セキュリティーの観点においては、オフィスの内外でノートパソコンから接続しているユーザーによってセキュリティー リスクが高まる可能性があります。特にユーザーが自動的に信頼され、ネットワーク アクセスが許可されている場合はこの点が顕著です。そしてユーザーの観点からすると、どのような場所からでもアクセスしやすい体制が求められています。

IT部門にとって今後検討が必要な3つの要素

各地の政府や自治体は物理的なオフィスの再開に向けて適切な措置を講じていますが、セキュリティーやネットワーク分野の担当者がオフィス再開の前に考慮すべき重要な要素が3つあります。

1 プライベート アプリへのあらゆる場所からのゼロトラスト アクセスを提供すること

多くの企業は、ゼロトラストが重要になるのはプライベート アプリケーションへのリモート アクセスを提供する場合のみだと誤解しています。このような認識を持つ企業は、ユーザーをネットワーク上に配置するVPNやVDIなどのリモート アクセス テクノロジーの代わりとしてゼロトラスト サービスを使用しています。オフィス内で作業する従業員は、ユーザーが既に境界内に存在しているために暗黙的に信頼され、多くの場合ネットワーク リソースへの接続が許可されています。担当部門が追加のセキュリティー対策としてネットワーク セグメンテーションを実装している可能性もありますが、これによってネットワークが非常に複雑化してしまいます。しかし、適切なゼロトラスト サービスを利用していれば、ネットワーク セグメンテーションは必要ありません。このゼロトラスト サービスは、ユーザーがリモートとオフィス内で作業する時に使用でき、オンプレミスでのネットワーク セグメンテーションに伴う複雑さに対処することなく、アプリケーションのレベルでのセグメンテーションを提供するのに利用できます。

2 一貫性を優先することで、実現し得る最高のユーザー エクスペリエンスを提供すること

複数の調査から、企業と従業員の双方がリモート ワークに満足していることが明らかになっています。多くの組織では、中核となる従業員がリモートで作業しているにもかかわらず、生産性が継続的に向上していることが示されていると同時に、多くの場合場所を問わず働ける柔軟性を従業員が好ましく感じています。このため、当社のお客様の中で、従業員がオフィスと自宅の両方で作業できるハイブリッド モデルに傾いている組織は多く見られます。そのため、ネットワークやセキュリティー分野の担当者は、従業員がオフィスを含むあらゆる場所からアプリケーションにアクセスする際に、シームレスで一貫性のあるエクスペリエンスを得られるように対応する必要があります。

3 マルウェアなどに感染したデバイスが企業ネットワークにアクセスするのを防ぐこと

リモート ワークが一般的になったことに伴い、CrowdStrike、Microsoft、Carbon Blackなどのエンドポイント セキュリティー サービスの人気が高まっていることも鍵となっています。当面の対応として、ノートパソコンやスマートフォンで作業をするユーザーは、自宅のパーソナル ネットワークでアプリにアクセスしてきました。これらのデバイスは物理的なオフィスに持ち込まれることがあるため、IT担当者がそれらを企業ネットワークに接続させないようにすることが重要です。代わりに、IT担当部門は、オフィスに戻ってくるすべてのデバイスがマルウェアなどに感染していないことを確認し、全体的な攻撃対象領域を減らし、脅威の影響を最小限に抑える必要があります。したがって、デバイスのポスチャーと健全性を把握するのは、特にハイブリッド ワークの確立に際する重要な要素となります。

オフィス内外での業務にゼロトラストを適用

ゼロトラストは、アイデンティティー ポリシーとビジネス ポリシーの2つの主要な基本要素に基づいています。

IPアドレスを使用する代わりに、アイデンティティーを通してユーザーの身元に関するコンテキストが提供されます。ネットワーク部門やセキュリティー部門によって設定されるビジネスポリシーによって、許可されたユーザーがどのプライベート アプリケーションにアクセスできるかが定められます。Zscaler Zero Trust Exchange™プラットフォームは、これらのポリシーをホストして適用し、許可されている場合は、アプリごと、セッションごとに1対1でアプリとユーザーの接続を仲介します。

ユーザーの場所は常に変化しているため、ネットワークに重点を置く必要はもうありません。ユーザーがオフィスに戻っていくなか、暗黙の信頼を付与するシステムから脱却し、ゼロトラスト ポリシーを実装することの重要性は一層高まっています。ゼロトラスト ネットワーク アクセスを活用することで、セキュリティーやスピード、一貫性と利便性をユーザーに提供し、IT部門が求める柔軟性とスケーラビリティを実現できます。

Zscaler Private Accessにより、オフィス内とリモートの従業員にプライベート アプリへのアクセスを提供

Zscaler Private Access™(ZPA™)は、パブリック クラウドやデータ センターで動作するプライベート アプリケーションへのシームレスなゼロトラスト アクセスを提供する、Zscalerのクラウド サービスです。従来型のアプリケーションだけでなく、Webベースのアプリケーションもサポートが可能です。このサービスは、SAMLベースのIDプロバイダーからの情報を使用し、お客様が定義したビジネスポリシーに基づいて、許可されたユーザーを特定のアプリケーションに接続します。VPNやVDIとは異なり、これはユーザーを企業ネットワークに配置せずに実行されるため、インバウンドのゲートウェイ スタックが不要になります。また、このサービスではアプリケーションがインターネットに露出されないため、リモートアクセスにおいて特に重要な、攻撃者に対するアプリの不可視化も実現できます。

ZPAは、暗号化されたインサイドアウト トンネル(1つはアプリから、もう1つはユーザーから)を使用して、ユーザーとデバイスの場所に基づいて、適切なサービス エッジ ロケーションでリアルタイムに接続を仲介します。これは、ユーザーからアプリケーションへの可能な限り最速なパスを確保し、中央のデータ センター ロケーションへのバックホールの必要性を排除する形式で行われます。サービス エッジは、Zscalerによってパブリックに、またはお客様によってプライベートにホストされ、後者の場合ローカルで実施するためにお客様のオンプレミスの支社またはデータセンターに拡張されます。いずれの場合も、サービス エッジはZscalerによって管理されます。

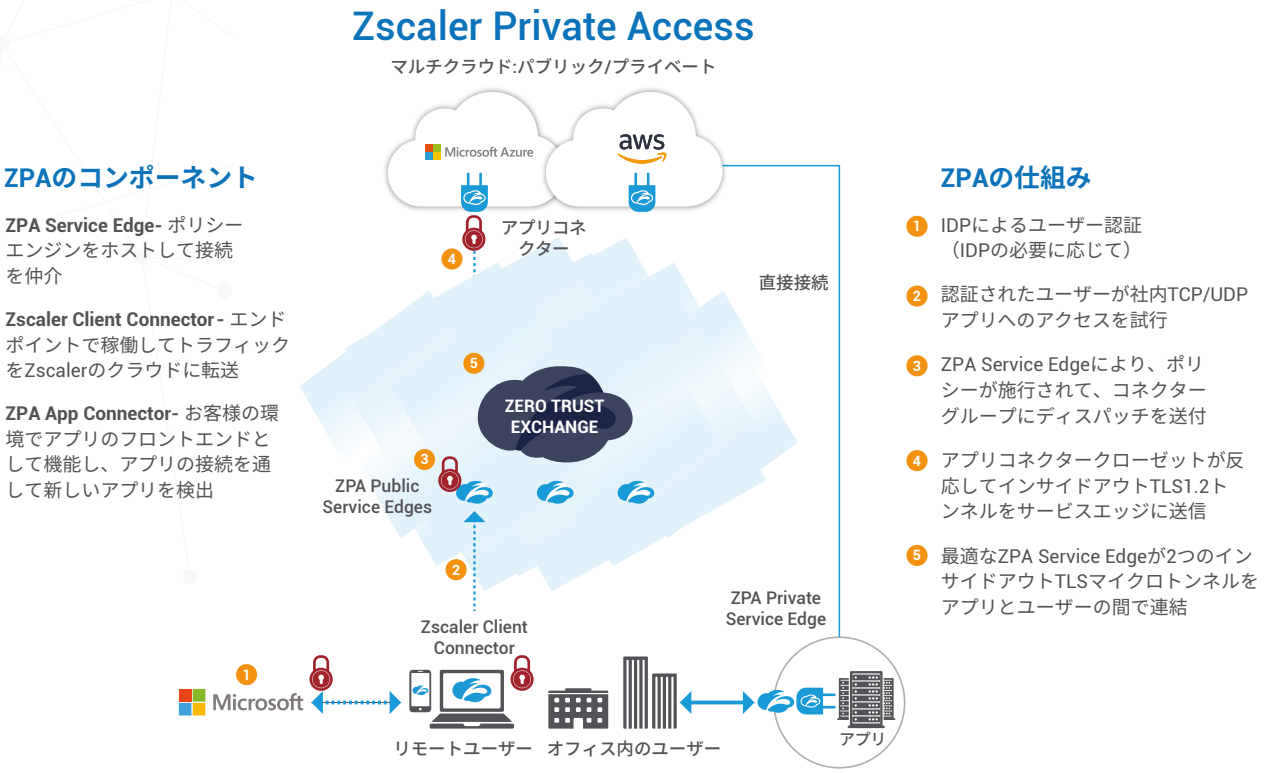
このサービスでは、ユーザーごと、アプリごとに接続されているため、ネットワーク セグメンテーションを必要とせず、代わりにアプリケーション セグメンテーションを提供します。これによりセグメンテーションが簡素化され、IT部門は送信元IPと接続先IPではなく、ユーザー名とホスト名でポリシーを定義することができます。

ZPAは、暗号化されたインサイドアウト トンネル(1つはアプリから、もう1つはユーザーから)を使用して、ユーザーとデバイスの場所に基づいて、適切なサービス エッジ ロケーションでリアルタイムに接続を仲介します。

オンプレミスでホストしながら、ゼロトラスト アーキテクチャーと同じメリットを実現

自らZPAのサービス エッジをホストすることを希望する企業のために、当社はZPA Private Service Edgeを導入しました。ZPA Private Service Edgeは、組織独自の環境でパブリックのZPA Service Edgeの完全な機能を提供する、プライベートのシングル テナント インスタンスです。お客様はZPA Private Service Edgeをオンサイトまたはクラウドサービスでホストし、管理はZscalerが行います。ZPA Private Service Edgeでは、関連するポリシーと設定をクラウドからダウンロードすることで、すべてのZPAポリシーをローカルに適用できます。

ZPA Private Service EdgeとZscalerがホストする従来型のZPAサービスは、組み合わせながら使用することが可能です。ZPAはユーザーと接続先の間の最速のパスを自動的に選択して、レイテンシーを排除します。



ZPA Private Service Edgeの主なメリット

複雑さとコストの低減

ZPA Private Service Edgeを用いることで、内部ファイアウォールや追加のアプライアンスが不要になります。これにより、コストが削減されるだけでなく、ローカル ユーザーにアプリケーション アクセスを提供するために複雑なネットワーク セグメントを構築する必要性もなくなります。

高い可用性

ZPA Private Service Edgeはアクセス ポリシーを数週間キャッシュし、インターネット接続が失われてもユーザーが安全に接続できるようにします。これにより、接続性に関係なくアプリケーション アクセスの可用性を持続できます。

高速なユーザー エクスペリエンス

ZPAは、ローカルのZPAのサービス エッジを優先し、ユーザーがアプリケーションに接続するための最短かつ最速のパスを自動的に決定します。オンプレミスとパブリック クラウドの仲介のデュアル アクセス機能は、ユーザーとアプリケーションの場所に関係なく、ユーザー パフォーマンスを自動的に最適化します。

ZSCALERを活用した、プライベート アプリへのオフィスの内外からのゼロトラスト アクセス

コンプライアンス

銀行や金融サービスなどの業界では、クラウドベースのサービスの利用に関する厳格なガイドラインがあります。ZPA Private Service Edgeは、オンプレミスでのサービスのホストを可能にすることで、こうした規制の準拠をサポートします。

ローカルで実施される一元化されたポリシー

ZPA Private Service Edgeは、ZPAのクラウド サービスに接続することで、最新のビジネス ポリシーを反映させます。これにより、関連するすべてのポリシーと設定が適用されます。インターネットに障害が発生した場合、ZPA Private Service Edgeはすべてのポリシーを14日間キャッシュし、プライベート アプリケーションへのローカルなユーザー アクセスが継続して適用されるようにします。

ZPA Private Service Edgeは、プライベート アプリケーションへの安全なアクセスを可能にするシンプルな方法を提供し、データ センターやクラウドのアプリケーションへのローカル、リモートのどちらのアクセスにおいても同一のユーザー エクスペリエンスを実現します。

ZPAについての詳細については、こちらにお問い合わせください：
sales@zscaler.com

ZPA Private Service Edgeの詳細は**こちら**

デモを申し込む

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、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。

Zscaler, Inc.
120 Holger Way
San Jose, CA 95134
+1 408.533.0288
www.zscaler.jp