ZEBRA SYSTEMS

CLOUDFLARE PARTNER NETWORK

Jak Cloudflare Access nahrazuje VPN

Vzestup práce na dálku zastihl mnoho společností nepřipravených. Mnohé organizace jenom zakoupily dostatek VPN licencí a navýšili kapacitu apliance pro podporu části svých týmů. Nárůst práce na dálku vystavuje obojí značným. nárokům.

Cloudflare Access Vám pomáhá redukovat zatížení Vaší VPN pomocí moderního přístupu k autentizaci pro interně spravované aplikace. Access zabezpečuje webové aplikace, SSH spojení, připojení ke vzdálené ploše a další protokoly pomocí globální sítě Cloudflare, kde je každý požadavek na zdroj ověřen podle identity.

Když jsou firemní nástroje chráněny pomocí Cloudflare Access, jsou vnímány jako aplikace SaaS, kde se zaměstnanci do nich mohou přihlašovat pomocí jednoduchého a konzistentního postupu.

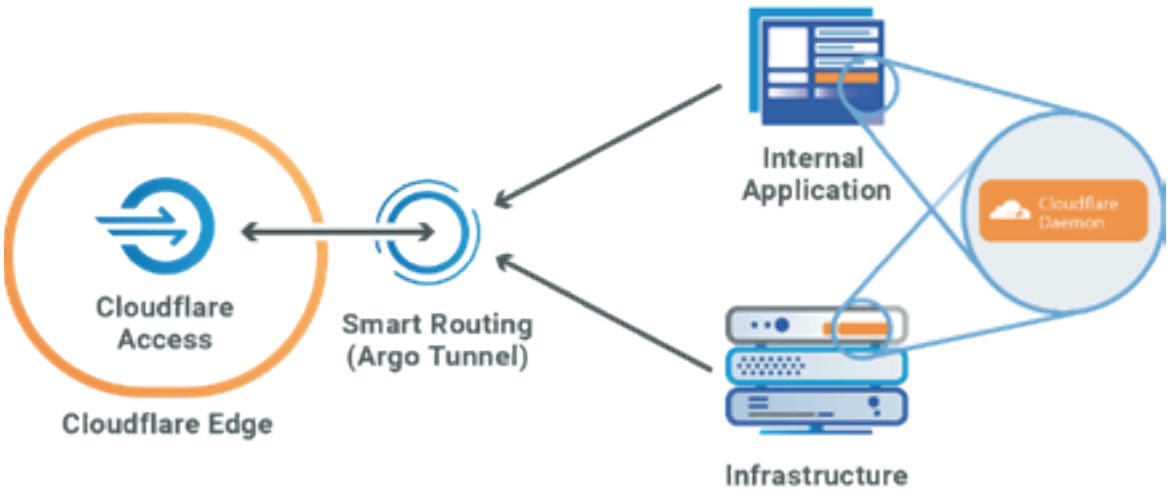
Zde je popsáno, jak Cloudflare Access nahrazuje VPN pomocí sítě Cloudflare.

1. Cloudflare Access bezpečně připojuje interní nástroje k Internetu

Týmy se připojují ke svým zdrojům pomocí Cloudflare Access pomocí bezpečného odchozího spojení, Argo Tunel, které běží ve Vaší infrastruktuře pro účely připojení aplikací a strojů do Cloudflare. Argo Tunel vystavuje webové servery bezpečně do Internetu bez otevírání portů firewallu a konfigurování ACL seznamů.

Tento tunel navazuje pouze odchozí spojení do sítě Cloudflare.

Bez ohledu na to, zda aplikace běží lokálně nebo hostované u poskytovatele cloudových služeb, Argo Tunel dovede Vaši infrastrukturu připojit do Cloudflare.

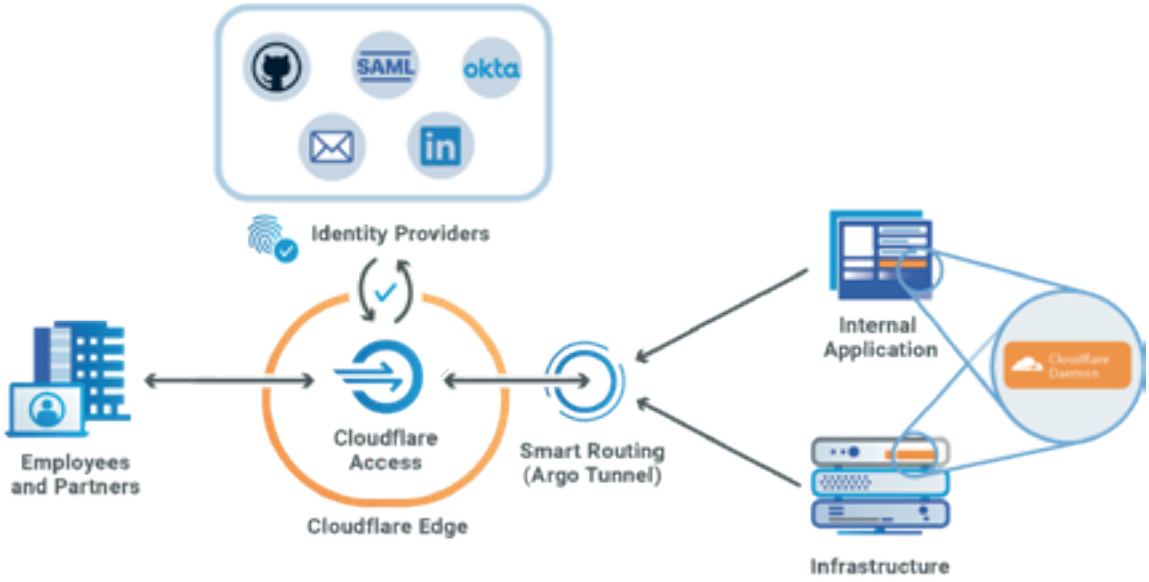


2. Požadavky na chráněné prostředky jsou směrovány přes hraniční zařízení Cloudflare

Argo Tunel používá technologii Argo Smart Routing pro směrování provozu nejrychlejší cestou v rámci sítě Cloudflare mezi uživatelem a datovým centrem nejbližším zdroji provozu.

Datová centra Cloudflare jsou dostupná do 100 milisekund pro 99 % obyvatel připojených k internetu v rozvinutém světě.

Když požadavek na Vaše prostředky dorazí na hraniční zařízení Cloudflare, Access zafunguje jako nárazník stojící před tímto zdrojem, který určuje, který požadavek smí vstoupit.

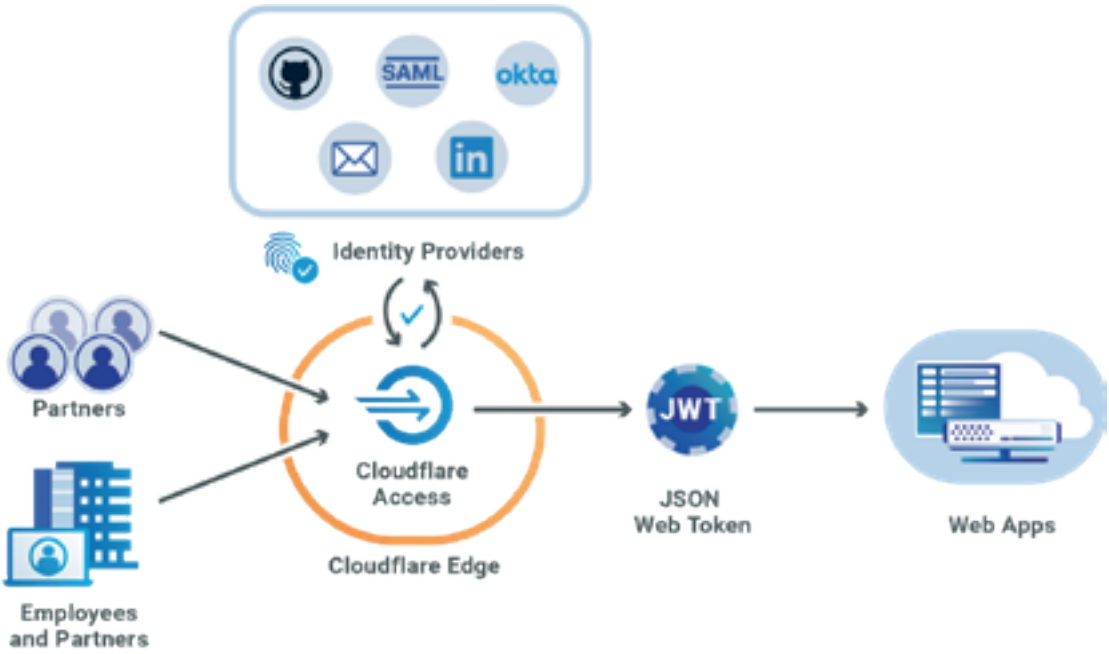


3. Na hraničním zařízení Cloudflare používá Access zásady nastavené u Vašeho poskytovatele identity (IDP) pro určení, které požadavky povolit a které zablokovat

Cloudflare Access se integruje s poskytovatelem identity Vaší organizace za účelem určení identity uživatele. Když se uživatel připojí k aplikaci, která je chráněná pomocí Cloudflare Access, bude vyzván k přihlášení u nastaveného poskytovatele identity.

Access podporuje poskytovatele spravované Vaším týmem, jako např. Okta©, G Suite© a AzureAD©, a k tomu navíc veřejně dostupné poskytovatele jako LinkedIn© a GitHub©.

Access lze využít pro současnou podporu několika poskytovatelů identity, a to včetně tenantů téhož typu.



Co můžete chránit pomocí Access

SSH Připojení

Protokol Secure Shell (SSH) umožňuje uživatelům připojování k infrastruktuře za účelem provádění činností jako např. vzdálené spouštění příkazů. Cloudflare Access dovede zabezpečit připojení přes Secure Shell (SSH). Když se uživatel pokusí přistupovat k prostředkům z příkazové řádky, Access spustí okno prohlížeče a požádá ho o přihlášení u jeho poskytovatele identity.

Webové aplikace

Access můžete využívat k ochraně interně spravovaných aplikací jako Jira, WordPress, GitLab a SAP, takže uživatelé se uživatelé mohou přihlásit za účelem přístupu do nich bez VPN. Cloudflare Access vyhodnocuje požadavky na Vaši aplikaci a určuje, zda jsou návštěvníci autorizovaní na základě zásad, které si definujete.

Připojení ke vzdálené ploše

Remote Desktop Protokol (RDP) uživatelům umožňuje připojení k ploše z jiného počítače. Cloudflare Access umožňuje koncovým uživatelům provést autentizaci u svého poskytovatele jednotného přihlášení (single sign-on - SSO) a připojit se ke sdíleným souborům přes RDP, aniž by použili VPN.

Další protokoly

Access lze využít k doplnění autentizace k protokolu Secure Messaging Block (SMB) pro přístup k úložištím souborů nebo k aplikacím, které používají libovolné TCP.

Podporovaní poskytovatelé identity

Cloudflare Access se pro určení identity uživatele integruje s poskytovatelem identity Vaší organizace. Když se uživatelé připojí k aplikací chráněné pomocí Cloudflare Access, budou požádáni o přihlášení pomocí nakonfigurovaného poskytovatele identity. Organizace mohou používat více poskytovatelů identity najednou bez jakýchkoli omezení.

- 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©