データシート

Cloud Connectorで ワークロード通信を保護

Direct-to-Cloudアーキテクチャによる、インターネットや プライベートアプリケーションへのワークロードの シンプルで安全なアクセス

クラウドの高度ネットワーク通信

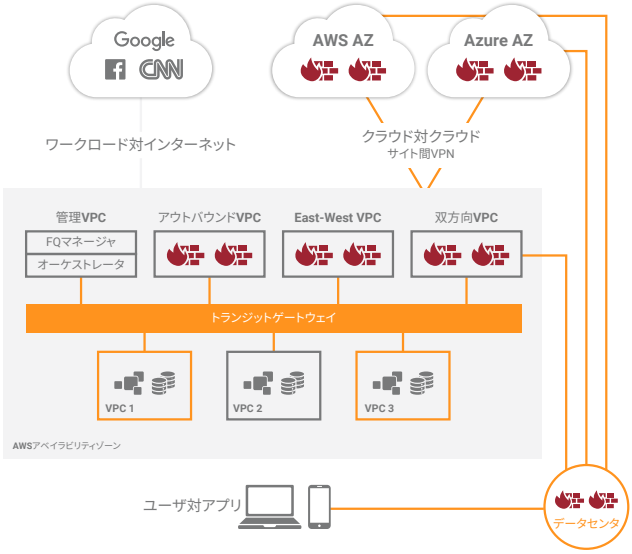
ワークロードのクラウドへの移行とユーザのモバイル化に伴い、ネットワークトランスフォーメーションビジネスを推進して競争力を維持することが多くの組織の急務となっています。従来型のネットワークを拡張し、ファイアウォールを使用して境界ベースのセキュリティを適用する方法は、現実的な解決策ではありません。インフラストラクチャを最新化を進める組織にとって、ワークロードの効率的な通信の確保は、絶対的な要件となりました。ゼットスケーラーのCloud Connectorは、ワークロード通信を全面的に再構築することで、インターネットやプライベートアプリケーションへのワークロードのシンプルかつ安全なアクセスを実現します。Cloud Connectorは、従来型のネットワークセキュリティとは異なり、実績あるゼットスケーラーのZero Trust Exchangeプラットフォームに構築されたDirect-to-Cloudアーキテクチャを採用しています。ネットワークトランスフォーメーションをCloud Connectorを採用して推進することで、セキュリティの強化、運用の簡素化、さらには、可視性、可用性、パフォーマンスの向上が可能になり、コスト削減などの多くのメリットが実現します。

従来型のネットワークセキュリティによるワークロード接続の課題

パブリッククラウドやデータセンタ環境でワークロードをインターネットや他のアプリケーションに接続する手段として従来型のネットワークやセキュリティのアーキテクチャを使用すると、次のような多くの課題に直面します。

- **脅威の水平移動やインターネットベース攻撃のリスク** - クラウド VPN、サイト間 VPN、ファイアウォール、 WANテクノロジなどのネットワーク中心の従来型の接続ソリューションを使用することで、お客様の信頼できるネットワークが他のクラウドやオンプレミスの環境にまで過剰に拡張され、ネットワークの攻撃対象領域が拡大します。セキュリティアプライアンス、ツール、非標準のポリシーを寄せ集めると、既知と未知のセキュリティカバレッジのギャップによってセキュリティリスクが増大します。
- **環境の複雑化** - 複雑なルートフィルタリング、複数のネットワークホップ、ネットワークやセキュリティの仮想アプライアンス、さらには従来型のこれらのモデルをクラウドに導入することで、ポリシー管理が断片化し、環境が複雑になります。このような複雑さの軽減が、マルチクラウドやハイブリッドクラウドの環境で標準化されたワークロード接続やセキュリティポリシーを適用しようとするセキュリティチームにとって困難な作業となっています。
- **可視性の欠如** - アプリケーションの接続パスを可視化できないために、ネットワークやセキュリティに死角が生まれます。クラウドワークロードの分散化が進み、環境の規模も拡大しています。このような分散型のワークロードを接続するには、不明確なマルチホップネットワークや複数のネットワーク /セキュリティアプライアンスの「デイジーチェーン」が必要になります。このような複雑な接続と一元的なログの欠如により、オペレータがアプリケーション通信を把握できません。
- **パフォーマンスとスケーラビリティの低下** - パブリッククラウド環境に存在するネットワークやセキュリティサービスの増加に伴い、トラフィックのヘアピンや一元的なセキュリティインスペクションとコントロールのためのチョークポイントが発生しています。
- **高コスト** - 従来型のネットワークセキュリティアプライアンス（ファイアウォール、 IPS、ルータ、その他のポイント製品など）、スケーラビリティの欠如を補うためのネットワークサービスの過剰なプロビジョニング、トランジットピアリングなどのクラウドネイティブサービスの利用の増加などにより、コストが増大します。

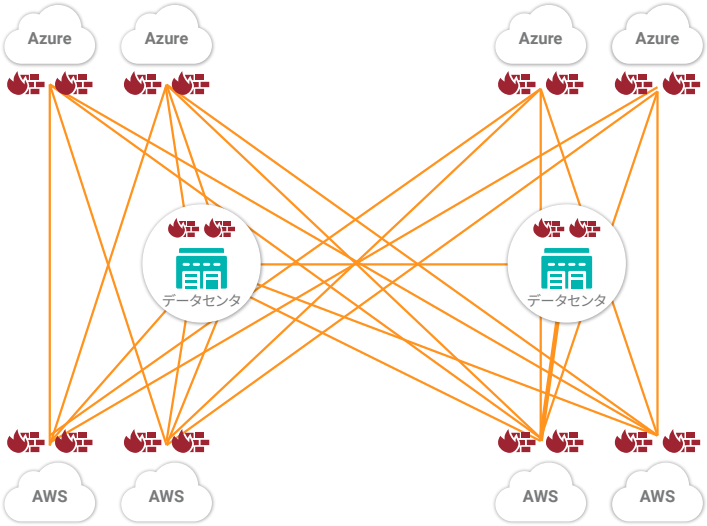
従来の方法：企業WANをクラウドに拡張する



コストが高く、運用が複雑で、ユーザエクスペリエンスが低下し、
WANの水平移動によりセキュリティが低下

企業ネットワーク　公共インターネット

マルチクラウドでは複雑さやリスクが何倍にもなる



サイト間VPNのメッシュ（従業員、パートナー、デバイス、顧客）
攻撃対象領域が拡大し、脅威の水平移動のリスクがある

企業ネットワーク

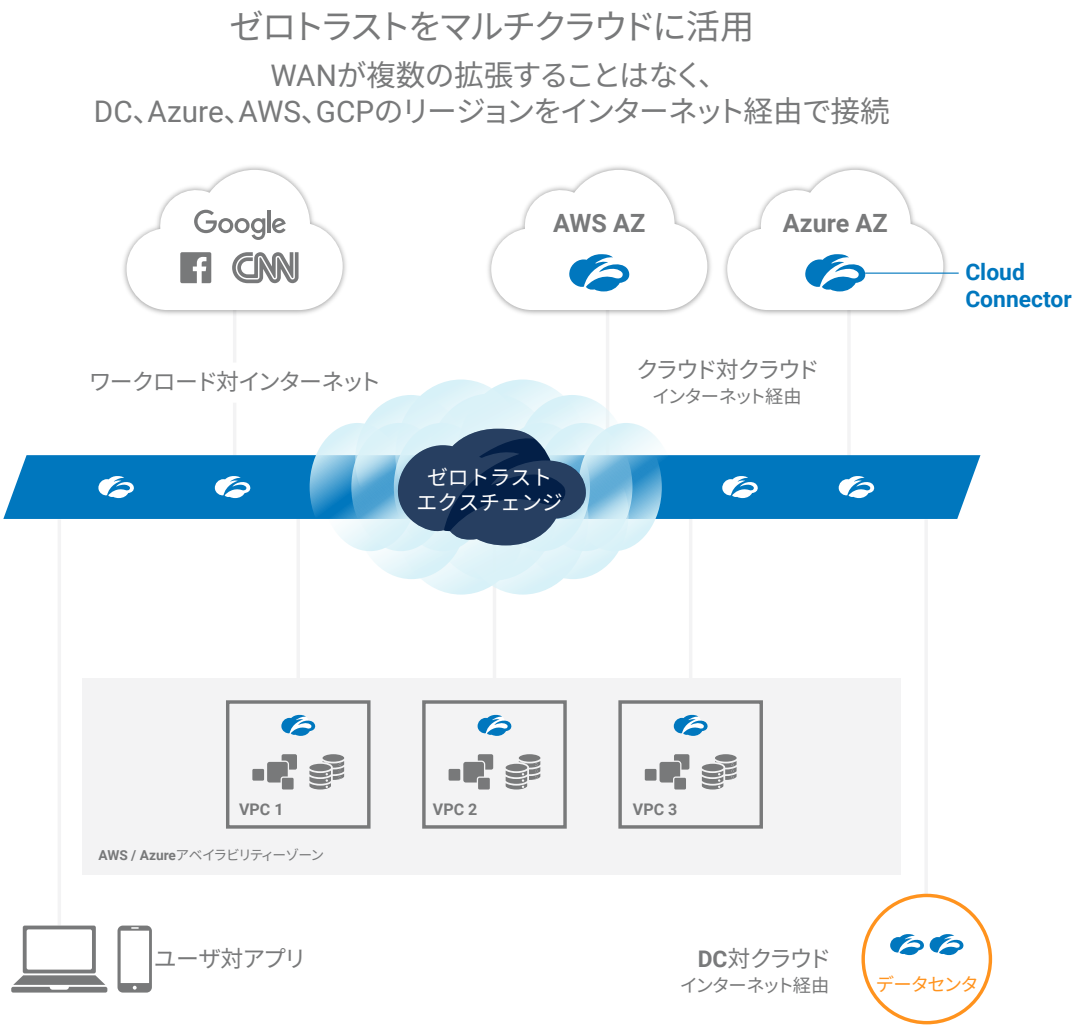
Cloud Connectorで実現するクラウドワークロードのゼロトラストアクセス

Cloud Connectorは、Direct-to-Cloudアーキテクチャの採用により、ワークロードにインターネットやプライベートアプリケーションへの高速でかつ高信頼性のアクセスを提供し、強力なセキュリティと運用の簡素化を実現します。Cloud Connectorは、完全プロキシアーキテクチャを使用してワークロードをインターネットやプライベートアプリケーションにダイレクト接続することで、ネットワーク攻撃対象領域を排除します。さらには、このアーキテクチャで、ルーティング、VPN、トランジットゲートウェイ、トランジットハブ、ファイアウォールが排除されるため、ワークロード通信が大幅に簡素化され、柔軟な転送が可能になり、実証済みのZIAとZPAのポリシーフレームワークを使用することでポリシー管理が容易になります。

Direct-to-Cloudアーキテクチャは、Zero Trust Exchangeを使うことで初めて可能になります。Cloud Connectorは、すべてのワークロード通信をZero Trust Exchangeに直接転送します。Zero Trust Exchangeで、ZIAまたはZPAのいずれかのポリシーを適用されて、ワークロード通信の完全セキュリティインスペクションとアクセスアイデンティティベースのコントロールが可能になります。ワークロード通信はさらに、Zero Trust Exchangeからインターネットやパブリッククラウドの他のプライベートアプリケーション、オンプレミスのデータセンタなどの送信先へと転送されます。この独自のアプローチには、3つの重要なメリットがあります。

- ネットワークベースのVPN接続からアイデンティティ /アプリケーションベースの通信に移行し、真のゼロトラストセキュリティを実現
- セキュリティを低下させることなく、従来型の「城を堀で囲む」アーキテクチャを排除でき、Squidプロキシ、NATゲートウェイ、IPSなどの従来型の製品は不要
- あらゆる場所に分散型でスケーラブルな接続を提供しつつ、ポリシー管理の一元化と自動化により、ワークロード通信を簡素化

Cloud Connectorは、ネットワークトランスフォーメーションの優先事項を様々な方法で解決するソリューションです。AWSリージョン、Microsoft Azure、Google Cloud、オンプレミスのデータセンタなどの分散型ネットワークや複数のクラウド間で、ゼロトラストの原則に基づき、ワークロード間の接続を拡張します。Cloud Connectorはさらに、パブリッククラウドやデータセンタのワークロードにセキュアインターネットアクセスを提供します。これらの機能はすべて、異種環境間のトラフィック転送、セキュリティ、ゼロトラストアクセスを可能にする統合ポリシープレーンを通じて提供されます。



コストと複雑さを軽減し、優れたユーザエクスペリエンスを提供
ゼロトラストモデルによる強力なセキュリティ

Cloud Connectorのメリット

複雑なネットワーク構成を必要としないシンプルな導入 - 従来型のアプローチには、トランジットゲートウェイ、トランジットハブ、SNATを経由する複雑なルーティング構成が必要で、これをVPCごと、クラウドごとに繰り返す必要がありますが、Cloud Connectorで必要なのは、インターネットへのデフォルトルートだけです。トラフィック転送やセキュリティのポリシー管理は、ワークロード通信の送信元や送信先に関係なく、Zero Trust Exchangeで一元化され、標準化されます。

Direct-to-Cloudによるエンドツーエンドの完全な可視性 - 従来の方法では、不明瞭なマルチホップネットワークに依存していたため、トラフィックの流れを把握するのが非常に困難で、ログも複数のネットワーク製品に分散していました。Cloud Connectは、クラウドへのダイレクト接続であるため、オペレータがワークロード通信を完全に可視化してコントロールでき、一元化されたログをリアルタイムでストリーミングし、SIEMや任意の監視ソリューションにエクスポートして相関付けや分析に利用できます。

中央のチョークポイントがないハイパースケーラビリティ - 従来型のアーキテクチャでは、トランジットゲートウェイ、ハブ、仮想ファイアウォールなどのスケーラビリティが欠如した中央のインフラストラクチャにすべてのトラフィックを送る必要があります。最新のZero Trust Exchangeアーキテクチャは、世界中に分散する150以上のハイパースケールのデータセンタで運用されており、水平方向のスケーラビリティにより、通信の増加にも柔軟に対応できます。

サービスを不必要に複製することなく高可用性を実現 - 既存のアプローチには、複数のファイアウォールとネットワーク構成の複雑な可用性アーキテクチャが必要で、複数のゾーン、リージョン、クラウドに複製する必要があるです。Cloud ConnectorのDirect-to-Cloudアーキテクチャは、必要なサービスがすべてZero Trust Exchangeで透過的に提供されるため、クラウドの構成要件が大幅に簡素化されます。お客様のサイトでは、転送とセキュリティにN+2の冗長性による自動フェイルオーバーが提供されます。

Zero Trust Exchangeが提供する合理的なサービスによるコスト削減 - サービスの過剰なプロビジョニングが不要になり、ファイアウォールのアイドルタイム、トランジットハブ、NATゲートウェイ、追加されたクラウド環境への複製のコストを削減できます。Cloud Connectorには、隠れたコストはありません。ネットワーキングやアクセスではなく、使用するセキュリティサービスに対して料金が請求され、お客様の環境の仮想ファイアウォールやプロキシのコストも不要になります。

Cloud Connectorの独自の価値

Cloud Connectorは、ビジネスポリシーを使用してユーザ、デバイス、アプリをあらゆるネットワーク、あらゆるクラウドで安全に接続するZero Trust Exchangeを基盤として構築されています。

- アプリケーションのワークロードは、基盤となる企業ネットワーク、VPN、WANに依存することなく、相互にダイレクト接続されます。
- アプリケーションが外部に公開されないため、攻撃対象領域なし
- 専用設計のマルチテナントプロキシアーキテクチャで、ポリシーを保持し、インスペクションし、適用
- スケーラブルなシングルスキャンとマルチアクセスのアーキテクチャにより、高パフォーマンスのインスペクションを実現
- Zscaler Internet AccessまたはZscaler Private Accessのポリシーによるインターネットとインターネット以外のトラフィックのきめ細かい転送ポリシー管理が可能
- AWS、Azure、Google Cloud、オンプレミスのデータセンタで、ポリシーの管理、トラフィックの監視、ログの追跡が統一され、標準化されます。

Cloud Connectorのユースケース

デジタルトランスフォーメーション

アプリケーションがクラウドに移行し、クラウドネイティブアプリケーションが構築されるようになると、ネットワークやセキュリティのオンプレミスモデルは崩壊します。デジタルトランスフォーメーションにはネットワークトランスフォーメーションが不可欠であり、ワークロード通信も新しいモデル、すなわち、ワークロードが基底となるネットワークから独立し、任意の送信先と安全に通信するモデルに移行することになります。Cloud Connectorは、デジタルトランスフォーメーションの実現を目標に構築されています。

VPNを使用しないワークロード接続

組織は、WANを拡張したりネットワーク攻撃対象領域を拡大させるVPNを利用したりすることなく、ワークロードをプライベートアプリケーションにダイレクト接続できるようになりました。

ゼロトラストの強制

ゼロトラストは、ネットワークが侵害され、信頼できない状態であると仮定します。Cloud Connectorはこのシナリオで、ネットワークを接続することなく、ワークロードをインターネットやプライベートアプリケーションにダイレクト接続します。すべての接続が監視され、監査の目的でログに記録されます。

クラウドワークロードのインターネットへのアクセスの保護

ワークロードは、ユーザの鏡像とも言えます。ワークロードもユーザと同様に、Zscaler Internet Access経由でクラウドにダイレクト接続され、同一のポリシーフレームワーク、セキュリティインスペクション、アクセスコントロールのメリットを活用できます。仮想ファイアウォールは必要ありません。

合併・買収

2つの異なるネットワークのマージは非常に困難で、時間もかかります。その過程では、IPの重複、ルーティングの問題、さらには、2つのネットワークのマージに伴うネットワーク攻撃対象領域の拡大に起因するセキュリティリスクの増大などの様々な問題に直面します。Cloud Connectorでは、ネットワークのマージは必要ありません。ネットワークをマージすることなく、あるネットワークのワークロードが別のネットワークのプライベートアプリケーションに迅速かつ中断なく接続できます。

ブランチの接続

Cloud Connectorのオンプレミス版であるBranch Connectorを利用すれば、ブランチのアプリケーションをプライベートアプリケーションやインターネットにとても簡単に接続できます。Branch ConnectorでSD-WANを補完でき、ゼットスケーラーはすべての主要 SD-WANベンダと提携しています。

機能ファクトシート

ゼロタッチプロビジョニングと自動デプロイメント

- AWS / Azureの定義済みテンプレートによるゼロタッチプロビジョニング
- 完全に自動化されたデプロイメント（AWS CloudFormation、Azure Resource Manager Templates、Terraform）
- ユーザの地理情報、アベイラビリティゾーン、VPC/VNETの動的検出
- SLA監視とフェイルオーバーを内蔵
- AWSやAzureのマーケットプレイスから入手可能

インターネットとインターネット以外のトラフィックに対するきめ細かい転送ポリシー

- トラフィックの送信オプション - ZIA、ZPA、またはダイレクト（ゼットスケーラーのサービスをバイパス）
- 柔軟なトラフィック選択基準 - ロケーション、サブロケーション、ロケーショングループ、5 タプル、またはFQDN
- 可用性の内蔵 - 次の利用可能サービス POPへのシームレスなフェイルオーバー

Cloud ConnectorとZIAによる転送とセキュリティの統一ポリシー

- ロケーションをVPC/VNETに対して動的に作成
- 動的なCloud ConnectorロケーションをZIAプラットフォームに同期
- Cloud Connectorが作成するロケーションは、既存のZIAロケーションのようなものです。IPS、SSLプロキシ、URLフィルタリング、データ保護などのあらゆるセキュリティポリシーを有効にできます。

ユーザからサーバ、サーバからサーバへの統一ゼロトラストポリシー

- ZPAがユーザ対アプリケーション、サーバ対サーバの統一ポリシーを提供
- 既存のZPAポリシーの強化により、新しいクライアントタイプ（Cloud Connector）を追加することでサーバ間接続をサポート
- AWS / Azure / データセンタのトラフィックの転送用に作成されたCloud ConnectorグループをZPAプラットフォームに同期

AWS / Azure / ブランチのConnectorの統一されたポリシー、コントロール、管理

- デバイスの状態やトラフィックを一元的に監視するダッシュボードをクラウドから提供
- Azure、AWS、ブランチの環境でフィルタリングが可能
- ZIA、ZPA、ダイレクト、DNSのフローカウントとバイトカウントを時系列で表示

統合ログインフラストラクチャであらゆる種類のトラフィックに対応

- ZIA、ZPA、ダイレクト（ゼットスケーラーをバイパス）へのトラフィックの詳細セッションログ
- パブリック DNSとプライベート DNSの両方ですべてのDNSトランザクションをログに記録
- NSSインフラストラクチャとの完全統合により、既存のNSSファイアウォール VMを使用したSIEMへのログのストリーミングが可能

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