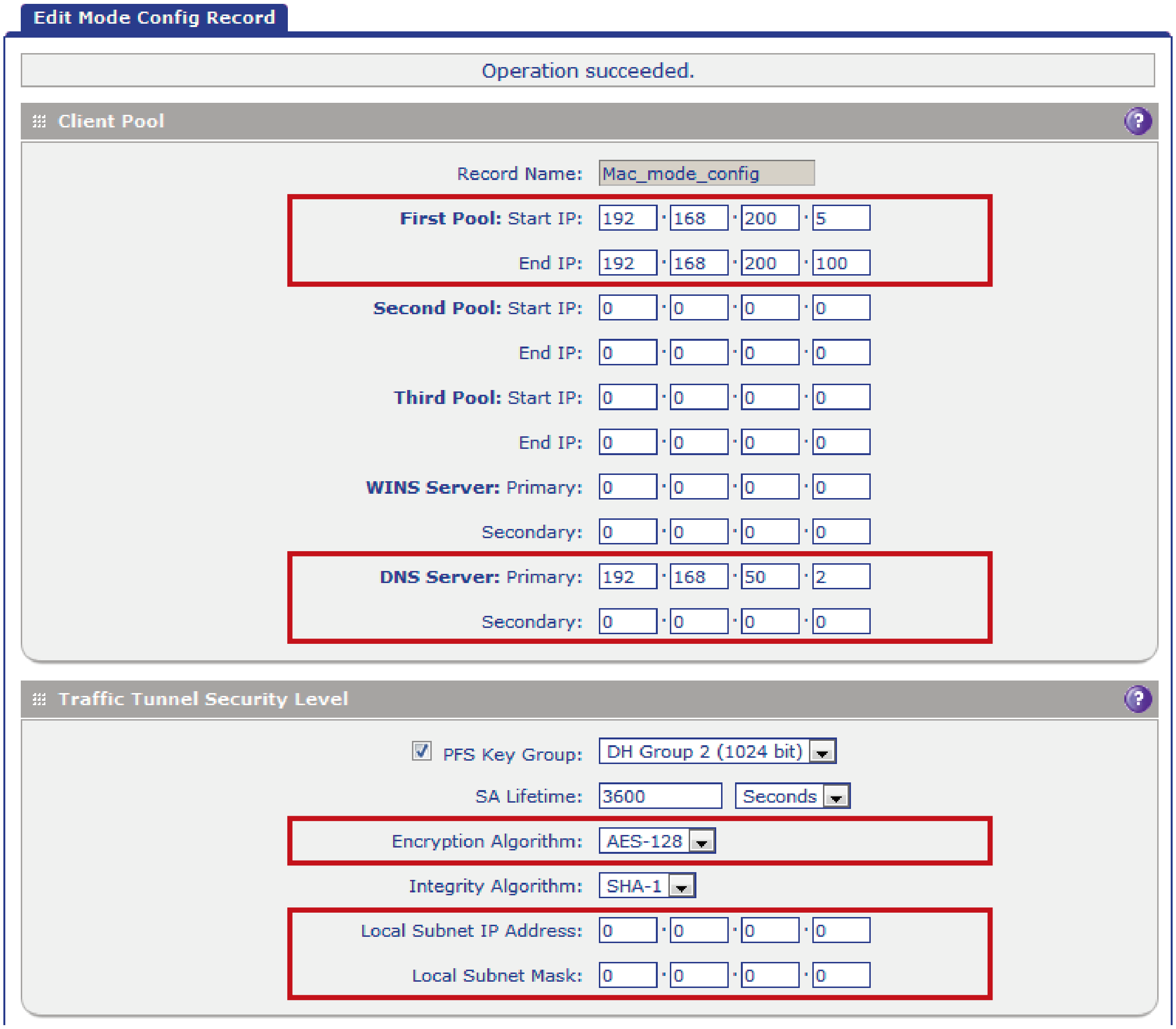
Use mode config to create a pool of IP addresses to assign the remote Mac VPN clients. Note that one or more IKE policies may use the same mode config record; a unique record for Mac VPN clients is not required.

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 Mac 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 follows:

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: Mac_mode_config

First Pool: Start IP: 192.168.200.5

End IP: 192.168.200.100

Second Pool: Start IP: 0.0.0.0

End IP: 0.0.0.0

Third Pool: Start IP: 0.0.0.0

End IP: 0.0.0.0

WINS Server: Primary: 0.0.0.0

Secondary: 0.0.0.0

DNS Server: Primary: 192.168.50.2

Secondary: 0.0.0.0

Traffic Tunnel Security Level

☑ PFS Key Group: DH Group 2 (1024 bit)

SA Lifetime: 3600 Seconds

Encryption Algorithm: AES-128

Integrity Algorithm: SHA-1

Local Subnet IP Address: 0.0.0.0

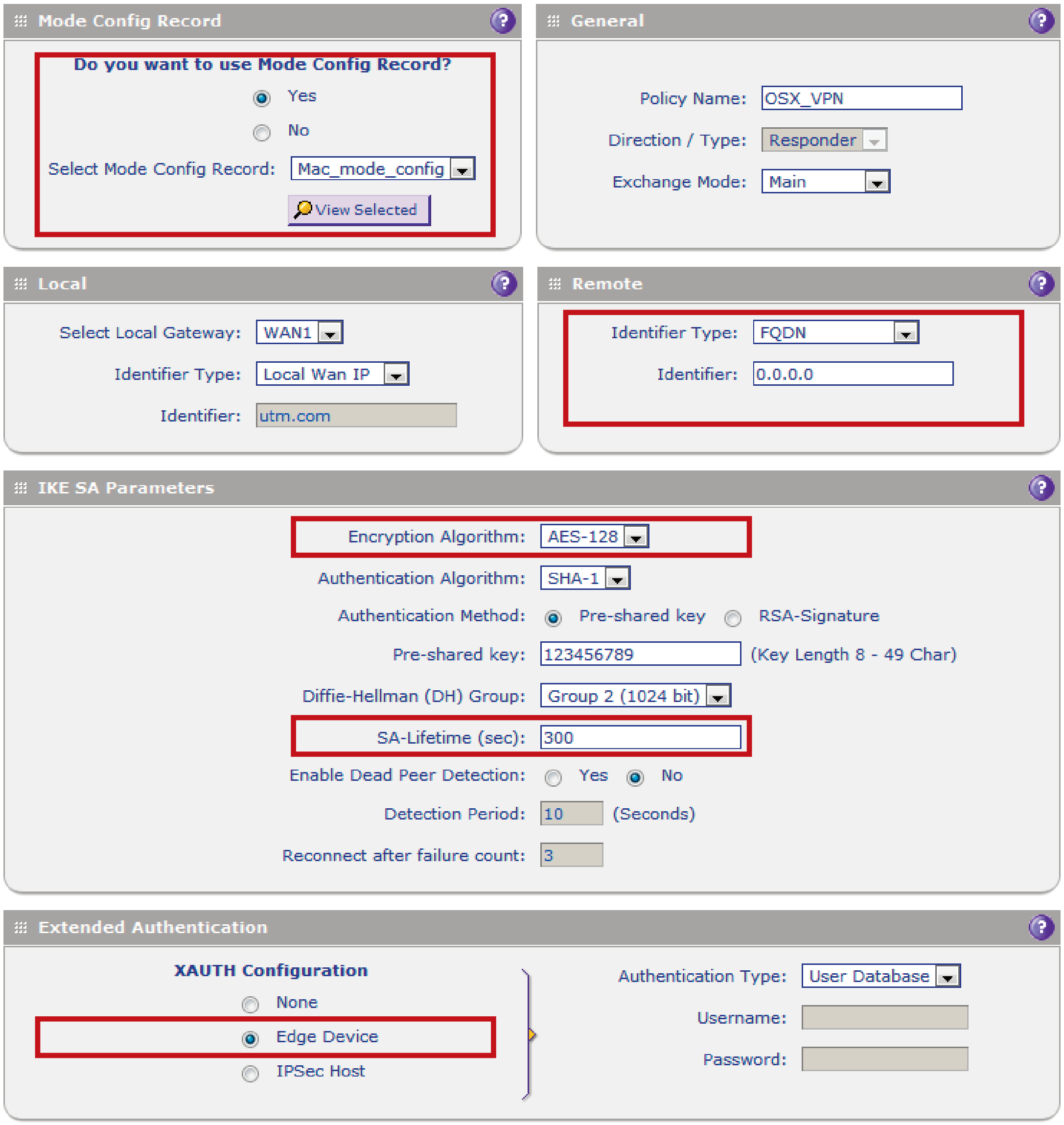
Local Subnet Mask: 0.0.0.0

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 Mac VPN client. As well the Remote Identifier data must be 0.0.0.0 as the Mac 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: Mac_mode_config

General

Policy Name: OSX_VPN

Direction / Type: Responder

Exchange Mode: Main

Local

Select Local Gateway: WAN1

Identifier Type: Local Wan IP

Identifier: utm.com

Remote

Identifier Type: FQDN

Identifier: 0.0.0.0

IKE SA Parameters

Encryption Algorithm: AES-128

Authentication Algorithm: SHA-1

Authentication Method: ● Pre-shared key ○ RSA-Signature

Pre-shared key: 123456789 (Key Length 8 - 49 Char)

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

SA-Lifetime (sec): 300

Enable Dead Peer Detection: ○ Yes ● No

Detection Period: 10 (Seconds)

Reconnect after failure count: 3

Extended Authentication

XAUTH Configuration

○ None

● Edge Device

○ IPSec Host

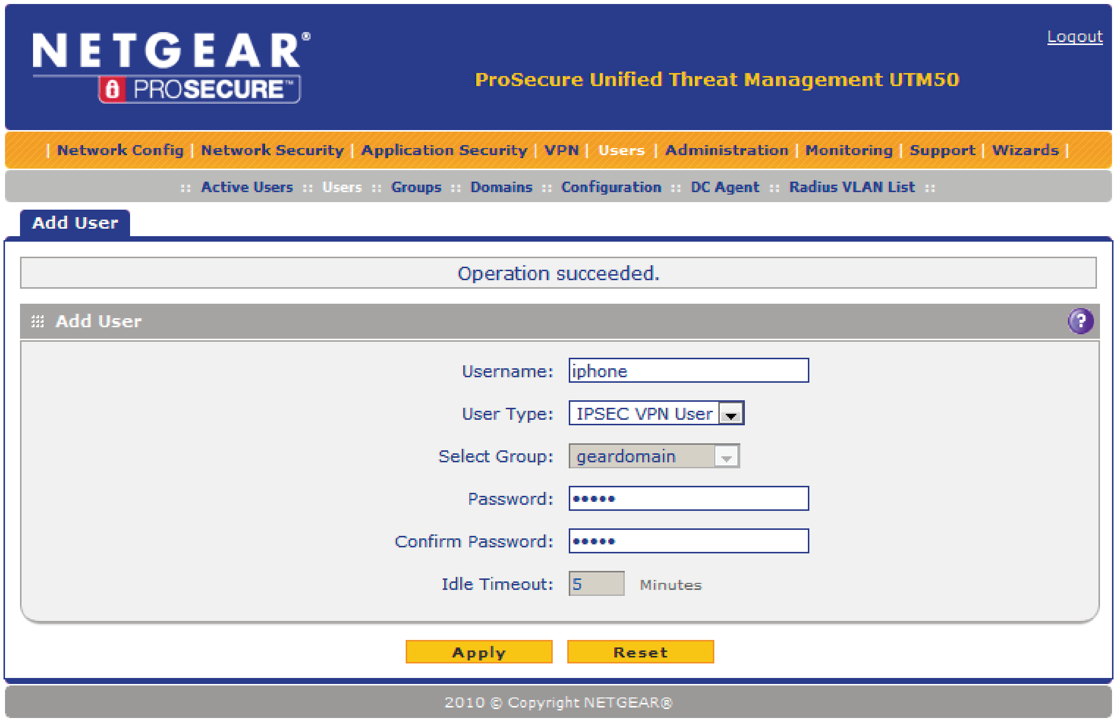
Authentication Type: User Database

Username:

Password:

Create an IPSec User Account

1. Go to **Users -> Users** and click on **Add**.
2. Enter the **Username** and select **IPSEC VPN User** as the **User Type**.
3. Enter the **Password** for the user.
4. Click **Apply**.


NETGEAR
PROSECURE
Logout
ProSecure Unified Threat Management UTM50
| Network Config | Network Security | Application Security | VPN | Users | Administration | Monitoring | Support | Wizards |
:: Active Users :: Users :: Groups :: Domains :: Configuration :: DC Agent :: Radius VLAN List ::
Add User
Apply
Reset
2010 © Copyright NETGEAR®

Operation succeeded.

Add User

Username: iphone

User Type: IPSEC VPN User

Select Group: geardomain

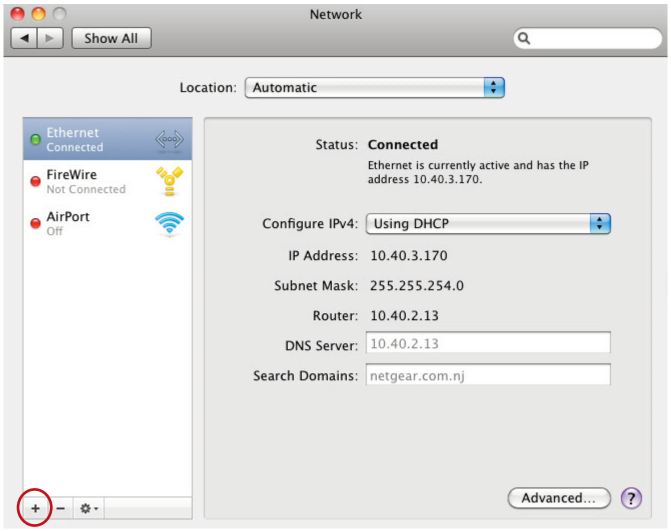
Password: •••••

Confirm Password: •••••

Idle Timeout: 5 Minutes

Mac VPN Client Configuration

1. Open System Preferences --> Network
2. Click the plus sign



Location: Automatic

Status: **Connected**

Ethernet is currently active and has the IP address 10.40.3.170.

Configure IPv4: Using DHCP

IP Address: 10.40.3.170

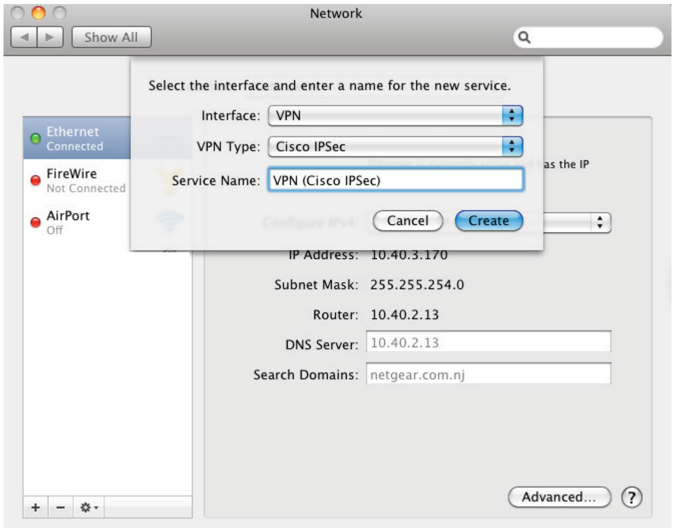
Subnet Mask: 255.255.254.0

Router: 10.40.2.13

DNS Server: 10.40.2.13

Search Domains: netgear.com.nj

3. Chose VPN as the interface. Choose Cisco IPSec as the VPN type, and supply a service name as a description (an arbitrary name for the connection, whatever makes sense to you).



Select the interface and enter a name for the new service.

Interface: VPN

VPN Type: Cisco IPSec

Service Name: VPN (Cisco IPSec)

IP Address: 10.40.3.170

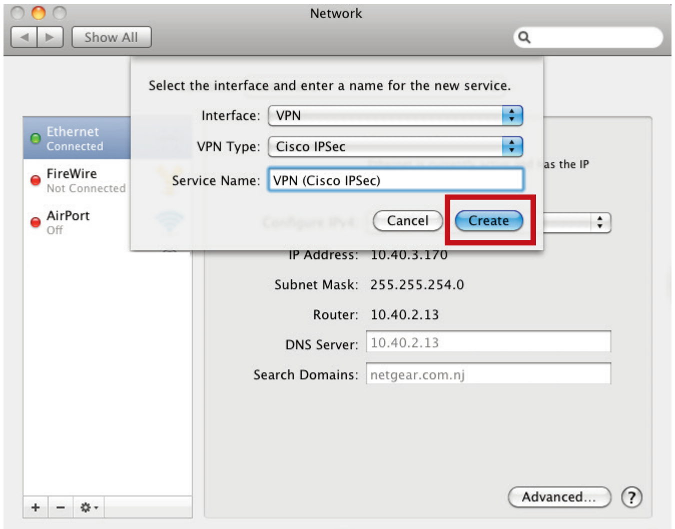
Subnet Mask: 255.255.254.0

Router: 10.40.2.13

DNS Server: 10.40.2.13

Search Domains: netgear.com.nj

4. Click Create.



Select the interface and enter a name for the new service.

Interface: VPN

VPN Type: Cisco IPSec

Service Name: VPN (Cisco IPSec)

IP Address: 10.40.3.170

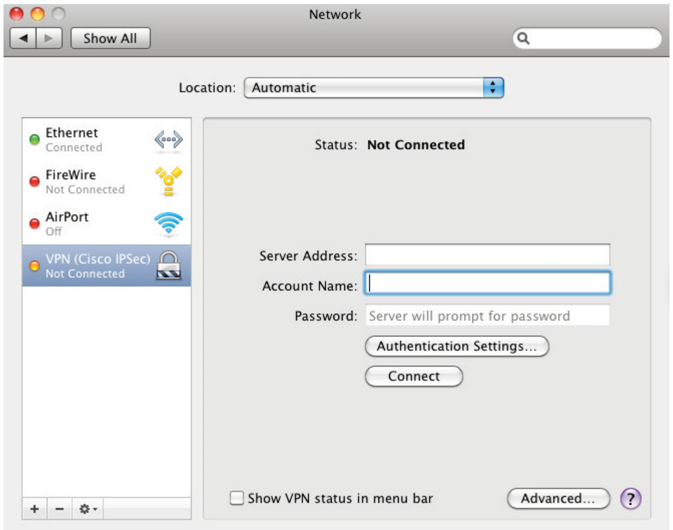
Subnet Mask: 255.255.254.0

Router: 10.40.2.13

DNS Server: 10.40.2.13

Search Domains: netgear.com.nj

5. Enter the Server Address and Account name.



Location: Automatic

Status: Not Connected

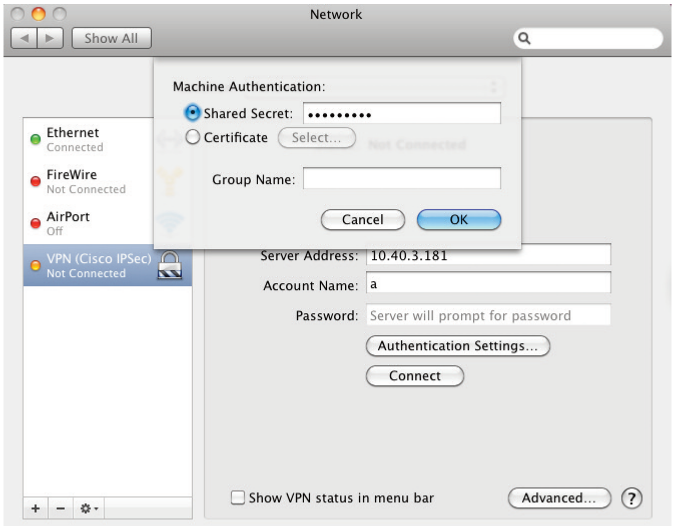
Server Address:

Account Name:

Password: Server will prompt for password

□ Show VPN status in menu bar

6. Click **Authentication Settings**, enter the Shared Secret, Click **OK**.



Network

Machine Authentication:

◉ Shared Secret: •••••••••

○ Certificate

Group Name:

Ethernet Connected

FireWire Not Connected

AirPort Off

VPN (Cisco IPSec) Not Connected

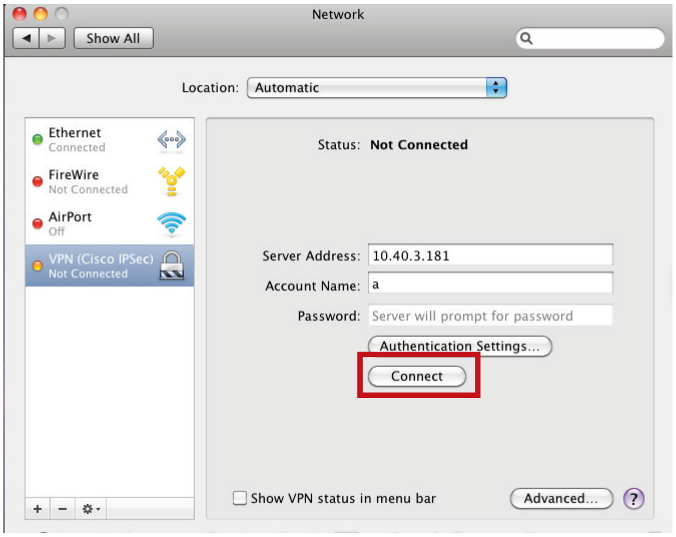
Server Address: 10.40.3.181

Account Name: a

Password: Server will prompt for password

□ Show VPN status in menu bar

7. Click **Connect**.



Network

Location: Automatic

Ethernet Connected

FireWire Not Connected

AirPort Off

VPN (Cisco IPSec) Not Connected

Status: **Not Connected**

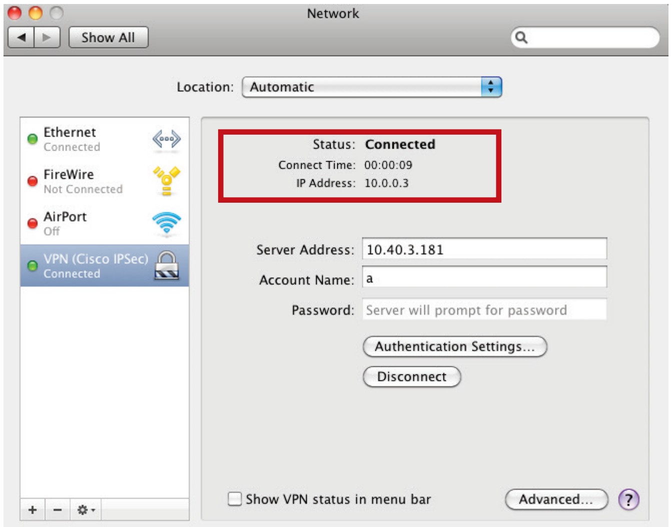
Server Address: 10.40.3.181

Account Name: a

Password: Server will prompt for password

□ Show VPN status in menu bar

The VPN tunnel between the UTM and Mac is now established.



Network

Location: Automatic

Ethernet Connected

FireWire Not Connected

AirPort Off

VPN (Cisco IPSec) Connected

Status: **Connected**

Connect Time: 00:00:09

IP Address: 10.0.0.3

Server Address: 10.40.3.181

Account Name: a

Password: Server will prompt for password

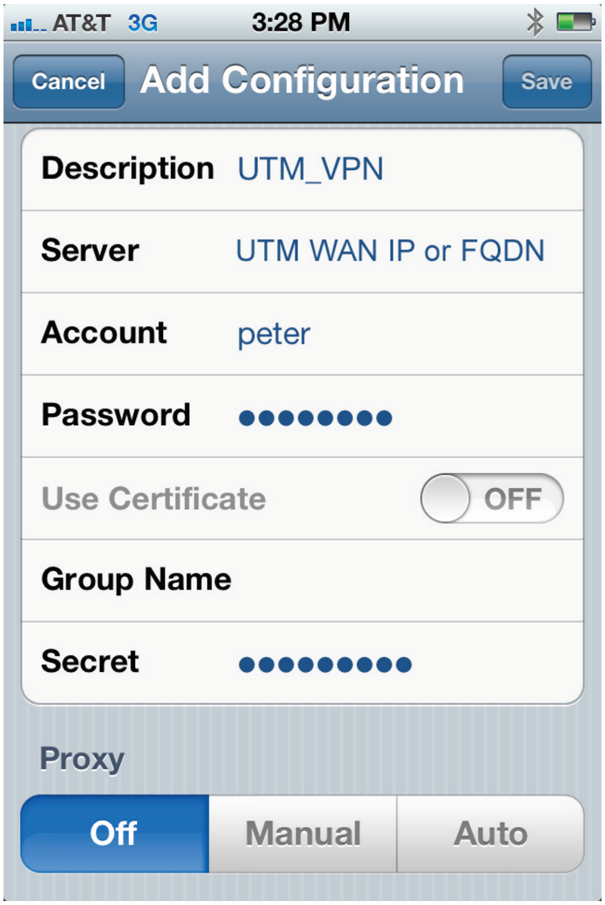
□ Show VPN status in menu bar

iOS VPN Client Configuration (for iPhone, iPad, iPod Touch)

First, select the IPSec tab.

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



Description UTM_VPN

Server UTM WAN IP or FQDN

Account peter

Password ●●●●●●●●

Use Certificate OFF

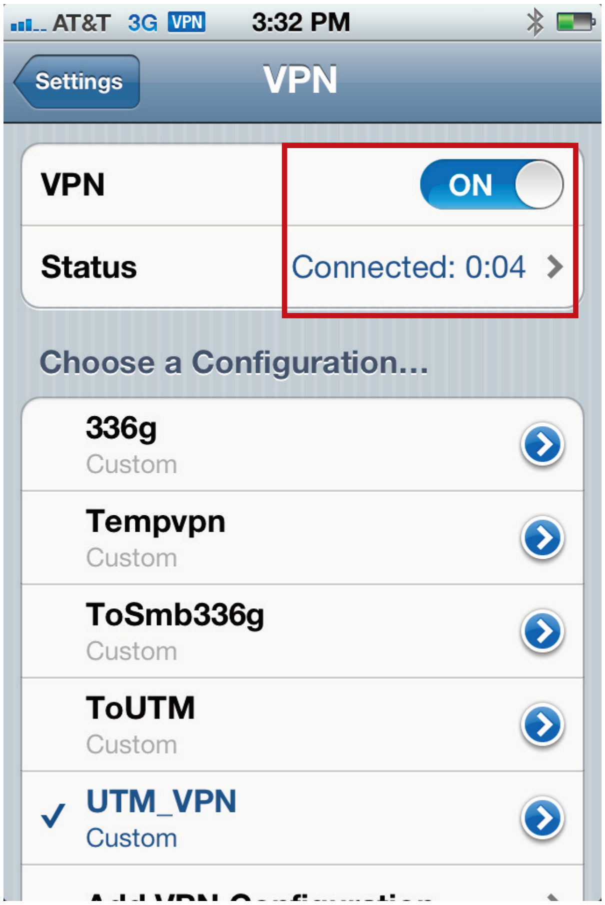
Group Name

Secret ●●●●●●●●●

Proxy

Off | Manual | Auto

The VPN tunnel between the UTM and Mac is now established.



VPN: ON

Status: Connected: 0:04

Conclusion

Following the steps above, we have successfully established an IPsec VPN connection between the UTM and an Apple OSX/iOS device. This will allow Macs/iPhones/iPads, etc. to securely access network resources remotely. For complete information on configuring ProSecure UTM Unified Threat Management appliances please reference the UTM Series Reference Manual.