



iPhone und VPNs (Virtuelle Private Netzwerke)



VPN-Protokolle

- Cisco IPSec
- L2TP/IPSec
- PPTP

Authentifizierungsmethode

- Kennwort (MS-CHAPv2)
- RSA SecurID
- CRYPTOCARD
- Zertifikate (PKCS1, PKCS12)
- Shared-Secret-Verfahren

Der sichere Zugriff auf private Unternehmensnetzwerke wird vom iPhone mithilfe der bekanntesten standardkonformen VPN-Protokolle sichergestellt. Die iPhone 2.0 Software unterstützt Cisco IPSec, L2TP over IPSec und PPTP. Wenn Ihr Unternehmen eines dieser Protokolle unterstützt, ist für die Verwendung des iPhones in einer VPN-Infrastruktur keine zusätzliche Netzwerkkonfiguration oder Software von Drittanbietern erforderlich.

Cisco IPSec-Implementierungen können die zertifikatbasierte Identifizierung mithilfe von standardkonformen x.509-Zertifikaten (PKCS1, PKCS12) nutzen. Für die tokenbasierte Zwei-Faktor-Identifizierung unterstützt das iPhone RSA SecurID und CryptoCard. Die Benutzer geben ihre PIN und ein vom Token generiertes Einmalpasswort direkt auf dem iPhone ein, wenn sie die VPN-Verbindung herstellen.

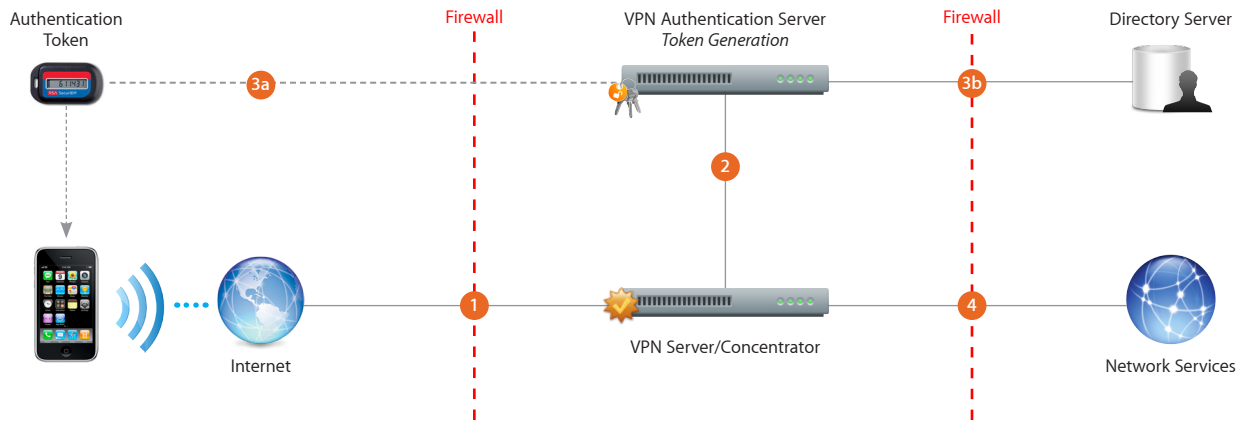
Das iPhone unterstützt auch die Shared-Secret-Identifizierung für Cisco IPSec- und L2TP/IPSec-Implementierungen. Für die einfache Identifizierung mithilfe von Benutzername und Kennwort unterstützt das iPhone MS-CHAPv2. Unabhängig von der Authentifizierungsmethode können vorkonfigurierte VPN-Einstellungen über ein Konfigurationsprofil an Benutzer verteilt oder auch direkt über das iPhone eingegeben werden.

Einrichtung von VPNs

- iPhone-Geräte lassen sich in die meisten VPN-Netzwerke integrieren, sodass in der Regel nur ein minimaler Konfigurationsaufwand erforderlich ist, um den Zugriff auf Ihr Netzwerk über das iPhone zu aktivieren. Zur Vorbereitung der Implementierung empfiehlt es sich, zunächst zu prüfen, ob die in Ihrem Unternehmen genutzten VPN-Protokolle und Identifizierungsverfahren vom iPhone unterstützt werden.
- Stellen Sie sicher, dass Ihre VPN-Konzentratoren die erforderlichen Standards unterstützen. Es empfiehlt sich auch, den Identifizierungspfad zu Ihrem RADIUS- oder Identifizierungsserver zu prüfen, damit sichergestellt ist, dass die vom iPhone unterstützten Standards innerhalb Ihrer Implementierung aktiviert sind.
- Wenn Sie beabsichtigen, eine zertifikatbasierte Identifizierung zu verwenden, muss sichergestellt sein, dass die Infrastruktur für den öffentlichen Schlüssel so konfiguriert ist, dass geräte- und benutzerbasierte Zertifikate vom entsprechenden Schlüsselverteilungsprozess unterstützt werden.
- Prüfen Sie das Zertifikatformat und die Kompatibilität mit dem Identifizierungsserver. Das iPhone unterstützt PKCS1 (.cer, .crt, .der) und PKCS12 (.p12, .pfx).
- Lassen Sie sich von Ihrem Lösungsanbieter bestätigen, dass Ihre Software und Ihre Geräteausstattung auf dem neuesten Stand ist, über die aktuellsten Sicherheits-Patches und die neueste Firmware verfügt.
- Weitere Dokumentation zum Cisco IPSec-Protokoll sowie Spezifikationen finden Sie unter www.cisco.com.

Implementierungsszenario für VPN

Dieses Beispiel zeigt eine typische Implementierung mit einem VPN-Server/-Konzentrator sowie einem VPN-Identifizierungsserver, der den Zugriff auf die Netzwerkdienste des Unternehmens steuert.



- 1 Das iPhone fordert Zugriff auf die Netzwerkdienste an (meist über eine PPP-Verbindung).
- 2 Der VPN-Server/-Konzentrator empfängt die Anforderung und leitet sie an den Identifizierungsserver weiter.
- 3a In einer Umgebung mit tokenbasierter Zwei-Faktor-Authentifizierung erstellt danach der Identifizierungsserver mit dem Schlüsselservers ein zeitsynchronisiertes Identifizierungs-Token. Falls ein Zertifikat oder eine Kennwortmethode eingesetzt wird, fährt der Identifizierungsprozess mit der Benutzervalidierung fort.
- 3b Sobald ein Benutzer authentifiziert ist, prüft der Identifizierungsserver die Benutzer- und Gruppenrichtlinien für den Netzwerkzugriff.
- 4 Nachdem die Benutzer- und Gruppenrichtlinien überprüft worden sind, gewährt der VPN-Server getunnelten und verschlüsselten Zugriff auf die Netzwerkdienste (meist über IPSec).