Cisco AnyConnect Secure Mobility Client para plataformas móviles

Cisco AnyConnect® Secure Mobility para plataformas móviles proporciona conectividad de red cifrada confiable y fácil de implementar en smartphones y tablets, ya que brinda acceso corporativo continuo a los usuarios en movimiento.

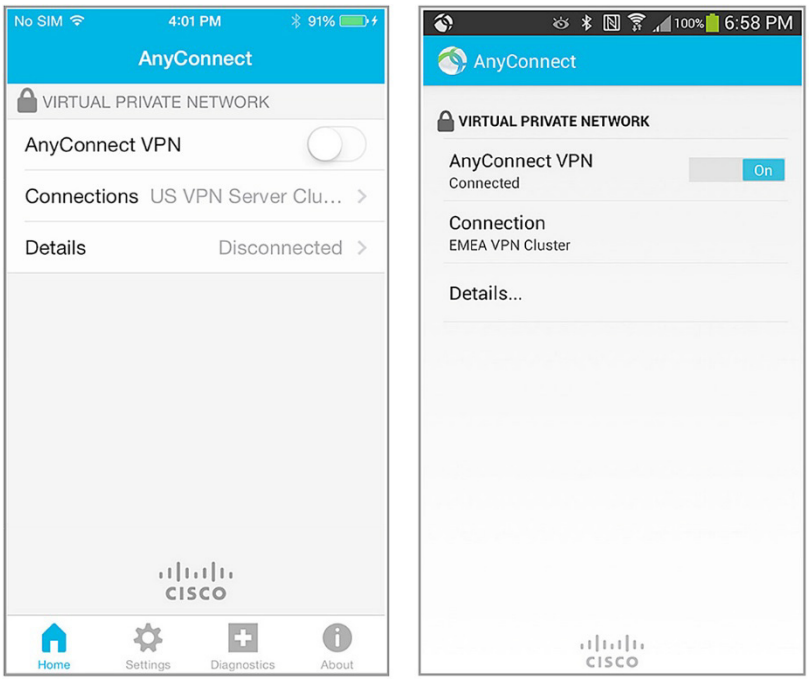
Descripción general del producto

Ahora puede proteger los smartphones y las tablets de los empleados con Cisco AnyConnect Secure Mobility Client para plataformas móviles, disponible para Apple iOS, Android, Windows Phone 8.1, Blackberry 10.3.2 y posteriores, determinados dispositivos de Amazon Kindle y Fire Phone, y Google Chrome OS (adelanto).

Independientemente de que los empleados accedan al correo electrónico de su empresa, a una sesión de equipo de escritorio virtual o a otras aplicaciones empresariales, el cliente AnyConnect ofrece una interfaz fácil de usar para acceder a la información fundamental para la empresa. El cliente utiliza seguridad de la capa de transporte de datagramas (DTLS), Intercambio de claves por Internet con seguridad IP versión 2 (IPsec IKEv2) y TLS (HTTP sobre TLS/SSL) para proporcionar aplicaciones fundamentales, incluidas las aplicaciones sensibles a la latencia como voz sobre IP (VoIP), con acceso cifrado a los recursos corporativos. AnyConnect 4.x admite funciones VPN por aplicación para IOS 8.3 o posterior.

La Figura 1 muestra un ejemplo de interfaz de usuario de AnyConnect en dispositivos Apple iOS y Android.

Figura 1. Interfaz de usuario en dispositivos Apple iOS y Android



Funciones y ventajas

La Tabla 1 muestra las características y los beneficios de AnyConnect Secure Mobility Client para plataformas móviles. La disponibilidad de las funciones depende de la plataforma. Consulte las notas de la versión de la plataforma y la documentación para conocer los detalles específicos de las funciones de un sistema operativo específico.

Tabla 1. Funciones y ventajas

Característica	Beneficio
Acceso y compatibilidad de software	**Disponible en mercados de aplicaciones** • **Apple App Store:** para Apple iOS 6.0 y posterior • **Google Play:** para Android 4.0 y posterior Tenga en cuenta que existen varias imágenes de AnyConnect disponibles; es importante seleccionar la imagen correcta para su dispositivo. Consulte las notas de la versión de Android para conocer los requisitos específicos. • **Windows Store:** para la actualización 1 de Windows Phone 8.1 y posterior • **BlackBerry App World**: para BlackBerry 10.3.2 y posterior • **Google Chrome OS**: para Chrome OS 43 y posterior (adelanto) • **Amazon Appstore:** para determinados dispositivos Kindle y Fire Phone
Acceso a red optimizado	• Adapta automáticamente sus túneles al método más eficaz basándose en las restricciones de red • Utiliza DTLS para proporcionar una conexión optimizada para el acceso a las aplicaciones basado en TCP y el tráfico sensible a la latencia, como el tráfico de VoIP • Utiliza TLS (HTTP sobre TLS/SSL) para habilitar la disponibilidad de la conectividad de red a través de entornos bloqueados • IPsec IKEv2 proporciona una conexión optimizada para el tráfico sensible a la latencia cuando las políticas de seguridad requieren el uso de IPsec (requiere Cisco Adaptive Security Appliance 8.4 o posterior) • Compatible con el equilibrio de carga de VPN de ASA
Compatible con la movilidad	• Se reanuda de forma transparente luego de un cambio de dirección IP, pérdida de conectividad o modo de espera del dispositivo
Compatible con la suspensión	• Compatible con el funcionamiento en suspensión del dispositivo
Cifrado	• Admite cifrado seguro, incluidos AES-256 y 3DES-168. (El dispositivo de gateway de seguridad debe tener una licencia para cifrado seguro activa) • Cifrado de próxima generación, incluidos los algoritmos Suite B de NSA, ESPv3 con IKEv2, claves RSA de 4096 bits, grupo 24 Diffie-Hellman y SHA2 mejorado (SHA-256 y SHA-384). Disponible únicamente para las conexiones IPsec IKEv2. Se requiere una licencia Apex para AnyConnect
Opciones de autenticación	• RADIUS • RADIUS con vencimiento de contraseña (MSCHAPv2) en NT LAN Manager (NTLM) • Soporte de contraseña de un solo uso (OTP) RADIUS (atributos de mensaje de estado y respuesta) • RSA SecurID • Active Directory o Kerberos • Certificado digital (compatible con el Protocolo simple de suscripción de certificados o SCEP integrado de AnyConnect para la implementación de credenciales) • Soporte genérico de Protocolo ligero de acceso a directorios (LDAP) • LDAP con vencimiento y antigüedad de contraseña • Certificado combinado y autenticación multifactor de nombre de usuario y contraseña (autenticación doble)
Experiencia homogénea del usuario	• El modo de cliente de túnel completo admite usuarios de acceso remoto que requieren una experiencia uniforme para el usuario similar a la de LAN
Control y administración de políticas centralizados	• Las políticas pueden configurarse previamente o configurarse de forma local, y actualizarse automáticamente desde el gateway de seguridad de VPN • El manipulador del Indicador universal de recursos (URI) para AnyConnect facilita las implementaciones a través de las URL incorporadas en páginas web o aplicaciones • Los certificados se pueden ver y administrar de manera local
Conectividad de red IP avanzada	• Política de acceso a la red de túneles total o dividida controlada por el administrador • Política de VPN por aplicación para iOS 8.3 y posterior (requiere Cisco ASA de la serie 5500-X con OS 9.3.2 o posterior y licencia Plus o Apex de AnyConnect) • Política de control de acceso

Característica	Beneficio
	Mecanismos de asignación de direcciones IP • Estática • Conjunto interno • Protocolo de configuración dinámica de host (DHCP) • RADIUS/LDAP
Localización	**Se incluyen las traducciones a los siguientes idiomas, además del inglés:** • Francés canadiense (fr-ca) • Checo (cs-cz) • Alemán (de-de) • Japonés (ja-jp) • Coreano (ko-kr) • Español para Latinoamérica (es-co) • Polaco (pl-pl) • Chino simplificado (zh-cn)
Dispositivos	• Están disponibles las estadísticas y la información de registro en el dispositivo • Los registros se pueden ver en el dispositivo • Los registros pueden enviarse fácilmente por correo electrónico a Cisco o a un administrador para su análisis

Compatibilidad con plataformas

AnyConnect Secure Mobility Client es compatible con todos los firewalls de próxima generación Cisco ASA de la serie 5500-X y modelos de Cisco Enterprise Firewall Edition de la serie 5500 que funcionan con la versión de software 8.0(4) de ASA o posteriores. Se recomienda usar las versiones de software actuales de ASA.

Algunas funciones requieren versiones posteriores del software de ASA o de los modelos ASA 5500-X.

Cisco admite el acceso por VPN con AnyConnect a Cisco IOS® versión 15.1(2)T o posterior, funcionando como gateway altamente seguro con ciertas limitaciones de las características. Consulte las Funciones no admitidas en la VPN con SSL de Cisco IOS para conocer los detalles. Consulte http://www.cisco.com/go/fn para obtener información de soporte adicional sobre las funciones de software de Cisco IOS.

Puede encontrar información adicional sobre compatibilidad en http://www.cisco.com/en/US/docs/security/asa/compatibility/asa-vpn-compatibility.html.

Opciones de licencias e información sobre pedidos

La Guía para realizar pedidos de AnyConnect trata el otorgamiento de licencias y contiene información para realizar pedidos sobre AnyConnect, VPN con SSL sin clientes y el uso de VPN por acceso remoto IKEv2 de terceros. Se requieren licencias Plus o Apex de AnyConnect para contar con soporte total para las plataformas y funciones. Los clientes que ya cuentan con licencias Essentials o Premium y Mobile pueden utilizar las versiones de iOS y Android (sin incluir las funciones de VPN por aplicación) hasta el 30 de abril de 2016. Todas las demás plataformas móviles requieren licencias Plus o Apex. No está permitida en ningún caso la conectividad de VPN con AnyConnect con los equipos de cabecera que no sean de Cisco. Para obtener más información, consulte la guía para realizar pedidos en http://www.cisco.com/c/dam/en/us/products/security/anyconnect-og.pdf.

Cisco Capital

Financiación para ayudarlo a alcanzar sus objetivos

Cisco Capital puede ayudarlo a adquirir la tecnología que necesita para lograr sus objetivos y mantener la competitividad. Podemos ayudarlo a reducir los gastos de capital. Acelere su crecimiento. Optimice sus inversiones monetarias y el ROI. La financiación de Cisco Capital le brinda flexibilidad en la adquisición de hardware, software, servicios y equipos complementarios de terceros. Y hay un solo pago previsible. Cisco Capital está disponible en más de 100 países. Para más información visite

Más información

- Página de inicio de Cisco AnyConnect Secure Mobility Client: http://www.cisco.com/go/anyconnect.
- Documentación de Cisco AnyConnect: http://www.cisco.com/c/en/us/support/security/anyconnect-secure-mobility-client/tsd-products-support-series-home.html.
- Firewalls de próxima generación Cisco ASA de la serie 5500-X: http://www.cisco.com/go/asa.
- Acuerdo de licencia y política de privacidad de Cisco AnyConnect: http://www.cisco.com/c/en/us/td/docs/security/vpn_client/anyconnect/anyconnect40/license/end_user/AnyConnect-SEULA-v4-x.html.

Reconocimientos

Este producto incluye software desarrollado por OpenSSL Project para utilizar en el juego de herramientas de OpenSSL.

Este producto incluye software criptográfico creado por Eric Young.

Este producto incluye software creado por Tim Hudson.

Este producto incluye la biblioteca de HTTP libcurl: Copyright 1996-2006, Daniel Stenberg.

Sede central en América
Cisco Systems, Inc.
San José. CA

Sede Central en Asia Pacífico
Cisco Systems (EE. UU.) Pte. Ltd.
Singapur

Sede Central en Europa
Cisco Systems International BV Amsterdam.
Países Bajos

Cisco cuenta con más de 200 oficinas en todo el mundo. Las direcciones, los números de teléfono y de fax están disponibles en el sitio web de Cisco: www.cisco.com/go/offices.

Impreso en EE. UU. C78-527494-09 10/15