Zscaler Private Access für Microsoft Azure

Sicherer Remote-Access zu internen Applikationen in Azure

zscaler™

SICHERER ZUGANG ZU MODERNEN CLOUD-LÖSUNGEN

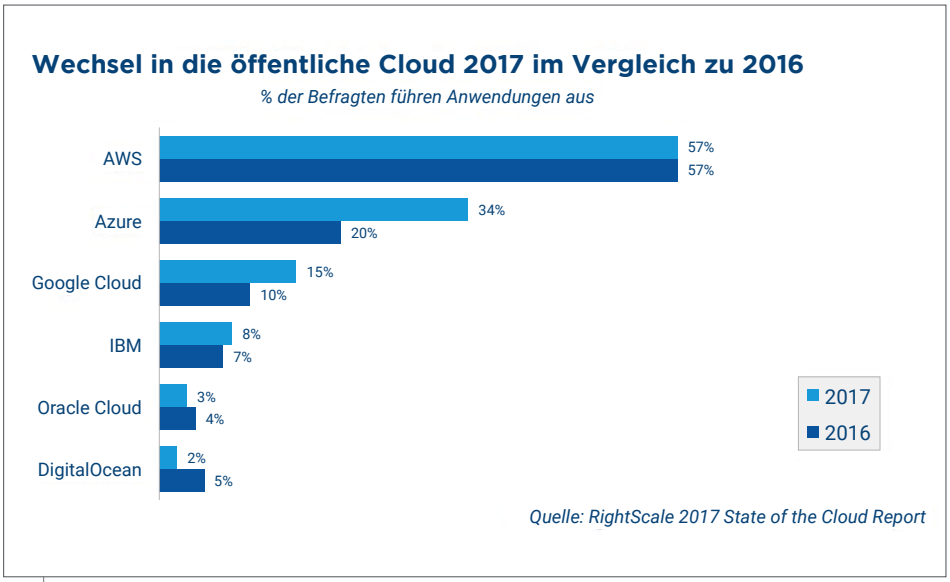
Warum Unternehmen zu Azure wechseln

Microsoft Azure ist zu einem festen Bestandteil der weltweiten IT-Transformation geworden. Mit Azure können Unternehmen ein globales, äußerst flexibles, vernetztes Netzwerk von Microsoft nutzen und dabei Kosten und Komplexität reduzieren, da die Infrastruktur als Service ausgeführt wird. Die Azure-Cloud gibt Unternehmen die Agilität, die sie benötigen, um elastisch zu skalieren und sich an veränderte Geschäftsanforderungen anzupassen.

Immer mehr Unternehmen erkennen diese Vorteile und verfolgen aktiv Initiativen zur Anwendungstransformation, die sich auf die Migration interner Anwendungen zu Azure konzentrieren. Diese Migration hat zum rapiden Wachstum von Azure innerhalb des Unternehmens geführt. 43 Prozent der Unternehmen führen Anwendungen inzwischen in Azure aus.

Azure ist außerdem sehr benutzerfreundlich und erleichtert mobilen Benutzern unabhängig von Standort oder Zeitzone den Zugriff auf Anwendungen und Services. Neben der Maximierung der Benutzerproduktivität haben die Annehmlichkeiten der Cloud zu einer Änderung des Status Quo hinsichtlich der Benutzererwartung geführt. Nachdem Remote-User nahtlosen Zugriff auf Cloud-Anwendungen erlebt haben, erwarten sie nun eine „Cloud-ähnliche“ Erfahrung für alle Applikationen, einschließlich intern verwalteter, in der Azure-Cloud gehosteter Anwendungen.

Damit Unternehmen und deren Benutzer die Vorteile der Verlagerung von Anwendungen in die Cloud ausschöpfen können, ist es jetzt an der Zeit, den Remote-Access zu überdenken.



Laut dem RightScale 2017 State of the Cloud Report stieg die Verwendung von Microsoft Azure innerhalb von Unternehmen im Jahr 2017 stark an.

Anwendungen wurden in die Cloud verlagert. Warum verlässt man sich beim Remote-Access dann immer noch auf das Rechenzentrum?

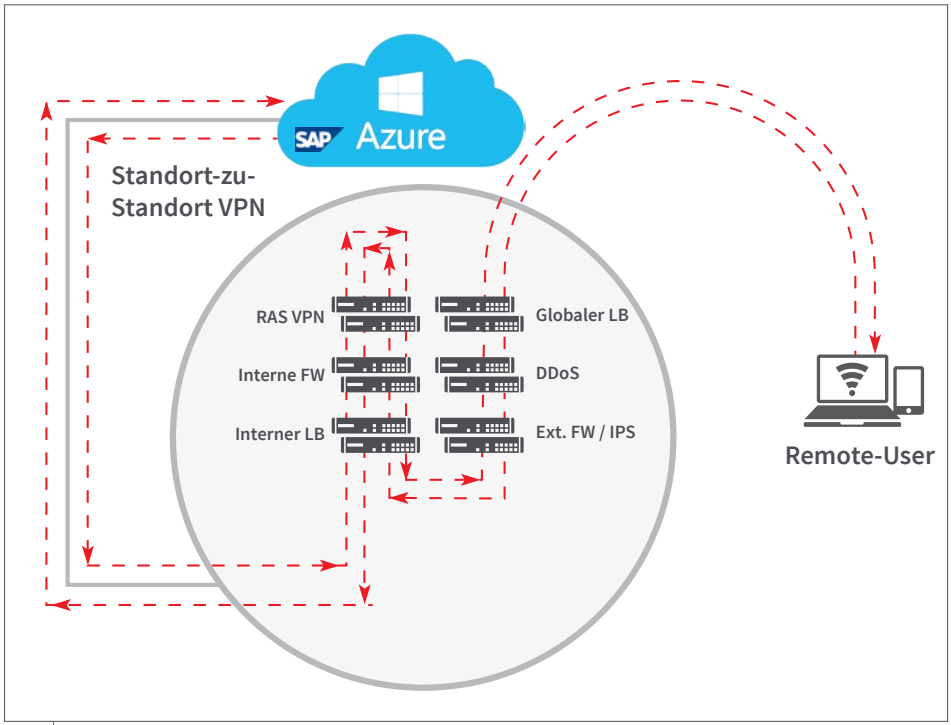
In den frühen Tagen der Cybersicherheit lag der Schwerpunkt auf dem Schutz von Daten und internen Anwendungen, die im Rechenzentrum ausgeführt wurden. Sicherheitsarchitekten hielten den Aufbau eines sicheren Perimeter rund um das Netzwerk für die beste Methode, um diesen Schutz zu gewährleisten. So entstand die Architektur der „Festung mit Burggraben“, mit der viele Sicherheitsteams heute vertraut sind.

Aus Netzwerksicht war eine Sicherheitsarchitektur auf der Grundlage von Festung-mit-Burggraben eine natürliche Ergänzung zum Hosten interner Anwendungen innerhalb eines einzigen Rechenzentrums. Es bedeutete, dass der gesamte Traffic von Remote-Usern oder Niederlassungen für den Zugriff auf Anwendungen per Backhauling zu diesem Rechenzentrum geleitet wurde. In vielen Fällen befand sich dieses Rechenzentrum in einem anderen Teil der Welt.

Inzwischen werden Anwendungen, die sich einst im Rechenzentrum befanden, in die Azure-Cloud verlagert. Dies sprengt den Rahmen eines sicheren Perimeter, da sich die Anwendungen, die geschützt werden müssen, nun außerhalb des Perimeter befinden. Die Hub-and-Spoke-Strategie des Weiterleitens von Traffic an ein zentrales Rechenzentrum ist bei Applikationen, die in Azure ausgeführt werden, ineffektiv. Dennoch sind heutige Lösungen für Remote-Access immer noch darauf angewiesen, Traffic zuerst zum Rechenzentrum weiterzuleiten. Angesichts mangelnder praktikabler Alternativen verwenden Unternehmen weiterhin Remote-Access-VPN.

Seit den 1990er Jahren gab es nur eine Methode, um Remote-Access zu internen Anwendungen zu gewähren: das Remote-Access Virtual Private Network (VPN). Da interne Applikationen aber zu Cloud-Anbietern wie Azure verlagert werden und immer mehr Remote-Mitarbeiter darauf zugreifen, ist es nicht mehr sinnvoll, den Traffic durch das Rechenzentrum zu leiten.

> “DMZs und veraltete VPNs wurden für die Netzwerke der 1990er Jahre entwickelt und sind inzwischen überholt, da ihnen die zum Schutz des digitalen Geschäfts notwendige Agilität fehlt.”
>
> *Gartner*
> September 2016



Der für das Internet bestimmte Traffic von Remote-Usern nimmt einen umständlichen Weg, wenn er durch den Security-Stack des Rechenzentrums geleitet wird, bevor er in die Cloud oder das offene Internet gelangt und danach durch denselben Stack die Rückreise antritt.

Probleme des Remote-Access-VPN

Schlechte Nutzererfahrung
Benutzer, die auf in der Azure-Cloud ausgeführte Anwendungen zugreifen wollen, müssen sich bei einem Remote-Access-VPN anmelden. Ihr Traffic wird durch ein Rechenzentrum statt direkt zu Azure geleitet.

Hohe Kosten und Komplexität
Remote-Access-VPNs benötigen mehrere Gateway-Appliances. Dies erschwert die Skalierung über verschiedene Regionen hinweg, da Teams die Gateways in jedem Rechenzentrum replizieren müssten. Remote-Access-VPNs mindern den Wert der Cloud, wie beispielsweise deren Elastizität, Einfachheit und Kostenersparnisse.

Angriffsrisiko
Remote-Access-VPNs lassen Benutzer auf das Unternehmensnetzwerk zugreifen. Dadurch wird das Netzwerk Malware oder anderen Angriffen auf die Sicherheit ausgesetzt, die von nicht vertrauenswürdigen Benutzergeräten ausgehen. Durch laterale Bewegung können sich Angriffe leichter auf mehrere Applikationen ausweiten.

Direkter Zugang zur Cloud mit Zscaler Private Access

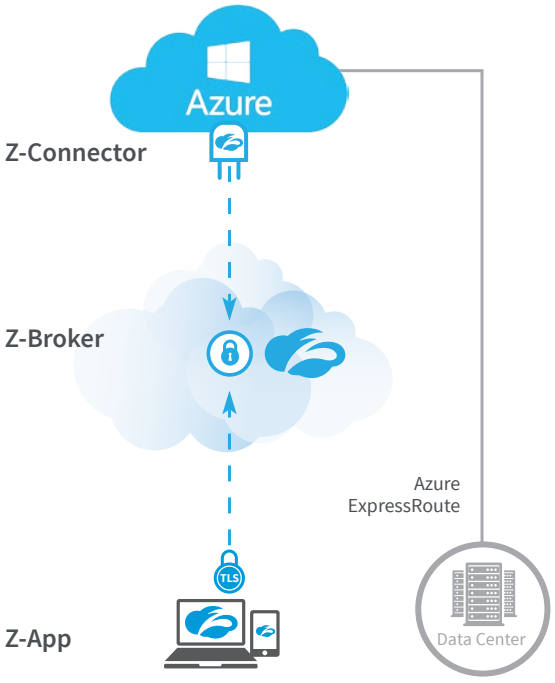
Zscaler Private Access (ZPA™) ist ein revolutionärer Service von Zscaler, der die Zscaler-Cloud nutzt, um sicheren Remote-Access zu internen Anwendungen bereitzustellen. Mit ZPA können sich Unternehmen von der VPN-basierten, auf das Rechenzentrum konzentrierten Denkweise lösen und sich einem moderneren Cloud-basierten Ansatz zuwenden.

Was ZPA so wertvoll macht ist die Fähigkeit, Remote-Usern die nahtlose Erfahrung zu vermitteln, die sie beim Zugriff auf interne Anwendungen erwarten, und Unternehmen gleichzeitig die notwendige Sicherheit und die Einfachheit für eine erfolgreiche Netzwerktransformation zu bieten.

Z-Connector:
ist vor Anwendungen platziert (ausgehende Verbindungen)

Z-Brokers:
Sichere Verbindung vom Benutzer zur Applikation

Z-App:
Fordert den Zugriff auf eine Applikation an



Zscaler Private Access für Azure

Unternehmen können jetzt die Vorteile der Azure-Cloud mit der erweiterten Sicherheit und dem softwaredefinierten Perimeter von ZPA kombinieren. Der Einsatz von ZPA macht Appliances für Remote-Access-VPN überflüssig – und beseitigt die mit ihnen verbundenen Fallstricke. Die ZPA-Lösung bietet allen Benutzern direkten Zugriff auf die Cloud und leitet sie schnell und nahtlos zu der in Azure ausgeführten Anwendung, statt sie über ein Remote-Access-VPN weiterzuleiten.

Schneller Zugriff auf Anwendungen in Azure für externe User

Dank der gemeinsamen Lösung kann Zscaler die globale Präsenz von Microsoft nutzen, um Remote-Usern einen schnelleren direkten Zugriff auf Cloud-Anwendungen innerhalb von Azure zu ermöglichen. Zscaler Enforcer Nodes (ZENs), eine Komponente der ZPA-Lösung, werden im Netzwerk von Azure ausgeführt, das Hunderte von Rechenzentren und weltweite Load Balancer umfasst. Der ZEN vermittelt eine Verbindung zwischen einem mobilen Benutzer und einer Anwendung und leitet anschließend diesen Traffic weiter. Z-Connector, die vor Anwendungen geschaltet sind, werden ebenfalls innerhalb von Azure ausgeführt und stellen ausgehende Verbindungen zu den ZENs her.

Die Kombination von ZPA und Azure garantiert, dass User-Traffic immer den für den Benutzerstandort optimalen Pfad durchläuft. Da Remote-User auf die nächstgelegene Anwendung zugreifen, verbessert sich die Nutzererfahrung und damit auch die Produktivität.

Neben einer schnellen Leistung erhalten Benutzer auch eine nahtlose Erfahrung. Bei einem VPN müssen sich Benutzer jedes Mal neu anmelden, wenn sie auf eine Anwendung zugreifen wollen. Mit der Z-App, die auf dem Mobilgerät des Benutzers installiert ist, brauchen sich berechtigte Benutzer nur einmal anmelden. Auf diese Weise werden Benutzer schneller mit ihren Anwendungen in Azure verbunden.

Mithilfe von Zscaler Private Access und dem Cloud-basierten Sicherheitsansatz von Azure können Unternehmen festlegen, wer auf welche internen Anwendungen zugreifen darf, selbst wenn diese vom Rechenzentrum zu Azure verlagert werden. Die gemeinsame Lösung basiert auf den vier Hauptgrundsätzen von Zscaler Private Access.

1 | **Benutzer befinden sich nicht im Netzwerk –** Benutzer erhalten niemals Zugang zum Unternehmensnetzwerk. Der Zugriff ist anwendungsspezifisch, ohne dass Richtlinien anhand von IP-Adressen oder ACL festgelegt werden müssen.

2 | **Anwendungen sind unsichtbar –** Interne IP-Adressen werden niemals im Internet offengelegt. Interne Applikationen befinden sich auf einem "Dark-Net" des Unternehmens und sind für Benutzer völlig unsichtbar, es sei denn, sie haben eine Zugangsberechtigung.

3 | **Das Internet wird zum neuen sicheren Netzwerk –** Zscaler Private Access nutzt das Internet für dynamische, anwendungsspezifische, TLS-basierte Ende-zu-Ende-Verschlüsselung. Alle Daten bleiben privat und Kunden können ihre eigenen PKIs verwenden.

4 | **Richtlinien ermöglichen eine Segmentierung auf Anwendungsebene –** Benutzer haben keinerlei Zugang zum Netzwerk. Sie können nur auf bestimmte Anwendungen zugreifen und jede Anwendungssitzung erhält einen eigenen Mikrotunnel.

Warum ZPA für Azure?

Bessere Erfahrung für Remote-User

- Schnellerer Zugriff auf Anwendungen in Azure
- Kein VPN-Client mehr für jeden Anmeldevorgang
- Nahtlose Erfahrung für Applikationen innerhalb von Azure oder im Rechenzentrum

Weniger Komplexität für Administratoren

- Einfache Implementierung innerhalb einer Stunde; keine Notwendigkeit zur Einrichtung von VPN-Gateways
- Anwendungssegmentierung, keine Netzwerksegmentierung
- Integration mit Azure AD
- Lässt sich in Anbieter von Single-Sign-On (SSO) wie Okta einbinden
- Kann neben Azure ExpressRoute eingesetzt werden

Sicherer Remote-Access zu internen Applikationen in Azure

- Benutzer sind niemals im Netzwerk
- Auf Richtlinien basierter Zugriff auf bestimmte Anwendungen in Azure
- Kein lateraler Zugang zu weiteren internen Anwendungen
- Sichtbarkeit aller in Azure ausgeführten Applikationen
- Sichtbarkeit sämtlicher stattfindenden Benutzeraktivitäten

Höherer Geschäftswert

- Da keine Hardware erworben werden muss, sinken die Kosten
- Steigerung der Produktivität von Remote-Usern
- Mit dem Dienstleistungsmodell wird die Sicherheit zu einem einfachen, vorhersehbaren Betriebsaufwand

> Zscaler vereinfacht die Reise von Unternehmen zur öffentlichen Azure-Cloud und zu hybriden Umgebungen...

Yousef Khalidi
VP, Microsoft
Azure Networking

Erste Schritte mit Zscaler Private Access und Azure

ZPA und Azure haben den Zugriff auf interne Anwendungen auf eine Art und Weise neu definiert, die den Wechsel in die Cloud und eine mobile Belegschaft möglich machen soll. Mit dieser neuen Lösung wird die Sicherheit – oft als Hemmnis für Veränderungen betrachtet – zum Mechanismus, der die Migration interner Anwendungen zu Azure beschleunigt.

Für weitere Informationen oder um eine Live-Demo zu sehen, kontaktieren Sie Zscaler per E-Mail unter **zpa@zscaler.com** oder besuchen Sie **zscaler.com/zpa-for-azure**.

zscaler™

SICHERER ZUGANG ZU MODERNEN CLOUD-LÖSUNGEN