DATENBLATT

Zero Trust für Cloud-Workloads

Workload Communications von Zscaler ermöglicht einfachen und sicheren Zugriff für Workloads auf das Internet und private Anwendungen, in öffentlichen und privaten Clouds, mit einer Direct-to-Cloud-Architektur.

Die Verlagerung von Workloads in die Cloud bedingt die dringende Modernisierung der Netzwerke, damit das Unternehmen wettbewerbsfähig bleibt. Herkömmliche netzwerkzentrierte Architekturen, die für statische Umgebungen konzipiert wurden, sind den Anforderungen von Cloud-Konnektivität – geschweige denn Multi-Cloud-Umgebungen – einfach nicht gewachsen. Entsprechend vergrößert sich mit der steigenden operativen Komplexität auch die Angriffsfläche.

Die Gewährleistung der effektiven und sicheren Workload-Kommunikation sollte zu den Grundanforderungen bei der Modernisierung der IT-Infrastruktur gehören. Die Zero Trust Exchange von Zscaler hat die Workload-Kommunikation völlig neu konzipiert und bietet einen einfachen sowie sicheren Zugang für Workloads zum Internet und zu privaten Anwendungen. Im Unterschied zur Legacy-Netzwerksicherheit verwendet Workload Communications eine Direct-to-Cloud-Architektur, die auf der bewährten Zero-Trust-Exchange-Plattform aufbaut. Durch den Umstieg auf Workload Communications zur Netzwerktransformation profitieren Kunden von zahlreichen Vorteilen wie besserer Sicherheit, einfacheren Betriebsabläufen, mehr Transparenz, höherer Verfügbarkeit, besserer Anwendungsperformance und geringeren Kosten.

Herausforderungen bei der Workload-Konnektivität mit Legacy-Netzwerksicherheit

Wenn Unternehmen 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 Cyberrisiko, insbesondere durch laterale Verbreitung von Bedrohungen, aufgrund veralteter netzwerkzentrierter 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 virtuellen Sicherheits-Appliances verschiedener Anbieter, Tools und nicht den Standards entsprechenden Richtlinien erhöht die Sicherheitsrisiken aufgrund bekannter und unbekannter Lücken in der Sicherheitsabdeckung. Dadurch sind potenzielle Datenverluste durch Hackerangriffe quasi vorprogrammiert.

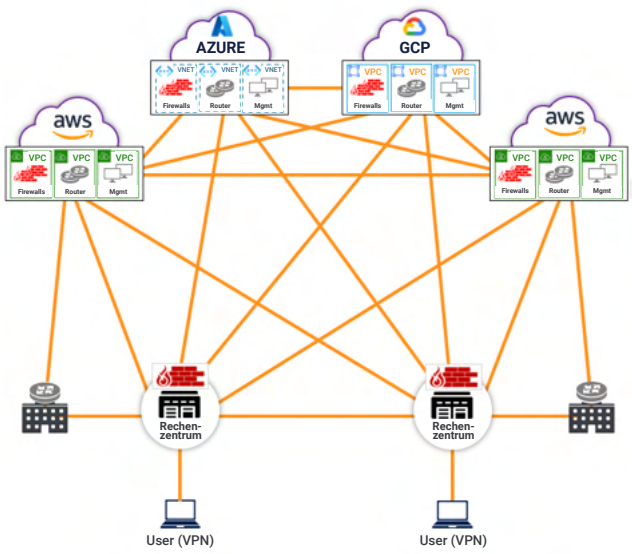
Eskalierende Komplexität aufgrund komplizierter Routenfilterung, mehrerer Netzwerkhops, virtueller Appliances für Netzwerk sowie Sicherheit und fragmentierter Richtlinienverwaltung durch die Einführung dieser Legacy-Modelle in die Cloud. Gleichzeitig geht der Trend zunehmend in Richtung einer agilen, kontinuierlichen und serviceorientierten Produktentwicklung sowie -lieferung. Die Eindämmung dieser Komplexität stellt Sicherheitsteams aufgrund der schwierigen Durchsetzung standardisierter Workload-Konnektivität und Sicherheitsrichtlinien in Multi- und Hybrid-Cloud-Umgebungen vor Herausforderungen.

Mangelnde Transparenz in den Verbindungspfaden zu Anwendungen verursacht tote Winkel im Netzwerk und bei der Sicherheit. Cloud-Workloads sind heute stärker verteilt und IT-Umgebungen umfangreicher als je zuvor. Für die Verbindung dieser verteilten Workloads sind undurchsichtige Multi-Hop-Netzwerke und ein „Daisy-Chaining“ mehrerer Netzwerk- und Sicherheits-Appliances erforderlich. Aufgrund dieser komplexen Konnektivität und einer mangelnden zentralen Protokollierung fehlen den Betreibern Einblicke in die Anwendungskommunikation.

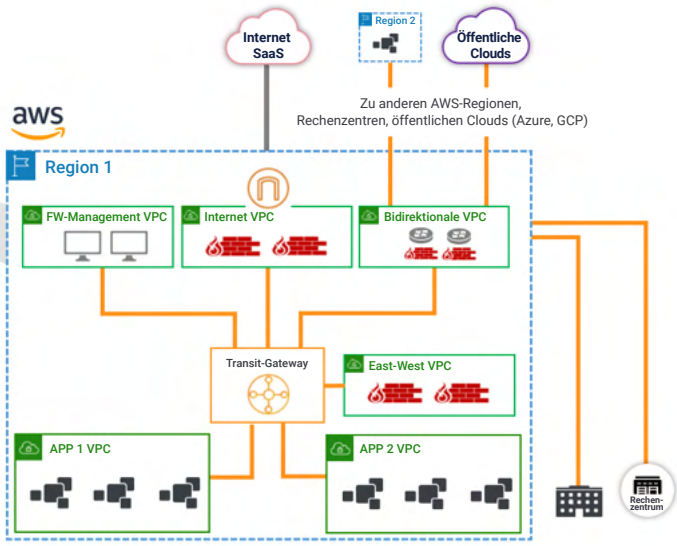
Unzureichende Performance und Skalierbarkeit durch Beibehaltung ungeeigneter Legacy-Ansätze zur Sicherung von Cloud-Verbindungen. In Legacy-Architekturen kommen zumeist eigene VMs für jede Sicherheitsfunktion zum Einsatz. Die daraus resultierende sequenzielle Überprüfung führt zu höherer Latenz. Zudem lassen sich diese Architekturen nicht schnell genug skalieren, um einen plötzlichen Traffic-Anstieg zu bewältigen.

Hohe Kosten aufgrund veralteter Netzwerksicherheits-Appliances (z. B. Firewalls, IPS, Router und andere Einzelprodukte), zu umfangreiche Bereitstellung von Netzwerkdiensten zum Ausgleich einer fehlenden Skalierbarkeit und die vermehrte Nutzung von Cloud-nativen Services wie Transit-Peering.

Extend the Corporate WAN to the Cloud
Single infected workload infects entire network



Herkömmliche Netzwerksicherheit wird an die Cloud angepasst
Komplexes Routing, IP-Überschneidungen/-Konflikte
Mehrere Firewalls und VMs, Squid-Proxys für Cybersicherheit und Datenschutz



Workload Communications wendet Zero-Trust-Prinzipien auf Cloud-Workloads an

Mit einer Direct-to-Cloud-Architektur, die hohe Sicherheit und eine einfache Bedienung bietet, gewährleistet Workload Communications den Workloads schnellen und zuverlässigen Zugriff auf das Internet und private Anwendungen. Workload Communications eliminiert die Netzwerk-Angriffsfläche, da Workloads über eine vollständige Proxy-Architektur direkt mit dem Internet und privaten Anwendungen verbunden werden. Diese Architektur vereinfacht die Konnektivität drastisch durch 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.

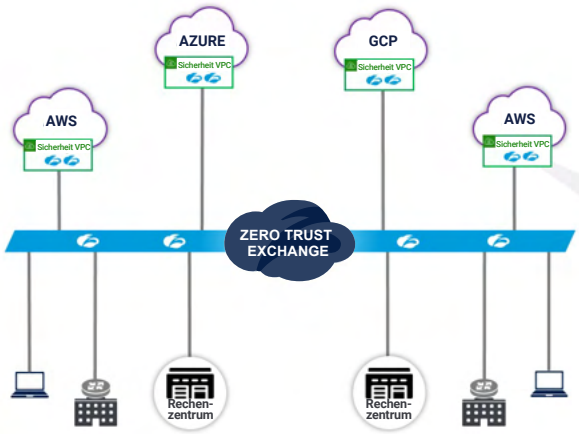
Die branchenweit einzigartige Direct-to-Cloud-Architektur wird durch den Einsatz von Zero Trust Exchange ermöglicht. Workload Communications leitet die gesamte Workload-Kommunikation direkt an die Zero Trust Exchange weiter, wo entweder ZIA- oder ZPA-Richtlinien für eine vollständige Sicherheitsüberprüfung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

- **Schutz vor Datenverlusten und minimale Angriffsfläche** – Durch die Direct-to-Cloud-Architektur wird der Traffic nicht über das Unternehmensnetzwerk geleitet. Somit sind Anwendungen für potenzielle Angreifer unsichtbar und das Risiko von Datenverlusten verringert sich entsprechend.
- **Vereinfachte Cloud-Verbindungen** – Die Zero-Trust-Architektur behebt Performance-Engpässe, indem IP-Überschneidungen entfernt, komplexes Routing vermieden und Workloads stattdessen direkt mit dem Internet bzw. mit anderen Anwendungen verbunden werden.

- **Hervorragende Anwendungsperformance auch bei hohem Datenvolumen** – Die Zscaler-Lösung basiert auf einer verteilten Architektur, in der jede eingehende Kommunikation unmittelbar an der Service Edge auf Identität und Kontext überprüft wird. So ist gewährleistet, dass Anwendungen unabhängig vom jeweiligen Hosting-Ort immer über den kürzesten Pfad verbunden werden. Das reduziert Latenzen und verbessert die Anwendungsleistung.

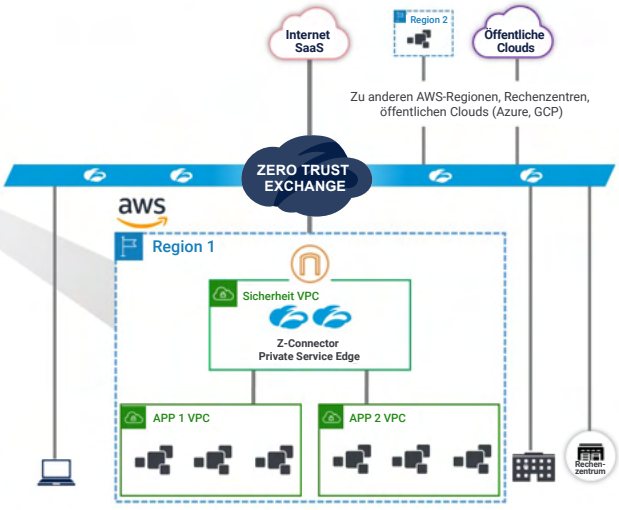
Workload Communications ist gleich in mehrfacher Hinsicht darauf ausgerichtet, Unternehmen bei der Umsetzung ihrer Prioritäten im Hinblick auf die Modernisierung der Infrastruktur zu unterstützen. Es erweitert die Workload-to-Workload-Konnektivität unter Verwendung von Zero-Trust-Prinzipien über nicht zusammenhängende Netzwerke und mehrere Clouds hinweg, einschließlich AWS-Regionen, Microsoft Azure, Google Cloud und lokaler Rechenzentren. Workload Communications bietet auch sicheren Internetzugriff für Workloads in öffentlichen Clouds und Rechenzentren. Diese Funktionen werden über eine einheitliche Richtlinienebene für die Weiterleitung von Traffic, Sicherheit und den Zero-Trust-Zugriff in diesen heterogenen Umgebungen bereitgestellt.

Cloud-Konnektivität mit Zero Trust
Sichere Workload-zu-Workload-Kommunikation und native Workload-Segmentierung ohne Erweiterung des WAN



Cloud-native Zero-Trust-Sicherheit
Sichert und vereinfacht Verbindungen zwischen Cloud und Internet, Cloud und Rechenzentrum, Cloud und Cloud

Vermeidet Einsatz mehrerer VMs (FWs, Squid-Proxys, Routing) und komplexes Routing (keine IP-Überschneidungen)



Vorteile von Workload Communications

- **Sicherheit von Workloads nach dem Zero-Trust-Prinzip.** Im Gegensatz zu herkömmlichen Kontrollen, die auf netzwerkzentrierter Sicherheit basieren, profitieren Workloads, wie oben erläutert, von Zero-Trust-Sicherheit, die auf Workload-Identität, Standort und anderen kontextbezogenen Attributen aufbaut.
- **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. Dagegen benötigt Workload Communications lediglich einen Standardpfad 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 erschwert. Darüber hinaus ist die Protokollierung über mehrere Netzwerkprodukte verteilt. Da Workload Communications 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 zur Korrelation und Analyse in ein SIEM oder eine beliebige Überwachungslösung exportiert werden.

- **Hochgradige Skalierbarkeit und Performance** ganz ohne zentrale Engpässe. In Legacy-Architekturen muss der gesamte Traffic über eine zentrale Infrastruktur geleitet werden. Dazu gehören Transit-Gateways, Hubs und virtuelle Firewalls, die nicht die notwendige Elastizität und Skalierbarkeit gewährleisten, um einen hohen Durchsatz zu bewältigen. Die moderne Architektur der Zero Trust Exchange läuft in über 150 Rechenzentren weltweit auf Hyperscale-Niveau und reagiert auf jeden Anstieg der Kommunikation mit einer elastischen, horizontalen Skalierung. Zusätzlich reduziert die Single-Pass-Architektur von Zscaler die Latenz und verbessert die Anwendungsperformance, indem User über weniger Hops verbunden werden.
- **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 Workload Communications 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 ein automatischer Failover mit N+2-Redundanz für die Weiterleitung und Sicherheit bereitgestellt.
- **Niedrigere Kosten durch optimierte Services, die durch die Zero Trust Exchange zur Verfügung stehen.** Die Zeiten der zu hohen Bereitstellung von Services, in denen Kunden für Leerlaufzeiten von Firewalls, Transit-Hubs und NAT-Gateways zahlen müssen, die in jeder Cloud-Umgebung repliziert werden und sich schnell aufsummieren, sind vorbei. Mit Workload Communications gibt es keine versteckten Kosten, und den Kunden werden nur die tatsächlich in Anspruch genommenen Sicherheitsdienste in Rechnung gestellt, jedoch keine Netzwerk- oder Zugriffsgebühren. Es besteht keine Notwendigkeit, für virtuelle Firewalls oder Proxys in den Kundenumgebungen zu bezahlen.

Alleinstellungsmerkmale von Workload Communications

Workload Communications 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 werden – unabhängig vom zugrunde liegenden Unternehmensnetzwerk, VPN oder WAN – direkt miteinander verbunden.
- Anwendungen sind für die Außenwelt unsichtbar und bieten keine Angriffsfläche
- Speziell entwickelte, mandantenfähige Proxy-Architektur, die Richtlinien speichert, prüft und durchsetzt
- Hochleistungsfähige Überprüfung durch eine skalierbare Single-Scan- und Multi-Access-Architektur
- Granulares Management der Weiterleitung von Internet- und Nicht-Internet-Traffic anhand der Richtlinien von Zscaler Internet Access oder Zscaler Private Access
- Einheitliche, standardisierte Richtlinien für AWS, Azure, Google Cloud und On-Premise-Rechenzentren. Darin inbegriffen sind die Verwaltung von Richtlinien, Überwachung des Traffics und Verfolgung von Protokollen.

Anwendungsfälle für Workload Communications

Digitale Transformation und Cloud-Migration
Durch die Migration vorhandener Anwendungen in die Cloud und die Entwicklung neuer Cloud-nativer Anwendungen werden die On-Premise-Modelle für Netzwerke und Sicherheit aufgebrochen. Die digitale Transformation erfordert eine Netzwerktransformation, die ein neues Modell für die Workload-Kommunikation ermöglicht: ein Modell, bei dem Workloads sicher und unabhängig vom zugrunde liegenden Netzwerk aus mit einem beliebigen Ziel kommunizieren. Workload Communications wurde speziell zur Unterstützung der digitalen Transformation entwickelt.

Workload-Konnektivität ohne VPNs
Unternehmen können Workloads jetzt direkt mit privaten Anwendungen verbinden, ohne ihr WAN zu erweitern oder auf VPNs angewiesen zu sein, was in beiden Fällen die Angriffsfläche des Netzwerks vergrößern würde.

Zero Trust zur Vorbeugung von Ransomware und Malware
Das Zero-Trust-Konzept beruht auf der Annahme, dass das Netzwerk kompromittiert wurde und nicht mehr vertrauenswürdig ist. In diesem Szenario verbindet Workload Communications die Workloads direkt mit dem Internet oder mit privaten Anwendungen, ohne Netzwerke zu verbinden. Dadurch wird die Angriffsfläche innerhalb des Netzwerks eliminiert und die laterale Verbreitung von Ransomware und anderen Bedrohungen in der IT-Umgebung verhindert. 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 ZIA direkt mit der Cloud verbunden werden und profitieren von einem identischen Policy-Framework sowie identischer Sicherheitsüberprüfung und Zugriffskontrolle. Virtuelle Firewalls sind nicht erforderlich.

Fusionen und Übernahmen
Die Zusammenführung zweier unterschiedlicher Netzwerke ist sehr kompliziert und zeitaufwendig. Die Schwierigkeiten reichen von IP-Überschneidungen über Routing-Probleme bis hin zu einem erhöhten Sicherheitsrisiko durch die erweiterte Netzwerkangriffsfläche, wenn zwei Netzwerke kombiniert werden. Mit Workload Communications erübrigt sich diese Zusammenführung – die Netzwerke können getrennt weiterarbeiten und die Workloads aus einer Umgebung schnell und störungsfrei mit privaten Anwendungen in einer anderen Umgebung verbunden werden.

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 Workload Communications und ZIA

- Standorte werden dynamisch für die VPCs/VNETs erstellt
- Dynamische Workload-Communications-Standorte werden mit der ZIA-Plattform synchronisiert
- Für Standorte, die von Workload Communications erstellt wurden, können dieselben Sicherheitsrichtlinien aktiviert werden wie für jeden anderen ZIA-Standort, 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
- Die vorhandene ZPA-Richtlinie wird um einen neuen Client-Typ (Workload Communications) erweitert, um Server-zu-Server-Konnektivität zu unterstützen
- Für die Weiterleitung von Traffic in AWS, Azure und im Rechenzentrum erstellte Workload-Communications-Gruppen werden mit der ZPA-Plattform synchronisiert

Einheitliche Richtlinien, Kontrolle und Verwaltung über AWS, Azure und Zweigstellenkonnektoren

- Zentrales Dashboard in der Cloud zur Überwachung von Gerätezustand und Traffic
- 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 Traffic an ZIA, ZPA und direkt (unter Umgehung der Zscaler-Services) erfassen
- Alle DNS-Transaktionen werden sowohl für öffentliche als auch für private DNS protokolliert.
- Vollständig mit der 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.de