ソリューション概要

Zscaler™ Private Access

アプリケーション／ユーザ単位で内部のプライベートアプリケーションへのアクセスを保護

ZSCALER PRIVATE ACCESSは、VPNのコスト、煩雑さ、セキュリティリスクのない、プライベートアプリケーション／アセットへのポリシーベースのセキュアアクセスを提供します。ZSCALER APPを使用した一元管理により、ZSCALERのCLOUD SECURITY PLATFORMのすべての機能をインターネットトラフィックに活用し、ポリシーベースで内部リソースへのアクセスを詳細に設定できます。

メリット

- 最適なセキュリティ：ユーザは、ネットワークではなく、アプリケーションにアクセスし、許可されているアプリケーションとリソースだけが表示されます。
- 付加価値：VPNハードウェアを購入、メンテナンス、アップグレードする必要はありません。緊急時に備えて冗長VPNや予備ユーザライセンスを用意する必要もなく、クラウドへと移行するためのサイト間VPNの設定も不要です。
- 優れたユーザエクスペリエンス：VPNクライアントにログインする必要はありません。アクセス権限のあるユーザであれば、アプリケーションが正しく動作します。
- 迅速な展開：アプリケーションの場所を自動的に検出し、必要なポリシーをプロビジョニングします。複雑なNAT／ACL／ファイアウォールポリシーの構成や管理は必要ありません。

仮想プライベートネットワーク（VPN）は、ユーザがデータセンタに直接接続されているオフィスを離れ、プライベートアプリケーションにリモートアクセスする際の標準的な方法として利用されてきました。

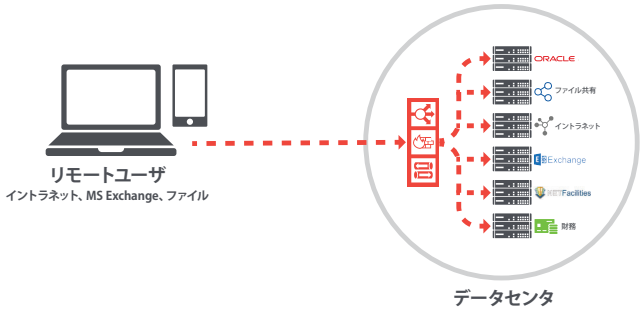
VPNによって、エンタープライズネットワーク境界が「信頼できる」ユーザにまで拡張されて、「オンネット」エクスペリエンスが提供されます。しかしながら、ネットワーク境界が進化し、業務用や個人用のアプリケーションでのクラウド利用の拡大に伴い、VPNのいくつかの特性が問題とされるようになりました。

「オンネット」ユーザエクスペリエンスのリスク

VPNは、アプリケーションではなく、ネットワークへのユーザアクセスを前提に設計されています。そのため、ネットワークに接続されてしまえば、マルウェアの拡散が可能になり、本来であれば制限するべき隣接アプリケーションにユーザがアクセスできてしまう可能性もあります。また、VPNコンセントレータはインバウンド接続要求に対して待機する必要があるため、攻撃の侵入口として悪用される可能性があります。

VPNがネットワークであることによる問題点

企業ネットワークは基幹業務に利用されるようになり、複雑化していますが、VPN利用の拡大によって、さらに複雑化に拍車がかかります。



VPNでのアプリケーションアクセスは実際にはネットワークアクセスである

VPNにも、企業ネットワークの他の部分と同様の高可用性が求められるようになったことも、複雑化の一つの要因です。高可用性を実現する手段として、一般的には、何ヵ所かにデータセンタを設置し、それぞれにロードバランサを用意して冗長構成にします。さらには、グローバルのロードバランサを用意して、特定の地域での災害発生時も可用性を確保し、同時使用ユーザ数を考慮して追加ライセンスを購入しなければならない場合もあります。

高コストのVPN

VPNでは、ネットワークアプライアンスのインストール、展開、メンテナンス、アップグレードが必要なため、コストが増大する可能性があります。また、接続を開始するクライアントソフトウェア、終端装置であるコンセントレータ、ユーザをサポートするヘルプデスクの人員が必要です。これらの初期／運用費用が、セキュリティリスク、ネットワークの複雑さ、およびビジネスの柔軟性の欠如によって発生する可能性のあるコストに加算されます。

クラウド環境におけるVPNの問題点

データセンタ統合が進む今、柔軟に拡大・縮小できるアプリケーションホスティングのニーズを解決する方法として、多くの企業が、クラウドに注目しています。ところが、リモートユーザがそれらの環境にアクセスする方法では、VPNによってユーザがネットワークに固定されるという問題は解消されません。リモートユーザのトラフィックをデータセンタとクラウドアプリケーションのサイト間VPN経由でクラウドベースアプリケーションに渡すために、インターネットを経由することになります。サンフランシスコからブエノスアイレス経由でロンドンに行くような、極めて非効率的な方法です。

このような欠点にもかかわらず、VPNは、リモートアクセスの実現可能な唯一の方法として、10年以上にわたって利用されてきましたが、ようやく、これに代わるソリューションが登場しました。

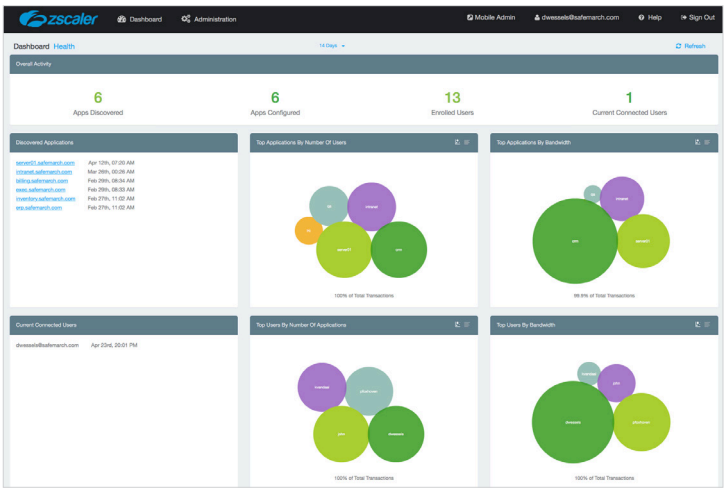
ZSCALER PRIVATE ACCESS

VPN以降初の革新的なセキュアリモートアクセス

Zscalerは、クラウド型セキュリティプラットフォームによるインターネットトラフィック保護のリーダとして、Secure Web Gateway、Cloud Application Visibility & Control、Cloud Sandboxing、DLP（情報漏えい対策）などの活用によって、世界中のあらゆる場所でやり取りされるインターネットトラフィックを保護します。

Zscaler Private Accessは、同じくクラウドベースで柔軟な拡大・縮小が可能なインフラから作成された、内部アプリケーション／アセットへのシームレスな接続を可能にするソリューションです。

Zscaler Private Accessは、IPによるダイレクトネットワーク接続の限界、コスト、複雑さから内部アセット／アプリケーションを切り離すことで、従来型VPNインフラの課題を解決します。

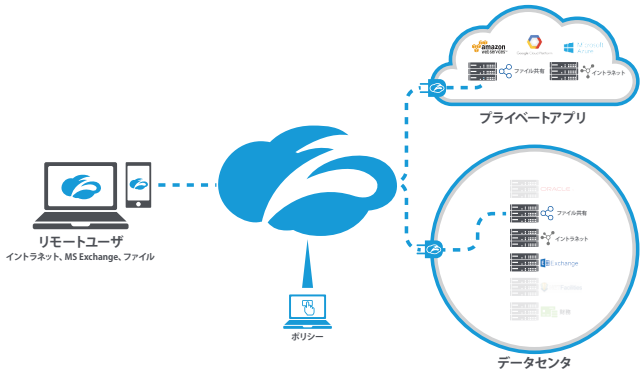


Zscaler App

Zscaler Private Accessを利用することで、クラウド、データセンタ、またはその両方に存在する内部プライベートアプリケーション／アセットへのシームレスな接続が可能になります。ポリシーベースのアクセスであるため、ネットワークの変化に動的に対応し、企業としてのアジリティとユーザエクスペリエンスの向上を可能にします。

Zscaler Private Accessには、VPN終端ハードウェアのプロビジョニングや、グローバルな分散型の冗長構成は必要ありません。データセンタ内の終端アプライアンスを経由することなく、クラウド内のアプリケーションにアクセスできます。Zscaler Private Accessは、ZscalerのCloud Security Platformと同様に1つのサービスとして機能するため、ハードウェアを購入する必要は一切ありません。

すべてのハードウェアとソフトウェアの管理がZscalerに移行されるため、レイテンシが短縮され、スケーラビリティが向上するだけでなく、IT部門による管理の作業と予算が不要になるというメリットもあります。Zscaler Private Accessは、既存の認証基盤と直接連携するため、シングルサインオンによって複雑性がさらに軽減されます。従来のネットワークベースのリモートアクセスソリューションでは数週間から数ヵ月の導入期間が必要ですが、Zscaler Private Accessであれば数時間で導入できます。



ユーザを最高パフォーマンスのアプリに自動ルーティング

セキュリティ強化とシームレスなアクセスの両立

全体コストの削減と複雑性の軽減だけでも大きなメリットですが、セキュリティこそが、Zscaler Private Accessソリューションの中核となる機能となっています。アセット／クライアント間の接続が確立されると、このソリューションを通過するトラフィックが完全に分離された状態が保証されます。Zscaler Private Accessは、プライベートアプリケーションのゼロトラストを前提に構築されているため、トラフィックは、Zscalerからも隔離されています。また、Zscaler Private Accessによってアセットがネットワークから抽象化されるため、物理的な場所に関係なく、シームレスなアクセスが保証され、機密情報が表示されないため、セキュリティが大幅に向上します。アプリケーション／アセットにルーティングしようとする動きはすべてブロックされます。

IPアドレスではなく、アプリケーションによって接続

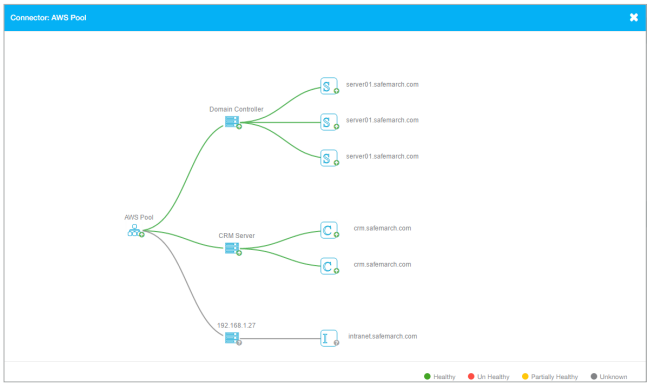
VPNは、アプリケーションではなく、ネットワークへのアクセスを提供するように設計されています。そのため、ネットワークに接続されてしまうとマルウェアの拡散が可能になり、本来であれば制限するべき隣接アプリケーションにユーザがアクセスできてしまう可能性もあります。また、VPNコンセントレータはインバウンド接続要求に対して待機する必要があるため、DDoS（分散型サービス拒否）攻撃などの侵入口として悪用される可能性があります。

VPNと関連機器のコストを削減

Zscalerが、グローバルなクラウドベースのセキュリティプラットフォームの一環として、すべてのハードウェアとソフトウェアを管理するため、ITの作業と予算の両方を削減でき、数時間で導入できます。さらに、Zscaler Private Accessは、Zscalerのクラウドセキュリティプラットフォームへのアクセスに用いられるものと同様のZscaler Appで展開できます。Zscaler Remote Access、Secure Web Gateway、DLP（情報漏えい対策）、Cloud Sandboxing、Cloud Firewallなどのプロビジョニングを単一アプリで実行できるため、「クライアントのスプロール化」が大幅に緩和されます。

アプリケーションの「オンネット」から「ダークネット」への移行と包括的な可視化の両立

Zscaler Private Accessでは、許可されたユーザ以外にアプリケーションが表示されることも、ルーティングされることもありません。また、アプリケーションレイヤで動作するため、かつてない高レベルの可視化も同時に実現します。アセット群の前にConnectorをプロビジョニングすると、実際にそこで実行中のアプリケーションを、ワイルドカード属性を使用して正確に検出できるようになります。お客様によっては、予想の10倍近くのアプリケーションが検出される場合もあります。そして、実行中のアプリケーションを把握できれば、詳細のアクセスルールを簡単に作成できるようになります。

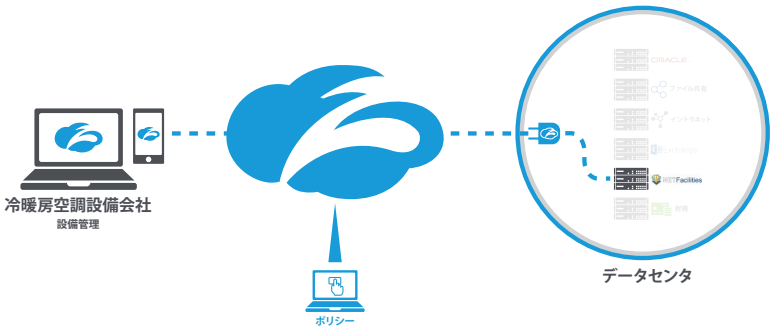


App Discoveryによる容易な展開

外注先やパートナーなどの会社に適切なアクセス権を付与

最近のセキュリティ違反のニュースから分かるように、内部アプリケーションへのアクセスを第三者に許可することには、常に危険が伴いますが、Zscaler Private Accessを用いれば、心配ありません。ネットワーク全体へのアクセスを全員に許可するのではなく、アプリケーション単位でのアクセスの詳細なプロビジョニングが可能です。各自の業務に不可欠なアプリケーションだけにアクセスできるようにし、それ以外へのアクセスをすべて禁止できます。合併や買収の後でも、プライベートIP範囲の重複、複雑なNATルール、あるいは膨大な量のアクセス制御リストに悩むことなく、アプリケーションアクセスをプロビジョニングできます。

Zscaler Cloud Security Platformは長年にわたり、ガートナーやフォレスターを始めとする調査会社によって、エンタープライズWebトラフィックの分野のマーケットリーダとして評価されています。Zscaler Private Accessによって、Zscalerプラットフォームの機能が拡張され、極めて重要なプライベートエンタープライズアプリケーションへのシンプルかつ安全なアクセスが可能になります。ネットワークとアプリケーションがZscaler Private Accessによって切り離されるため、物理的なデータセンタ、クラウドデータセンタ、または複数の拠点のどのような組み合わせであっても、アプリケーションのIPアドレスを意識する必要はありません。



アプリケーションアクセスを関連会社やパートナーにまで拡張

機能	プロフェッショナル	ビジネス	エンタープライズ
ユーザ／アプリケーションの可視 — ユーザごとに、プライベートおよび内部アプリケーションの使用状況を一元的に可視化	✓	✓	✓
プライベートアプリケーションへのセキュアなアクセス — （パブリック／プライベート／ハイブリッドクラウド、またはレガシーデータセンタを問わず）プライベートおよび内部アプリケーションを、インターネットを介さずに安全に利用	✓	✓	✓
アプリケーション単位のマイクロセグメンテーション（最大5つのアプリケーション） — ユーザまたはグループ単位で、アプリケーションごとにアクセスルールを指定	✓	✓	✓
アプリケーション／サーバディスカバリ — ユーザのリクエストにより、ワイルドカードポリシーに基づきアプリケーションおよびサーバのロケーションを表示	✓	✓	✓
アプリケーション専用エンタープライズダークネットおよびDDoSプロテクション — 接続権限を持つユーザのみアプリケーションを表示	✓	✓	✓
ポリシーの定義・管理専用単一コンソール — グローバル展開に関するすべてのポリシーを一元的に定義・管理	✓	✓	✓
パッシブヘルスモニタリング — アクセスがリクエストされるたびにアプリケーションのヘルス状態をモニタリング	✓	✓	✓
Zscaler App — Zscaler Internet AccessおよびZscaler Private Accessサービススイートにアクセスする際に軽量のアプリケーションを利用	✓	✓	✓
アプリケーションを無制限に定義 — ユーザからのリクエストの際に、すべてのアプリケーションにマイクロセグメンテーションを適用		✓	✓
一貫したヘルスモニタリング — アプリケーションのヘルス状態を一貫してモニタリングすることで、ポートの有効性とユーザによるアプリケーションへの接続を常に確保		✓	✓
デバイスのポスチャーエンフォースメント — デバイスのフィンガープリント、証明書、および他のポスチャーをチェック		✓	✓
顧客専用PKI — 顧客ごとに提供される証明書により、完全なプライバシーを確保			✓
二重暗号化 — 顧客専用のPKIを用いてマイクロトンネルを暗号化			✓
リアルタイムのユーザトランザクションビュー — 瞬時にログを取得し、エンドユーザをサポート			✓

CONTACT US

Zscaler, Inc.
110 Rose Orchard Way
San Jose, CA 95134, USA
+1 408.533.0288
+1 866.902.7811

www.zscaler.com

FOLLOW US

facebook.com/zscaler
linkedin.com/groups/zscaler
twitter.com/zscaler
youtube.com/zscaler
blog.zscaler.com