CLOUDFLARE

SINTESI DELLA SOLUZIONE

Proteggi i flussi di lavoro DevOps

Connettività Zero Trust per la tua pipeline CI/CD
e flussi di lavoro da servizio a servizio

Accesso semplice e sicuro per DevOps

Connettività e sicurezza agili come i tuoi flussi di lavoro
L'interazione complessa della pipeline di integrazione continua e distribuzione continua (CI/CD) è famosa per essere agile, quindi la connettività e la sicurezza che supportano questi flussi di lavoro dovrebbero corrispondere. Tuttavia, i team DevOps si affidano troppo spesso alle VPN tradizionali per ottenere l'accesso remoto a vari strumenti operativi e di sviluppo.

Perché gli strumenti tradizionali di accesso remoto non sono all'altezza

Le VPN sono intrinsecamente non sicure

Per l'accesso remoto non accontentarti delle VPN: sono scomode da gestire e suscettibili di sfruttamento con vulnerabilità note o zero-day.

Gli sviluppatori non amano l'attrito

La sicurezza deve "funzionare" perché, indipendentemente dal gruppo di dipendenti, gli sviluppatori sono in grado di trovare soluzioni alternative creative che riducano gli attriti del flusso di lavoro.

Gli strumenti non sono agili

Dovrebbero essere accettate modifiche ad hoc delle politiche di sicurezza, nonché l'accesso temporaneo Zero Trust per gli appaltatori o gli operatori di pronto intervento in caso di emergenza.

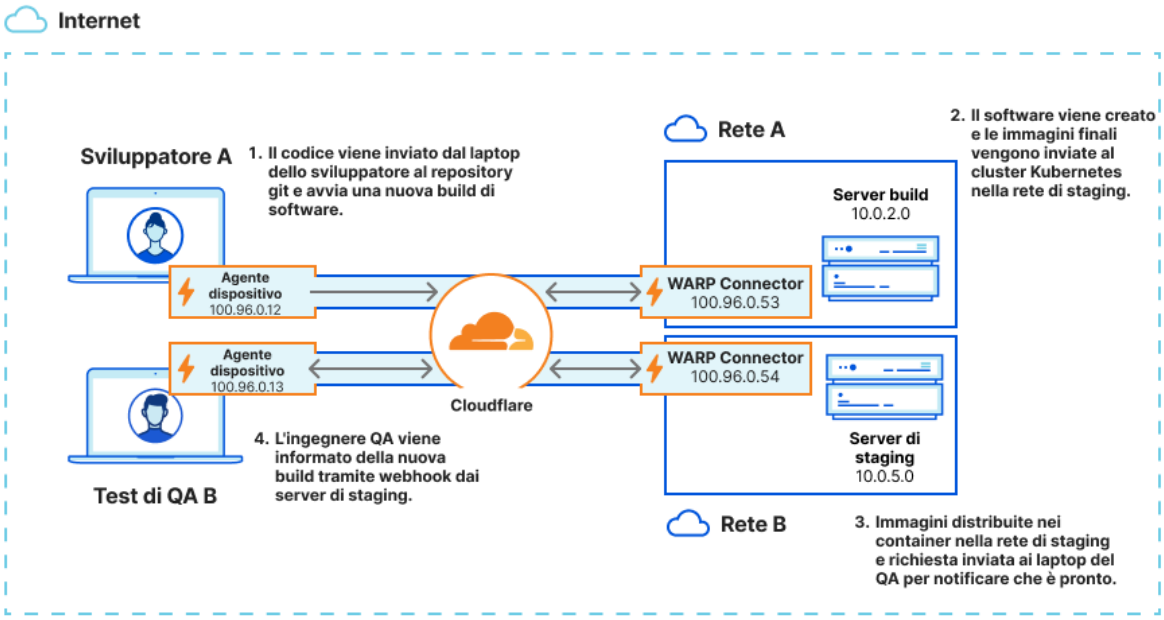
Estensione di ZTNA a DevOps

Connettività mesh e traffico bidirezionale
Zero Trust Network Access (ZTNA) funziona bene per l'accesso sicuro e con meno privilegi da parte dell'utente all'app (compresi gli sviluppatori che accedono ai server SSH), ma dovrebbe estendersi ulteriormente ai casi d'uso di rete sicura che coinvolgono traffico avviato dal server o bidirezionale. Ciò segue una tendenza emergente che immagina un modello di connettività mesh sovrapposta su cloud, VPC o segmenti di rete senza fare affidamento sui router.

Per una vera connettività any-to-any, i clienti hanno bisogno della flessibilità per coprire tutti i casi d'uso di connettività di rete e accesso alle app. Non tutti gli on-ramp di rete dei fornitori SASE possono estendersi oltre il traffico avviato dal client senza introdurre modifiche al routing di rete o compromessi di sicurezza, quindi le affermazioni generiche "any-to-any" potrebbero non essere ciò che sembrano inizialmente.

In che modo Cloudflare può essere d'aiuto

Cloudflare estende la portata di ZTNA per garantire che tutti i casi d'uso utente-app siano coperti, oltre a reti sicure mesh e peer-to-peer (P2P) per rendere le opzioni di connettività quanto più ampie e flessibili possibile. I flussi di lavoro da servizio a servizio di DevOps possono essere eseguiti in modo efficiente sulla stessa piattaforma che realizza ZTNA, sostituzione VPN o SASE di livello aziendale.



Cloudflare funge da “collante” di connettività tra tutti gli utenti e le risorse DevOps, indipendentemente dal flusso di traffico in ogni fase. Questa stessa tecnologia, ad esempio, WARP Connector, consente agli amministratori di gestire diverse reti private con intervalli IP sovrapposti: VPC e RFC1918, supportare il traffico avviato dal server e la connettività delle app P2P (ad esempio, SCCM, AD, traffico VoIP e SIP) su reti private esistenti, creare reti private P2P (ad esempio, flussi di risorse CI/CD) e instradare il traffico in modo deterministico. Le organizzazioni possono anche automatizzare la gestione della propria piattaforma SASE con il provider Terraform di Cloudflare.

Parliamo di un accesso semplice e sicuro per la tua organizzazione

Richiedi un workshop

CLOUDFLARE

Non sei ancora pronto per una conversazione dal vivo?

Scopri di più sulla nostra architettura di riferimento SASE.