Cisco AnyConnect Secure Mobility Client per piattaforme mobili

Cisco AnyConnect® Secure Mobility Client per piattaforme mobili fornisce connettività di rete crittografata affidabile e facile da implementare da smartphone e tablet insieme all'accesso aziendale persistente per i dipendenti mobili.

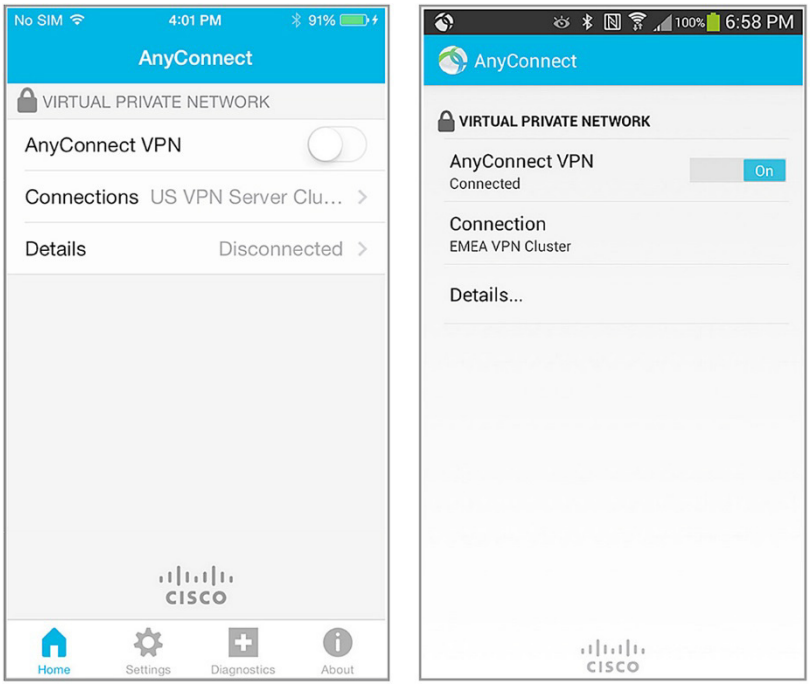
Panoramica del prodotto

Ora è possibile proteggere gli smartphone e i tablet dei dipendenti con il Cisco AnyConnect Secure Mobility Client per piattaforme mobili, disponibile per Apple iOS, Android, Windows Phone 8.1, BlackBerry 10.3.2 e versioni successive, alcuni dispositivi selezionati Amazon Kindle e Fire Phone e Google Chrome OS (versione di anteprima).

Sia che un dipendente abbia bisogno di accedere all'e-mail aziendale, a una sessione desktop virtuale o ad altre applicazioni aziendali, il client AnyConnect rappresenta un'interfaccia intuitiva per le informazioni business-critical. Il client utilizza Datagram Transport Layer Security (DTLS), IP Security Internet Key Exchange versione 2 (IPsec IKEv2) e TLS (HTTP su TLS/SSL) per fornire applicazioni business-critical, comprese le applicazioni sensibili alla latenza come voice over IP (VoIP), con accesso crittografato alle risorse aziendali. AnyConnect 4.x supporta le funzionalità VPN per app per iOS 8.3 e versioni successive.

La figura 1 mostra un esempio dell'interfaccia utente di AnyConnect sui dispositivi Apple iOS e Android.

Figura 1. L'interfaccia utente sui dispositivi Apple iOS e Android



Funzionalità e vantaggi

La tabella 1 elenca le funzionalità e i vantaggi di AnyConnect Secure Mobility Client per piattaforme mobili. Le funzionalità disponibili variano in base alla piattaforma utilizzata. Per i dettagli sulle specifiche funzionalità supportate per un particolare sistema operativo, vedere le note di rilascio per le piattaforme e la documentazione.

Tabella 1. Funzionalità e vantaggi

Funzionalità	Vantaggio
Accesso e compatibilità del software	**Disponibile negli store delle applicazioni** • **Apple App Store:** per Apple iOS 6.0 e versioni successive • **Google Play:** per Android 4.0 e versioni successive Si tenga presente che sono disponibili immagini diverse di AnyConnect, perciò è importante selezionare l'immagine corretta per il proprio dispositivo. Per i requisiti specifici, vedere le note di rilascio per Android. • **Windows Store:** per Windows Phone 8.1 Update 1 e versioni successive • **BlackBerry App World:** per BlackBerry 10.3.2 e versioni successive • **Google Chrome OS:** per Chrome OS 43 e versioni successive (anteprima) • **Amazon Appstore:** per dispositivi Kindle e Fire Phone selezionati
Accesso ottimizzato alla rete	• Adatta automaticamente il tunneling al metodo più efficiente possibile in base ai vincoli di rete • Utilizza DTLS per fornire una connessione ottimizzata per l'accesso alle applicazioni basato su TCP e il traffico sensibile alla latenza, come il traffico VoIP • Utilizza TLS (HTTP su TLS/SSL) per assicurare la disponibilità della connettività di rete attraverso ambienti bloccati • IPsec IKEv2 fornisce una connessione ottimizzata per il traffico sensibile alla latenza quando le policy di sicurezza richiedono l'utilizzo di IPsec (richiede Cisco Adaptive Security Appliance 8.4 o versione successiva) • Compatibile con il bilanciamento del carico VPN di ASA
Supporta la mobilità	• Effettua il ripristino in modo trasparente dopo il cambio di indirizzo IP, la perdita della connettività o lo standby dei dispositivi
Risparmia la batteria	• Compatibile con la modalità di inattività dei dispositivi
Crittografia	• Supporta la crittografia solida, tra cui AES-256 e 3DES-168. (Per il dispositivo gateway di sicurezza deve essere abilitata una licenza di crittografia solida). • Crittografia di nuova generazione, comprensiva di algoritmi Suite B NSA, ESPv3 con IKEv2, chiavi RSA a 4096 bit, Diffie-Hellman gruppo 24 e SHA2 potenziato (SHA-256 e SHA-384). Disponibile soltanto per le connessioni IPsec IKEv2. È necessaria una licenza AnyConnect Apex.
Opzioni di autenticazione	• RADIUS • RADIUS con scadenza password (MSCHAPv2) su NT LAN Manager (NTLM) • Supporto RADIUS One-Time Password (OTP) (attributi messaggi di stato e risposta) • RSA SecurID • Active Directory o Kerberos • Certificato digitale (compatibile con Simple Certificate Enrollment Protocol, o SCEP, integrato in AnyConnect per l'implementazione delle credenziali) • Supporto del protocollo generico LDAP (Lightweight Directory Access Protocol) • LDAP con scadenza e cambio obbligatorio della password • Autenticazione multifattore combinata di certificato e nome utente-password (autenticazione doppia)
Esperienza degli utenti coerente	• La modalità client full-tunnel supporta gli utenti con accesso remoto cui serve un'esperienza utente di tipo LAN coerente
Controllo e gestione delle policy centralizzati	• Le policy possono essere preconfigurate o configurate localmente e possono essere aggiornate automaticamente dal gateway di sicurezza VPN • Il gestore Universal Resource Indicator (URI) per AnyConnect facilita l'implementazione mediante URL incorporati nelle pagine Web o nelle applicazioni • I certificati possono essere visualizzati e gestiti localmente

Funzionalità	Vantaggio
Connettività di rete IP avanzata	• Policy di accesso alla rete con split-tunneling o all-tunneling controllata dall'amministratore • Policy VPN per app per iOS 8.3 e versioni successive (richiede Cisco ASA 5500-X con OS 9.3.2 o versione successiva e licenza AnyConnect Plus o Apex) • Policy di controllo degli accessi **Meccanismi di assegnazione dell'indirizzo IP:** • Statico • Pool interno • DHCP (Dynamic Host Configuration Protocol) • RADIUS/LDAP
Lingue	**Oltre alla versione inglese, sono disponibili le versioni nelle seguenti lingue:** • Francese canadese (fr-ca) • Ceco (cs-cz) • Tedesco (de-de) • Giapponese (ja-jp) • Coreano (ko-kr) • Spagnolo latino americano (es-co) • Polacco (pl-pl) • Cinese semplificato (zh-cn)
Diagnostica	• Sono disponibili statistiche e dati di log sul dispositivo. • È possibile visualizzare i log del dispositivo. • I log possono essere inviati facilmente per e-mail a Cisco o a un amministratore per essere analizzati.

Compatibilità con le piattaforme

Il client AnyConnect Secure Mobility è compatibile con tutti i modelli Cisco ASA serie 5500-X Next-Generation Firewall e Cisco serie 5500 Enterprise Firewall Edition che usano il software ASA versione 8.0(4) o successiva. È consigliato usare le versioni attuali del software ASA.

Alcune funzionalità richiedono versioni successive del software ASA o modelli ASA 5500-X.

Cisco supporta l'accesso VPN AnyConnect a Cisco IOS® Release 15.1(2)T o versioni successive come gateway estremamente sicuro con alcune funzionalità limitate. Per ulteriori informazioni, consultare la pagina delle funzionalità non supportate con Cisco IOS SSL VPN. Per ulteriori informazioni sul supporto di Cisco IOS Software, consultare http://www.cisco.com/go/fn.

Ulteriori informazioni sulla compatibilità sono disponibili alla pagina http://www.cisco.com/en/US/docs/security/asa/compatibility/asa-vpn-compatibility.html.

Informazioni sulle licenze e sugli ordini

La Guida agli ordini di AnyConnect riporta le informazioni sulle licenze e sugli ordini per AnyConnect, SSL VPN senza client e VPN di terze parti con accesso remoto IKEv2. Per il supporto completo delle piattaforme e delle funzionalità sono richieste licenze AnyConnect Plus o Apex. I clienti che possiedono licenze Essentials o Premium e Mobile possono utilizzare le versioni per iOS e Android (escluse le funzionalità VPN per app) fino al 30 aprile 2016. Tutte le altre piattaforme mobili richiedono licenze Plus o Apex. Non è mai consentita la connettività VPN AnyConnect ad apparecchiature di headend non Cisco. Per ulteriori informazioni, consultare la Guida agli ordini all'indirizzo http://www.cisco.com/c/dam/en/us/products/security/anyconnect-og.pdf.

Cisco Capital

Finanziamenti per aiutare i clienti a centrare i propri obiettivi

I finanziamenti Cisco Capital possono essere utili per riuscire ad acquistare la tecnologia necessaria per conseguire i propri obiettivi e mantenersi competitivi. Cisco aiuta a ridurre le spese in conto capitale (CapEx), accelerare la crescita e ottimizzare gli investimenti e il ROI. I finanziamenti Cisco Capital garantiscono flessibilità nell'acquisto di hardware, software, servizi e apparecchiature integrative di terze parti. Ed è previsto un unico pagamento fisso. Cisco Capital è disponibile in oltre 100 paesi. Altri dettagli.

Per ulteriori informazioni

- Home page di Cisco AnyConnect Secure Mobility Client: http://www.cisco.com/go/anyconnect.
- Documentazione di Cisco AnyConnect: http://www.cisco.com/c/en/us/support/security/anyconnect-secure-mobility-client/tsd-products-support-series-home.html.
- Cisco ASA serie 5500-X Next-Generation Firewall: http://www.cisco.com/go/asa.
- Contratto di licenza e informativa sulla privacy di Cisco AnyConnect: http://www.cisco.com/c/en/us/td/docs/security/vpn_client/anyconnect/anyconnect40/license/end_user/AnyConnect-SEULA-v4-x.html.

Riconoscimenti

Questo prodotto include software sviluppato dal progetto OpenSSL per l'utilizzo nell'OpenSSL Toolkit.

Questo prodotto include software crittografico creato da Eric Young.

Questo prodotto include software creato da Tim Hudson.

Questo prodotto comprende la libreria libcurl HTTP: Copyright 1996-2006, Daniel Stenberg.

Sede centrale Americhe
Cisco Systems Inc.
San Jose. CA (USA)

Sede centrale Asia e Pacifico
Cisco Systems (USA) Pte. Ltd.
Singapore

Sede centrale Europa
Cisco Systems International BV Amsterdam,
Paesi Bassi

Le sedi Cisco nel mondo sono oltre 200. Gli indirizzi, i numeri di telefono e di fax sono disponibili sul sito web Cisco all'indirizzo **www.cisco.com/go/offices**.

Stampato negli Stati Uniti C78-527494-09 10/15