Ontvang de kennis van Cisco AnyConnect Secure Mobility Client

Doel

Dit artikel concentreert zich op de eigenschappen, specificaties en voordelen van het gebruik van Cisco AnyConnect. Raadpleeg het artikel AnyConnect-licenties voor de RV340-Series routers voor informatie over AnyConnect-licenties op de RV340 Series routers.

Softwareversie

4.2.030-13 (Releaseopmerkingen)

Functies en specificaties

Functie	Voordelen en details
VPN-toegang met externe toegang	
Ondersteuning voor breedbandbesturingssysteem	• Windows 10, 8.1, 8 en 7 • Mac OS X 10.8 en hoger • Linux Intel (x64) • Zie het AnyConnect Mobile informatieblad voor mobiel platform.
Geoptimaliseerde netwerktoegang: VPN-protocolkeuze SSL (TLS en DTLS); IPsec IKEv2	• AnyConnect biedt een keuze voor VPN-protocollen, zodat beheerders kunnen gebruikmaken van elk protocol dat het best op hun zakelijke behoeften aansluit. • Ondersteuning voor tunneling omvat SSL (TLS 1.2 en DTLS) en IPsec IKEv2 van de volgende generatie. • DTLS biedt een geoptimaliseerde verbinding voor latentiegevoelig verkeer, zoals VoIP-verkeer of TCP-gebaseerde toepassingstoegang. • TLS 1.2 (HTTP over TLS of SSL) helpt de beschikbaarheid van netwerkconnectiviteit te verzekeren door middel van afgesloten omgevingen, waaronder die die web proxy-servers gebruiken. • IPsec IKEv2 biedt een geoptimaliseerde verbinding voor gevoelig verkeer met latentie wanneer het beveiligingsbeleid gebruik van IPsec vereist.
Optimale selectie van gateways	• Bepaal en maakt connectiviteit op het optimale netwerk-access point, waardoor de noodzaak voor eindgebruikers om de dichtstbijzijnde locatie te bepalen wordt geminimaliseerd.
Mobiliteitsvriendelijk	• Ontworpen voor mobiele gebruikers • Kan worden ingesteld zodat de VPN-verbinding behouden blijft tijdens wijzigingen in IP-adres, het verlies van connectiviteit of hibernatie of standby. • Met Trusted Network Detectie kan de VPN-verbinding automatisch worden verbroken wanneer een eindgebruiker op kantoor is en verbinding maakt wanneer een gebruiker op een externe locatie is.
Versleuteling	• AES-256 en 3DES-168. (Het security gateway-apparaat moet zijn voorzien van een sterke crypto-licentie.) • NSA Suite B-algoritmen, ESPv3 met IKEv2, 4096-bits RSA-

	toetsen, Diffie-Hellman groep 24 en uitgebreide SHA2 (SHA-256 en SHA-384). Is alleen van toepassing op IPsec IKEv2-verbindingen. Er is een AnyConnect Apex-licentie vereist.
Breed bereik van installatie- en verbindingsopties	**Installatieopties:** • Preimplementatie, inclusief Microsoft Installer • Automatische security gateway-implementatie (beheerrechten zijn vereist voor eerste installatie) door ActiveX (alleen Windows) en Java **Verbinding:** • Standalone door systeempictogram • Door browser geïnitieerd (weblancering) • Een clientloze portal gestart • Door CLI geïnitieerd • API gestart
Breed scala van verificatieopties	• RADIUS • RADIUS met wachtwoordafloop (MSCHAPv2) naar NT LAN Manager (NTLM) • Ondersteuning van één keer RADIUS-wachtwoord (OTP) (status- en antwoordberichtkenmerken) • RSA SECurID (inclusief SoftID-integratie) • Actieve map voor Kerberos • Geïntegreerde certificeringsinstantie (CA) • Digitaal certificaat of smartcard (inclusief ondersteuning voor machinecertificaten), automatisch of door de gebruiker geselecteerd • Lichtgewicht Directory Access Protocol (LDAP) met wachtwoordafloop en veroudering • Generic LDAP-ondersteuning • Gecombineerde verificatie van certificaten en gebruikersaam-wachtwoord (dubbele authenticatie)
Consistente gebruikerservaring	• De volledige tunnelclientmodus ondersteunt gebruikers van toegang op afstand die een consistente LAN-achtige gebruikerservaring nodig hebben. • Meervoudige leveringsmethoden helpen te zorgen voor brede compatibiliteit van AnyConnect. • Gebruiker kan geduwde updates uitstellen. • Er is een feedback-optie voor de klant beschikbaar.
Gecentraliseerde beleidscontrole en -beheer	• Het beleid kan lokaal worden ingesteld of ingesteld en kan automatisch worden bijgewerkt vanaf de VPN-beveiligingsgateway. • API voor implementaties van AnyConnect via webpagina's of toepassingen. • De controle- en gebruikerswaarschuwingen zijn afgegeven voor onvertrouwde certificaten. • Certificaten kunnen lokaal worden bekeken en beheerd.
Geavanceerde IP-netwerkconnectiviteit	• Openbare connectiviteit naar en van IPv4- en IPv6-netwerken • Toegang tot interne IPv4- en IPv6-netwerkbronnen • Door beheerder beheerde splitsingen en tunneling van het netwerktoegangsbeleid • Toegangsbeheerbeleid • Per-app VPN-beleid voor Google Android (Lollipop) en Samsung KNOX (nieuw in release 4.0) vereist Cisco ASA met OS 9.3 of hoger en AnyConnect 4.0 (licenties) **Mechanismen voor IP-adrestoewijzing:** • Statisch • Interne pool

	• Dynamic Host Configuration Protocol (DHCP) • RADIUS/LDAP
robuuste naleving van uniforme endpoints (Apex-licentie vereist)	• Beoordeling en herstel van endpoints wordt ondersteund voor bekabelde en draadloze omgevingen (ter vervanging van de Cisco Identity Services Engine NAC Agent). Vereist Identity Services Engine 1.3 of hoger met Identity Services Engine Apex-licentie. • Cisco Hostscan probeert de aanwezigheid van antivirussoftware, persoonlijke firewallsoftware en Windows-servicepakketten op het endpointsysteem te detecteren voordat u netwerktoegang verleent. • De beheerders hebben ook de optie om aangepaste polariteitscontroles te definiëren op basis van de aanwezigheid van actieve processen. • Een Hostscan detecteert de aanwezigheid van een watermerk op een extern systeem. Het watermerk kan worden gebruikt om activa te identificeren die eigendom zijn van bedrijven en daardoor gedifferentieerde toegang verschaffen. De mogelijkheid van watermark-controle omvat de systeemregistratiewaarden, het bestaan van een bestand dat overeenkomt met een vereiste checksum van CRC32, het aanpassen van IP-adressenbereik en certificaten die zijn afgegeven door of aan een overeenstemmende certificaatautoriteit. Aanvullende capaciteiten worden ondersteund voor toepassingen die niet aan de eisen voldoen. • De functies variëren per besturingssysteem. Zie de Host Scan Support-kaarten voor meer informatie.
Clientfirewallbeleid	• Biedt extra bescherming voor gesplitste tunneling-configuraties. • Gebruikt in combinatie met de AnyConnect-client om uitzonderingen voor lokale toegang mogelijk te maken (bijvoorbeeld afdrukken, ondersteuning van aangesloten apparaten enzovoort). • Ondersteunt poortgebaseerde regels voor IPv4- en netwerk- en IP-toegangscontrolelijsten (ACL's) voor IPv6. • Beschikbaar voor Windows- en Mac OS X-platforms.
Localisatie	**Naast het Engels zijn de volgende taalvertalingen opgenomen:** • Tsjechisch (cs-cz) • Duits (de-de) • Spaans (ES-ES) • Frans (fr-fr) • Japans (ja-jp) • Koreaans (ko-kr) • Pools (pl-pl) • Vereenvoudigd Chinees (zh-cn) • Chinees (Taiwan) (zh-tw) • Nederlands (nl-nl) • Hongaars (hu-hu) • Italiaans (it-it) • Portugees (Brazilië) (pt-br) • Russisch (ru-ru)
Eenvoudig beheer van cliënten	• Beheerders kunnen automatisch software en beleidsupdates van het head-end security apparaat distribueren, waardoor er een eind is gekomen aan de toediening van clientsoftwareupdates. • Beheerders kunnen bepalen welke functies u ter beschikking kunt stellen voor de configuratie van de eindgebruiker. • Beheerders kunnen een endpointscript activeren op het moment dat u een verbinding maakt met het domein wanneer u geen domeinaanmelding kunt gebruiken.

	• Beheerders kunnen de zichtbaar-berichten van de eindgebruiker volledig aanpassen en lokaliseren.
Profieleditor	• AnyConnect-beleid kan rechtstreeks worden aangepast via Cisco Adaptieve Security apparaat Manager (ASDM).
diagnostiek	• Er zijn statistieken op het apparaat en loginformatie beschikbaar. • Logs kunnen op het apparaat worden bekeken. • Logs kunnen eenvoudig per e-mail worden verzonden naar Cisco of een beheerder voor analyse.
Federal Information Processing Standard (FIPS)	• FIPS 140-2 niveau 2-compatibel (platform, optie en versiebeperkingen van toepassing)
Secure-mobiliteit en -netwerkzichtbaarheid	
Integratie met webbeveiliging (Licentie voor Cloud Web Security vereist)	• Gebruikt Cloud Web Security, de grootste wereldwijde provider van Web Security (Software-as-a-Service, SaaS), om malware te besparen op bedrijfsnetwerken en het internetgebruik van werknemers te controleren en beschermen. • Ondersteunt cloudgehost configuraties en dynamisch laden. • Biedt organisaties flexibiliteit en keuze door cloudgebaseerde services te ondersteunen naast de op gebouwen gebaseerde services. • Integreert met web security applicatie. • Ondersteunt betrouwbare netwerkdetectie. • Vereist het beveiligingsbeleid in elke transactie, onafhankelijk van de locatie van de gebruiker. • Vereist altijd op zeer veilige netwerkconnectiviteit met een beleid om netwerkconnectiviteit toe te staan of te ontkennen indien de toegang niet beschikbaar wordt. • Detecteert hotspots en portalen in gevangenschap.
Netwerkzichtbaarheidsmodule (Apex-licentie vereist)	• Ontdek potentiële gedragsanomalieën door het gebruik van de applicatie te controleren. • Maakt informatie over netwerkontwerp mogelijk. • Kan gebruiksgegevens delen met een groeiend aantal IPFIX-compatibele netwerkanalysetools (Internet Protocol Flow Information Exporteren).
Advanced Malware Protection (AMP) voor endpoints (Advanced Malware Protection voor endpoints afzonderlijk gelicentieerd)	• Vereenvoudig de mogelijkheid van bedreigingsservices voor AnyConnect-endpoints door Cisco Advanced Malware Protection te distribueren en te activeren voor endpoints. • breidt de bedreigingsservices voor endpoints op afstand uit, waardoor de dekking van endpoints toeneemt. • Biedt proactievere bescherming om verder te verzekeren dat een aanval snel wordt verzacht op het elders geplaatste eindpunt.
Ondersteuning voor breedbandbesturingssysteem	• Windows 10, 8.1, 8 en 7 • Mac OS X 10.8 en hoger
Network Access Manager en 802.1X	
Mediaondersteuning	• Ethernet (IEEE 802.3) • Wi-Fi (IEEE 802.11a/b/g/n)
Netwerkverificatie	• IEEE 802.1X-2001, 802.1X-2004 en 802.1X-2010 • Maakt bedrijven in staat om één enkel 802.1X authenticatiekader in te zetten voor toegang tot zowel bekabelde als draadloze netwerken. • Beheer van de gebruiker- en apparaatidentiteit en de netwerktoegangsprotocollen die vereist zijn voor een zeer veilige toegang. • Optimaliseert de gebruikerservaring bij het aansluiten op een Cisco uniform bekabeld en draadloos netwerk.

Extensible Authentication Protocol (EAP)-methoden	• EAP-Transport Layer Security (TLS) • EAP-Protected Extensible Authentication Protocol (PEAP) met de volgende innerlijke methoden: - MAP-TLS - EAP-MSCHAPv2 - EAP-Generic Token Card (GTC) • EAP-Flexibele verificatie via Secure Tunneling (FAST) met de volgende innerlijke methoden: - MAP-TLS - EAP-MSCHAPv2 - EAP-GTC • EAP-Tunneled TLS (TTLS) met de volgende binnenmethoden: - Wachtwoord-verificatieprotocol (PAP). - Challenge Handshake Authentication Protocol (CHAP). - Microsoft CHAP (MSCHAP). - MSCHAPv2 - MAP5 - EAP-MSCHAPv2 • Lichtgewicht EAP (LEAP), alleen Wi-Fi • EAP-Message Digest 5 (MD5), beheerst, alleen Ethernet • EAP-MSCHAPv2, beheerst, alleen Ethernet • EAP-GTC, beheerst, alleen Ethernet
Draadloze coderingsmethoden (hiervoor is 802.11 NIC-ondersteuning nodig)	• Open • Wired Equivalent Privacy (EVN) • Dynamisch EFUNECT • Wi-Fi beschermde Access (WAP) voor ondernemingen • WAP2 Enterprise • Persoonlijk (WAP-PSK) • Persoonlijk (WAP2-PSK) • CCKM (vereist Cisco CB21AG draadloze NIC)
Draadloze encryptieprotocollen	• Teller mode met Cipher Block Chaining Message Verification Code Protocol (CCMP) met het Advanced Encryption Standard (AES)-algoritme • TKIP (Temporal Key Integrity Protocol) met behulp van het Rugged Center 4 (RC4) stream-algoritme
Sessiehervatting	• Hervatting van de RFC2716-sessie (EAP-TLS) met EAP-TLS, EAP-FAST, EAP-PEAP en EAP-TTLS • OPNIEUW OPEN STAATloze sessie • PMK-ID-caching (Proactieve toetakeling of opportunistische toetakeling), alleen Windows XP
Ethernet-encryptie	• Media Access Control: IEEE 802.1AE (MACsec) • Belangrijk beheer: MACsec-sleutelovereenkomst (MKA) • Defineert een beveiligingsinfrastructuur op een bekabeld Ethernet-netwerk om gegevensvertrouwelijkheid, gegevensintegriteit en verificatie van gegevensoorsprong te bieden. • Garandeert communicatie tussen vertrouwde componenten van het netwerk.
Eén verbinding per keer	• Maakt slechts één verbinding met het netwerk mogelijk, waardoor alle anderen worden losgekoppeld. • Geen overbrugging tussen adapters. • Ethernet-verbindingen krijgen automatisch prioriteit.
Complexe servervalidatie	• Ondersteunt "eindigt met" en "exacte overeenkomst" regels. • Ondersteuning voor meer dan 30 regels voor servers zonder naamsgemeenschappelijkheid.

EAP-Chaining (EAP-FASTv2)	• Verschillende toegang op basis van ondernemings- en niet-bedrijfsmiddelen. • valideert gebruikers en apparaten in één MAP-transactie.
Handhaving van ondernemingsverbinding (ECE)	• Helpt ervoor te zorgen dat gebruikers alleen verbinding maken met het juiste bedrijfsnetwerk. • Beletten dat gebruikers tijdens hun kantoor verbinding kunnen maken met een toegangspunt van derden om op het internet te surfen. • Belet gebruikers toegang tot het gastnetwerk in te stellen. • Elimineert logge zwarte lijsten.
Next-generation encryptie (Suite B)	• Ondersteunt de nieuwste cryptografische standaarden. • Elliptische curve Diffie-Hellman sleuteluitwisseling • Ellips Curve Digital Signature Algorithm (ECDSA), certificaten
Credentials typen	• Interactieve gebruikerswachtwoorden of Windows-wachtwoorden • RSA SecureID-penningen • Eenmaal wachtwoord (OTP)-penningen • Smartcards (Axalto, Gemplus, SafeNet iKey, Alladin). • X.509-certificaten. • Elliptic Curve Digital Signature Algorithm (ECDSA), certificaten.
Ondersteuning voor Remote-desktop	• Verifieert externe gebruikersreferenties aan het lokale netwerk bij gebruik van het Remote Desktop Protocol (RDP).
Ondersteunde besturingssystemen	• Windows 10, 8.1, 8 en 7