DATENBLATT

Absicherung der Workload Communications mit Cloud Connector

Einfacher, sicherer Zugriff für Workloads auf das Internet und private Anwendungen mit einer Direct-to-Cloud-Architektur.

Erweiterte Netzwerkkommunikation für die Cloud

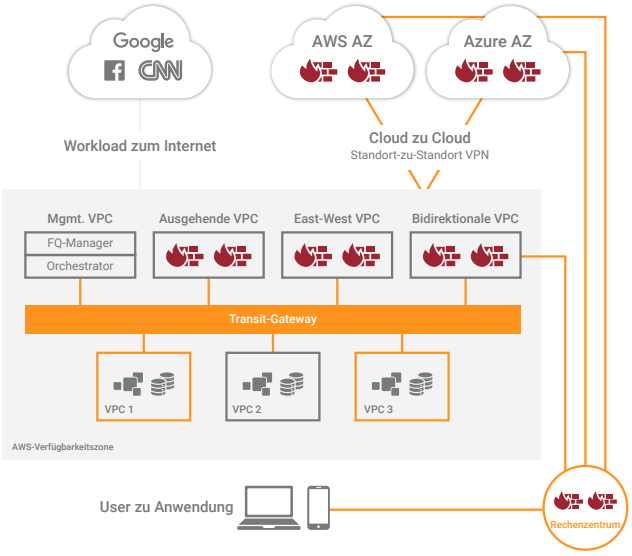
Angesichts der Verlagerung von Workloads in die Cloud und der zunehmenden Mobilität der User müssen Unternehmen ihre Netzwerke dringend umgestalten, um ihre Wettbewerbsfähigkeit zu sichern. Es ist nicht mehr möglich, Legacy-Netzwerke zu erweitern und die Sicherheit am Perimeter des Netzwerks mit Firewalls zu gewährleisten. Für Organisationen, die ihre Infrastruktur modernisieren, ist die Gewährleistung einer effektiven Workload-Kommunikation zu einer grundlegenden Anforderung geworden. Der Cloud Connector von Zscaler hat die Workload-Kommunikation völlig neu konzipiert und bietet einen einfachen und sicheren Zugang für Workloads zum Internet und zu privaten Anwendungen. Im Gegensatz zur Legacy-Netzwerksicherheit verwendet Cloud Connector eine Direct-to-Cloud-Architektur, die auf der bewährten Zero Trust Exchange-Plattform von Zscaler aufbaut. Durch den Umstieg auf Cloud Connector zur Netzwerktransformationen profitieren Kunden von zahlreichen Vorteilen: besserer Sicherheit, einfacheren Betriebsabläufen, mehr Transparenz, höherer Verfügbarkeit, höherer Leistung und geringeren Kosten.

Herausforderungen bei der Workload-Konnektivität mit Legacy-Netzwerksicherheit

Wenn Organisationen versuchen, Workloads mit dem Internet oder mit anderen Anwendungen in öffentlichen Cloud- oder Rechenzentrumsumgebungen zu verbinden, stehen sie vor einer Reihe von Herausforderungen, wenn sie Legacy-Netzwerk- und Legacy-Sicherheitsarchitekturen nutzen. Dazu zählen:

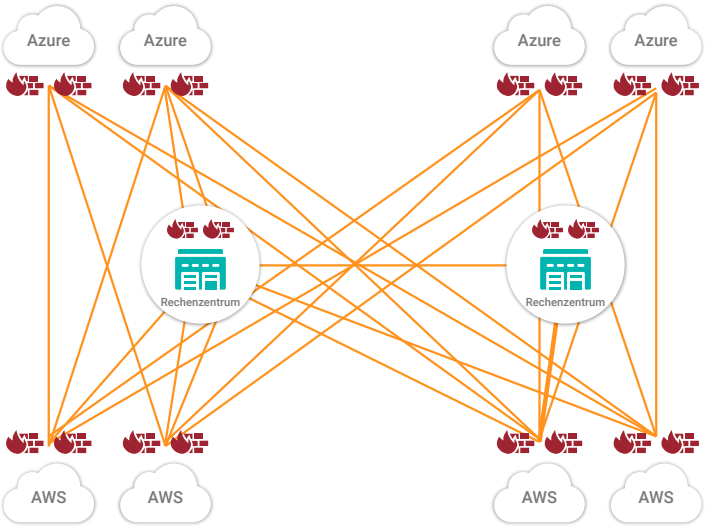
- **Erhöhtes Risiko von lateralen Bedrohungen und internetbasierten Angriffen** durch veraltete netzwerkzentrierte Konnektivitätslösungen wie Cloud-VPNs, Site-to-Site-VPNs, Firewalls oder WAN-Technologien, die das vertrauenswürdige Netzwerk eines Kunden über das Internet auf andere Clouds und On-Premise-Umgebungen ausdehnen und so die Angriffsfläche des Netzwerks vergrößern. Ein Flickenteppich aus Sicherheitsappliances, Tools und nicht standardisierten Policys erhöht die Sicherheitsrisiken aufgrund bekannter und unbekannter Lücken in der Sicherheitsabdeckung.
- **Übermäßige Komplexität** aufgrund komplizierter Routenfilterung, mehrerer Netzwerksprünge, virtueller Appliances für Netzwerk und Sicherheit und fragmentierter Richtlinienverwaltung durch die Einführung dieser Legacy-Modelle in die Cloud. Die Eindämmung dieser Komplexität fällt Sicherheitsteams aufgrund der schwierigen Durchsetzung standardisierter Workload-Konnektivität und Sicherheitsrichtlinien in Multi- und Hybrid-Cloud-Umgebungen schwer.
- **Mangelnde Transparenz** in den Verbindungspfaden zu Anwendungen sorgt für tote Winkel im Netzwerk und bei der Sicherheit. Cloud-Workloads verteilen sich immer stärker und Umgebungen werden immer umfangreicher. Für die Verbindung dieser verteilten Workloads sind undurchsichtige Multi-Hop-Netzwerke und Verkettungen mit mehreren Netzwerk- und Sicherheits-Appliances erforderlich. Aufgrund dieser komplexen Konnektivität und einer mangelnden zentralen Protokollierung fehlen den Betreibern Einblicke in die Anwendungskommunikation.
- **Schlechte Leistung und Skalierbarkeit** aufgrund der zunehmenden Anzahl von Netzwerk- und Sicherheitsdiensten in öffentlichen Cloud-Umgebungen, einer gehemmten Traffic-Geschwindigkeit und Engpässen für die zentralisierte Sicherheitsüberprüfung und -kontrolle.
- **Hohe Kosten** aufgrund veralteter Netzwerksicherheits-Appliances (z. B. Firewalls, IPS, Router und andere Einzelprodukte), Überprovisionierung von Netzwerkdiensten zum Ausgleich einer fehlenden Skalierbarkeit und die vermehrte Nutzung von Cloud-nativen Services wie Transit-Peerering.

Legacy-Modell: Erweiterung des unternehmenseigenen WAN in die Cloud



Teuer, komplexe Betriebsabläufe, langsame Anwendererfahrung, unzureichende Sicherheit aufgrund lateraler Bewegungen über das WAN

Multi-Cloud lässt Komplexität und Risiko um ein Vielfaches ansteigen



Ein Netz aus Site-to-Site-VPNs (Belegschaft, Partner, Geräte, Kunden)
Erhöhte Angriffsfläche und Risiko der lateralen Ausbreitung von Bedrohungen

Unternehmensnetzwerk Öffentliches Internet

Unternehmensnetzwerk

Cloud Connector bietet Zero-Trust-Zugang für Cloud-Workloads

Cloud Connector bietet Workloads schnellen und zuverlässigen Zugriff auf das Internet und private Anwendungen mit einer Direct-to-Cloud-Architektur, die hohe Sicherheit und eine einfache Bedienung bietet. Cloud Connector eliminiert die Angriffsfläche für das Netzwerk, da Workloads über eine vollständige Proxy-Architektur direkt mit dem Internet und privaten Anwendungen verbunden werden. Darüber hinaus vereinfacht diese Architektur die Workload-Kommunikation durch die Eliminierung von Routing, VPNs, Transit-Gateways, Transit-Hubs und Firewalls. Außerdem ermöglichen die bewährten ZIA- und ZPA-Policy-Frameworks eine flexible Weiterleitung sowie die Vereinfachung der Richtlinienverwaltung.

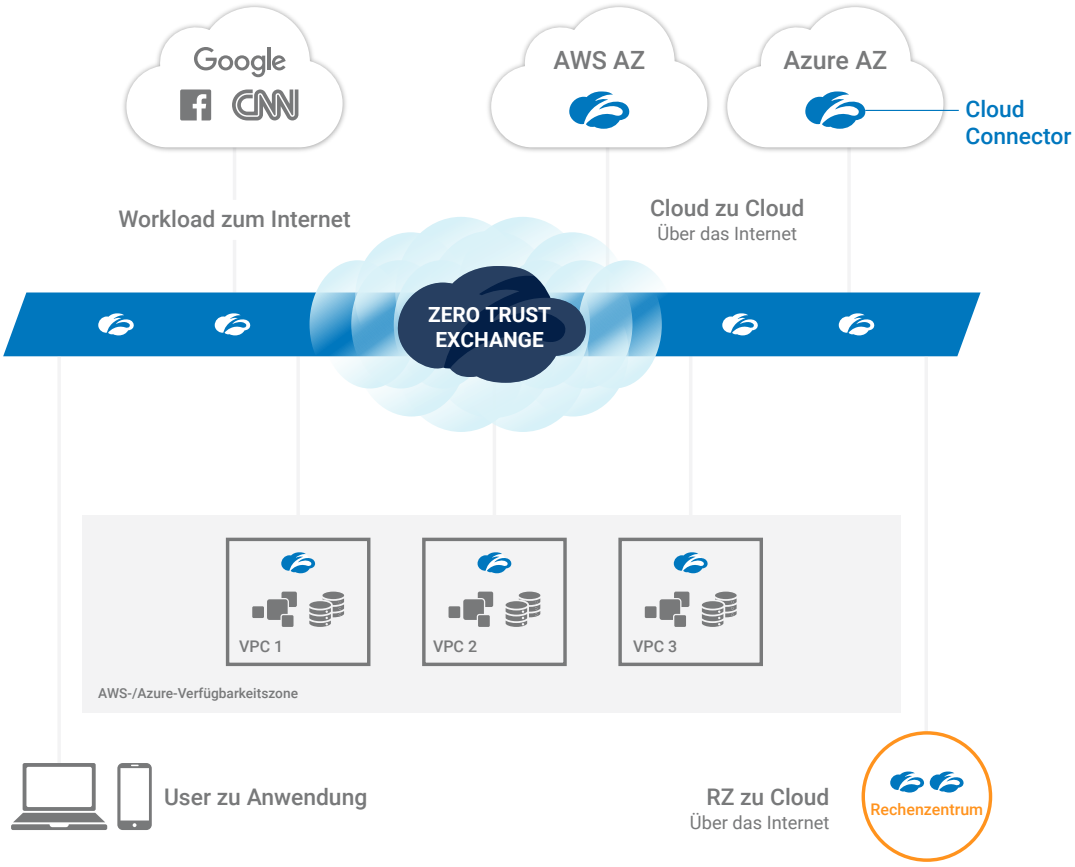
Die Direct-to-Cloud-Architektur ist ausschließlich durch den Einsatz von Zero Trust Exchange möglich. Cloud Connector leitet die gesamte Workload-Kommunikation direkt an die Zero Trust Exchange weiter, wo entweder ZIA- oder ZPA-Richtlinien für eine vollständige Sicherheitsüberprüfung und identitätsbasierte Kontrolle der Workload-Kommunikation angewendet werden können. Von der Zero Trust Exchange wird die Kommunikation an ein beliebiges Ziel weitergeleitet – sei es das Internet oder andere private Anwendungen in einer öffentlichen Cloud oder einem On-Premise-Rechenzentrum. Dieser einzigartige Ansatz bietet drei wesentliche Vorteile:

- Ebnet den Weg von netzwerkbasierter VPN-Konnektivität hin zu identitäts- und anwendungsbasierter Kommunikation für echte Zero-Trust-Sicherheit
- Eliminiert die veraltete Festung-mit-Burggraben-Architektur und damit die Notwendigkeit für alte Produkte wie Squid-Proxys, NAT-Gateways, IPSs usw., ohne die Sicherheit zu beeinträchtigen
- Bietet verteilte, skalierbare Konnektivität, wo immer sie benötigt wird, und zentralisiert und automatisiert die Richtlinienverwaltung zur Vereinfachung der Workload-Kommunikation

Cloud Connector ist in mehrfacher Hinsicht darauf ausgerichtet, Unternehmen bei der Umsetzung ihrer Prioritäten bei der Netzwerkumstellung zu unterstützen. Es erweitert die Workload-to-Workload-Konnektivität unter Verwendung von Zero-Trust-Prinzipien über zusammenhanglose Netzwerke und mehrere Clouds hinweg, einschließlich AWS-Regionen, Microsoft Azure, Google Cloud und lokaler Rechenzentren. Cloud Connector bietet auch sicheren Internetzugang für Workloads in öffentlichen Clouds und Rechenzentren. All diese Funktionen werden über eine einheitliche Richtlinienebene für die Weiterleitung von Traffic, Sicherheit und den Zero-Trust-Zugriff in diesen heterogenen Umgebungen bereitgestellt.

Zero-Trust-Modell für Multi-Cloud-Umgebungen

eine Ausweitung des WAN in die Cloud. Verbindung von DC, Azure, \rAWS und GCP-Regionen über das Internet



Reduzierte Kosten und Komplexität, hervorragende User Experience, mehr Sicherheit durch Zero-Trust.

Vorteile von Cloud Connector

Einfachere Bereitstellung ohne komplizierte Netzwerkkonfigurationen. Herkömmliche Ansätze erfordern komplexe Routing-Konfigurationen durch Transit-Gateways, Transit-Hubs und SNAT, die für jeden VPC und jede Cloud wiederholt werden müssen. Im Gegensatz dazu benötigt Cloud Connector lediglich eine Standardroute zum Internet. Die Richtlinienverwaltung für die Weiterleitung von Traffic und die Sicherheit ist in der Zero Trust Exchange zentralisiert und standardisiert, unabhängig von Quelle oder Ziel der Workload-Kommunikation.

Vollständige End-to-End-Transparenz mit Direktverbindung zur Cloud. Die veraltete Vorgehensweise basiert auf undurchsichtigen Multi-Hop-Netzwerken, was die Analyse des Traffics sehr schwierig macht. Darüber hinaus ist die Protokollierung über mehrere Netzwerkprodukte verteilt. Da Cloud Connect direkt mit der Cloud verbunden ist, erhalten die Betreiber vollständige Transparenz und Kontrolle darüber, wie Workloads kommunizieren. Die Protokollierung wird zentralisiert und in Echtzeit gestreamt. Protokolle können für Korrelation und Analyse in ein SIEM oder eine beliebige Überwachungslösung exportiert werden.

Hyper-Skalierbarkeit ohne zentrale Engpässe. Legacy-Architekturen erfordern, dass der gesamte Traffic über eine zentrale Infrastruktur geleitet wird. Dazu gehören Transit-Gateways, Hubs und virtuelle Firewalls, die nicht über die Elastizität und Skalierbarkeit verfügen, um einen hohen Durchsatz zu bewältigen. Die moderne Zero Trust Exchange-Architektur arbeitet mit mehr als 150 Rechenzentren weltweit auf Hyperscale-Niveau und reagiert auf jeden Anstieg der Kommunikation mit einer elastischen, horizontalen Skalierung.

Hohe Verfügbarkeit ohne unnötige Replizierung von Services. Bisherige Ansätze erfordern eine komplexe Verfügbarkeitsarchitektur mit mehreren Firewalls und Netzwerkkonfigurationen, die über mehrere Zonen, Regionen und Clouds repliziert werden müssen. Die Direct-to-Cloud-Architektur von Cloud Connector vereinfacht die Anforderungen an die Cloud-Konfiguration erheblich, da alle erforderlichen Dienste transparent und in großem Umfang in der Zero Trust Exchange verfügbar sind. Am Standort des Kunden wird eine automatische Ausfallsicherung mit N+2-Redundanz für die Weiterleitung und Sicherheit bereitgestellt.

Niedrigere Kosten durch optimierte Services, die durch die Zero Trust Exchange zur Verfügung stehen. Kunden müssen keine Vielzahl von Services mehr bereitstellen und für Leerlaufzeiten von Firewalls, Transit-Hubs und NAT-Gateways zahlen, die sich in jeder Cloud-Umgebung wiederholen und sich schnell summieren. Mit Cloud Connector gibt es keine versteckten Kosten, und den Kunden werden nur die in Anspruch genommenen Sicherheitsservices in Rechnung gestellt, jedoch keine Netzwerk- oder Zugangsgebühren. Es besteht keine Notwendigkeit, für virtuelle Firewalls oder Proxys in den Kundenumgebungen zu bezahlen.

Cloud Connector bietet herausragenden Nutzen

Cloud Connector basiert auf der Zero Trust Exchange von Zscaler, die User, Geräte und Anwendungen unter Verwendung von Unternehmensrichtlinien über jedes Netzwerk und jede Cloud sicher und in großem Umfang miteinander verbindet.

- Anwendungs-Workloads sind, unabhängig von dem zugrunde liegenden Unternehmensnetzwerk, VPN oder WAN, direkt miteinander verbunden.
- Anwendungen sind für die Außenwelt unsichtbar und haben keine Angriffsfläche.
- Speziell entwickelte, mandantenfähige Proxy-Architektur, die Richtlinien speichert, prüft und durchsetzt
- Die Hochleistungsüberprüfung erfolgt durch eine skalierbare Single-Scan- und Multi-Access-Architektur
- Feinkörniges Management von Weiterleitungsrichtlinien für Internet- und Nicht-Internet-Traffic, unter Verwendung von Zscaler Internet Access oder Zscaler Private Access Policys
- Einheitliche, standardisierte Policys für AWS, Azure, Google Cloud und On-Premise-Rechenzentren. Dazu gehören die Verwaltung von Richtlinien, die Überwachung des Traffics und die Verfolgung von Protokollen.

Anwendungsfälle für Cloud Connector

Digitale Transformation

Da Unternehmen ihre Anwendungen in die Cloud migrieren und Cloud-native Anwendungen entwickeln, werden die On-Premise-Modelle für Netzwerke und Sicherheit aufgebrochen. Die digitale Transformation erfordert eine Netzwerktransformation, die in einem neuen Modell für die Workload-Kommunikation eingesetzt wird; ein Modell, bei dem Workloads sicher und unabhängig vom zugrunde liegenden Netzwerk aus mit einem beliebigen Ziel kommunizieren. Cloud Connector wurde speziell für die digitale Transformation entwickelt.

Workload-Konnektivität ohne VPNs

Organisationen können Workloads jetzt direkt mit privaten Anwendungen verbinden, ohne ihr WAN zu erweitern oder auf VPNs angewiesen zu sein, was die Angriffsfläche des Netzwerks vergrößern würde.

Erfordernis von Zero Trust

Zero Trust geht davon aus, dass das Netzwerk beeinträchtigt wurde und nicht mehr vertrauenswürdig ist. In diesem Szenario verbindet Cloud Connector Workloads direkt mit dem Internet oder mit privaten Anwendungen, ohne Netzwerke zu verbinden. Jede Verbindung wird zu Prüfzwecken überwacht und protokolliert.

Sicherer Cloud-Workload-Zugriff auf das Internet

Workloads können als Spiegelbilder der User betrachtet werden. Genau wie die User können Workloads über Zscaler Internet Access direkt mit der Cloud verbunden werden und profitieren von demselben Policy-Framework, derselben Sicherheitsüberprüfung und derselben Zugriffskontrolle. Virtuelle Firewalls sind nicht erforderlich.

Fusionen und Übernahmen

Die Zusammenführung zweier unterschiedlicher Netzwerke ist kompliziert und zeitaufwendig. Probleme reichen von IP-Überschneidungen über Routing-Probleme bis hin zu einem erhöhten Sicherheitsrisiko durch erweiterte die Netzwerkangriffsfläche, wenn zwei Netzwerke kombiniert werden. Mit Cloud Connector müssen die Netzwerke nicht zusammengeführt werden. Sie können getrennt arbeiten und die Workloads aus einer Umgebung schnell und störungsfrei mit privaten Anwendungen in einer anderen Umgebung verbunden werden.

Zweigstellenanbindung

Die Verbindung von Zweigstellenanwendungen mit privaten Anwendungen oder mit dem Internet ist mit Branch Connector, einer On-Premise-Version von Cloud Connector, viel einfacher geworden. Branch Connector ergänzt SD-WANs, und Zscaler arbeitet mit allen großen SD-WAN-Anbietern zusammen.

Funktionsdatenblatt

Zero-Touch-Bereitstellung und automatisches Deployment

- Zero-Touch-Bereitstellung mit systemdefinierten Vorlagen für AWS und Azure
- Vollständig automatisiertes Deployment (AWS CloudFormation, Azure Resource Manager Templates und Terraform)
- Dynamische Erkennung der geografischen Regionen, Verfügbarkeitszonen, VPC/VNETs der Kunden
- Integrierte SLA-Überwachung und Failover
- Verfügbar im AWS Marketplace und Azure Marketplace

Granulare Weiterleitungsrichtlinie für Internet- und Nicht-Internet-Traffic

- Optionen zum Senden des Traffics an ZIA, ZPA oder direkt (unter Umgehung der Zscaler-Services)
- Flexible Traffic-Auswahlkriterien für Standort, Unterstandort, Standortgruppe, 5 Tupel oder FQDN
- Integrierte Verfügbarkeit mit nahtlosem Failover zum nächsten verfügbaren Service-POP

Einheitliche Richtlinien für Weiterleitung und Sicherheit mit Cloud Connector und ZIA

- Standorte werden dynamisch für die VPCs/VNETs erstellt
- Dynamische Cloud-Connector-Standorte werden mit der ZIA-Plattform synchronisiert
- Standorte, die von Cloud Connectors erstellt wurden, sind wie jeder andere vorhandene ZIA-Standort. Alle Sicherheitsrichtlinien können aktiviert werden – einschließlich IPS, SSL-Proxy, URL-Filterung und Datenschutz

Einheitliche Zero-Trust-Policy für User-zu-Server und Server-zu-Server

- ZPA bietet eine einheitliche Richtlinie für User-zu-Anwendung und Server-zu-Server
- Vorhandene ZPA-Richtlinie wird um einen neuen Client-Typ (Cloud Connector) erweitert, um Server-zu-Server-Konnektivität zu unterstützen
- Für die Weiterleitung von Traffic in AWS, Azure und im Rechenzentrum erstellte Cloud-Connector-Gruppen werden mit der ZPA-Plattform synchronisiert.

Einheitliche Richtlinien, Kontrolle und Verwaltung über AWS, Azure und Branch Connectors

- Zentralisiertes Dashboard in der Cloud zur Überwachung von Gerätezustand und Datenverkehr
- Filterung verfügbar für Azure-, AWS- und Zweigstellen-Deployments
- Zeitreihen für Flow- und Byte-Count für ZIA, ZPA, Direct und DNS

Konsolidierte Protokollierungsinfrastruktur für alle Arten von Traffic

- Detaillierte Sitzungsprotokolle, die den an ZIA, ZPA und direkt (Zscaler-Bypass) fließenden Traffic erfassen
- Alle DNS-Transaktionen werden sowohl für öffentliche als auch für private DNS protokolliert
- Vollständig in die NSS-Infrastruktur integriert, vorhandene NSS-Firewall-VM kann zum Streaming der Protokolle an SIEM verwendet werden

Zscaler, Inc.
120 Holger Way
San Jose, CA 95134, USA
+1 408 533 0288
www.zscaler.com