GESTALTUNGSLEITFADEN

CLOUDFLARE

Cloudflare One – unsere SASE-Plattform

+49 89 2555 2276 | enterprise@cloudflare.com | www.cloudflare.com/de-de/

INHALTSVERZEICHNIS

Zielsetzung dieses Leitfadens **3**

Vorher und nachher: Die transformative Kraft von Cloudflare **4**

- Sichere, schnelle, zuverlässige und datenschutzfreundliche Verbindungen für alle Nutzer 5
- Vereinfachte Vernetzung und Sicherheit für öffentliche Ressourcen 6–7
- Vereinfachte Vernetzung und Sicherheit für nicht öffentliche Ressourcen 8–9
- Vereinfachte Vernetzung und Sicherheit für alle Ressourcen 10
- Eine einzige Plattform für einfachste Vernetzung und Sicherheit 11

Anwendungsfall Nr. 1: Sicherer Zugriff auf Webanwendungen **12**

- Herkömmliche Struktur – Einstieg 13
- Herkömmliche Struktur – Sicherheitslücken 14
- Herkömmliche Struktur – erforderliche Sicherheitserweiterungen 15
- Struktur von Cloudflare One 16
- Diagramme im Vergleich 17
- Tabellen im Vergleich 18

Anwendungsfall Nr. 2: DNS-Filterung **19**

- Herkömmliche Struktur – Einstieg 20
- Herkömmliche Struktur – betriebliche Schwächen 21
- Herkömmliche Struktur – erforderliche Netzwerkanpassungen 22
- Struktur von Cloudflare One 23
- Diagramme im Vergleich 24
- Tabellen im Vergleich 25

Hinweis: Weitere Anwendungsfälle werden zu gegebener Zeit hinzugefügt.

Zielsetzung dieses Leitfadensv

Dieser Gestaltungsleitfaden richtet sich an technisch orientierte Anwender und bietet anschauliche Beispiele dazu, wie Unternehmen ihre Netzwerk- und Sicherheitsarchitektur mit unserer SASE-Plattform Cloudflare One vereinfachen und verstärken können. Cloudflare One verbindet Netzwerkanbindungsservices mit Zero Trust-Sicherheitsdiensten, die alle über das globale Netzwerk von Cloudflare bereitgestellt werden.

Im ersten Abschnitt dieses Gestaltungsleitfadens liegt der Schwerpunkt auf einer ganzheitlichen Neugestaltung und Modernisierung. Hier werden die verschiedenen möglichen Konnektivitäts- und Sicherheitskomponenten präsentiert, die auf den ein- und ausgehenden Netzwerk-Traffic sowie auf Anwendungen ausgelegt sind, die Cloudflare vor- und nachgeschaltet sind. Der herkömmliche Ansatz einer zentralisierten Perimetersicherheit, der sich auf Lösungen verschiedener Anbieter stützt, wird dem Cloudflare-Modell mit einem globalen Netzwerk gegenübergestellt, das auf eine einzige, modulare Plattformarchitektur zurückgreift.

In den folgenden Abschnitten werden gängige Anwendungsfälle erörtert. Zunächst wird untersucht, wie das jeweilige Problem normalerweise bei der herkömmlichen Herangehensweise gelöst wird. Anschließend schauen wir uns an, wie Cloudflare One darauf eine effizientere Antwort mit einer besseren Nutzererfahrung findet.

Es wurden zwei Anwendungsfälle ausgewählt, die bei den Kunden besonders verbreitet sind, diese spiegeln aber in keinster Weise das gesamte Spektrum der Funktionen von Cloudflare One wider.

- Sicherer Zugang für nicht öffentliche und öffentliche Anwendungen
- DNS-Filterung für lokal und remote arbeitende Beschäftigte

Wir werden diesem Leitfaden nach und nach weitere Anwendungsfälle hinzufügen. Unter anderem werden wir uns mit dem sicheren Zugang zu nicht öffentlichen Netzwerken und dem erweiterten Schutz vor Bedrohungen und von Daten befassen.

Vorher und nachher: Die transformative Kraft von Cloudflare

Sichere, schnelle, zuverlässige und datenschutzfreundliche Verbindungen für alle Nutzer

Beliebiger Nutzer

Unternehmen müssen zwei Nutzergruppen sichere, schnelle, zuverlässige und datenschutzfreundliche Verbindungsmöglichkeiten bieten.

Verwaltete Nutzer sind Mitarbeitende, die mit einem Firmen- oder Privatgerät von zu Hause, vom Büro oder von einem anderen Standort aus auf eine Ressource zugreifen.

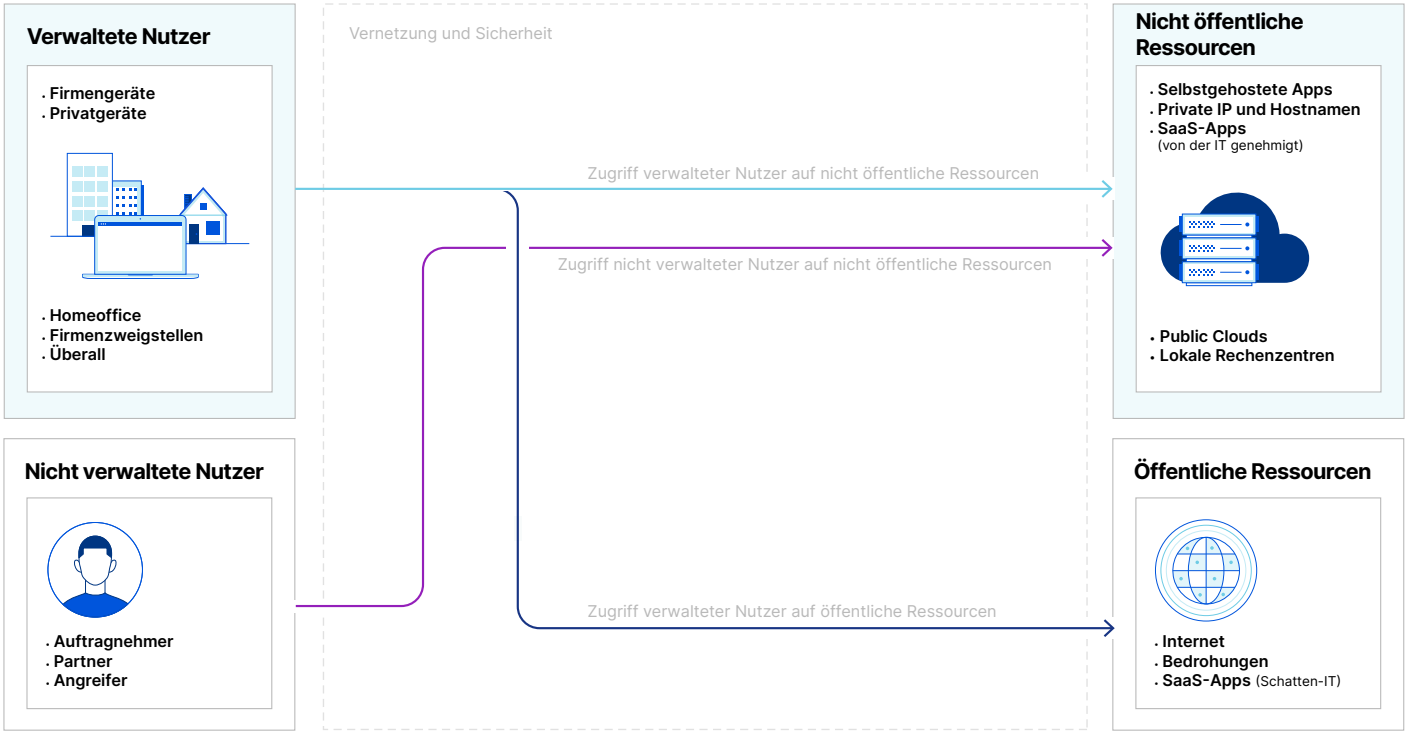
Nicht verwaltete Nutzer sind unter anderem Auftragnehmer oder Partner, die berechtigt sind, auf eine Ressource zuzugreifen – aber auch Angreifer, die nicht über eine solche Berechtigung verfügen.

Beliebige Ressource

Unternehmen müssen für zwei Ressourcengruppen eine Zugriffsrechteverwaltung ermöglichen, bei der Daten und Systeme vor Bedrohungen geschützt sind.

Zu **nicht öffentlichen Ressourcen** zählen selbst gehostete Applikationen und private IPs oder Hostnamen innerhalb von Public Clouds und lokalen Rechenzentren, sowie SaaS-Anwendungen, die von der IT-Abteilung genehmigt wurden.

Unter **öffentlichen Ressourcen** im Internet sind unter anderem nicht genehmigte SaaS-Applikationen sowie Bedrohungen zu verstehen.



Vernetzungs- und Sicherheitslage vor und nach Einführung von Cloudflare

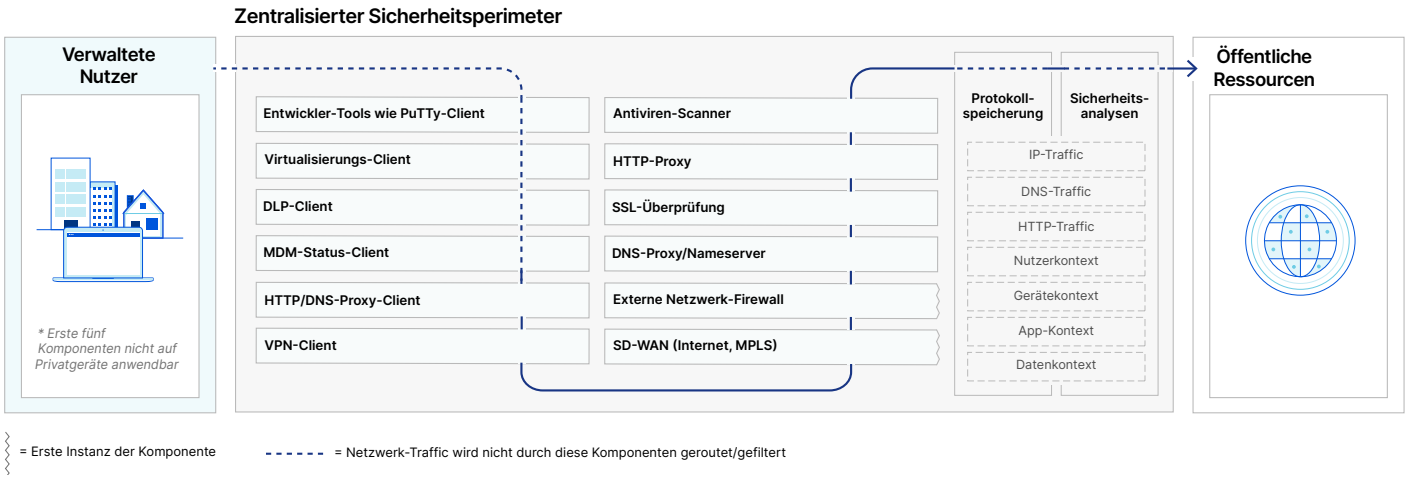
Auf den folgenden Seiten zeigt eine Reihe von Vorher-Nachher-Schaubildern Schritt für Schritt die Vernetzungs- und Sicherheitskomponenten, die Unternehmen benötigen, um verwalteten Nutzern den Zugriff auf öffentliche Ressourcen sowie verwalteten und nicht verwalteten Usern den Zugriff auf nicht öffentliche Ressourcen zu erlauben.

Das erste „Vorher"-Diagramm bildet die Endpunktgeräte und Netzwerk-Appliances ab, die in in einem zentralisierten Perimetersicherheitsmodell zum Einsatz kommen.

Die zugehörige „Nachher"-Grafik zeigt, wie vergleichbare Cloud-Dienste über das globale Netzwerk von Cloudflare bereitgestellt werden.

1a. Vereinfachte Vernetzung und Sicherheit für öffentliche Ressourcen

Vor Einführung von Cloudflare



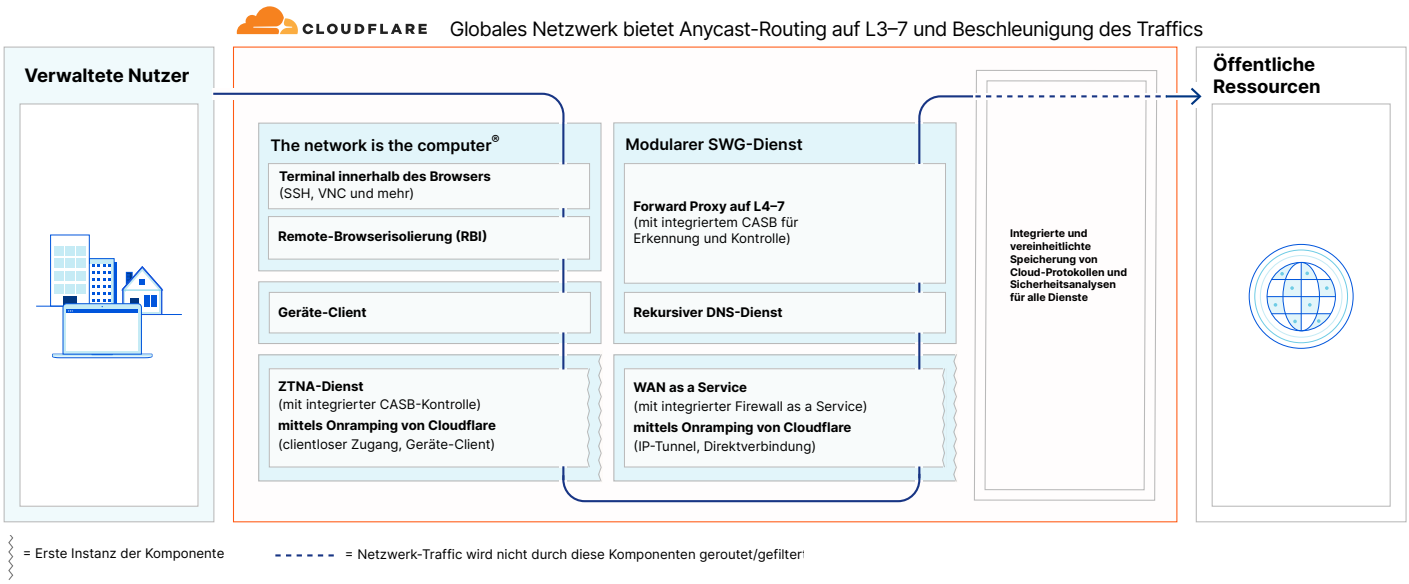
Verwaltete Nutzer (bei Zugriff auf öffentliche und nicht öffentliche Ressourcen)

IT-Abteilungen mussten für Vernetzung und Sicherheit die Verwaltung vieler Clients gewährleisten. Schlimmer noch: Sie konnten sich nicht um Privatgeräte kümmern. Entwickler-Tools und VPN für nicht öffentlichen Zugang. HTTP/DNS-Proxy für öffentlichen Zugang. Virtualisierung, Vorbeugung von Datenverlust und Verwaltung von mobilen Geräten für einen besseren Schutz.

Öffentliche Ressourcen

Beschäftigte in der IT-Sicherheit nutzen VPN-Clients oder SD-WAN, um Traffic von remote oder im Büro arbeitenden Nutzern durch die Netzwerk-Firewall, den DNS-Proxy, die SSL-Überprüfung, den HTTP-Proxy und den Antiviren-Scanner zu leiten und auf diese Weise öffentliche Ressourcen vor dem Zugriff Unbefugter zu schützen.

Nach Einführung von Cloudflare



Verwaltete Nutzer (bei Zugriff auf öffentliche und nicht öffentliche Ressourcen)

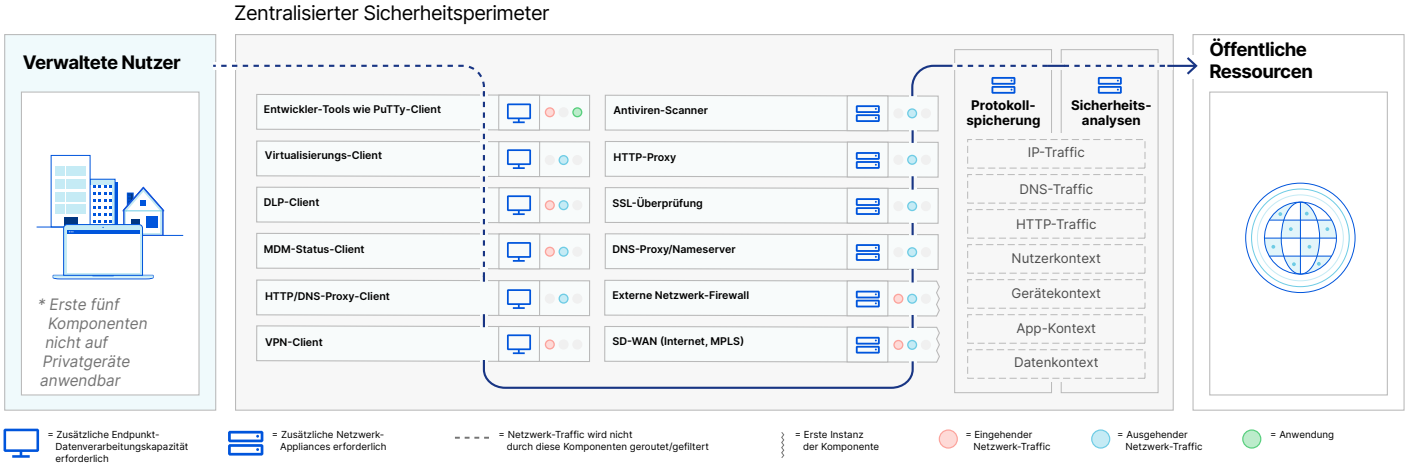
Das Netzwerk übernimmt viele Aufgaben des Computers oder ein Client bündelt zahlreiche Aufgaben.

Öffentliche Ressourcen

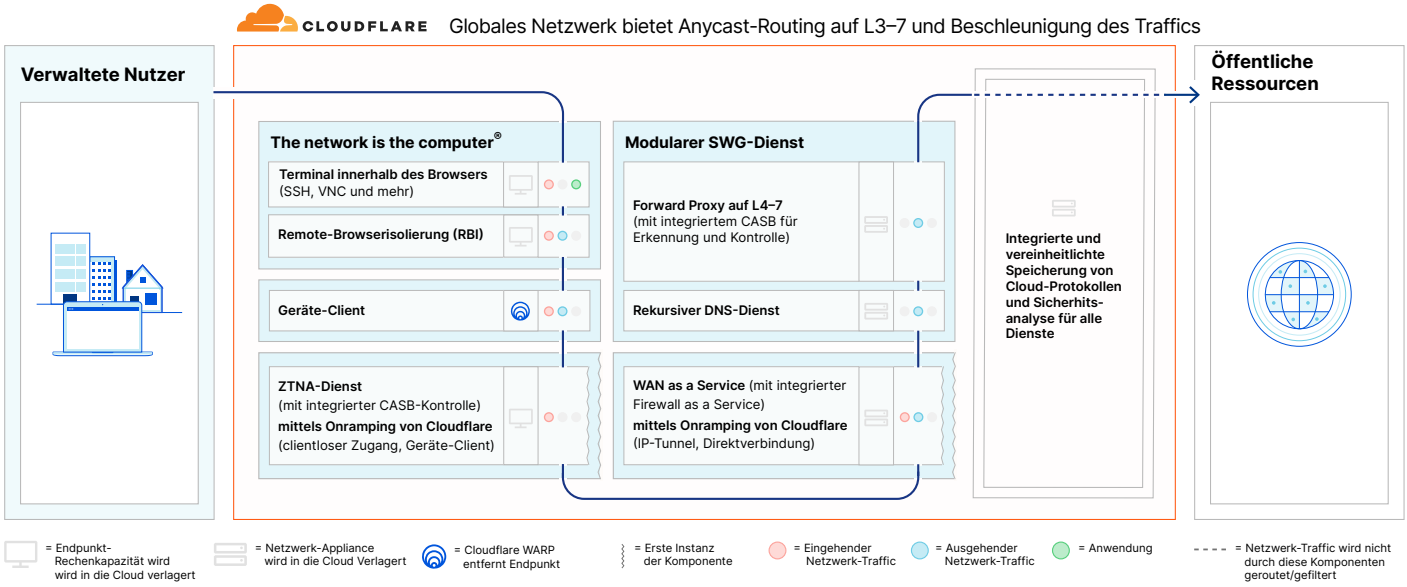
Unser modularer Secure Web Gateway (SWG)-Service überprüft Traffic in einem einzigen Arbeitsdurchgang vor oder nach Einführung unseres WAN as a Service und/oder unserer Zero Trust-Netzwerkszugangslösung mit integrierter Sicherheit.

1b. Vereinfachte Vernetzung und Sicherheit für öffentliche Ressourcen

Vor Einführung von Cloudflare



Nach Einführung von Cloudflare



Cloudnative Dienste

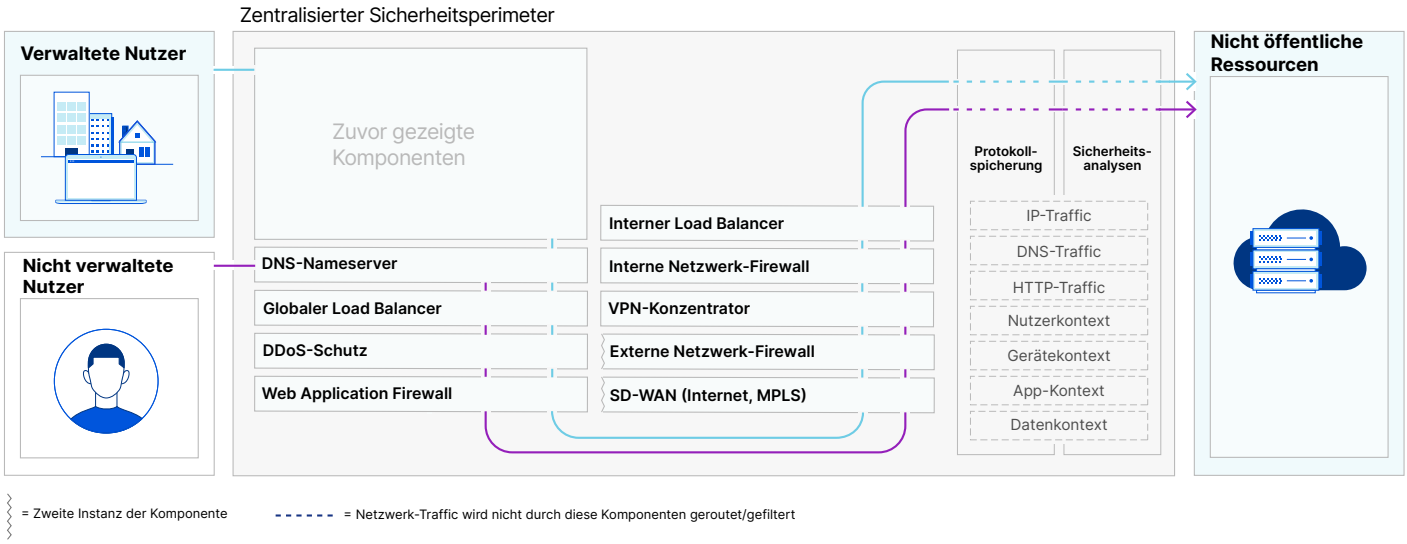
Die Anforderungen an Endgeräte und Netzwerk-Appliances sind niedriger.

Modulare Architektur

Zur Gewährleistung lückenloser Sicherheit und Performance werden der Protokollstapel für ein- und ausgehenden Traffic und der Anwendungsstapel zusammengeführt.

2a. Vereinfachte Vernetzung und Sicherheit für nicht öffentliche Ressourcen

Vor Einführung von Cloudflare



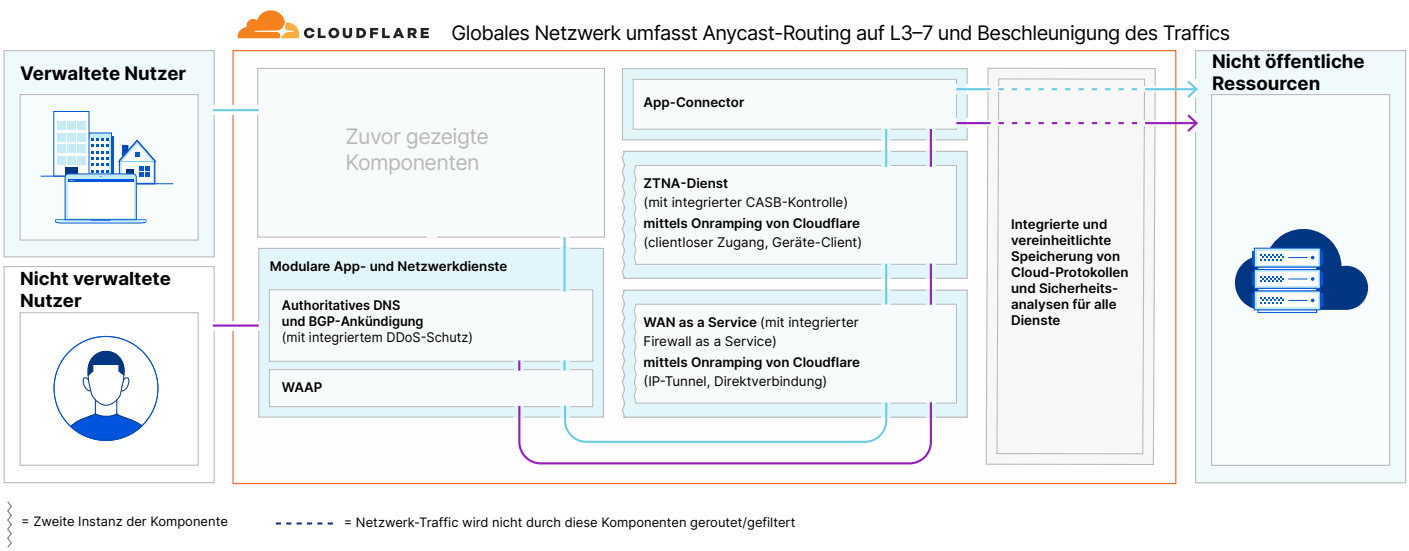
Nicht verwaltete Nutzer

Netzwerkteams mussten die öffentliche Bekanntgabe der Verfügbarkeit nicht öffentlicher Ressourcen gegenüber Auftragnehmern und Partnern verwalten und den Schutz vor DDoS-Angriffen und der Ausnutzung von Sicherheitslücken gewährleisten.

Nicht öffentliche Ressourcen (Zugriff von verwalteten und nicht verwalteten Nutzern

Beschäftigte in der IT-Sicherheit nutzten VPN-Clients oder SD-WAN, um Traffic von Nutzern durch die Netzwerk-Firewall, VPN-Konzentratoren und Load Balancer zu leiten und auf diese Weise nicht öffentliche Ressourcen vor dem Zugriff Unbefugter zu schützen.

Nach Einführung von Cloudflare



Nicht verwaltete Nutzer

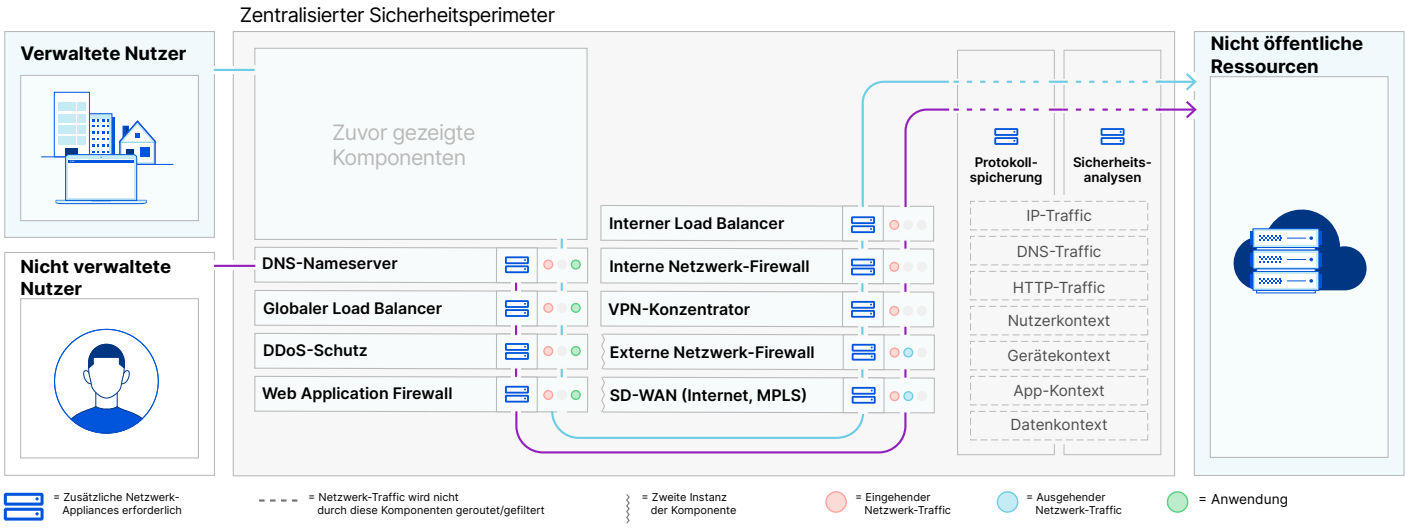
Unsere modularen Anwendungs- und Netzwerkdienste nehmen ihnen diese Last entweder vor oder nach Einführung unserer Zero Trust-Netzwerkszugangslösung oder unseres WAN as a Service mit integrierter Sicherheit ab.

Nicht öffentliche Ressourcen (Zugriff von verwalteten und nicht verwalteten Nutzern

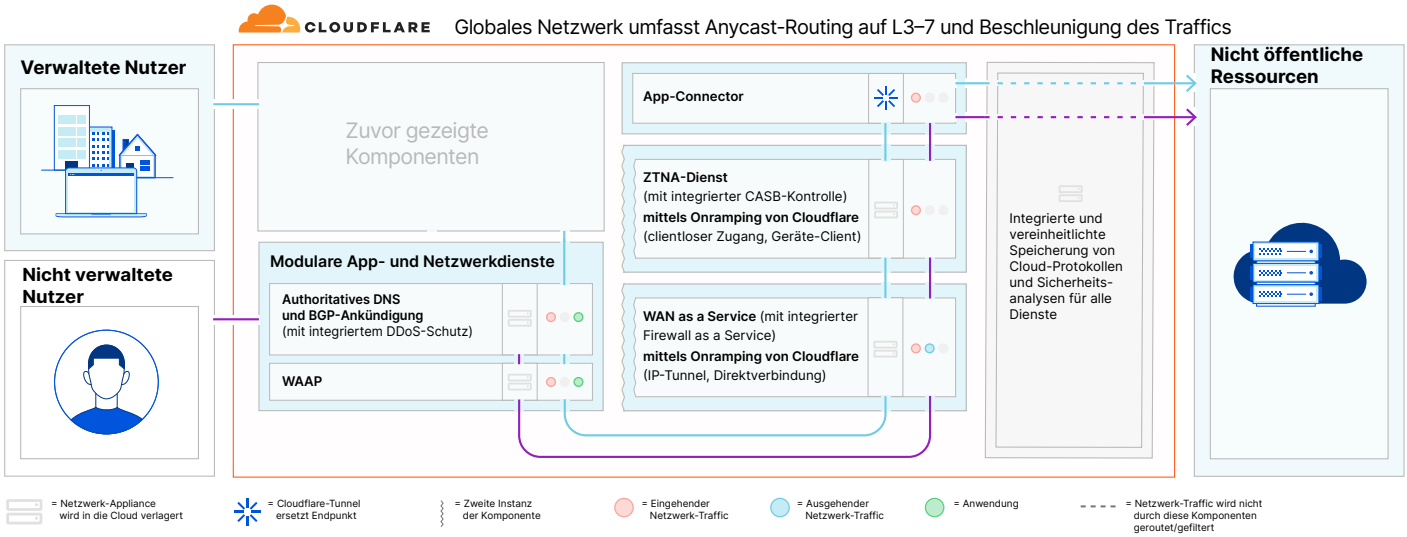
Unsere Zero Trust-Netzwerkzugangslösung und/oder unser WAN as a Service-Dienst mit integrierter Sicherheit setzten unseren App-Connector ein, um die Zugriffsverwaltung zu vereinfachen.

2b. Vereinfachte Vernetzung und Sicherheit für nicht öffentliche Ressourcen

Vor Einführung von Cloudflare



Nach Einführung von Cloudflare



Cloudnative Dienste

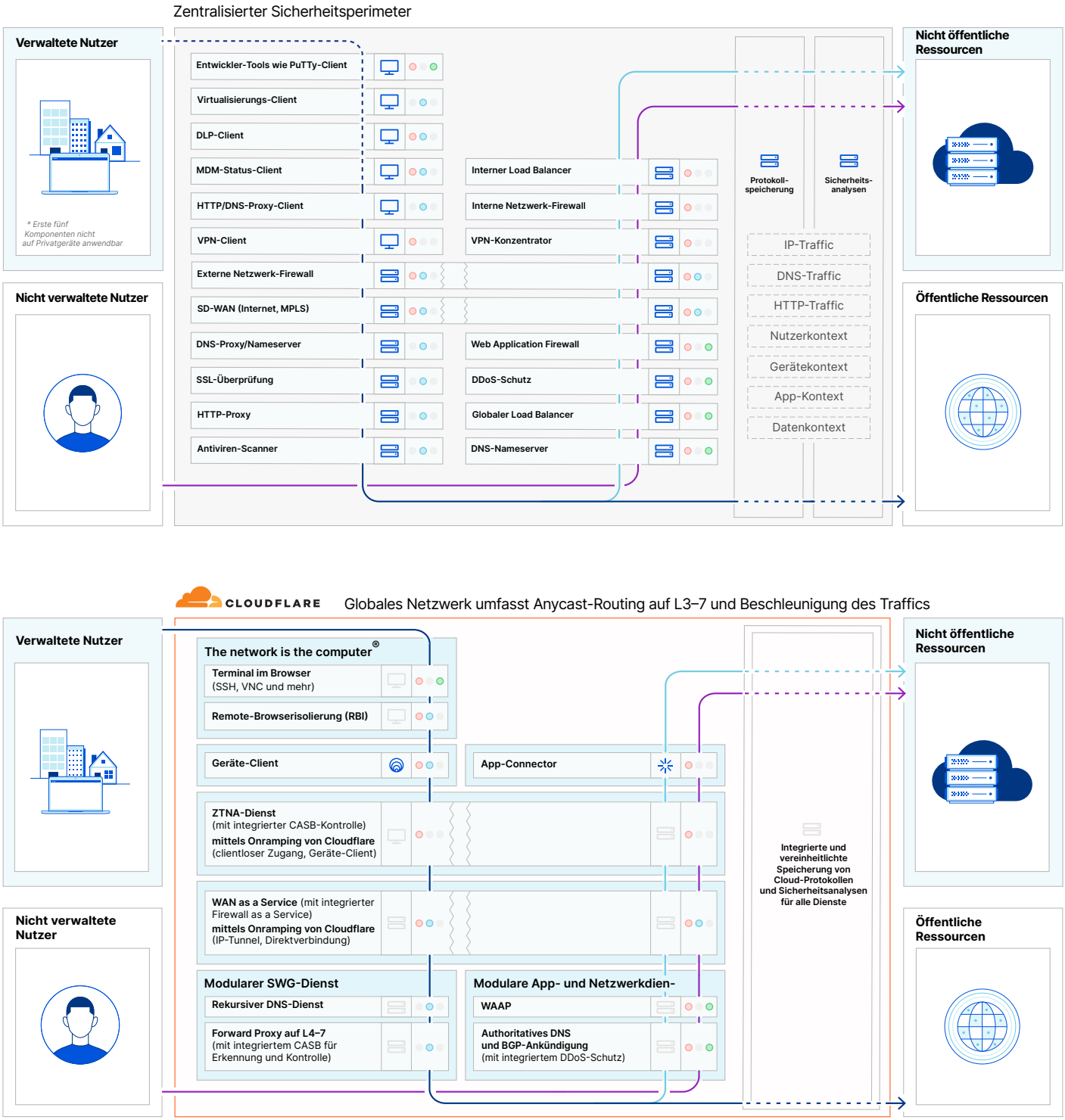
Die Anforderungen an Endgeräte und Netzwerk-Appliances sind niedriger.

Modulare Architektur

Zur Gewährleistung lückenloser Sicherheit und Performance werden der Protokollstapel für ein- und ausgehenden Traffic und der Anwendungsstapel zusammengeführt.

Vereinfachte Vernetzung und Sicherheit für alle Ressourcen

Hier wurden Schaubild 1 und 2 kombiniert.



Nachher

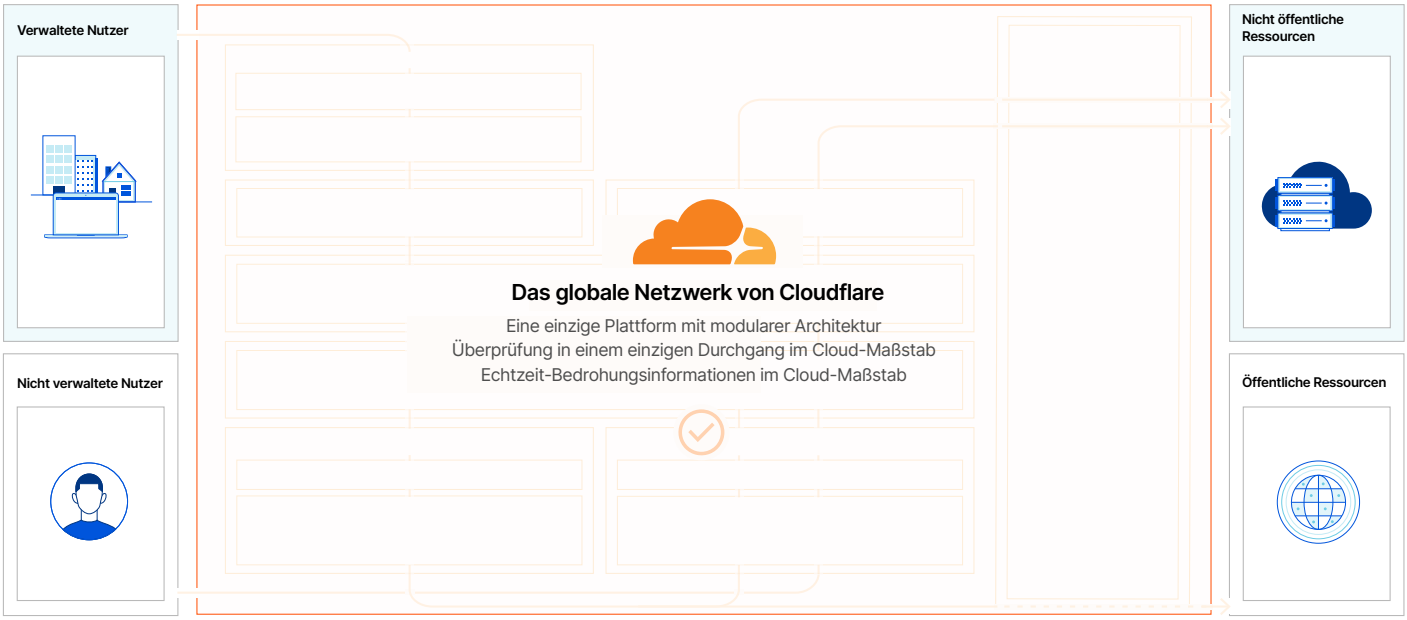
Vernetzungs- und Sicherheitskomponenten werden beim Zugriff jedes beliebigen Nutzers auf jede beliebige Ressource wiederverwendet, was sowohl die Effizienz erhöht als auch die Nutzererfahrung verbessert. Außerdem decken unsere Lösung für Zero Trust-Netzwerkzugang (Zero Trust Network Access – ZTNA) und unser WAN as a Service-Angebot Einzelelemente ab, die traditionell von IT-, Netzwerk- und IT-Sicherheitsabteilungen isoliert verwaltet wurden.

Eine einzige Plattform für einfachste Vernetzung und Sicherheit

Zentralisiertes Sicherheitsperimetermodell und globales Cloudflare-Netzwerk im Vergleich

Vorher

IT-, Netzwerks- und Sicherheitsmitarbeitende nutzten die Lösungen verschiedener Anbieter, die jeweils eine andere Architektur aufwiesen. Das machte Punkt-zu-Punkt-Integrationen erforderlich, die zu Verbindungs- und Sicherheitslücken führten, wodurch die Performance beschnitten wurde.



Nachher

Mitarbeitende aus allen Abteilungen setzten dieselbe Plattform mit modularer Architektur ein, wodurch Lücken im System und Performance-Einbußen vermieden werden. Unsere gesamte Plattform ist überall im Einsatz und so angelegt, dass sie sich Ihren Bedürfnissen anpasst, nicht umgekehrt. Gleichgültig, wie viele Dienste Sie einsetzen und in welcher Reihenfolge: Alle arbeiten reibungslos zusammen.

Anwendungsfall Nr. 1: Sicherer Zugriff auf Webanwendungen

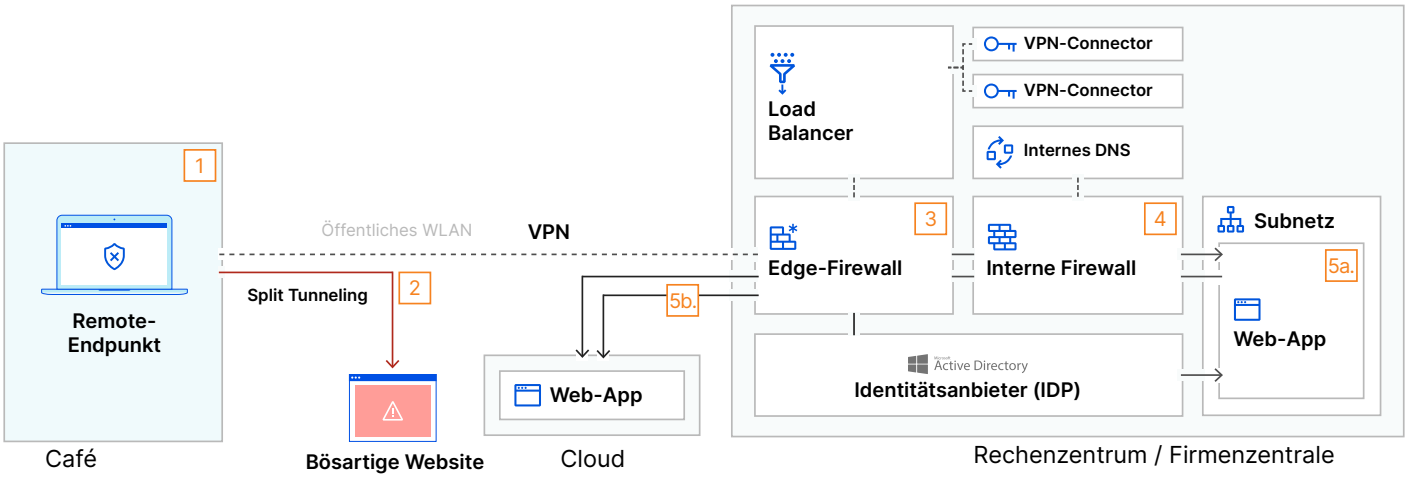
Herkömmliche Struktur – Einstieg

Dieses Schaubild zeigt eine traditionelle Methode, Fernzugriff auf Webanwendungen zu erlauben. In diesem Fall greift ein remote arbeitender Mitarbeitender auf Firmenressourcen zu, und zwar sowohl auf eine nicht öffentliche (selbstgehostete) als auch eine öffentliche (cloudbasierte) Webapplikation.

Die Grafik umfasst einige der gängigsten Sicherheitsmaßnahmen, die jedes seriöse Unternehmen einsetzen würde, darunter eine Edge-Firewall, eine interne Firewall zur Segmentierung und ein VPN.

In diesem Szenario wird von links nach rechts die Lebensdauer einer Sitzung abgebildet, und zwar von dem Zeitpunkt an, zu dem sich ein Nutzer von einem öffentlichen Standort aus anmeldet. Spätere Abbildungen bauen auf dieser Konstellation auf.

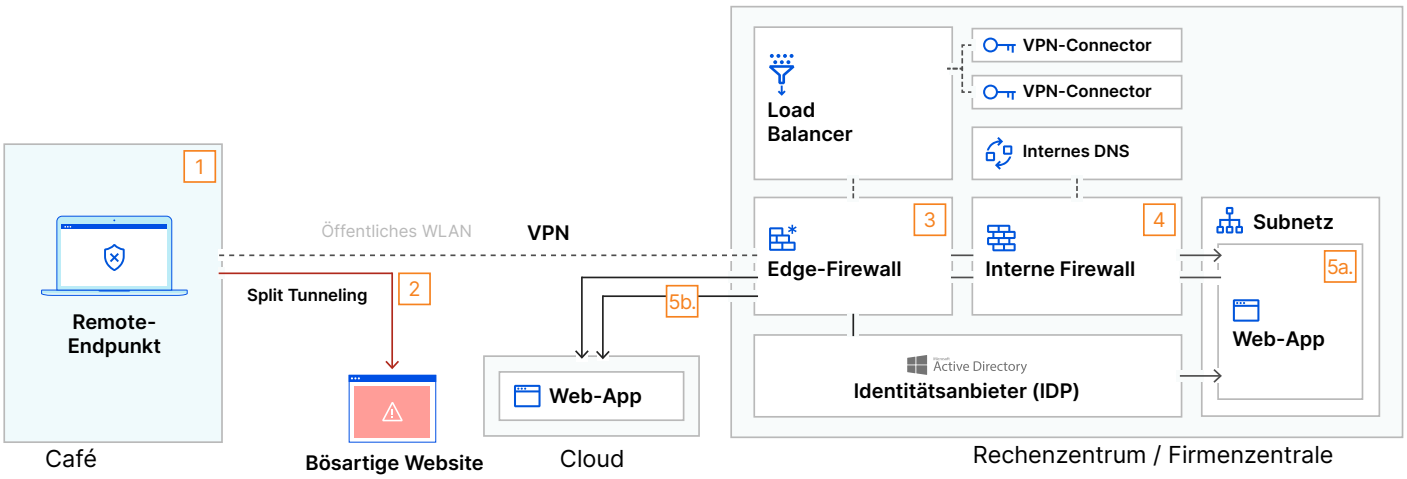
Hinweis:: Diese Grafik zeigt nur die Geräte, Appliances und Datenströme, die für diese konkreten Abläufe im Netzwerk relevant sind. Sie gibt somit keinen vollständigen Überblick über sämtliche Technologien, die in einer herkömmlichen Netzwerkarchitektur zum Einsatz kommen.



	Netzwerk-/Sicherheitsoperation
1	Ein Gerät greift aus der Ferne über das öffentliche WLAN auf Firmenressourcen zu
2	Die Anfrage des Geräts erreicht die Edge des Unternehmens über einen VPN-Client, wohingegen der restliche Traffic per Split Tunneling übertragen wird
3	VPN-Verbindung wird an der Edge-Firewall oder bei einem VPN-Konzentrator hinter der Firewall beendet
4	Firewall-Richtlinie erlaubt Remote-Nutzer Zugang zu dem Subnetz der nicht öffentlichen Webanwendung
5	Nutzer greift nach erfolgter Authentifizierung mittels IDP über private IP/URL auf Web-App **[5a.]** oder öffentliche URL **[5b.]** zu

Herkömmliche Struktur – Sicherheitslücken

In dieser Abbildung wird eine weitere Spalte hinzugefügt. Diese hebt Sicherheitsprobleme hervor, die mit jedem konkreten Schritt in diesem Szenario einhergehen und ein Unternehmen bestimmten Risiken aussetzen.

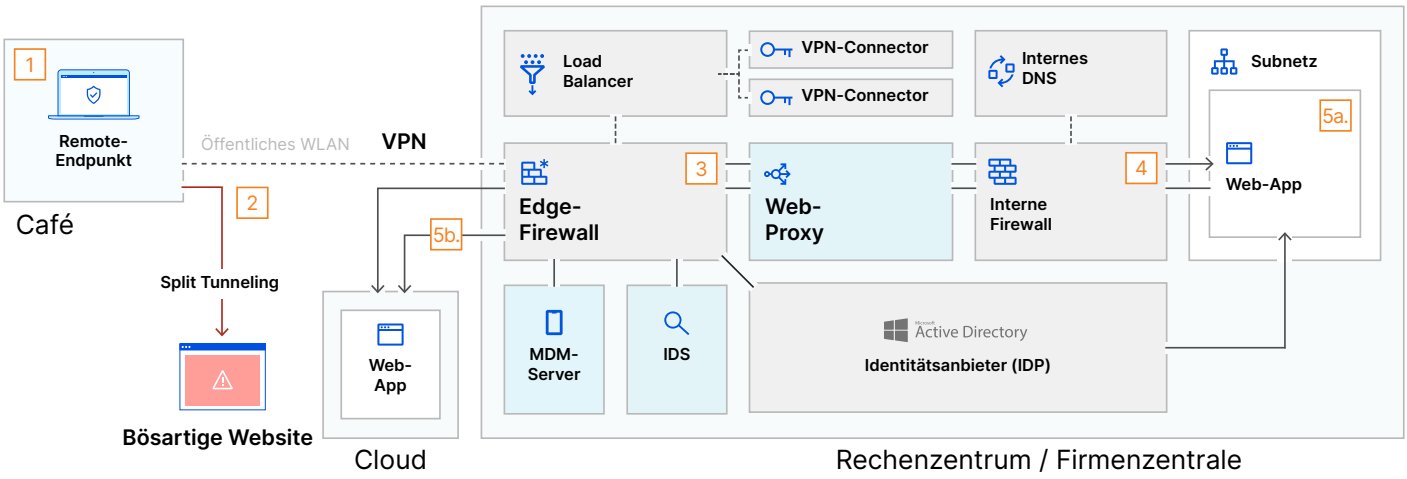


	Netzwerk-/Sicherheitsoperation	Relevante herkömmliche Lösung	Schwachpunkt herkömmlicher Struktur
1	Ein Gerät greift aus der Ferne über das öffentliche WLAN auf Firmenressourcen zu	VPN-Client des Unternehmens	Ein nicht abgesichertes Gerät im öffentlichen WLAN ist ein Ziel für Kriminelle
2	Die Anfrage des Remote-Endpunkts erreicht die Edge des Unternehmens über einen VPN-Client, wohingegen der restliche Traffic per Split-Tunneling übertragen wird	VPN-Client des Unternehmens	VPN-spezifische Sicherheitslösung schützt keinen per Split Tunneling übertragenen Traffic
3	VPN-Verbindung wird an der Edge-Firewall oder bei einem VPN-Konzentrator hinter der Firewall beendet	Load Balancer Edge-Firewall VPN-Konzentrator	Aufgrund der Regeln für eingehenden Traffic der Firewall bzw. des VPN sind Ports/Protokolle ggf. dem Internet ausgesetzt, wodurch sich die Angriffsfläche erhöhen kann
4	Firewall-Richtlinie erlaubt Remote-Nutzer Zugang zu dem Subnetz der nicht öffentlichen Webanwendung	Interne Firewall	Der Nutzer erhält auch Zugang zu Ressourcen, die von seiner Funktion im Unternehmen nicht abgedeckt sind
5	Nutzer greift nach erfolgter Authentifizierung mittels IDP über private IP/URL auf Web-App [5a.] oder öffentliche URL [5b.] zu	Active Directory Internes DNS (nicht öffentlich)	Ist der Endpunkt kompromittiert, ist die App/das Netzwerk des Unternehmens gefährdet

Herkömmliche Struktur – erforderliche Sicherheitserweiterungen

Zur Lösung der durch die gerade beschriebenen strukturellen Fehler verursachten Probleme muss das Unternehmen seine bestehende Netzwerkinfrastruktur anpassen. In dieser Grafik wird eine weitere Spalte hinzugefügt, die gängige Lösungen zum Schutz von Nutzern und Ressourcen auflistet.

Durch zusätzliche Sicherheitsmaßnahmen nimmt die Unübersichtlichkeit zu. Außerdem steigen die laufenden Verwaltungskosten für die herkömmliche Umgebung, die vermutlich eine Vielzahl von Anbietern umfasst.



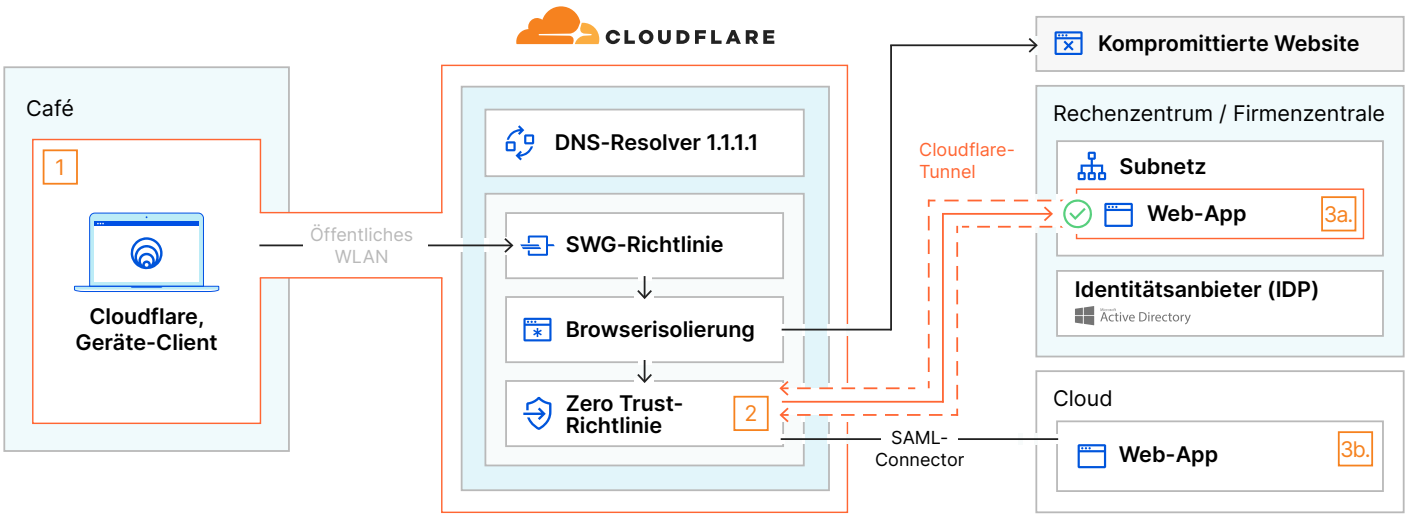
	Netzwerk-/Sicherheitsoperation	Relevante herkömmliche Lösung	Schwachpunkt herkömmlicher Struktur	Erforderliche Sicherheitserweiterung
1	Ein Gerät greift aus der Ferne über das öffentliche WLAN auf Firmenressourcen zu	VPN-Client des Unternehmens	Ein nicht abgesichertes Gerät im öffentlichen WLAN ist ein Ziel für Kriminelle	Plattform zum Endpunktschutz
2	Die Anfrage des Geräts erreicht die Edge des Unternehmens über einen VPN-Client, wohingegen der restliche Traffic per Split Tunneling übertragen wird	VPN-Client des Unternehmens	VPN-spezifische Sicherheitslösung schützt keinen per Split Tunneling übertragenen Traffic	Split Tunneling wird deaktiviert
3	VPN-Verbindung wird an der Edge-Firewall oder bei einem VPN-Konzentrator hinter der Firewall beendet	Load Balancer Edge-Firewall VPN-Konzentrator	Aufgrund der Regeln für eingehenden Traffic der Firewall bzw. des VPN sind Ports/Protokolle ggf. dem Internet ausgesetzt, wodurch sich die Angriffsfläche erhöhen kann	Angriffserkennungs-system
4	Firewall-Richtlinie erlaubt Remote-Nutzer Zugang zu dem Subnetz der nicht öffentlichen Webanwendung	Interne Firewall	Der Nutzer erhält auch Zugang zu Ressourcen, die von seiner Funktion im Unternehmen nicht abgedeckt sind	Web-Proxy
5	Nutzer greift nach erfolgter Authentifizierung mittels IDP über private IP/URL auf Web-App **[5a.]** oder öffentliche URL **[5b.]** zu	Active Directory Internes DNS (nicht öffentlich)	Ist der Endpunkt kompromittiert, ist die App/das Netzwerk des Unternehmens gefährdet	Server für Mobilgeräteverwaltung

Struktur von Cloudflare One

Die folgende Grafik verdeutlicht, wie eine einfachere, effizientere Herangehensweise für sicheren Anwendungszugriff durch die Einführung von Cloudflare One aussehen könnte.

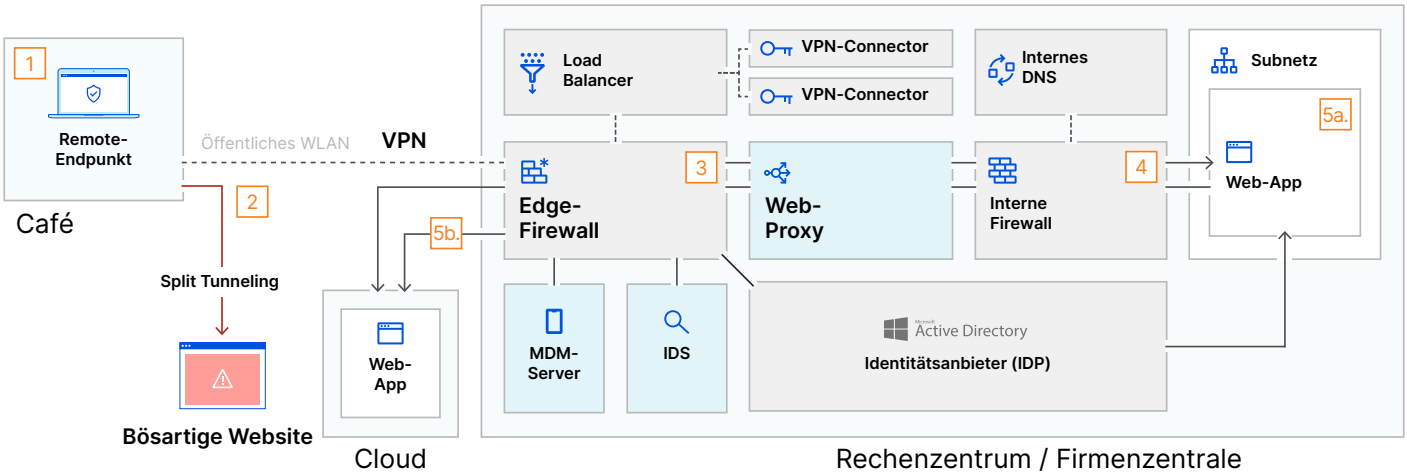
In diesem Fall wird ein Großteil der herkömmlichen Netzwerkarchitektur, die zuvor dargestellt wurde, auf Cloudflare übertragen. Viele der bestehenden strukturellen Fehler werden auf diese Weise ohne den Einsatz zusätzlicher Lösungen behoben.

Mit Cloudflare One fließt der Datenverkehr zwischen dem Remote-Nutzer und den Ressourcen des Unternehmens durch das globale Cloudflare-Netzwerk, wo er in einem einzigen Arbeitsdurchgang überprüft wird. Alle unten dargestellten Dienste werden in allen Rechenzentren von Cloudflare betrieben, die auf über 250 Städte in mehr als 100 Ländern verteilt sind.

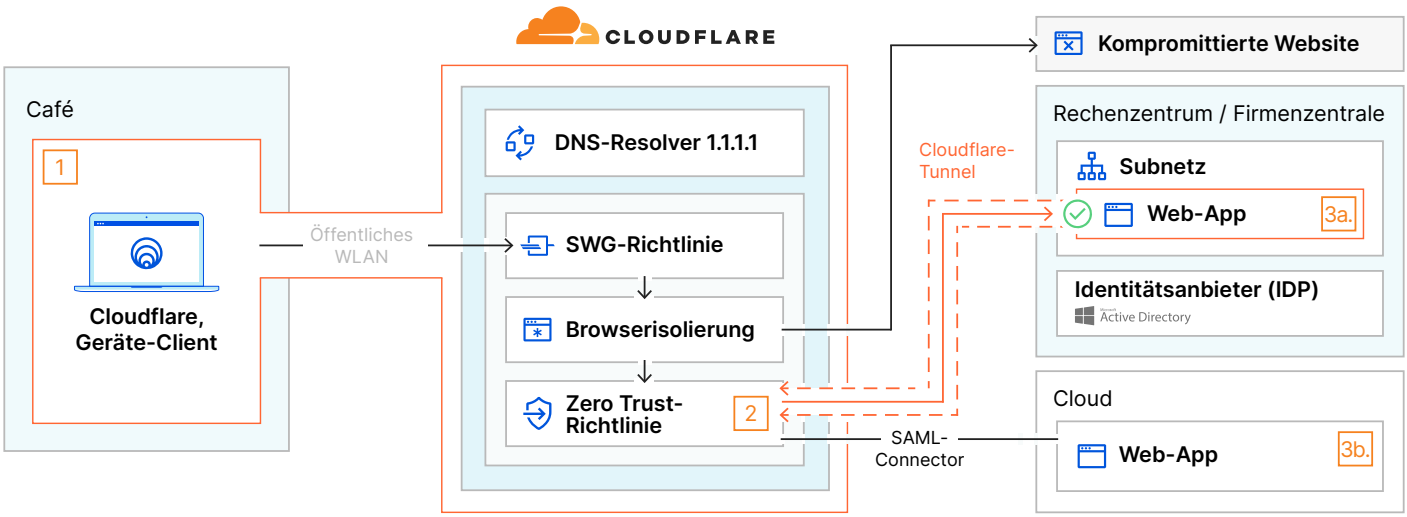


	Netzwerk-/Sicherheitsoperation	Relevante Cloudflare One-Komponente	Behebung des strukturellen Schwachpunkts
1	Ein Gerät verbindet sich aus der Ferne über Cloudflare mit Firmenressourcen und dem Internet	Geräte-Client von Cloudflare Secure Web Gateway-Richtlinie Browserisolierung	Lokaler Secure Web Gateway-Client lässt Cloudflare One den für das Nutzergerät bestimmten DNS/HTTP/Netzwerk-Traffic mittels Gateway-Richtlinie filtern Browserisolierung federt die Auswirkungen erfolgreicher Angriffe durch Malware auf Websites ab
2	Nutzer durchläuft im Cloudflare-Netzwerk Identitäts- und Gerätestatusprüfungen	Zero Trust-Richtlinie	Zero Trust-Richtlinie führt Überprüfung des Gerätestatus durch, bevor der Zugang genehmigt wird, wodurch sich das Risiko kompromittierter Geräte verringert Zero Trust-Richtlinie führt Nutzerauthentifizierung nur für die Ressource und nicht für das zugrundeliegende Netzwerk durch, was laterale Bewegungen verhindert
3	Zugriff auf [nicht öffentliche| öffentliche] Web-App direkt über [Cloudflare-Tunnel | SAML-Connector]	Cloudflare Tunnel 1.1.1.1 DNS-Auflösung	Cloudflare-Tunnel stellt eine sichere Verbindung zur Web-Anwendung her und macht explizite Firewall-Regeln überflüssig

Herkömmliche Struktur – erforderliche Sicherheitserweiterungen



Struktur von Cloudflare One



Herkömmliche Struktur – erforderliche Sicherheitserweiterungen

	Netzwerk-/Sicherheitsoperation	Relevante herkömmliche Lösung	Schwachpunkt herkömmlicher Struktur	Erforderliche Sicherheitserweiterung
1	Ein Gerät greift aus der Ferne über das öffentliche WLAN auf Firmenressourcen zu	VPN-Client des Unternehmens	Ein nicht abgesichertes Gerät im öffentlichen WLAN ist ein Ziel für Kriminelle	Plattform zum Endpunktschutz
2	Die Anfrage des Geräts erreicht die Edge des Unternehmens über einen VPN-Client, wohingegen der restliche Traffic per Split Tunneling übertragen wird	VPN-Client des Unternehmens	VPN-spezifische Sicherheitslösung schützt keinen per Split Tunneling übertragenen Traffic	Split Tunneling wird deaktiviert
3	VPN-Verbindung wird an der Edge-Firewall oder bei einem VPN-Konzentrator hinter der Firewall beendet	Load Balancer Edge-Firewall VPN-Konzentrator	Aufgrund der Regeln für eingehenden Traffic der Firewall bzw. des VPN sind Ports/Protokolle ggf. dem Internet ausgesetzt, wodurch sich die Angriffsfläche erhöhen kann	Angriffserkennungs-system
4	Firewall-Richtlinie erlaubt Remote-Nutzer Zugang zu dem Subnetz der nicht öffentlichen Webanwendung	Interne Firewall	Der Nutzer erhält auch Zugang zu Ressourcen, die von seiner Funktion im Unternehmen nicht abgedeckt sind	Web-Proxy
5	Nutzer greift nach erfolgter Authentifizierung mittels IDP über private IP/URL auf Web-App **[5a.]** oder öffentliche URL **[5b.]** zu	Active Directory Internes DNS (nicht öffentlich)	Ist der Endpunkt kompromittiert, ist die App/das Netzwerk des Unternehmens gefährdet	Server für Mobilgeräteverwaltung

Struktur von Cloudflare One

	Netzwerk-/Sicherheitsoperation	Relevante Cloudflare One-Komponente	Behebung des strukturellen Schwachpunkts
1	Ein Gerät verbindet sich aus der Ferne über Cloudflare mit Firmenressourcen und dem Internet	**Geräte-Client von Cloudflare** **Secure Web Gateway-Richtlinie** **Browserisolierung**	Lokaler Secure Web Gateway-Client lässt Cloudflare One den für das Nutzergerät bestimmten DNS/HTTP/Netzwerk-Traffic mittels Gateway-Richtlinie filtern Browserisolierung federt die Auswirkungen erfolgreicher Angriffe durch Malware auf Websites ab
2	Nutzer durchläuft im Cloudflare-Netzwerk Identitäts- und Gerätestatusprüfungen	**Zero Trust-Richtlinie**	Zero Trust-Richtlinie führt Überprüfung des Gerätestatus durch, bevor der Zugang genehmigt wird, wodurch sich das Risiko kompromittierter Geräte verringert Zero Trust-Richtlinie führt Nutzerauthentifizierung nur für die Ressource und nicht für das zugrundeliegende Netzwerk durch, was laterale Bewegungen verhindert
3	Zugriff auf [nicht öffentliche| öffentliche] Web-App direkt über [Cloudflare-Tunnel | SAML-Connector]	**Cloudflare-Tunnel** **DNS-Resolver 1.1.1.1**	Cloudflare-Tunnel stellt eine sichere Verbindung zur Web-Anwendung her und macht explizite Firewall-Regeln überflüssig

Anwendungsfall Nr. 2: DNS-Filterung

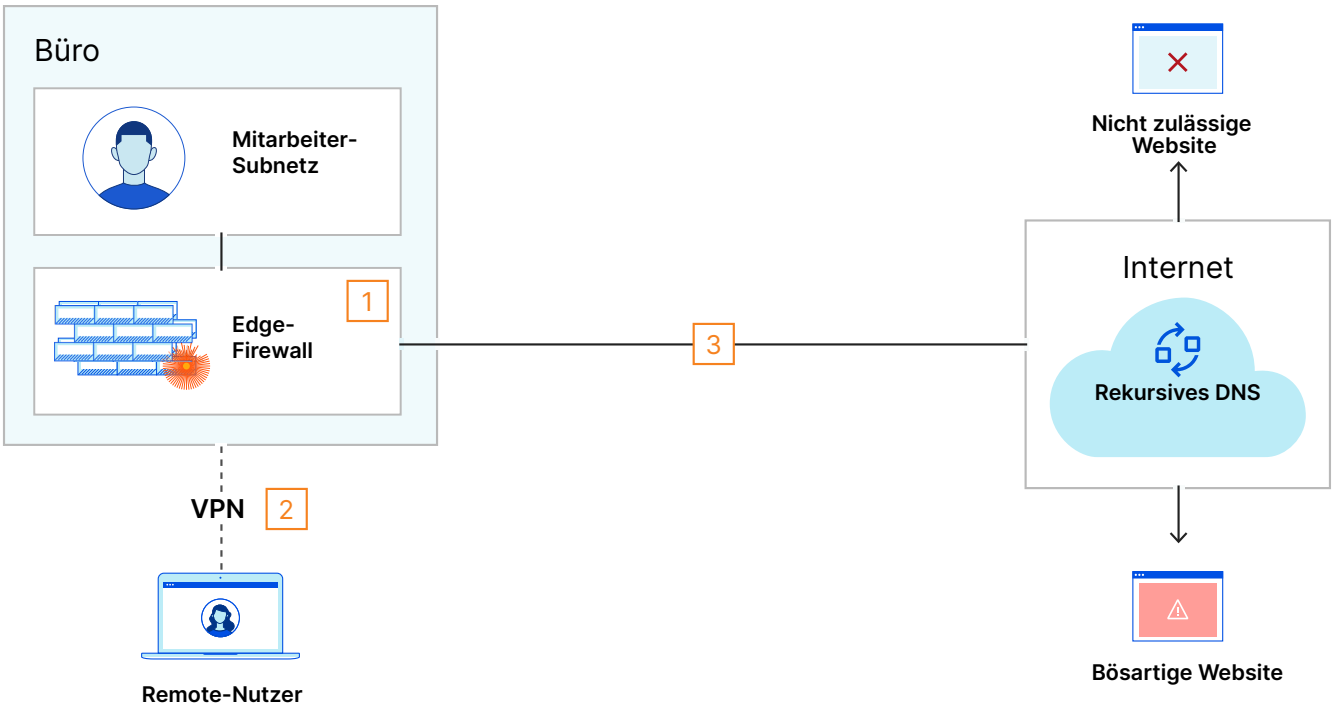
Herkömmliche Struktur – Einstieg

Dieses Schaubild zeigt DNS-Filterung für Beschäftigte inner- und außerhalb des Firmenstandorts bei Unternehmen mit einer herkömmlichen Umgebung.

Normalerweise werden dafür integrierte Funktionen lokaler Lösungen wie einer Firewall verwendet. Der Traffic von Remote-Nutzern wird zunächst vollständig durch einen VPN-Tunnel geleitet und kann so diese Firewall passieren.

Zum Auflösen von Website-IPs schickt das Unternehmen seine DNS-Abfragen an einen rekursiven DNS-Server (wie 8.8.8.8 von Google).

Hinweis: Genau wie in anderen Abschnitten dieses Leitfadens werden auch bei dieser herkömmlichen Umgebung nicht alle Technologien dargestellt, die in einem Büro eingesetzt werden, sondern nur diejenigen, die in diesem konkreten Anwendungsfall zum Einsatz kommen.



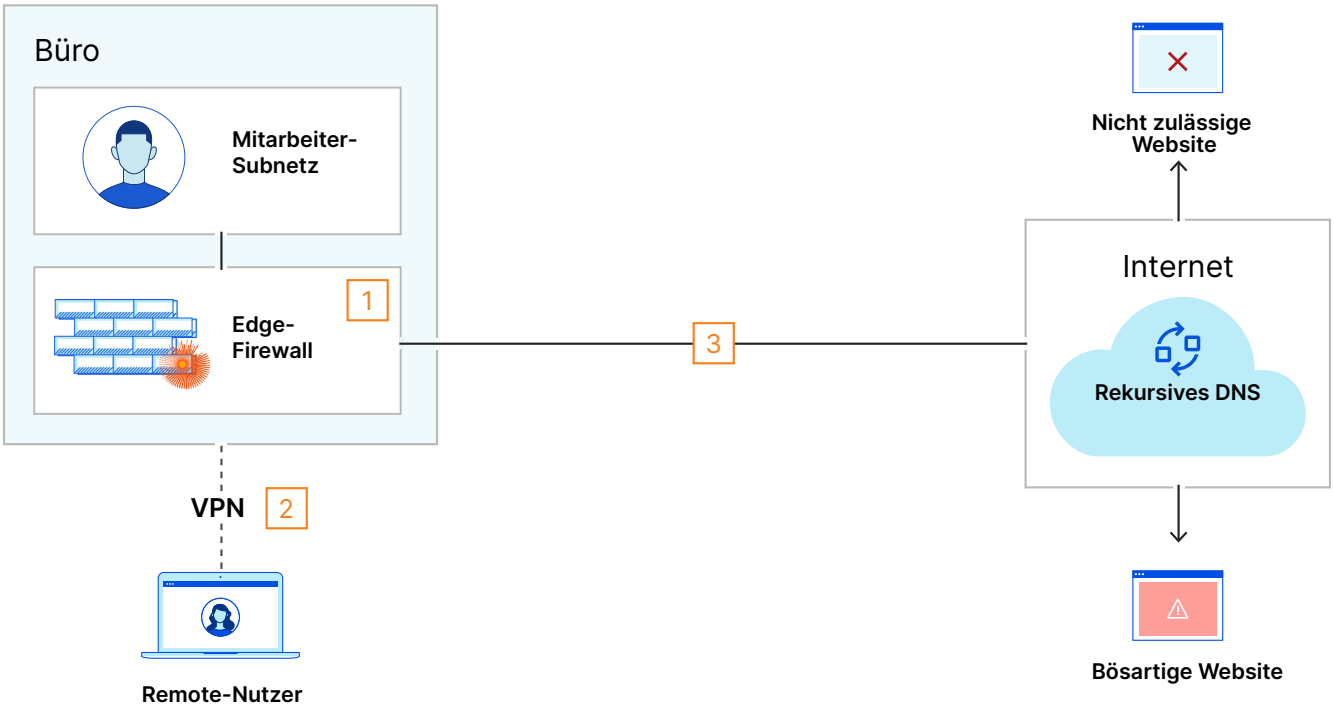
	DNS-bezogenes Ereignis
1	Die Inhalte von DNS-Anfragen eines Nutzers vor Ort werden durch die entsprechende Funktion der Edge-Firewall auf Sicherheitsrisiken hin gefiltert
2	Die DNS-Anfragen eines Remote-Nutzers werden gefiltert, nachdem er sich mit dem Full Tunnel-VPN des Unternehmens verbunden hat
3	Ausgehende DNS-Anfragen werden unverschlüsselt übertragen

Herkömmliche Struktur – betriebliche Schwächen

Die nächste Abbildung wird um eine Spalte erweitert, in der die mit dieser herkömmlichen Struktur verbundenen Probleme aufgeführt sind.

Die größte Herausforderung besteht darin, dass zur DNS-Filterung in großem Maßstab auf lokale Hardware zurückgegriffen wird, worunter früher oder später die Performance für sämtliche Nutzer leidetd – vor allem, wenn diese Hardware auch für andere wichtige Dienste genutzt wird (wie das Beenden der VPN-Verbindung des Remote-Nutzers).

Außerdem schafft das (standardmäßige) Versenden von unverschlüsselten DNS-Abfragen einen neuen Angriffsvektor mit unbekanntem Risiko.



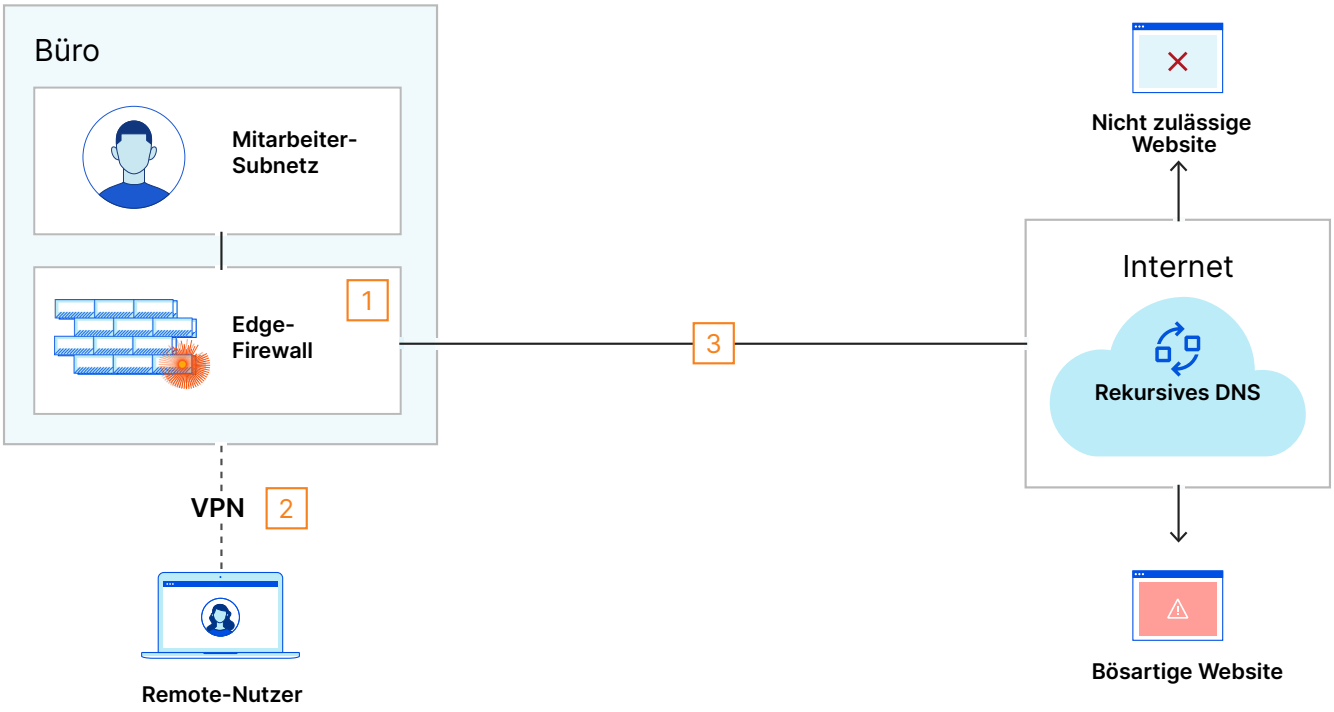
	DNS-bezogenes Ereignis	Relevante Komponente	Struktureller Schwachpunkt
1	Die Inhalte von DNS-Anfragen eines Nutzers vor Ort werden durch die entsprechende Funktion der Edge-Firewall auf Sicherheitsrisiken hin gefiltert	Edge-Firewall	Werden der Edge-Firewall zu viele wichtige Aufgaben übertragen, kann das die Performance unternehmensweit beeinträchtigen
2	Die DNS-Anfragen eines Remote-Nutzers werden gefiltert, nachdem er sich mit dem Full Tunnel-VPN des Unternehmens verbunden hat	VPN-Konzentrator Edge-Firewall	Ein Full Tunnel-VPN schafft eine „Doppelbelastung“ hinsichtlich der Datenpakete aus dem Internet, was die Traffic-Übermittlung per Tunnel für das gesamte Internet verlangsamen kann
3	Ausgehende DNS-Anfragen werden unverschlüsselt übertragen	UDP 53	DNS-Anfragen per UDP-Port 53 sind unverschlüsselt und deshalb öffentlich. Somit kann darüber das Verhalten von Nutzern im Web ausspioniert werden

Herkömmliche Struktur – erforderliche Netzwerkanpassungen

Zur Lösung der durch die gerade beschriebenen strukturellen Schwächen verursachten Probleme muss das Unternehmen seine bestehende Netzwerkinfrastruktur anpassen. In dieser Grafik wird eine weitere Spalte hinzugefügt, in der gängige Lösungen und deren Nachteile aufgelistet werden.

In diesem Fall treibt die Anschaffung neuer Hardware zur Bewältigung zusätzlicher Nutzer oder eine höhere Bandbreitenausschöpfung im Lauf der Zeit die Investitions- und Betriebskosten in die Höhe.

Beim Versuch, diesen Ansatz zu skalieren, sind Unternehmen oft mit erheblichen Problemen konfrontiert. Viele vermeiden aufgrund entsprechender betrieblicher Bedenken die DNS-Filterung sogar vollständig.



	DNS-bezogenes Ereignis	Relevante Komponente	Struktureller Schwachpunkt	Lösung ohne Cloudflare
1	Die Inhalte von DNS-Anfragen eines Nutzers vor Ort werden durch die entsprechende Funktion der Edge-Firewall auf Sicherheitsrisiken hin gefiltert	Edge-Firewall	Werden der Edge-Firewall zu viele wichtige Aufgaben übertragen, kann das die Performance unternehmensweit beeinträchtigen	Separate DNS-Filter
2	Die DNS-Anfragen eines Remote-Nutzers werden gefiltert, nachdem er sich mit dem Full Tunnel-VPN des Unternehmens verbunden hat	VPN-Konzentrator Edge-Firewall	Ein Full Tunnel-VPN schafft eine „Doppelbelastung“ hinsichtlich der Datenpakete aus dem Internet, was die Traffic-Übermittlung per Tunnel für das gesamte Internet verlangsamen kann	Erhöhung der ISP-Bandbreite Upgrade der Hardware Aktivierung von Spilt Tunneling*
3	Ausgehende DNS-Anfragen werden unverschlüsselt übertragen	UDP 53	DNS-Anfragen per UDP-Port 53 sind unverschlüsselt und deshalb öffentlich. Somit kann darüber das Verhalten von Nutzern im Web ausspioniert werden	DNS over TLS/HTTPS

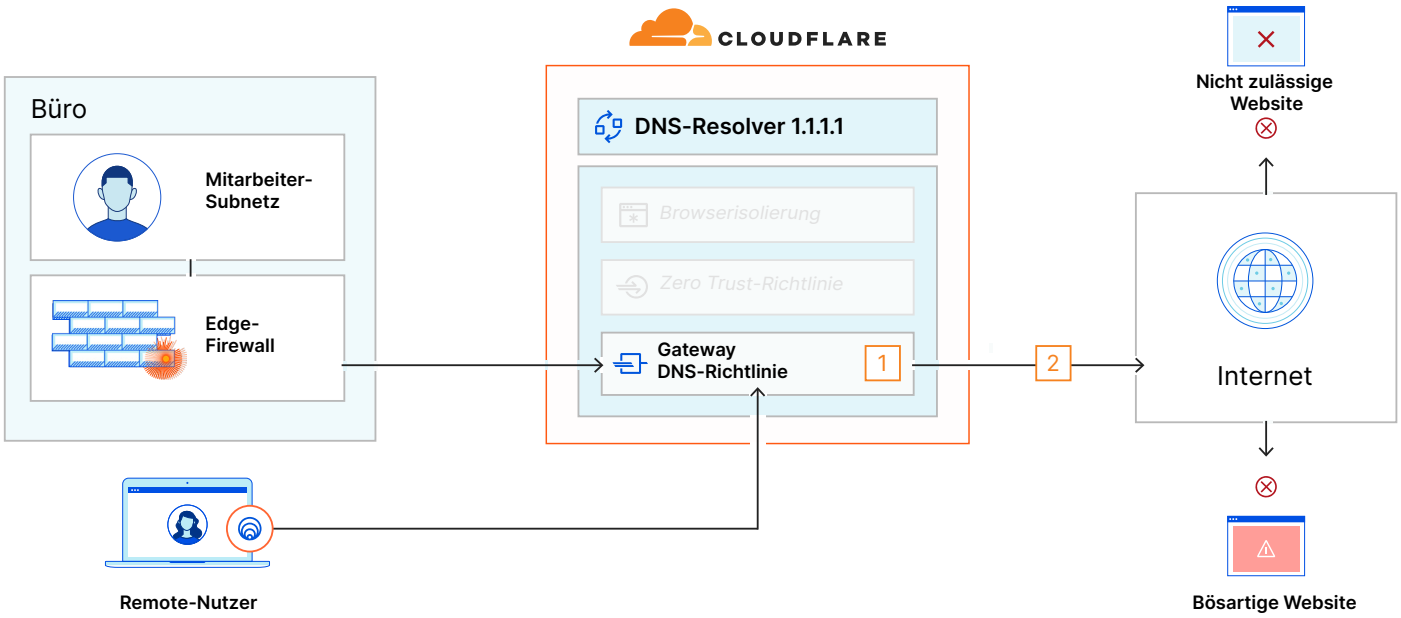
Struktur von Cloudflare One

Unternehmen, die Cloudflare One nutzen, leiten ihren Traffic zu dem globalen Netzwerk von Cloudflare und können daher DNS-Filterung für die gesamte Belegschaft durchführen, ohne sich über die Kapazitätsgrenzen ihrer lokalen Hardware Gedanken machen zu müssen.

Die DNS-Filterung von Cloudflare ist sowohl für lokale Nutzer als auch für Remote-User leicht zu implementieren:

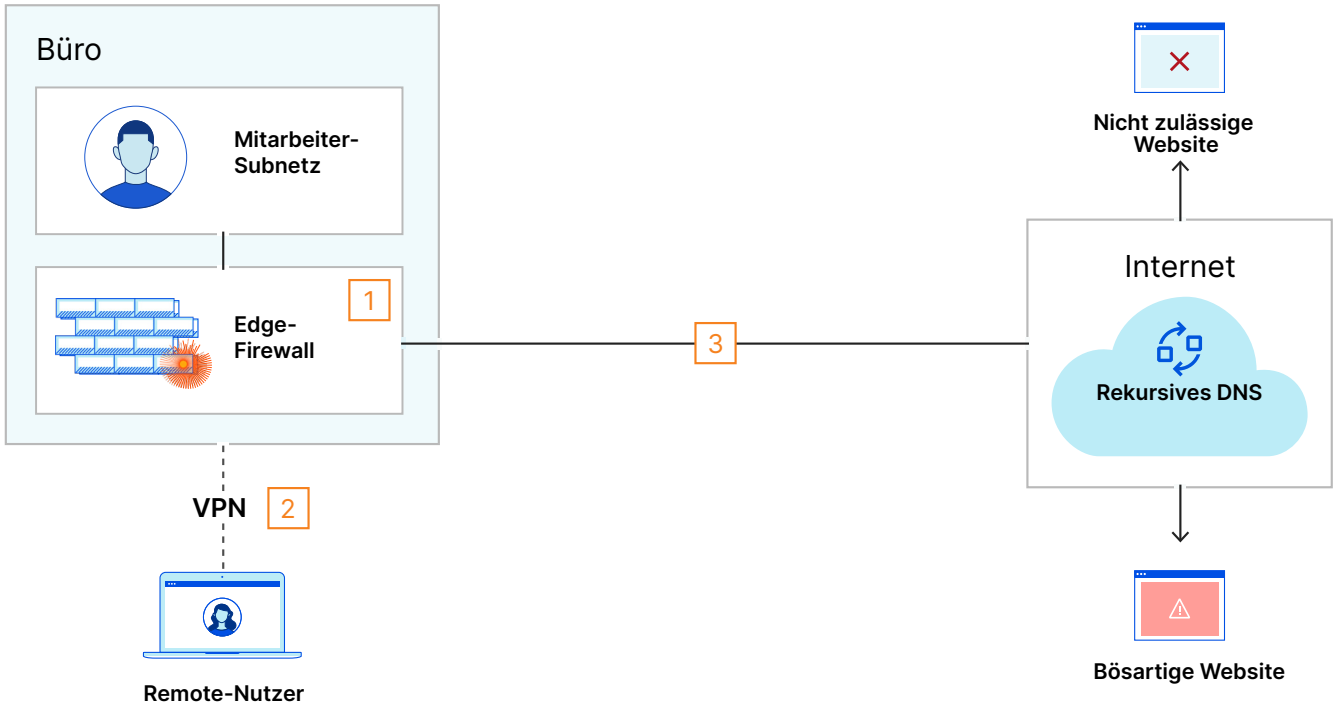
- Der Traffic von Nutzern am Firmenstandort wird anhand der Ausgangs-IP von der Edge-Firewall an Cloudflare übertragen
- Der Traffic von Remote-Nutzern wird von unserem Geräte-Client an Cloudflare übertragen

Außerdem unterstützt der 1.1.1.1-DNS-Resolver von Cloudflare DNS over TLS/HTTPS, wodurch das Sicherheitsproblem beseitigt wird, das für die herkömmliche Umgebung aufgeführt ist.

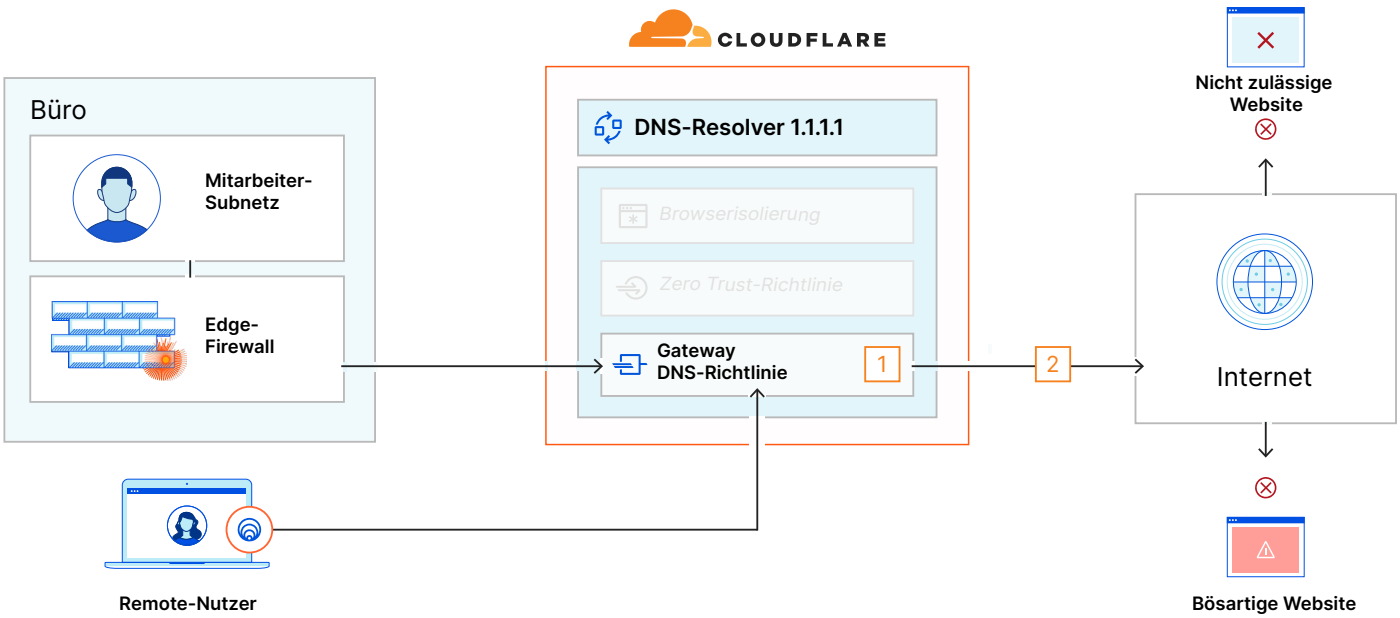


	DNS-bezogenes Ereignis	Relevante Cloudflare One-Komponente	Behebung des strukturellen Schwachpunkts
1	Der Inhalt der DNS-Anfragen von Nutzern vor Ort und von externen Standorten wird von Cloudflare gefiltert	Secure Web Gateway	Gateway DNS-Richtlinien übernehmen die DNS-Filterung für lokale Hardware (oder ermöglichen sie erstmalig)
2	Die DNS-Anfragen des Unternehmens werden vor dem Versenden verschlüsselt	DNS-Resolver 1.1.1.1	Der 1.1.1.1-DNS-Resolver von Cloudflare unterstützt DNS over TLS/HTTPS, verschlüsselt DNS-Anfragen und verhindert feindliche Erkundungsmaßnahmen

Herkömmliche Struktur



Struktur von Cloudflare One



Herkömmliche Struktur

	DNS-bezogenes Ereignis	Relevante Komponente	Struktureller Schwachpunkt	Lösung ohne Cloudflare
1	Die Inhalte von DNS-Anfragen eines Nutzers vor Ort werden durch die entsprechende Funktion der Edge-Firewall auf Sicherheitsrisiken hin gefiltert	Edge-Firewall	Werden der Edge-Firewall zu viele wichtige Aufgaben übertragen, kann das die Performance unternehmensweit beeinträchtigen	Separate DNS-Filter
2	Die DNS-Anfragen eines Remote-Nutzers werden gefiltert, nachdem er sich mit dem Full Tunnel-VPN des Unternehmens verbunden hat	VPN-Konzentrator Edge-Firewall	Ein Full Tunnel-VPN schafft eine „Doppelbelastung“ hinsichtlich der Datenpakete aus dem Internet, was die Traffic-Übermittlung per Tunnel für das gesamte Internet verlangsamen kann	Erhöhung der ISP-Bandbreite Upgrade der Hardware Aktivierung von Spilt Tunneling*
3	Ausgehende DNS-Anfragen werden unverschlüsselt übertragen	UDP 53	DNS-Anfragen per UDP-Port 53 sind unverschlüsselt und deshalb öffentlich. Somit kann darüber das Verhalten von Nutzern im Web ausspioniert werden	DNS over TLS/HTTPS

Struktur von Cloudflare One

	DNS-bezogenes Ereignis	Relevante Cloudflare One-Komponente	Behebung des strukturellen Schwachpunkts
1	Der Inhalt der DNS-Anfragen von Nutzern vor Ort und von externen Standorten wird von Cloudflare gefiltert	Secure Web Gateway	Gateway DNS-Richtlinien übernehmen die DNS-Filterung für lokale Hardware (oder ermöglichen sie erstmalig)
2	Die DNS-Anfragen des Unternehmens werden vor dem Versenden verschlüsselt	DNS-Resolver 1.1.1.1	Der 1.1.1.1-DNS-Resolver von Cloudflare unterstützt DNS over TLS/HTTPS, verschlüsselt DNS-Anfragen und verhindert feindliche Erkundungsmaßnahmen