

JUNIPER SECURE CONNECT

Panoramica del prodotto

[Juniper® Secure Connect](#) è un'applicazione SSL VPN e IPSec altamente flessibile che offre ai lavoratori da remoto un accesso sicuro alle risorse aziendali e cloud, fornendo connettività affidabile e sicurezza coerente a qualsiasi dispositivo, ovunque. Juniper Secure Connect è disponibile per dispositivi desktop e mobili, tra cui Windows, Apple macOS, iOS, iPadOS e Android. In combinazione con [i firewall della serie SRX](#), consente alle organizzazioni di ottenere rapidamente prestazioni e connettività ottimali dal client al cloud, riducendo i rischi estendendo la visibilità e l'applicazione a utenti e dispositivi, ovunque si trovino.

Descrizione prodotto

Le organizzazioni sono sempre più distribuite, principalmente grazie al lavoro da remoto e all'espansione delle filiali. La protezione di questo traffico distribuito richiede una visibilità approfondita della rete e la capacità di applicare le policy in ogni punto di connessione.

Juniper Secure Connect consente alle organizzazioni di fornire un accesso sicuro agli utenti finali sfruttando la connettività IP. Lavorando con i firewall serie SRX Juniper Networks® come punto di terminazione SSL VPN e IPSec di fascia alta, distribuiti nel campus, in un data center o nel cloud, Juniper Secure Connect consente l'accesso sicuro alle risorse vitali dai dispositivi utente che eseguono Windows, Apple macOS, iOS, iPadOS e Android™. La distribuzione di Secure Connect è semplice: l'applicazione client deve garantire l'utilizzo della policy più aggiornata a ogni connessione. Non è necessaria alcuna interazione con l'utente finale o l'amministratore per ridurre i tempi di distribuzione e risoluzione dei problemi in corso.

Architettura e componenti chiave

Offerto come licenza aggiuntiva per i firewall serie SRX, Juniper Secure Connect sfrutta la connettività IP per fornire un accesso sicuro agli utenti da qualsiasi luogo. Juniper Secure Connect funziona con i firewall serie SRX in fattori di forma fisici, virtuali e as-a-service, fornendo connettività e sicurezza di rete per supportare utenti, dispositivi e dati ovunque si trovino.

L'applicazione Juniper Secure Connect offre funzionalità aggiuntive che aumentano la sicurezza e l'usabilità. Queste funzionalità includono l'autenticazione biometrica e la convalida automatica delle policy prima di stabilire una connessione. L'applicazione utilizza un accesso pre-dominio di Windows per garantire che i dispositivi Windows siano convalidati

e aggiornati con l'ultimo criterio di gruppo Active Directory durante l'accesso, che utilizza soluzioni di autenticazione multifattore esterne.

Le policy di sicurezza vengono applicate ai dispositivi tramite Juniper Secure Connect. Queste policy potrebbero trattare questo traffico come se non fosse attendibile. Secure Connect sfrutta Juniper Networks® AppSecure, il sistema di prevenzione delle intrusioni (IPS), la sicurezza dei contenuti e la prevenzione avanzata delle minacce per estendere la sicurezza ai dispositivi remoti. Questo garantisce una sicurezza coerente nell'intera rete e fornisce il livello appropriato di accesso sicuro.

Juniper Secure Connect sfrutta policy di sicurezza coerenti che consentono alle organizzazioni di fornire una protezione efficace dalle minacce da e verso filiali, uffici domestici e dipendenti che lavorano da remoto all'interno di altre reti, consentendo alle organizzazioni di garantire architetture ed esperienze sicure.

I flussi di dati possono essere identificati dall'applicazione, dall'utente, dall'indirizzo IP e dall'URL, consentendo ai team IT di dare priorità o ispezionare più approfonditamente alcuni di questi flussi di dati. Con Juniper Secure Connect, la policy può richiedere che tutto il traffico venga instradato attraverso Connessione VPN o configurata per supportare il tunneling split, garantendo che il traffico può prendere il percorso migliore e più sicuro.

Tabella 1. Caratteristiche e vantaggi

Funzionalità	Description	Vantaggio
Disponibile per dispositivi desktop e mobili	Disponibile per sistemi operativi Windows, Apple macOS, iOS, iPadOS e Android.	Fornisce un accesso flessibile e sicuro per i dispositivi gestiti e non gestiti
Configurazione zero touch	Utilizza la convalida sicura e automatica della policy più recente, garantendo che gli utenti ottengano sempre la policy di sicurezza corretta.	Offre una policy di sicurezza sempre aggiornata, che garantisce la sicurezza degli utenti e l'accesso a le risorse corrette in qualsiasi momento.
Autenticazione multifattoriale e biometrica	Supporta l'autenticazione multifattore esterna da soluzioni di autenticazione multifattore (MFA) leader di settore per aumentare la sicurezza. Supporta anche l'autenticazione biometrica integrata sui dispositivi con supporto hardware.	Migliora la sicurezza aziendale sfruttando una seconda forma di autenticazione per gli utenti remoti.
Sicurezza e visibilità complete	L'accesso degli utenti tramite Juniper Secure Connect deve essere soggetto a IPS, Juniper Advanced Threat Prevention e sicurezza avanzata per identificare e bloccare le minacce sconosciute e note provenienti da reti non aziendali.	Riduce i rischi e fornisce visibilità per garantire che gli utenti con accesso remoto non introducano minacce note o sconosciute.

Juniper Security Director Cloud

[Security Director Cloud](#) è l'esperienza di gestione semplice e senza interruzioni di HPE, fornita in un'unica interfaccia utente per connettere le distribuzioni attuali dei clienti con i loro futuri rollout architetturati. La gestione è al centro della strategia di sicurezza connessa di Juniper e aiuta le organizzazioni a proteggere ogni punto di connessione sulla rete per salvaguardare utenti, dati e infrastruttura.

Le organizzazioni possono proteggere la propria architettura con policy di sicurezza coerenti in qualsiasi ambiente—on-premise, basato su cloud, cloud-delivered e ibrido, ed espandere zero trust a tutte le parti della rete, dall'edge al data center, fino alle applicazioni e ai microservizi. Con Security Director Cloud, le organizzazioni hanno visibilità ininterrotta, configurazione delle policy, amministrazione e informazioni collettive sulle minacce in un unico posto.

HPE incontra i nostri clienti nel loro percorso architetturativo, li aiuta a sfruttare gli investimenti esistenti e li consente di passare alla loro architettura preferita a un ritmo ottimale per il business automatizzando la transizione con la sicurezza Director Cloud.

Juniper Secure Edge

[Juniper Secure Edge](#) protegge la forza lavoro ovunque con l'accesso rapido, affidabile e sicuro di cui ha bisogno. Offre funzionalità SSE full-stack, tra cui FWaaS, SWG e CASB con DLP, ZTNA e protezione avanzata dalle minacce per proteggere l'accesso alle applicazioni web, SaaS e on-premise e fornire agli utenti una sicurezza che li segue ovunque si trovino.

HPE incontra i clienti dove si trovano e li porta dove vogliono andare sfruttando quello che hanno ed estendendo le loro iniziative zero trust a un'architettura cloud-delivered senza rompere la banca o il team operativo.

Juniper Secure Edge, gestito da Security Director Cloud, utilizza un unico framework di policy che consente di creare policy di sicurezza una sola volta per seguire utenti, dispositivi e dati ovunque si trovino. I clienti non devono ricominciare da zero quando adottano sicurezza fornita dal cloud. Con la nostra procedura guidata con tre clic, i clienti possono facilmente sfruttare le policy edge del campus esistenti e tradurle in una policy SSE. Poiché utilizza un unico framework di policy, indipendentemente dal modello di deployment, Secure Edge applica le policy di sicurezza esistenti dei deployment tradizionali al suo modello fornito sul cloud in pochi clic, riducendo gli errori di configurazione e i rischi.

Che si tratti di proteggere utenti remoti, sedi di campus e filiali, cloud privato, cloud pubblico o data center di cloud ibrido, HPE offre gestione unificata e visibilità ininterrotta su tutte le architetture. In questo modo, i team operativi possono facilmente colmare efficacemente i loro investimenti attuali con gli obiettivi architetturati futuri, tra cui SASE. I clienti possono gestire la sicurezza ovunque e ovunque, on-premise, nel cloud e dal cloud, con policy di sicurezza che seguono utenti, dispositivi e dati ovunque si trovino, il tutto da un'unica interfaccia utente.

Gli utenti hanno accesso rapido, affidabile e sicuro ai dati e alle risorse di cui hanno bisogno, garantendo esperienze utente eccezionali. I team di sicurezza IT ottengono una visibilità senza interruzioni sull'intera rete, sfruttando al contempo gli investimenti esistenti, aiutandoli a passare a un'architettura fornita dal cloud al loro ritmo.

Juniper Secure Edge fornisce policy di sicurezza coerenti che seguono l'utente, il dispositivo e i dati senza dover copiare o ricreare set di regole. È semplice distribuire il controllo delle applicazioni, la prevenzione delle intrusioni, il filtraggio del contenuto e del web forniti dal cloud e una prevenzione efficace delle minacce senza compromettere la visibilità o applicazione della sicurezza.

Diversi test di terze parti hanno costantemente convalidato HPE Juniper Networking come la tecnologia di sicurezza più efficace sul mercato negli ultimi cinque anni, con oltre il 99% di efficacia di sicurezza in tutti i casi d'uso.

Tabella 2. Specifiche

Caratteristiche	Windows	MacOS	iOS/iPadOS	Android
Crittografia di nuova generazione	Sì	Sì	Sì	Sì
VPN SSL basata su client	Sì	Sì	Sì	Sì
Dead peer detection (DPD)	Sì	Sì	Sì	Sì
Tunnel diviso	Sì	Sì	Sì	Sì
Autenticazione a più fattori (MFA)	Sì	Sì	Sì	Sì
Autenticazione biometrica	Sì	Sì	Sì	Sì
Configurazione delle applicazioni zero-touch	Sì	Sì	Sì	Sì
Controlli di compliance pre-accesso	Sì	Sì	Sì	Sì
Durata della licenza e del supporto di Juniper Secure Connect	1, 3 o 5 anni			

Informazioni per l'ordinazione

Per iniziare a utilizzare Juniper Secure Connect e accedere alle informazioni sulle licenze software, utilizza i seguenti link dal sito di supporto di HPE:

- [Windows](#)
- [macOS](#)
- [iOS/iPadOS](#)
- [Android](#)

Per saperne di più, visita la pagina [How to Buy](#) su www.juniper.net. Le licenze Juniper Secure Connect sono impilabili e l'utilizzo delle licenze si basa sugli utenti attuali connessi al firewall head-end SRX Series.

Informazioni su Hewlett Packard Enterprise

HPE è leader nella tecnologia aziendale essenziale, che riunisce la potenza dell'AI, del cloud e del networking per aiutare le organizzazioni a ottenere di più. In qualità di pionieri delle possibilità, la nostra innovazione e le nostre competenze migliorano il modo in cui le persone vivono e lavorano. Consentiamo ai nostri clienti di tutti i settori di ottimizzare le prestazioni operative, trasformare i dati in previsioni e massimizzare il loro impatto. Libera le tue ambizioni più audaci con HPE. Scopri di più su [HPE.com](https://www.hpe.com).

Esclusione di responsabilità: La presente scheda tecnica è stata tradotta in tedesco/francese/italiano/spagnolo/giapponese/coreano utilizzando l'intelligenza artificiale per maggiore praticità. Si noti che la traduzione non è stata rivista o verificata da traduttori umani e, come risultato, ci potrebbero essere errori o alterazioni linguistiche di piccola entità. Per informazioni più precise e affidabili, consultare la versione originale della scheda tecnica in lingua inglese.

Visita [HPE.com](https://www.hpe.com)

[Avvia chat](#)

© Copyright 2025 Hewlett Packard Enterprise Development LP. Le informazioni contenute nel presente documento sono soggette a modifica senza preavviso. Le uniche garanzie per i prodotti e i servizi Hewlett Packard Enterprise sono quelle espressamente indicate nelle dichiarazioni di garanzia esplicite che accompagnano tali prodotti e servizi. Nulla di quanto contenuto nel presente documento potrà essere interpretato come garanzia supplementare. Hewlett Packard Enterprise declina ogni responsabilità per eventuali omissioni ed errori tecnici o editoriali contenuti nel presente documento.

Android è un marchio registrato di Google LLC. Active Directory e Windows sono marchi o marchi registrati di Microsoft Corporation negli Stati Uniti e/o in altri Paesi. Tutti i marchi di terzi appartengono ai rispettivi titolari.

a00150844ITE, Rev. 1

HEWLETT PACKARD ENTERPRISE

[hpe.com](https://www.hpe.com)

