CLOUDFLARE

KURZDARSTELLUNG

Arbeitsplätze an unterschiedlichen Orten absichern

Einheitlicher, bedarfsgerechter und ortsunabhängiger Schutz über eine einzige Steuerungsebene

Verlagerung der Sicherheit in die Cloud

Mit Cloudflare die Komplexität und das Risiko für Bürostandorte reduzieren

Nachdem sich mobiles Arbeiten etabliert hat, überdenken viele Unternehmen nun die IT-Sicherheit ihrer Bürostandorte – unabhängig davon, ob sie auf Appliances in Rechenzentren zurückgreifen oder einen direkten, ungesicherten Internetzugang erlauben.

Ihr Hauptaugenmerk liegt jetzt darauf, ihren Anwendern innerhalb und außerhalb des Firmennetzwerks durchgängigen Schutz und ein stimmiges Nutzererlebnis zu bieten. Meistens müssen sie dafür isoliert arbeitende Werkzeuge wie VPN, Web-Proxys und Firewalls durch eine einzige, über die Cloud bereitgestellte Sicherheitsplattform ersetzen.

Bei der Modernisierung des Schutzes von Bürostandorten bieten sich aus Sicht von Cloudflare zwei Anwendungsfälle besonders an.

Empfohlener Anwendungsfall:

Absicherung des Anwendungszugriffs mit Zero Trust als VPN-Ersatz

Um der lateralen Ausbreitung im gesamten Firmennetzwerk einen Riegel vorzuschieben, können feinjustierte identitätsbezogene Richtlinien für jede einzelne Anwendung durchgesetzt werden.

- **Schritt 1:** Integration Ihrer Identitätsanbieter
- **Schritt 2:** Schutz jeder beliebigen Webanwendung über einen Browser
- **Schritt 3:** Absicherung von SSH-, VNC- und RDP-Umgebungen über einen Browser

> **Zweigstellen- und Remote-Zugriff erfolgen über eine einzige Implementierung, um einheitliche Richtlinien zu gewährleisten und die Anzahl der erforderlichen Lösungsanbieter zu minimieren. ZTNA kann als Ergänzung oder Ersatz für das traditionelle VPN eingesetzt werden, um möglichst wenig in veraltete Technologie zu investieren.[1]**
>
> Gartner

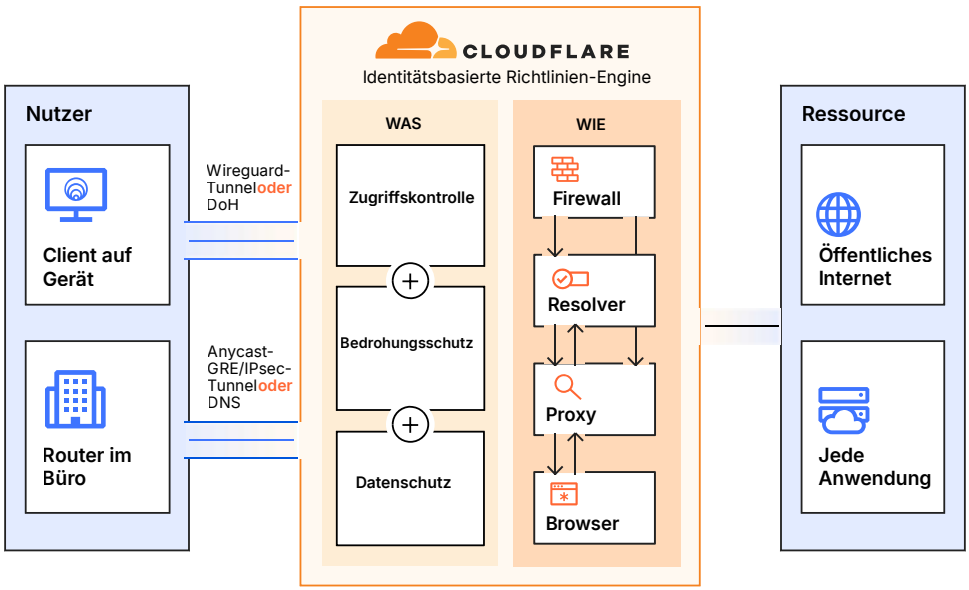
Empfohlener Anwendungsfall:

Filterung des Internetzugangs für einheitliches Sicherheitsniveau mit kurzer Amortisationszeit

Nutzer in Büros werden zunächst mit DNS-Filterung und später mit umfassenderen Überprüfungen an allen Standorten geschützt. Der Traffic wird nicht mehr über lokale Sicherheits-Appliances in Rechenzentren geleitet.

- **Schritt 1:** Weiterleitung des DNS-Traffic zum globalen Cloudflare-Netzwerk
- **Schritt 2:** Einrichtung einer standortbasierten DNS-Filterung zum Schutz vor Ransomware, Phishing und anderen Bedrohungen aus dem Internet
- **Schritt 3:** Kontrolle der Datenströme durch Durchsetzung von DNS-, HTTP-, Netzwerk- und Browserisolierungs-Regeln mit unbegrenzter TLS 1.3-Prüfung

So funktioniert's



Bereitstellung ohne Client zur Überprüfung des Zugriffs und zum Filtern der DNS-Anfragen von Bürostandorten.

Bereitstellung mit dem Geräte-Client von Cloudflare für besseren Überblick und größere Kontrolle über alle Nutzer und Geräte.

Abbildung 1: Mit Cloudflare Zero Trust wird Traffic von Bürostandorten in einem einzigen Durchgang verifiziert, gefiltert, isoliert und überprüft.

Flexibler Einstieg

Sie können zunächst Cloudflare für die DNS-Auflösung über Netzwerk-Router verwenden. Zu gegebener Zeit können Sie dann L3-Traffic über Ihre GRE- oder IPsec-Tunnel an unser globales Netzwerk senden – oder Ihre gewohnte SD-WAN-Routing-Methode nutzen.

Alternativ kann der Cloudflare-Client auf verwalteten Geräten für die DNS- und HTTP-Filterung und -Überprüfung eingesetzt werden.

Schnelle, global skalierbare Richtliniendurchsetzung

Alle Funktionen zur Gewährleistung von Sicherheit, Performance und Zuverlässigkeit können auf jedem Server in jedem Rechenzentrum an unseren gut 275 Standorten in über 100 Ländern ausgeführt werden.

Aufgrund der Größe unseres Netzwerks können die Schutzmaßnahmen immer schnell mit Single Pass-Überprüfung in der Nähe von Büros und Nutzern durchgesetzt werden, wo auch immer sich diese befinden.

Diese Anwendungsfälle können in den folgenden sechs bis zwölf Monaten in Erwägung gezogen werden

Zurückgewinnung der Kontrolle über SaaS-Anwendungen

Sie können die Risiken der von Mitarbeitenden im Büro und im Homeoffice genutzten Schatten-IT ermitteln und neutralisieren.

Mit CASB-Richtlinien, die sich über ein einziges Cloudflare-Dashboard aktivieren lassen, werden Datenlecks und Compliance-Verstöße verhindert. Wie das funktioniert, erfahren Sie hier.

Auslagerung von MPLS-Traffic

Teure, veraltete und langsame private MPLS-Verbindungen werden ersetzt.

Durch die Steuerung des Traffics von Zweigstellen, Rechenzentren und Public Cloud-Diensten über das globale Netzwerk von Cloudflare lässt sich bestehende WAN-Architektur vereinfachen. Wie das geht, erfahren Sie hier.

1. Gartner Hype Cycle for Network Security, 2021 | GARTNER und HYPE CYCLE sind eingetragene Handels- und Dienstleistungsmarken von Gartner, Inc. und/oder den Tochtergesellschaften des Unternehmens in den USA und anderen Ländern, die im Folgenden mit Genehmigung verwendet werden. Alle Rechte vorbehalten. Alle Rechte vorbehalten.

REV:BDES-6043.2024AUG06