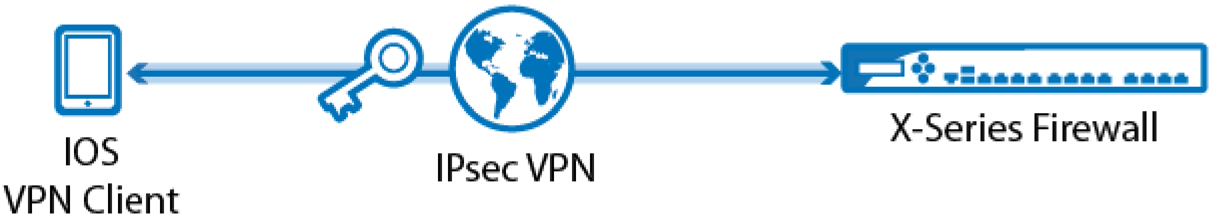
How to Configure Apple iOS VPN Client for IPsec VPN with Certificate Authentication

https://campus.barracuda.com/doc/28475731/

Because certificates longer than 512-bit do not work for iOS VPN clients with iOS version 6.0, it is recommended that you update to the latest version of iOS.

For client-to-site IPsec VPN connections, you can use Apple iOS devices. Follow the steps in this article to configure Apple iOS devices for IPsec VPN connections with the Barracuda NextGen Firewall X-Series.



Before you Begin

To use Apple iOS devices to connect to a client-to-site IPsec VPN, you must have the following:

- Apple device with iOS 5.1 or above.
- How to Configure a Client-to-Site VPN with Certificate Authentication.
- Root, server, and client certificates that meet the requirements set by Apple.
  The following table shows the required X.509 certificates, their settings, and where they must be installed.

X.509 Certificate Type	Installation Device	File Type	Chain of Trust	X.509 Extensions and Values
Root Certificate	Barracuda NextGen Firewall X-Series + Apple iOS Device	PEM	Trust Anchor	◦ Mandatory option for key usage**:** **Certificate sign**; **CRL sign**.

Server Certificate	Barracuda NextGen Firewall X-Series	PKCS12	End Instance	◦ **Subject Alternative Name**: Only use the DNS tag with a FQDN which resolves to the IP address the VPN Service or a wildcard certificate. Do not use the IP tag. E.g., *DNS:vpnserver.yourdomain.com or DNS:** ◦ **Key Usage -** Including the "Digital Signature" flag.
Client Certificate	Apple iOS Device	PKCS12	End Instance	◦ **Key Usage** - Including the "Digital Signature" flag.

When creating X.509 certificates:

- Do not use identical **Subject Alternative Names** settings. **Subject Alternative Names** must also not contain the management IP address of the X-Series Firewall.
- Only use the X.509 extensions that are listed in the table above.

Example iOS Certificate Settings

Root Certificate

Tab	Setting	Value
Status	**Signature Algorithm**	sha1WithRSAEncryption
Subject	**RFC 2253**	emailAddress=support@barracuda.com,OU=documentation,O=Barracuda Networks,L=Innsbruck,ST=Tirol,C=AT
	Hash	7b6d2374
Extensions	**X509v3 Basic Constraints**	CA:TRUE
	X509v3 Key Usage	Digital Signature, Key Agreement, Certificate Sign

Server Certificate

Tab	Setting	Value
Status	**Signature Algorithm**	sha1WithRSAEncryption
Subject	**RFC 2253**	emailAddress=support@barracuda.com,OU=docu,O=Barracuda Network AG,L=Innsbruck,ST=Tyrol,C=AT
	Hash	cc0460b5

Issuer	**RFC 2253**	emailAddress=support@barracuda.com,OU=documentation,O=Barracuda Networks,L=Innsbruck,ST=Tirol,C=AT
	Hash	7b6d2374
Extensions	**X509v3 Key Usage**	Digital Signature, Key Agreement, Certificate Sign
	X509v3 Subject Alternative Name:	DNS:vpnserver.yourdomain.com

Client Certificate

Tab	Setting	Value
Status	**Signature Algorithm**	sha1WithRSAEncryption
Subject	**RFC 2253**	emailAddress=support@barracuda.com,OU=documentation,O=Barracuda Networks,L=Innsbruck,ST=Tyrol,C=AT
	Hash	c2b06d20
Issuer	**RFC 2253**	emailAddress=support@barracuda.com,OU=documentation,O=Barracuda Networks,L=Innsbruck,ST=Tirol,C=AT
	Hash	7b6d2374
Extensions	**X509v3 Key Usage**	Digital Signature

Configure the Apple iOS Device

Import the certificates

You must import the root and the client certificate on the Apple iOS device. You can import the certificate via email or by downloading it from a web server. If you are using a Mobile Device Management (MDM) server, you can also push the certificates to your devices.

Configure the Client-To-Site VPN

To configure an Apple iOS device for IPsec VPN connections with the X-Series Firewall:

1. On the iOS device, tap **Settings > General > VPN > Add VPN Configuration**.
2. On the **Add VPN configuration** screen, tap the **IPsec** tab.
3. Configure the following settings:
    - **Server** – The Subject Alternative Name used in your certificates.

    - **Account** and **Password** – The XAUTH username and password.
    - **Use Certificate** – Enable this setting.
    - **Certificate** – The X.509 client certificate.
4. Tap **Save** in the top right corner. The VPN configuration then appears on the **VPN** screen.

Connect to the VPN with the Apple iOS Device

After configuring the Apple device, you can connect to the IPsec VPN.

On your Apple iOS device, tap **Settings** and then turn on **VPN**. After a few seconds, the VPN icon appears in the status bar to indicate that the connection is successful.

> Establishing VPN through NAT can be problematic. If you experience connection losses, increase the UDP timeout on the NAT'd device. For example, the iPhone sends keepalive packets every 60 seconds, so you can enter any value over 60 seconds.
>
> Unfortunately, many cell phone providers use NAT to connect mobile devices to the internet. Contact your cell phone provider support for help.

Figures