DATENBLATT

Zscaler Private Access™

Schneller, sicherer Zugriff auf private Anwendungen mit Zero Trust Network Access (ZTNA) aus der Cloud

Unternehmen verlagern private Applikationen, die früher ausschließlich im Rechenzentrum ausgeführt wurden, in öffentliche Clouds. Gleichzeitig suchen sie nach Wegen, wie sie die Produktivität von Benutzern, die von jedem beliebigen Ort aus und auf jedem Gerät arbeiten, gewährleisten können. Der Schlüssel zum Erfolg liegt in der richtigen Balance zwischen Sicherheit und Nutzererfahrung.

Heute weitet sich der Sicherheitsperimeter vom Unternehmensnetzwerk auf jeden Ort aus, an dem sich Benutzer verbinden und Anwendungen ausgeführt werden. Herkömmliche Netzwerksicherheitsarchitekturen sind für moderne Workflows weniger relevant, da sie im Rechenzentrum verankert sind und auf Appliances basieren. Diese Architekturen wurden nicht für die Welt der Cloud und Mobilität konzipiert und waren nie so skalierbar wie ein Cloud-Service.

Netzwerkbasierte Architekturen sind aufgrund von übermäßigem Vertrauen zudem verwundbar. Remote-Benutzer, die sich über eine genehmigte Liste von IP-Adressen (per VPN) verbinden, gelten automatisch als vertrauenswürdig und erhalten Zugang zum Netzwerk über eine Firewall, die häufig dem Internet ausgesetzt ist. On-Premise-Benutzer im Netzwerk können sich lateral darin bewegen. Letztendlich führt inhärentes Vertrauen zu Risiken und überprivilegiertem Netzwerkzugang.

Das Sicherheitsparadigma muss sich vom statischen Netzwerk-Perimeter lösen und sich stattdessen auf die Entität, die Ressourcen und das Benutzergerät konzentrieren. Aufgrund dieser Schwerpunktverlagerung empfiehlt Gartner Unternehmen die Einführung eines ZTNA-Service (Zero Trust Network Access) zur Absicherung des Zugriffs auf private Anwendungen.

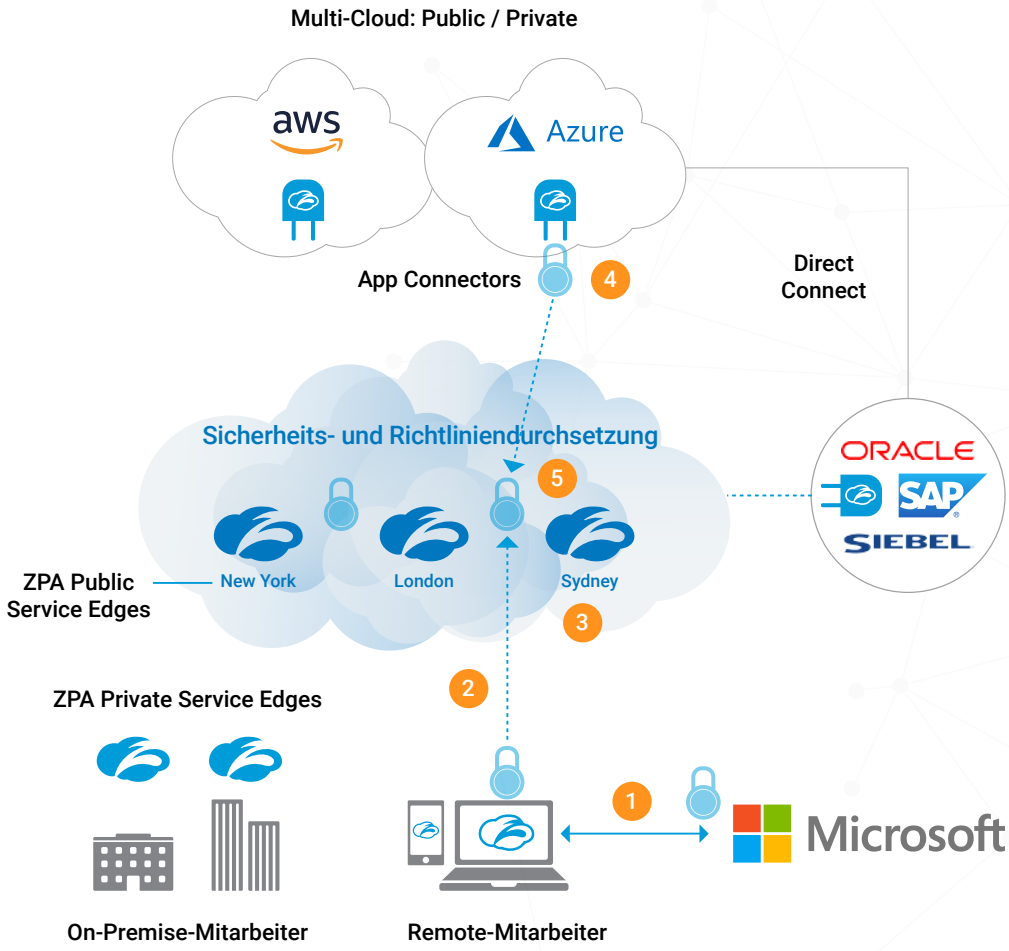
Zscaler Private Access: Zugriff auf private Anwendungen mit Zero Trust Network Access neudefinieren

Zscaler Private Access (ZPA™) ist ein Cloud-Service, der mithilfe einer verteilten Architektur schnellen und sicheren Zugriff auf private Anwendungen On-Premise oder in der öffentlichen Cloud bietet. Der Service gewährt Zugang anhand von vier Grundprinzipien:

- Anwendungszugriff sollte kontextabhängig sein und keinen Netzwerkzugang erfordern
- Es sollten von innen nach außen gehende Verbindungen verwendet werden, um Anwendungen für nicht autorisierte Benutzer unsichtbar zu machen
- Anwendungssegmentierung sollte Benutzer mit einer bestimmten Anwendung verbinden und laterale Bewegung begrenzen
- Das Internet muss zum neuen Transportnetz des Unternehmens werden

Wenn ein Benutzer (Mitarbeiter, Drittanbieter oder Kunde) auf eine Anwendung zuzugreifen versucht, werden die Nutzeridentität und die Gerätestellung mittels Zscaler™ Client Connector Software (ehemals Zscaler App) verifiziert, der auf dem Benutzergerät installiert wird. Die Richtlinien werden überprüft, und eine ZPA Service Edge ermittelt, wo sich die nächstgelegene Anwendungsinstanz befindet. ZPA verwendet den Client-Standort und bestimmt die dem Benutzer nächstgelegene Anwendung, je nachdem, was ein ZPA App Connector (schlanke VM) sehen kann. Schließlich werden zwei ausgehende Tunnel, einer vom Client Connector auf dem Gerät, der andere vom App Connector von einer ZPA Service Edge zusammengefügt. All dies findet automatisch und in Echtzeit statt.

Eine ZPA Service Edge kann entweder von Zscaler in der Cloud gehostet (ZPA Public Service Edge) oder vor Ort in der Infrastruktur des Kunden ausgeführt werden (ZPA Private Service Edge). In beiden Fällen werden sie von Zscaler verwaltet, ohne dass Appliances erforderlich sind. Unten sehen Sie einen Überblick über die ZPA-Architektur



So funktioniert es:

1. Benutzerauthentifizierung mit IDP (nur beim ersten Mal)
2. Autorisierter Benutzer versucht, auf eine Applikation zuzugreifen; Client-Connector-Tunnel wird erstellt
3. Die ZPA Service Edge setzt Richtlinien durch und benachrichtigt alle Connector.
4. Der am nächsten an der Anwendung platzierte App Connector sendet einen von innen nach außen gehenden Tunnel an die ZPA Service Edge
5. Die ZPA Service Edge fügt die Verbindung zwischen Applikation und Benutzer zusammen

Stärkung des Unternehmens mithilfe von ZPA

Vermittlung einer Cloud-ähnlichen Nutzererfahrung

Mit ZPA erhalten Mitarbeiter, Auftragnehmer und Kunden eine völlig nahtlose Erfahrung, denn ZPA:

- Vermittelt eine konsistente Zugangserfahrung sowohl für Remote- als auch für On-Premise-Benutzer
- Lässt sich mit gängigen Identitätsanbietern (Azure AD, Okta, Ping usw.) für Single Sign-On integrieren
- Verwendet Browser-Zugang für Benutzer eigener Geräte und Drittparteien, die auf Web-Anwendungen zugreifen, sodass keine Notwendigkeit für einen Endgeräte-Agenten besteht

Verbesserte Transparenz aller Aktivitäten von Benutzern und Anwendungen

ZPA liefert die Intelligenz, die Administratoren benötigen, um zu verstehen, wer auf Anwendungen zugreift, einschließlich:

- Erkennung von Applikationen, die in Ihrer öffentlichen Cloud ausgeführt werden, und Durchsetzung von granularen Zugangskontrollen
- Ermöglichung von Echtzeit-Einsicht in Benutzeraktivitäten und den Zustand von Anwendungen, Servern, und Konnektoren
- Automatisches Streamen von Audit-Logs der Benutzer zu Ihrem SIEM-Anbieter

Legen Sie granulare Richtlinien auf Basis bestimmter Benutzer und Anwendungen fest

ZPA stellt eine zentrale Plattform bereit, die der IT die Kontrolle über den Anwendungszugriff gibt, indem:

- In der Zscaler-Cloud gehostete Richtlinien verwendet werden, um zu bestimmen, welche Benutzer auf welche Applikationen zugreifen dürfen
- Richtlinien für Benutzer, Benutzergruppen, Anwendungen und Anwendungsgruppen definiert und verwaltet werden
- Anwendungszugriff je nach Benutzer und Applikation als granularere Alternative zur Netzwerksegmentierung segmentiert wird

Gewährleisten Sie sicheren Zugang zu allen öffentlichen und privaten Cloud-Umgebungen

ZPA unterstützt den Zugriff auf Applikationen sowohl im Rechenzentrum als auch in öffentlichen Cloud-Umgebungen (Azure, AWS und GCP), da:

- Sicherer und konsistenter Zugang unabhängig vom Ausführungsort der Applikation ermöglicht wird
- Sowohl VPN Gateway-Security-Stack als auch Backhauling von Traffic zum Rechenzentrum vor dem Weiterleiten in die Cloud überflüssig wird
- Beschleunigung der Applikations-Migration durch Bereitstellung eines ZPA App Connector in nur fünf Minuten

Beschleunigung von M&A und Veräußerungen

ZPA beseitigt Networking als Hindernis für den Erwerb von neuem geistigem Eigentum oder den Verkauf von Unternehmensteilen und bietet folgende Vorteile:

- Verkürzung der Aufbauzeit für Infrastrukturen von acht Monaten auf zwei Wochen
- Keine Notwendigkeit mehr für die Anschaffung von zusätzlichem Equipment (z. B. Firewalls, Router und Switches)
- Nutzung einer einzigen Sicherheitsplattform für alle erworbenen oder veräußerten Vermögenswerte
- Unterstützung mehrerer Identitätsanbieter und Vermittlung einer nahtlosen Nutzererfahrung über einzelne Entitäten hinweg

	ZPA Professional Edition	ZPA Business Edition	ZPA Transformation Edition
Schwerpunkte			
• ZPA-Plattform: Globale Abdeckung (Über 150 Rechenzentren), hohe Verfügbarkeit und niedrige Latenz • Authentifizierung: Support für SAML-Authentifizierung und SCIM • Sicherer Zugriff auf alle privaten TCP- und UDP-basierten Applikationen • Zscaler Client Connector: Agenten für Windows, MacOS, iOS und Android • Unternehmens-Darknet mit DDoS-Schutz • Erkennung von Anwendungen und Servern • Durchsetzung der Standardgerätestellung	✓	✓	✓
Business-Funktionen			
• Browser-Zugang (sicherer Zugriff ohne Client auf browserbasierte Applikationen)	✓	✓	✓
• ZPA Benutzerportal	✓		
• Log-Streaming-Service			
• Kontinuierliche Zustandsüberwachung für alle Applikationen			
• Kontinuierliche Überwachung des App Connector			
Transformations-Funktionen			
• Support für mehrere Identitätsanbieter			✓
• Doppelte Verschlüsselung mit kundenseitiger PKI			
ZTNA-Komponenten			
• Mikrosegmentierung nach Anwendungssegmenten (Benutzer-zu-Applikation)	Bis zu 10	Bis zu 100	Unbegrenzte
• ZPA App Connector	Paare/1.000 Benutzer (maximal: 10)	Paare/500 Benutzer (maximal: 100)	Paare/300 Benutzer (maximal: 300)
• ZPA Private Service Edge für On-Premise ZTNA		Paar/ 10.000 Benutzer (maximal: 5)	Paar/5000 Benutzer (maximal: 10)
• Serverlizenzen für Mikrosegmentierung (Server-zu-Server), erfordert Cloud Connector		1 Server/500 Seats	1 Server/100 Seats
• Mikrosegmentierung für Workloads (App-zu-App), erfordert Edgewise-Service			1 Server/100 Seats
• Zscaler B2B Pro-Plattform – ZTNA für Kunden			1 TB/50.000 Benutzer (maximal: 4 TB)

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, die in 150 Rechenzentren auf der ganzen Welt verfügbar ist, ist die weltweit größte Inline-Cloud-Sicherheitsplattform.

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