



iPhone et réseaux privés virtuels (VPN)



Protocoles VPN

- Cisco IPSec
- L2TP/IPSec
- PPTP

Méthodes d'authentification

- Mot de passe (MS-CHAPv2)
- RSA SecurID
- CRYPTOCARD
- Certificats (PKCS1, PKCS12)
- Authentification par secret partagé

iPhone permet un accès sécurisé aux réseaux privés d'entreprise en utilisant les principaux protocoles VPN. Le logiciel iPhone 2.0 prend en charge Cisco IPSec, L2TP sur IPSec et PPTP. Si votre organisation prend en charge l'un de ces protocoles, aucune configuration réseau ni application de tierce partie n'est nécessaire pour connecter iPhone à votre VPN.

Les déploiements Cisco IPSec peuvent bénéficier de l'authentification par certificats à l'aide de certificats numériques x.509 standard de l'industrie (PKCS1, PKCS12). Pour l'authentification à deux facteurs, iPhone prend en charge RSA SecurID et CRYPTOCARD. Les utilisateurs saisissent leur code PIN et leur mot de passe à utilisation unique généré par jeton directement sur leur iPhone lorsqu'ils établissent une connexion VPN.

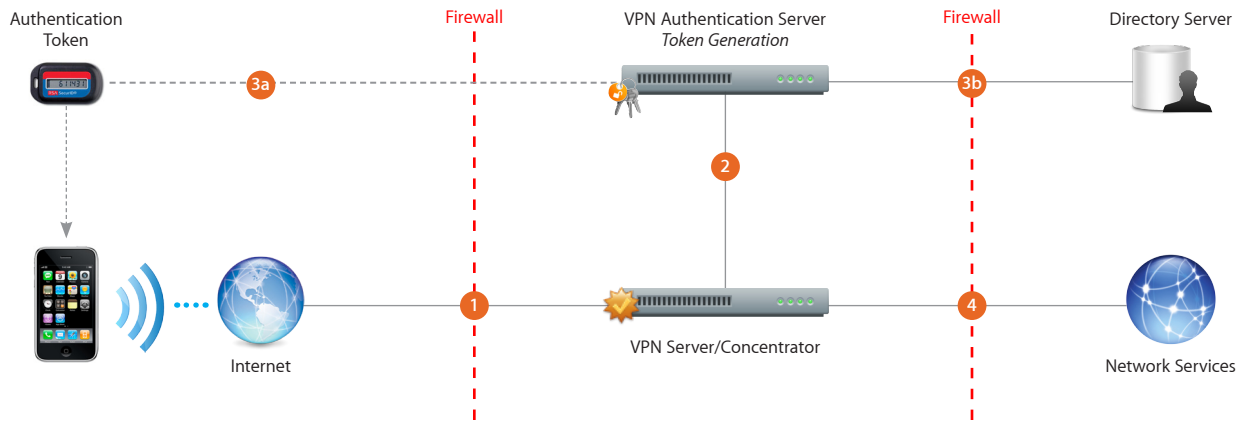
iPhone prend en charge l'authentification par secret partagé pour les déploiements Cisco IPSec et L2TP/IPSec. En ce qui concerne l'authentification par nom d'utilisateur et mot de passe simple, iPhone prend en charge MS-CHAPv2. Quelle que soit la méthode d'authentification utilisée, des paramètres VPN prédéfinis peuvent être transmis aux utilisateurs via un profil de configuration ou saisis directement dans iPhone.

Configuration VPN

- iPhone s'intègre à la plupart des réseaux VPN existants. La configuration nécessaire pour qu'un iPhone puisse accéder à votre réseau doit donc être minimale. La meilleure manière de préparer le déploiement consiste à vérifier si les protocoles VPN et les méthodes d'authentification utilisés par votre entreprise sont pris en charge par iPhone.
- Assurez-vous que vos concentrateurs VPN sont bien compatibles avec les normes. Il est aussi recommandé de vérifier le chemin d'authentification jusqu'à votre serveur RADIUS ou VPN pour vous assurer que les normes prises en charge par iPhone sont activées au sein de votre implémentation.
- Si vous comptez utiliser l'authentification par certificats, assurez-vous que votre infrastructure à clé publique est configurée de manière à prendre en charge les certificats d'appareil et d'utilisateur avec le processus de distribution de clés correspondant.
- Vérifiez que le format des certificats est compatible avec le serveur d'authentification. iPhone prend en charge PKCS1 (.cer, .crt, .der) et PKCS12 (.p12, .pfx).
- Vérifiez auprès de votre fournisseur de solutions que les derniers correctifs de sécurité et programmes internes sont bien installés sur vos logiciels et votre équipement.
- Des informations complémentaires sur le protocole et les spécifications Cisco IPSec sont disponibles à l'adresse www.cisco.com.

Scénario de déploiement VPN

Cet exemple présente un déploiement standard avec un serveur/concentrateur VPN et avec un serveur d'authentification VPN contrôlant l'accès aux services réseau de l'entreprise.



- 1 iPhone demande l'accès aux services réseau (généralement via une connexion PPP).
- 2 Le serveur/concentrateur VPN reçoit la requête, puis la transmet au serveur d'authentification.
- 3a Dans un environnement d'authentification à deux facteurs, le serveur d'authentification génère alors un jeton synchronisé en temps avec le serveur de clés. Si une méthode de certificat ou de mot de passe est déployée, le processus d'authentification procède à l'identification de l'utilisateur..
- 3b Une fois l'utilisateur identifié, le serveur d'authentification valide les stratégies d'accès réseau d'utilisateur et de groupe.
- 4 Une fois les stratégies d'utilisateur et de groupe validées, le serveur VPN autorise un accès crypté par tunnel aux services réseau (généralement via IPSec).