



# iPhone e Virtual Private Networks (VPN)



## Protocolli VPN

- Cisco IPSec
- L2TP/IPSec
- PPTP

## Metodi di autenticazione

- Password (MS-CHAPv2)
- RSA SecurID
- CRYPTOCARD
- Certificati (PKCS1, PKCS12)
- Shared Secret

L'accesso sicuro alle reti aziendali private è disponibile su iPhone tramite i più diffusi protocolli VPN standard di settore. Il software iPhone 2.0 supporta Cisco IPSec, L2TP over IPSec e PPTP. Se la vostra organizzazione supporta uno di questi protocolli, non saranno necessarie ulteriori configurazioni di rete o applicazioni terze parti per connettere iPhone alla vostra VPN.

I deployment Cisco IPSec possono utilizzare l'autenticazione basata su certificato tramite i certificati digitali x.509 standard di settore (PKCS1, PKCS12). Per l'autenticazione basata su token a due fattori, iPhone supporta RSA SecurID nonché CRYPTOCARD. Gli utenti immettono il PIN e la password unica generata tramite token direttamente in iPhone quando stabiliscono una connessione VPN.

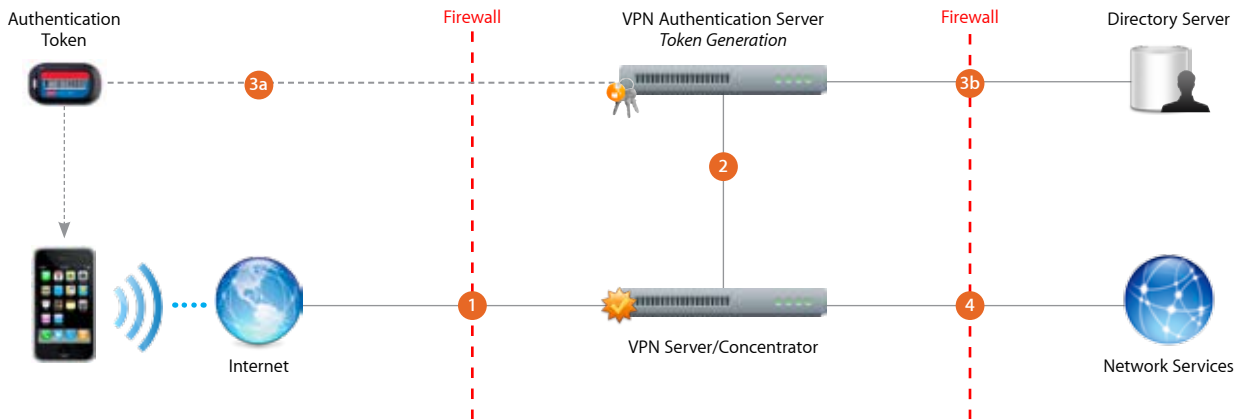
iPhone supporta l'autenticazione Shared Secret per deployment Cisco IPSec e L2TP/IPSec. E per l'autenticazione di base di nome utente e password, iPhone supporta MS-CHAPv2. Indipendentemente dal metodo di autenticazione, le impostazioni VPN preconfigurate possono essere distribuite agli utenti tramite un profilo di configurazione o immesse direttamente in iPhone.

## Configurazione VPN

- Poiché iPhone si integra con gran parte delle reti VPN esistenti, è richiesta unicamente una minima configurazione per abilitare l'accesso di iPhone alla vostra rete. Il modo migliore per preparare il deployment consiste nell'assicurarsi che iPhone sia compatibile con i metodi di autenticazione e i protocolli VPN esistenti della vostra azienda.
- Verificate la compatibilità degli standard esistenti con i vostri VPN Concentrator. Consigliamo inoltre di rivedere il percorso di autenticazione al vostro server di autenticazione RADIUS o VPN per assicurarvi che gli standard supportati su iPhone siano abilitati nella vostra attuale implementazione.
- Se prevedete di utilizzare l'autenticazione basata su certificato, assicuratevi che PKI (Public Key Infrastructure) sia configurata per supportare i certificati basati su dispositivo e utente con il processo di distribuzione corrispondente.
- Verificate la compatibilità del formato del certificato e del server di autenticazione. iPhone supporta PKCS1 (.cer, .crt, .der) e PKCS12 (.p12, .pfx).
- Contattate i vostri fornitori per verificare che il vostro software e le vostre apparecchiature siano aggiornati con i più recenti firmware e patch di sicurezza.
- Per ulteriore documentazione sul protocollo e le specifiche Cisco IPSec, visitate [www.cisco.com](http://www.cisco.com).

## Scenario di deployment VPN

Questo esempio illustra un deployment tipico con un VPN Server/Concentrator oltre a un server di autenticazione VPN che controlla l'accesso ai servizi della rete aziendale.



- 1 iPhone richiede accesso ai servizi di rete (generalmente su una connessione PPP).
- 2 Il VPN Server/Concentrator riceve la richiesta e la trasmette al server di autenticazione.
- 3a In un ambiente di autenticazione a due fattori, il server di autenticazione gestisce quindi una generazione di codici token sincronizzata con il key server. Se si esegue il deployment tramite certificato o password, il processo di autenticazione prosegue con la convalida dell'utente.
- 3b Dopo l'autenticazione dell'utente, il server di autenticazione convalida le policy di accesso di utente e gruppo.
- 4 Dopo la convalida delle policy di utente e gruppo, VPN Server fornisce un accesso con tunneling e codificato ai servizi di rete (generalmente via IPSec).