How Cloudflare Access Replaces a VPN

The rise of remote work has caught many companies off guard. Many organizations have only purchased enough VPN licenses and appliance capacity to support a subset of their teams. The surge in remote work is putting considerable strain on both.

Cloudflare Access helps you reduce strain on your VPN with a modern approach to authentication for internally-managed applications. Access secures web apps, SSH connections, remote desktops and other protocols with Cloudflare's global network, where every request to the resource is evaluated for identity. When corporate tools are protected with Access, they feel like SaaS apps, and employees can log in to them with a simple and consistent flow.

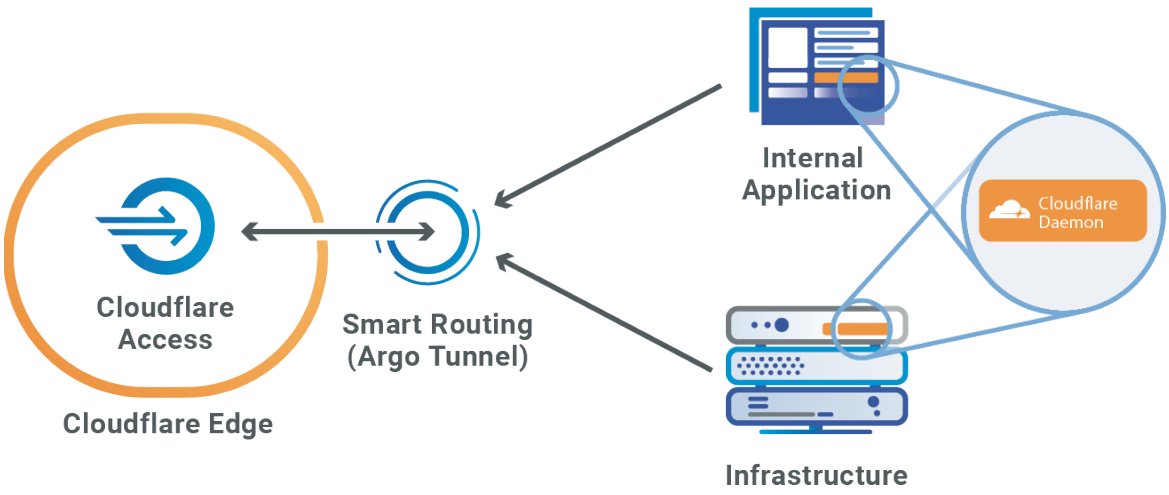
Here's how Cloudflare Access replaces a VPN with Cloudflare's network.

1. Cloudflare Access securely connects internal tools to the Internet

Teams connect their resources to Access through a secure outbound connection, Argo Tunnel, which runs in your infrastructure to connect applications and machines to Cloudflare. Argo Tunnel exposes web servers securely to the Internet without opening up firewall ports and configuring ACLs.

That tunnel makes outbound-only calls to the Cloudflare network.

Regardless of whether applications run on-premise or hosted in a cloud provider, Argo Tunnel can connect your infrastructure to Cloudflare.

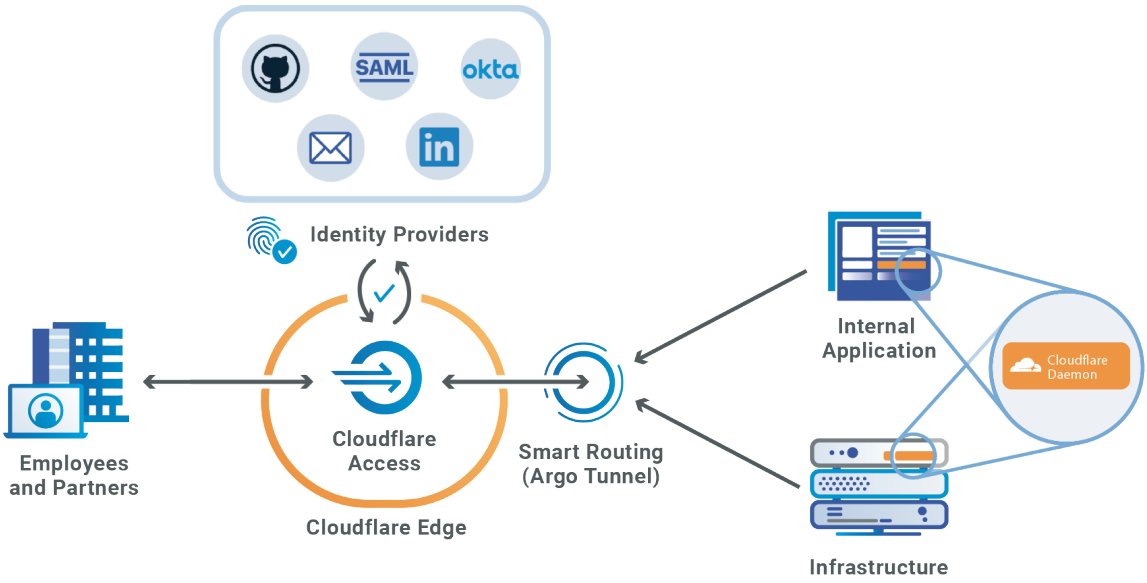


2. Requests to protected resources are routed through Cloudflare's edge

Argo Tunnel uses Argo Smart Routing technology to route traffic over the fastest path within the Cloudflare network between the user and the data centers closest to your origin.

Cloudflare data centers operate within 100 milliseconds of 99% of Internet-connected population in the developed world.

When a request to your resource hits Cloudflare's edge, Access acts like a bouncer standing in front of the resource, determining which requests get allowed in.

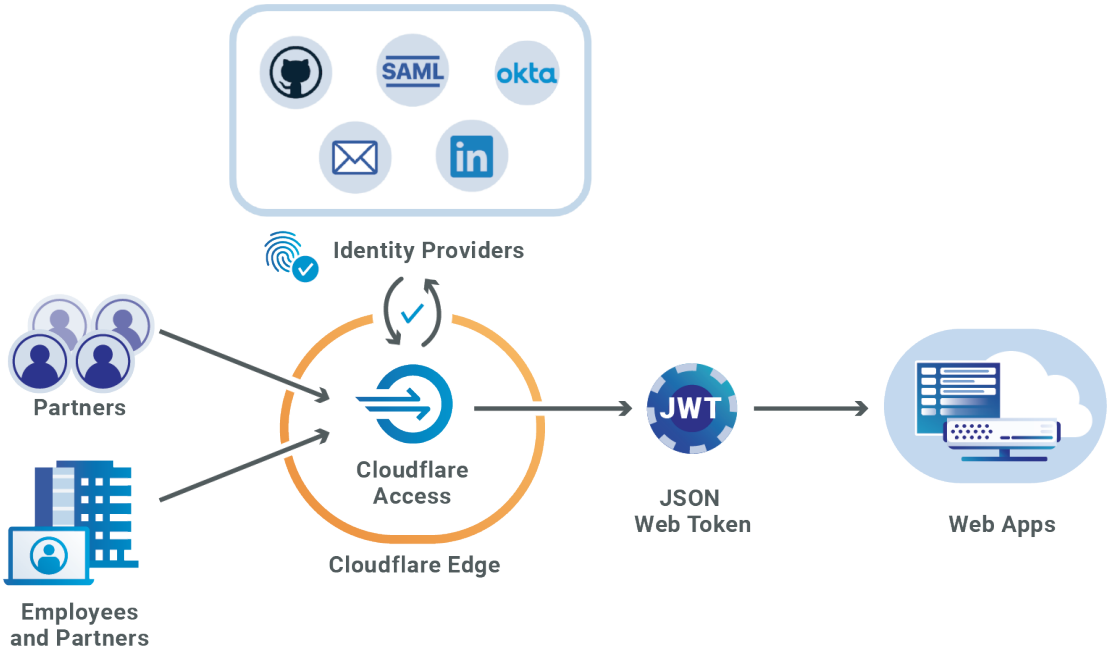


3. At Cloudflare's edge, Access applies policies set in your Identity Provider (IDP) to allow or block requests

Cloudflare Access integrates with your organization's identity provider to determine a user's identity. When users connect to an application protected by Access, they will be prompted to login with the identity provider configured.

Access supports providers that are maintained by your team, like Okta©, G Suite©, and AzureAD©, in addition to publicly available providers like LinkedIn© and GitHub©.

You can use Access to support multiple identity providers simultaneously, including tenants of the same type.



What you can protect with Access

SSH Connections

Secure Shell (SSH) protocol allows users to connect to infrastructure to perform activities like remote command execution. Cloudflare Access can secure connections over Secure Shell (SSH). When users attempt to reach resources from command lines, Access launches a browser window prompting them to login with their identity provider

Web Applications

Use Access to protect internally-managed applications like Jira, WordPress, GitLab and SAP, so users can login to access them without a VPN. Cloudflare Access evaluates requests to your application and determines whether visitors are authorized based on policies you define.

Remote Desktops

The Remote Desktop Protocol (RDP) allows users to connect to a desktop from a different machine. Cloudflare Access lets end users authenticate with their single sign-on (SSO) provider and connect to shared files over RDP without being on a VPN.

Other Protocols

You can use Access to add authentication to Secure Messaging Block (SMB) fileshares or applications that use arbitrary TCP.

Supported Identity Providers

Cloudflare Access integrates with your organization's identity provider to determine a user's identity. When users connect to an application protected by Access, they will be prompted to login with the identity provider configured. Organizations can use multiple identity providers at once with no limits.

- GSuite©
- Okta©
- Microsoft Azure AD©
- Centrify©
- Yandex©
- Citrix ADC©
- Facebook©
- Generic OIDC©
- GitHub©
- Google©
- JumpCloud SAML©
- KeyCloak SAML©
- LinkedIn©
- PingIdentity©
- OneLogin (OIDC and SAML)©
- One Time Pin (OTP) Login©
- Atlassian© Jira and Confluence SSO
- Redash©

Sign up for Access today at teams.cloudflare.com