



iPhone and Virtual Private Networks (VPN)



VPN protocols

- Cisco IPSec
- L2TP/IPSec
- PPTP

Authentication methods

- Password (MS-CHAPv2)
- RSA SecurID
- CRYPTOCard
- Certificates (PKCS1, PKCS12)
- Shared secret

Secure access to private corporate networks is available on iPhone using the most popular industry-standard VPN protocols. iPhone 2.0 software 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.

Cisco IPSec deployments can take advantage of certificate-based authentication via industry-standard x.509 digital certificates (PKCS1, PKCS12). For two-factor token-based authentication, iPhone supports RSA SecurID as well as CRYPTOCard. Users enter their PIN and token-generated, one-time password directly on their iPhone when establishing a VPN connection.

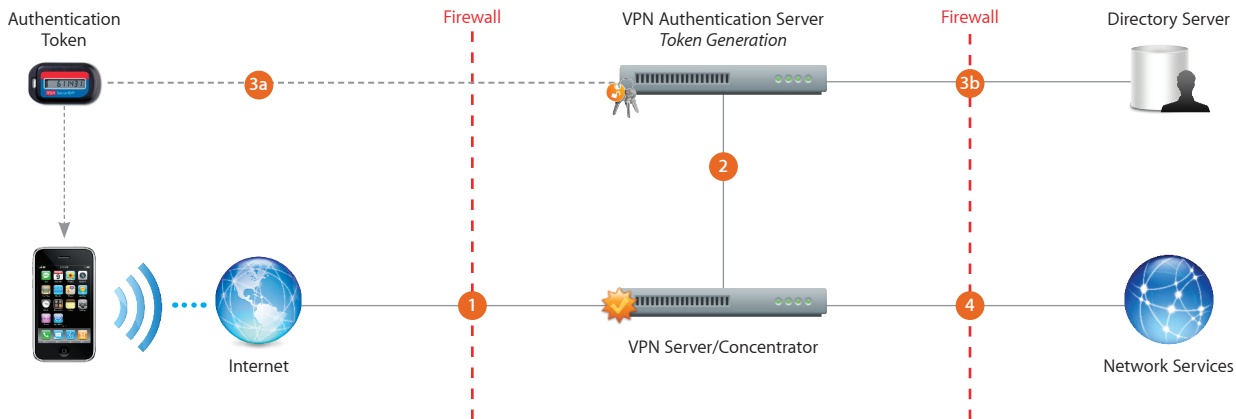
iPhone supports shared secret authentication for Cisco IPSec and L2TP/IPSec deployments. And for basic username and password authentication, iPhone supports MS-CHAPv2. Regardless of the authentication method, preconfigured VPN settings can be distributed to users via a Configuration Profile or entered directly on iPhone.

VPN Setup

- Because iPhone integrates with most existing VPN networks, minimal configuration should be necessary to enable iPhone access to your network. The best way to prepare for deployment is to ensure iPhone is compatible with your company's existing VPN protocols and authentication methods.
- Ensure compatibility of existing standards with your VPN concentrators. It's also a good idea to review the authentication path to your RADIUS or VPN authentication server to ensure standards supported on iPhone are enabled within your existing 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.
- Verify certificate format and authentication server compatibility. iPhone supports PKCS1 (.cer, .crt, .der) and PKCS12 (.p12, .pfx).
- Check with your solution providers to confirm that your software and equipment are up to date with the latest security patches and firmware.
- For additional documentation regarding the Cisco IPSec protocol and specifications, visit www.cisco.com.

VPN Deployment Scenario

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



- 1 iPhone requests access to network services (typically over a PPP connection).
- 2 The VPN server/concentrator receives the request, then passes the request to the authentication server.
- 3a 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 or a password method is deployed, the authentication process proceeds with user validation.
- 3b Once a user is authenticated, the authentication server validates user and group network access policies.
- 4 After user and group policies are validated, the VPN server provides tunneled and encrypted access to network services (typically via IPSec).