CLOUDFLARE

SOLUTION BRIEF

Secure DevOps Workflows

Zero Trust connectivity for your CI/CD pipeline and service-to-service workflows

Simple, secure access for DevOps

Connectivity and security as agile as your workflows

Complex continuous integration and continuous delivery (CI/CD) pipeline interaction is famous for being agile, so the connectivity and security supporting these workflows should match. However, DevOps teams too often rely on traditional VPNs to accomplish remote access to various development and operational tools.

Why traditional remote access tools fall short

VPNs are inherently insecure

Don't settle for VPNs for remote access, which are cumbersome to manage and susceptible to exploit with known or zero-day vulnerabilities.

Developers hate friction

Security needs to "just work" because of any employee group, developers are capable of finding creative workarounds that decrease workflow friction.

Legacy tools aren't agile

Ad hoc security policy changes should be accommodated, as well as temporary Zero Trust access for contractors or on-call incident responders.

Extending ZTNA to DevOps

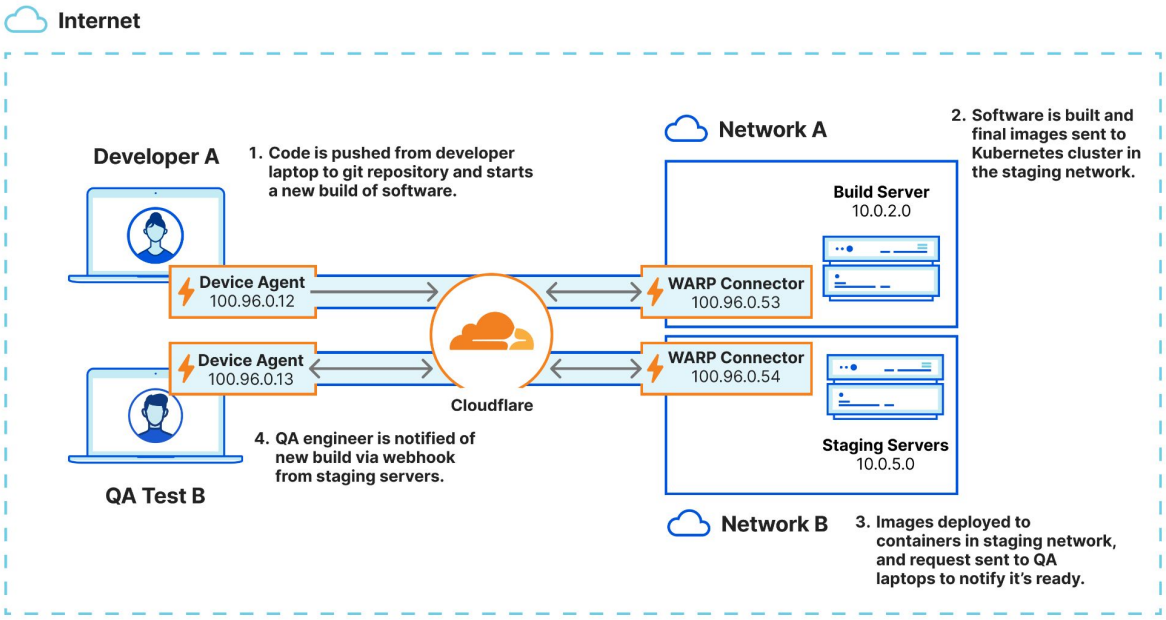
Mesh connectivity and bidirectional traffic

Zero Trust Network Access (ZTNA) works well for secure, least-privileged user-to-app access (including developers accessing SSH servers), but it should extend further to secure networking use cases that involve server-initiated or bidirectional traffic. This follows an emerging trend that imagines an overlay mesh connectivity model across clouds, VPCs, or network segments without a reliance on routers.

For true any-to-any connectivity, customers need flexibility to cover all of their network connectivity and app access use cases. Not every SASE vendor's network on-ramps can extend beyond client-initiated traffic without introducing network routing changes or security tradeoffs, so generic "any-to-any" claims may not be what they initially seem.

How Cloudflare can help

Cloudflare extends the reach of ZTNA to ensure all user-to-app use cases are covered, plus mesh and peer-to-peer (P2P) secure networking to make connectivity options as broad and flexible as possible. DevOps service-to-service workflows can run efficiently on the same platform that accomplishes ZTNA, VPN replacement, or enterprise-class SASE.



Cloudflare acts as the connectivity "glue" across all DevOps users and resources, regardless of the flow of traffic at each step. This same technology, i.e., WARP Connector, enables admins to manage different private networks with overlapping IP ranges — VPC & RFC1918, support server-initiated traffic and P2P apps (e.g., SCCM, AD, VoIP & SIP traffic) connectivity over existing private networks, build P2P private networks (e.g., CI/CD resource flows), and deterministically route traffic. Organizations can also automate management of their SASE platform with Cloudflare's Terraform provider.

Not quite ready for a live conversation?

Keep learning more in our SASE reference architecture.