Cisco AnyConnect Secure Mobility Client para plataformas móviles

Cisco AnyConnect® Secure Mobility Client para plataformas móviles proporciona una conectividad de red cifrada fácil de implementar y fiable desde smartphones y tablets, además de acceso corporativo persistente para empleados que trabajan de manera remota.

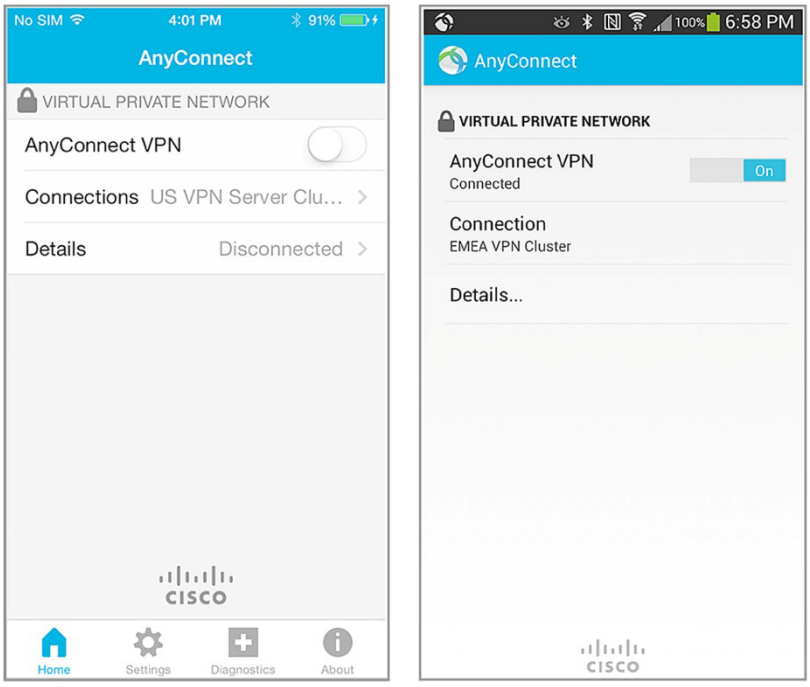
Descripción general del producto

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

Si un empleado accede al correo electrónico empresarial, a una sesión de escritorio virtual o a otras aplicaciones empresariales, el cliente AnyConnect ofrece una interfaz de usuario fácil de usar que muestra información crítica para la empresa. El cliente utiliza los protocolos Seguridad de la capa de transporte del datagrama (DTLS), Intercambio de claves de Internet con seguridad IP, versión 2 (IPsec IKEv2) y TLS (HTTP a través de TLS/SSL) a fin de proporcionar aplicaciones vitales para la empresa, incluidas aquellas sensibles a la latencia, como la voz sobre IP (VoIP), con acceso cifrado a los recursos corporativos. AnyConnect 4.x admite funciones VPN por aplicación para iOS 8.3 y versiones posteriores.

En la figura 1 se muestra una interfaz del usuario de AnyConnect de muestra en los dispositivos Apple iOS y Android.

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



© 2015 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

Características y ventajas

En la tabla 1 se enumeran las características y ventajas de AnyConnect Secure Mobility Client para plataformas móviles. La disponibilidad de las funciones varía según la plataforma. Consulte las notas de la versión de la plataforma y la documentación para obtener detalles sobre las funciones admitidas en cada sistema operativo concreto.

Tabla 1. Características y ventajas

Característica	Ventaja
Software: compatibilidad y acceso	**Disponible en mercados de aplicaciones** • **Apple App Store:** para Apple iOS 6.0 y versiones posteriores • **Google Play:** para Android 4.0 y versiones posteriores Tenga en cuenta que hay varias imágenes de AnyConnect disponibles, por lo que 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 Windows Phone 8.1, actualización 1 y posteriores • **BlackBerry App World:** para BlackBerry 10.3.2 y versiones posteriores • **Google Chrome OS:** para Chrome OS 43 y versiones posteriores (versión de presentación) • **Amazon Appstore:** para determinados dispositivos Kindle y Fire Phone
Acceso a la red optimizado	• Adapta automáticamente su tunelación al método más eficiente posible en función de los requisitos de red. • Utiliza DTLS con objeto de proporcionar una conexión optimizada para el acceso de las aplicaciones basado en TCP y el tráfico sensible a la latencia, como el tráfico VoIP. • Utiliza TLS (HTTP sobre TLS/SSL) para garantizar la disponibilidad de la conectividad de red en los 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 (se requiere el appliance de seguridad adaptativa Cisco Adaptive Security Appliance 8.4 o versiones posteriores). • Compatible con el balanceo de carga ASA VPN
Movilidad fácil de usar	• Se reanuda de forma transparente después de un cambio de dirección IP, de una pérdida de conectividad o del modo en espera de un dispositivo.
Batería fácil de usar	• Compatible con el modo inactivo de los dispositivos
Cifrado	• Admite cifrado avanzado, como AES-256 y 3DES-168. (El dispositivo de gateway de seguridad debe tener habilitada una licencia para cifrado avanzado). • Cifrado de última generación, incluidos los algoritmos de la Suite B de la NSA, ESPv3 con IKEv2, claves RSA de 4096 bits, Diffie-Hellman grupo 24 y SHA2 mejorado (SHA-256 y SHA-384). Se aplica solamente a las conexiones IKEv2 de IPsec. Se necesita una licencia AnyConnect Apex.
Opciones de autenticación	• RADIUS • RADIUS con expiración de la contraseña (MSCHAPv2) para NT LAN Manager (NTLM) • Asistencia RADIUS con contraseña de un solo uso (OTP) (atributos de mensajes de respuesta y estado) • RSA SecurID • Active Directory o Kerberos • Certificado digital (compatible con el protocolo de inscripción de certificado simple (SCEP) de AnyConnect para la implementación de las credenciales) • Compatibilidad con el protocolo ligero de acceso a directorios (LDAP) genérico • LDAP con vencimiento y antigüedad de contraseñas • Combinación de certificado y autenticación multifactor de nombre de usuario y contraseña (doble autenticación)
Experiencia de usuario uniforme	• El modo de cliente de túnel completo admite usuarios con acceso remoto que requieran una experiencia de usuario uniforme similar a la que ofrece una LAN.
Control y gestión de políticas centralizados	• Es posible preconfigurar las políticas o configurarlas de manera local. También se pueden actualizar automáticamente desde el gateway de seguridad VPN. • El controlador del indicador de recursos universal (URI) para AnyConnect facilita la implementación a través de URL integradas en páginas web o aplicaciones. • Es posible visualizar y gestionar los certificados localmente

© 2015 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

Característica	Ventaja
Conectividad de red IP avanzada	• Políticas de acceso a redes con túnel dividido o túnel completo controladas por el administrador. • Política VPN por aplicación para iOS 8.3 y versiones posteriores (requiere Cisco ASA 5500-X con OS 9.3.2 o versiones posteriores y licencia AnyConnect Plus o Apex) • Políticas de control de acceso **Mecanismos de asignación de dirección IP:** • Static • Conjunto interno • Protocolo de configuración dinámica de host (DHCP) • RADIUS/LDAP
Localización	**Además del inglés, se incluyen las traducciones a los siguientes idiomas:** • Francés canadiense (fr-ca) • Checo (cs-cz) • Alemán (de-de) • Japonés (ja-jp) • Coreano (ko-kr) • Español de Latinoamérica (es-co) • Polaco (pl-pl) • Chino simplificado (zh-cn)
Análisis	• Hay disponible información de inicio de sesión y de estadísticas en el dispositivo. • Los registros se pueden ver en el dispositivo. • Los registros se pueden enviar fácilmente por correo electrónico a Cisco o a un administrador para su análisis.

Compatibilidad de la plataforma

AnyConnect Secure Mobility Client es compatible con todos los modelos de firewalls de última generación Cisco ASA serie 5500-X y el firewall Cisco serie 5500 Enterprise Edition que funcionan con el software Cisco ASA, versión 8.0(4) y posteriores. Se recomienda el uso de la versión actual del software ASA.

Determinadas funciones requieren la última versión del software ASA o los modelos ASA 5500-X.

Cisco admite el acceso VPN AnyConnect a Cisco IOS® versión 15.1(2)T o posteriores que funcionen como gateway de alta seguridad con determinadas limitaciones de funcionalidad. Consulte Funciones no admitidas en Cisco IOPS SSL VPN para obtener más información sobre los detalles. Consulte http://www.cisco.com/go/fn para obtener más información sobre la compatibilidad de funciones del software IOS de Cisco.

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

Información de pedidos y opciones de licencias

En la guía de pedidos de AnyConnect encontrará información sobre pedidos y licencias para AnyConnect, VPN SSL sin cliente y el uso de VPN de acceso remoto IKEv2 de terceros. Se requieren licencias AnyConnect Plus o Apex para conseguir una compatibilidad total con las funciones y las plataformas. Los clientes que cuenten con licencias Essentials, Premium o Mobile existentes pueden usar las versiones de iOS y Android (excluidas las funciones VPN por aplicación) hasta el 30 de abril de 2016. El resto de las plataformas móviles requieren licencias Plus o Apex. No se permite la conectividad de VPN AnyConnect con equipos de cabecera que no sean de Cisco. Para obtener más información, consulte la guía de pedidos en http://www.cisco.com/c/dam/en/us/products/security/anyconnect-og.pdf.

© 2015 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

Cisco Capital

Financiación para ayudarle a alcanzar sus objetivos

La financiación de Cisco Capital puede ayudarle a adquirir la tecnología que necesita para lograr sus objetivos y seguir siendo competitivo. Podemos ayudarle a reducir el CapEx. Acelere su crecimiento. Optimice su inversión y el ROI. La financiación de Cisco Capital le ofrece flexibilidad a la hora de adquirir hardware, software, servicios y equipamiento complementario de otras empresas. Y solamente hay un pago predecible. Cisco Capital está disponible en más de 100 países. Más información.

Para obtener 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 última generación Cisco ASA serie 5500-X: http://www.cisco.com/go/asa.
- Política de privacidad y acuerdo de licencia 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 su uso en OpenSSL Toolkit.

Este producto incluye software criptográfico escrito por Eric Young.

Este producto incluye software escrito por Tim Hudson.

Este producto incorpora la biblioteca 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 y los números de teléfono y fax se encuentran en la Web de Cisco en www.cisco.com/go/offices.

Cisco y el logotipo de Cisco son marcas comerciales o marcas registradas de Cisco o de sus filiales en EE. UU. y en otros países. Si desea consultar una lista de las marcas comerciales de Cisco, visite www.cisco.com/go/trademarks. Las marcas registradas de terceros que se mencionan aquí son de propiedad exclusiva de sus respectivos propietarios. El uso de la palabra "partner" no implica la existencia de una asociación entre Cisco y cualquier otra empresa. (1110R)

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

© 2015 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.