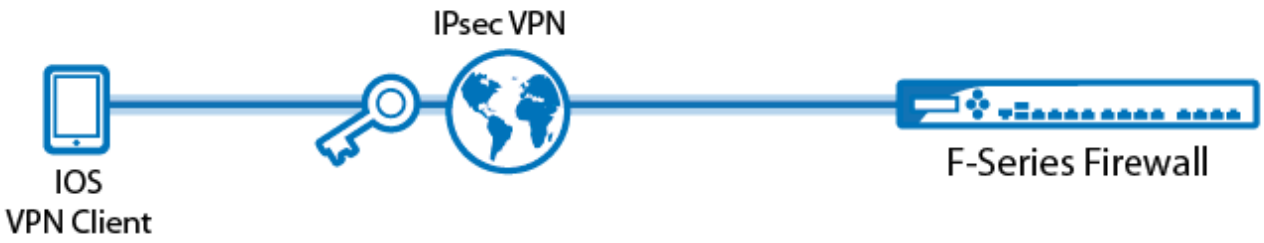
How to Configure Apple iOS Devices for Client-to-Site VPN Connections with Certificate Authentication

https://campus.barracuda.com/doc/46209000/

For instructions how to more easily configure and manage a client-to-site VPN using CudaLaunch as the VPN client, see CudaLaunch and F-Series Firewall Configuration for CudaLaunch.

To connect to a client-to-site VPN with an iOS device, you can either manually configure the built-in IPsec VPN client, or use the TINA client included in CudaLaunch to automatically configure the client for you. Always upgrade to the latest iOS version for your device. iOS 6.0 and older do not support certificates longer than 512 bit. Follow the steps in this article to configure Apple iOS devices for IKEv1 IPsec VPN connections with certificate authentication.



In this article:

Requirements

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
- Client-to-Site IPsec VPN with certificate-based authentication
- XAUTH to add user/password 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 F-Series + Apple iOS Device	PEM	Trust Anchor	◦ Mandatory option for key usage**:** **Certificate sign**; **CRL sign**.
Server Certificate	Barracuda NextGen Firewall F-Series	PKCS12	End Instance	◦ **Subject Alternative Name**: Only use the DNS tag with a FQDN which resolves to the IP address the VPN Service. Do not use the IP tag. E.g., *DNS:vpnserver.yourdomain.com* ◦ **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 Barracuda NextGen Firewall F-Series.
- Only use the X.509 extensions that are listed in the table above.

Configure the Apple iOS Device

Before you begin:

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.

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

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 it.
   - **Certificate** – The X.509 client certificate.

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

1. Client2SiteiOS.png