Introduzione a Cisco AnyConnect Secure Mobility Client

Obiettivo

Il presente articolo verte sulle funzionalità, le specifiche e i vantaggi dell'uso di Cisco AnyConnect. Per informazioni sulle licenze AnyConnect sui router serie RV340, consultare l'articolo Licenze AnyConnect per i router serie RV340.

Versione del software

4.2.03013 (Note release)

Caratteristiche e specifiche

Funzionalità	Vantaggi e dettagli
VPN ad accesso remoto	
Ampio supporto del sistema operativo	• Windows 10, 8.1, 8 e 7 • Mac OS X 10.8 e versioni successive • Linux Intel (x64) • Per informazioni sulla piattaforma mobile, vedere il foglio dati AnyConnect Mobile.
Accesso alla rete ottimizzato: Scelta protocollo VPN SSL (TLS e DTLS); IPsec IKEv2	• AnyConnect offre una scelta di protocolli VPN, in modo che gli amministratori possano utilizzare il protocollo più adatto alle loro esigenze aziendali. • Il supporto del tunneling include SSL (TLS 1.2 e DTLS) e IPsec IKEv2 di nuova generazione. • DTLS fornisce una connessione ottimizzata per il traffico sensibile alla latenza, come il traffico VoIP o l'accesso alle applicazioni basato su TCP. • TLS 1.2 (HTTP su TLS o SSL) aiuta a garantire la disponibilità della connettività di rete tramite ambienti bloccati, inclusi quelli che usano server proxy Web. • IPsec IKEv2 offre una connessione ottimizzata per il traffico sensibile alla latenza quando i criteri di sicurezza richiedono l'uso di IPsec.
Selezione ottimale del gateway	• Determina e stabilisce la connettività al punto di accesso alla rete ottimale, eliminando la necessità per gli utenti finali di determinare la posizione più vicina.
Facile da trasportare	• Progettato per gli utenti mobili • Può essere configurato in modo che la connessione VPN rimanga stabilita durante la modifica dell'indirizzo IP, la perdita di connettività, l'ibernazione o lo standby. • Con Trusted Network Detection, la connessione VPN può disconnettersi automaticamente quando un utente è in ufficio e connettersi quando un utente si trova in una postazione remota.
Crittografia	• AES-256 e 3DES-168. (Il dispositivo gateway di sicurezza deve avere una licenza strong-crypto abilitata.)

	• Algoritmi NSA Suite B, ESPv3 con IKEv2, chiavi RSA a 4096 bit, gruppo Diffie-Hellman 24 e SHA2 migliorato (SHA-256 e SHA-384). Si applica solo alle connessioni IPsec IKEv2. È richiesta una licenza AnyConnect Apex.
Ampia gamma di opzioni di distribuzione e connessione	**Opzioni di implementazione:** • Predistribuzione, incluso Microsoft Installer • Distribuzione automatica del gateway di sicurezza (per l'installazione iniziale sono necessari diritti amministrativi) da ActiveX (solo Windows) e Java **Modalità di connessione:** • Indipendente dall'icona di sistema • Avviato dal browser (avvio Web) • Portale senza client avviato • CLI avviata • API avviata
Vasta gamma di opzioni di autenticazione	• RAGGIO • RADIUS con scadenza password (MSCHAPv2) per NT LAN Manager (NTLM) • Supporto OTP (One-Time Password) RADIUS (attributi del messaggio di stato e risposta) • RSA SecurID (inclusa l'integrazione SoftID) • Active Directory o Kerberos • Autorità di certificazione (CA) incorporata • Certificato digitale o smart card (incluso il supporto per certificati del computer), auto o selezionato dall'utente • Lightweight Directory Access Protocol (LDAP) con scadenza e durata della password • Supporto LDAP generico • Autenticazione multifattore combinata nome utente e password (doppia autenticazione)
Esperienza utente coerente	• La modalità client full-tunnel supporta gli utenti con accesso remoto che richiedono un'esperienza utente coerente simile a quella di una LAN. • L'uso di più metodi di consegna garantisce un'ampia compatibilità di AnyConnect. • L'utente può rinviare gli aggiornamenti push. • L'opzione per il feedback sull'esperienza del cliente è disponibile.
Gestione e controllo centralizzati delle policy	• I criteri possono essere preconfigurati o configurati localmente e possono essere aggiornati automaticamente dal gateway di sicurezza VPN. • L'API per AnyConnect semplifica le distribuzioni tramite pagine Web o applicazioni. • La verifica e gli avvisi utente vengono emessi per i certificati non attendibili. • I certificati possono essere visualizzati e gestiti localmente.
Connettività di rete IP avanzata	• Connettività pubblica da e verso reti IPv4 e IPv6 • Accesso alle risorse di rete IPv4 e IPv6 interne • Criteri di accesso alla rete per lo split-tunneling e il tunneling completo controllati dall'amministratore • Criteri di controllo di accesso • Criteri VPN per app per Google Android (Lollipop) e Samsung KNOX (novità della release 4.0; richiede Cisco ASA 5500-X con OS 9.3 o versioni successive e licenze AnyConnect 4.0) **Meccanismi di assegnazione degli indirizzi IP:**

	• Statico • Pool interno • DHCP (Dynamic Host Configuration Protocol) • RADIUS/LDAP
Solida conformità degli endpoint unificati (è richiesta la licenza Apex)	• La valutazione e il monitoraggio della postura degli endpoint sono supportati per ambienti cablati e wireless (in sostituzione dell'agente NAC di Cisco Identity Services Engine). Richiede Identity Services Engine 1.3 o versione successiva con licenza Identity Services Engine Apex. • Cisco Hostscan cerca di rilevare la presenza di software antivirus, software firewall personale e service pack di Windows sul sistema dell'endpoint prima di concedere l'accesso alla rete. • Gli amministratori hanno anche la possibilità di definire controlli di postura personalizzati in base alla presenza di processi in esecuzione. • Hostscan rileva la presenza di una filigrana su un sistema remoto. La filigrana può essere utilizzata per identificare i cespiti di proprietà dell'azienda e fornire di conseguenza un accesso differenziato. La funzionalità di verifica della filigrana include i valori del Registro di sistema, l'esistenza dei file corrispondente al checksum CRC32 richiesto, la corrispondenza dell'intervallo di indirizzi IP e i certificati rilasciati da o a un'autorità di certificazione corrispondente. Sono supportate funzionalità aggiuntive per le applicazioni non conformi. • Le funzioni variano a seconda del sistema operativo. Per informazioni dettagliate, vedere i grafici Host Scan Support.
Criteri firewall client	• Offre una maggiore protezione per le configurazioni di tunneling con split. • Utilizzato in combinazione con il client AnyConnect per consentire eccezioni di accesso locale (ad esempio, stampa, supporto di dispositivi collegati e così via). • Supporta regole basate sulle porte per IPv4 e elenchi di controllo di accesso (ACL) IPv6 e di rete. • Disponibile per piattaforme Windows e Mac OS X.
Localizzazione	**Oltre all'inglese, sono incluse le seguenti traduzioni:** • Ceco (cs-cz) • Tedesco (de-de) • Spagnolo (es-es) • Francese (fr-fr) • Giapponese (ja-jp) • Coreano (ko-kr) • Polacco (pl-pl) • Cinese semplificato (zh-cn) • Cinese (Taiwan) (zh-tw) • Olandese (nl-nl) • Ungherese (hu-hu) • Italiano (it-it) • Portoghese (Brasile) (pt-br) • Russo (ru-ru)
Facilità di amministrazione dei client	• Gli amministratori possono distribuire automaticamente gli aggiornamenti di software e policy dall'appliance di sicurezza headend, eliminando così l'amministrazione associata agli aggiornamenti software del client. • Gli amministratori possono determinare quali funzionalità rendere disponibili per la configurazione dell'utente finale.

	• Gli amministratori possono attivare uno script endpoint quando non è possibile utilizzare gli script di accesso al dominio durante i tempi di connessione e disconnessione. • Gli amministratori possono personalizzare e localizzare completamente i messaggi visibili all'utente finale.
Editor profili	• Le policy AnyConnect possono essere personalizzate direttamente da Cisco Adaptive Security Device Manager (ASDM).
Diagnostica	• Sono disponibili statistiche e informazioni di registrazione sul dispositivo. • È possibile visualizzare i log sul dispositivo. • I log possono essere facilmente inviati via e-mail a Cisco o a un amministratore per l'analisi.
FIPS (Federal Information Processing Standard)	• FIPS 140-2 conforme al livello 2 (restrizioni per piattaforma, funzionalità e versione applicate)
Mobilità sicura e visibilità della rete	
Integrazione della sicurezza Web (licenza Cloud Web Security richiesta)	• Utilizza Cloud Web Security, il più grande fornitore globale di sicurezza Web SaaS (Software-as-a-Service), per tenere il malware lontano dalle reti aziendali e controllare e salvaguardare l'uso Web dei dipendenti. • Supporta configurazioni ospitate nel cloud e caricamento dinamico. • Offre alle organizzazioni flessibilità e scelta supportando servizi basati sul cloud oltre a servizi basati sulla sede. • Si integra con Web Security Appliance. • Supporta Il Rilevamento Di Reti Attendibili. • Impone i criteri di sicurezza in ogni transazione, indipendentemente dalla posizione dell'utente. • Richiede una connettività di rete altamente sicura sempre attiva con un criterio per autorizzare o negare la connettività di rete se l'accesso non è disponibile. • Rileva gli hotspot e i portali in cattività.
Network Visibility Module (è richiesta la licenza Apex)	• Scoprire potenziali anomalie di comportamento monitorando l'utilizzo delle applicazioni. • Consente decisioni di progettazione della rete più informate. • Può condividere i dati di utilizzo con un numero crescente di strumenti di analisi della rete compatibili con IPFIX (Internet Protocol Flow Information Export).
Advanced Malware Protection (AMP) per Endpoints Enabler (AMP for Endpoints concesso in licenza separatamente)	• Semplifica l'abilitazione dei servizi di minacce agli endpoint AnyConnect distribuendo e abilitando Cisco AMP for Endpoints. • Estende i servizi di minaccia degli endpoint agli endpoint remoti, aumentando la copertura delle minacce degli endpoint. • Fornisce una protezione più proattiva per garantire ulteriormente che un attacco venga rapidamente mitigato sull'endpoint remoto.
Ampio supporto del sistema operativo	• Windows 10, 8.1, 8 e 7 • Mac OS X 10.8 e versioni successive
Network Access Manager e 802.1X	
Supporto multimediale	• Ethernet (IEEE 802.3) • Wi-Fi (IEEE 802.11a/b/g/n)
Autenticazione di rete	• IEEE 802.1X-2001, 802.1X-2004 e 802.1X-2010 • Consente alle aziende di distribuire un singolo framework di autenticazione 802.1X per accedere a reti cablate e wireless. • Gestisce l'identità di utenti e dispositivi e i protocolli di accesso alla rete necessari per un accesso altamente sicuro. • Ottimizza l'esperienza dell'utente durante la connessione a una rete cablata e wireless unificata di Cisco.

Metodi EAP (Extensible Authentication Protocol)	• EAP-Transport Layer Security (TLS) • EAP-Protected Extensible Authentication Protocol (PEAP) con i seguenti metodi interni: - EAP-TLS - EAP-MSCHAPv2 - GTC (EAP-Generic Token Card) • EAP-Flexible Authentication via Secure Tunneling (FAST) con i seguenti metodi interni: - EAP-TLS - EAP-MSCHAPv2 - EAP-GTC • EAP-Tunneled TLS (TTLS) con i seguenti metodi interni: - Protocollo PAP (Password Authentication Protocol). - Protocollo CHAP (Challenge Handshake Authentication Protocol). - CHAP Microsoft (MSCHAP). - MSCHAPv2 - EAP-MD5 - EAP-MSCHAPv2 • EAP leggero (LEAP), solo Wi-Fi • EAP-Message Digest 5 (MD5), configurazione amministrativa, solo Ethernet • EAP-MSCHAPv2, configurazione amministrativa, solo Ethernet • EAP-GTC, configurazione amministrativa, solo Ethernet
Metodi di crittografia wireless (è necessario il supporto NIC 802.11 corrispondente)	• Apri • WEP (Wired Equivalent Privacy) • WEP dinamico • WPA (Wi-Fi Protected Access) Enterprise • WPA2 Enterprise • WPA personale (WPA-PSK) • WPA2 Personal (WPA2-PSK) • CCKM (richiede una scheda di rete wireless Cisco CB21AG)
Protocolli di crittografia wireless	• Modalità contatore con CCMP (Cipher Block Chaining Message Authentication Code Protocol) che utilizza l'algoritmo AES (Advanced Encryption Standard) • TKIP (Temporal Key Integrity Protocol) con la cifratura di flusso RC4 (Rivest Cipher 4)
Ripresa della sessione	• RFC2716 (EAP-TLS) - Ripresa della sessione con EAP-TLS, EAP-FAST, EAP-PEAP e EAP-TTLS • Ripresa della sessione senza stato EAP-FAST • Cache PMK-ID (Proactive Key Caching o Opportunistic Key Caching), solo Windows XP
crittografia Ethernet	• Controllo accesso ai supporti: IEEE 802.1AE (MACsec) • Gestione chiavi: MKA (MACsec Key Agreement) • Definisce un'infrastruttura di sicurezza su una rete Ethernet cablata per fornire la riservatezza, l'integrità e l'autenticazione dei dati di origine. • Salvaguarda la comunicazione tra i componenti attendibili della rete.
Una connessione alla volta	• Consente una sola connessione alla rete, disconnettendo tutte le altre. • Nessun bridging tra schede. • Le connessioni Ethernet hanno automaticamente la priorità.
Convalida complessa dei server	• Supporta le regole "termina con" e "corrispondenza esatta". • Supporto di oltre 30 regole per i server senza compatibilità dei

	nomi.
Concatenamento EAP (EAP-FASTv2)	• Differenziazione dell'accesso in base alle risorse aziendali e non aziendali. • Convalida utenti e dispositivi in una singola transazione EAP.
Applicazione Enterprise Connection (ECE)	• Garantisce che gli utenti si connettano solo alla rete aziendale corretta. • Impedisce agli utenti di connettersi a un punto di accesso di terze parti per navigare su Internet mentre sono in ufficio. • Impedisce agli utenti di stabilire l'accesso alla rete guest. • Elimina la fastidiosa blacklist.
Crittografia di nuova generazione (Suite B)	• Supporta gli standard di crittografia più recenti. • Scambio chiavi Diffie-Hellman a curva ellittica • Certificati ECDSA (Elliptic Curve Digital Signature Algorithm)
Tipi di credenziali	• Password utente interattive o password di Windows • Token RSA SecurID • Token One-Time Password (OTP) • Smartcard (Axalto, Gemplus, SafeNet iKey, Alladin). • Certificati X.509. • Certificati ECDSA (Elliptic Curve Digital Signature Algorithm).
Supporto desktop remoto	• Autentica le credenziali dell'utente remoto nella rete locale quando si utilizza Remote Desktop Protocol (RDP).
Sistemi operativi supportati	• Windows 10, 8.1, 8 e 7