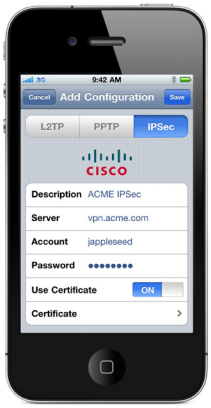
iPhone in Business
Virtual Private Networks (VPN)



Secure access to private corporate networks is available on iPhone using established industry-standard VPN protocols. Users can easily connect to enterprise systems via the built-in VPN client or through third-party applications from Juniper and Cisco.

Out of the box, iPhone supports Cisco IPSec, L2TP over IPSec, and PPTP. If your organization supports one of these protocols, no additional network configuration or third-party applications are required to connect iPhone to your VPN.

Additionally, iPhone supports SSL VPN, enabling access to Juniper SA Series and Cisco ASA SSL VPN servers. Users simply download a VPN client application developed by Juniper or Cisco from the App Store to get started. Like other VPN protocols supported on iPhone, SSL VPN can be configured manually on iPhone or via Configuration Profile.

iPhone supports industry-standard technologies such as IPv6, proxy servers, and split-tunneling, providing a rich VPN experience when connecting to corporate networks. And iPhone works with a variety of authentication methods including password, two-factor token, and digital certificates. To streamline the connection in environments where certificate-based authentication is used, iPhone features VPN On Demand, which dynamically initiates a VPN session when connecting to specified domains.

Supported Protocols and Authentication Methods

SSL VPN
Supports user authentication by password, two-factor token, and certificates.

Cisco IPSec
Supports user authentication by password, two-factor token, and machine authentication by shared secret and certificates.

L2TP over IPSec
Supports user authentication by MS-CHAP v2 Password, two-factor token, and machine authentication by shared secret.

PPTP
Supports user authentication by MS-CHAP v2 Password and two-factor token.

VPN On Demand

For configurations using certificate-based authentication, iPhone supports VPN On Demand. VPN On Demand will establish a connection automatically when accessing predefined domains, providing a seamless VPN connectivity experience for iPhone users.

This is a feature of iOS that does not require additional server configuration. The configuration of VPN On Demand takes place via a Configuration Profile or can be configured manually on the device.

The VPN On Demand options are:

Always
Initiates a VPN connection for any address that matches the specified domain.

Never
Does not initiate a VPN connection for addresses that match the specified domain, but if VPN is already active, it may be used.

Establish if needed
Initiates a VPN connection for addresses that match the specified domain only after a DNS look-up has failed.

VPN Setup

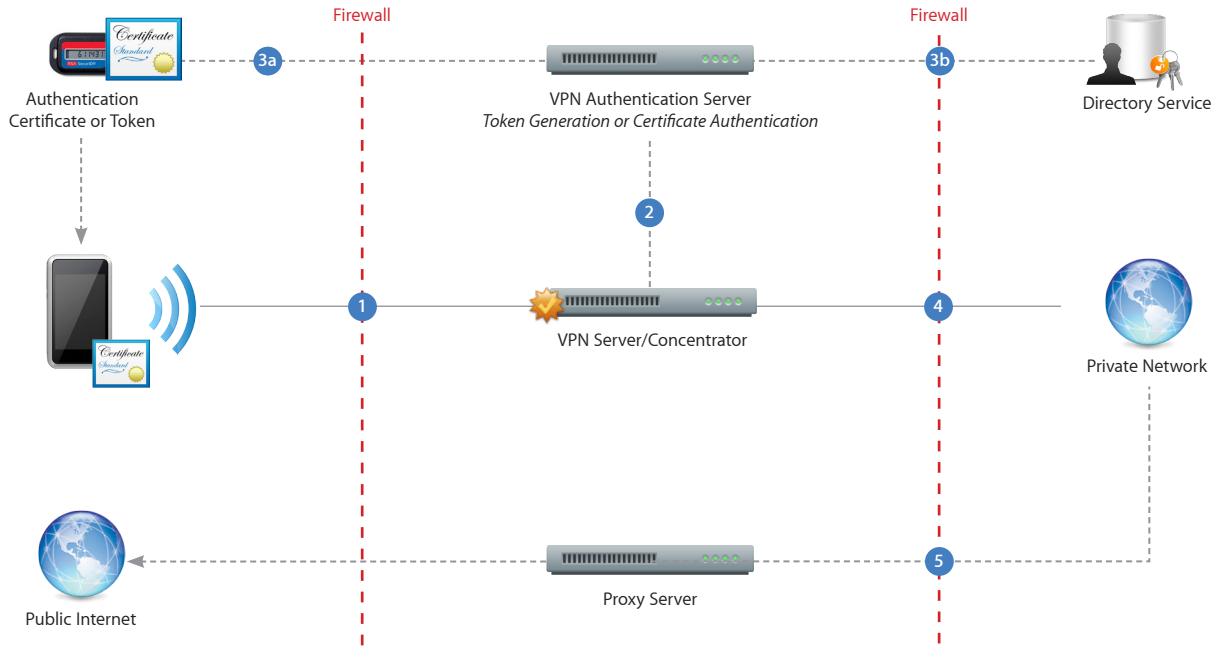
- iPhone integrates with many existing VPN networks, with minimal configuration necessary. The best way to prepare for deployment is to check whether iPhone supports your company's existing VPN protocols and authentication methods.
- It's recommended that you review the authentication path to your authentication server to make sure standards supported by iPhone are enabled within your implementation.
- If you plan to use certificate-based authentication, ensure you have your public key infrastructure configured to support device- and user-based certificates with the corresponding key distribution process.
- If you want to configure URL-specific proxy settings, place a PAC file on a web server that is accessible with the basic VPN settings and ensure that it is hosted with the application/x-ns-proxy-autoconfig MIME type.

Proxy Setup

For all configurations you can also specify a VPN proxy. To configure a single proxy for all connections, use the Manual setting and provide the address, port, and authentication if necessary. To provide the device with an auto-proxy configuration file using PAC or WPAD, use the Auto setting. For PACS, specify the URL of the PACS file. For WPAD, iPhone will query DHCP and DNS for the appropriate settings.

Deployment Scenario

The example depicts a typical deployment with a VPN server/concentrator as well as an authentication server controlling access to enterprise network services.



1. iPhone requests access to network services.
2. The VPN server/concentrator receives the request and then passes it to the authentication server.
3. In a two-factor token environment, the authentication server would then manage a time-synchronized token key generation with the key server. If a certificate authentication method is deployed, an identity certificate needs to be distributed to iPhone prior to authentication. If a password method is deployed, the authentication process proceeds with user validation.
4. Once a user is authenticated, the authentication server validates user and group policies.
5. After user and group policies are validated, the VPN server provides tunneled and encrypted access to network services.
6. If a proxy server is in use, iPhone connects through the proxy server for access to information outside the firewall.

For more information regarding VPN on iPhone, visit www.apple.com/iphone/business/integration

 June 2010 L419828A