Conozca Cisco AnyConnect Secure Mobility Client

Objetivo

Este artículo se centra en las características, especificaciones y ventajas del uso de Cisco AnyConnect. Para obtener información sobre las licencias de AnyConnect en los routers de la serie RV340, vea el artículo Licencia de AnyConnect para los routers de la serie RV340.

Versión del software

4.2.03013 (Notas de la versión)

Características y especificaciones

Función	Ventajas y detalles
VPN de acceso remoto	
Amplia compatibilidad con sistemas operativos	• Windows 10, 8.1, 8 y 7 • Mac OS X 10.8 y posteriores • Linux Intel (x64) Consulte la hoja de datos de AnyConnect Mobile para obtener información sobre la plataforma móvil.
Acceso a la red optimizado: SSL de elección del protocolo VPN (TLS y DTLS); IPsec IKEv2	• AnyConnect ofrece una variedad de protocolos VPN, de modo que los administradores pueden utilizar el protocolo que mejor se adapte a sus necesidades empresariales. • La compatibilidad con tunelización incluye SSL (TLS 1.2 y DTLS) e IPsec IKEv2 de última generación. • DTLS proporciona una conexión optimizada para el tráfico sensible a la latencia, como el tráfico VoIP o el acceso a aplicaciones basado en TCP. • TLS 1.2 (HTTP a través de TLS o SSL) ayuda a garantizar la disponibilidad de la conectividad de red a través de entornos bloqueados, incluidos los que utilizan servidores proxy web. • IPsec IKEv2 proporciona una conexión optimizada para el tráfico sensible a la latencia cuando las políticas de seguridad requieren el uso de IPSec.
Selección de gateway óptima	• Determina y establece la conectividad al punto de acceso a la red óptimo, eliminando la necesidad de que los usuarios finales determinen la ubicación más cercana.
Movilidad sencilla	• Diseñado para usuarios móviles • Se puede configurar de modo que la conexión VPN permanezca establecida durante los cambios de dirección IP, la pérdida de conectividad, la hibernación o la espera. • Con Trusted Network Detection, la conexión VPN puede desconectarse automáticamente cuando un usuario final se encuentra en la oficina y conectarse cuando un usuario se encuentra en una ubicación remota.
Cifrado	• AES-256 y 3DES-168. (El dispositivo de gateway de seguridad

	debe tener habilitada una licencia de cifrado seguro). • Algoritmos de la Suite B de la NSA, ESPv3 con IKEv2, claves RSA de 4096 bits, grupo Diffie-Hellman 24 y SHA2 mejorado (SHA-256 y SHA-384). Se aplica solamente a las conexiones IKEv2 de IPsec. Se necesita una licencia AnyConnect Apex.
Amplia gama de opciones de implementación y conexión	Opciones de implementación: • Preimplementación, incluido Microsoft Installer • Implementación automática de gateway de seguridad (se requieren derechos administrativos para la instalación inicial) por ActiveX (sólo Windows) y Java Modos de conexión: • Independiente por el icono del sistema • Iniciado por explorador (lanzamiento web) • Portal sin cliente iniciado • Iniciada CLI • Se ha iniciado la API
Amplia gama de opciones de autenticación	• RADIUS • RADIUS con vencimiento de contraseña (MSCHAPv2) para NT LAN Manager (NTLM) • Compatibilidad con contraseña de RADIUS única (OTP) (atributos de mensaje de estado y respuesta) • RSA SecurID (incluida la integración de SoftID) • Active Directory o Kerberos • Autoridad de certificación integrada (CA) • Certificado digital o tarjeta inteligente (incluida la compatibilidad con certificados de máquina), seleccionado automáticamente o por el usuario • Protocolo ligero de acceso a directorios (LDAP) con vencimiento y antigüedad de la contraseña • Soporte LDAP genérico • Certificado combinado y autenticación multifactor de nombre de usuario y contraseña (doble autenticación)
Experiencia de usuario uniforme	• El modo de cliente de túnel completo admite usuarios de acceso remoto que necesitan una experiencia de usuario uniforme similar a la de una LAN. • Varios métodos de entrega ayudan a garantizar una amplia compatibilidad de AnyConnect. • El usuario puede aplazar las actualizaciones introducidas. • La opción de comentarios sobre la experiencia del cliente está disponible.
Control y gestión centralizados de políticas	• Las políticas se pueden preconfigurar o configurar localmente y se pueden actualizar automáticamente desde el gateway de seguridad VPN. • La API para AnyConnect facilita las implementaciones a través de páginas web o aplicaciones. • Se emiten comprobaciones y advertencias de los usuarios para los certificados no fiables. • Los certificados se pueden ver y administrar localmente.
Conectividad de red IP avanzada	• Conectividad pública hacia y desde redes IPv4 e IPv6 • Acceso a los recursos de red IPv4 e IPv6 internos • Política de acceso a la red de tunelización dividida y tunelización completa controlada por el administrador • Política de control de acceso • Política de VPN por aplicación para Google Android (Lollipop) y

	Samsung KNOX (novedad en la versión 4.0; requiere Cisco ASA 5500-X con OS 9.3 o posterior y licencias AnyConnect 4.0) **Mecanismos de asignación de dirección IP:** • Estático • Grupo interno • Protocolo de configuración dinámica de host (DHCP) • RADIUS/LDAP
Sólido cumplimiento unificado de terminales (Se requiere licencia Apex)	• Se admite la evaluación y la remediación del estado del terminal para entornos por cable e inalámbricos (en sustitución del Cisco Identity Services Engine NAC Agent). Requiere Identity Services Engine 1.3 o posterior con la licencia Apex de Identity Services Engine. • Cisco Hostscan busca detectar la presencia de software antivirus, software de firewall personal y paquetes de servicios de Windows en el sistema de terminales antes de conceder acceso a la red. • Los administradores también tienen la opción de definir comprobaciones de estado personalizadas basadas en la presencia de procesos en ejecución. • El análisis de host detecta la presencia de una marca de agua en un sistema remoto. La marca de agua se puede utilizar para identificar los activos propiedad de la empresa y, como resultado, proporcionar un acceso diferenciado. La función de verificación de marca de agua incluye valores del registro del sistema, existencia de archivos que coinciden con una suma de comprobación CRC32 requerida, coincidencia de intervalo de direcciones IP y certificados emitidos por o a una autoridad de certificados coincidente. Se admiten capacidades adicionales para aplicaciones que no cumplen las normativas. • Las funciones varían según el sistema operativo. Vea los gráficos de Soporte de Escaneo de Host para obtener información detallada.
Política de firewall del cliente	• Proporciona protección adicional para las configuraciones de tunelización dividida. • Se utiliza junto con el cliente de AnyConnect para permitir excepciones de acceso local (por ejemplo, impresión, soporte de dispositivos atados, etc.). • Admite reglas basadas en puertos para IPv4 y listas de control de acceso IP (ACL) y de red para IPv6. • Disponible para plataformas Windows y Mac OS X.
Localización	**Además del inglés, se incluyen las traducciones en los siguientes idiomas:** • Checo (cs-cz) • Alemán (de-de) • Español (es-es) • Francés (fr-fr) • Japonés (ja-jp) • Coreano (ko-kr) • Polaco (pl-pl) • Chino simplificado (zh-cn) • Chino (Taiwán) (zh-tw) • Holandés (nl-nl) • Húngaro (hu-hu) • Italiano (it-it) • Portugués (Brasil) (pt-br) • Ruso (ru-ru)

Facilidad de administración de clientes	• Los administradores pueden distribuir automáticamente actualizaciones de software y políticas desde el dispositivo de seguridad de cabecera, eliminando así la administración asociada a las actualizaciones de software del cliente. • Los administradores pueden determinar qué capacidades deben estar disponibles para la configuración del usuario final. • Los administradores pueden activar un script de terminal en los momentos de conexión y desconexión cuando no se pueden utilizar los scripts de inicio de sesión de dominio. • Los administradores pueden personalizar y localizar por completo los mensajes visibles para el usuario final.
Editor de perfiles	• Las políticas de AnyConnect se pueden personalizar directamente desde Cisco Adaptive Security Device Manager (ASDM).
Diagnóstico	• Hay disponible información de registro y 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.
Federal Information Processing Standard (FIPS)	• Cumple con el nivel 2 de FIPS 140-2 (se aplican restricciones de plataforma, función y versión)
Movilidad segura y visibilidad de la red	
Integración de seguridad web (Se requiere licencia de Cloud Web Security)	: Utiliza Cloud Web Security, el mayor proveedor global de seguridad web de software como servicio (SaaS), para mantener el malware alejado de las redes corporativas y controlar y proteger el uso web de los empleados. • Admite configuraciones alojadas en la nube y carga dinámica. • Ofrece a las organizaciones flexibilidad y opciones al admitir servicios basados en la nube, además de servicios basados en las instalaciones. • Se integra con el dispositivo de seguridad web. • Admite Detección De Red De Confianza. • Aplica la política de seguridad en cada transacción, independientemente de la ubicación del usuario. • Requiere conectividad de red sumamente segura y siempre activa con una política para permitir o denegar la conectividad de red si el acceso deja de estar disponible. • Detecta puntos de conexión y portales cautivos.
Módulo de visibilidad de red (Se requiere licencia Apex)	• Descubra posibles anomalías en el comportamiento mediante la supervisión del uso de la aplicación. • Permite tomar decisiones de diseño de red más fundamentadas. • Puede compartir los datos de uso con un número cada vez mayor de herramientas de análisis de red compatibles con el protocolo IPFIX (Internet Protocol Flow Information Export).
Habilitador de protección frente a malware avanzado (AMP) para terminales (AMP para terminales tiene licencia por separado)	• Simplifica la habilitación de servicios de amenazas para terminales AnyConnect mediante la distribución y habilitación de CiscoAMP para terminales. • Amplía los servicios de amenazas de terminales a terminales remotos, lo que aumenta la cobertura de amenazas de terminales. • Proporciona una protección más proactiva para garantizar que un ataque se mitigue rápidamente en el terminal remoto.
Amplia compatibilidad con sistemas operativos	• Windows 10, 8.1, 8 y 7 • Mac OS X 10.8 y posteriores
Network Access Manager y 802.1X	
Compatibilidad con medios	• Ethernet (IEEE 802.3)

	• Wi-Fi (IEEE 802.11a/b/g/n)
Autenticación de red	• IEEE 802.1X-2001, 802.1X-2004 y 802.1X-2010 • Permite a las empresas implementar un único marco de autenticación 802.1X para acceder a las redes por cable e inalámbricas. • Gestiona la identidad del usuario y del dispositivo, así como los protocolos de acceso a la red necesarios para un acceso altamente seguro. • Optimiza la experiencia del usuario al conectarse a una red unificada de Cisco por cable e inalámbrica.
Métodos de protocolo de autenticación extensible (EAP)	• EAP-seguridad de la capa de transporte (TLS) • EAP-protocolo de autenticación extensible protegido (PEAP) con los siguientes métodos internos: - EAP-TLS - EAP-MSCHAPv2 - EAP-Tarjeta de testigo genérica (GTC) • EAP-autenticación flexible mediante tunelación segura (FAST) con los siguientes métodos internos: - EAP-TLS - EAP-MSCHAPv2 - EAP-GTC • EAP-TLS tunelado (TTLS) con los siguientes métodos internos: - Protocolo de autenticación de contraseña (PAP). - Protocolo de autenticación por desafío mutuo (CHAP). - Microsoft CHAP (MSCHAP). - MSCHAPv2 - EAP-MD5 - EAP-MSCHAPv2 • EAP ligero (LEAP), solo Wi-Fi • EAP-Message Digest 5 (MD5), configuración administrativa, solo Ethernet • EAP-MSCHAPv2, con configuración administrativa, solo Ethernet • EAP-GTC, configuración administrativa, solo Ethernet
Métodos de encriptación inalámbrica (requiere la correspondiente compatibilidad con NIC 802.11)	• Abrir • Privacidad equivalente a conexión con cables (WEP) • WEP dinámica • Acceso Wi-Fi protegido (WPA) Enterprise • WPA2 Enterprise • WPA Personal (WPA-PSK) • WPA2 Personal (WPA2-PSK) • CCKM (requiere Cisco CB21AG Wireless NIC)
Protocolos de cifrado inalámbrico	• Modo de contador con protocolo de código de autenticación de mensajes de encadenamiento de bloqueo de cifrado (CCMP) mediante el algoritmo estándar de cifrado avanzado (AES) • Protocolo de integridad de clave temporal (TKIP) mediante el cifrado de flujo Rivest Cipher 4 (RC4)
Reanudación de sesión	• Reanudación de sesión RFC2716 (EAP-TLS) mediante EAP-TLS, EAP-FAST, EAP-PEAP y EAP-TTLS • Reanudación de sesión sin estado EAP-FAST • Almacenamiento en caché de PMK-ID (almacenamiento en caché de clave proactiva o almacenamiento en caché de claves oportunista), solo en Windows XP
encripción Ethernet	• Control de acceso a los medios: IEEE 802.1AE (MACsec) • Gestión clave: Acuerdo de clave MACsec (MKA)

	• Define una infraestructura de seguridad en una red Ethernet con cables para proporcionar confidencialidad de datos, integridad de datos y autenticación del origen de los datos. • Protege la comunicación entre los componentes de confianza de la red.
Una conexión a la vez	• Permite solamente una conexión a la red, desconectando a todos los demás. • No hay conexión en puente entre adaptadores. • Las conexiones Ethernet tienen prioridad automáticamente.
Validación compleja del servidor	• Admite las reglas "termina con" y "coincidencia exacta". • Compatibilidad con más de 30 reglas para servidores sin elementos comunes de nombres.
EAP-Encadenamiento (EAP-FASTv2)	• Diferenciación del acceso en función de los recursos empresariales y no empresariales. • Valida usuarios y dispositivos en una única transacción EAP.
Aplicación de conexión empresarial (ECE)	• Ayuda a garantizar que los usuarios se conectan únicamente a la red corporativa correcta. • Evita que los usuarios se conecten a un punto de acceso de terceros para navegar por Internet mientras se encuentran en la oficina. • Evita que los usuarios establezcan el acceso a la red de invitados. • Elimina las engorrosas listas negras.
Cifrado de última generación (Suite B)	• Admite los estándares criptográficos más recientes. • Intercambio de claves Elliptic Curve Diffie-Hellman • Certificados del algoritmo de firma digital de curva elíptica (ECDSA)
Tipos de credenciales	• Contraseñas de usuario interactivas o contraseñas de Windows • Tokens RSA SecurID • Tokens de contraseña única (OTP) • Tarjetas inteligentes (Axalto, Gemplus, SafeNet iKey, Alladin). • Certificados X.509. • Certificados del algoritmo de firma digital de curva elíptica (ECDSA).
Soporte de escritorio remoto	• Autentica las credenciales de usuario remoto en la red local al utilizar el protocolo de escritorio remoto (RDP).
Sistemas operativos compatibles	• Windows 10, 8.1, 8 y 7