CLOUDFLARE

SOLUTION BRIEF

Sécurisez les flux de travail DevOps

Une connectivité Zero Trust pour votre pipeline d'intégration/de déploiement en continu et vos flux de travail de service à service

Un accès simple et sécurisé pour les DevOps

Une connectivité et une sécurité aussi agiles que vos flux de travail

L'interaction complexe avec le pipeline d'intégration et de déploiement en continu (Continuous Integration and Continuous Delivery, CI/CD) est célèbre pour son agilité. La connectivité et la sécurité soutenant ces flux de travail devraient donc correspondre. Toutefois, les équipes de DevOps se reposent trop souvent sur des VPN traditionnels pour établir un accès à distance à divers outils opérationnels et de développement.

Les lacunes des outils traditionnels d'accès à distance

Les VPN sont intrinsèquement non sécurisés

N'optez pas pour les VPN pour l'accès à distance, car ils sont fastidieux à gérer et susceptibles à l'exploitation via des vulnérabilités connues ou zero-day.

Les développeurs détestent les frictions

La sécurité doit faire plus que « simplement fonctionner », car entre tous les groupes de collaborateurs, les développeurs sont capables de trouver des solutions de contournement créatives permettant de réduire les frictions au sein des flux de travail.

Les outils d'ancienne génération ne donnent pas dans l'agilité

Les modifications ponctuelles des politiques de sécurité doivent être possibles, de même que l'accès Zero Trust temporaire pour les sous-traitants ou les intervenants d'astreinte en cas d'incident.

Étendre le ZTNA aux DevOps

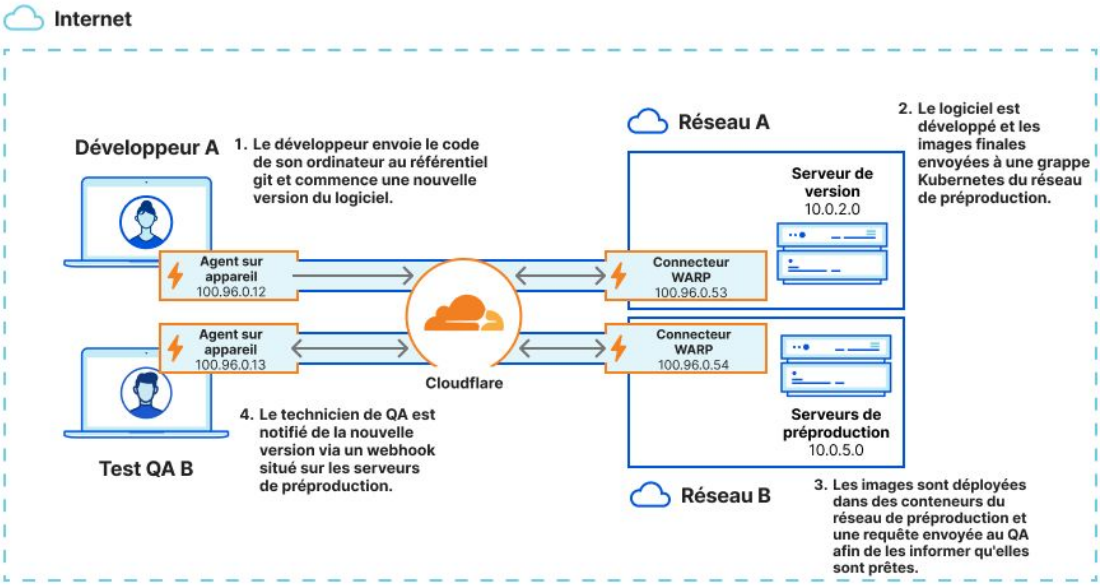
Connectivité maillée et trafic bidirectionnel

L'accès réseau Zero Trust (ZTNA) (Zero Trust Network Access, ZTNA) fonctionne bien pour l'accès sécurisé et de moindre privilège des utilisateurs aux applications (notamment l'accès des développeurs aux serveurs SSH), mais il devrait s'étendre davantage aux scénarios de mise en réseau sécurisée impliquant du trafic initié par un serveur ou bidirectionnel. Cette idée suit une tendance émergente qui imagine un modèle de connectivité maillée en superposition sur l'ensemble des clouds, des VPC ou des segments réseau, sans faire appel à des routeurs.

Pour profiter d'une véritable connectivité point à point (any-to-any), les clients ont besoin de la flexibilité nécessaire pour couvrir l'ensemble de leurs scenarios de connectivité au réseau et aux applications. Les accès réseau direct (on-ramp) proposés par les fournisseurs de SASE ne peuvent pas tous être étendus au-delà du trafic initié par le client sans modification du routage réseau ou compromis sur la sécurité. Les prétentions « any-to-any » génériques peuvent donc ne pas être ce qu'elles paraissent à l'origine.

Ce que Cloudflare peut vous apporter

Cloudflare étend la portée du ZTNA afin de faire en sorte que tous les scénarios utilisateur-application soient couverts, plus la mise en réseau sécurisée en maillage et en peer-to-peer (P2P), de manière à rendre les options de connectivité aussi larges et flexibles que possible. Les flux de travail DevOps service à service peuvent être exécutés efficacement sur la même plateforme que celle qui permet le ZTNA, le remplacement du VPN ou le SASE de niveau professionnel.



Cloudflare fait office de « colle » pour la connectivité de l'ensemble des utilisateurs et des ressources DevOps, indépendamment du flux de trafic à chaque étape. La technologie WARP Connector permet aux administrateurs de gérer différents réseaux privés aux plages IP redondantes (VPC et RFC1918, prise en charge du trafic initié par le serveur et la connectivité aux applications P2P — p. ex. trafic SCCM, AD, VoIP et SIP — sur les réseaux existants). Elle peut aussi permettre de construire des réseaux privés P2P (p. ex. flux de ressources CI/CD) et router le trafic de manière déterministe. Les entreprises peuvent également automatiser la gestion de leur plateforme SASE grâce au fournisseur Terraform de Cloudflare.

Discutons d'un accès simple et sécurisé pour votre entreprise

Demander un atelier

CLOUDFLARE

Vous n'êtes pas encore prêt à avoir une discussion en direct ?

Vous trouverez davantage d'informations dans notre architecture SASE de référence.