Cisco AnyConnect Secure Mobility Client für mobile Plattformen

Der Cisco AnyConnect® Secure Mobility Client für mobile Plattformen ermöglicht Smartphones und Tablets einen unkomplizierten, zuverlässigen Zugriff auf das Unternehmensnetzwerk über eine unterbrechungsfreie verschlüsselte Verbindung.

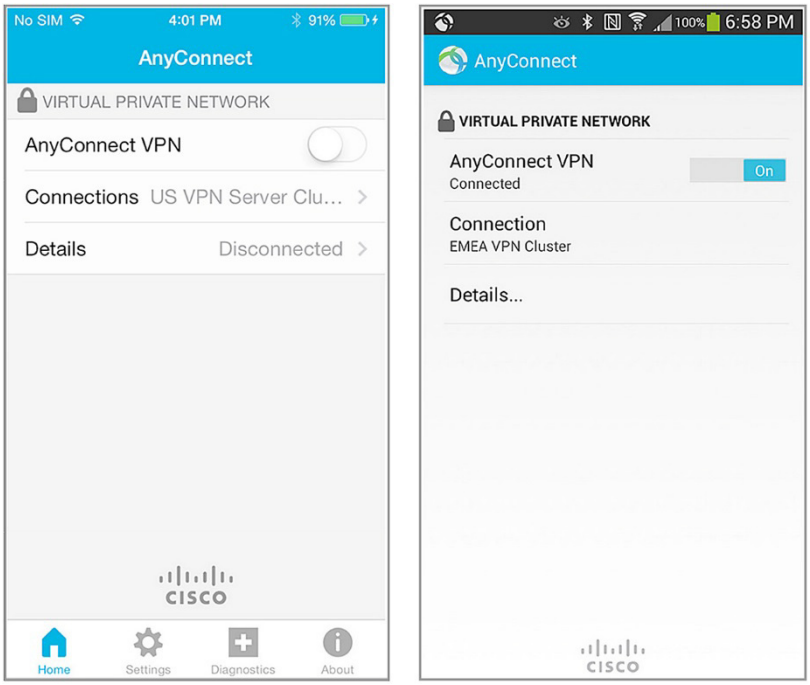
Produktübersicht

Der Cisco AnyConnect Secure Mobility Client für mobile Plattformen kann auf zahlreichen Smartphones und Tablets verwendet werden. Unterstützt werden Apple iOS, Android, Windows Phone 8.1, BlackBerry 10.3.2 oder höher, ausgewählte Amazon Kindle- und Fire Phone-Geräte sowie Google Chrome OS (Preview-Version).

Unabhängig davon, ob geschäftliche E-Mails, virtuelle Desktop-Sitzungen oder andere Unternehmensanwendungen – der AnyConnect Client bietet eine benutzerfreundliche Oberfläche für den Zugriff auf geschäftskritische Informationen aller Art. Der Client nutzt Datagram Transport Layer Security (DTLS), IP Security Internet Key Exchange Version 2 (IPsec IKEv2) und TLS (HTTP über TLS/SSL), um unternehmenskritischen und latenzempfindlichen Anwendungen wie Voice-over-IP (VoIP) verschlüsselten Zugriff auf Unternehmensressourcen zu ermöglichen. AnyConnect 4.x unterstützt Per-App-VPN-Funktionen für iOS 8.3 oder höher.

Abbildung 1 zeigt beispielhaft die Benutzeroberfläche von AnyConnect auf einem Apple iOS- und einem Android-Gerät.

Abbildung 1. Benutzeroberfläche auf einem Apple iOS- und einem Android-Gerät



Funktionen und Vorteile

In Tabelle 1 sind die Funktionen und Vorteile des Cisco AnyConnect Secure Mobility Client für mobile Plattformen aufgeführt. Die verfügbaren Funktionen variieren je nach Plattform. Details dazu, welche Funktionen auf welchen Betriebssystemen unterstützt werden, finden Sie in den Plattform-Versionshinweisen und in der Dokumentation.

Tabelle 1. Funktionen und Vorteile

Funktion	Vorteil
Softwarezugriff und -kompatibilität	**Verfügbar in den jeweiligen App-Marketplaces** • **Apple App Store:** für Apple iOS 6.0 oder höher • **Google Play:** für Android 4.0 oder höher Stellen Sie sicher, dass Sie unter den verfügbaren AnyConnect-Images das richtige für Ihr Gerät auswählen. Nähere Informationen zu Systemanforderungen finden Sie in den Android-Versionshinweisen. • **Windows Store:** für Windows Phone 8.1 Update 1 oder höher • **Blackberry App World:** für Blackberry 10.3.2 oder höher • **Google Chrome OS:** für Chrome OS 43 oder höher (Preview) • **Amazon Appstore:** für ausgewählte Kindle- und Fire Phone-Geräte
Optimierter Netzwerkzugriff	• Auf Basis der vorliegenden Netzwerkeinschränkungen automatische Anpassung des Tunneling-Protokolls an die effizienteste Methode • Optimierte Verbindung über DTLS für TCP-basierten Anwendungszugriff und latenzempfindlichen Datenverkehr wie VoIP • TLS (HTTP über TLS/SSL) gewährleistet Verfügbarkeit von Netzwerkverbindungen in gesperrten Umgebungen • IPsec IKEv2 optimiert Verbindungen für latenzempfindlichen Datenverkehr, wenn die Sicherheitsrichtlinien die Verwendung von IPsec erfordern (Cisco Adaptive Security Appliance 8.4 oder höher erforderlich) • Kompatibel mit ASA VPN-Load-Balancing
Mobility-orientiert	• Transparente Fortsetzung nach IP-Adressänderungen, Verbindungsabbrüchen oder Geräte-Standby
Akku-freundlich	• Kompatibel mit Geräte-Ruhezustand
Verschlüsselung	• Unterstützt starke Verschlüsselung wie AES-256 und 3DES-168 (Auf dem Sicherheits-Gateway-Gerät muss eine Lizenz für starke Verschlüsselung aktiviert sein.) • Verschlüsselung der nächsten Generation, einschließlich NSA Suite B-Algorithmen, ESPv3 mit IKEv2, 4096-Bit-RSA-Schlüssel, Diffie-Hellman-Gruppe 24 und erweitertes SHA2 (SHA-256 und SHA-384). Nur für IPsec IKEv2-Verbindungen verfügbar. Diese Funktion setzt eine AnyConnect Apex-Lizenz voraus.
Authentifizierungsoptionen	• RADIUS • RADIUS mit Kennwortablauf (MSCHAPv2) an NT LAN Manager (NTLM) • RADIUS One Time Password (OTP)-Unterstützung (Status- und Antwortattribute) • RSA SecurID • Active Directory oder Kerberos • Digitales Zertifikat (kompatibel mit dem in AnyConnect integrierten Simple Certificate Enrollment Protocol (SCEP) zur Bereitstellung der Anmeldedaten) • Generische LDAP-Unterstützung (Lightweight Directory Access Protocol) • LDAP mit Kennwortablauf und zeitlicher Befristung von Kennwörtern • Kombinierte mehrstufige Zertifikats- und Benutzernamen-/Kennwortauthentifizierung (doppelte Authentifizierung)
Konsistentes Benutzererlebnis	• Der Full-Tunnel-Clientmodus unterstützt Remote-Benutzer, die eine konsistente, LAN-ähnliche Umgebung benötigen.
Zentrale Richtlinienkontrolle und zentrales Richtlinienmanagement	• Richtlinien können vorkonfiguriert oder lokal konfiguriert und automatisch über das VPN-Sicherheits-Gateway aktualisiert werden. • Der URI-Handler (Universal Resource Indicator) für AnyConnect vereinfacht die Bereitstellung über in Webseiten oder Anwendungen eingebettete URLs. • Zertifikate können lokal angezeigt und verwaltet werden.

Funktion	Vorteil
Fortschrittliche IP-Netzwerkanbindung	• Administratorgesteuerte Netzwerkzugriffsrichtlinien für Split-Tunneling und für das Senden aller Daten über den Tunnel • Per-App-VPN-Richtlinie für iOS 8.3 oder höher (erfordert Cisco ASA 5500-X mit OS 9.3.2 oder höher und AnyConnect Plus- oder Apex-Lizenz) • Zugriffskontrollrichtlinie **Zuordnungsmechanismen für IP-Adressen:** • Statisch • Interner Pool • Dynamic Host Configuration Protocol (DHCP) • RADIUS/LDAP
Lokalisierung	**Neben Englisch sind die folgenden Übersetzungen im Lieferumfang enthalten:** • Französisch (Kanada) (fr-ca) • Tschechisch (cs-cz) • Deutsch (de-de) • Japanisch (ja-jp) • Koreanisch (ko-kr) • Spanisch (Lateinamerika) (es-co) • Polnisch (pl-pl) • Chinesisch (vereinfacht) (zh-cn)
Diagnose	• Statistiken und Protokollierungsinformationen sind direkt auf dem Gerät verfügbar. • Protokolle können auf dem Gerät angezeigt werden. • Protokolle können einfach zur Analyse per E-Mail an Cisco oder an Administratoren gesendet werden.

Plattformkompatibilität

Der AnyConnect Secure Mobility Client ist mit allen Cisco Next-Generation Firewalls ASA 5500-X und Cisco Firewall der Serie 5500 Enterprise Editions kompatibel, auf denen die ASA-Softwareversion 8.0(4) oder höher ausgeführt wird. Die Verwendung der aktuellen ASA-Softwareversionen wird empfohlen.

Bestimmte Funktionen erfordern neuere ASA-Softwareversionen oder ASA 5500-X-Modelle.

Cisco unterstützt den AnyConnect-VPN-Zugriff über Cisco IOS® Version 15.1(2)T oder höher, das als hochsicheres Gateway mit gewissen Funktionseinschränkungen fungiert. Weitere Einzelheiten finden Sie unter Features Not Supported on the Cisco IOS SSL VPN (Nicht unterstützte Funktionen im Cisco IOS SSL-VPN). Weitere Informationen zur Unterstützung der Cisco IOS-Softwarefunktionen finden Sie unter http://www.cisco.com/go/fn.

Weitere Informationen zur Kompatibilität finden Sie unter http://www.cisco.com/en/US/docs/security/asa/compatibility/asa-vpn-compatibility.html.

Lizenzierungsoptionen und Bestellung

Informationen zur Lizenzierung und Bestellung von AnyConnect, Clientless-SSL-VPN sowie IPsec IKEv2 Remote-Access-VPN-Clients von Drittanbietern finden Sie in der Bestellanleitung zu AnyConnect. Zur Unterstützung sämtlicher Plattformen und Funktionen sind AnyConnect Plus- oder Apex-Lizenzen erforderlich. Kunden mit bestehenden Essentials- oder Premium- und Mobility-Lizenzen sind berechtigt, die iOS- und Android-Versionen (mit Ausnahme von Per-App-VPN-Funktionen) bis zum 30. April 2016 zu verwenden. Für alle anderen mobilen Plattformen sind Plus- oder Apex-Lizenzen erforderlich. AnyConnect VPN-Verbindungen mit Head-End-Geräten anderer Hersteller als Cisco sind in keinem Fall zulässig. Weitere Informationen finden Sie in der Bestellanleitung unter http://www.cisco.com/c/dam/en/us/products/security/anyconnect-og.pdf.

Cisco Capital

Auf Ihre Ziele abgestimmte Finanzierungslösungen

Mit Cisco Capital können Sie die Technologien erwerben, die Sie benötigen, um Ihre geschäftlichen Ziele zu erreichen und wettbewerbsfähig zu bleiben. Mit unserer Unterstützung senken Sie Ihre Kapitalausgaben, beschleunigen Ihr Wachstum und optimieren Ihren Return-on-Investment. Cisco Capital bietet Ihnen flexible Optionen für die Finanzierung von Hardware, Software, Services und zusätzlichen Drittanbietergeräten – das alles bei planbarer Zahlung. Cisco Capital ist in mehr als 100 Ländern verfügbar. Weitere Informationen.

Weitere Informationen

- Homepage für Cisco AnyConnect Secure Mobility Client: http://www.cisco.com/go/anyconnect.
- Dokumentation zu Cisco AnyConnect: http://www.cisco.com/c/en/us/support/security/anyconnect-secure-mobility-client/tsd-products-support-series-home.html.
- Cisco Next-Generation Firewalls der Serie ASA 5500-X: http://www.cisco.com/go/asa.
- Lizenzvereinbarung und Datenschutzrichtlinie für Cisco AnyConnect: http://www.cisco.com/c/en/us/td/docs/security/vpn_client/anyconnect/anyconnect40/license/end_user/AnyConnect-SEULA-v4-x.htm.

Danksagungen

Dieses Produkt enthält von OpenSSL Project entwickelte Software zur Verwendung mit dem OpenSSL-Toolkit.

Dieses Produkt enthält eine von Eric Young entwickelte Verschlüsselungssoftware.

Dieses Produkt enthält von Tim Hudson entwickelte Software.

Dieses Produkt enthält die HTTP-Bibliothek libcurl: Copyright 1996-2006, Daniel Stenberg.

Hauptgeschäftsstelle Nord- und Südamerika
Cisco Systems, Inc.
San Jose, CA

Hauptgeschäftsstelle Asien-Pazifik-Raum
Cisco Systems (USA) Pte. Ltd.
Singapur

Hauptgeschäftsstelle Europa
Cisco Systems International BV Amsterdam,
Niederlande

Cisco verfügt über mehr als 200 Niederlassungen weltweit. Die Adressen mit Telefon- und Faxnummern finden Sie auf der Cisco Website unter www.cisco.com/go/offices.

Gedruckt in den USA C78-527494-09 10/15