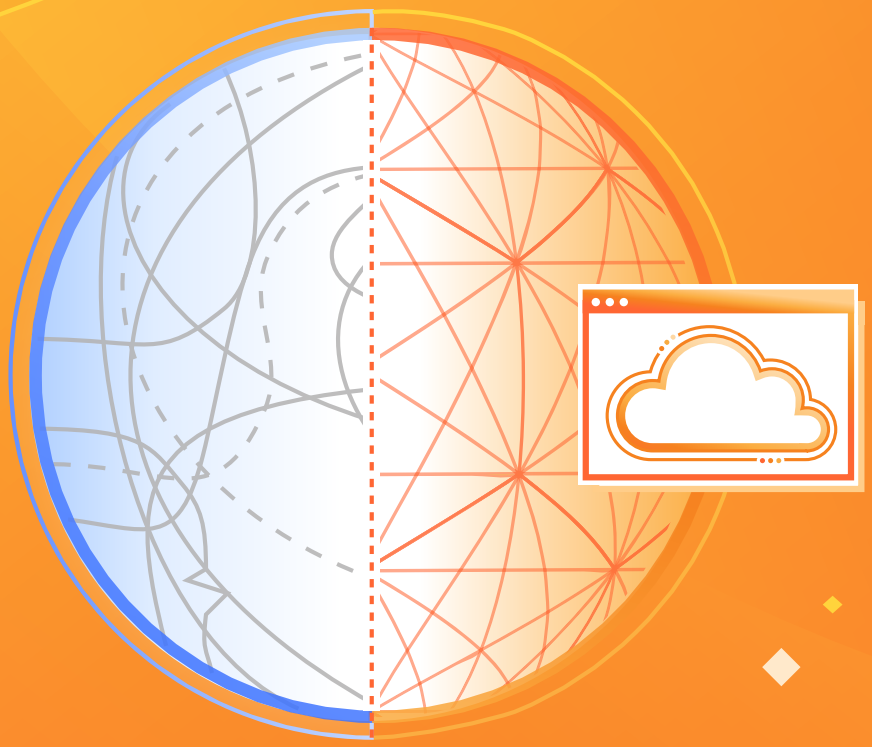
CLOUDFLARE

WHITEPAPER

Eine Strategie für die Modernisierung Ihres Netzwerks



Inhalt

3 **Alte Netzwerke – eine Hürde für die digitale Modernisierung**

4 **Die notwendigen Schritte**

5 **Vier Hauptpfade des Netzwerk-Traffics**

6 **Die Connectivity Cloud von Cloudflare**

7 **Wichtige Anwendungsbereiche der Netzwerkmodernisierung**

7 Anbindung von Zweigstellen

8 Schutz öffentlich zugänglicher Infrastruktur

9 Vereinfachung des Firmennetzwerks

9 Abschaffung der DMZ

10 Ersatz von VPN durch ZTNA

10 Beseitigung von übermäßigem Vertrauen im LAN

10 Schnellere Anbindung bei Fusionen und Übernahmen

11 Vernetzung und Absicherung von Clouds

12 **Nächste Schritte**

Alte Netzwerke – eine Hürde für die digitale Modernisierung

Wenn sich die Geschäftsbedingungen von einem Tag auf den anderen ändern können, ist Agilität ein Muss. Doch Anpassungsfähigkeit ist nicht nur auf Führungs- und Entscheidungsebene verlangt. Die gesamte Firma muss in der Lage sein, sich zu wandeln. Voraussetzung dafür sind Systeme, die sich modifizieren lassen, ohne dabei zusammenzubrechen. Ein Unternehmen muss sich auf andere Ertragsmodelle einstellen, neue Anwendungen unterstützen und Menschen auf der ganzen Welt miteinander vernetzen können.

Eine größere Flexibilität ist eines der Hauptziele digitaler Modernisierungsprojekte, bei denen Unternehmen umrüsten, um Wettbewerbsvorteile zu erlangen. Das gilt insbesondere für herkömmliche Firmennetzwerke, denen bei der Ermöglichung von Kommunikation und Zusammenarbeit eine zentrale Rolle zukommt. Bislang hat sich das Firmennetzwerk Veränderungen beharrlich widersetzt, und das aus gutem Grund. Schließlich wurde es entwickelt, um Erschütterungen im System standzuhalten. Zudem sind Veränderungen mit großen Kosten und Anstrengungen verbunden.

Manchmal kann man sich darauf vorbereiten, weil sie sich allmählich vollziehen. Ein Beispiel dafür sind die Auswirkungen der Cloud-Einführung auf Rechenzentren. Bei Netzwerken jedoch treiben externe Marktkräfte einen schnellen Wandel voran, der manchmal sogar praktisch über Nacht erfolgt. In der Pandemie hat sich beispielsweise gezeigt, wie schwierig für einige Firmen die schnelle Erweiterung der Kapazitäten für produktives Arbeiten im Homeoffice war. Gleichzeitig musste man in Anbetracht des großen Anteils am Budget, der durch ungenutzte Netzwerkkapazität in leeren Büros verschlungen wurde, die Kosten im Griff behalten.

Manche Unternehmen waren dieser Herausforderung aber sehr wohl gewachsen: Sie haben sich nicht nur angepasst, sondern waren dabei auch noch geschäftlich erfolgreich. Das war nicht nur richtigen Entscheidungen in den Führungsetagen zu verdanken, sondern auch der Wandlungs- und Umsetzungsfähigkeit der jeweiligen Firmen. CIO können daraus die Lehre ziehen, dass sie Veränderungsstrategien entwickeln und zur Unterstützung künftiger Bedürfnisse technisch umrüsten müssen. Sie sollten kurz gesagt dafür sorgen, dass die IT den Wandel nicht verzögert, sondern beschleunigt.

Doch angesichts enormer Investitionen in lokale Netzwerke fällt die Entscheidung für eine Modernisierung nicht leicht. Um deren Vorteile voll ausschöpfen zu können, muss man zunächst Ziele definieren. Anhand dieser lässt sich dann in Erfahrung bringen, welche Änderungen erforderlich sind.

Die notwendigen Schritte

Wenn man sich ansieht, wie sich die Best Practices der Netzwerkgestaltung im Lauf der Zeit gewandelt haben, gibt es einen guten Grund für die große Komplexität. Jahrzehntelang haben Unternehmen ihre Netzwerke Schicht um Schicht mit neuer Technik ausgebaut und verstärkt. Mit jeder neuen Generation und Innovation im Bereich Netzwerktechnik hat das Netzwerk an Komplexität gewonnen. Eine Möglichkeit zur Vereinfachung gab es nicht.
Oft wurde es durch das Hinzufügen von Technik sogar noch komplizierter, die Geschwindigkeit, Widerstandskraft und Sicherheit von Systemen zu gewährleisten.

Mit Netzwerk- und Sicherheitsdiensten, die über die Cloud bereitgestellt werden, stehen wir nun am Anfang des nächsten Generationswechsels bei Firmennetzwerken. Denn wenn Unternehmen cloudbasierte Dienste als Verlängerung ihres Netzwerks nutzen, können sie neue Anwendungsfälle abdecken, ihre Reichweite erhöhen und Applikationen weit über Rechenzentren hinaus absichern. Damit bietet sich ihnen die Möglichkeit, ihr Netzwerk stark zu vereinfachen, weil die Bereitstellung von Services über die bereits bestehende Verbindung des Netzwerks zu dem PoP des Cloud-Dienstleisters erfolgt und somit keine Unterbrechung dieser Verbindung zur Einbindung weiterer Appliances erforderlich ist. An den Abläufen zwischen dem lokalen Netzwerk und dem Cloud-Dienst ändert sich nichts, während die cloudbasierten Services integriert und genutzt werden.

Das Problem besteht darin, dass nicht jede über die Cloud bereitgestellte Netzwerk- und Sicherheitsplattform auf die gleiche Art und Weise aufgebaut ist. Zudem sind die Unterschiede oft nicht ohne Weiteres erkennbar. Viele lassen sich durch Modernisierungsmaßnahmen nur begrenzt optimieren. Um die Unterschiede zu erkennen, müssen die Ziele der Netzwerkmodernisierung klar definiert werden. Nur so lässt sich verhindern, dass man ein kompliziertes System durch ein anderes, nicht weniger komplexes ersetzt.

Vier Hauptpfade des Netzwerk-Traffics

Um den erforderlichen Umfang eines Projekts zur Netzwerkmodernisierung zu ermitteln, sollte man sich bewusst machen, dass ein Netzwerk eine große Zahl an Kontaktpunkten abdeckt. Bei einigen von diesen bestehen infrastrukturelle Überschneidungen (wenn sich zum Beispiel eingehender, ausgehender und interner Traffic eines Kernnetzwerks an einem Punkt kreuzen), andere befinden sich außerhalb (wie im Fall von Public Cloud-Netzwerken).

Eingehender Traffic: Da bestimmte Bereiche des Netzwerks über das Internet zugänglich sind, müssen Schutzvorkehrungen getroffen werden, damit eingehender Datenverkehr das Unternehmen nicht lahmlegen oder missbrauchen kann. Gleichzeitig muss aber auch sichergestellt sein, dass der Traffic legitimer Nutzer weiterhin sein Ziel erreicht. Abwehrmaßnahmen des klassischen Perimetermodells sind erstens nicht unüberwindbar und erfordern zweitens Kapazitäten zur Bewältigung von DDoS-Angriffen.

Ausgehender Traffic: Verbindungen mit dem Internet und cloudbasierten Anwendungen erfordern Richtlinien, die Leitplanken für sichere Geschäftspraktiken bieten – etwa den Schutz vor Bedrohungen und Datenausschleusung. Weil sich die Nutzer an den unterschiedlichsten Orten befinden können, haben Unternehmen eine Kombination aus verschiedenen nach außen gerichteten Sicherheitstechnologien implementiert. Dazu gehören lokale Appliances wie Firewalls (wenn sich der Nutzer im Netzwerk befindet), DNS-Resolver-Dienste sowie cloudbasierte Proxys wie Secure Web Gateway und CASB (für Remote-Nutzer).

WAN-Netzwerke: Das WAN und der von ihm abgedeckte Bereich (der sowohl die Zentrale als auch Zweigstellen umfasst) werden so umgestaltet, dass sie „Cloud First"-Initiativen und IoT-fähige Geräte unterstützen. Bei herkömmlichen Netzwerkstrukturen wird die Umleitung der Daten zu Rechenzentren zugunsten direkt mit dem Internet kommunizierender Architekturen vermieden. Die in diesen Bereichen der Netzwerktechnologie zu verzeichnenden rasanten Fortschritte haben die Integration des Sicherheitsaspekts paradoxerweise komplizierter gemacht. In vielen Fällen hängt der Weg, den der Datenverkehr intern einschlägt, nach wie vor von Sicherheitsappliances an der Edge ab. Das behindert Unternehmen, die Veränderungen vorantreiben wollen.

Public Cloud-Netzwerke: Unternehmen nutzen zum Aufbau ihrer Anwendungen mehrere Clouds. Dadurch wird es immer schwieriger, zeit- und ressourcenaufwendiger, Netzwerk- und Sicherheitskonfigurationen für Direktverbindungen einzurichten und zu verwalten. Insbesondere die Zeit sollte besser in die Projektentwicklung investiert werden.

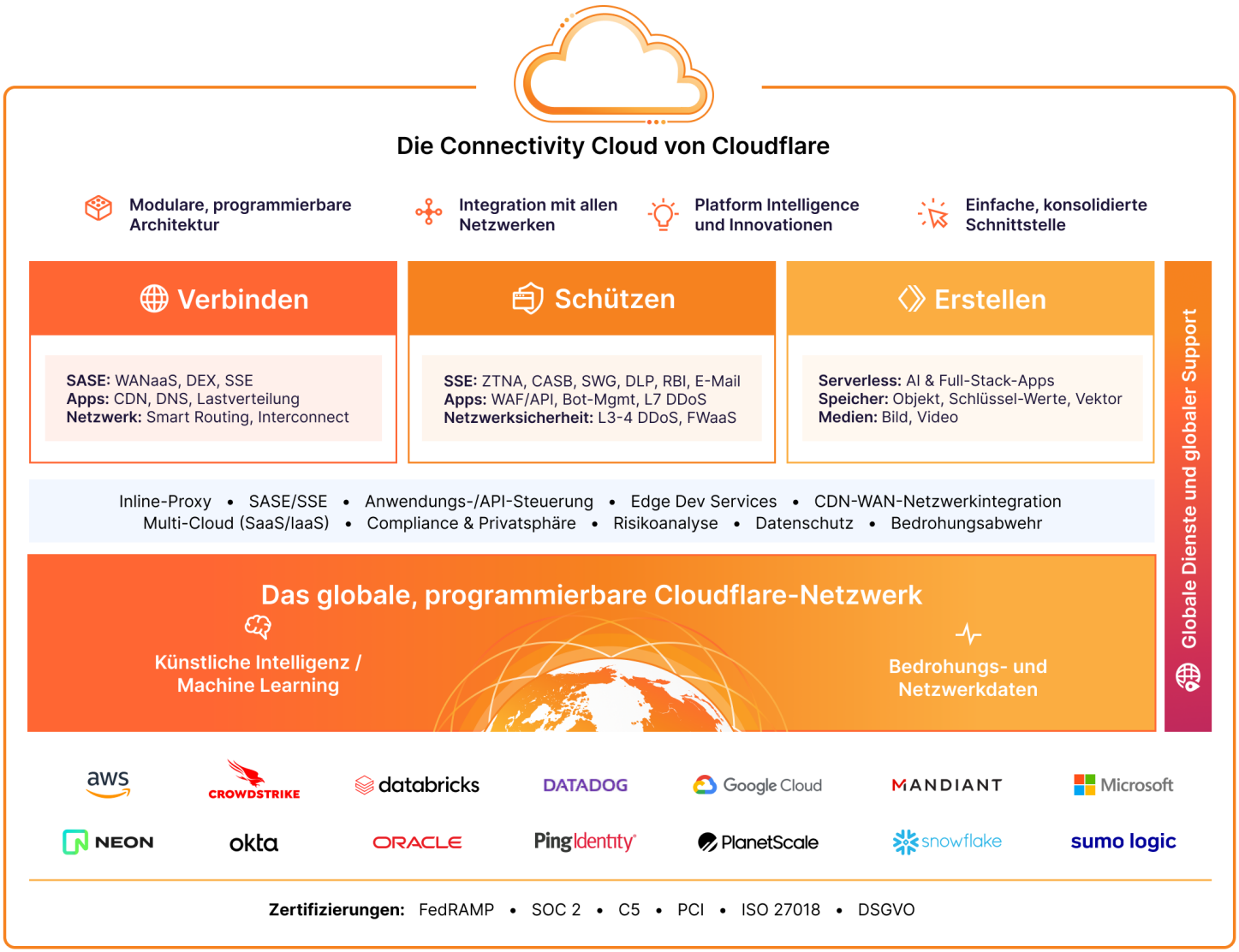
Für jeden dieser Traffic-Pfade stehen Unternehmen eine Reihe von Technologien zur Verfügung, die sie in ihrem Netzwerk implementieren oder über die Cloud einsetzen können. Bei Modernisierungsprojekten sind solche Pfade in unterschiedlichen Richtungen betroffen. Deshalb müssen bei der Planung solcher Upgrades sämtliche Richtungen einbezogen werden. Sonst drohen Fehler in der Architektur, aufgrund derer sich die Vorteile einer solchen Transformation nicht voll ausschöpfen lassen oder bestimmte Anwendungsfälle nicht berücksichtigt werden, weshalb dann weitere Technologien eingesetzt werden müssen.

Die Connectivity Cloud von Cloudflare

Für die Modernisierung Ihres Netzwerks sollten Sie die Connectivity Cloud von Cloudflare in Erwägung ziehen. Diese stellt mit einer modularen, programmierbaren Architektur Netzwerks- und Sicherheitsdienste für Nutzer und sämtliche cloudfähigen Infrastrukturen und Anwendungen eines Unternehmens bereit. So lassen sich nicht nur die Modernisierungsanforderungen der Gegenwart, sondern auch der Zukunft erfüllen.

Dank Cloudflare sind Dienste ohne die Einbindung zusätzlicher Appliances verfügbar. So können Funktionen ergänzt und neue Anwendungsfälle unterstützt werden. Die Verbindung zu einem Anycast-Rechenzentrum von Cloudflare bleibt die gleiche, während Sie über eine gemeinsame Verwaltungsschnittstelle zur Traffic-Verarbeitung Dienste konfigurieren und bereitstellen können. Auf diese Weise lässt sich der aktuelle Bedarf decken, während gleichzeitig eine Plattform zur Unterstützung künftiger Anwendungsfälle und der gesamten Netzwerkmodernisierung aufgebaut wird.

Anstatt Ihre eigene Infrastruktur rund um den Globus auszubauen, nutzen Sie doch einfach unsere. So profitiert Ihr Unternehmen von der Spitzengeschwindigkeit des globalen Cloudflare-Netzwerks, das mit Direktverbindungen zu nahezu jedem Service- und Cloud-Provider 95 Prozent aller Internetnutzer innerhalb von rund 50 ms erreichen kann.



Wichtige Anwendungsbereiche der Netzwerkmodernisierung

Beginnen Sie mit Anwendungsfällen, die für Ihre geschäftlichen Aktivitäten relevant sind und Ihrem Unternehmen den größten Nutzen bringen. Eine vorgeschriebene Reihenfolge gibt es dabei nicht, da jedes Unternehmen seine eigenen Prioritäten hat. Es kommt darauf an, dass Sie den kurzfristigen Anforderungen gerecht werden und gleichzeitig eine Architektur schaffen, die Ihre Netzwerkmodernisierung unterstützt. Auf welchem Weg Sie dies genau bewerkstelligen, ist nachrangig.

	Modernisierungsprojekte
Anbindung von Zweigstellen Kosten senken und Nutzererfahrung verbessern	• Von MPLS auf die Connectivity Cloud umstellen • Von SD-WAN auf die Connectivity Cloud umstellen
Schutz öffentlich zugänglicher Infrastruktur Lebensdauer von Investitionen in Firewalls und DMZ verlängern	• Beanspruchung von Netzwerk-Firewalls reduzieren • Sicherheit von der DMZ auf die Connectivity Cloud verlagern
Vereinfachung des Firmennetzwerks Zero Trust für höhere Sicherheit und geringere Investitionsausgaben implementieren	• Die DMZ verkleinern/abschaffen • VPN durch ZTNA ersetzen • Übermäßiges Vertrauen im LAN beseitigen • Anbindung bei Fusionen und Übernahmen beschleunigen
Vernetzung und Absicherung von Clouds Die Vorzüge jeder Cloud in Ihren Anwendungen nutzen	• Apps entwickeln und absichern • Kernfunktionen mit Entwicklungsdiensten bündeln

Anbindung von Zweigstellen

Eine wichtige Komponente bei WAN-Netzwerken ist die Eingliederung kleinerer Standorte wie Zweigstellen oder Filialen, die in der Lage sein müssen, Nutzer und Geräte mit Anwendungen zu verbinden. Bei herkömmlichen „Hub and Spoke"-Architekturen wurden Standorte über teure MPLS-Leitungen mit dem Rechenzentrum verbunden. Doch wegen eines wachsenden Bedarfs an Support für cloudbasierte Anwendungen nutzen immer mehr Unternehmen Architekturen, die per Breitband direkt mit dem Internet verbunden sind.

Mit SD-WAN wollte man die Zuverlässigkeit von Netzwerkverbindungen erhöhen, aber bei dieser Lösung wird dem Sicherheitsaspekt nicht vollständig Rechnung getragen. Die meisten SD-WAN-Architekturen greifen zur Durchsetzung von Sicherheitsrichtlinien über das SD-WAN-Netz auf schwerfällige Appliances an der Edge und lokale Firewalls zurück. Die SSE/SASE-Integration wird nur für den ausgehenden Datenverkehr verwendet.

Nutzen Sie die Connectivity Cloud von Cloudflare für die Anbindung von Zweigstellen und unterstützen Sie Ihren kompletten Migrationspfad, ob als Ergänzung oder als Ersatz für bestehende Services. Cloudflare verwendet für die Bereitstellung von Netzwerk- und Sicherheitsservices eine Architektur, die auf dem Ansatz „schlanke Edge / mächtige Cloud" beruht. Mit Cloudflare Magic WAN können Sie Verbindungen zwischen Netzwerkstandorten vereinfachen – seien es Zweigstellen, Geschäfte oder Produktionsstätten. Die Lösung bietet zur Verringerung der Kosten und Betriebskomplexität sichere und schnelle Verbindungen und Routing-Dienste für das Firmennetzwerk. Was die Sicherheit betrifft, wird Cloudflare Magic Firewall reibungslos zusammen mit Magic WAN eingesetzt. Das ermöglicht Ihnen die Durchsetzung von Netzwerkkontrollrichtlinien in Nord/Süd- oder Ost/West-Richtung, während der Datenverkehr das Netzwerk von Cloudflare durchläuft.

Schutz öffentlich zugänglicher Infrastruktur

Das Firmennetzwerk und die DMZ sind adressierbar und dem Internet ausgesetzt. Somit müssen Maßnahmen ergriffen werden, um Angreifer daran zu hindern, Schaden anzurichten. In einer perfekten Welt könnten herkömmliche Netzwerk-Firewalls den gesamten unerwünschten Datenverkehr prüfen und abweisen. Doch jede Firewall hat nur begrenzte Kapazitäten (verfügbare Bandbreite, Auslastung/Rechenleistung, Anzahl der Sitzungen usw.). Ob ein Angriff Erfolg hat, hängt von seiner Größenordnung ab. Die Frage ist, ob er so stark ausfällt, dass das Unternehmen nicht mehr auf verschiedenen Netzwerkprotokollebenen arbeiten kann.

Dabei geht es nicht nur um die Menge des Datenverkehrs. Durch die Aufnahme von eingehendem Traffic wird eine Angriffsfläche für nicht authentifizierten/vorauthentifizierten Datenverkehr geschaffen. Schwachstellen in Anwendungen und Betriebssystemen können von einem Angreifer selbst dann ausgenutzt werden, wenn er kein Konto für das System hat. Eine weitere große Gefahrenquelle ist Credential Stuffing, der Missbrauch bekannter Benutzernamen/Passwörter aus anderen Datenlecks. Durch die Anwendung der Zero Trust-Prinzipien auf Applikationen in der DMZ können Unternehmen die Gefahr, die das Internet darstellt, verringern oder eventuell sogar ganz neutralisieren.

Durch eine mehrschichtige Verteidigung („Defense in Depth“) lässt sich der Schutz des Netzwerks verbessern und bösartiger Datenverkehr noch vor der öffentlich zugänglichen Infrastruktur abfangen.
Die Cloudflare-Lösung Magic Transit mit der integrierten Magic Firewall, die über das Anycast-Netzwerk bereitgestellt werden, fungieren als Eingangstür zum Unternehmen. Sie filtern schädlichen und überflüssigen Datenverkehr heraus und lassen nur unbedenklichen Traffic passieren.

Wenn Netzwerk-Firewalls DDoS-Abwehr auf einer Appliance durchführen, muss die Verbindung noch verarbeitet werden, bevor sie unterbrochen werden kann. Mit Cloudflare sendet unser Netzwerk das Präfix des Kunden. So wird Traffic angezogen, der ansonsten für die Perimeter-Firewall bestimmt wäre. Dank Anycast können wir DDoS-Angriffe effektiv abfangen, indem wir die Last auf alle unsere Rechenzentren verteilen. Die Mitglieder des Botnetzes sehen den nächstgelegenen Anycast-PoP, der den Datenverkehr gemäß den Richtlinien von Magic Transit und Magic Firewall verarbeitet.

Vereinfachung des Firmennetzwerks

Diese Vereinfachung bringt eine Reihe von Vorteilen einer Modernisierung mit sich. IT-Teams können für eine größere Zuverlässigkeit des Netzwerks sorgen, wenn ein kleinerer Teil seiner Komponenten fehleranfällig ist. Außerdem lässt sich eine höhere Sicherheit gewährleisten, indem bei den Zugriffsrechten konsequent ein Zero Trust-Ansatz angewandt wird.

Zur Vereinfachung Ihrer Netzwerkstruktur sollten Sie Folgendes in Betracht ziehen:

Abschaffung der DMZ

Netzwerk-DMZ bereiten im Betrieb Probleme, da sie besonders anfällig für Zero-Day-Angriffe sind. Bei diesen wird kein interner Netzwerkzugriff benötigt, um mit den Servern in der DMZ zu kommunizieren. Damit das nicht ausgenutzt oder missbraucht werden kann, müssen Unternehmen wachsam bleiben.

Früher kamen DMZ eine wichtige Rolle zu. Die Frage ist aber, ob sie heute noch notwendig sind. Als Netzwerkkonstrukt verlieren sie an Bedeutung, da sich Anwendungen auch auf andere Weise erstellen und hosten lassen.

- Für öffentlich zugängliche Applikationen bietet eine Verlagerung von Workloads in die Public Cloud sowohl wirtschaftliche als auch technische Vorteile.
- Bei einem SaaS-Modell müssen viele Arten von öffentlichen und privaten Anwendungen überhaupt nicht auf einer vom Kunden verwalteten Infrastruktur laufen.

Daher ist es unter dem Aspekt der Sicherheit und des Netzwerkdesigns nur pragmatisch, sich zu überlegen, wie man den Bedarf an einer DMZ reduzieren oder ganz auf sie verzichten kann. Das ist nicht nur aus betrieblicher Sicht sinnvoll, sondern vereinfacht auch die Architektur erheblich, da die sie unterstützende Netzwerkinfrastruktur (Firewall, WAF und Load Balancer) wegfällt.

Was ist mit privaten Anwendungen, die in der DMZ angesiedelt werden, um Mitarbeitenden, Partnern und Auftragnehmern Zugang zu ermöglichen? Es wäre sicherer, sie in einem privaten Netzwerk zu isolieren und Mitarbeitenden und Partnern den Zugriff per Zero Trust Network Access (ZTNA) zu erlauben.

So wird auf effektive Weise die Angriffsfläche verringert, weil kein an die Anwendung gerichteter Traffic mehr im Netzwerk eingeht. Bei ZTNA wird ein kontextbezogener, vermittelter Zugang zu Ressourcen über die Connectivity Cloud von Cloudflare gewährt. Auf diese Weise müssen keine Ports in der Netzwerk-Firewall mehr geöffnet werden. Außerdem hat die IT-Sicherheitsabteilung einen vollständigen Überblick darüber, wer auf welche Ressource Zugriff hat.

Ersatz von VPN durch ZTNA

Heute werden immer seltener VPN für den Anwendungszugriff verwendet. Unter dem Aspekt des Netzwerkdesigns ist es unpraktisch, Nutzer über einen sehr langen Tunnel zum Internet und der Cloud zu leiten. Außerdem stellt die Netzwerkeinbindung von Nutzern (und potenziell kompromittierten Endpunkten) per VPN ein erhebliches Sicherheitsrisiko dar.

Ein VPN wird auch nicht ausschließlich für den Anwendungszugriff verwendet. Bei manchen Konstellationen benötigen Unternehmen eine umfassendere Netzwerkanbindung eines Endpunkts, z. B. bei der Endpunktverwaltung und der vom Server initiierten Kommunikation. In diesen Fällen wird traditionell die Netzwerkkonnektivität des VPN in beide Richtungen genutzt. Diesen Anforderungen waren die frühen ZTNA-Produkte auf dem Markt aber nicht gewachsen. Deshalb blieb Unternehmen nichts anderes übrig, als ZTNA und VPN parallel zu verwenden.

Zur Modernisierung ihrer Netzwerkinfrastruktur können Unternehmen die verschiedenen Funktionen mit ZTNA von Cloudflare zusammenführen. Denn Cloudflare bietet ihnen die Möglichkeit, sowohl klassische ZTNA-Anwendungsfälle als auch Server-initiierte Datenübertragungen in beide Richtungen zu unterstützen. Das erleichtert es ihnen, ihre Anforderungen an den Anwendungszugriff durch die Abschaffung des VPN zu verschlanken. Außerdem trägt dies zu einer höheren Sicherheit und Vereinfachung bei.

Beseitigung von übermäßigem Vertrauen im LAN

Beim hybriden Arbeiten macht es inzwischen kaum noch einen Unterschied, ob man sich im Büro befindet oder an einem anderen Ort. Das gilt insbesondere dann, wenn dabei häufig öffentliche, nicht vertrauenswürdige Netzwerke genutzt werden, etwa in Cafés und Coworking Spaces.

In gewisser Weise ist das öffentliche Netzwerk Sinnbild für Zero Trust: Niemand hat privilegierten Zugang und niemand oder nichts ist vertrauenswürdig. Wenn das in einem gemeinsam genutzten Arbeitsbereich, im Homeoffice und in einem Café prinzipiell funktioniert, warum kann dann nicht auch im Firmennetzwerk auf Vertrauen verzichtet werden?

Um das zu bewerkstelligen, muss die Netzwerkstruktur gar nicht weiterentwickelt werden, vielmehr vereinfacht sie sich. Tatsächlich ist es viel sicherer, das gesamte Netzwerk als nicht vertrauenswürdig zu betrachten, als einen erweiterten Zugang für authentifizierte Nutzer zu schaffen und zur Erstellung von Verbindungen zu Ressourcen Netzwerkrichtlinien zu verwenden. Mit einem SASE-Sicherheitskonzept erhalten Unternehmen Zugriff auf die benötigten Anwendungen mit angemessenem Schutz, ohne dass das Netzwerk selbst als vertrauenswürdig eingestuft werden muss. Beim Zero Trust-Ansatz geht es nicht darum, das Netzwerk vertrauenswürdiger zu machen. Vielmehr wird ihm Vertrauen entzogen, bis ein besserer, sichererer Zustand ohne explizite und übermäßige Zugriffsrechte erreicht ist, wie sie bisher gang und gäbe waren.

Schnellere Anbindung bei Fusionen und Übernahmen

Unternehmen nutzen Fusionen und Übernahmen, um sich Zugang zu geschäftlichen Ressourcen und Kompetenzen zu verschaffen, die ihnen sonst nicht unmittelbar zur Verfügung stünden. Um diese Chance aber wirklich ergreifen und von Synergieeffekten einer solchen Verschmelzung profitieren zu können, ist eine schnelle Umsetzung erforderlich. Doch genau dazu sind IT-Abteilungen oft nicht in der Lage, weil Anwendungen und die zugrunde liegende Netzwerkinfrastruktur zweier Unternehmen nur selten nahtlos ineinandergreifen.

Um die Anbindung bei Fusionen und Übernahmen zu beschleunigen, können Unternehmen den Zugriff auf Anwendungen als eine von der Netzwerkintegration getrennte Aufgabe betrachten. Die Entwicklung einer gemeinsamen Netzwerkarchitektur kann sich über mehrere Jahre erstrecken. Der Anwendungszugriff muss jedoch nicht von einem so weit entfernten Meilenstein abhängig sein.

Das liegt daran, dass die Situation an Tag eins praktisch ein Zero Trust-Anwendungsfall ist: Vertrauenswürdige Nutzer benötigen immer noch Zugriff auf Applikationen, auch wenn sie sich in nicht vertrauenswürdigen Netzwerken befinden. Mit Cloudflare One können die Zugriffsmöglichkeiten erweitert werden. Die Lösung ermöglicht Anbindungen für Fusionen und Übernahmen, ohne dass der Zugang zu zusammengeführten Netzwerken vorausgesetzt wird.

Vernetzung und Absicherung von Clouds

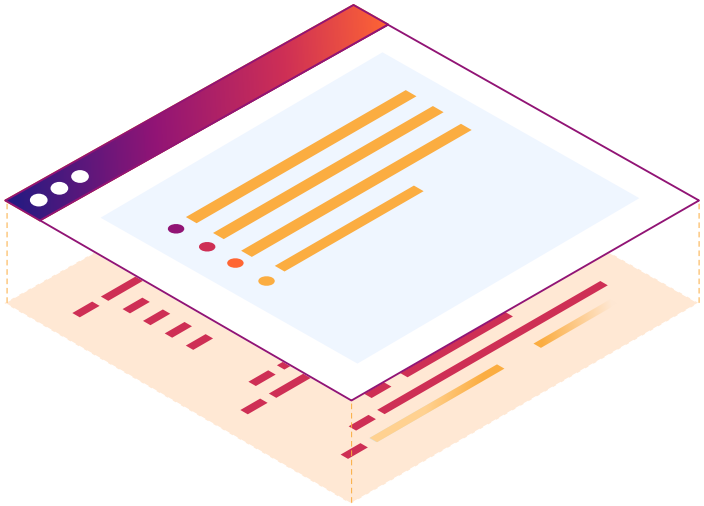
Mit Voranschreiten der Entwicklung in der Cloud wird es möglich, Komponenten in einer Cloud in einer anderen wiederzuverwenden. So wie jedes Unternehmen mit der Zeit zu einer Multi-Cloud wird, muss auch jedes Unternehmen irgendwann Public Cloud-Netzwerke verwalten. Die Anwendungsentwicklung ist in der Regel auf einen bestimmten Bereich bezogen. Das bedeutet, dass DevOps-Teams in verschiedenen Teilen des Unternehmens oft die Tools bevorzugen, mit denen sie am vertrautesten sind. Unternehmensintern Fähigkeiten zur Verwaltung der Konnektivität für mehrere Clouds zu entwickeln, ist aber kompliziert, weil dabei Instrumentarien verwendet werden müssen, die auf völlig unterschiedlichen Frameworks aufbauen.

Was ebenfalls zur Komplexität von Multi-Clouds beiträgt, sind Hybrid Clouds, die private und öffentliche Clouds in sich vereinen. Solche Netzwerke werden manchmal mit Diensten für exklusive Netzwerkverbindungen wie AWS Direct Connect aufgebaut, die jedoch unter Umständen kostspielig und auf nur eine Cloud beschränkt sind. Bei der Entwicklung von Multi-Cloud-Anwendungen möchten sich Unternehmen nicht unbedingt die Kosten für die Ausstattung jeder einzelnen Cloud mit exklusiven Netzwerkdiensten aufbürden.

Anstatt sich mit der Vernetzung und Sicherheit einzelner Anwendungen untereinander zu befassen, können mit Cloudflare Public Cloud-Netzwerkservices koordiniert und angebunden werden. Unserer Überzeugung nach ist die Connectivity Cloud von Cloudflare für eine solche Architektur ideal, da sie als Kanal für den Datenverkehr zwischen Clouds durch das weitläufige Cloudflare-Netzwerk perfekt geeignet ist. Mit den zusätzlichen Verwaltungsfunktionen für Public Cloud-Netzwerke können Kunden nun auch die Einrichtung von Workload-Konnektivität über Cloudflare steuern.

Die Public Cloud-Netzwerkdienste von Cloudflare beschränken sich nicht auf die Orchestrierung der zugrunde liegenden Strukturen. Unsere Architektur geht noch einen Schritt weiter: Sie stellt Entwicklerdienste zur Erschaffung von Multi-Cloud-Anwendungen und zur Integration in solche Applikationen bereit. Die Entwicklerplattform bietet ein vielfältiges Ökosystem mit fundamentalen, auf dem Open Source-Prinzip und offenen Standards aufbauenden Technologien. Sie können selbst bestimmen, welche Bestandteile der Entwicklerplattform Sie nutzen und welche nicht, ohne auf die Dienste einer bestimmten Cloud beschränkt zu sein.

Nächste Schritte



Wenden Sie sich an Cloudflare, um die nächsten Schritte zur Modernisierung Ihres Netzwerks zu unternehmen. Wir können Ihnen bei der Entwicklung Ihrer Strategie helfen, denn wir haben bereits mit Tausenden von Kunden bei der Umstellung ihrer Architektur auf unsere Connectivity Cloud eng zusammengearbeitet.

Weitere Informationen finden Sie unter http://www.cloudflare.com/de-de/

© 2024 Cloudflare, Inc. Alle Rechte vorbehalten.
Das Cloudflare-Logo ist ein Markenzeichen von Cloudflare.
Alle weiteren Unternehmens- und Produktnamen sind ggf.
Markenzeichen der jeweiligen Unternehmen.

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

REV:BDES-5483.2024JAN30