Zscalerが実現するAWSへのシンプルで安全な移行

AWSクラウド導入フレームワークへの
Zscaler Private Accessのマッピング

目次

はじめに

本書では、Zscaler™がネットワークとセキュリティの目標を達成するためにさまざまな課題を解消し、導入を加速させる方法を解説します。Zscaler Private Access (ZPA)™がAWSへの移行におけるユースケースにどのように適用されるかを理解することで、ソリューション全体に対する構造化されたアプローチを提供できるほか、ZPAがアプリケーションの移行を実現する方法を詳細に把握できます。

Zscalerを一般企業や公的機関のプロジェクトに採用する場合、ZPAアーキテクチャーは、ユーザーやアプリケーションの俊敏性を強化し、アプリケーションの迅速な移行に不可欠な要素となります。

ZPAは、クラウドへの移行前、移行中、移行後のすべての段階において、承認されたユーザーによるワークロードへのアクセスや操作を常に管理し、エンドユーザー エクスペリエンス全体を向上させるうえで重要な役割を果たします。

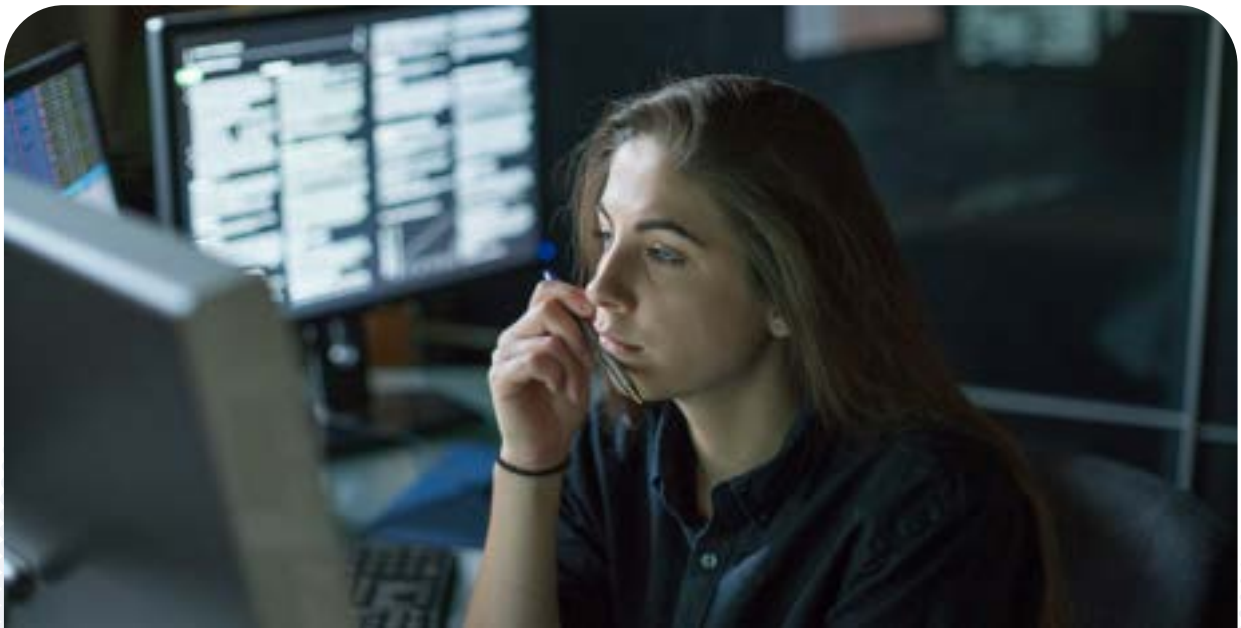
Zscaler Private Accessアーキテクチャーのベスト プラクティスは、クラウドへの移行に発生する以下のフェーズで中心的な役割を果たします。

- 準備と計画
- ポートフォリオと検出
- 運用計画と配信
- 移行と検証
- 継続的な運用

Zscaler Private Access (ZPA)のメリット：

- **アプリケーションの移行とクラウド導入の迅速化**
- **AWSでホストされているアプリへのユーザー アクセスをきめ細かく制御**
- **移行前後のワークロード アクセスをアクティブに管理**
- **アプリの可視性をエンドツーエンドで提供し、ユーザー エクスペリエンスを向上**

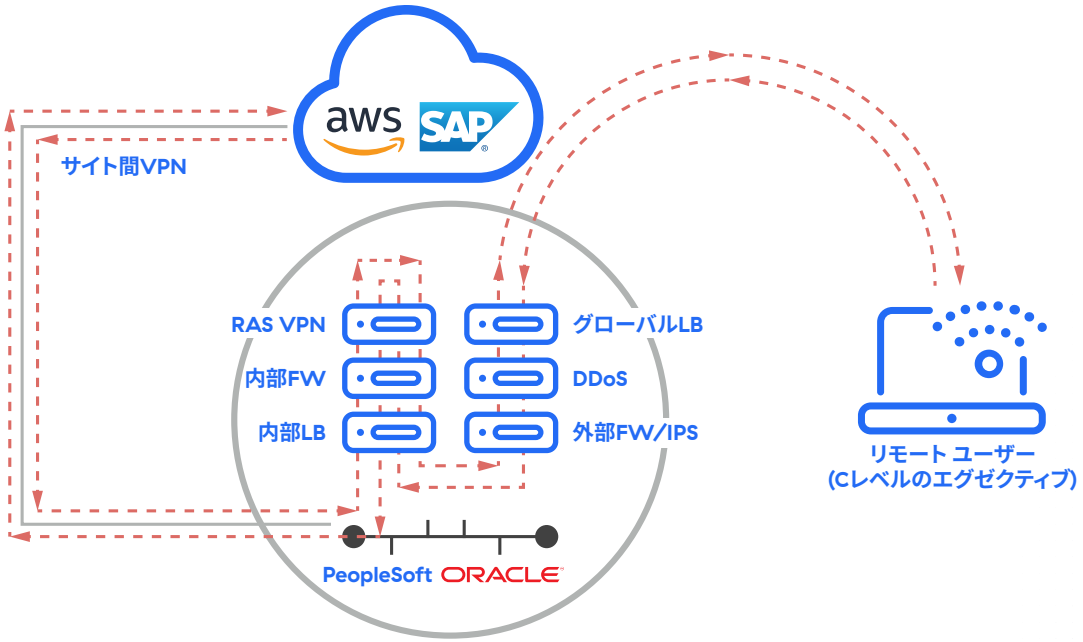
本書では、ワークロードをAWSへ移行させるプロセスを中心に説明しますが、ZPAソリューションや関連するソフトウェア定義の境界ソリューションは、AWSの導入だけに限定されるものではありません。ZPAは、ハイブリッドのIT環境をサポートし、コンサルティング業務で定義されたアプリケーション移行フレームワークを強化するためにも利用できます。



Zscaler Private Access: 内部アプリケーションへのアクセスの保護

Zscaler Private Accessは、プライベート データセンターまたはパブリック クラウドのどちらでホストされている場合であっても、内部アプリケーションへの安全なアクセスを提供します。Zscalerは、これまでのVPNベースのネットワーク アクセスのエクスペリエンスを向上させるとともに、従来のネットワークとセキュリティの課題を解消してコストや複雑性を軽減します。

多くの組織は、オンプレミスでデータセンター中心のハードウェア ベースの従来型ネットワーク インフラストラクチャーを、次のような一元化されたリモート アクセス ソリューションへと移行することから始めます。

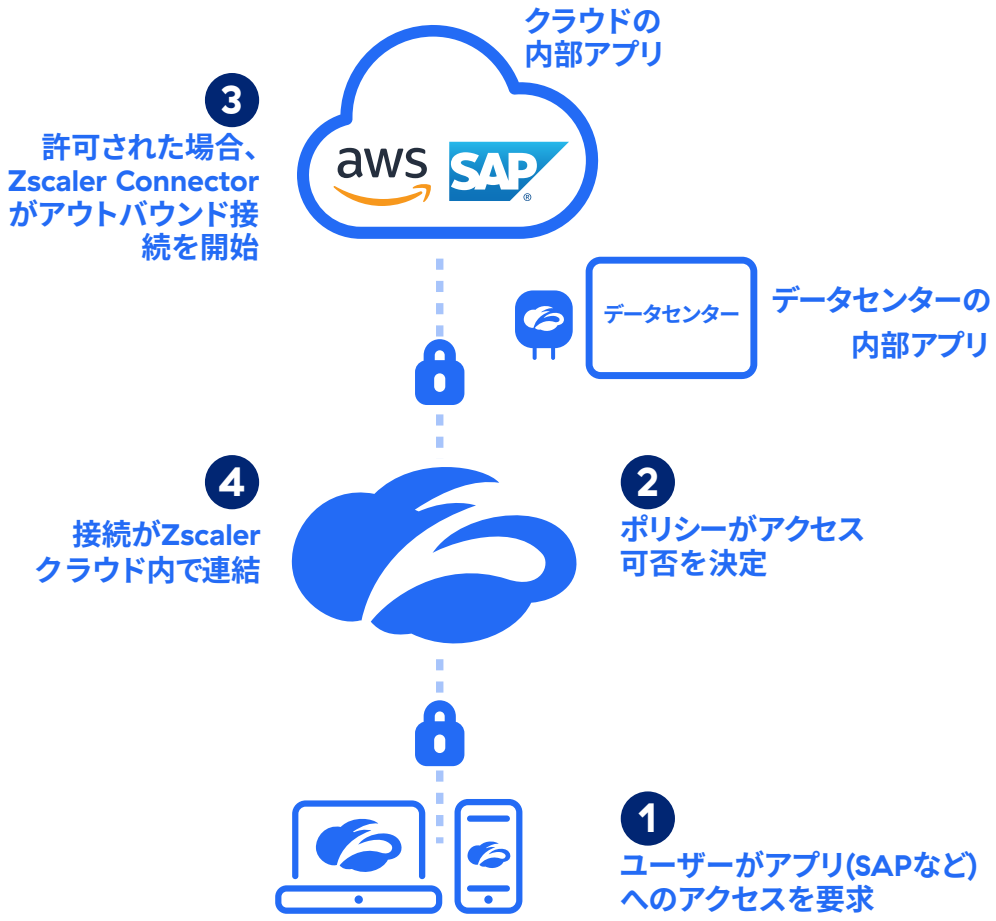


従来のデータセンター中心のリモート アクセス アプローチ(Zscaler導入前)

Zscaler Private Accessは、ソフトウェア定義の境界(SDP)ソリューションを提供します。ユーザー エクスペリエンスに重点を置いたこのソリューションは、クラウドに移行する現代のアジャイルなビジネス コミュニティーの拡張やその他のニーズに対応する目的に特化しており、従来のリモート アクセスVPNソリューションとは根本的に異なります。

Zscalerのグローバル クラウド アーキテクチャーを活用するZscaler Private Accessは、プライベート アプリケーションへのゼロトラスト アクセスを確立します。ユーザーとデバイスはSAMLを介した認証に基づいて信頼され、ユーザーが認証されると、AWSのApp ConnectorからZscalerクラウドへのインサイドアウト接続が提供されます。そして、承認されたユーザーとそのアプリケーションの間に安全な接続が確立されます。

Zscaler Private Accessでは、アプリケーションへのアクセスはグローバルなセキュリティ クラウド経由でフェデレーションされるため、ネットワークは単なる輸送手段に過ぎません。きめ細かなポリシーベースのアクセスを使用して認証されたユーザーを承認されたアプリケーションに接続するため、パブリック クラウドをプライベートに保つことができます。



ユーザーをネットワークに接続することなく、
ポリシーに基づいた安全なアクセスを提供するZscaler

ユーザーやデバイスのセキュリティ態勢は、アプリケーションへのアクセスが許可される前に検証されるため、アクセス権がないユーザーにアプリケーションが表示されることはありません。また、アプリケーションがZscalerクラウド経由でフェデレーションされるため、AWSや組織のデータセンターへのインバウンド接続が発生せず、ACLとセキュリティ グループがシンプルになるというメリットもあります。また、ネットワークではなく、ユーザーとデバイス情報に基づいたポリシーであるため、可視性と柔軟性も向上します。

Zscaler Private Accessによって、AWS VPCあるいは物理データセンターのどちらであっても、許可されたアプリケーションに同時にアクセスできるようになります。ネットワークをユーザーから抽象化し、アプリケーションへの最短パス接続を提供することで、エクスペリエンスが向上し、ネットワーク アーキテクチャーが簡素化され、セキュリティに対する可視性と管理を強化できます。

アプリケーションの迅速な移行

Zscaler Private Accessを活用して、移行の予備的なビジネス ケースをサポートすることができます。既存のアプリケーション インフラストラクチャーを定量化する課題は多岐にわたりますが、Zscalerのこのアプローチを通して、従来の環境とAWSの環境の両方でシームレスなユーザー エクスペリエンスを実現するフレームワークが提供されます。従来のインフラストラクチャーとそれに関連する構成、および継続的な管理業務に代わるものが、ポリシーベースのアクセス制御です。

移行の全体的なスケジュールを短縮できるのは、アーキテクチャーやコンサルティング業務の責任者にとってメリットになります。ZPAは、従来のネットワーク インフラストラクチャーを変更することなく、AWSへのワークロード移行時にユーザー アクセスの管理を可能にするプラットフォームを提供します。AWSでホストされるプライベート アプリケーションにユーザーを接続する際の要件であった従来のVPNハードウェアが不要となるほか、AWS Direct Connectでリモート ユーザーが最適ではないトラフィック パスでデータセンターを経由し、AWS環境に接続されることもなくなります。

ZPAプラットフォームの採用により、AWS、複数の地域、ハイブリッド環境でホストされるアプリケーションへのユーザー アクセスをきめ細かく制御できます。このアプローチによって、クラウドの導入が簡素化され、安全に移行を進められるようになります。

ZPAは、ユーザー エクスペリエンスの向上、変更管理プロセスの大幅な削減、エンドツーエンドのアプリケーションの可視化、一元的なポリシー管理による移行対象のグループや場所の選択を可能にすることで、迅速な移行と快適なユーザー エクスペリエンスを実現します。

強化されたアイデンティティーおよびアクセス管理：

- **事前承認されていないユーザーやデバイスにはアプリを非表示**
- **DDoS攻撃やサードパーティーからの不正なアクセスなどの最新のセキュリティ脅威に対処**
- **マルウェアによる内部ネットワークの水平移動を制限**

SAP、Oracle、Microsoftのワークロードなどのビジネス アプリケーションをAWSに移行する場合、ネットワークやセキュリティのアプローチが移行計画の遅い段階に先延ばしされる傾向にありますが、これにより多くの問題や遅延が発生していることが、AWSやAPNのコンサルティング パートナー ソリューション アーキテクトからも報告されています。プロジェクトの開始時にZPAなどの明確で優れたソリューションを組み込むことで、これらの課題を正しく理解し、予測して回避できるようになります。

このプロセスによって、クラウド アーキテクト、IT、ネットワーク、セキュリティの関係者が、準備と計画の段階から連携して移行に取り組むベースを形成できます。

導入の規模や範囲を考慮した場合、IaaSへのアプリケーションの移行は非常に有益です。しかし、最初に直面する一般的な課題として、ユーザーがアクセスするすべてのアプリケーションに加えて、移行対象とするアプリケーションも特定する必要があります。そして多くの場合、IT担当者の予測をはるかに上回る数のアプリケーションが検出されることになります。ZPAは、プライベート アプリケーションの検出とレポートの機能で、物理データセンター内のアクセスされるすべてのアプリケーションを可視化します。これにより、コンサルティング組織や企業がIaaSクラウドに移行するアプリケーションに優先順位を設定し、それらのアプリケーションに対するセキュリティ制御を強化できるようになります。

AWSに移行するワークロードを特定することはできますが、アプリケーションをユーザーに安全に提供するにあたって、アプリケーションがクラウド配信用に設計されていない場合は大きな課題となります。

IaaS経由での提供には、アイデンティティーとアクセスの管理は不可欠です。しかし、事前に承認されたユーザーやデバイス以外のすべてのユーザに対してアプリケーションを非表示にすることで、このアクセス制御をさらに強化できます。これは、DDoS攻撃、サードパーティーからの不正なアクセス、そしてマルウェアによる内部ネットワークの水平移動など、最新のセキュリティ脅威への対処に有効です。

従来のアプローチから脱却し、クラウドファーストのセキュアなゼロトラスト モデルに移行したことで、従業員や請負業者のアクセス権を細かく制御できるようになりました。

MAN Energy Solutions、ITインフラストラクチャー アーキテクト、
Tony Fergusson氏

セキュリティの強化

Zscaler Private Accessは、アプリケーションの場所に関係なく、ユーザーをアプリケーションに接続するためのきめ細かいポリシー フレームワークを提供します。ZPAは、ユーザーをネットワークに接続することなく、ネットワーク全体をユーザーから抽象化します。このアプリケーション接続には、次のようなメリットがあります。

- 要求時に確立される暗号化されたTLSトンネル経由で、複数の環境(AWS、オンプレミス、ハイブリッド)のアプリケーションにアクセスできる。
- ユーザーはネットワークに接続することなく、内部アプリケーションにアクセスできる。
- IPアドレス指定はデータセンター内で重複する可能性があるが、ネットワークがユーザーから抽象化されるため、重複が問題にならない。
- アプリケーション アクセス ポリシーはZscalerクラウドで評価され、ユーザーとデバイスのアクセスが認証されている場合のみ、アプリ環境で動作するApp Connector経由でアウトバウンド接続が確立される。デバイスまたはアプリ環境へのインバウンド接続は発生しない。
- アプリケーションごと、ユーザーまたは属性ごとのきめ細かなポリシーは、組織またはMSPが作成、管理できる。

ZPAは、ネットワーク全体ではなく、各ユーザーが業務に必要なアプリケーションのみにアクセスを許可することで、従来のVPNアプローチよりも強力なセキュリティを提供します。このアプローチによって、一般的な不正侵入やマルウェアからの保護を可能にするセキュリティ態勢が実現します。また、AWSを利用する組織向けに、完成形のゼロトラストアプローチの導入をサポートします。

AWSへの移行フレームワークに関連して、ZPAはアプリケーション固有のユーザー アクセスを可能にし、AWSに展開されたすべてのワークロードに一貫したアプローチを提供します。業務に必要な特定のアプリケーションのみにアクセスを制限することで、会社のセキュリティ態勢が強化されます。ユーザーの業務上の役割に加えて、デバイス管理の状態もアプリケーション リクエストのコンテキストとして利用されます。ZPAは、どのユーザーがどのデバイスからどのアプリケーションにアクセスできるかをきめ細かく制御する仕組みと手法を提供することで、AWSのお客様がAWSの責任共有モデルにおける自らの役割を果たすことをサポートします。

Zscaler Private AccessによるAWSへの迅速な移行

準備と計画

Zscaler Private Accessを使用することで、AWSの迅速な導入が可能になり、プロジェクトの目標達成に必要な多くのフェーズを回避できます。とくに、移行において最も重要であるにもかかわらず、往々にして見落とされるユーザーに関する基準値を確立します。

ZPAによって、以下が可能になります。

- ユーザーとそのユーザーが利用しようとするアプリケーションの間に抽象化レイヤーを提供することで、「アイデンティティー」を新しい境界として活用する。
- 企業ネットワーク境界の内外を問わず、ユーザーを本質的に信頼しないセキュリティ態勢を前提とする。ユーザーはIAM (アイデンティティーとアクセスの管理)ソリューションを介して認証され、複数のポリシー制御に従ってアプリケーションへのアクセスが許可されるため、IAMソリューションから返されるSAML属性に基づいた制御が可能になります。
- 多要素認証(MFA)を使用したリスクベースのアプローチを実装する。
- 特権アクセスの必要性を軽減し、インバウンド アクセスの攻撃対象領域を最小限にする。これは、内部アプリケーションに対するユーザー要求を傍受し、ユーザーをアプリに接続する前にポリシーを適用することで可能になります。結果として、インターネットだけでなく、未承認の内部ユーザーに対してもアプリケーションが不可視化されます。
- ユーザーが企業ネットワークまたは公衆ネットワークのどちらにいても、ユーザーのワークフローに影響を与えることなく統合するため、ストレスのないエクスペリエンスを提供する。Zscaler Client Connector (旧Zscaler App)がインストールされている場合、ユーザーの場所や使用するデバイスに関係なく、アプリケーションに接続するための操作は一切発生しません。

ここでは、AWSのクラウド移行プラクティスの推奨事項に記載され、多くの組織やコンサルティング業務でも採用される、以下の手順とそのメリットについて概説します。

- **準備と計画**
- **ポートフォリオと検出**
- **運用計画と配信**
- **移行と検証**
- **継続的な事業運営と将来を見据えた投資**

ポートフォリオと検出

現在、多くの組織がクラウドファーストのビジネスに移行を進めています。Zscalerでは、クラウド移行戦略を推進するにあたり、次のような課題の回避が必須であると認識しています。

- アプリケーションをプライベート データセンターからパブリック クラウドに移行する際に発生するユーザー エクスペリエンスの低下。これには、ユーザーに対するアプリケーションの利用方法の継続的な教育とアプリケーションのパフォーマンスに関連する複雑性という2つの理由があります。
- プライベート データセンターをパブリック クラウドに接続することで発生するネットワークの複雑性。
- グローバル ビジネスに必要な処理能力を測定、管理、予測するためのコストと複雑性。
- 信頼されたユーザーと信頼されていないユーザーをネットワークに接続することで発生する、重大なセキュリティ脅威と不確実性。

Zscaler Private Accessは、以下の3つの主要なセキュリティ設計フェーズを通じて内部アプリケーションを可視化することで、これらの課題の解決を支援します。

- 検出：ユーザー アクセスを活用したアプリケーション検出機能が、組織内でどの内部アプリケーションが使用され、その後どのアプリケーションがAWSから使用されているかを示します。
- チューニング：アプリケーションが検出されると、ポリシーのチューニングを行い、移行前にベースラインを確立します。これにより、AWSに移行した際の露出が回避され、移行完了までの時間も短縮されます。
- 運用：アプリケーションのセグメント化により、完全な運用に必要なセキュリティと配信の態勢に合わせてポリシーを迅速かつきめ細かく適用します。

導入事例：

グローバル大手飲料メーカーは500以上のアプリケーションをオンプレミスで運用していましたが、ZscalerはMFAやその他の属性を含むチューニングを手掛け、わずか95分でIT部門を立ち上げました。運用環境は、当初の展開からほとんど変更されていません。

Zscaler Private Accessは、ユーザーのワークフローにスムーズに統合されるため、検出フェーズを加速できます。ユーザーは、使用したいアプリにそのままアクセスでき、エンドポイント クライアントなどのセキュリティ ソフトウェアと最初にやり取りする必要はありません。ユーザーは、新規または従来型のどちらのアプリケーションであっても、アクセス方法を理解する必要がなくなり、管理者は、アプリケーション フローをエンドツーエンドで完全に可視化できます。

運用計画と配信

AWSに移行するアプリケーションを特定したら、ユーザーにアプリケーションを配信する方法を決定します。基本的には、次の3つの方法から選択します。

仮想化 - 非公開

- アプリケーションの現在のアーキテクチャーを理解する。3階層の環境(Webサーバー、アプリ サーバー、データベース サーバー)でそれぞれのコンポーネントが仮想化され、順番にAWSに移行されます。
- フロントエンドを最初に移行する。アプリ サーバー、データベース サーバーについては、VPNまたはDirect Connectなどの専用接続経由でそのまま使用できます。
- アプリケーションは「非公開」のままであり、VPNまたは専用接続経由でのみアクセスできる。

Zscalerを採用したことで、当社の敏捷性が高まりました。各部署からも在宅勤務を続けられることに対して感謝の声が届いています。Zscalerは基本的に従来のVPNシステムを淘汰しています。

Henry M. Jackson財団、CTO、Marc De Serio氏

仮想化 - 公開

- フロントエンドのWebサーバーがインターネットから直接利用できるようになる(最初の方法に類似)。
- アプリケーションが外部に公開される。
- アプリケーションに対するインバウンド/アウトバウンドのコンテンツを制御するWAF (Webアプリケーション ファイアウォール)、DDoS対策、ユーザー アクセスを制限するIAM (アイデンティティーとアクセスの管理)の実装が必要になる。

クラウドに合わせた再設計

- 現在の形式では移行できない、または移行しないアプリケーション。
- フロントエンドをCloudFrontを使用してEC2またはサーバーレスに移動する(Webサーバーの再利用と再コーディング)。
- 中間層をEC2またはサーバーレスに移動する(ミドルウェアの再利用)。
- バックエンドをRDS/Auroraなどに移動する(スキーマ、DBなどの更新)。
- IAMでアクセスを制御する。WAFでコンテンツを制御する。
- 新しいアーキテクチャーへの移行に合わせて、ユーザー エクスペリエンスとアクセスを変更する。

アプリケーションの公開には、数値化できるセキュリティ リスクがあります。アプリケーションによっては、再構築あるいは仮想化のどちらであっても、このリスクはビジネス上許容できる場合があります。ZPAであれば、アプリケーションを外部に公開しつつ、ブラウザーベースのアクセスを利用して同じセキュリティ アーキテクチャーを提供できます。この方法では同じSAML認証をZPAで使用し、同じZPAアーキテクチャーをインバウンドなしのアクセスに使用すると同時に、同じポリシー フレームワークと可視性が提供されます。

しかし、SAPなどの多くのアプリケーションの場合、アプリケーションをインターネットに直接公開することはリスクが高いため、AWSへの移行の一環として、セキュリティを強化する必要があります。ZPAを使用することで、セキュリティを強化し、アプリケーションが外部に公開されないように計画することができます。

移行と検証

移行の進行状況を把握することは非常に重要です。Zscaler Private Accessを利用することで、アプリケーションが使用されている場所とそれに関連するセキュリティ ポリシーを可視化できます。

Zscaler Private Accessは、ユーザーとアプリの間の抽象化レイヤーとして機能します。アプリの場所がデータセンターからパブリック クラウドやVPCへと変更されても、ユーザー エクスペリエンスが低下することはありません。ユーザーがアプリケーションに直接接続することはなく、すべてのトラフィックがZPAのクラウド サービスを経由します。さらに、ユーザーがネットワークに接続されることはないため、セキュリティ態勢が強化されます。すべてのZPA通信が、データセンターまたはパブリック クラウドからZPAのクラウド サービスへのアウトバウンド接続であるため、データセンターのファイアウォールまたはACLは、すべてのインバウンド接続を拒否するように構成でき、データセンターやVPCが外部に公開されることはありません。

Zscaler Private Accessを組織のSOC (セキュリティ オペレーション センター)と統合することで、SIEMフィードやレポート/分析を実行できます。ZPA管理コンソールでアプリケーションやユーザーのグラフィカル表示を確認でき、ポリシーを変更することでアプリケーションへのユーザー アクセスを制御できます。

Zscalerは移行サービスを提供していませんが、移行を検証し、提供されるユーザー エクスペリエンスがビジネス要件に沿っていることを確認するプロセスを強化します。ZPAによってアプリケーションの移行状況が可視化されるため、組織やコンサルタントは常に最新の状態を確認できます。

導入事例：

英国政府にとって、ZPAはAWSにアプリケーションとアクセスを提供する不可欠なツールとなっています。ゼロトラスト モデルを採用したことで、すべてのアプリがZPA経由でのみ使用されています。

継続的な事業運営と将来を見据えた投資

Zscaler Private Accessは、AWSならびに組織の管理者がアプリ単位やユーザー単位のカスタム ポリシーをグローバルに作成できるため、ネットワークベースのセグメンテーションに起因する複雑さが軽減されます。

- シンプルなポリシーにより、アイデンティティーとアプリケーションに基づいてアクセスをセグメント化する。
- 管理が困難なIPアドレスベースのポリシーの作成や実装が不要になるため、アプリケーションの利用者に影響を与えることなく、社内でのアジャイルな運用が可能になる。DevSecOpsを活用し、アプリケーションをプライベート クラウドからパブリック クラウドに移行しつつ、パブリック クラウドをプライベートに保つ。
- サードパーティーや請負業者がアクセスできるアプリケーションに対して、優れた可視性と制御を提供する。
- Zscalerは、Zscalerクラウドと先進の機能に継続的に投資する。多くのグローバル組織のトラフィックを学習し、新たな要件に対応しながら投資を続けることで、それぞれの組織が他では得られない優れた可視性を提供します。ZPAへの投資によって、継続的な付加価値が追加されます。

従来のリモート アクセスVPNインフラストラクチャーでは、ユーザーが常にネットワーク上に存在するため、攻撃対象領域が拡大してすべての移行戦略にリスクをもたらします。Zscaler Private Accessは、以下の4つの主要なセキュリティ原則を実装することで、このリスクを解消します。

- ユーザーを内部ネットワークに入れることなく、VPCまたは物理データセンターのプライベート アプリケーションに接続する。
- 許可されていないユーザーにはアプリケーションを公開しない。
- 複雑でコストのかかるネットワーク セグメンテーションに依存することなく、VPCやセキュリティ グループ、およびその他のサービス機能に密接に連携させることで、アプリケーションをセグメント化する。
- 攻撃対象領域を拡大してユーザー エクスペリエンスを複雑にしかねないVPNから脱却し、インターネットを安全なネットワーク トランスポートとして使用する。

このアプローチであれば、水平移動が許可されていないアプリケーションにアクセスすることはありません。さらに、アクセスが許可されていないアプリケーションをユーザーが目にすることはなく、ローカルまたはホストされている環境のインターネットのどちらであっても、ポート スキャンやその他の方法で検出することはできません。アプリケーションがユーザーからインバウンド接続を受け取ることはありません。

導入事例：

MAN Energy Solutionsは、提携するデベロッパーに対して必要なDevOps環境とアプリにのみアクセスを許可しています。提携パートナーへのアクセス許可は攻撃対象領域を生み出す危険性がありましたが、アイデンティティーベースのアクセス制御によってそのリスクを回避しています。

まとめ

ZPAは、クラウドへの移行前、移行中、移行後のすべての段階において、承認されたユーザーによるワークロードへのアクセスや操作を常に管理し、エンドユーザー エクスペリエンス全体を向上させるうえで重要な役割を果たします。

変革の主なメリットは以下のとおりです。

- 変革と移行のプロジェクトにかかるスケジュールの短縮
- 移行したアプリのセキュリティ態勢の強化
- アプリの移行中と移行後のユーザー エクスペリエンスの向上

ZPA導入のユース ケースには以下が含まれます。

- クラウドの採用やアプリの移行
- 合併と買収
- サードパーティー アクセス

Zscaler Private Accessは、限定的または全面的な導入のどちらにも対応しています。ZPAはAWS上に構築されており、ZPA Public Service EdgeはAWSおよび世界中の他の場所に展開されています。Zscaler App ConnectorsはVPC内にあり、Zscaler Client Connectorは、主要なPCおよびモバイル デバイスのOSをサポートする軽量アプリです。無料トライアル版、正規のPOC、またはPOCに代わる段階的な本番環境での展開については、Zscalerまでお問い合わせください。ZPAは、プライベート オファーをサポートするSaaS製品として、AWS Marketplaceで利用できます。

参考資料

以下の資料も併せて参照してください。

Zscalerのホーム ページ：www.zscaler.jp

ZPAのホーム ページ：www.zscaler.jp/products/zscaler-private-access

AWS向けZPAのホーム ページ：www.zscaler.jp/products/zpa-for-aws

サポートおよび技術関連資料：help.zscaler.com/zia?filter=documentation

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

AWSクラウド導入フレームワーク：aws.amazon.com/professional-services/CAF/

AWS責任共有モデル：aws.amazon.com/compliance/shared-responsibility-model/

zscaler™ | Experience your world, secured.™

Zscalerについて
Zscaler (NASDAQ: ZS)は、より効率的で、俊敏性や回復性に優れたセキュアなデジタル トランスフォーメーションを加速しています。Zscaler Zero Trust Exchangeは、ユーザー、デバイス、アプリケーションをどこからでも安全に接続させることで、数多くのお客様をサイバー攻撃や情報漏洩から保護しています。世界150拠点以上のデータ センターに分散されたSASEベースのZero Trust Exchangeは、世界最大のインライン型クラウド セキュリティ プラットフォームです。詳細は、**zscaler.jp**をご覧いただくか、Twitterで**@zscaler**をフォローしてください。

+1 408.533.0288 Zscaler, Inc. (HQ) • 120 Holger Way • San Jose, CA 95134 zscaler.jp