Zero Trust-Netzwerkzugriff mit Private Routing

Laterale Bewegungen verhindern und die Abhängigkeit von VPNs reduzieren

Wenn netzwerkbasierten Kontrollmechanismen (wie VPNs und IP-Standortbeschränkung) für den Anwendungszugriff Vertrauen geschenkt wird, kann das die Angriffsfläche erhöhen, die Sichtbarkeit einschränken und für Frustration bei den Endnutzern sorgen. Der Zero Trust-Netzwerkzugriff von Cloudflare ist mit Identitätsanbietern und Endpunktschutz-Plattformen kompatibel. Es werden Zero Trust-Regeln mit Verweigerung als Grundeinstellung durchgesetzt, die den Zugriff auf Firmenanwendungen, interne IP-Bereiche und Hostnamen beschränken. Die Lösung stützt sich auf das ausgedehnte und leistungsstarke Anycast-Netzwerk von Cloudflare und erlaubt damit schnellere Nutzerverbindungen als ein VPN.

Cloudflare hat den Zero Trust-Netzwerkzugriff intern eingeführt. Das sind die Ergebnisse:

- Reduzierung der Angriffsfläche um 91 %[1]
- zweifache Kosteneinsparung durch verringerten IT-Aufwand
- ca. 80 % Zeiteinsparung bei der Bearbeitung von Tickets mit VPN-Bezug
- Rückgang des Ticketumfangs um ca. 70 %
- Produktivitätszugewinn von mehr als 300 Jahresstunden beim Onboarding neuer Mitarbeiter

Was kann Access?

Jede Anwendung schützen

Cloudflare ist nicht auf bestimmte Identitätsanbieter oder Anwendungen festgelegt. Somit kann jede Anwendung – ob als SaaS, cloudbasiert oder lokal bereitgestellt – mit dem gewünschten Identitätsanbieter geschützt werden.

Nutzer mit oder ohne Client flexibel verbinden

Webanwendungs- und SSH-Verbindungen lassen sich auch ohne Client-Software oder eine Konfiguration auf Endnutzerseite erleichtern. Für Anwendungen außerhalb des Webs, RDP-Verbindungen und Private Routing genügt ein einziger Client, der alle Anwendungsfälle des Internet- und Anwendungszugriffs abdeckt.

Mehrere Identitätsanbieter bündeln

Um Migrationen, Übernahmen und den Zugriff von Drittnutzern sicherer zu machen, sind alle von einem Unternehmen eingesetzten Identitätsanbieter (unter anderem Okta und Azure AD) integrierbar. Für den temporären Zugriff kann die Verwendung von Einmal-PINs freigeschaltet werden und es besteht die Möglichkeit, soziale Netzwerke wie LinkedIn und GitHub zur Bestätigung der Identität zu nutzen.

Laterale Bewegung zwischen Firmenressourcen beschränken

IP-Firewall und Zero Trust-Regeln ermöglichen hochwirksame und einheitliche Authentifizierungsmethoden selbst bei älteren Anwendungen.

Geräteabhängige Zugriffsrichtlinien durchsetzen

Bevor Zugriff gewährt wird, sollte das Sicherheitsniveau des Geräts geprüft werden, also etwa das Vorhandensein eines Gateway-Clients, die Seriennummer und das mTLS-Zertifikat. So lässt sich gewährleisten, dass nur sichere und bekannte Geräte eine Verbindung zu den Ressourcen herstellen können. Möglich ist dies etwa durch die Integration der Gerätezustandsprüfung von EPP (Endpoint Protection Platform) -Anbietern wie Crowdstrike, Carbon Black, Sentinel One und Tanium.

Nutzeraktivität für jede beliebige Anwendung protokollieren

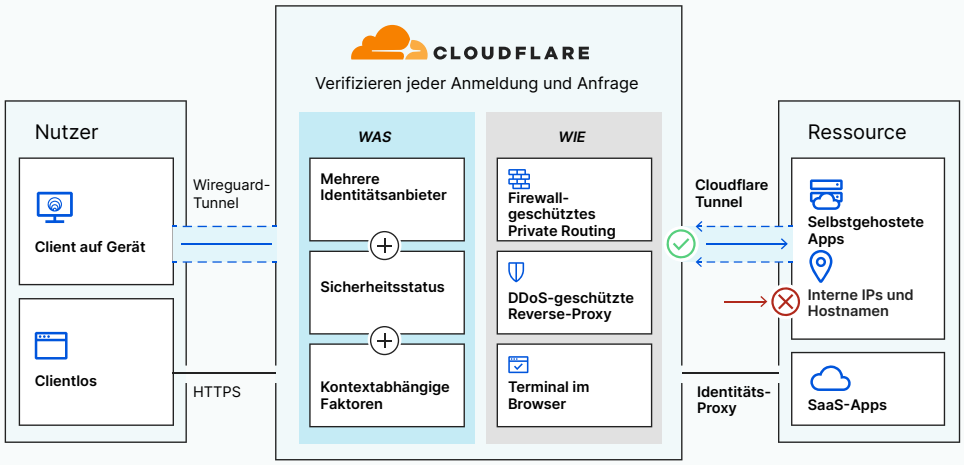
Innerhalb von geschützten Anwendungen kann jede einzelne Anfrage protokolliert werden – nicht nur An- und Abmeldungen. Aktivitätsprotokolle können in Cloudflare zusammengefasst oder an einen SIEM-Anbieter übermittelt werden.

[1]Bei Kombination von Zero Trust-Netzwerkzugriff und Surfen im Internet

Cloudflare macht den Unterschied

- **Unschlagbare Performance**: Anfragen werden mittels optimiertem und erkenntnisgestütztem Routing über das Anycast-Netzwerk von Cloudflare schneller weitergeleitet. Der Zugriff auf Web-Anwendungen erfolgt im Durchschnitt 30 % schneller und die Paketumlaufzeit bei TCP-Verbindungen verringert sich um 17 %. Unsere Erkenntnisse basieren auf der Analyse von Netzwerkdaten für 25 Millionen HTTP-Anfragen pro Sekunde und 39.000 neuen TCP-Verbindungen pro Sekunde.
- **Einfachere Verwaltung**: Die Steuerung von Funktionen wie dem Zero Trust-Netzwerkzugriff, Secure Web Gateway oder der Remote-Browserisolierung erfolgt über eine einzige Schnittstelle. Administratoren verfügen so über ein einheitliches und gewachsenes Verwaltungssystem, anstatt mühevoll mit Lösungen von verschiedenen externen Anbietern hantieren zu müssen.
- **Überprüfung in einem Durchgang**: Traffic wird weltweit schnell und einheitlich verifiziert, gefiltert, isoliert und überprüft. Jeder Cloudflare-Dienst wird in jedem Rechenzentrum an unseren mehr als 250 Standorten weltweit bereitgestellt.

So funktioniert's



Die Nutzer stellen die Verbindung zu den Firmenressourcen nicht über ein VPN, sondern über einen Client oder einen Webbrowser her. Während des Routings und der Beschleunigung von Anfragen durch die Cloudflare Edge werden diese anhand von Zero Trust-Regeln bewertet, wobei Informationen von Ihren Identitätsanbietern und Geräten ebenso wie weiterer Kontext berücksichtigt werden. Früher benötigten RDP-Software, SMB-Dateibetrachter und andere Thick-Client-Programme ein VPN für private Netzwerkverbindungen. Doch heute können Teams beliebigen TCP-oder UDP-Traffic privat durch das Cloudflare-Netzwerk leiten. Dort wird er in einem einzigen Durchgang beschleunigt, verifiziert und gefiltert, was höhere Performance und Sicherheit ermöglicht.

„Dank Cloudflare Access mussten wir kein eigenes Identitäts- und Zugriffsmanagementsystem entwickeln. Für die durch Access geschützten Anwendungen entfiel die Integration von Funktionen zur Nutzerberechtigung. Wir entschieden uns, voll und ganz auf die Lösung zu setzen. Jedes Mitglied unseres Unternehmens hat ein Konto."

Jim Tyrell
Head of Infrastructure bei Canva

„Hier bei Delivery Hero sind wir immer bestrebt, unseren Kunden ein tolles Erlebnis zu bieten. Cloudflare Access hilft uns dabei, dasselbe für unsere internen Teams zu erreichen: Die Lösung bietet ihnen eine sichere Arbeitsumgebung und macht den Einsatz eines VPNs für den Zugriff auf alle unsere Anwendungen weltweit überflüssig."

William Carminato
Senior Director, Engineering bei Delivery Hero

IAM (Identity and Access Management)-Integrationen

Active Directory · okta · Google Workspace · PingIdentity · CITRIX · Centrify · onelogin · SAML, OIDC

EEP (Endpoint Protection Platform)-Integrationen

CROWDSTRIKE · vmware Carbon Black · SentinelOne · TANIUM

Wichtigste Funktionen

Einheitliche Richtlinien	
Benutzerdefinierte Richtlinien für Anwendungs-, Privatnetzwerk- und Internetzugang	**Unbegrenzt**
Authentifizierung durch Identitätsanbieter oder Konten bei sozialen Netzwerken	✓
Ermittlung des Gerätestatus durch Integration in Drittlösungen und Cloudflare	✓
Massenimport im CSV-Format von Seriennummernlisten von Firmengeräten	✓

Höhere Transparenz	
Speicherung von Aktivitätsprotokollen	**6 Monate**
Identitätsbasierte Detailansichten für Länder und Geräte	✓
Übertragung von Protokollen an Cloud-Speicher oder SIEMs	✓

Sichere Verbindungen	
Clientbasierte verschlüsselte Internetverbindungen (WARP-Client)	**Win, Mac, iOS, Android**
Sicherer clientloser Zugriff auf selbst gehostete Applikationen und SaaS-Anwendungen	✓
Private Verbindungen für selbstgehostete Anwendungen, interne IPs und Hostnamen (Cloudflare Tunnel)	✓

Einfache Interoperabilität	
Endpunkt- und Mobilitätsmanagements-Integrationen	✓
Split Tunneling für lokale Verbindungen oder VPN-Verbindungen	✓
Eigenständige Client-Registrierung für nicht verwaltete Geräte	✓
Anpassbarer App-Launcher	✓
Parallele Unterstützung verschiedener Identitätsanbieter zur Authentifizierung	✓
Allgemeine und kundenspezifische Konnektoren zur Unterstützung von SAML und OIDC	✓
Tokenbasierte Authentifizierung für automatisierte Dienste	✓
Zertifikatsbasierte Authentifizierung für IoT und andere mTLS-Anwendungsfälle	✓

Keine Abstriche bei der Performance	
Durch SLA garantierte Verfügbarkeit	**100 %**
Eines der schnellsten Netzwerke (unter 50 ms von über 250 PoPs entfernt)	✓
Schnellster, datenschutzfreundlicher DNS-Resolver (7–31 ms über mehr als 250 PoPs)	✓
Blitzschnelle Richtlinienaktualisierungen (unter 500 ms an mehr als 250 PoPs)	✓
Blitzschneller Remote-Browser (kein Pixel-Pushing; wird auf unserem Netzwerk betrieben, nicht in einer Dritt-Cloud)	**Zusätzlich buchbar**

Sie würden gern mehr erfahren?

Unter www.cloudflare.com/de-de/products/zero-trust/access/ können Sie ein Konto eröffnen, das für bis zu 50 Nutzer kostenlos ist.