



El iPhone y las Redes Privadas Virtuales (VPN)



Protocolos de VPN

- IPSec de Cisco
- L2TP/IPSec
- PPTP

Métodos de autenticación

- Contraseña (MS-CHAPv2)
- RSA SecurID
- CRYPTOCARD
- Certificados (PKCS1, PKCS12)
- Secreto compartido

El acceso seguro a redes corporativas privadas está disponible en el iPhone mediante la mayoría de los protocolos de VPN estándar más conocidos. El *software* iPhone 2.0 es compatible con IPSec de Cisco, L2TP por IPSec y PPTP. Si tu organización admite uno de estos protocolos, no necesitas ningún otro tipo de configuración ni aplicaciones de terceros para conectar el iPhone a tu VPN.

Las instalaciones de IPSec de Cisco pueden aprovechar la autenticación basada en certificados mediante los certificados digitales x.509 estándar (PKCS1 y PKCS12). En el caso de autenticación bifactor por *token*, el iPhone admite tanto RSA SecurID como CRYPTOCARD. El usuario introduce su PIN y su contraseña de un solo uso generada por *token* en el iPhone al establecer una conexión VPN.

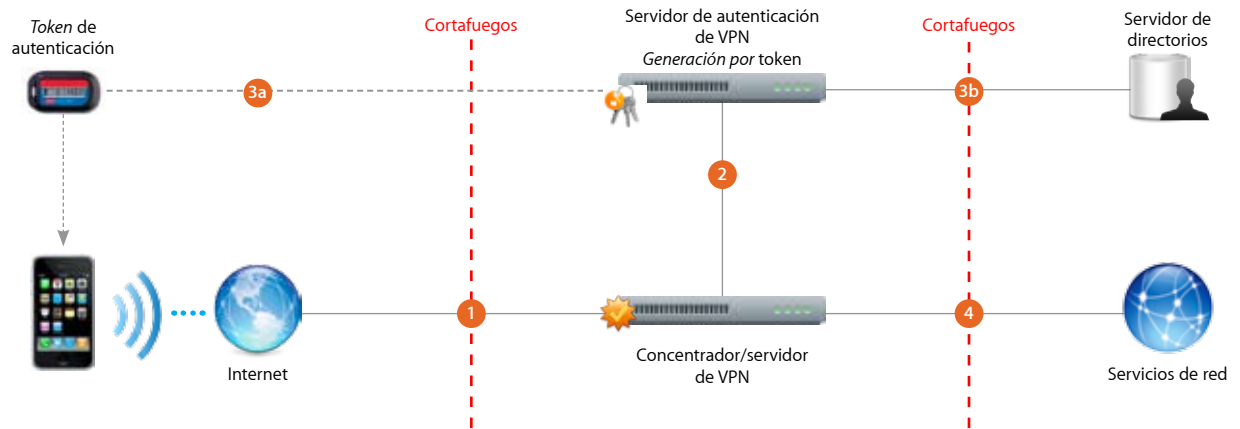
El iPhone admite la autenticación de secreto compartido para instalaciones IPSec de Cisco y L2TP/IPSec. Para la autenticación básica de nombre de usuario y contraseña, el iPhone admite MS-CHAPv2. Independientemente del método de autenticación, se pueden distribuir ajustes preconfigurados de VPN entre los usuarios a través de un perfil de configuración, o bien se pueden introducir directamente en el iPhone.

Configuración de VPN

- Dado que el iPhone se integra con la mayoría de redes VPN existentes, el acceso del iPhone a la red se puede realizar con una configuración mínima. La mejor forma de preparar esta instalación consiste en comprobar la compatibilidad del iPhone con los protocolos de VPN y los métodos de autenticación presentes en tu empresa.
- Comprueba la compatibilidad de los estándares existentes con tus concentradores de VPN. También es buena idea repasar la ruta de autenticación de tu servidor de autenticación de VPN o RADIUS para comprobar que los estándares compatibles con el iPhone están activados en la instalación actual.
- Si tienes la intención de usar un sistema de autenticación basado en certificados, comprueba que tu infraestructura de claves públicas está configurada para admitir certificados basados en usuarios y dispositivos, y los correspondientes procesos de distribución de claves.
- Comprueba la compatibilidad del formato del certificado y del servidor de autenticación. El iPhone admite PKCS1 (.cer, .crt y .der) y PKCS12 (.p12 y .pfx).
- Consulta con tus proveedores para confirmar que el *software* y el equipo están actualizados con los últimos parches de seguridad y firmware.
- Si deseas más documentación sobre el protocolo y las especificaciones de IPSec de Cisco, visita www.cisco.com.

Ejemplo de implantación de VPN

Este ejemplo ilustra una implantación típica con un servidor/concentrador de VPN, además de un servidor de autenticación de VPN para el control del acceso a los servicios de red de la empresa.



- 1 El iPhone solicita acceso a los servicios de red (normalmente a través de una conexión PPP).
- 2 El servidor/concentrador de VPN recibe la solicitud y la pasa al servidor de autenticación.
- 3a En un entorno de autenticación de doble factor utilizando *token*, el servidor de autenticación administra la generación de una clave *token* sincronizada temporalmente con el servidor de claves. Si hay instalado algún sistema de certificados o contraseñas, el proceso de autenticación continúa con la validación del usuario.
- 3b Después de la autenticación del usuario, el servidor de autenticación valida las políticas de acceso a la red de grupos y usuarios.
- 4 Después de esta validación, el servidor de VPN proporciona el tunelado y el acceso cifrado a los servicios de red (normalmente a través de IPSec).