ゼットスケーラーで
シンプルかつ安全にAWSへの移行を実現

Zscaler Private Accessによる
AWS Cloud Adoption Frameworkへのマッピング

目次

はじめに

本書は、ネットワークやセキュリティの目標の達成にあたって直面する問題をゼットスケーラーで解消することで、迅速な採用が可能にする方法を紹介します。

Zscaler Private Access（ZPA）をAWS移行のユースケースに活用することで、ソリューション全体に構造化アプローチを提供し、ZPAによってアプリケーションの迅速な移行を実現する方法を解説します。

ゼットスケーラー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アーキテクチャは、ユーザやアプリケーションの俊敏性の向上とアプリケーションの迅速な移行の実現に不可欠な要素となります。

ZPAの中核となるのは、承認されたユーザによる、クラウドへの移行前、移行時、移行後のワークロードへのアクセスややり取りを常に管理しつつ、全体的なエンドユーザエクスペリエンスを向上させる機能です。

Zscaler Private Accessアーキテクチャのベストプラクティスは、お客様の次のようなクラウド移行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
- 運用計画とデリバリ
- 移行と検証
- 継続的な運用

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SDP（Software-Defined Perimeter）ソリューションは、AWSの導入だけに対応するものではありません。ZPAは、ハイブリッドIT環境をサポートし、コンサルティングプラクティスによって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あるいはパブリッククラウドのどちらでホスティングされる場合であっても、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。

ゼットスケーラーによって解決できるアーキテクチャの課題としては、ネットワークやセキュリティの従来型アプローチの高いコストと複雑さ、従来型のVPNベースのネットワークアクセスのユーザエクスペリエンスの低さなどが挙げられます。ほとんどのお客様は、オンプレミスでデータセンタ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。

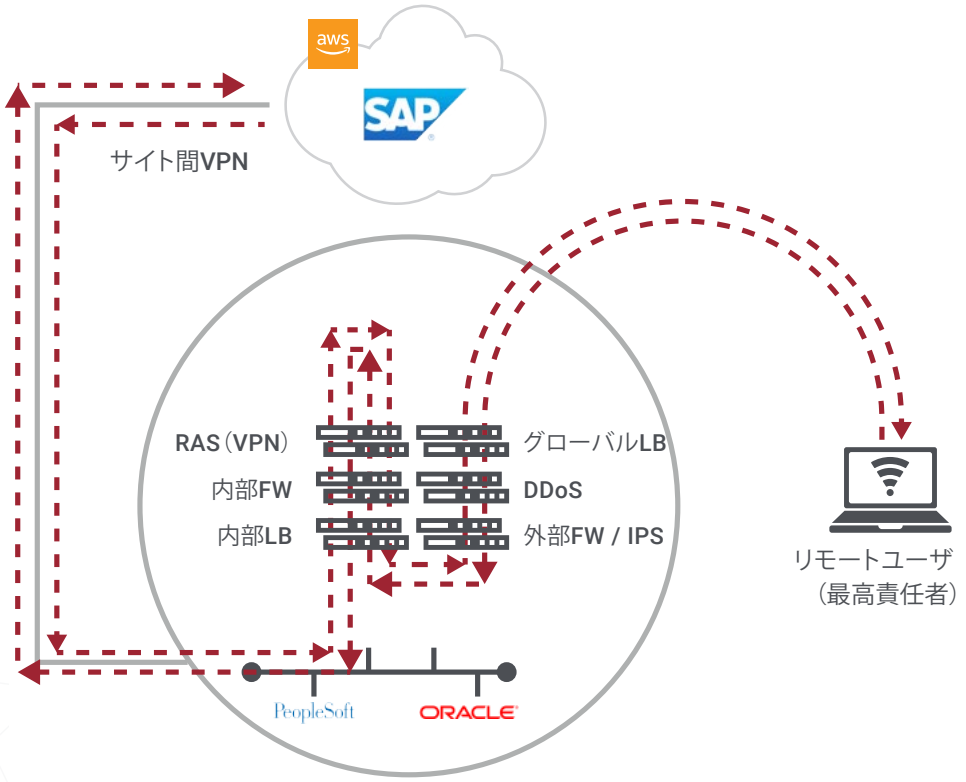

図1.従来のデータセンタ中心のリモートアクセスアプローチ

Zscaler Private Accessは、2007年のDISA（アメリカ国防情報システム局）による草案に基づくユーザエクスペリエンスを重視するセキュリティ手法であるSDP（Software-Defined Perimeter）のソリューションを提供します。ZPAは従来のリモートアクセス VPNソリューションとはまったく異なるセキュリティ手法で、クラウドへの移行を進めている今日のアジャイルビジネスコミュニティのニーズに対応できるように設計されています。

Zscaler Private Accessは、ゼロトラストモデルの実装により、ゼットスケーラーのクライアントソフトウェアを使用し、ゼットスケーラーのグローバルクラウドアーキテクチャを活用する、プライベートアプリケーションへのアクセスを提供します。いかなるトラストも前提とせずに、ユーザとデバイスに基づくSAML認証を採用することで、複数の属性をポリシーに対して返すことができ、認証されると、AWSのアプリケーションのフロントエンドとして動作するZPA Connectorからゼットスケーラーのクラウドへの内部から外部への接続が確立され、アプリケーションがユーザ接続に連結されます。これにより、許可されたユーザと特定のアプリケーションの間にセキュアセグメントが作成されます。

ZPAによって、ネットワークが単なるトランスポートとなり、アプリケーションアクセスがグローバルセキュリティクラウド経由でフェデレーションされます。ポリシーベースのきめ細かいアクセスを使用して、認証されたユーザのみが許可されたアプリケーションにアクセスできるようになるため、パブリッククラウドをプライベートの状態にできます。

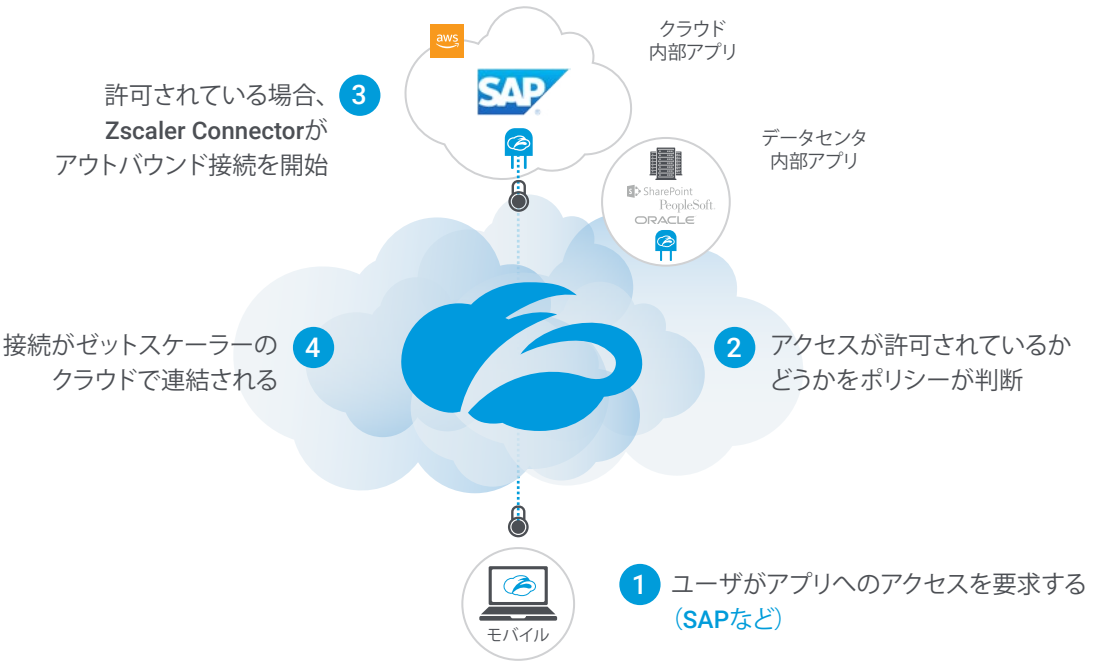

図2. オフネットワークのユーザのポリシーベースの安全なアクセス

ユーザやデバイスのセキュリティポスチャはアプリケーションアクセスが許可される前に評価されるため、アクセスの権限がないユーザにアプリケーションが表示されることはありません。さらには、アプリケーションがゼットスケーラークラウド経由でフェデレーションされるため、AWSインスタンスやお客様のデータセンタへのインバウンド接続は存在せず、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、ネットワークオブジェクトではなく、ユーザ /デバイス情報に基づく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のどちらであっても、許可されたアプリケーションにユーザが同時にアクセスできるようになります。ユーザをネットワークに繋げることなく、アプリケーションへの最短パス接続を提供することで、ユーザ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が簡素化され、セキュリティに対する可視性とコントロールが強化されます。

アプリケーションの迅速な移行

Zscaler Private Accessは、移行を進める際の試験的なビジネスケースをサポートする目的で活用することもできます。既存のアプリケーションインフラストラクチャの定量化にあたっては、さまざまな課題に直面しますが、ゼットスケーラーはこのアプローチを通して、従来型とAWSの両方の環境でシームレスなユーザエクスペリエンスを実現するフレームワークを提供します。ポリシーベースのアクセスコントロールは、従来のインフラストラクチャとそれに関連する構成や継続的な管理に代わるものです。

移行の全体的なスケジュールを短縮できるのは、アーキテクチャやコンサルティングプラクティスの責任者にとってのメリットです。ZPAは、従来型のネットワークインフラストラクチャ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アクセスのコントロールを可能にするプラットフォームを提供します。AWSでホスティングされるプライベートアプリケーションへのユーザの接続にあたり、従来のVPNハードウェアが不要となり、AWS Direct Connectでリモートユーザが最適とは言えないトラフィックパスでデータセンタを経由し、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ティングされるアプリケーションへのユーザアクセスをきめ細かくコントロールできます。このアプローチによって、クラウドの導入が簡素化され、安心して移行を進められるようになります。

ZPAは、ユーザエクスペリエンスを向上させ、変更管理プロセスの大幅に削減し、エンドツーエンドのアプリケーションの可視性を提供し、さらには、一元的なポリシー管理の使用によって移行するグループや場所の選択を可能にすることで、迅速な移行を支援し、最高のユーザエクスペリエンスを提供します。

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に移行する場合に、ネットワーキングやセキュリティのアプローチが移行計画 /実行サイクルの遅い時期に先延ばしされることがよくあります。結果として多くの困難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定期的に報告されています。プロジェクトの開始時に計画のツールボックスに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、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、ネットワーキング、セキュリティの分野の関係者が一丸となって移行に取り組むベースを形成できますが、一般的に準備および計画の段階に組み込まれていることは稀と言えます。

これらのアプリケーションにとって、IaaSへの移行は有力な選択肢であり、導入の規模と範囲を考えれば、多くの場合にそのメリットは明白です。しかし、最初に直面する一般的な課題として、ユーザがアクセスするすべてのアプリケーションに加えて、移行の候補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エグゼクティブ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を提供し、お客様の物理データセンタ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とお客様が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関するセキュリティコントロールを強化することができます。

お客様はAWSに移行するワークロードを簡単に特定できますが、加えて、アプリケーションを安全にユーザに提供する方法を決定する必要があります。これは、アプリケーションがクラウドベースの配信を前提に設計されていない場合に大きな課題となります。

IAM（アイデンティティとアクセス管理）は、IaaSでの提供にあたって極めて重要な要素となりますが、事前に承認されたユーザ /デバイス以外にアプリケーションが表示されないようにすることで、このアクセスコントロールをさらに強化でき、DDoS攻撃、サードパーティのソースからの不正アクセス、マルウェアの内部ネットワークでの水平移動などの最新のセキュリティ脅威への対策に役立ちます。

セキュリティの強化

Zscaler Private Accessは、きめ細かいポリシーフレームワークを提供することで、アプリケーションが存在する場所に関係なく、ユーザによるアプリケーションへの接続を可能にします。ZPAは、ユーザ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、次のような複数のメリットがあります。

- ユーザは、オンデマンドで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ます。
- ユーザをオンネットワークにすることなく、内部アプリケーションへのアクセスを可能にします。
- IPアドレス指定がデータセンタ内で重複する場合がありますが、ネットワークがユーザから抽象化されるため、重複が問題になることはありません。
- アプリケーションアクセスポリシーがゼットスケーラーのクラウドで評価されます。ユーザ + デバイスのアクセスが認証されると、アプリケーション環境で動作するコネクタ経由でアウトバウンドのアプリケーション接続が確立されます。アプリ環境がインターネットに公開されることはなく、デバイスやアプリ環境へのインバウンド接続は発生しません。
- アプリケーション単位、ユーザ /属性単位のきめ細かいポリシーを、お客様または MSPが記述し、メンテナンスできます。

ZPAは、ネットワーク全体ではなく、それぞれの役割に必要なアプリケーションへのアクセスのみをユーザに許可することで、従来型のVPNアプローチより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、最も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ポスチャが実現します。また、ゼットスケーラーは、完成形のゼロトラストアプローチを採用するAWSのお客様をサポートし、迅速な導入を可能にします。

ZPAは、AWS移行フレームワークに関連する機能として、アプリケーション固有のユーザアクセスを可能にする、AWSに導入されるすべてのワークロードに対する一貫性あるアプローチを提供します。ユーザの役割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、セキュリティポスチャが強化されます。さらには、ユーザの役割に加えて、デバイス管理ステータスをアプリケーション要求のコンテキストとして使用することもできます。ZPAが提供する、アプリケーションへのアクセスを許可するユーザやデバイスのきめ細かいコントロールを可能にする方法を利用することで、お客様は、AWS責任共有モデルにおいて自らの責任を確実に果たすことができます。

Zscaler Private AccessによるAWSへの迅速な移行

このセクションでは、AWSクラウド移行プラクティスの推奨事項に記載され、多くのお客様やコンサルティングプラクティスでも採用される、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
- 運用計画とデリバリ
- 移行と検証
- 継続的な運用 — 将来への投資

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、従来であれば目標達成のために必要であった多くのプロジェクトフェーズを回避できます。具体的には、移行において最も必要で重要であるにもかかわらず、見過ごされることの多い、ユーザのベースラインを確立します。

ZPAによって、以下が可能になります。

- ユーザとユーザ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を提供することで、「アイデンティティ」を新しい境界として活用します。
- 企業ネットワーク境界の内側または外側のどちらにいるかに基づいてユーザを信頼するのではなく、IAM（アイデンティティとアクセスの管理）ソリューションを使用してユーザを認証し、複数のポリシーコントロールに従ってアプリケーションへのアクセスを許可し、IAMソリューションから返されるSAML属性に基づくコントロールを可能にします。
- 多要素認証（MFA）を使用することで、リスクベースのアプローチを可能にします。
- 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します。内部アプリケーションに対するユーザ要求を傍受し、ユーザをアプリに接続する前にポリシーを適用することでこれを実現し、結果として、インターネットと未許可の内部ユーザの両方にアプリケーションが公開されないようにします。
- ユーザが会社またはパブリックのどちらでオンネットワークであるかにかかわらず、ユーザの通常のワークフローに透過的に統合することで、円滑なユーザエクスペリエンスを実現します。Zscaler Appがインストールされていれば、アプリケーションの場所や使用するデバイスに関係なく、いかなるアクションも必要とすることなく、ユーザがアプリケーションに接続できます。

ポートフォリオと検出

現在、多くのお客様がクラウドファーストのビジネスへの移行を進めています。ゼットスケーラーでは、クラウド移行イニシアチブへの移行にあたり、お客様が次のような課題を回避したいと考えていることを十分に理解しています。

- アプリケーションをプライベートデータセンタからパブリッククラウドへの移行に伴う、ユーザエクスペリエンスの低下
  これには、ユーザ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さという2つの理由があります
- プライベートデータセンタをパブリッククラウドに接続することにで発生する、ネットワークの複雑さ
- グローバルビジネスに必要な処理能力のサイジング、管理、予測のコストと複雑さ
- 信頼されたユーザと信頼されていないユーザをオンネットワークに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**：ユーザアクセスドリブンのアプリケーション検出によって、組織内で利用される内部アプリケーションとAWSから利用されるアプリケーションを明らかにします。
- **チューニング**：アプリケーションが検出されたら、移行に先立ってポリシーをチューニングしてベースラインを確立できます。これにより、AWSへの移動後の情報漏洩のリスクを回避し、最終デリバリまでの時間を短縮できます。
- **本番運用**：アプリケーションセグメンテーションにより、完全本番環境に必要なセキュリティとデリバリポスチャに合わせたポリシーの迅速かつきめ細かい適用が可能になります。

Zscaler Private Accessは、ユーザのワークフローへの透過的な統合によって、検出フェーズを加速させます。ユーザは、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。

成功事例：世界的な飲料メーカーのIT部門では、95分で500以上のオンプレミスのアプリケーションが検出されました。MFAやその他の属性をチューニングし、初期導入後はほとんど変更することなく本番環境を運用しています。

運用計画とデリバリ

AWSに移行するアプリケーションが特定されたら、ユーザへのアプリケーションのデリバリ方法を決定します。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を理解します。3階層の環境（Webサーバ、アプリケーションサーバ、データベースサーバ）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。
- フロントエンドが最初に移行されますが、アプリケーションサーバ / データベースサーバについては、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ます。

仮想化 - 公開

- 最初の方法に似ていますが、フロントエンド Webサーバをインターネットから直接利用できます。
- アプリケーションが外部に公開されます。
- WAF（Webアプリケーションファイアウォール）を実装することで、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とDDoS保護をコントロールし、IAM（アイデンティティとアクセスの管理）を実装してユーザアクセスを制限する必要があります。

クラウドに合わせた再設計

- 現在の形式で移行できない、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でEC2またはサーバレスに移動 - Webサーバを転用し、再コーディング
- 中間層をEC2またはサーバレスに移動 - ミドルウェアを転用
- バックエンドをRDS/Auroraなどに移動 - スキーマ、DBなどを更新
- IAMでアクセスをコントロール、WAFでコンテンツをコントロール
- 新しいアーキテクチャへの移行に合わせて、ユーザエクスペリエンスとアクセスを変更

アプリケーションの公開にはセキュリティリスクがあり、それを数値化できます。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、このリスクがビジネスに受け入れられるものである場合があります。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を提供でき、この方法によって、同じSAML認証をZPAで使用し、インバウンドなしのアクセスに同じZPAアーキテクチャを使用し、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は、アプリケーションをインターネットにそのまま公開するリスクは大きすぎるため、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であれば、移行の計画が可能になり、その移行の一環として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できます。

移行と検証

移行の一環として、どこまで移行が進行しているのかを把握することが重要です。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、ユーザとアプリの間の抽象化レイヤの役割を果たします。アプリの場所がデータセンタからパブリッククラウドやVPCへと変更されても、ユーザエクスペリエンスが低下することはありません。ユーザがアプリケーションにダイレクト接続することはなく、すべてのトラフィックがZPAクラウドサービスを通過します。さらには、ユーザがオンネットワークになることがないため、セキュリティポスチャが強化されます。すべてのZPA通信が、データセンタまたはパブリッククラウドからZPAクラウドサービスへのアウトバウンド接続であるため、データセンタのファイアウォールやACLを構成することで、すべてのインバウンド接続を拒否するようにでき、データセンタ / VPCが外部に公開されることはありません。

Zscaler Private Accessをお客様のSOC（セキュリティオペレーションセンタ）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アクセスをコントロールできます。

ゼットスケーラーは、移行サービスを提供していませんが、移行を検証するプロセスを強化することで、提供されるユーザエクスペリエンスがビジネス要件を満足することを確認します。ZPAによってアプリケーション移行の進行状況が可視化されるため、お客様やコンサルタントが常に最新の状態を確認できます。

成功事例：英国政府。ZPAは、アプリケーションとAWSへのアクセスの提供に使用される必須ツールとなりました。このお客様は、ゼロトラストモデルを採用しており、すべてのアプリをZPA経由で使用します。

継続的な運用 — 将来への投資

Zscaler Private Accessであれば、AWSやお客様の管理者が、アプリ単位、ユーザ単位のカスタムポリシーをグローバルスケールで作成できるため、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、アイデンティティとアプリケーションに基づいてアクセスをセグメンテーションします。
- 管理が困難なIPアドレスベースのポリシー作成や実装が不要になります。アプリケーションの利用者へ影響を及ぼすことなく社内でのアジャイル運用が可能になります。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が外部に公開されないようにできます。
- サードパーティや取引先にアクセスを許可しているアプリケーションに関する優れた可視性とコントロールをお客様に提供します。
- ゼットスケーラーは、ゼットスケーラーのクラウドと先進の機能に継続的に投資しています。グローバルな多くの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、それぞれの組織に固有の他では得られない優れた可視性を提供します。ZPAの投資によって、将来継続する付加価値が追加されます。

従来型のリモートアクセス VPNインフラストラクチャでは、ユーザを常にオンネットワークの状態にさせるために、攻撃対象領域が拡大し、移行戦略においてもリスクとなります。

Zscaler Private Accessは、以下の4つの主要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。

- ユーザをオンネットワークにすることなく、(VPCまたは物理 DC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に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を利用することなく、VPC、セキュリティグループ、その他のサービス機能に密接に連携させることで、アプリケーションセグメンテーションを実現する
- 攻撃対象領域を拡大し、ユーザエクスペリエンスを複雑にするVPNを利用することなく、インターネットをセキュア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、水平移動によって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が目にすることはなく、ローカルまたはホスティングされた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からダイレクトインバウンド接続を受け取ることはありません。

成功事例：MAN Energy Solutions - パートナーの開発者が、それぞれが必要とするDevOps環境とアプリだけにアクセスできるようになりました。以前の環境では、パートナーアクセスが潜在的な攻撃対象領域となっていましたが、アイデンティティベースのアクセスコントロールによって、これらのユーザとデバイスがオフネットワークになったことで、この問題が解消されました。

まとめ

Zscaler Private Accessの中核となるのは、クラウドへの移行前、移行時、移行後のワークロードへの承認されたユーザによるワークロードへのアクセスややり取りを常に管理しつつ、全体的なエンドユーザエクスペリエンスを向上させる機能です。

トランスフォーメーションの主なメリット

- トランスフォーメーションと移行プロジェクトのタイムラインの短縮
- 移行されたアプリのセキュリティポスチャの強化
- アプリケーションの移行中と移行後のユーザエクスペリエンスの向上

ZPAの主なユースケース

- クラウドの採用やアプリケーションの移行
- 合併・買収
- サードパーティアクセス

Zscaler Private Accessには、Limited（一部）またはAll-in（すべて）のモダリティの導入方法があります。ZPAはAWSベースで構築されています。Zscaler Enforcement Nodeは、AWSだけでなく、世界中の他の場所に置くこともでき、Zscaler ConnectorはVPCに置かれます。Zscaler Appは、すべての主要およびモバイルデバイスのオペレーティングシステムをサポートする軽量アプリです。無料の試用版と正規のPOCに加えて、POCを本番環境のロールアウトに合わせて追加する方法もあります。ZPAはAWS MarketplaceでSaaS契約リストとして提供されており、プライベートオファーをサポートしています。

参考資料

以下の資料も併せて参照ください。

Zscalerウェブサイト：ZPA概要

Zscalerウェブサイト：ZPA for AWS概要

サポート /技術関連資料

MAN Energy Solutions様 活用事例

AWS Cloud Adoption Framework

AWS責任共有モデル

ゼットスケーラーについて

ゼットスケーラーは2008年に、「アプリケーションのクラウド移行に伴って、セキュリティもクラウドに移行する必要がある」という、シンプルで力強い概念に基づき設立されました。ゼットスケーラーは現在、世界中の数千の組織のクラウド対応の運用への移行を支援しています。

ゼットスケーラー株式会社
東京都千代田区大手町1-9-2
大手町フィナンシャルシティ
グランキューブ3階
www.zscaler.jp