ゼロトラスト ゲートウェイ

ホワイトペーパー

目次

概要

Zscaler Zero Trust Gateway (ZTGW)サービスを使うと、AWS内のワークロード トラフィックを最小限の手間で保護することが可能です。ZscalerがAWS上のセキュリティ インフラの構築、運用、メンテナンスをすべて管理するため、クラウド環境のセキュリティを迅速に実現できます。このフルマネージド サービスにより、お客様自身でコネクター用仮想マシン(VM)を展開または管理する必要がなくなり、ネイティブのクラウド テクノロジーを通じて、包括的で高可用、かつスケーラブルなソリューションが提供されます。お客様は、拡張性やインフラ管理を気にすることなく、本来のビジネスに専念することができます。

ユース ケース

ZTGWサービスは、ZscalerのZero Trust Cloud製品に不可欠なコンポーネントです。このソリューション スイートは、パブリック クラウド環境内のワークロードやサーバーにかかわるネットワーク セキュリティのイノベーションや技術を推進し、特化型ソリューションを提供しています。

具体的な機能については、以下のユース ケースをご参照ください。

- **インターネットへの出力通信の保護:** ZTGWは、Webプロキシや出口用ファイアウォールに代わり、AWS VPCからの出力トラフィックを保護します。すべての出力トラフィックをZero Trust Exchangeに接続し、VPC内のあらゆるAWSサービスやワークロードに対して、包括的な可視化、制御、検査、脅威保護、データ保護を提供します。
- **入力トラフィックの保護:** ZTGWは、外部公開されているアプリケーションへの入力トラフィックを保護します。レイヤー4ベースのステートフル ルールにより、悪意のある攻撃からアプリケーションを守ります。
- **プライベート アプリケーションの接続:** リージョン間や、他社クラウド(Azure、GCP、OCIなど)、オンプレミスのデータ センターに対し、ネットワーク アクセス権を与えることなく、プライベート アプリケーションへの接続を提供します。これによりZscaler Private Access (ZPA)の機能をパブリック クラウド上のワークロードに拡張します。
- **安全なEast-Westセグメンテーション:** ZTGWにより、VPCとDirectConnect間で、東西間のマクロセグメンテーションが容易になり、レイヤー4ルールのローカル施行が可能になります。この機能により、トラフィック制御のための従来型ファイアウォールが不要になり、コスト削減が期待できます。
- **安全なインバウンド制御:** ZTGWを使用すると、組織はレイヤー4ルールを利用して、AWS Direct Connect経由のオンプレミス データセンターとAWS間のトラフィック制御を行うことができ、同時にインターネットからアプリケーションにアクセスする際のインバウンド接続用のレイヤー4ファイアウォールの必要性を低減します。
- **安全なプライベート接続:** ZTGWは、AWS DirectConnectとAzure Express Routeを利用して、データ センターとマルチクラウド環境の間に、制御された安全なネットワーク トラフィックを提供します。
- **ポリシーベースの転送:** 送信元/宛先IP、ドメイン、ユーザー定義のタグなどの基準を使用して、クラウドの出力トラフィックをより適切に制御します。
- **静的なIPアドレス:** Zscalerからの出力トラフィックに、お客様のZscalerテナント専用に割り当てられた静的IPアドレスを利用できます。

メリット

ZTGWは、全体的なエクスペリエンスを向上させる優れたモデルを提供し、組織に大きなメリットをもたらします。Zscalerがインフラ管理とそれに伴うコストの全責任を負うため、運用負荷の削減をさらに進めることができます。

スマートな設定

Zscalerがすべてのインフラ設定を担当します。膨大な事前準備を必要とせず、リソースを迅速にアクティブ化し、わずか数分でパブリック クラウドのトラフィックを保護します。

リソース ライフサイクル管理/ワークフロー制御

パブリック クラウドにおいて不可欠なこの機能は、リソースの作成から廃棄までの管理を効率化します。メトリクスの追跡と迅速な対応を通じたコストの最適化に重点を置いています。

自動スケーリング

Zscalerは、ネイティブのパブリック クラウドの適応型スケーリングを活用し、トラフィック量、スループット、帯域幅に関するお客様の懸念を解消します。これにより、お客様は独自の環境内のリソースとは異なり、管理、設定、トラブルシューティングの手間を省くことができます。

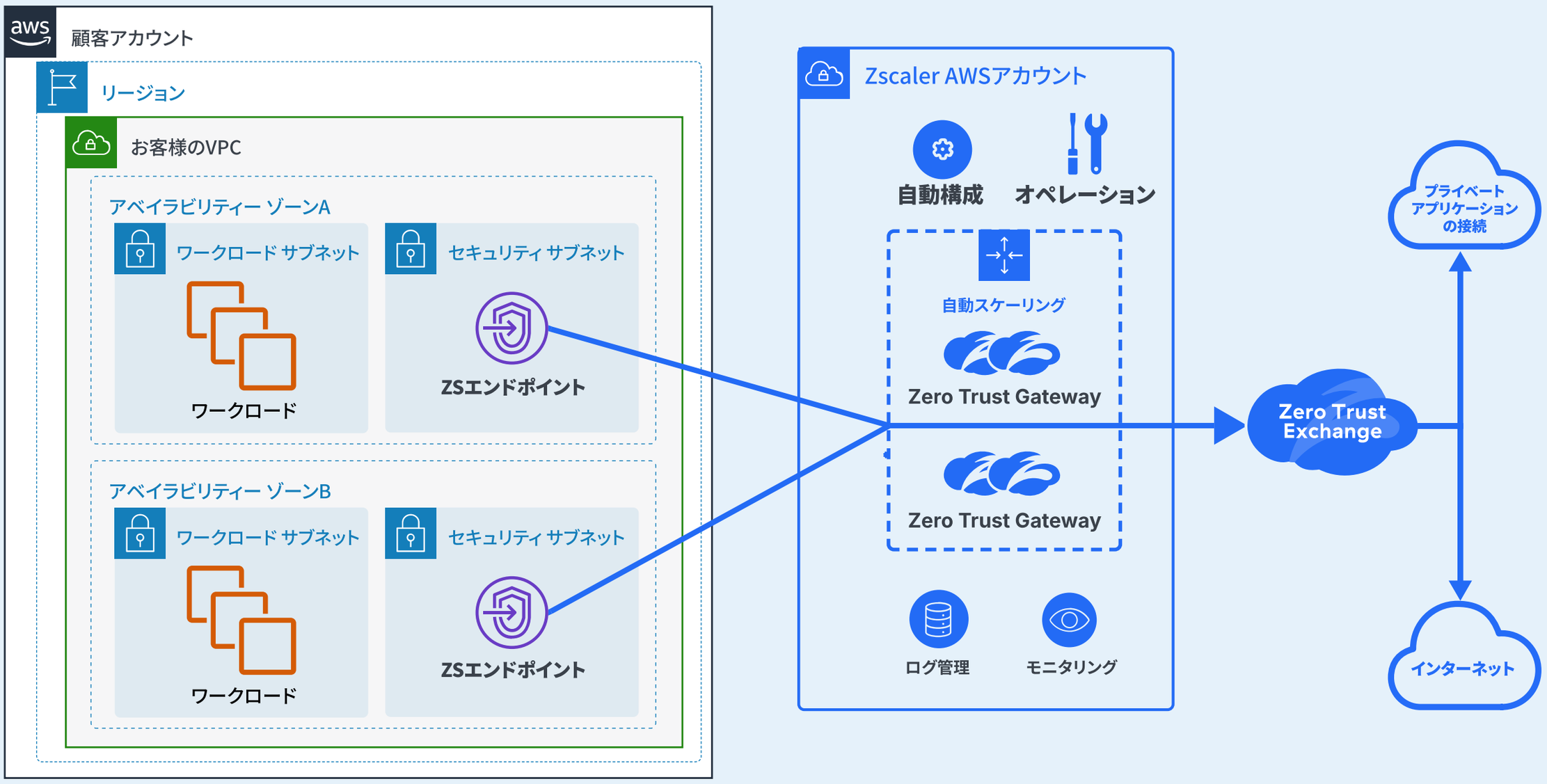
監視/可視性

パブリック クラウドのデフォルトのログ記録や監視機能には制限があることが多いですが、Zscalerは、詳細なログを提供し、詳細な可視性を実現します。また、イベントに応じたネイティブな適応型スケーリングを組み込んでおり、すべてのパケットを監視できるため、包括的なインサイトと制御が確保されます。

管理/ログ記録の一元化

マルチクラウドのログを単一のポータルで集中管理できます。これにより管理が簡素化され、リアルタイムの監視、トラブルシューティング、迅速なインシデント対応が可能になります。また、さまざまなクラウド展開におけるレポート作成や監査プロセスも効率化されます。

ZTGW FOR AWSが新登場。AWS VPCエンドポイントを接続するだけで作動



このサービスは、Zscalerにより包括的に管理されます。広範なZero Trust Exchangeと同様、お客様は基盤となるインフラを管理する必要がありません。これは、15年以上にわたり世界最大規模のセキュリティ クラウドを運用してきた、Zscalerの実証済みの能力を拡張したものです。豊富な経験と専門知識を活かしてこのクラウド サービスを拡大し、AWSからの接続をZTGW経由で円滑に提供します。

お客様が、AWS Transit Gateway、AWS Cloud WAN、分離されたVPCs、あるいはそれらを組み合わせた環境のいずれを標準として採用していても、ZTGWは接続を円滑化することが可能です。展開戦略は、主に以下の観点(次ページ参照)により異なります。

展開オプション

本書は導入ガイドではありませんが、Zscalerの視点からZTGWのコンセプトを説明します。後続のセクションで、AWSネットワーク トポロジーについて詳しく掘り下げていきます。

Zscaler ZTGWの導入にあたって、既存のAWSネットワーク トポロジーを変更する必要はありません。Zscalerは、あらゆる一般的なトポロジーに対応しています。これらの構成を視覚化した図解も提示します。パブリック クラウド環境におけるイノベーションの急速な進歩を考えると、将来的にはさらに多くのオプションが利用可能になる可能性があります。本書でカバーされていない潜在的なソリューションについてご質問がある場合は、ご遠慮なくAWSおよびZscalerの担当者までお問い合わせください。

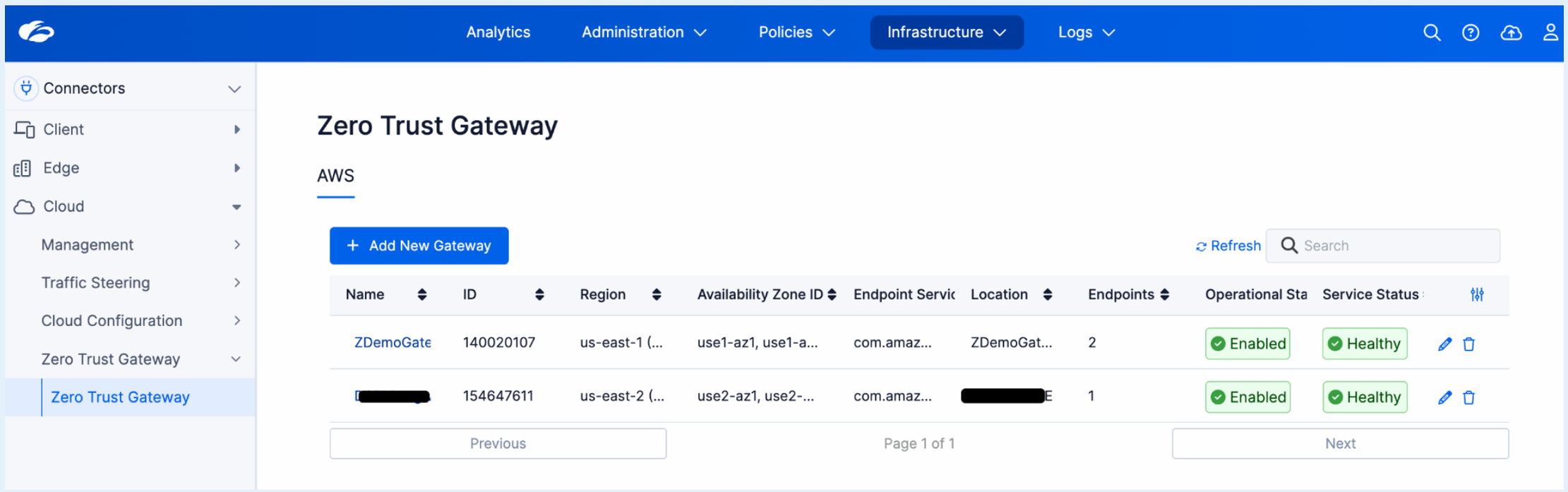
ZTGWの必要数は、AWSリージョン、アベイラビリティー ゾーン、環境の分離状況によって異なります。本番/非本番VPCの区別がなく、2つのAZを持つ単一のリージョンには、2つのZTGWが必要です。本番/非本番環境のVPC/TGWが別々にある場合は、トラフィックを分離するために、それぞれの環境に専用のZTGWセットが必要になる場合があります。VPCエンドポイントは、AWSのネットワーク トポロジーや要件に応じて、中央に集約するか、各ワークロードVPCに配置するかを選択できます。

Zero Trust Gatewayの作成

1つのZTGWは単一のAWSリージョン内で稼働し、複数のアベイラビリティー ゾーン(AZ)をカバーします。各ZTGWでは、最低2つのAZを選択する必要があります。選択されたAZ内では、Zscalerのアカウント側でマネージド コネクターが展開および拡張され、現時点で1つのZTGWあたり最大10Gbpsのスループットを提供します。

各ZTGWは、同じAWSリージョン内のAWS Gateway Load Balancer (GWLB)のVPCエンドポイントからの接続をサポートします。ネットワーク トポロジーにもよりますが、これは幅広く対応が可能です。例えば、リージョンごとのセキュリティVPC内に配置された2つのVPCエンドポイントから、最大50個の分離されたVPC (それぞれがリージョンZTGWに接続された独自のVPCエンドポイントを持ちます)までサポートします。

複数のZTGWが異なるリージョンに展開されていることを示す例



ZTGWの重要な側面は、Zscaler Internet Access (ZIA)のユーザーには馴染みのある、ロケーション オブジェクトとして機能することです。他のトラフィック転送手法と同様に、ZTGWはZIAおよびZPAの両方と同期されたロケーションを表します。これにより、VPC CIDR、タグ検出による特定の属性、またはVPCエンドポイントIDによって定義されたサブロケーションの使用が可能になります。この機能により、ポリシー制御とレポートの柔軟性が向上し、VPCごとにZTGWを展開する必要がなくなります。

AWS内に別個の本番環境、非本番環境、テスト環境を持つ組織を考えてみましょう。トラフィックの分離は組織のポリシーによって決定されます。これらすべてのVPCがリージョンごとに1つのAWS Transit Gatewayに接続する場合は、リージョンごとに1つのZTGWで十分です。ただし、リージョン内の分離のために3つの個別のTGWが使用されている場合は、すべてのTGWを同じZTGWに接続し、サブロケーションを利用して本番環境、非本番環境、テスト環境を区別するか、別々のZTGWを3つ展開するかを選択できます。

AWSネットワーク トポロジーとZTGWエンドポイントの展開場所に基づくサポートのフロー

AWSネットワーク トポロジー	VPC間	同一VPC内のサブネット間
ゼロトラスト ゲートウェイ		
セキュリティVPC内にトランジット ゲートウェイを配置したリージョンZTGWエンドポイント	あり	なし
セキュリティVPC内にCloud WANを配置したリージョンZTGWエンドポイント	あり	なし
VPCあたりのZTGWエンドポイント数	なし	あり

注: これらを組み合わせることで、すべてのユース ケースに対応できます。すべてのモデルがZIAおよびZPAへのトンネリングをサポートします

AWS Transit Gatewayを使用した集約型モデル

AWS Transit Gatewayを活用している組織は、ZTGW VPCエンドポイントをセキュリティVPCや検査用VPCなどの既存のVPCにシームレスに統合できます。あるいは、ZTGW VPCエンドポイントを含む新しいVPCを構築し、それを既存のTransit Gatewayに接続することも可能です。この構成により、デフォルト ルート(0.0.0.0/0)をZTGW VPCエンドポイントに向ける、あるいはさまざまな個別のアプリケーション向けのトラフィックを選択的にルーティングするといったことが可能になります。

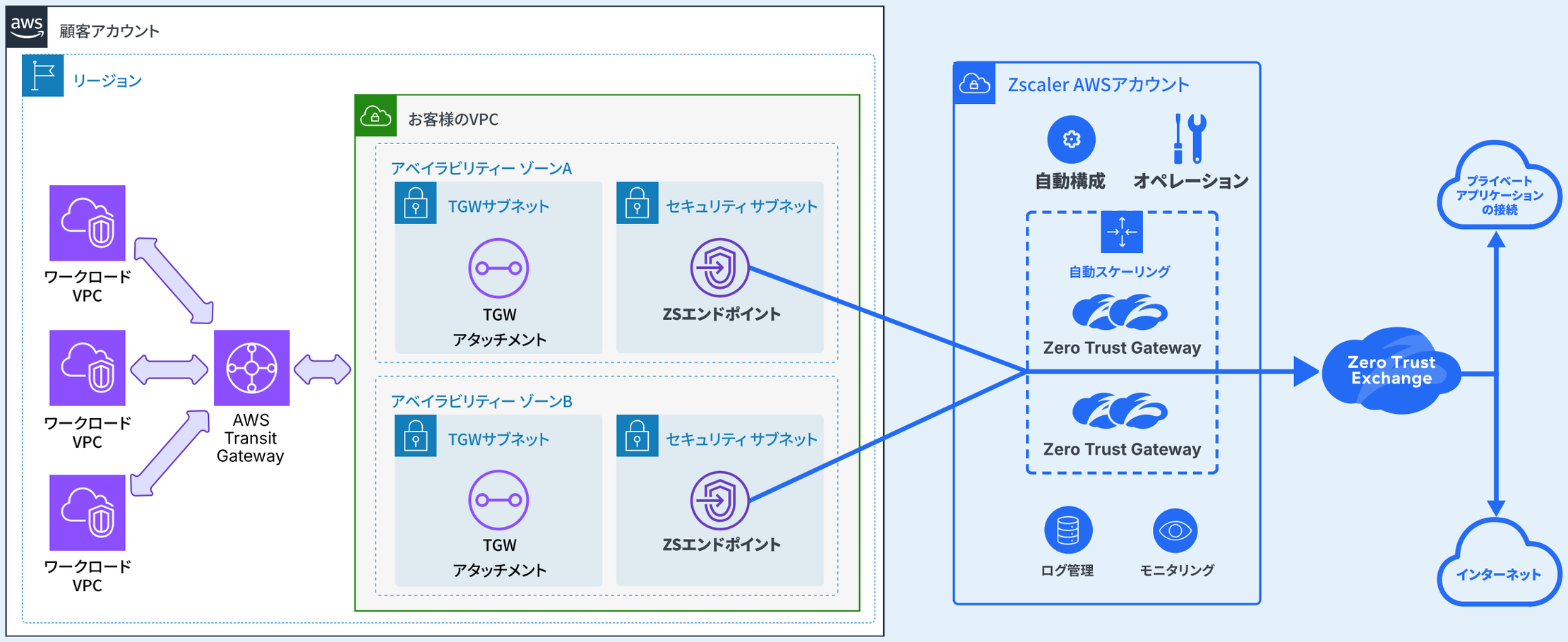
このモデルでは、同一リージョン内にある複数のTransit Gatewayを同じZTGWに接続することも、あるいは環境(本番、非本番、開発など)ごとに各Transit Gatewayを分離するために、個別のZTGWサービスを構築することもできます。

ZTGW VPCエンドポイントを、各ワークロードVPCに直接配置するのではなく、集約型VPCに配置した場合、以下のユース ケースに対応できます。

ZIA経由のインターネット出口のセキュリティ

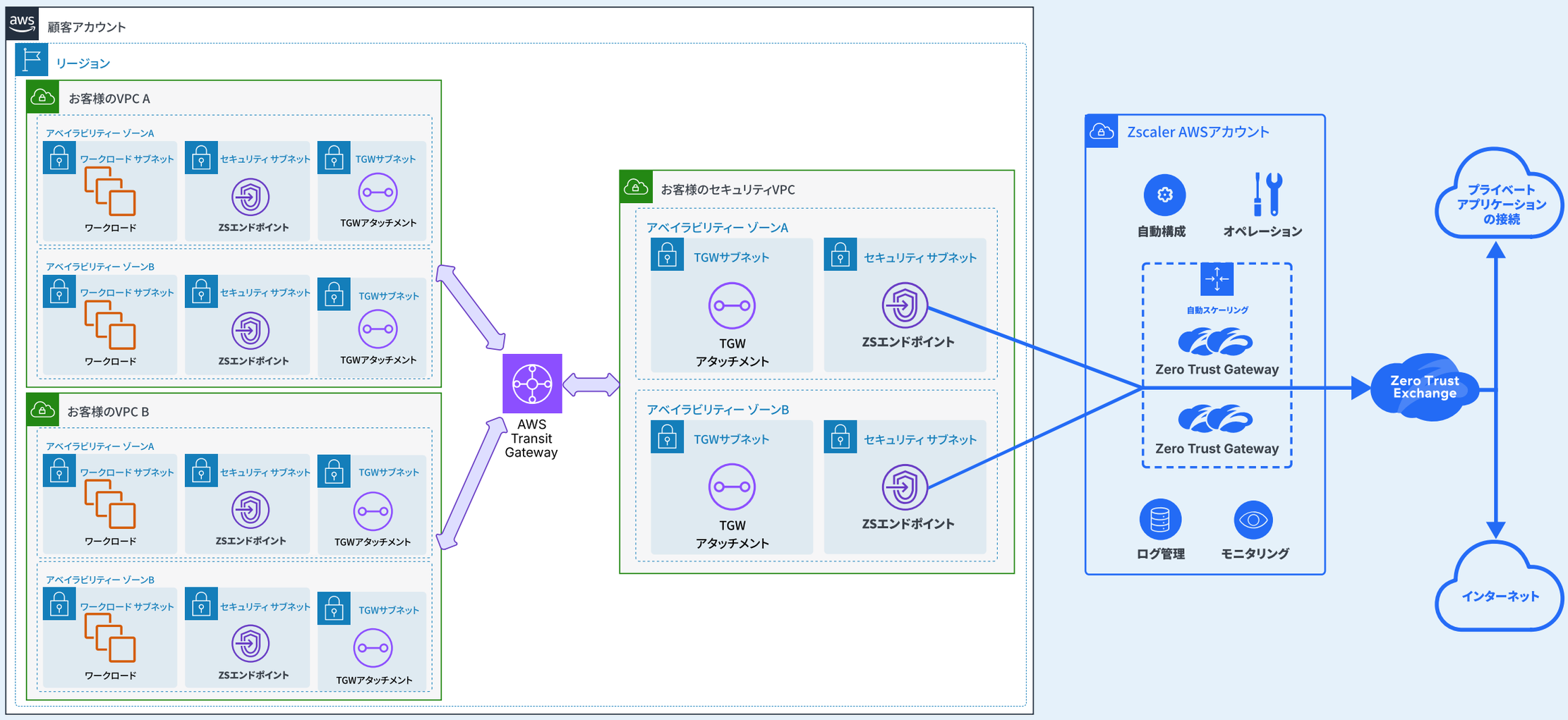
ZPA経由のプライベート アプリケーション アクセス

同じTGW内のVPC間のEast–Westファイアウォール ルール



TGW集約型エンドポイントとワークロードVPCエンドポイントを使用したハイブリッド モデル

このトポロジーは、お客様から頻繁にリクエストされるものではありませんが、例示的に掲載するのは重要な目的があるためです。それは、このネットワーク アーキテクチャーにおいて、前述した東西方向の通信のユース ケースすべてに効果的に対応するためには、ZTGW VPCエンドポイントの戦略的な配置が不可欠であるということです。VPC間のトラフィックだけでなく、各VPC内のサブネット間やサブネット内部のトラフィックも、包括的に可視化して制御できるようにするためには、この配置が必要です。



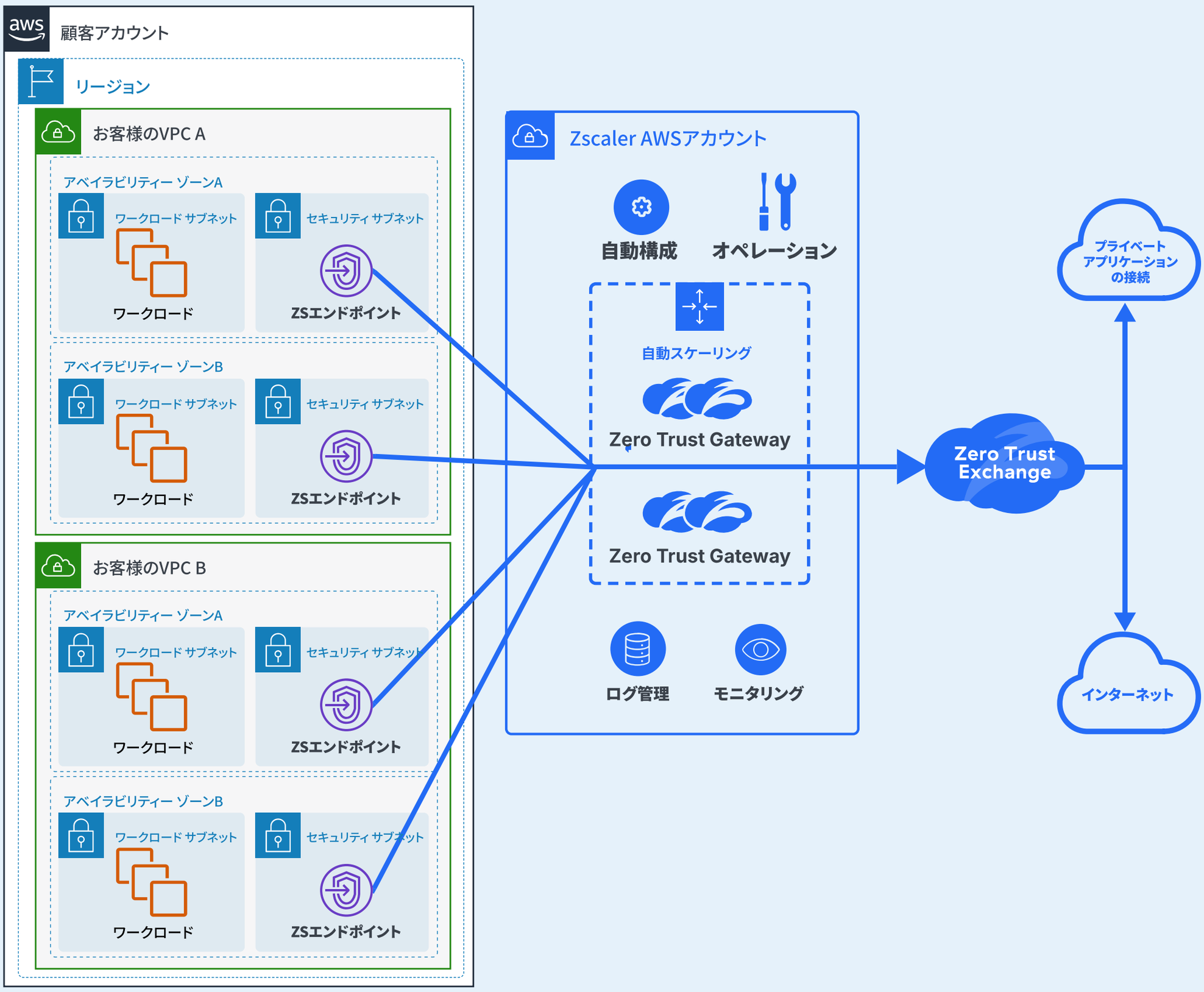
分離されたワークロードVPCを用いた分散型モデル

ZTGW VPCエンドポイントを、Transit Gatewayに接続した集約型セキュリティVPCではなく、
各ワークロードVPCに配置する場合、以下のユース ケースがサポートされます。

ZIA経由のインターネット出口のセキュリティ

ZPA経由のプライベート アプリケーション アクセス

同じTGW内のVPC間のEast-Westファイアウォール ルール



ZTGWサービス アーキテクチャー

ZTGWサービスは主に2つのサービスに分かれています。

コントロール プレーン

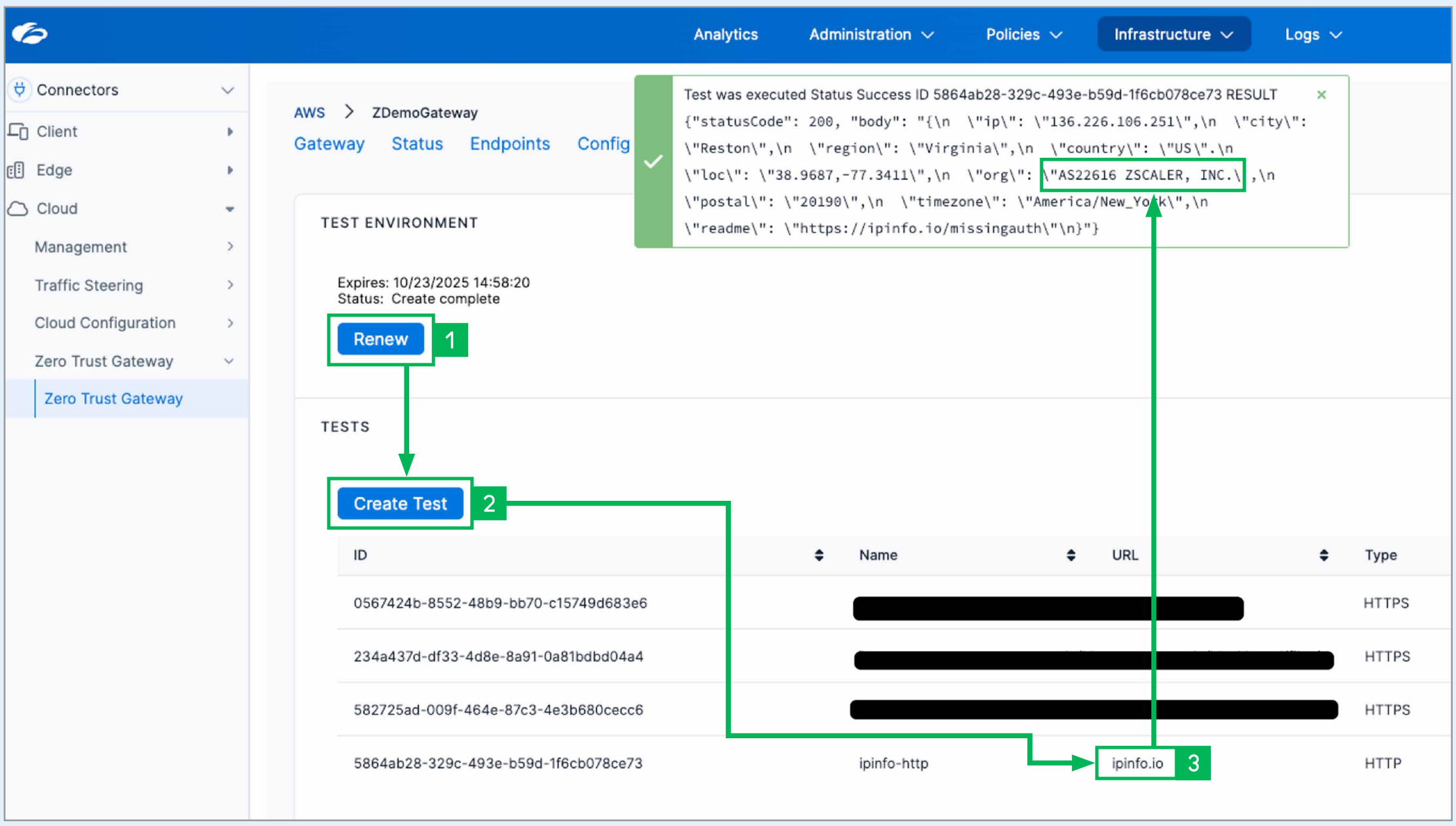
**サービスの設定とオーケスト
レーションを担います**

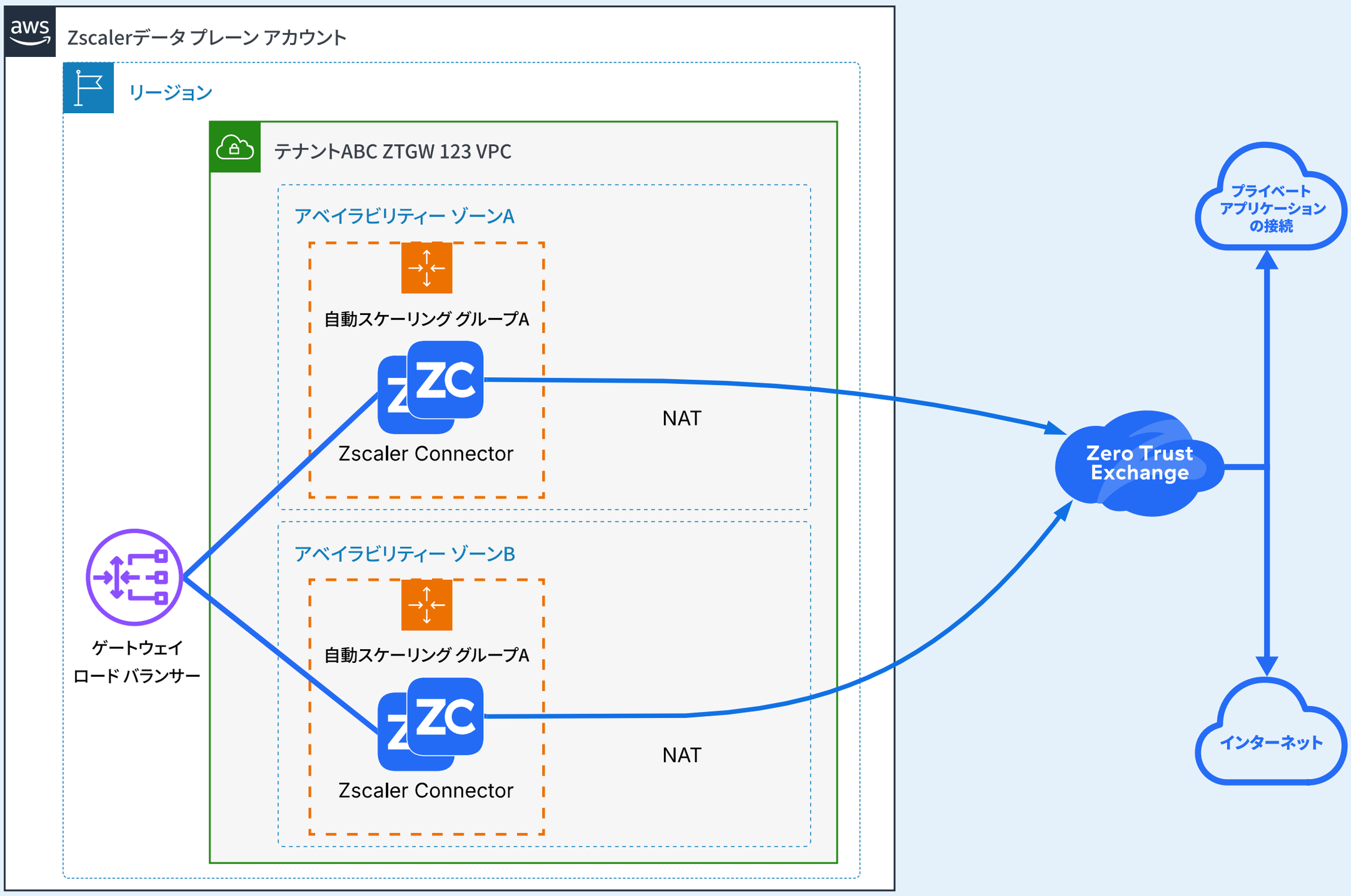
データ プレーン

**お客様のワークロード トラフィック
が流れる場所です**

コントロール プレーンは、専用のZscaler所有のAWSアカウント上で、最新のAWSネイティブ サービスを用いて構築されたマルチテナント サービスです。ログ記録、メトリクス収集、メンテナンス、新しいZTGWの配置、ソフトウェア アップデート、ルールの同期などの様々な操作は、このコントロール プレーンを介して行われます。また、過去の設定履歴、統計データ、分析機能もここに集約されています。お客様のトラフィックがコントロール プレーンを通過することはありませんが、オプションで実施可能なトラフィック テストについては、コントロール プレーンを通じて管理されます。

複数のZTGWが異なるリージョンに展開されていることを示す例





Zscalerは、サービスのレジリエンスとコスト効率を高めるために、絶えず改善と革新を続けています。現在、ZTGW Connectorsは、Zscaler Internet Access (ZIA)やZscaler Private Access (ZPA)への安全なトンネル接続に加え、Connectorからのトラフィックの直接送信や、東西方向のローカル トラフィックへのポリシー施行を行うことができます。

ZTGWの安全な設計

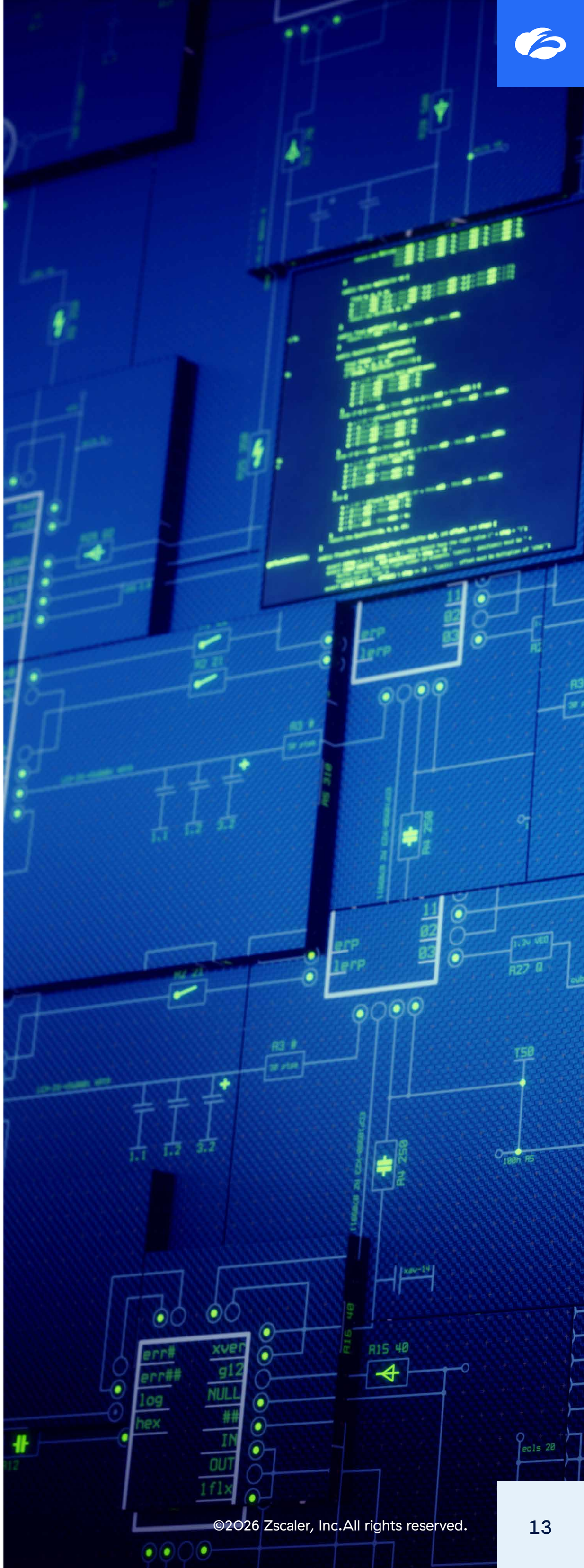
ZTGWサービスのコントロール プレーンおよびデータ プレーンは、多層防御とベスト プラクティスに基づいて設計されており、お客様のデータの完全性を確保し、サービスへのアクセスを承認されたリクエストのみに厳格に制限することができます。本サービスの設計に関するより詳細な情報については、Zscalerの担当者までお問い合わせください。

- ZTGWの基盤となるゲートウェイ ロード バランサー(GWLB)サービスは、Zscalerポータル内でお客様が許可したAWSアカウント(AWSアカウントID、またはTag Discoveryサービスと連携したアカウントで定義)からのVPCエンドポイント接続リクエストのみを受け入れます。許可されていない他のAWSアカウントが、お客様のZTGWサービスを検出したり接続したりすることはできません。

- Zscalerのセキュリティ部門は、最小特権の原則や強固なIAMポリシーなどのベスト プラクティスを確実に順守するため、展開前および継続的に厳格なサービス レビューを実施します。また、クラウド セキュリティ ポスチャー管理(CSPM)ツールを活用し、設定ミスやセキュリティ ドリフトを予防的に検知して修正します。

- 各ZTGWはシングル テナントとして動作します。つまり、異なるテナントやお客様のワークロード トラフィックが、同じZTGW Connectors内で混在することはありません。これにより、ZTGWサービス内での完全なネットワーク分離が保証されます。

- ZTGWのコントロール プレーンとデータ プレーンのサービスは、それぞれ個別のAWSアカウントに分かれています。



メリット

AWSへのZscaler ZTGWの導入により、組織は運用上の課題に悩まされることなく、ポリシー、可視性、そしてセキュリティ ポリシーを優先できるようになります。主なメリットを5つ紹介します。

シンプルな展開プロセス

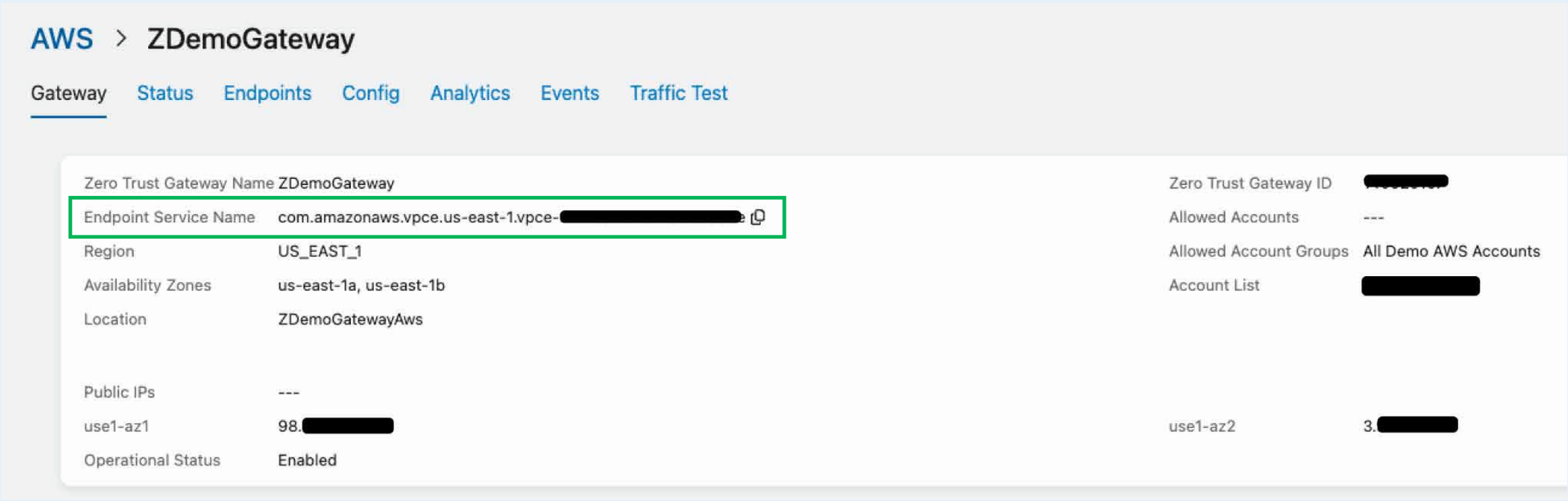
ZTGWの展開は5分以内で完了します。場所の名称、リージョン、アベイラビリティー ゾーン、信頼できるAWSアカウント情報を入力すると、ZscalerのAWSアカウント内に新しいZTGWサービスが展開されます。完了後、Zscalerコンソールにサービス名が表示されます。

各事業部門へサービス名を通知して各VPCからVPCエンドポイントを接続させるか、AWS CloudFormationやTerraformを用いて自動化するかに関係なく、作業プロセスは展開から接続操作に移行します。AWSのルート テーブルが更新され、トラフィック(デフォルト ルート0.0.0.0/0など)が、ZTGW VPCエンドポイントに送信されます。その後Zscalerを介して、セキュリティ ポリシーが管理されます。

業務上の負担の軽減

共同責任モデルが適用される一般的なEC2インスタンスベースのソリューションとは異なり、ZTGWはZscalerが完全に管理するフルマネージド サービスです。お客様の責任範囲は、ZTGWサービスに接続されているVPCエンドポイントが許可されたAWSアカウント内にあることの確認と、ルーティングの適切な設定の徹底のみに限定されます。ZTGWサービスは、Zscaler側のAWSアカウントにおいて、複数のアベイラビリティー ゾーンとAuto Scalingを活用して運用されているため、ネイティブなAWSサービスのように機能します。これにより、キー ローテーションや、トラブルシューティングのためのSSHアクセス、設定の更新といった作業が不要になります。ZscalerはCloud ConnectorなどのEC2インスタンスの更新を管理していますが、ZTGWにおいては、大規模な変更時であってもお客様による介入は不要です。Zscalerが提供するログやメトリクスなどの広範な運用インサイトは、このソリューションを通じてお客様に提供されるメリットをさらに強化します。世界最大規模のセキュリティ クラウドを運用してきたZscalerの実績が、ZTGW接続ソリューションへと拡張されました。

AWSから接続するためのエンドポイント サービス名を含むZTGWの詳細例



自動スケーリング

Zscaler ZTGWは、AWS Auto Scalingを活用してスループットの制限に対処します。この設計により、ZTGWはコストを最適化しつつ、トラフィックの持続的な需要やバーストに対応できます。現在、各リージョンのZTGWは最大10Gbpsをサポートしており、今後さらにスループットを増加する計画です。合計で10Gbpsを超えるスループット要件が必要な場合は、ZTGWインスタンスを複数のリージョンや環境に分散させることで対応します。

コスト削減と統合

AWSサービスを活用するクラウドネイティブなソリューションであるZTGWは、コストの最適化が可能です。変動要因が多いため、一律のコスト計算式を提示することは困難ですが、月間の通信量(GB/月)が増えるほど、コスト削減効果は高まる相関関係にあります。削減効果は主に以下の3つの領域に分類されます。

既存のセキュリティ サービス費用を除いたコストの最小削減額(削減額は条件により異なります

ZTGWのコスト削減		
領域	**コスト**	**サービス**
EC2コンピューティング	AWS利用料	EC2インスタンス(時間単位) EC2 Amazon Elastic Block Storage (EBS)
VPCネットワーキング	AWS利用料	インターネットへのデータ転送量(DTO) NAT (ネットワーク アドレス変換)ゲートウェイ インターネット ゲートウェイ パブリックIPアドレス GWLBサービス GWLBクロスゾーン データ転送
オペレーション	AWSおよびソフト利用料	Amazon CloudWatch ソリューションの導入と管理に要する時間および必要とされる専門知識の大幅な削減

以下では、ZTGWがこれらのコスト削減にどのように寄与するかを詳しく解説します。

計算

ZTGWサービスはAWS内でネイティブに動作するため、Zscalerとの接続のためにEC2インスタンスを展開および管理する必要がありません。従来、AWS VPCのネットワーク トラフィックを保護するには、リージョン数、VPC数、およびスループットに応じて多数のEC2インスタンスが必要でした。例えば単一のVPCを保護する場合や、Transit Gatewayを利用して特定のワークロードをセキュリティVPCに集約して保護する場合でも、小規模な高可用性のペアで、月額最低100ドルのコストが発生することがありました。

ネットワーキング

Zscaler ZTGW for AWSは、従来のEC2ベースのファイアウォール ソリューションと比較して、セキュリティを強化するだけでなく、大幅なネットワーク コストの削減を実現します。従来の手法では、パブリックIPアドレスを使用する場合でもNATゲートウェイの背後に配置する場合でも、多額のデータ転送量(DTO)とNATゲートウェイの費用が発生することが一般的でした。

ネットワーキング コストの主な要因は以下の3つです。

- **DTOコスト:** 月間のGBあたりの処理量に基づきます。データ転送量が多い場合、階層型料金により数百ドルから数万ドルに達することがあります。
- **NATゲートウェイのランタイム コスト:** トラフィックがない状態でも、NATゲートウェイの維持には毎月数百ドルのコストがかかる場合があります。
- **NATゲートウェイのGBあたり処理量:** DTOと同様にデータ量に基づくため、10TB以上の処理では月額数百ドルが加算される可能性があります。

ZTGWは、サービス自体をZscaler側のAWSアカウントでホストすることで、これらのコストを軽減します。お客様側で発生するネットワーキング コストは、ZTGWサービスに接続するためのGWLB VPCエンドポイントの時間料金とデータ処理料金のみです。トラフィックは、お客様のAWSアカウントからではなく、AWS PrivateLinkを介してZscaler側からAWSを抜けていくため、お客様側のDTOおよびNATゲートウェイのコストは完全に排除される点が重要です。

Zero Trust Cloudプラットフォームの一部としてZTGWのサブスクリプション(必要なZTGW数と月間データ量に基づく)は必要ですが、AWS内でのサービス アーキテクチャーにより、TCO(総所有コスト)が削減され、そのコスト節約分をお客様に還元することが可能です。

お客様のAWS環境における具体的な削減見込みについては、Zscalerの担当者までお問い合わせください。また、AWSの請求および使用状況コンソールやAWS料金計算ツール(https://calculator.aws)を使用して、現在のコストのベースラインを算出することもできます。

オペレーション

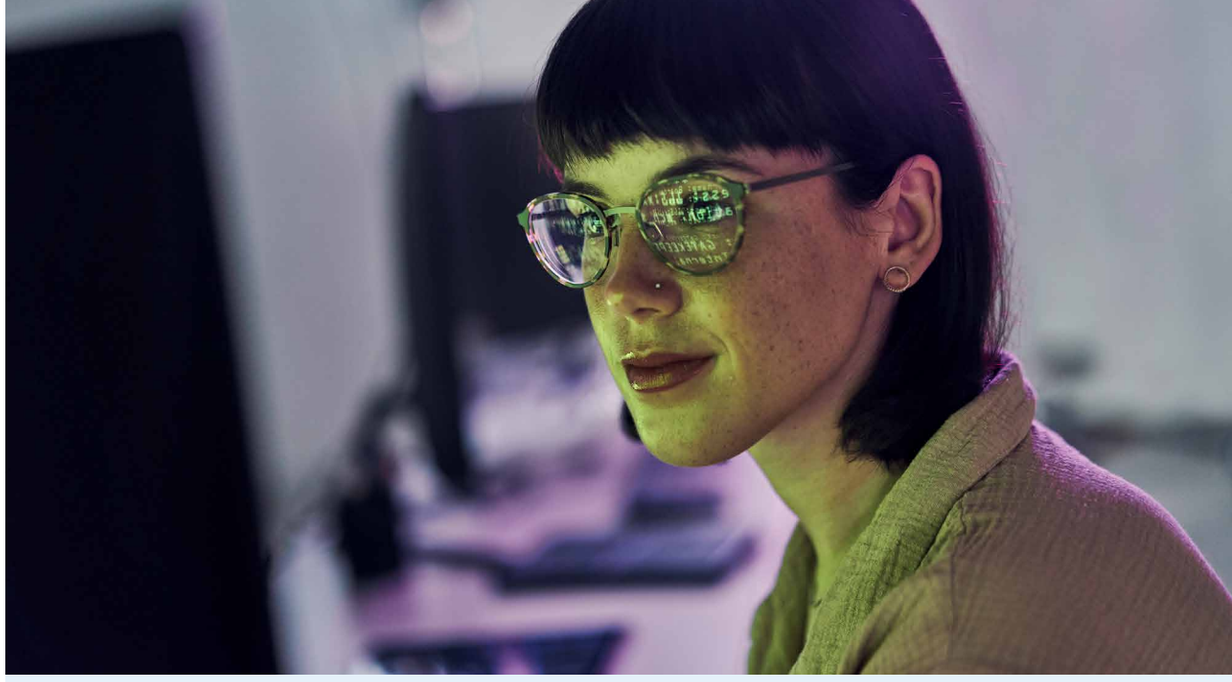
ZTGWは、AWS内でEC2インスタンスベースのセキュリティ アプライアンスを構築、管理、トラブルシューティングする手間を排除するため、日々の運用と計画が簡素化されます。これにより、主に以下のような利点が得られます。

- **サイズ設定の簡素化：**ZscalerがZTGW VPCエンドポイントのサイズ設定を管理するため、リージョンごとの出口における内部的なサイズ設定作業が不要になります。

- **複雑な設定の軽減：**ZTGWでは、ZTGW VPCエンドポイントの接続とルート テーブルの更新のみで展開が完了します。セキュリティ アプライアンス、負荷分散、自動スケーリングのための複雑なTerraformの変更は不要です。

- **可視性と制御の一元化：**すべてのトラフィックがZscalerを経由することで、エンドツーエンドの可視化と制御が可能になります。セキュリティ管理が統合され、複数のベンダーやツールの必要がなくなります。

要約：Zscaler ZTGWは、Security as a Serviceを実現することで、シンプルさとコスト削減の両面で大きなメリットをもたらします。これにより、組織はセキュリティ ポリシーの精緻化に集中できます。ZTGWによって得られるメリットに関する詳細は、次のセクションの各種リソースを参照してください。



リソース

サービスについての詳細は、次のブログをお読みください。
https://www.zscaler.com/jp/blogs/product-insights/zscaler-zero-trust-cloud-zero-trust-gateway

ビデオ、閲覧資料、インタラクティブ デモを含む詳細は、Zero Trust Gateway Hubでご確認いただけます。
https://app.storylane.io/hub/dlvieowha6az

Zero Trust Cloudの展開オプションの詳細は、次をご覧ください。
https://www.zscaler.com/jp/resources/solution-briefs/deployment-models-for-zero-trust-cloud.pdf

ZTGWの追加の構成情報は、Zscalerヘルプポータルのドキュメントでご覧いただけます。
https://help.zscaler.com/jp/cloud-branch-connector/what-zero-trust-gateways

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™プラットフォームは、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SSE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.com/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.com/jp**

zscaler™

Zero Trust Everywhere