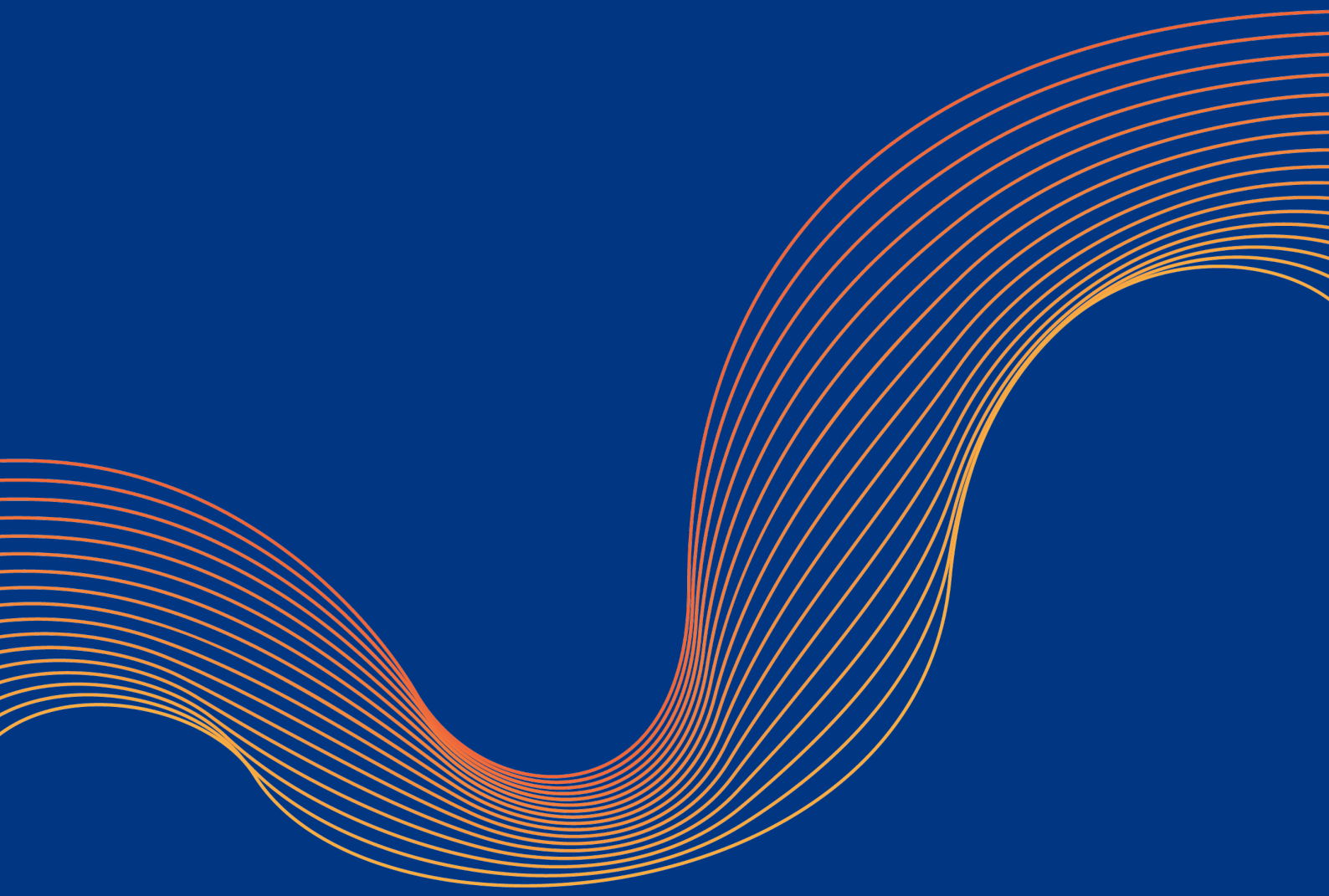
WHITEPAPER

CLOUDFLARE

Kann VPN durch ZTNA abgelöst werden? Drei Modelle für den Fernzugriff im Vergleich



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

INHALT

EINLEITUNG

Ein sicherer und reibungsloser Fernzugriff ist ein entscheidender Erfolgsfaktor für Unternehmen. Er steigert die Produktivität von Remote-Benutzern und reduziert den Zeitaufwand von IT-Teams für die Erstellung und Aufrechterhaltung der Verbindungen zwischen Nutzern und Anwendungen. Gleichzeitig sorgt er für Agilität und Ausfallsicherheit. Allerdings stellt der Remote-Zugriff für viele Unternehmen weiter eine Herausforderung dar.

Früher boten VPNs eine einfache Möglichkeit, wenige Remote-Benutzer für kurze Zeit mit Unternehmensnetzwerken zu verbinden. Mit der Zeit wurden Arbeitsteams jedoch immer weiter verteilt, die Remote-Arbeit wurde in Organisationen immer beliebter. Seither müssen Unternehmen eine sichere Verbindung ihrer Remote-Benutzer für längere Zeiträume gewährleisten. Dadurch zeigten sich die Schwächen dieses Ansatzes. Sie reichen von unzureichender Performance und erhöhten Sicherheitsrisiken bis hin zu Bedenken hinsichtlich der Skalierbarkeit.

Unternehmen wenden sich aufgrund der wachsenden Anforderungen an den Fernzugriff zunehmend von traditionellen VPN-Implementierungen ab und setzen auf sicherere und leistungsfähigere Lösungen. Der Zero Trust-Netzwerkzugang (Zero Trust Network Access – ZTNA) sorgt für Sicherheit rund um bestimmte Anwendungen, private IPs und Hostnamen. Standardmäßig zugelassene VPN-Verbindungen werden durch Richtlinien mit standardmäßiger Verweigerung des Zugriffs ersetzt. Der Zugriff wird auf Grundlage von Identität und Kontext gewährt.

Im Jahr 2020 erfolgte etwa 5 % der gesamten Fernzugriffsaktivität per ZTNA. Aufgrund der Beschränkungen des traditionellen VPN-Zugangs und der Notwendigkeit einer präziseren Zugangs- und Sitzungskontrolle wird erwartet, dass dieser Anteil bis 2024 auf 40 % ansteigen wird.[1]

Obwohl ZTNA für Unternehmen gegenüber VPN mehrere eindeutige Vorteile – und erweiterte Funktionen – bietet, haben viele Firmen festgestellt, dass dieses Verfahren kein vollwertiger Ersatz für die VPN-Infrastruktur ist. Aber da ZTNA-Lösungen immer robuster und VPNs immer problematischer werden, ändert sich das schnell. In diesem Whitepaper werden VPNs und ZTNA-Fernzugriffslösungen gegenübergestellt, um ihre Vorteile und Grenzen aufzuzeigen und gleichzeitig die wichtigsten Überlegungen für Migrationsprojekte zu beleuchten. Es wird erklärt, wie Cloudflare ZTNA bereitstellt. Außerdem haben wir eine Reihe von Handlungsempfehlungen für die Umstellung einer bestehenden VPN-Infrastruktur auf eine schnellere und sicherere Zero Trust-Konnektivität für Remote-Benutzer zusammengestellt.

[1] *Riley, Steve, MacDonald, Neil, und Orans, Lawrence. „Market Guide for Zero Trust Network Access." Gartner Research, https://www.gartner.com/en/documents/3986053/market-guide-for-zero-trust-network-access. Letzter Zugriff am 21. Juni 2021. Siehe Tabelle 1 für weitere Einzelheiten.*

ANSATZ NR. 1: HERKÖMMLICHES VPN

Seit Jahrzehnten ermöglichen es VPNs Unternehmen, ihre Remote-Benutzer mit einem gewissen Maß an Privatsphäre und Sicherheit mit Unternehmensnetzwerken zu verbinden. Anwender müssen vertrauliche Informationen nicht mehr über das öffentliche Internet abrufen, wo jeder Angreifer Daten ausspähen oder stehlen könnte. Mit VPNs können sie über eine verschlüsselte Verbindung sicher auf interne Ressourcen zugreifen.

Die beiden gängigsten Arten der VPN-Implementierung sind clientbasierte VPNs und clientlose SSL-VPNs. Jede weist ihre eigenen Vor- und Nachteile auf:

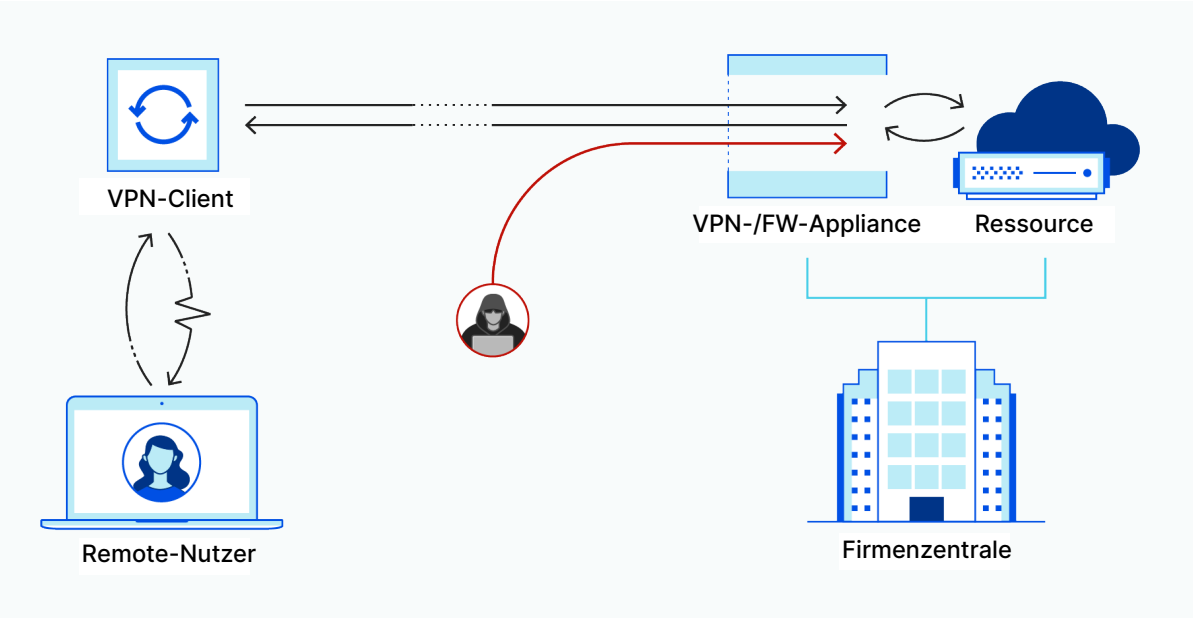
Clientbasierte VPNs verbinden Remote-Benutzer über einen verschlüsselten Tunnel mit einem privaten Netzwerk. Diese Verbindung wird über eine Softwareanwendung oder einen Client hergestellt. Dabei müssen sich die User einmal mit einem Benutzernamen und einem Passwort authentifizieren, um dauerhaften Zugriff auf alle Ressourcen innerhalb dieses Netzwerks zu erhalten.

Vorteil: Wenn Nutzer die Verbindung mit Anwendungen und internen Hosts einmal hergestellt haben, können sie sich im System lateral frei bewegen und rasch auf mehrere Ressourcen zugreifen.

Nachteile:

- **Nicht für Roaming-Benutzer und mobile Geräte konzipiert**. Wenn Benutzer unterwegs sind, verbinden sich sowohl ihre Laptops als auch ihre mobilen Geräte nahtlos neu, wenn die drahtlosen Netzwerke wechseln. VPN-Clients sind jedoch nicht in der Lage, diese Neuverbindungen reibungslos zu bewältigen, sodass Benutzer den VPN-Client immer wieder zum Neustart und zur erneuten Authentifizierung zwingen müssen. Dies führt zu Produktivitätsverlusten und verursacht IT-Tickets.
- **Mangelnde Übersicht.** Bei dieser Methode beendet die VPN-Infrastruktur den verschlüsselten Tunnel vom VPN-Client hinter der internen Firewall des Rechenzentrums. Obwohl diese Verbindungen protokolliert werden, gibt es keine anwendungsspezifischen, zentralisierten Protokolle, aus denen hervorgeht, auf welche Anwendungen die Benutzer zugegriffen haben oder welche Aktionen sie innerhalb der Anwendung durchgeführt haben.

Clientless SSL-VPN-Portale erlauben es einigen wenigen Remote-Benutzern, sich mit manchen browserbasierten Anwendungen innerhalb eines privaten Netzwerks zu verbinden. Ermöglicht wird diese Verbindung durch einen Webserver, der in die Netzwerk-Appliance integriert ist, auf der der VPN-Dienst läuft.	**Vorteil:** Anstatt einen Client auf einem Gerät zu verwenden, kann jeder Webbrowser das SSL-Zertifikat des Portals nutzen. So lässt sich eine verschlüsselte HTTPS-Verbindung herstellen, um Auftragnehmer auf nicht verwalteten Geräten zu unterstützen. **Nachteile:** • **Sicherheitsbedenken.** Die meisten VPN-Konfigurationen innerhalb des Rechenzentrums gewähren den Benutzern uneingeschränkten Zugriff. Dies stellt ein Problem für Unternehmen dar, die nicht wollen, dass Auftragnehmer und andere externe Arbeitskräfte uneingeschränkten Zugriff auf sensible Ressourcen und Anwendungen erhalten. • **Nicht auf eine hohe Anzahl simultaner Benutzer ausgelegt.** Im Gegensatz zu modernen Cloud-Diensten kann der Webserver des Portals nicht elastisch skaliert werden, um eine höhere Nachfrage zu befriedigen. Stattdessen müssen mehr Netzwerk-Appliances installiert und die Last verteilt werden, um das Portal zu skalieren. Das ist oft teuer, kompliziert und ineffektiv, da die übrigen Funktionen der Appliance möglicherweise nicht ausreichend genutzt werden. • **Bei Clientless SSL-VPN-Portalen sind Firewall-Ports und Webserver Angriffen ausgesetzt.** Damit der Webserver, auf dem das Portal gehostet wird, interne Anwendungen erreichen kann, müssen Administratoren Eingangs-Ports der Firewall öffnen und sie damit externen Angriffen aussetzen. Sowohl die offenen Ports als auch der Webserver selbst müssen vor DDoS- und Webanwendungsangriffen geschützt werden, was eine komplexere Konfiguration erfordert und höhere Kosten mit sich bringt.



VPNs bieten zwar grundlegenden Datenschutz für Remote-Benutzer, wurden aber nicht mit Blick auf Sicherheit oder Skalierbarkeit entwickelt. Traditionell haben Unternehmen VPNs eingesetzt, um einige wenige Remote-Benutzer für kurze Zeit mit dem Unternehmensnetzwerk zu verbinden. Mit der zunehmenden Verbreitung von Remote-Arbeit steigt jedoch auch die Zahl der VPN-Probleme:

- **Benutzer registrieren eine unzureichende Performance.** Wenn die VPN-Infrastruktur nicht über die Kapazität verfügt, den von den Mitarbeitern erzeugten Traffic-Durchsatz und die gleichzeitigen Verbindungen zu bewältigen, verlangsamt sich die Internetverbindung der Benutzer. Sind VPNs sowohl vom User als auch vom Anwendungsserver, auf den er zuzugreifen versucht, weit entfernt, führt die daraus resultierende Übertragungszeit außerdem zu höherer Latenz.
- **Unternehmensnetzwerke sind anfällig für Angriffe.** VPNs verwenden in der Regel eine perimeterbasierte Architektur („Castle-and-Moat-Modell“, „Burg und Burggraben“), bei der ein Benutzer uneingeschränkten Zugang zu allen Unternehmensressourcen erhält, sobald er sich mit einem Netzwerk verbindet. Da es keine integrierte Methode gibt, um den Zugriff auf kritische Infrastrukturen und Daten zu begrenzen, müssen Unternehmen kostspielige und komplexe Sicherheitsdienste wie Firewalls der nächsten Generation und Netzwerkzugangskontrollen konfigurieren. Anderenfalls sind sie anfällig für böswillige laterale Bewegungen, die zu größeren Datenschutzverletzungen führen.

Das Problem mit gehosteten VPN-Diensten

Einige Anbieter haben die Netzwerk-Appliance, auf der der VPN-Dienst läuft, in die Public Cloud verlagert. Dort wird sie als virtuelle Maschine (VM) in einem oder mehreren Rechenzentren betrieben.
Das VPN kann mit zusätzlichen Sicherheitsdiensten gebündelt (oder mit diesen gekoppelt) sein, muss es aber nicht.

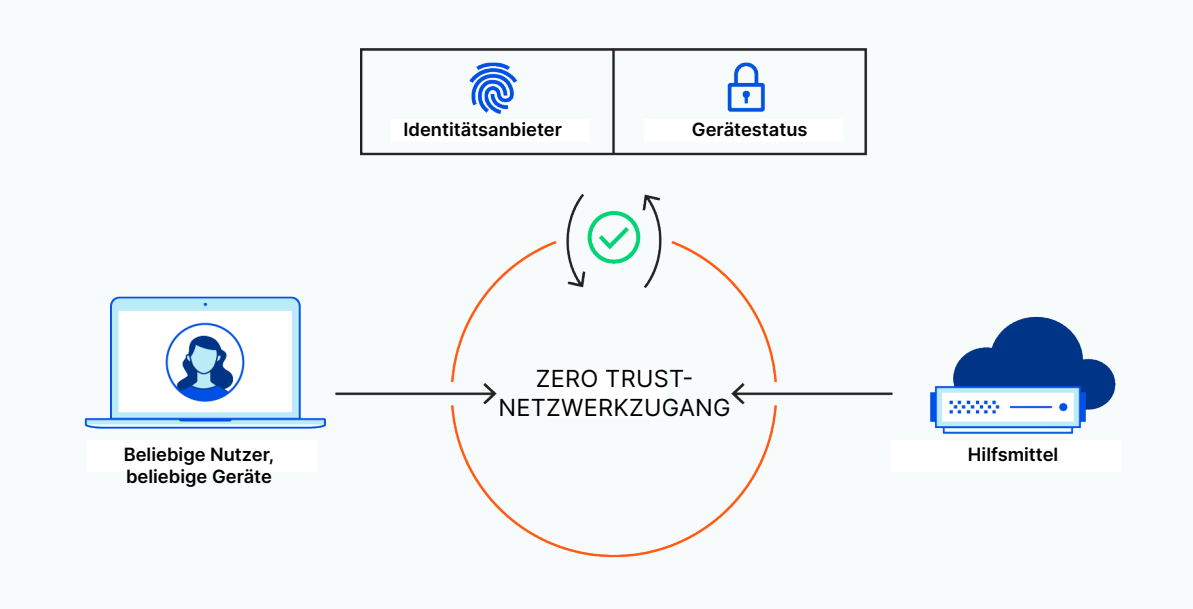
Die Auslagerung eines VPN in die Cloud scheint einige der bei Hardware-VPN-Appliances auftretenden Skalierungsprobleme zu lösen. Sie bringt jedoch auch erhebliche Herausforderungen in Bezug auf Sicherheit und Skalierbarkeit mit sich.

Nehmen wir zum Beispiel ein Unternehmen, das eine vollständige NGFW (Next Generation Firewall, Firewall der nächsten Generation) hostet, bei der das VPN mit einer Firewall und zusätzlichen Sicherheitsfunktionen kombiniert wird. Da die NGFW als Komplettpaket angeboten wird, ist es nicht möglich, bestimmte Funktionen bei Bedarf unabhängig zu skalieren. Vielmehr ist in diesem Fall die Skalierung des gesamten Diensts erforderlich. Dazu müssen mehr VMs hochgefahren werden, um einen kleinen Teil der Rechenlast jeder VM umzuverteilen. Dies ist nicht nur eine unpraktische und unhandliche Lösung, sondern verursacht wahrscheinlich auch hohe Kosten, wenn die Anforderungen des Unternehmens an den Fernzugriff weiter steigen.

ANSATZ NR. 2: ZERO TRUST-NETZWERKZUGANG (ZTNA)

Zero Trust-Sicherheit vermeidet viele der mit VPN verbundenen Nachteile. Sie beruht auf dem Prinzip, dass keinem Benutzer oder Gerät innerhalb oder außerhalb eines Netzwerks standardmäßig vertraut werden kann. Um das Risiko und die Auswirkungen von Datenschutzverletzungen, internen Angriffen und anderen Bedrohungen zu reduzieren, gilt bei einem Zero Trust-Ansatz Folgendes:

- jede Anmeldung und Anfrage wird authentifiziert und protokolliert
- alle Benutzer und Geräte müssen sich verifizieren
- die Informationen, auf die jeder Benutzer und jedes Gerät zugreifen kann, werden je nach Identität und Kontext eingeschränkt
- eine Ende-zu-Ende-Verschlüsselung wird hinzugefügt, um Anwendungen und Daten innerhalb des Netzwerks zu isolieren



Wie bei VPN gibt es auch bei ZTNA mehrere Konfigurationsmöglichkeiten:

1. **Bei einem clientlosen (oder durch den Dienst initiierten) ZTNA** wird anstelle eines Clients der vorhandene Browser verwendet, um eine sichere Verbindung herzustellen und Benutzergeräte zu authentifizieren. Traditionell war der clientlose ZTNA auf Anwendungen mit HTTP/HTTPS-Protokollen beschränkt, aber die Kompatibilität wird schnell erweitert.[2]
   - **Vorteil:** Der clientlose ZTNA nutzt eine Reverse-Proxy-Verbindung, um den direkten Zugriff auf Anwendungen zu verhindern. So wird Benutzern der Zugang zu Applikationen und Daten verwehrt, für die sie keine Berechtigung haben, und Administratoren erhalten mehr Kontrolle und Flexibilität bei der Verwaltung.
2. **Im Fall eines clientbasierten (oder vom Endpunkt initiierten) ZTNA** wird Software auf einem Benutzergerät installiert, bevor eine verschlüsselte Verbindung zwischen dem kontrollierenden Agenten und autorisierten Anwendungen hergestellt werden kann.
   - **Vorteil:** Ein clientbasierter ZTNA ermöglicht Administratoren einen besseren Überblick über den Gerätestatus, den Standort und den Risikokontext von Benutzern, die auf Anwendungen zugreifen, sodass detailliertere Richtlinien erstellt und durchgesetzt werden können. Da diese Methode nicht auf HTTP/HTTPS beschränkt ist, kann sie auch für den Zugriff auf eine breitere Palette von Nicht-HTTP-Anwendungen verwendet werden – z. B. solche, die auf SSH, RDP, VNC, SMB und andere TCP-Verbindungen angewiesen sind.

[2] Mit Stand vom Juni 2021 unterstützt die ZTNA-Lösung von Cloudflare den clientlosen Zugriff auf SSH- und VNC-Anwendungen; die Unterstützung von RDP ist geplant.

Schwierigkeiten bei der ZTNA-Implementierung

ZTNA bietet zwar eindeutige Vorteile gegenüber herkömmlichen VPNs, ist aber kein makelloser Ansatz zur Sicherung des Netzwerkzugangs für Remote-Benutzer. Unternehmen müssen die Vor- und Nachteile der Einführung des Zero Trust-Modells abwägen. Dabei können sie auf eine oder mehrere der folgenden Herausforderungen stoßen:

Die Lösungen sind nicht wirklich cloudnativ

Wenn ein Anbieter keinen cloudbasierten ZTNA anbietet, müssen seine Kunden die Software in ihren eigenen Rechenzentren installieren. In diesem Fall entgehen den Benutzern wichtige Vorteile wie eine sofortige Skalierbarkeit und unbegrenzter Durchsatz.

Dienstleister bieten möglicherweise keine clientbasierten und clientlosen ZTNA-Optionen an

Dies schränkt den Wert für Unternehmen ein, die Benutzer mit Nicht-HTTP-Applikationen wie Remote-Desktops, SSH-Anwendungen oder Filesharing-Diensten verbinden müssen.

Die Konfiguration kann kompliziert und zeitaufwändig sein

Anbieter, die keine Unterstützung für die Orchestrierung und Automatisierung von Richtlinien (in Form von Tools wie Terraform) bieten, können den Administratoren mehr manuelle Arbeit aufbürden – zusätzlich zu der Konfiguration, die bereits in einem Identitätsanbieter erfolgt.

DER CLOUDFLARE-ANSATZ FÜR DEN FERNZUGRIFF

Die Sicherung und Skalierung des Fernzugriffs sollte reibungslos verlaufen, das System nicht mit schwerfälligen Sicherheitslösungen überfrachten und weder Performance-Einbußen noch unnötige Kosten verursachen. Cloudflare versetzt Teams in die Lage, alle Anwendungsfälle des Fernzugriffs zu bewältigen, mit den folgenden Vorteilen:

- **Einfaches, risikoloses Onboarding für Benutzer und Administratoren.** Cloudflare lässt sich problemlos mit bestehenden Identitätsanbietern und Endpunktschutzplattformen kombinieren, um Zero Trust-Richtlinien durchzusetzen, die den Zugriff auf Unternehmensanwendungen und -ressourcen beschränken.
- **Flexibilität für clientbasierte und clientlose ZTNA-Implementierungen**. Cloudflare bietet clientlose Unterstützung für Verbindungen zu Web-, SSH-, VNC- (und bald auch RDP-) Anwendungen sowie clientbasierte Unterstützung für Nicht-HTTP-Anwendungen und privates Routing zu internen IPs.

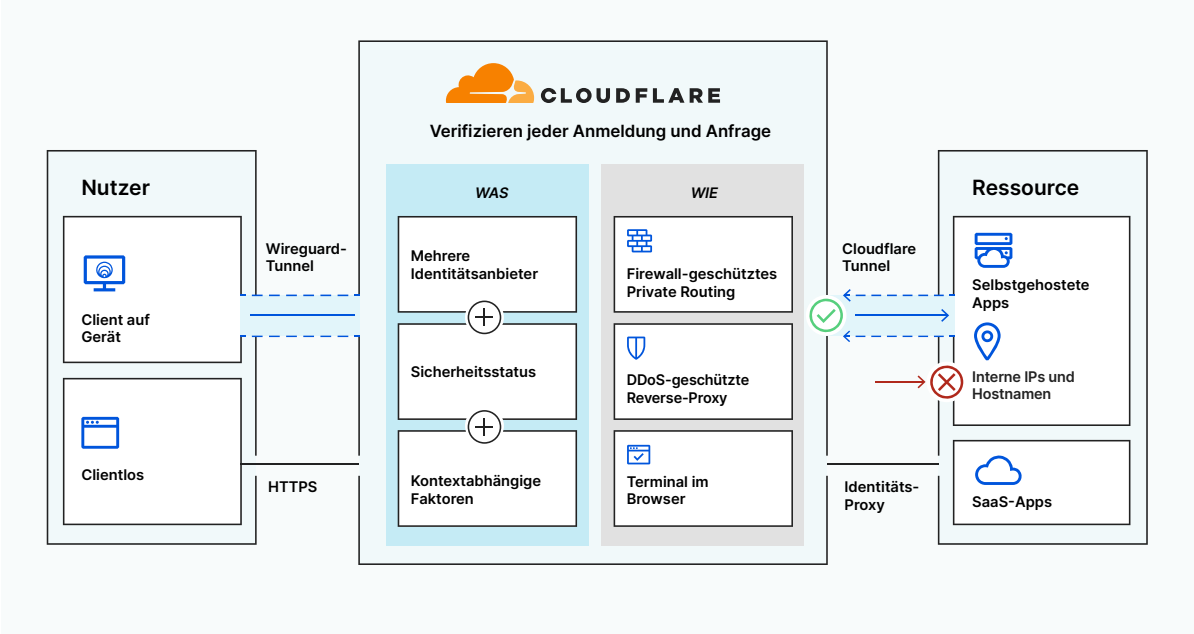


Tabelle 1: Wie Cloudflare die Herausforderungen beim Fernzugriff angeht

⚠ Problem	✓ Lösung	⚙ Umsetzung durch Cloudflare
Schwer zu skalieren	Globales Edge-Netzwerk	Skalierungsprobleme plagen sowohl VPNs als auch ZTNA-Dienste, die nicht cloudnativ sind, und erschweren den Zugriff auf Anwendungen und Daten für Remote-Benutzer. Das globale Anycast-Netzwerk von Cloudflare ermöglicht den Benutzern schnellere Verbindungen als ein VPN. Außerdem sorgt es dafür, dass Remote-Teams jeder Größe bei Bedarf sicher und zügig auf Unternehmensressourcen zugreifen können – ohne zusätzliche zeitaufwändige Konfiguration durch Administratoren.
Schlechte Kompatibilität mit Mobilgeräten	Schlanker Client	VPNs und ZTNA-Lösungen, die IPSec- und SSL-Protokolle nutzen, erreichen auf Mobil- und Roaming-Geräten oft nur eine schlechte Performance. Der WARP-Client von Cloudflare verwendet deshalb das modernere Wireguard-Protokoll. Dieses wird im Userspace ausgeführt, um eine breitere Palette von Betriebssystemoptionen zu unterstützen, die das System für die Nutzer schneller machen. Der WARP-Client von Cloudflare kann auf Windows-, MacOS-, iOS-, Android- und bald auch auf Linux-Geräten konfiguriert werden.
Kein integrierter oder nur schwacher DDoS-Schutz	Branchenführender integrierter DDoS-Schutz	Ohne integrierten DDoS-Schutz sind Unternehmen oft gezwungen, zusätzliche Sicherheitsdienste miteinander zu verketten, was Konfigurations-, Skalierungs- und Sicherheitsprobleme verursachen kann. Das mehr als 67 Tbit/s-schnelle Cloudflare-Netzwerk bietet integrierten DDoS-Schutz für jeden ZTNA-Modus und verteidigt Netzwerke gegen die größten volumetrischen Angriffe.
Beschränkungen des Protokolls	Unterstützung für Anwendungen außerhalb des Web	✓ Modus-Kompatibilität: clientloser ZTNA für SSH/VNC-Anwendungen; clientbasierter ZTNA für alle anderen Anwendungen außerhalb des Web
Keine integrierte Netzwerk-Firewall	Integrierte Netzwerk-Firewall	Mit zunehmender Größe der Unternehmensnetzwerke wird auch mehr Sicherheitshardware benötigt, deren Rechenlast geschultert werden muss. Die Folge sind Abstriche hinsichtlich Kosten, Performance und Sicherheit. Cloudflare ermöglicht es Administratoren, Richtlinien für Netzwerk-Firewalls am Netzwerkrand durchzusetzen. So können sie genau kontrollieren, welche Arten von Daten ihr Netzwerk erreichen und verlassen. Außerdem erhalten sie einen besseren Einblick in den Datenverkehr im Netzwerk. ✓ Modus-Kompatibilität: clientbasierter ZTNA
Mangel an präziser Steuerung	Integriertes Secure Web Gateway (SWG)	Die unerlaubte Nutzung von Anwendungen kann erhebliche Sicherheitsprobleme für Unternehmen verursachen. Ohne strenge Richtlinien haben Benutzer die Möglichkeit, auf sensible Daten und andere Unternehmensressourcen zuzugreifen und diese zu manipulieren. Die Kombination von ZTNA mit SWG ermöglicht Administratoren eine präzisere Kontrolle von Benutzern und Gerätezugriffsrechten innerhalb von Anwendungen. So haben User und rollenbasierte Gruppen nur Zugriff auf die Ressourcen, die sie benötigen. ✓ Modus-Kompatibilität: clientbasierter ZTNA

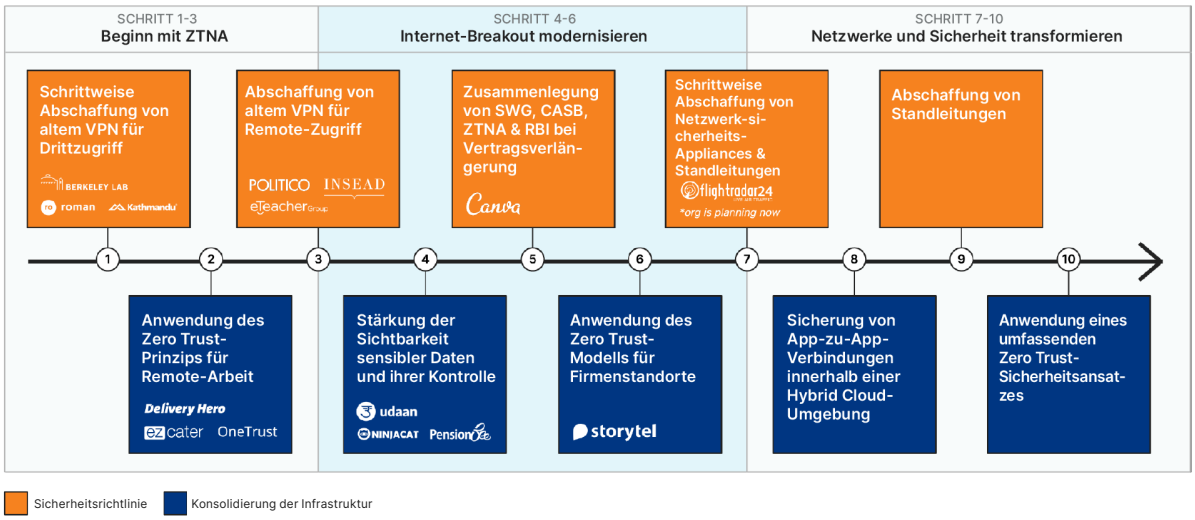
DER WEG VON VPN ZUM ZERO TRUST-NETZWERKZUGANG

Die Verheißungen von Zero Trust können für IT-Sicherheitsverantwortliche während einer langen und mühsamen Umstellung auf VPN-freie Sicherheitslösungen an Glanz verlieren. Aber es ist möglich, ein VPN ohne Abstriche bei der Protokollunterstützung oder Funktionalität durch Zero Trust-Netzwerkzugang zu ersetzen.

Der empfohlene Migrationspfad hängt von den geschäftlichen Prioritäten eines Vorhabens ab:

- Wenn eine schnellere Verbindung zu Anwendungen Priorität hat, sollte **clientbasierter ZTNA zuerst für Applikationen außerhalb des Web** eingeführt werden.
- Steht die Verbesserung der Sicherheit der Anwendungszugriffregeln ganz oben auf der Liste? Dann sollten **Webanwendungen** zuerst an die Reihe kommen.

Der Ersatz des VPN ist nur der erste Schritt bei einer umfassenden Umgestaltung eines Netzwerks. Da die Umstellung auf ein SASE-Modell schier unmöglich erscheinen kann, möchten wir einen gängigen Weg zur Zero Trust-Sicherheit auf Grundlage der von unseren Kunden gewählten Vorgehensweise aufzeigen:



Erfahren Sie mehr darüber, wie Sie mithilfe der Zero Trust-Plattform von Cloudflare erst die Abhängigkeit von Ihrem VPN verringern und es schließlich ersetzen können.

Mehr dazu

Sehen Sie sich einen Vergleich zwischen VPN und ZTNA aus der Praxis an und erfahren Sie, wie Cloudflare Access die Sicherheit für den Anwendungszugriff erhöht.

Demo ansehen

ANHANG

Modernisierung integrierter Internetzugänge

Die Implementierung von ZTNA ist ein wichtiger Schritt bei der Einführung eines Secure Access Service Edge (SASE)-Modells. **Cloudflare One** ist eine umfassende Network as a Service (NaaS)-Lösung, die Unternehmensnetzwerke für Teams jeder Größe vereinfacht und absichert. Mit Cloudflare One können Unternehmen:

- **Zero Trust-Zugriff nutzen.** Breite Sicherheitsperimeter werden durch eine Eins-zu-eins-Überprüfung jeder Anfrage an jede Ressource ersetzt. Zero Trust-Regeln können bei jeder Verbindung zu den Unternehmensanwendungen durchgesetzt werden – unabhängig davon, wo sich die Nutzer befinden und wer sie sind.
- **Internet-Traffic sichern.** Wenn sich Bedrohungen im Internet schnell weiterentwickeln, müssen Abwehrmaßnahmen ihnen unbedingt immer einen Schritt voraus sein. Cloudflare One schützt Remote-Mitarbeiter vor Gefahren aus dem Netz und setzt Richtlinien durch, die verhindern, dass wertvolle Daten das Unternehmen verlassen. Dies geschieht durch die Durchsetzung der Zero Trust-Browserisolierung auf jeder Website – mit einem reibungslosen und blitzschnellen Benutzererlebnis.
- **Büros und Rechenzentren schützen und vernetzen.** Unternehmensnetzwerke sind allzu kompliziert geworden. Das führt dazu, dass der Nutzer-Traffic bis zu seinem Bestimmungsort oft mehrere Stationen durchlaufen muss. Mit Cloudflare One können Unternehmen solche Standorte über eine einheitliche Cloud-Plattform schützen.

Sie möchten mehr über Cloudflare One erfahren? Dann ist unsere zehnminütige Einführung mit Demo das Richtige für Sie.

Umgestaltung des Netzwerks

In Kürze werden die Zero Trust- und WAN as a Service-Angebote von Cloudflare zusammengeführt, sodass Beschäftigte durchgängig auf Unternehmensressourcen zugreifen können – egal, wo sie gerade arbeiten.

Aktuell ermöglichen VPN- und WAN-Produkte Mitarbeitern den Zugriff auf Ressourcen, die sich innerhalb des privaten Unternehmensnetzwerks befinden. Aber sie zwingen Sie dazu, Konnektivität und Sicherheitsrichtlinien auf andere Weise zu verwalten.

Doch nun bietet Cloudflare eine einheitliche Kontrollebene mit größerer Flexibilität, damit dieselben Zero Trust-Sicherheitsrichtlinien auf die gesamte Belegschaft und sämtliche Arbeitsplätze eines Unternehmens angewandt werden können und sich Firmen nicht mehr mit diversen Einzelprodukten plagen müssen.

Mehr erfahren Sie unter https://www.cloudflare.com/de-de/cloudflare-one/.