Lernen Sie den Cisco AnyConnect Secure Mobility Client kennen

Ziel

Dieser Artikel behandelt die Funktionen, Spezifikationen und Vorteile der Verwendung von Cisco AnyConnect. Weitere Informationen zur AnyConnect-Lizenzierung für Router der Serie RV340 finden Sie im Artikel AnyConnect-Lizenzierung für Router der Serie RV340.

Software-Version

4.2.03013 (Versionshinweise)

Funktionen und Spezifikationen

Funktion	Vorteile und Details
VPN für Remote-Zugriff	
Umfassende Unterstützung für Betriebssysteme	• Windows 10, 8.1, 8 und 7 • Mac OS X 10.8 und höher • Linux Intel (x64) * Informationen zu mobilen Plattformen finden Sie im Datenblatt zu AnyConnect Mobile.
Optimierter Netzwerkzugriff: Auswahl des VPN-Protokolls SSL (TLS und DTLS); IPsec IKEv2	• AnyConnect bietet eine Auswahl an VPN-Protokollen, sodass Administratoren jedes Protokoll verwenden können, das ihren geschäftlichen Anforderungen am besten entspricht. • Tunneling-Unterstützung umfasst SSL (TLS 1.2 und DTLS) und IPsec IKEv2 der nächsten Generation. • DTLS bietet eine optimierte Verbindung für latenzempfindlichen Datenverkehr wie VoIP-Datenverkehr oder TCP-basierten Anwendungszugriff. • TLS 1.2 (HTTP über TLS oder SSL) gewährleistet die Verfügbarkeit der Netzwerkverbindungen in gesperrten Umgebungen, einschließlich Umgebungen, die Webproxy-Server verwenden. • IPsec IKEv2 bietet eine optimierte Verbindung für latenzempfindlichen Datenverkehr, wenn Sicherheitsrichtlinien die Verwendung von IPsec erfordern.
Optimale Gateway-Auswahl	• Ermittelt und stellt die Verbindung zum optimalen Access Point für das Netzwerk her, sodass Endbenutzer nicht mehr den nächstgelegenen Standort ermitteln müssen.
Mobilitätsfreundlich	• Entwickelt für mobile Benutzer • Kann so konfiguriert werden, dass die VPN-Verbindung bei IP-Adressänderungen, Verbindungsausfällen oder im Ruhezustand oder im Standby-Modus aufrechterhalten wird. • Mit Trusted Network Detection kann die VPN-Verbindung automatisch getrennt werden, wenn sich ein Endbenutzer im Büro befindet, und eine Verbindung herstellen, wenn sich ein Benutzer an einem Remote-Standort befindet.

Verschlüsselung	• AES-256 und 3DES-168. (Für das Sicherheits-Gateway-Gerät muss eine Lizenz für starke Verschlüsselung aktiviert sein.) • NSA Suite B-Algorithmen, ESPv3 mit IKEv2, 4096-Bit-RSA-Schlüssel, Diffie-Hellman-Gruppe 24 und erweitertes SHA2 (SHA-256 und SHA-384). Gilt nur für IPsec-IKEv2-Verbindungen. Eine AnyConnect Apex-Lizenz ist erforderlich.
Breite Palette von Bereitstellungs- und Verbindungsoptionen	**Bereitstellungsoptionen:** • Vorbereitstellung, einschließlich Microsoft Installer • Automatische Sicherheits-Gateway-Bereitstellung (für die Erstinstallation sind Administratorrechte erforderlich) durch ActiveX (nur Windows) und Java **Verbindungsmodi:** • Standalone durch Systemsymbol • Vom Browser initiiert (Webstart) • Clientless-Portal initiiert • CLI initiiert • API initiiert
Umfangreiche Authentifizierungsoptionen	• RADIUS • RADIUS mit Kennwortablauf (MSCHAPv2) an NT LAN Manager (NTLM) • RADIUS One Time Password (OTP)-Unterstützung (Status- und Antwortattribute) • RSA SecurID (einschließlich SoftID-Integration) • Active Directory oder Kerberos • Embedded Certificate Authority (CA) • Digitales Zertifikat oder Smartcard (einschließlich Unterstützung für Computerzertifikate), automatische oder benutzerspezifische • Lightweight Directory Access Protocol (LDAP) mit Kennwortablauf und Alterung • Generische LDAP-Unterstützung • Kombinierte mehrstufige Zertifikats- und Benutzernamen-Kennwort-Authentifizierung (doppelte Authentifizierung)
Konsistentes Anwendererlebnis	• Der Full-Tunnel-Client-Modus unterstützt Remote-Benutzer, die eine konsistente LAN-ähnliche Benutzererfahrung benötigen. • Mehrere Bereitstellungsmethoden gewährleisten eine umfassende Kompatibilität von AnyConnect. • Benutzer können Push-Updates zurückstellen. • Die Feedback-Option zum Kundenerlebnis ist verfügbar.
Zentralisierte Richtlinienkontrolle und -verwaltung	• Richtlinien können vorkonfiguriert oder lokal konfiguriert werden und automatisch vom VPN-Sicherheits-Gateway aktualisiert werden. • API für AnyConnect vereinfacht die Bereitstellung über Webseiten oder Anwendungen. • Prüfen und Benutzerwarnungen werden für nicht vertrauenswürdige Zertifikate ausgegeben. • Zertifikate können lokal angezeigt und verwaltet werden.
Erweiterte IP-Netzwerkverbindung	• Öffentliche Verbindungen zu und von IPv4- und IPv6-Netzwerken • Zugriff auf interne IPv4- und IPv6-Netzwerkressourcen • Administratorgesteuerte Netzwerkzugriffsrichtlinien für Split-Tunneling und für das Senden aller Daten über den Tunnel • Zugriffskontrollrichtlinie • Per-app VPN-Richtlinie für Google Android (Lollipop) und Samsung KNOX (neu in Version 4.0) erfordert Cisco ASA 5500-X mit OS 9.3 oder höher und AnyConnect 4.0-Lizenzen) **Mechanismen für die IP-Adresszuweisung:**

	• Statisch • Interner Pool • Dynamic Host Configuration Protocol (DHCP) • RADIUS/LDAP
Robuste einheitliche Endgeräte-Compliance (Apex-Lizenz erforderlich)	• Endpoint-Statusüberprüfung und -sanierung werden für kabelgebundene und Wireless-Umgebungen unterstützt (ersetzt den Cisco Identity Services Engine NAC Agent). Erfordert Identity Services Engine 1.3 oder höher mit Identity Services Engine-Apex-Lizenz. • Cisco Hostscan sucht nach Antivirus-Software, persönlicher Firewall-Software und Windows-Service Packs auf dem Endgerätesystem, bevor dieser Zugriff auf das Netzwerk gewährt wird. • Administratoren können zudem benutzerdefinierte Statusprüfungen auf der Grundlage der ausgeführten Prozesse definieren. • Hostscan erkennt das Vorhandensein eines Wasserzeichens auf einem Remote-System. Das Wasserzeichen kann verwendet werden, um Vermögenswerte in Unternehmenseigentum zu identifizieren und einen differenzierten Zugang zu ermöglichen. Die Funktion zur Überprüfung von Wasserzeichen umfasst Registry-Werte, das Vorhandensein einer Datei, die mit einer erforderlichen CRC32-Prüfsumme übereinstimmt, IP-Adressbereichszuordnung und Zertifikate, die von oder an eine entsprechende Zertifizierungsstelle ausgestellt wurden. Zusätzliche Funktionen werden für Anwendungen unterstützt, die die Compliance nicht erfüllen. • Die Funktionen variieren je nach Betriebssystem. Detaillierte Informationen hierzu finden Sie in den Host Scan Support Charts.
Client-Firewall-Richtlinie	• Bietet zusätzlichen Schutz für Split-Tunneling-Konfigurationen. • Wird in Verbindung mit dem AnyConnect-Client verwendet, um Ausnahmen für den lokalen Zugriff zuzulassen (z. B. Drucken, Tethered Device Support usw.). • Unterstützt portbasierte Regeln für IPv4 sowie Netzwerk- und IP-Zugriffskontrolllisten (ACLs) für IPv6. • Verfügbar für Windows- und Mac OS X-Plattformen.
Lokalisierung	**Neben Englisch sind folgende Übersetzungen enthalten:** • Tschechisch (cs-cz) • Deutsch (de-de) • Spanisch (es-es) • Französisch (fr-fr) • Japanisch (ja-jp) • Koreanisch (ko-kr) • Polnisch (pl-pl) • Chinesisch (vereinfacht) (zh-cn) • Chinesisch (Taiwan) (zh-tw) • Niederländisch (nl-nl) • Ungarisch (hu-hu) • Italienisch (it-it) • Portugiesisch (Brasilien) (pt-br) • Russisch (ru-ru)
Einfache Client-Administration	• Administratoren können Software- und Richtlinien-Updates automatisch über die Headend-Sicherheits-Appliance verteilen, wodurch die Verwaltung von Client-Software-Updates entfällt.

	• Administratoren können festlegen, welche Funktionen für die Endbenutzerkonfiguration verfügbar sind. • Administratoren können beim Verbinden und Trennen ein Endpunktskript auslösen, wenn Domänen-Anmeldeskripts nicht verwendet werden können. • Administratoren können die für Endbenutzer angezeigten Meldungen vollständig anpassen und lokalisieren.
Profileditor	• AnyConnect-Richtlinien können direkt über den Cisco Adaptive Security Device Manager (ASDM) angepasst werden.
Diagnose	• On-Device-Statistiken und Protokollierungsinformationen sind verfügbar. • Protokolle können auf dem Gerät angezeigt werden. • Protokolle können problemlos per E-Mail an Cisco oder einen Administrator zur Analyse gesendet werden.
Federal Information Processing Standard (FIPS)	• FIPS 140-2 Level 2-kompatibel (es gelten Einschränkungen hinsichtlich Plattform, Funktion und Version)
Sichere Mobilität und Netzwerktransparenz	
Integration von Web Security (Cloud Web Security-Lizenz erforderlich)	* Verwendet Cloud Web Security, den weltweit größten Anbieter von Software-as-a-Service (SaaS)-Internetsicherheit, um Malware von Unternehmensnetzwerken fernzuhalten und die Internetnutzung der Mitarbeiter zu kontrollieren und zu schützen. • Unterstützt Cloud-gehostete Konfigurationen und dynamisches Laden. • Bietet Unternehmen Flexibilität und Auswahlmöglichkeiten, indem sie neben standortbasierten Services auch Cloud-basierte Services unterstützen. • Kann in die Web Security Appliance integriert werden. • Unterstützt Trusted Network Detection. • Erzwingt Sicherheitsrichtlinien für jede Transaktion, unabhängig vom Standort des Benutzers. • Erfordert eine stets verfügbare, hochsichere Netzwerkverbindung mit einer Richtlinie, die Netzwerkverbindungen zulässt oder verweigert, wenn der Zugriff nicht mehr verfügbar ist. • Erkennt Hotspots und Captive Portale.
Network Visibility-Modul (Apex-Lizenz erforderlich)	• Erkennen von möglichen Verhaltensanomalien durch Überwachung der Anwendungsnutzung • Ermöglicht fundiertere Entscheidungen beim Netzwerkdesign. • Kann Nutzungsdaten mit einer wachsenden Anzahl von IPFIX-fähigen (Internet Protocol Flow Information Export) Netzwerkanalysetools austauschen.
Enabler für Advanced Malware Protection (AMP) für Endgeräte (AMP für Endgeräte wird separat lizenziert)	• Vereinfacht die Bereitstellung von Bedrohungsdiensten für AnyConnect-Endpunkte durch die Verteilung und Aktivierung von CiscoAMP für Endgeräte. • Erweitert Bedrohungsservices für Endgeräte auf Remote-Endgeräte und verbessert so die Abdeckung von Endgeräten. • Bietet proaktiven Schutz, um sicherzustellen, dass Angriffe am Remote-Endpunkt schnell abgewehrt werden.
Umfassende Unterstützung für Betriebssysteme	• Windows 10, 8.1, 8 und 7 • Mac OS X 10.8 und höher
Network Access Manager und 802.1X	
Medienunterstützung	• Ethernet (IEEE 802.3) • Wi-Fi (IEEE 802.11a/b/g/n)
Netzwerkauthentifizierung	• IEEE 802.1X-2001, 802.1X-2004 und 802.1X-2010 • Ermöglicht die Bereitstellung eines einzigen 802.1X-Authentifizierungs-Frameworks für den Zugriff auf kabelgebundene

	und Wireless-Netzwerke. • Verwaltet die Benutzer- und Geräteidentität sowie die für den hochsicheren Zugriff erforderlichen Netzwerkzugriffsprotokolle. • Optimiert die Benutzerfreundlichkeit bei der Verbindung mit einem Cisco Unified Wired- und Wireless-Netzwerk.
Extensible Authentication Protocol (EAP)-Methoden	• EAP-Transport Layer Security (TLS) • EAP-Protected Extensible Authentication Protocol (PEAP) mit den folgenden internen Methoden: - EAP-TLS - EAP-MSCHAPv2 - EAP-Generic Token Card (GTC) • EAP-Flexible Authentication via Secure Tunneling (FAST) mit den folgenden internen Verfahren: - EAP-TLS - EAP-MSCHAPv2 - EAP-GTC • EAP-Tunneled TLS (TTLS) mit folgenden internen Verfahren: - Password Authentication Protocol (PAP) - Challenge Handshake Authentication Protocol (CHAP) - Microsoft CHAP (MSCHAP). - MSCHAPv2 - EAP-MD5 - EAP-MSCHAPv2 • Lightweight EAP (LEAP), nur Wi-Fi • EAP-Message Digest 5 (MD5), vom Administrator konfiguriert, nur für Ethernet • EAP-MSCHAPv2, vom Administrator konfiguriert, nur Ethernet • EAP-GTC, vom Administrator konfiguriert, nur Ethernet
Wireless-Verschlüsselungsmethoden (entsprechende 802.11-NIC-Unterstützung erforderlich)	• Öffnen • Wired Equivalent Privacy (WEP) • Dynamisches WEP • Wi-Fi Protected Access (WPA) Enterprise • WPA2 Enterprise • WPA Personal (WPA-PSK) • WPA2 Personal (WPA2-PSK) • CCKM (erfordert Cisco CB21AG Wireless NIC)
Wireless-Verschlüsselungsprotokolle	• Zählermodus mit Cipher Block Chaining Message Authentication Code Protocol (CCMP) unter Verwendung des AES-Algorithmus (Advanced Encryption Standard) • Temporal Key Integrity Protocol (TKIP) unter Verwendung der Rivest Cipher 4 (RC4)-Stream-Verschlüsselung
Sitzungswiederaufnahme	• RFC2716 (EAP-TLS)-Sitzungswiederaufnahme unter Verwendung von EAP-TLS, EAP-FAST, EAP-PEAP und EAP-TTLS • Wiederaufnahme der Stateless EAP-FAST-Sitzung • PMK-ID-Caching (Proactive Key Caching oder Opportunistic Key Caching), nur Windows XP
Ethernet-Verschlüsselung	• Media Access Control: IEEE 802.1AE (MACsec) • Schlüsselverwaltung: MACsec Key Agreement (MKA) • Definiert eine Sicherheitsinfrastruktur in einem kabelgebundenen Ethernet-Netzwerk, um Datenvertraulichkeit, Datenintegrität und Authentifizierung der Datenherstellung bereitzustellen. • Schützt die Kommunikation zwischen vertrauenswürdigen Komponenten des Netzwerks.
Eine Verbindung gleichzeitig	• Ermöglicht nur eine einzige Verbindung zum Netzwerk und trennt

	alle anderen. • Kein Bridging zwischen Adaptern. • Ethernet-Verbindungen haben automatisch Priorität.
Komplexe Servervalidierung	• Unterstützt Regeln für "Endet mit" und "exakte Übereinstimmung". • Unterstützung für mehr als 30 Regeln für Server ohne Namenskonsistenz.
EAP-Chaining (EAP-FASTv2)	• Differenziert den Zugriff basierend auf Ressourcen des Unternehmens und von anderen Anbietern. • Validiert Benutzer und Geräte in einer einzigen EAP-Transaktion.
Enterprise Connection Enforcement (ECE)	• Hilft sicherzustellen, dass sich Benutzer nur mit dem richtigen Unternehmensnetzwerk verbinden. • Verhindert, dass sich Benutzer mit einem Drittanbieter-Access Point verbinden, um im Büro im Internet zu surfen. • Verhindert, dass Benutzer auf das Gastnetzwerk zugreifen. • Vermeidet umständliche Blacklisting.
Verschlüsselungstechnologie der nächsten Generation (Suite B)	• Unterstützt die neuesten kryptografischen Standards. • Elliptic Curve Diffie-Hellman-Schlüsselaustausch • Elliptic Curve Digital Signature Algorithm (ECDSA)-Zertifikate
Zertifikatstypen	• Interaktive Benutzerkennwörter oder Windows-Kennwörter • RSA SecurID-Token • Einmalkennwort (OTP)-Token • Smartcards (Axalto, Gemplus, SafeNet iKey, Alladin). • X.509 Zertifikate. • Elliptic Curve Digital Signature Algorithm (ECDSA)-Zertifikate.
Remote-Desktop-Unterstützung	• Authentifiziert Anmeldeinformationen von Remote-Benutzern für das lokale Netzwerk, wenn Remote Desktop Protocol (RDP) verwendet wird.
Unterstützte Betriebssysteme	• Windows 10, 8.1, 8 und 7