Einfache und sichere Migration zu AWS mit Zscaler

AWS Cloud Adoption Framework: Integration mit Zscaler Private Access

Inhaltsverzeichnis

Einführung

In diesem Dokument wird erläutert, wie Zscaler™ eine schnellere Umstellung von Usern auf AWS unterstützt, indem Reibungspunkte beseitigt werden, die die Realisierung von netzwerk- und sicherheitsbezogenen Unternehmenszielen behindern. Es werden verschiedene Anwendungsfälle für den Einsatz von Zscaler Private Access™ (ZPA™) bei der Migration zu AWS aufgezeigt. Damit soll ein strukturierter Ansatz für die Gesamtlösung bereitgestellt und veranschaulicht werden, wie ZPA die Verlagerung von Anwendungen beschleunigt.

Bei Projekten des privaten und öffentlichen Sektors, an denen Zscaler beteiligt ist, wird ZPA zur Verbesserung der Benutzer- und Anwendungsagilität eingesetzt, was die Anwendungsmigration beschleunigt.

Die Kernfunktion von ZPA besteht darin, den Zugang von autorisierten Benutzern zu — und ihre Interaktion mit — Workloads vor, während und nach der Migration in die Cloud zu regeln und gleichzeitig die Gesamterfahrung der Endnutzer zu verbessern.

Vorteile von Zscaler Private Access (ZPA):

- **Schnellere Verlagerung von Anwendungen und Umstellung auf die Cloud**
- **Granulare Kontrollmechanismen für den User-Zugriff auf Anwendungen in AWS**
- **Verwaltung des Workload-Zugriffs vor und nach der Umstellung**
- **Lückenlose Transparenz für alle Anwendungen bei optimaler User Experience**

Die konzeptionellen Best Practices von Zscaler Private Access spielen eine zentrale Rolle in folgenden Cloud-Migrationsphasen des Kunden:

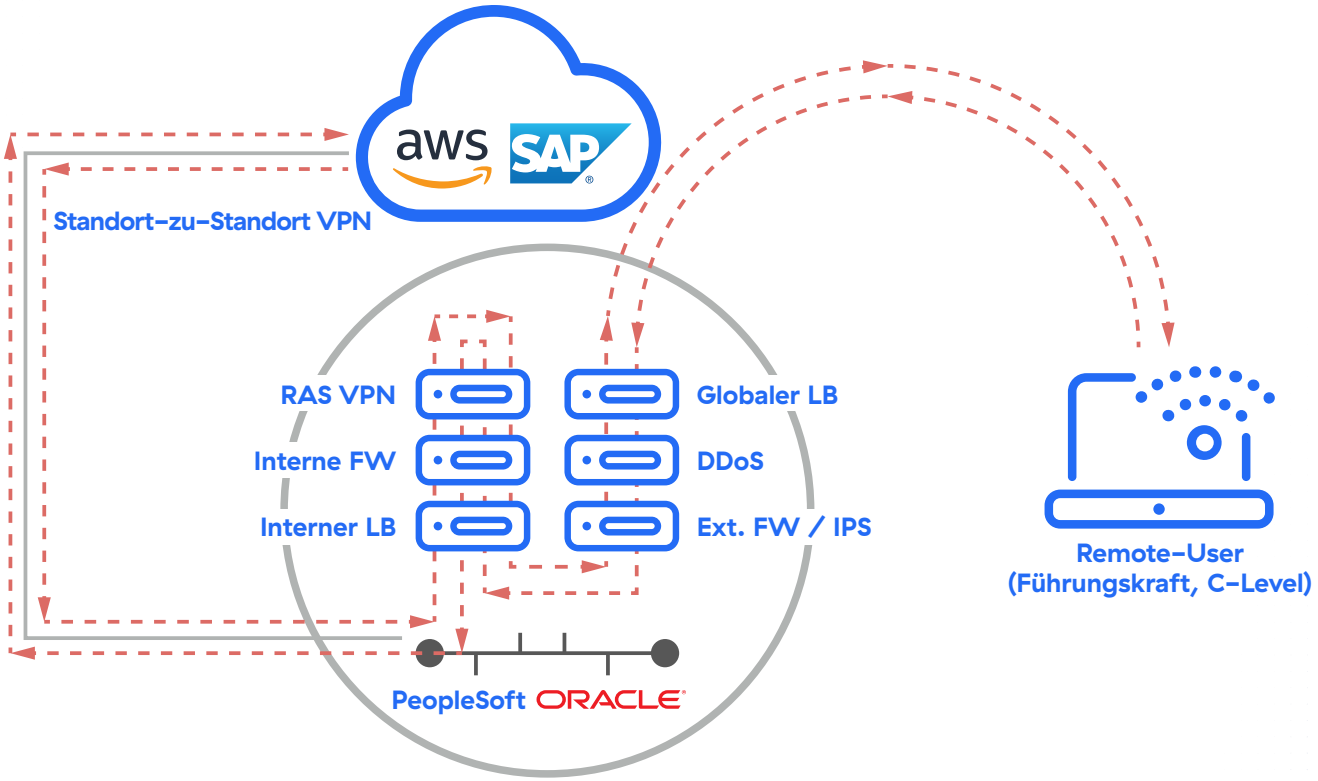
- Vorbereitung und Planung
- Portfolio und Erkennung
- Operative Planung und Durchführung
- Migration und Validierung
- Laufender Betrieb

Obwohl sich dieses Dokument auf die Migration von Workloads zu AWS konzentriert, sind die ZPA-Lösung und verwandte Software Defined Perimeter-Lösungen nicht nur für AWS-Deployments verwendbar. ZPA unterstützt hybride IT-Umgebungen und kann als Ergänzung zu Frameworks für die Anwendungsmigration verwendet werden, die auf Beratungspraxis beruhen.

Zscaler Private Access: Absicherung des Zugangs zu internen Anwendungen

Zscaler Private Access ermöglicht sicheren Zugriff auf interne Anwendungen, die entweder im privaten Rechenzentrum oder in öffentlichen Cloud-Umgebungen gehostet werden können. Zscaler reduziert Kosten und Komplexität herkömmlicher Netzwerk- und Sicherheitsarchitekturen und überzeugt im Vergleich zu VPN-basierten Zugriffslösungen mit einer erheblich verbesserten User Experience.

Die meisten Kunden beginnen mit einer traditionellen, auf das On-Premise-Rechenzentrum konzentrierten, hardwarebasierten Netzwerkinfrastruktur mit zentralisierten Remote-Access-Lösungen wie dieser:



OHNE ZSCALER: Herkömmlicher RZ-basierter Ansatz für Remotezugriff

Zscaler Private Access (ZPA) stellt eine SDP-Lösung (Software Defined Perimeter) bereit. Dabei handelt es sich um einen neuartigen Ansatz, der sich grundlegend von herkömmlichen VPN-Lösungen für den Remotezugriff unterscheidet. Mit SDP profitieren zukunftsfähige agile Unternehmen bei der Umstellung auf die Cloud von einer Lösung, die speziell auf Skalierbarkeit und optimale Anwendererfahrungen ausgelegt ist.

Zscaler Private Access basiert auf unserer globalen Cloud-Architektur und stellt den Zugriff auf interne Anwendungen gemäß dem Zero-Trust-Konzept her. Entsprechend wird keine Verbindung automatisch als vertrauenswürdig eingestuft. Stattdessen müssen User und Gerät bei jeder Zugriffsanforderung über SAML authentifiziert werden. Nach der erfolgreichen Authentifizierung des Users wird eine ausgehende Verbindung von einem App Connector in AWS zur Zscaler-Cloud hergestellt. Dort werden befugte User sicher mit den jeweils benötigten Anwendungen verbunden.

Mit Zscaler Private Access wird der Anwendungszugriff über eine globale Security Cloud vermittelt, sodass das Netzwerk lediglich zum Transport dient. Authentifizierte User werden über granulare richtlinienbasierte Zugriffskontrollen mit den Anwendungen verbunden, für die sie Zugriffsberechtigungen haben. Die öffentliche Cloud-Umgebung des Unternehmens bleibt somit privat.

MIT ZSCALER: Sicherer, richtlinienbasierter Zugriff ohne Platzieren der User im Netzwerk

Da die Sicherheitsstellung von Benutzer und Gerät bewertet wird, bevor Zugriff auf eine Anwendung gewährt wird, bleiben Anwendungen für Benutzer unsichtbar, die keine Zugangsberechtigung haben. Da die Anwendungen über die Zscaler-Cloud geleitet werden, gibt es keine eingehenden Verbindungen zur AWS-Instanz oder zum Rechenzentrum des Kunden, wodurch ACLs und Sicherheitsgruppen einfacher werden. Die Richtlinie basiert auf Informationen über Benutzer/Geräte statt auf Netzwerkobjekten, was für größere Transparenz und Flexibilität sorgt.

Zscaler Private Access ermöglicht Benutzern den gleichzeitigen Zugriff auf zugelassene Anwendungen sowohl in ihren AWS-VPCs als auch in ihren physischen Rechenzentren. Die Abtrennung des Netzwerks vom Benutzer und die Bereitstellung des kürzesten Verbindungspfades zur Anwendung verbessert die Nutzererfahrung, vereinfacht die Netzwerkarchitektur und bietet mehr Transparenz und Kontrolle für die Sicherheit.

Beschleunigung der Anwendungsmigration

Zscaler Private Access kann zur Unterstützung eines vorläufigen Business Case für die Umstellung auf AWS eingesetzt werden.Die Quantifizierung einer bestehenden Anwendungsinfrastruktur bringt zahlreiche Herausforderungen mit sich. Zscaler stellt mit diesem Ansatz ein Framework bereit, das eine nahtlose User Experience sowohl in herkömmlichen als auch in AWS-Umgebungen gewährleistet. Richtlinienbasierte Zugriffskontrolle bietet eine effektivere Alternative zu herkömmlichen Infrastrukturen, deren Konfiguration und Verwaltung mit geringerem Aufwand verbunden ist.

Die Architektur- oder Beratungspraxisleitung kann den Gesamtzeitrahmen für die Migration potenziell verkürzen. ZPA stellt eine Plattform bereit, von der aus der Benutzerzugang während der Migration von Workloads zu AWS kontrolliert werden kann, ohne dass Änderungen an der bestehenden Netzwerkinfrastruktur vorgenommen werden müssen. Es bedarf weder VPN-Hardware als Voraussetzung, um Benutzer mit privaten, in AWS gehosteten Anwendungen zu verbinden, noch AWS Direct Connect, um Remote-Benutzer über den suboptimalen Traffic-Pfad durch das Rechenzentrum in die AWS-Umgebung zu leiten.

Die Einführung der ZPA-Plattform ermöglicht eine granulare Kontrolle des Benutzerzugriffs auf Anwendungen, die in AWS, in mehreren Regionen und in einer hybriden Umgebung gehostet werden. In der Praxis kann dieser Ansatz sowohl den Wechsel in die Cloud vereinfachen, als auch dem Kunden die Möglichkeit geben, während der Migration Vertrauen zu seiner User-Community aufzubauen.

Stärkung des Identitäts- und Access-Management:

- **Anwendungen sind nur für befugte User/Geräte sichtbar, die über SAML authentifiziert wurden**
- **Unterstützt die Abwehr aktueller Bedrohungen und Sicherheitsrisiken wie DDoS-Angriffe und unbefugte Zugriffsversuche externer Dritter**
- **Schränkt die laterale Bewegungsfreiheit ein und verhindert so die Ausbreitung von Malware innerhalb des internen Netzwerks**

Durch die Verbesserung der Nutzererfahrung, der drastischen Reduzierung des Änderungskontrollprozesses, der Bereitstellung von Ende-zu-Ende-Transparenz und der Fähigkeit, mithilfe von zentralisierter Richtlinienverwaltung einzelne Gruppen/Standorte für die Migration auszuwählen, versetzt ZPA Unternehmen in die Lage, schneller zu migrieren und eine optimale Nutzererfahrung zu erzielen.

Wenn Geschäftsanwendungen wie SAP-, Oracle- oder Microsoft-Workloads zu AWS verlagert werden, kommt es häufig vor, dass Networking- und Sicherheitsansätze zurückgestellt werden, um später im Migrationszyklus angegangen zu werden. AWS und APN Consulting Partner Solution Architects berichten regelmäßig über daraus resultierende Reibungen und Verzögerungen. Diese Reibung kann erkannt, antizipiert und vermieden werden, wenn eine elegante, gut durchdachte Lösung wie ZPA beim Projektstart im Planungsumfang enthalten ist.

Dieser Prozess führt Cloud-Architekten sowie IT-, Networking- und Sicherheitsakteure oftmals in einem positiven Diskurs zusammen, der normalerweise kein Bestandteil der Vorbereitungs- und Planungsphase ist.

Für jene Anwendungen wird die Migration zu IaaS angesichts ihres Volumens und des Deployment-Umfangs attraktiv und oftmals offensichtlich sein. Wir stellen jedoch fest, dass es am Anfang in der Regel eine Herausforderung ist, alle Anwendungen zu identifizieren, auf die Benutzer zugreifen und die ebenso verlagert werden sollen. Zeitweise ist die Anzahl der entdeckten Applikationen viel höher als IT-Verantwortliche geschätzt haben. ZPA bietet Erkennung und Reporting von privaten Anwendungen, um Kunden einen Einblick in alle Applikationen zu geben, auf die in ihrem physischen Rechenzentrum zugegriffen wird. Dies hilft der Beratungsfirma und dem Kunden bei der Priorisierung der Applikationen, die zur IaaS-Cloud verlagert werden sollen, und trägt zu besseren Sicherheitskontrollen für diese Anwendungen bei.

Das vereinfacht die Entscheidung, welche Workloads auf AWS umgestellt werden sollen. Die sichere Bereitstellung von Anwendungen, die nicht für eine Cloud-basierte Bereitstellung konzipiert sind, stellt allerdings eine erhebliche Herausforderung dar.

Identitäts- und Access-Management ist eine unverzichtbare Voraussetzung für die Bereitstellung auf IaaS. Zur Verstärkung dieser Zugriffskontrolle können Sicherheitsarchitekturen so konfiguriert werden, dass Anwendungen erst nach erfolgreicher Authentifizierung für User bzw. Geräte sichtbar sind. Dadurch lassen sich neuartige Bedrohungen wie DDoS-Angriffe, unbefugte Zugriffsversuche externer Dritter und die laterale Ausbreitung von Malware im internen Netzwerk abwehren.

Durch Implementierung des Zero-Trust-Modells konnten wir von herkömmlichen Sicherheitslösungen auf einen zukunftsfähigen, sicheren, Cloud-nativen Ansatz umstellen. Damit haben wir zugleich granulare Kontrolle über User-Berechtigungen, sodass alle Mitarbeiter und externen Auftragnehmer ausschließlich auf die jeweils benötigten Ressourcen zugreifen können.

Tony Fergusson, IT-Infrastruktur-Architekt, MAN Energy Solutions

Erhöhte Sicherheit

Zscaler Private Access verwendet ein granulares Richtlinien-Framework, um Benutzer mit Anwendungen zu verbinden, unabhängig davon, wo sich diese Anwendungen befinden. ZPA verbindet Benutzer nicht mit dem Netzwerk, sondern trennt es vollständig vom Benutzer ab. Diese Anwendungskonnektivität hat zahlreiche Vorteile:

- Benutzer können über verschlüsselte TLS-Tunnel, die bei Bedarf hochgefahren werden, auf Anwendungen in verschiedenen Umgebungen (AWS, On-Premise oder Hybrid) zugreifen.
- Benutzer können auf interne Applikationen zugreifen, ohne jemals Zugang zum Netzwerk zu erhalten.
- In den Rechenzentren kann es zu Überschneidungen bei der IP-Adressierung kommen. Aufgrund der Trennung zwischen Netzwerk und User spielt die Überschneidung keine Rolle.
- Die Richtlinien für den Anwendungszugriff werden in der Zscaler-Cloud durchgesetzt. Erst nach erfolgreicher Authentifizierung des Zugriffs für User und Gerät wird eine ausgehende Verbindung zur Anwendung über den betreffenden Anwendungskonnektor hergestellt. Die Anwendungsumgebung ist im Internet unsichtbar, d. h. es werden keine eingehenden Verbindungen zum Gerät oder zur Anwendungsumgebung zugelassen.
- Granulare Richtlinien für einzelne Anwendungen und einzelne User/Attribute können vom Kunden selbst oder einem MSP erstellt und verwaltet werden.

Da Benutzern nur Zugang zu benötigten Anwendungen statt auf das gesamte Netzwerk gewährt wird, bietet ZPA mehr Sicherheit als ein herkömmliches VPN. Dieser Ansatz ermöglicht eine Sicherheitsstellung, die inhärent effektiver vor den gängigsten Formen des Eindringens und vor Malware schützt. Darüber hinaus unterstützt und beschleunigt Zscaler die Einführung eines endgültigen Zero-Trust-Ansatzes für Kunden von AWS.

Im Rahmen des Frameworks für die Umstellung auf AWS ermöglicht ZPA die Durchsetzung anwendungsspezifischer Richtlinien für den User-Zugriff und gewährleistet somit einen konsistenten Ansatz für alle in AWS bereitgestellten Workloads. Indem Usern nur Zugriff auf spezifische Anwendungen gewährt wird, die für ihre jeweilige Rolle unbedingt erforderlich sind, stärkt das Unternehmen seinen Sicherheitsstatus. Neben der User-Rolle können bei der Verarbeitung von Zugriffsanforderungen auch Kontextdaten zum Gerätestatus berücksichtigt werden. ZPA stellt Mechanismen und Methoden zur Verwaltung granularer Kontrollrichtlinien für den Zugriff von Usern und Geräten auf Anwendungen bereit, die AWS-Kunden bei der Einhaltung ihrer Verpflichtungen gemäß dem Modell der geteilten Verantwortung unterstützen.

Wie Zscaler Private Access die Migration zu AWS beschleunigt

Vorbereitung und Planung

Zscaler Private Access kann die schnellere Umstellung auf AWS unterstützen, da mehrere Projektphasen entfallen, die ansonsten zur erfolgreichen Umsetzung der Migration erforderlich wären. Insbesondere wird die Definition von Mindestanforderungen für den User-Zugriff unterstützt — ein wesentlicher, aber häufig vernachlässigter Aspekt der Umstellung.

Mit ZPA können Kunden:

- Identitätsbasierter Zugriff: Zwischen Usern und den jeweils angeforderten Anwendungen wird eine Trennschicht eingebaut.
- Stärkung der Sicherheitsstatus: User, die sich innerhalb des Netzwerkperimeters befinden, werden nicht automatisch als vertrauenswürdig eingestuft. Stattdessen müssen sie sich über eine IAM-Lösung (Identity & Access Management) authentifizieren und erhalten unter Berücksichtigung verschiedener Richtlinienkontrollen Zugriff auf die benötigten Anwendungen. Die Kontrollen können auf SAML-Attributen basieren, die aus der IAM-Lösung übernommen werden.
- Einen risikobasierten Ansatz mit Multifaktorauthentifizierung (MFA) nutzen.
- Die Notwendigkeit von hoch privilegiertem Zugang reduzieren und die Angriffsfläche für jeglichen eingehenden Zugriff drastisch minimieren. Dies wird erreicht, indem Benutzeranfragen für interne Anwendungen abgefangen und Richtlinien durchgesetzt werden, bevor der Benutzer mit der Applikation verbunden wird. Auf diese Weise werden Anwendungen sowohl für das Internet als auch für nicht autorisierte interne Benutzer unsichtbar.
- Reibungslose User Experience: Die Lösung ermöglicht eine transparente Integration in die normalen Arbeitsabläufe — unabhängig davon, ob sich der User über ein unternehmenseigenes oder ein öffentliches Netzwerk verbindet. Wenn der Zscaler Client Connector (früher Zscaler App) installiert ist, muss der User nichts weiter tun, sondern wird unabhängig vom jeweiligen Standort oder Gerät mit den benötigten Anwendungen verbunden.

Die Handlungsempfehlungen zur Umstellung auf AWS werden sowohl von AWS-Kunden als auch in der Beratungspraxis häufig übernommen. Im Folgenden werden weitere Einzelheiten und Vorteile verschiedener Maßnahmen erläutert, auf die darin Bezug genommen wird:

- **Vorbereitung und Planung**
- **Portfolio und Erkennung**
- **Operative Planung und Durchführung**
- **Migration und Validierung**
- **Laufender Betrieb und zukünftige Investitionen**

Portfolio und Erkennung

Viele Kunden sind derzeit auf dem Weg, ein Cloud-First-Unternehmen zu werden. Bei Zscaler wissen wir, dass Kunden bei ihren Initiativen zur Cloud-Migration unter anderem folgende Probleme vermeiden möchten:

- Schlechte Nutzererfahrung im Zuge der Verlagerung von Anwendungen von privaten Rechenzentren in die öffentliche Cloud — verursacht sowohl durch die permanente Instruktion der Benutzer, wie die Anwendungen zu verwenden sind, als auch durch die Komplexität im Zusammenhang mit der Anwendungsleistung.
- Netzwerkkomplexität aufgrund der Anbindung privater Rechenzentren an die öffentliche Cloud.
- Kosten und Komplexität der Dimensionierung, Verwaltung und der Einschätzung der gewünschten Kapazität, die Ihr globales Unternehmen benötigt.
- Erhebliche Sicherheitsbedrohung und Ungewissheit hinsichtlich der Zulassung von vertrauenswürdigen und nicht vertrauenswürdigen Benutzern zum Unternehmensnetzwerk

Zscaler Private Access meistert diese Herausforderungen, indem während der folgenden drei wichtigen Phasen des Sicherheitsdesigns Einblick in interne Applikationen gewährt wird:

- Erkennung: Die Erkennung von Anwendungen auf der Basis von User-Zugriffen liefert wertvolle Informationen zur Nutzung von Anwendungen vor und nach der Umstellung auf AWS.
- Tuning: Für erkannte Anwendungen können vor der Umstellung auf AWS Richtlinien mit Mindestanforderungen definiert werden. Dadurch wird die Exposition von Anwendungen nach der Verlagerung in AWS vermieden und eine schnellere Bereitstellung ermöglicht.
- Produktion: Durch Anwendungssegmentierung wird die schnelle, granulare Durchsetzung von Richtlinien ermöglicht, die zur Gewährleistung der Sicherheit bei Bereitstellung in einer Produktivumgebung erforderlich ist.

Kunden-Spotlight:

Bei einem großen globalen Getränkehersteller wurden über 500 lokal installierte Anwendungen erkannt. Die Aktivierung der Zscaler-Lösung für die IT dauerte 95 Minuten; im Rahmen des Tunings wurden MFA und andere Attribute definiert. Seit dem Ersteinsatz wurden so gut wie keine Änderungen am Produktiv-Deployment vorgenommen.

Zscaler Private Access hilft bei der Beschleunigung der Erkennungsphase, da es sich transparent in den Workflow der Benutzer integrieren lässt. Benutzer greifen einfach auf die gewünschte Applikation zu, ohne zuvor mit einer Sicherheitssoftware, wie einem Endgeräteklienten, interagieren zu müssen. Benutzer brauchen nicht mehr zu lernen, wie auf eine neue oder alte Anwendung zugegriffen wird, und Administratoren haben vollständigen Ende-zu-Ende-Einblick in die Anwendungsnutzung.

Operative Planung und Durchführung

Wenn Kunden die Anwendungen identifizieren, die zu AWS migriert werden, entscheiden sie, wie die Anwendung den Benutzern zur Verfügung gestellt werden soll. Dies geschieht im Wesentlichen in einer von drei Formen:

Virtualisierung — Privat halten

- Analyse der aktuellen Anwendungsarchitektur: In einer dreischichtigen Umgebung (Web-Server, App-Server, Datenbank-Server) werden die einzelnen Komponenten nacheinander virtualisiert und in AWS verlagert.
- Das Front-End könnte als erstes migriert werden, während der App-Server/Datenbank-Server über VPN oder eine zugeordnete Verbindung wie Direct Connect verfügbar bleibt.
- Die Anwendung bleibt „privat“ und nur über VPN oder die dedizierte Verbindung zugänglich.

Zscaler hat uns sehr agil gemacht. Von anderen Abteilungen haben wir sehr viel positives Feedback bekommen, weil sie weiterhin im Homeoffice arbeiten können. Dank Zscaler hat das herkömmliche VPN endgültig ausgedient.“

Marc De Serio, CTO, Henry M. Jackson Foundation (HJF)

Virtualisierung — Öffentlich machen

- Ähnliches Verfahren wie im vorigen Abschnitt beschrieben; jedoch wird der Frontend-Webserver direkt im Internet zugänglich gemacht.
- Die Anwendung ist öffentlich auflösbar.
- Es muss eine Web Application Firewall (WAF) zur Kontrolle von ein-/ausgehenden Inhalten der Anwendung, DDoS-Schutz sowie Identitäts- und Zugangsmanagement für die Einschränkung des Benutzerzugriffs implementiert werden.

Architekturumgestaltung für die Cloud

- Anwendungen, die in ihrer aktuellen Form nicht migriert werden können oder sollen.
- Front-End wird auf EC2 oder serverlos mit CloudFront umgestellt — Web-Server wird umfunktioniert und neu kodiert.
- Middle Tier wird auf EC2 oder serverlos umgestellt — Umfunktionieren der Middleware.
- Back-End wird auf RDS/Aurora/usw. umgestellt — Aktualisierungsschema, DB usw.
- IAM kontrolliert den Zugang; WAF kontrolliert den Inhalt.
- Nutzererfahrung und Zugang ändern sich in Übereinstimmung mit der Migration zu einer neuen Architektur.

Die Entscheidung, Anwendungen öffentlich zugänglich zu machen, bringt ein quantifizierbares Sicherheitsrisiko mit sich. Sowohl beim Netzwerkumbau als auch bei der Virtualisierung wird dieses Risiko in bestimmten Fällen vom Unternehmen als zumutbar eingestuft. Die ZPA-Sicherheitsarchitektur gewährleistet ein identisches Schutzniveau für öffentlich zugängliche Anwendungen mit browserbasiertem Zugriff. Dies beinhaltet die Nutzung von SAML-Authentifizierung in ZPA, die Blockierung eingehender Verbindungen sowie ein identisches Richtlinien-Framework mit der entsprechenden Transparenz.

Bei anderen Anwendungen wie z. B. SAP wiederum wäre die unmittelbare Exposition im Internet mit einem unverhältnismäßig hohen Risiko verbunden. Entsprechend muss die Umstellung auf AWS mit einer Verschärfung der Sicherheitsmaßnahmen einhergehen. ZPA unterstützt Unternehmen nicht nur bei der Planung der Umstellung, sondern ermöglicht auch eine Stärkung des Sicherheitsstatus. Anwendungen, die privat bleiben sollen, werden nicht im Internet veröffentlicht.

Migration und Validierung

Die Analyse der erzielten Fortschritte ist ein wichtiges Element der Umstellung. Zscaler Private Access liefert Informationen zur Nutzung von Anwendungen sowie zur Durchsetzung der entsprechenden Sicherheitsrichtlinien.

Zscaler Private Access fungiert als Trennschicht zwischen User und Anwendung. Anwendungen können vom Rechenzentrum in eine öffentliche Cloud-Umgebung oder auch von einer VPC in eine andere VPC verlagert werden, ohne dass die User Experience dadurch beeinträchtigt wird. User werden niemals direkt mit Anwendungen verbunden; stattdessen wird der Traffic durch den ZPA Cloud-Service geleitet. Der Sicherheitsstatus des Unternehmens wird gestärkt, da die User keinen Netzwerkzugang erhalten. ZPA vermittelt ausschließlich ausgehende Verbindungen vom Rechenzentrum oder einer öffentlichen Cloud zum ZPA Cloud-Service. Entsprechend können die Firewalls oder ACLs im Rechenzentrum jetzt so konfiguriert werden, dass keine eingehenden Verbindungen zugelassen werden. Dadurch wird das Rechenzentrum bzw. die VPC nach außen hin komplett unsichtbar und bietet keine externe Angriffsfläche.

Zscaler Private Access lässt sich für SIEM-Feed und Reporting/Analytik in das Security Operations Center (SOC) des Kunden integrieren. Grafische Darstellung von Anwendungen und Benutzer wird über die ZPA-Verwaltungskonsole bereitgestellt, und es können Richtlinienänderungen vorgenommen werden, um den Benutzerzugriff auf Anwendungen zu kontrollieren.

Zscaler bietet selbst zwar keine Migrations-Services an, unterstützt jedoch den Prozess der Migrationsvalidierung und stellt sicher, dass die gelieferte Nutzererfahrung den Geschäftsanforderungen entspricht. Kunden und Beratern Einblick in die Fortschritte der Anwendungsmigration zu ermöglichen, ist eine wesentlicher Vorteil von ZPA.

Kunden-Spotlight:

Die britische Regierung setzt ZPA zur Bereitstellung von Anwendungen in und Zugriff auf AWS ein. Im Rahmen der Umstellung auf ein Zero-Trust-Konzept wird der Zugriff auf Anwendungen ausschließlich über ZPA ermöglicht.

Laufender Betrieb und zukünftige Investitionen

Mit Zscaler Private Access können AWS und kundenseitige Administratoren weltweit unternehmensspezifische Richtlinien für einzelne Anwendungen und einzelne User erstellen und durchsetzen. Dadurch lässt sich die durch netzwerkbasierte Segmentierung verursachte Komplexität reduzieren.

- Einfache Richtlinien, um den Zugriff basierend auf Identität und Anwendung zu segmentieren.
- Mit ZPA entfällt der Verwaltungsaufwand für die Erstellung und Implementierung adressbasierter Richtlinien. Konkret wird dadurch mehr Agilität im internen Betrieb ohne Beeinträchtigung der User Experience für Anwendungsnutzer möglich. Zur Verlagerung von Anwendungen aus privaten in öffentliche Cloud-Umgebungen kommen DevSecOps-Verfahren zum Einsatz. ZPA gewährleistet, dass Ressourcen in öffentlichen Cloud-Umgebungen privat bleiben.
- Kunden erhalten mehr Transparenz und Kontrolle darüber, auf welche Anwendungen Drittanbieter und Auftragnehmer zugreifen dürfen.
- Zscaler investiert kontinuierlich in die Zscaler-Cloud und die Weiterentwicklung von deren Fähigkeiten. Die Fortschritte basieren auf Erfahrungen und Anforderungen von Kunden, deren Traffic sich auf viele globale Organisationen erstreckt und denen wir einen Umfang und eine Transparenz bieten, die keine Organisation allein replizieren kann. Dadurch wird die Investition in ZPA weiterhin einen Mehrwert erbringen.

Die Infrastruktur herkömmlicher Remote-Access-VPNs stellt ein Risiko für jede Migrationsstrategie dar, da durch Platzierung der User im Netzwerk die Angriffsoberfläche vergrößert wird. Zscaler Private Access eliminiert dieses Risiko durch Implementierung von vier Sicherheitsprinzipien:

- User können mit privat gehosteten Anwendungen (in VPCs oder physischen RZs) verbunden werden, ohne Zugang zu internen Netzwerken zu erhalten.
- Anwendungen niemals für unautorisierte Benutzer freigeben
- ZPA unterstützt Anwendungssegmentierung als weniger komplexe und kostspielige Alternative zur Netzwerksegmentierung, die eng an VPCs, Security Groups und anderen Service-Funktionen ausgerichtet ist.
- Das Internet wird als sichere Netzwerktransport-Option genutzt, sodass Unternehmen nicht mehr auf VPNs angewiesen sind, die die Angriffsfläche vergrößern und die User Experience beeinträchtigen.

Dieser Ansatz bewirkt, dass es keine laterale Bewegung zu nicht autorisierten Anwendungen geben kann. Darüber hinaus bleiben die Anwendungen, auf die der Benutzer nicht zugreifen darf, vollständig unsichtbar; sie können per Port Scan oder anderer Mechanismen nicht entdeckt werden, wenn sie entweder lokal oder aus dem Internet an die gehostete Umgebung übertragen werden. Anwendungen erhalten keine eingehenden Verbindungen direkt von Benutzern.

Kunden-Spotlight:

MAN Energy Solutions gewährt Entwicklungspartnern ausschließlich Zugriff auf die jeweils benötigten DevOps-Umgebungen und Anwendungen. Die Gewährleistung des Zugriffs für externe Partner stellte zuvor eine potenzielle Angriffsfläche dar. Die damit verbundenen Risiken konnten nun minimiert werden, indem identitätsbasierte Zugriffskontrollen verhindern, dass diese User und ihre Geräte im Netzwerk platziert werden.

Fazit

Zscaler Private Access ist primär dafür konzipiert, durch aktive Verwaltung vor, während und nach der Umstellung auf die Cloud befugten Usern den Zugriff auf und die Interaktion mit Workloads zu ermöglichen und dabei eine optimale Anwendererfahrung für Enduser zu gewährleisten.

ZPA bietet eine Reihe von Vorteilen zur Unterstützung der Unternehmenstransformation:

- Verkürzung der Zeitrahmen von Transformation und Migration
- Verbesserung der Sicherheitsstellung von migrierten Applikationen
- Bessere Nutzererfahrung während und nach der Anwendungsmigration

Anwendungsfälle für die Einführung von ZPA:

- Wechsel in die Cloud und Anwendungsmigration
- Fusionen und Übernahmen
- Zugang von Drittparteien

Zscaler Private Access kann in begrenztem Umfang oder als Komplettlösung eingesetzt werden. ZPA baut auf AWS auf, und ZPA Public Service Edge wird in AWS sowie an weiteren Standorten weltweit bereitgestellt. Die Anwendungskonnektoren von Zscaler sind in VPCs implementiert. Der Zscaler Client Connector ist eine ressourcenschonende Anwendung, die alle gängigen Betriebssysteme für PCs und Mobilgeräte unterstützt. Auf Anfrage stellen wir Ihnen gerne eine kostenlose Testversion, einen förmlichen POC oder anstelle des POCs eine schrittweise Produkteinführung bereit. ZPA ist im AWS Marketplace in der Rubrik SaaS-Verträge von Privatanbietern erhältlich.

Quellenangaben

Weitere Ressourcen zur Information:

Homepage von Zscaler: www.zscaler.de

Homepage von ZPA: www.zscaler.de/products/zscaler-private-access

Homepage von ZPA für AWS: www.zscaler.de/products/zpa-for-aws

Support and technische Dokumente: help.zscaler.com/zia?filter=documentation

MAN Energy Solutions: www.zscaler.de/resources/case-studies/man-energy-solutions.pdf

Framework für den Wechsel in die Cloud mit AWS aws.amazon.com/professional-services/CAF/

Prinzip der geteilten Verantwortung bei AWS: aws.amazon.com/compliance/shared-responsibility-model/

zscaler™ | Experience your world, secured.™

Über Zscaler
Zscaler (NASDAQ: ZS) beschleunigt die digitale Transformation, damit Kunden agiler, effizienter, stabiler und sicherer arbeiten können. Zscaler Zero Trust Exchange schützt Tausende Kunden mittels sicherer Verbindungen zwischen Benutzern, Geräten und Anwendungen an jedem beliebigen Standort vor Cyberangriffen und Datenverlust. Die SASE-basierte Zero Trust Exchange ist in über 150 Rechenzentren auf der ganzen Welt verfügbar und die weltweit größte Inline-Cloud-Sicherheitsplattform. Informieren Sie sich auf **zscaler.de** oder folgen Sie uns auf Twitter **@zscaler**.

+1 408 533 0288 Zscaler, Inc. (Hauptsitz) • 120 Holger Way • San Jose, CA 95134, USA zscaler.de