Guide für Netzwerkarchitekten zur Beschleunigung von Fusionen und Übernahmen mithilfe eines Zero-Trust-Network-Access-Service

Autor:

Nathan Howe

ZPA Architect, Zscaler

zscaler™

Fusionen und Übernahmen (M&As) können für Geschäftsleiter, CIOs und die für eine erfolgreiche IT-Integration verantwortlichen Netzwerkarchitekten extrem nervenaufreibend sein. M&As sind oftmals hochkarätige Events und müssen so schnell wie möglich abgewickelt werden, damit das Unternehmen eine Kapitalrendite erzielen kann. Aber M&As fungieren auch als Katalysator für eine Modernisierung innerhalb eines Unternehmens, da sie ein Anlass sind, neue Technologien zur Standardisierung der Sicherheit über mehrere Entitäten hinweg einzuführen, um allen Benutzern eine nahtlose Erfahrung zu bieten und die beste Infrastruktur zu implementieren.

Wenn Teams moderne Cloud-basierte Technologien einsetzen wollen, ist es meist Aufgabe der Netzwerkarchitekten, neue Wege für die Verbindung von Benutzern und Anwendungen zu finden, sicherzustellen, dass sich Produkte gut in bestehende Systeme integrieren lassen, und den M&A-Prozess zu beschleunigen. Den richtigen Ansatz zu ermitteln, ist angesichts der Unmenge von relativ neuen Lösungen auf dem Markt nicht einfach, und es muss auch sichergestellt werden, dass ihre Implementierung die Produktivität der Benutzer nicht stört oder den Betrieb behindert.

Um diese Modernisierung zu realisieren, haben viele Netzwerkarchitekten damit begonnen, ZTNA-Services (Zero Trust Network Access) einzusetzen, um Benutzer mit Applikationen zu verbinden. ZTNA-Technologien sind eine schnellere und sicherere Alternative zu den etablierten, netzwerkzentrierten Prozessen, die das Konvergieren unterschiedlicher Netzwerke und das Bearbeiten sich überschneidender IP-Adressen mittels NAT-Verfahren beinhalten – ein Prozess, der alleine schon neun bis zwölf Monate dauern kann.

In diesem Architektur-Guide werden wir folgende Aspekte behandeln:

- Unterschiede in der Architektur herkömmlicher Zugangstechnologien und ZTNA
- Referenzarchitektur für die Bereitstellung von ZTNA während eines M&A-Prozesses
- Phasen, die es bei der Einführung von ZTNA in mehreren Entitäten zu berücksichtigen gilt
- Expertentipps und Überlegungen zur Beschleunigung der IT-Integration bei M&As mit ZTNA

Bevor wir beginnen, nehmen Sie sich bitte einen Moment Zeit, um „A Tale of Two M&A Journeys“ zu lesen. Der Blog vermittelt einen Kurzüberblick über etablierte Methoden der IT-Integration während M&A im Vergleich zu einer ZTNA-basierten Implementierung.

In diesem Guide werden wir ein typisches Unternehmensszenario als Beispiel verwenden. Mutterunternehmen SE, ein Hersteller mit Sitz in Frankfurt, Deutschland, erwirbt Tochterunternehmen PA und muss nahtlos skalieren, um Benutzern das Arbeiten zu ermöglichen und sie in beiden Umgebungen mit wichtigen Anwendungen der jeweiligen Umgebung zu verbinden. Früher bedeutete dies eine Überschneidung des RFC1918-Adressraums, was die Verknüpfung der beiden Netzwerke erschwert. Darüber hinaus plant das Mutterunternehmen weitere Übernahmen und wird eine einheitliche Lösung benötigen, um den Benutzerzugang in den unterschiedlichen Umgebungen zu ermöglichen.

Derzeitige M&A-Architektur von Mutterunternehmen SE

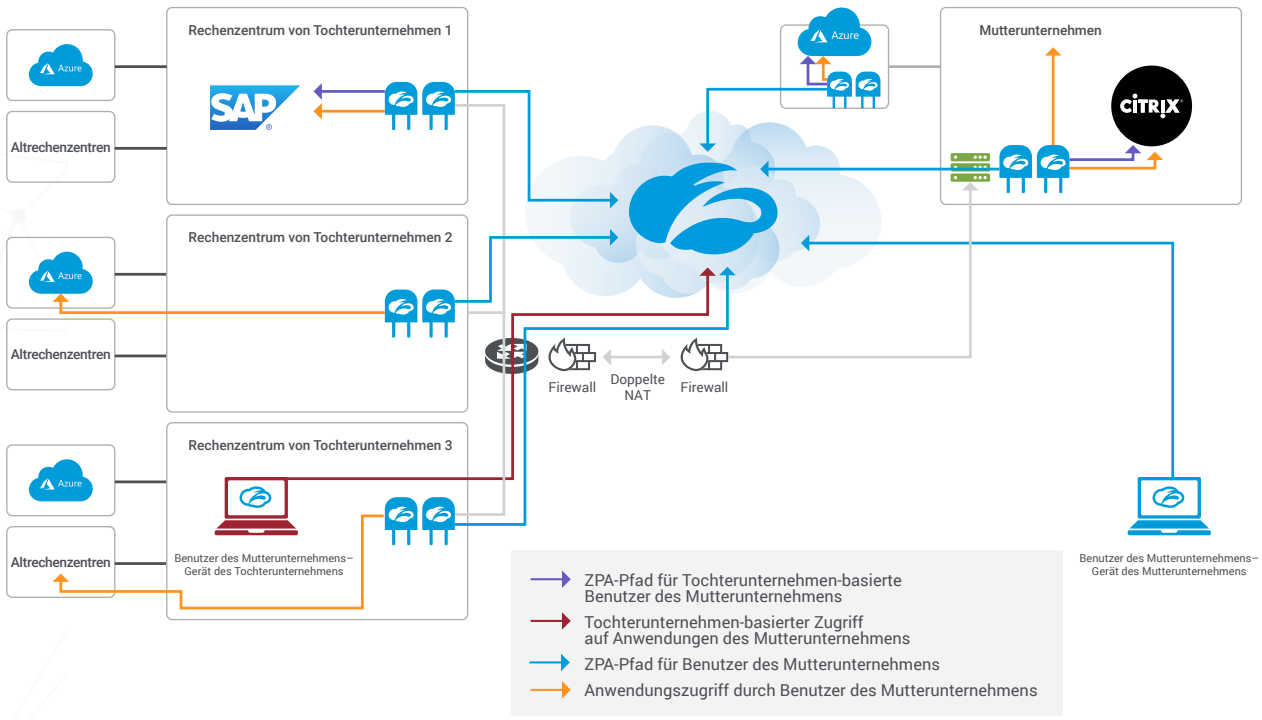
Das Mutterunternehmen beginnt sich damit zu befassen, wie der Zugang entsprechend der neuen Anforderungen geregelt werden kann. Jedes PA ist isoliert und teilt keine Ressourcen, alle nutzen jedoch die Infrastruktur des Rechenzentrums sowie Microsoft Azure. Langfristiges Ziel ist es, die Anwendungen aus diesen Altstandorten, sowohl Rechenzentrum als auch Azure, in das Unternehmensnetzwerk der Mutterfirma (BCN) zu migrieren.

Der derzeitige Zugangspfad für die Geräte des Mutterunternehmens zu den PA-Regionen (und anschließend der umgekehrte Pfad für PA-Benutzer zu den Anwendungen des Mutterunternehmens) führt durch eine traditionelle M&A-Architektur aus vernetzten Firewalls mit doppelten NAT- und DNS-Kontrollen an der Netzwerkgrenze. Dieser komplexe Prozess ist zeitaufwendig und kostspielig, insbesondere für Netzwerke mit erheblicher interner IP-Überschneidung oder unterschiedlichem Grad von Sicherheitshygiene.

Das Mutterunternehmen SE möchte ein einfacheres Architekturmodell, um schnell und problemlos einen granularen unternehmensübergreifenden Zugang bereitzustellen. Das Mutterunternehmen will dieses Modell testen, indem es eine Cloud-basierte Umgebung aufbaut und so tut, als handele es sich dabei um ein M&A-Ökosystem. Man erwägt die Nutzung von Zscaler Private Access™ (ZPA™). ZPA ist der Zscaler™ Software Defined Perimeter, ein Service, der sichere Konnektivität zu privaten Applikationen bietet, die im Rechenzentrum und in Hybrid- oder Multicloud-Umgebungen ausgeführt werden, ohne das Netzwerk für Benutzer zu öffnen.

Die Vision des Mutterunternehmens für eine Architektur von morgen

Die Zunahme von Remote-Benutzern und die Menge der von ihnen konsumierten Anwendungen belasten die Netzwerkinfrastruktur des Mutterunternehmens. ZPA wird die Belastung verringern und es Mitarbeiten und Partnern ermöglichen, ihre Aufgaben so effizient wie möglich zu erfüllen, ohne dass die Sicherheit gefährdet wird. Die IT wird zudem von der größeren Transparenz und Agilität sowie der Vereinfachung profitieren, die ZPA bietet.



Hochrangiger Antrag auf M&A-Zugang beim Mutterunternehmen

Beim Mutterunternehmen benötigen nicht nur mobile Mitarbeiter sicheren Zugang zu Anwendungen; auch die Mitarbeiter im Büro müssen sich direkt mit Cloud-basierten Anwendungen verbinden können. Mit einem ZTNA-Service wie ZPA erhält das Mutterunternehmen:

Globalen, einheitlichen, sicheren und einfachen Zugang: Die Fähigkeit, auf Anwendungen unabhängig von ihrem Standort zugreifen zu können, spielt eine geschäftskritische Rolle. Da sich Applikationen an verschiedenen Standorten befinden, sollten Sicherheits- und Zugangskontrolle auf alle Benutzer weltweit angewendet werden.

Erhöhte Sicherheit, Transparenz und Kontrolle: Der gesamte Traffic-Fluss muss kontrolliert werden, um sicherzustellen, dass nur autorisierte Benutzer auf Anwendungen zugreifen können. Teams haben nun Einblick in alles, worauf Benutzer zugreifen. Darüber hinaus können Sie bisher unbekannte Applikationen identifizieren und dann die entsprechenden Maßnahmen ergreifen.

Kostenvermeidung: Sicherheits- und Netzwerkinfrastruktur, die einst dazu diente, Remote-Benutzern Zugang zu Ihrer Infrastruktur zu gewähren – und sie damit offenzulegen – kann im Rahmen dieses Projekts entfernt werden. Gleichzeitig können die Kosten für VPN, Netzwerkinfrastruktur und Softwareverwaltung minimiert werden.

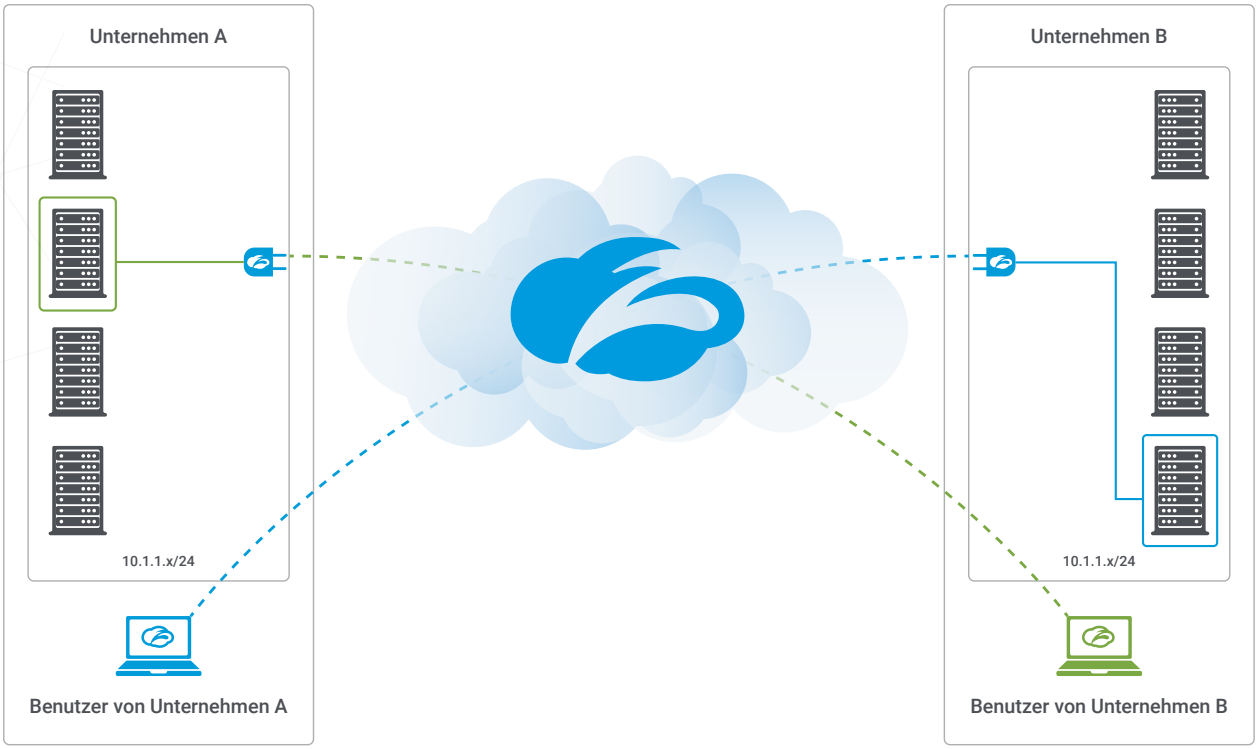
Cloud-Fähigkeit: Wenn Anwendungen in die Cloud und Benutzer in die Mobilität wechseln, kann Sicherheit nur noch am Endgerät oder in der Cloud platziert werden. Mithilfe von ZTNA kann das Mutterunternehmen Cloud-Anwendungen ohne Belastung der Infrastruktur übernehmen.

Abkopplung des Anwendungszugangs vom Netzwerk: Wechseln Sie zu einem Modell des Anwendungszugriffs, das Identität und Stellung statt Netzwerkkonnektivität für den Zugang verwendet.

Beabsichtigter Endzustand des Mutterunternehmens

Wie das Diagramm zeigt, liefert Zscaler einen optimierten Pfad zu Anwendungen im Rechenzentrum oder in Cloud-Umgebungen in globalem Rahmen. Benutzer des Mutterunternehmens werden mit der globalen Cloud-Plattform von Zscaler verbunden und Zscaler wird daraufhin der einzige Pfad für den gesamten privaten Anwendungs-Traffic. Der Ansatz von Zscaler vereint alle Richtlinienkontrollen, das Reporting und die Transparenz auf einer einheitlichen Plattform. Diversität und Ausfallsicherheit werden sowohl durch die verteilte Zscaler-Cloud als auch durch App-Connector-Gruppen und Redundanz gewährleistet. Entscheidend ist, das Zscaler während dieser Umstellung die konsistente Endnutzererfahrung und die Richtlinienkontrollen bereitstellt, die das Unternehmen benötigt.

Wir werden die empfohlenen Phasen der Einführung von ZTNA im Tochterunternehmen durch das Mutterunternehmen untersuchen und wie dadurch allen Benutzern der Zugriff auf private Anwendungen ermöglicht wird, die in ihren Umgebungen ausgeführt werden. Am Ende wird der gesamte für interne Applikationen bestimmte Traffic aus den kombinierten Rechenzentren und Cloud-Umgebungen der Organisation über ZPA an die Zscaler-Cloud weitergeleitet.



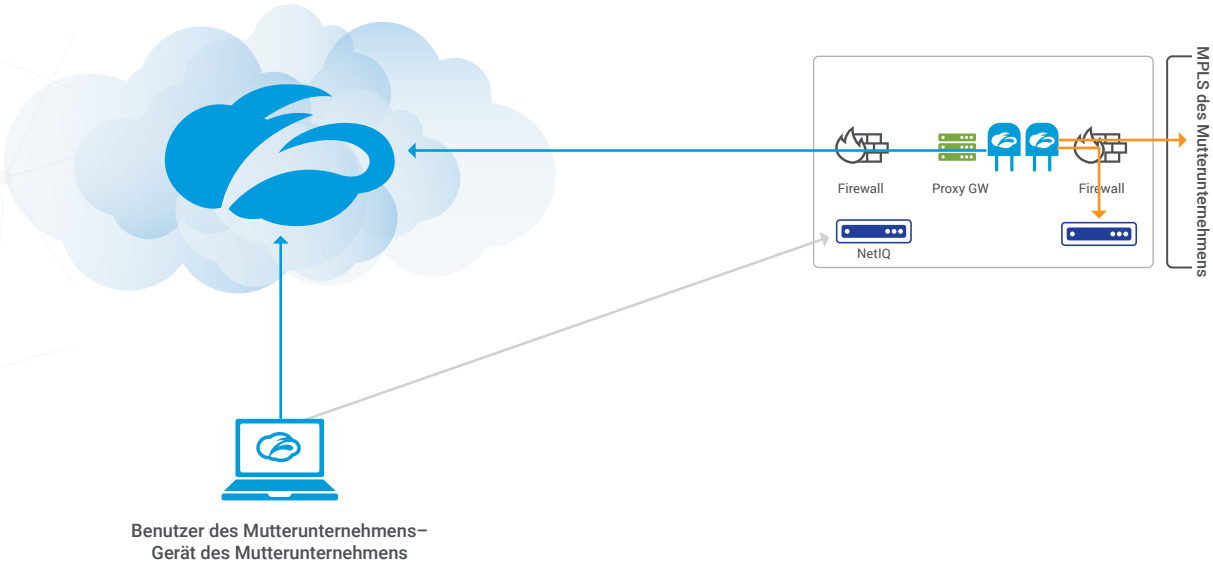
Statt Benutzer ins Netzwerk einzubinden und Konnektivität über einen Remote-Access-Service wie VPN bereitzustellen, ermöglicht ZPA dem Mutterunternehmen den Einsatz einer Software Defined Perimeter-(ZTNA)-Lösung.

Mit dem ZPA-Service werden Anwendungen unabhängig davon, wo sie ausgeführt werden, über Inside-Out-Konnektivität mit Benutzern verbunden, ohne sie ins Netzwerk zu stellen. Anwendungen sind niemals dem Internet ausgesetzt, da sie nicht auf eingehende Pings reagieren. Deshalb sind sie für unbefugte Benutzer völlig unsichtbar, was DDoS-Angriffe verhindert. ZPA entdeckt auch bisher unbekannte Applikationen, die entweder im Mutter- oder im Tochterunternehmen ausgeführt werden, und wendet dann granulare Kontrollen auf sie an.

Ein schrittweiser Ansatz für die Einführung von ZTNA zur Beschleunigung von M&A

Phase 1 Zugangspriorisierung

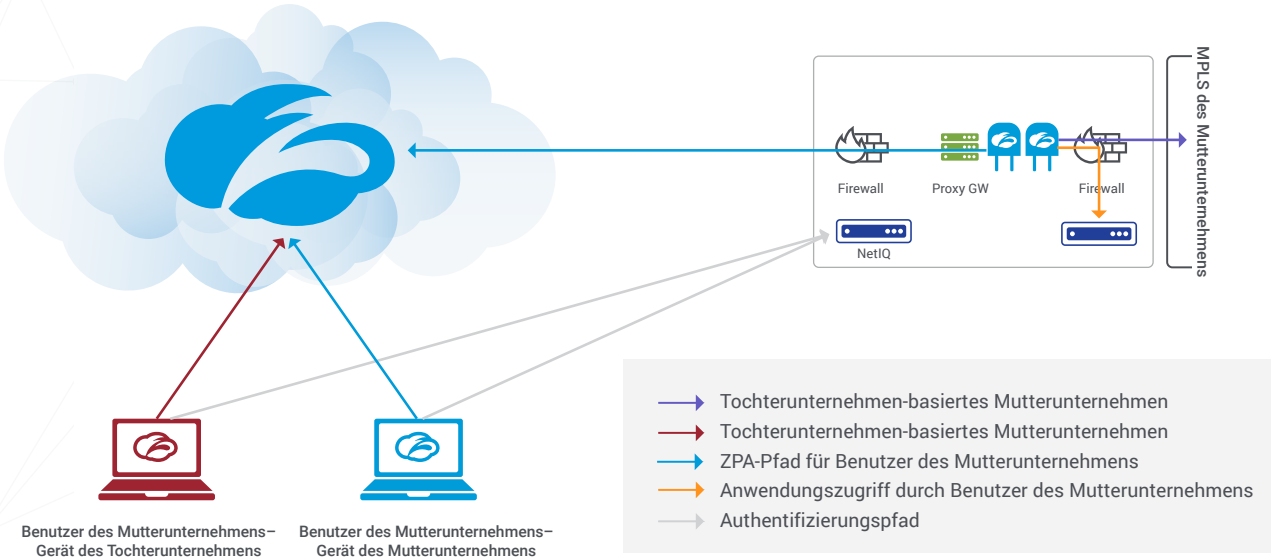
Die erste Etappe dieser Reise sollte die Einrichtung mehrerer Applikations-Connector am Firmensitz des Mutterunternehmens in Frankfurt, Deutschland, sein. Dadurch erhält der Zugangspfad auf Seiten des Mutterunternehmens Ausfallsicherung und Load Balancing. Diese Connector werden weiterhin die Konnektivität für die bestehenden Benutzer des Mutterunternehmens herstellen und so die Kontinuität für die nächste Testphase gewährleisten. Die Connector werden hier ihre Verbindungen zur ZPA-Cloud über den Proxy-Server des Unternehmens herstellen. Dieser Proxy ist eines der drei Haupt-Internet-Gateways des Mutterunternehmens; für den Connector wurde eine bestimmte Regel festgelegt. Alle TLS-Tunnel zu Zscaler laufen über eine Umgehungsregel (authentifiziert und SSL) durch den *serverproxy.MotherCompany.net:8080*.



Zur Authentifizierung wird weiterhin der SAML-Identitäts-Anbieter des Unternehmens genutzt. Sobald Benutzer authentifiziert sind, wird ihr privater Anwendungs-Traffic mittels des ZTNA-Service gesendet und über den in Frankfurt platzierten Connector mit Anwendungen verbunden. Sobald Richtlinienkontrollen entsprechend der Normen des Mutterunternehmens konfiguriert sind, können weitere Benutzer von der veralteten VPN-Plattform (Juniper, Pulse, Cisco AnyConnect usw.) auf ZPA umgestellt werden.

Phase 2 Einbeziehung weiterer M&A-Benutzer

Die zweite Etappe bei der Reise des Mutterunternehmens mit ZTNA sollte die Ermöglichung des Zugangs für eine Reihe von Testbenutzern sein, die Geräte des Tochterunternehmens verwenden. Diese Geräte werden mit Anwendungen verbunden, die innerhalb des Ökosystems des Mutterunternehmens ausgeführt werden. Nach Abschluss wird dieser Test über den ZTNA-Service die erfolgreiche und sichere Konnektivität zwischen neuen Benutzern und bestehenden internen Anwendungen im Ökosystem des Mutternehmens belegen.



Phase 3 Vollständige M&A-Abwicklung

In dieser Phase sollten Sie den granularen Zugriff auf interne Anwendungen durch Benutzer des Mutterunternehmens und Benutzer des Mutterunternehmens mit Geräten des Tochterunternehmens definieren, sodass nur bestimmte Benutzer Verbindungen zu bestimmten Anwendungen herstellen können. Diese granularen Zugangsregeln sind der Grundstein zum Aufbau eines vollständigen Zero-Trust-Sicherheitsmodells, das zukünftige IT-Operationen des Mutterunternehmens antreiben kann.

Die Bereitstellung von granularem Anwendungszugang, Transparenz und Kontrolle ist fundamentaler Bestandteil von ZTNA-Services wie ZPA. Außerdem ist die Installation einfach und kann in drei Hauptbereiche unterteilt werden:

01 Anwendungsdefinition und granulare Richtliniendefinition

Die Kriterien für den Zugang basieren auf Benutzerattributen, die über die Verzeichnisdienste des Mutterunternehmens zugeteilt werden. Durch Angleichung dieser Mitgliedschaften, Attribute und Aufgaben können die Zugangsrichtlinien verwendet werden, um zu kontrollieren, wer genau dazu berechtigt ist, auf die Anwendungen des Mutterunternehmens zuzugreifen.

02 Beispiele für solche Kontrollen könnten sein:

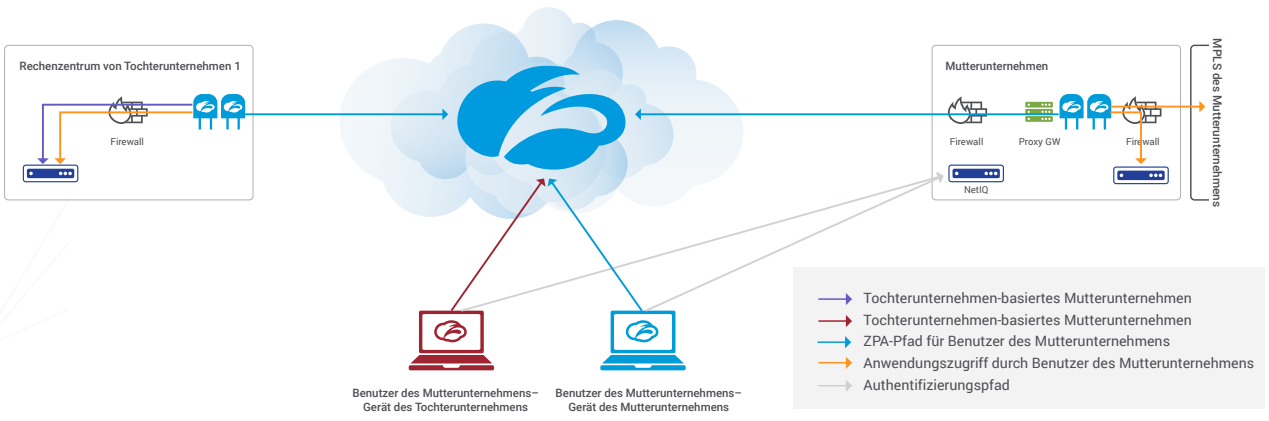
- Definition von spezifischen Richtlinien für den Zugriff von Mitarbeitern auf Anwendungssegmente, wobei die Benutzeridentität als Kontrolle dient.
- Drittparteien den Zugang zu bestimmten Anwendungen ermöglichen, wobei zur Kontrolle sowohl festlegt wird, wer darauf zugreift als auch auf was zugegriffen wird

03 Applikations-Erkennung

Das Überprüfen der im Rahmen des Erkennungsprozesses identifizierten Anwendungen ermöglicht es dem Mutterunternehmen, bestimmte Anwendungen „auszumerzen" und Richtlinien festzulegen, um den Zugriff auf diese Applikationen entweder zu blockieren oder zu genehmigen. Zscaler empfiehlt, entdeckte Anwendungen in Kategorien einzuteilen, die es dem Mutterunternehmen erlauben, prioritätsorientierte Maßnahmen zu ergreifen, beispielsweise kritische, mittlere und niedrige Priorität.

Diagnostikanalyse zur Gewinnung von Erkenntnissen

Der Inhalt der Diagnostik innerhalb des ZTNA-Service gibt dem Mutterunternehmen die Möglichkeit, Probleme in der Netzwerkinfrastruktur zu analysieren, zu überprüfen und zu verstehen. Durch Fokussierung auf Fehler- und Richtlinienblockierung kann das Team des Mutterunternehmens falsch konfigurierte Anwendungen, Netzwerke und selbst die Latenzzeit des Anwendungszugriffs identifizieren.



Zusätzlich zur zentralisierten Kontrolle der ZTNA-Umgebung, die es ermöglicht zu definieren, wer auf was zugreifen darf, kann das Mutterunternehmen den Zugang auf Netzwerkebene isolieren und definieren, indem Firewall- oder ACL-Kontrollen im Netzwerk des Mutterunternehmens durchgeführt werden (die genauen Designanforderungen müssen von den Sicherheits- und Netzwerkteams des Mutterunternehmens ermittelt werden.) Mithilfe des ZTNA-Service kann das Mutterunternehmen eine höchst sichere Isolation aufbauen, indem ein Connector zum alleinigen eingehenden Pfad zu Anwendungen bestimmt wird.

Da der ZPA App Connector überall im Netzwerk des Mutterunternehmens platziert werden kann, um ausgehenden Traffic über einen Proxy-Service weiterzuleiten, kann das Mutterunternehmen entscheiden, wie granular die Connector auf Netzwerkebene verteilt werden.

Phase 4 Einbeziehung der Cloud

Sobald der Zscaler-Service am Hauptapplikationsstandort des Mutterunternehmens und an den Standorten des Tochterunternehmens in Betrieb ist, wird ZTNA den direkten und sicheren Zugang zum Standort der öffentlichen Cloud ermöglichen. Bei Azure beispielsweise erfolgt der Zugriff durch Platzierung des App Connector innerhalb der notwendigen Regionen oder Ressourcengruppen von Microsoft Azure, je nach Architektur des Mutterunternehmens. Im Fall von ZPA findet der Anwendungszugriff standardmäßig und dynamisch den jeweils direktesten Pfad vom Benutzer zur Anwendung und dirigiert den für Azure bestimmten Traffic so über den verfügbaren Connector.

Da das Mutterunternehmen Azure auch in Zukunft nutzen will, können seine Netzwerkteams einfach weitere ZPA App Connector in den entsprechenden Azure-Regionen einsetzen. Auf diese Weise können die Cloud-Ziele für einen flexiblen, nahtlosen, granularen Anwendungszugriff sowohl heute als auch in der Zukunft umgesetzt werden.

Schlussgedanken

Durch die Einführung von ZTNA kann das Mutterunternehmen SE zu einem Modell wechseln, bei dem die Klientenrechner nicht im selben Netzwerk wie die Produktionsdienste betrieben werden. Anstatt des Netzwerksitzes werden Benutzeridentität und Gerätekontext zu den Kontrollen, auf deren Basis Zugang zu den Anwendungen gewährt wird. Solche Kontrollen stehen im Einklang mit Bestrebungen, das Service-Netzwerk vom Benutzernetzwerk abzutrennen.

Wir hoffen, dass die in diesem Architekturdokument enthaltenen Ratschläge für Sie hilfreich waren. ZTNA hat die Art und Weise, wie Teams Sicherheit gewährleisten, grundlegend verändert und es ihnen ermöglicht, die Integration im Verlauf von M&A von neun bis 12 Monaten auf wenige Wochen zu verkürzen. Wir empfehlen Ihnen, ZTNA unbedingt für Ihre nächste M&A-Transaktion in Betracht zu ziehen.

Zscaler hat viele Unternehmensarchitekten dabei unterstützt, ZTNA erfolgreich zu konzipieren und zu implementieren, um neu zu definieren, wie sie den Zugriff auf ihre Anwendungen während eines M&A-Prozesses absichern können. Mithilfe der ZTNA-Lösung von Zscaler können Architekten ihre Aktivitäten vereinfachen und standardisierte Sicherheitspraktiken für alle Applikationen und Assets in diesem Prozess bereitstellen.

Um mehr über Zscaler zu erfahren und wie man Zscaler zur Beschleunigung von Fusionen und Übernahmen sowie bei Veräußerungsprozessen einsetzen kann, besuchen Sie zscaler.com/solutions/MA-divestitures.

Sie können sich auch bei einem kostenlosen 7-tägigen Testlauf von ZPA anmelden: zscaler.com/zpa-interactive

Zscaler, Inc.
110 Rose Orchard Way
San Jose, CA
+1 408 533 0288
www.zscaler.com