ホワイトペーパー

ゼロトラスト・ネットワーク・アクセス（ZTNA）の実現に向けた詳細な計画

このガイドの対象読者

ネットワークアーキテクト、セキュリティエンジニア、CTO、CISO、IT およびセキュリティに関するその他の意思決定者に役立つガイドです。

ゼロトラスト・ネットワーク・アクセス（ZTNA）プロジェクトのスコーピング、設定、展開、実行、管理の責任者は、このガイドを利用することで、考え得るメリットやさまざまなシステムの違いを総合的に確認することができます。このガイドでは次のことについて取り上げます。

- 従来のアプリケーション・アクセス・アプローチの限界とセキュリティ欠陥、および ZTNA が必要である理由
- ZTNA の構成要素と仕組み
- Akamai Enterprise Application Access と Akamai MFA を利用することで、どのように迅速かつ簡単に ZTNA を実現できるか

ビジネス界の変化とサイバー脅威の増大に伴い、企業はサイバー防御を見直しています。多くの企業は、すべての関係者が一元的にアプリケーションにアクセスできるようにする従来のネットワーキングアーキテクチャが原因で脆弱性が生じていることに気付いています。城を堀で囲うように、境界の防御を固めればその内側にいるすべての人の安全が確保されると考える従来のセキュリティアプローチは、現代のモバイル接続とクラウドの環境においては、企業がサイバー攻撃のリスクにさらされる原因となっています。それに対し、先見性のある企業はゼロトラスト・アーキテクチャの概念を取り入れて重要な資産を保護しようとしています。どんなゼロトラスト・プロジェクトにおいても、基本的な原則はネットワークを保護することです。このホワイトペーパーでは、従来のハブ・アンド・スポーク型のネットワークセキュリティが現在ではもはや不十分であること、ZTNA へ移行することで重要な資産をより適切に保護し、包括的なゼロトラスト・アーキテクチャの要として機能する方法について、詳しく説明します。

かつてないペースでのビジネスの変化

企業によるテクノロジーの運用方法や使用方法がかつてないスピードで進化しています。コンピューティングが発展したことにより、オンプレミスのデータセンターでビジネスアプリケーションをホスティングするのではなく、複数のパブリッククラウド、プライベートクラウド、またはハイブリッドなアプローチ（オンプレミスとパブリック／プライベートクラウドの併用）が使用されるようになりました。

また、ビジネスモデルの進化により、企業間でのコラボレーションの増加に拍車がかかり、パートナーとサプライヤーにアプリケーションやリソースにアクセスを提供する必要性が高まりました。

さらに、企業はテレワークやハイブリッドワークを活用し続けており、ユーザーは今やどこからでも管理デバイスと非管理デバイスの両方でビジネスアプリケーションやリソースにアクセスしています。

このような変化に伴い、アプリケーションへのアクセスを管理する従来のアプローチではもはや不十分になっており、企業はアプリケーションをホスティング先やユーザーの所在地を問わずセキュアなアクセスを可能にする新たなアプローチを採用する必要があります。

従来のアプリケーションアクセス

20 年以上もの間、企業は強固なセキュリティ境界を構築するためにファイアウォールに依存し、その境界の内側にいるユーザーを信用してきました。これは、ネットワークを堀のある城のように扱うことに似ています。分厚い壁と厳重に警備された門が城（この場合はネットワーク）を保護する境界を形成して、正しい認証情報を持つユーザーのみがアクセスできます。内側に入れたあと、ユーザーは Microsoft Active Directory などのアイデンティティプロバイダー（IdP）ソリューションを通じて提供される ID に基づいて、特定のアプリケーションにアクセスできる、というわけです。

しかし実際には、フラットなネットワークでは、ユーザーはネットワーク全体への IP アクセスを持っており、他のサーバーやアプリケーションを探索できてしまうのです。たとえば、IdP が正しく設定されていれば、ユーザーは給与支払アプリケーションがホストされているサーバーを見つけることができる可能性があります。ただし、アプリケーションにログインしようとすると、アクセスが拒否されます。

このような自由なラテラルムーブメント（横方向の移動）の問題を解決するために、企業は仮想ローカル・アクセス・ネットワーク（VLAN）を介して、アプリケーションをファイアウォールの背後にある個別のセグメントに分け、個々のユーザーやグループに対して、今では古典的な IP 範囲ベースのルールを適用しました。このプロセスは脆弱であり、ミスも起こりやすくなります。誰かがメンテナンスを行っていて、マシンを新しいラックに移動したり、IP を新しい範囲に割り当て直す必要が生じたりするというシナリオを考えてみてください。ユーザーは前触れなくロックアウトされ、そのためサポートへの電話が殺到することになります。または、ソフトウェアのアップグレード時にアプリケーションのアーキテクチャが変更され、ユーザーはそのワークフローの一環として別のマシンにリダイレクトされます。その際、ファイアウォールのルールが更新されていないため、特定のユーザーやグループはそのマシンにアクセスできない可能性があります。

このアーキテクチャは非常に複雑であり、ダウンタイムをゼロにするためには、どのような変更においてもアプリケーションオーナー、ネットワーク管理者、セキュリティグループの間で綿密に調整を行う必要があります。

そのような調整が失敗した場合に何が起こるかは、ご存知のとおりです。管理者たちはベストプラクティスに従いたいと考えています。しかし、どうしようもない局面では、恐ろしいことに IP ANY／ANY ALLOW ルールをその場しのぎで追加することになり、影響を受けるユーザーは、根本的な問題が診断されて修復されるまで、すべてにアクセスできるようになるのです。しかし多くの場合、後戻りしてその変更を取り消す時間はなく、このようなその場しのぎによって会社のセキュリティ体制が次第に衰退していきます。

VPN による複雑性、パフォーマンス、セキュリティに関する課題の増加

一般的に、リモートユーザーは仮想プライベートネットワーク（VPN）を利用して境界内でホストされているオンプレミスアプリケーションにアクセスし、そこから直接トンネルを通じて会社のネットワークにアクセスします。

ユーザーによるアプリケーションへのアクセスを管理するために、企業は多くの場合、専用のアプリケーション・デリバリー・コントローラーを追加するか、VPN ソリューションに組み込まれているアクセス制御を使用します。その目的は、ユーザーがどこにいても、アプリケーションへのアクセス許可の一貫性を確保することです。境界の内側にいるときに CRM アプリケーションへのアクセスを拒否されるユーザーに対しては、VPN を通じて接続している場合もアクセスを拒否しなければなりません。それが目標ではありますが、この 2 つのユースケース間でアプリケーションのアクセス許可を同期させることは困難であり、その場しのぎの対応が行われると、ユーザーが意図しないアプリケーションへのアクセス権の取得につながる可能性があります。

業務委託先、パートナー、サプライヤーによるアプリケーションへのアクセス

また、企業は多くの場合、VPN を使用して業務委託先、パートナー企業、サプライヤーがリモートでアプリケーションにアクセスできるようにします。たとえば、サプライヤーが外部から財務システムにアクセスして請求書を提出できるようにする場合があります。VPN を通じてサードパーティがアプリケーションにアクセスできるようにすると、企業はエンドツーエンドのセキュリティを確保できなくなり、さらなるセキュリティリスクが発生します。VPN アクセスを行うサードパーティのデバイスが侵害されると、攻撃者がその企業の社内ネットワークにアクセスできるようになります。

VPN とパフォーマンス

パフォーマンスに関しても、同じトレードオフが生じます。最もシンプルな VPN では、すべてのトラフィックがデータセンターのインフラに戻ります。その結果、ヘアピン効果によってインターネットプロパティや SaaS（Software-as-a-Service）へのアクセス速度が極端に低下し、トラフィックが倍近くに増加する可能性があります。

このようなパフォーマンスへの負担を克服するために、管理者は多くの場合、スプリットトンネルを使用し、VPN を通過させる IP 範囲とインターネットに直接エグレスを行う IP 範囲を指定します。この方法は、内部境界が 1 つだけの場合は非常に簡単で効果的です。しかし、複数のデータセンターや仮想プライベート・クラウド・プロバイダーを追加すると、格段に複雑になってきます。管理者は、すべてのデータセンターに VPN アグリゲーターを導入するかどうかや、マルチポイント分割トンネルを効率的に管理する方法を決定する必要があります。

これは、VPN に価値がないということではありません。むしろその逆です。複数のデータセンターインフラがある場合のサイト間アクセスは、VPN がメリットをもたらすケースの 1 つと言えます。しかし、ネットワークレベルのアクセスは、アプリケーションにアクセスするユーザーにとって正しいパラダイムではありません。なぜなら、ネットワークレベルのアクセスは、簡便性と、セキュリティとパフォーマンスとの間で、不自然な妥協を強いるからです。

ネットワークベースのアプリケーションアクセスは攻撃者にとって好都合

ここまでは、全従業員にネットワークレベルのアクセスを許可することに伴うリスクと課題について論じました。しかし、このアプローチによって企業がさらされるリスクは他にもあります。窃取されたユーザー認証情報やセキュリティの脆弱性を悪用するサイバー犯罪者も、ネットワーク全体に自由にアクセスできるようになる可能性があるのです。たとえば、攻撃者が漏えいした従業員の認証情報を使って VPN アクセスを取得した場合、攻撃者は、ネットワーク内を横方向に移動して、価値の高い標的を探し、アクセスし、攻撃することができます。

このアプローチによって破滅的な侵害が可能に

理論的には、これらのアプローチによってフリクションを最小限に抑え、アプリケーションアクセスを安全に管理することは可能です。お客様によっては、既にそれらをいくつか組み合わせて使用しているかもしれません。問題は、それらのアプローチを実行、維持し、その間ずっと適切なセキュリティとパフォーマンスを実現することは極めて困難であり、常に適切には運用できないことです。多くの場合、企業は、従業員がアプリケーションにアクセスできているため、すべてが最適に機能しているはずだと自らを納得させています。その場しのぎの対応の結果、油断に付け込まれて、甚大な侵害やパフォーマンスの低下が発生し、業務が停止したり従業員の生産性が大幅に低下したりすることになります。

ゼロトラストのアプローチによるアプリケーションへのアクセス

境界セキュリティのアプローチにはもともと欠陥があり、それによってアプリケーションへのアクセスの管理に関する固有の課題が生じることを考慮すれば、新しいゼロトラストのサイバーセキュリティモデルはより良い代替手段となります。ゼロトラストは、2010 年に Forrester Research が発案したフレームワークであり、企業が IT インフラ、セキュリティポリシー、ビジネスプロセスを変革するために使用しています。

その背後にある本質は非常にシンプルですが、非常に強力です。それは、信頼とは場所に帰属するものではないということです。ファイアウォールの内側にあるというだけで、そこにあるものを信用すべきではありません。そうではなく、どんなアクションも、発生する場所を問わず、明示的に許可されている場合のみ信用しなければなりません。究極的には、発生すべきアクションのみが発生してよいということです。必要のないアクションに対する暗黙の信頼は、完全に排除しなければなりません。それによってリスクが生じることはあっても、価値が生まれることはないからです。

そのためには強力な認証と認可が必要であり、信頼が確立されるまでシステムはデータを転送してはなりません。さらに、分析、フィルタリング、ロギングを使用して、ふるまいを検証し、侵害の兆候を継続的に監視しなければなりません。

このように考え方を根本的に変えれば、過去 10 年間に発生した膨大な数のセキュリティ侵害に打ち勝つことができます。攻撃者はもはや、境界の弱点を悪用し、城の内側に侵入して機微な情報を窃取したり、アプリケーションを侵害したりすることはできません。アクセスするために渡らなければならない堀はありません。あるのはアプリケーションとユーザーのみであり、アクセスするためには事前に相互認証し、認可を検証する必要があります。

ゼロトラスト・ネットワーク・アクセス

ZTNA はこのような原則の基に構築されたアーキテクチャであり、強力な認証、認可、コンテキストに基づいてアプリケーションやリソースへの安全なアクセスを実現します。ZTNA アーキテクチャは、ネットワーク全体ではなく、ユーザーが仕事をする上で必要なアプリケーションにのみアクセスできるようにします。ZTNA のアプローチを取り入れれば、ユーザーがどこにいるかは重要ではなくなり、境界の内側と外側という概念がなくなります。オンプレミス、パブリッククラウド、プライベートクラウドのどれでアプリケーションがホストされているかは重要ではありません。認証されたユーザーのみが、使用を許可されたアプリケーションにアクセスできるからです。

たとえば、営業部門の従業員は営業職に関わるアプリケーションにのみアクセスでき、人事アプリケーションや財務アプリケーションにはアクセスできません。

Akamai の ZTNA の仕組み

Akamai Enterprise Application Access と Akamai MFA を利用することで、ZTNA インフラに移行することができます。これは、ゼロトラストを実現するための重要かつ不可欠なステップとなりえます。

Enterprise Application Access は、クラウド上のアイデンティティ認識型プロキシ（IAP）であり、脅威インテリジェンス、デバイスポスチャー、ユーザーアイデンティティ情報などのリアルタイムの信号に基づいて決定をきめ細かく行うことができる柔軟な適応型サービスです。Akamai MFA は、アクセスを要求しているユーザーが本人であることを極めて強力な認証によって確認する多要素認証サービスです。

初めに、Enterprise Application Access コネクターという小規模な仮想マシンを実行します。この仮想マシンはファイアウォールの内側にありますが、アプリケーションに接続することができます。また、この仮想マシンは DMZ 内にある必要はなく、むしろあってはなりません。アドレスがプライベート IP 空間上にあるようにし、インターネットから直接到達できないようにする必要があります。つまり、ファイアウォール内に配置する他のアプリケーションとまったく同じように扱う必要があります。

マルチクラウド環境をサポートするために、コネクターはオンプレミス・データ・センター内にも、プライベートクラウドやパブリッククラウドにも展開できます。

Enterprise Application Access コネクターは、Akamai Connected Cloud 上の IAP への暗号化されたアウトバウンド接続を即座に確立します。IAP に接続すると、コネクターは設定をダウンロードし、接続に対応できる状態になります。コネクターと IAP の接続はアウトバウンドであるため、すべてのインバウンドファイアウォール接続を閉じて、アプリケーションを公衆インターネット上ではほぼ見えない状態にすることができます。

IAP は、ユーザーがアプリケーションに接続する前に発生するすべての前処理（認証、認可、デバイスのセキュリティとポスチャーのチェックなど）を実行します。ユーザーがアプリケーションにアクセスしようとすると、DNS CNAME によって Akamai に転送され、IAP に接続されます。エンドユーザーとそのデバイスがすべてのチェックに合格すると、認証、多要素認証、およびシングルサインオンへとルーティングされ、その後、デバイスのアイデンティティ機能が実行されます。

ユーザーとマシンが認可されると、そのエンドユーザーからの接続が Enterprise Application Access コネクターからのアウトバウンド接続と結合されます。ユーザーセッションからのトラフィックは、このつなぎ合わされた IAP を介して送信され、要求されたアプリケーションやサービスに接続されます。その時点で、完全なデータパスが確立され、その後のアクセスはすべて、アイデンティティ、デバイス、およびユーザーコンテキストに基づいて継続的かつ動的に判断されます。

このアクセス方法には、明確で重要な利点があります。それは、パフォーマンスとセキュリティが最も重視されるアクティビティを、134 か国、4,200 か所以上の Akamai の拠点のうち、エンドユーザーに最も近いエッジで実行できるという点です。

さらに、アプリケーションへの機微なイングレス経路はアプリケーションのリバーストンネルを介するため、境界の IP は見えなくなり、ボリューム型攻撃のリスクが軽減されます。

Enterprise Application Access は、複数のディレクトリーやアイデンティティ・サービス・プロバイダーを使用している企業のアイデンティティインフラとも直接統合できるため、既存のアイデンティティインフラやアーキテクチャを変更せずに、ZTNA を迅速に展開できます。

現代的な認証プロトコルをサポートしていない古いアプリケーションがある場合、Enterprise Application Access は IdP ブリッジ機能によって SAML ベースの IdP に認証を提供し、認証トークンを古いアプリケーションがサポートしている認証プロトコルに変換します。

Enterprise Application Access のような IAP ベースのアプローチには、アプリケーションレベルのアクセス権を提供できるという強みがあります。アプリケーションレベルのアクセス方式を使用すれば、パフォーマンスとセキュリティは複雑さの問題と切り離されます。

相互にローカルなアプリケーション（たとえば、同じデータセンターまたは同じ仮想プライベートクラウドにホストされているものなど）をすべて、1 つのプライベートネットワーク IP 空間または restricted VLAN に割り当て、そのマイクロ境界内にアクセスプロキシを配置します。それで完了です。

アプリケーションオーナーはアクセスプロキシに独自のセキュリティポリシー（誰が何にどのような目的でアクセスできるかに関するポリシー）を設定できます。そしてさらに有利なのは、ユーザーがどこにいてもかまわないという点です。オンプレミスとオフプレミスの区別はありません。なぜなら、エンドユーザーを含めて、ネットワーク境界というものが存在しないからです。喫茶店で仕事をしている従業員も、オフィスで仕事をしている従業員も同じです。重要なのは、そのユーザーが認証されているかどうか、そしてマシンが安全であるかどうかだけです。

アプリケーションレベルのアクセス方式を使用すると、展開や使用が容易なうえに、クラス最高レベルのパフォーマンスを実現できます。アプリケーションがどこでホストされていても、またユーザーがどこにいても、ユーザーはインターネットを使用して直接アプリケーションにアクセスできます。アグリゲーターや経路内にない中間物を介することなく、インターネットで宛先までパケットをルーティングできるのです。

実際、アプリケーションレベルのアクセス方式では、内部ネットワークがシンプルなゲスト Wi-Fi と一体化していることも少なくありません。ゼロトラストの本当の効果を引き出すためには、社内ユーザーを外部ユーザーと分けて特別扱いしてはならないということを覚えておいてください。いかなるユーザーもデフォルトで信用してはなりません。

ZTNA の理想の最終形

オンプレミスでもオフプレミスでも、すべてのユーザーは、アプリケーションがどこでホストされているかを問わず、ID を認識するアクセスプロキシを経由してから全てのアプリケーションにアクセスする必要があります。そして、これらのプロキシは標準認証だけでなく、（Akamai MFA のような）フィッシング対抗の多要素認証も使用する必要があります。また、特定のアプリケーションへのアクセスを許可するデバイス基準を取得する堅牢なデバイスポスチャー機能も必要です。

Akamai は、ZTNA は認証と認可で終わるものではないと考えています。ゼロトラストの原則に対応するためには、最初の認証および認可段階でチェックするすべてのパラメーターを、アクティベートセッションの間、監視を続ける必要があります。変化が検知された場合は、それがどんな変化であろうと、アクション（ユーザーの再認証、アプリケーションへのアクセスの無効化や制限など）をトリガーしなければなりません。

アクセスプロキシに追加すべき重要なセキュリティシステムの 1 つとして、WAAP（Web アプリケーションと API の保護）が挙げられます。これは、故意かそうでないかを問わず、エンドユーザーが内部アプリケーションに対してアプリケーションレベルの攻撃を行えないようにするシステムです。他にも、人間／ボットの検知などの先進的なシステムを非 API サイトで活用し、適正なエンドポイントの背後でマルウェアによるなりすましが発生しないようにすることができます。Akamai は IAP で、WAAP、ボット検知、ふるまい分析、キャッシングを追加することができます。そうすることで、クラス最高レベルのパフォーマンスを実現し、潜在的な攻撃者を物理的な場所、アプリケーション、データからできる限り遠ざけることができます。

アプリケーションをオンラインにして、アクセスプロキシ経由でアクセスできるようにすると、分散型サービス妨害（DDoS）防御の重要性が増します。マイクロ境界とアクセスプロキシに対する攻撃を吸収できるプロバイダーと協力すれば、負荷が集中しても運用を継続できるようになります。

最後にもう 1 つ重要なことがあります。アプリケーションがクラス最高レベルのパフォーマンスを発揮できるようにするとともに、アクセス方式の変化をユーザーに受け入れてもらうだけでなく、支持してもらうためには、アクセスプロキシが接続されているネットワーク自体がパフォーマンスの面でメリットを提供できなければなりません。具体的には、コンテンツ・デリバリー・ネットワークとインターネット・ルーティング・オーバーレイを活用すべきです。これらを組み入れることで、アクセスを可能にするだけでなく、従来方式よりもパフォーマンスを強化できます。

脅威からの保護

Akamai Enterprise Application Access のようなソリューションは、お客様のアプリケーションを攻撃者から保護します。しかし、デバイスがマルウェアに感染したり、フィッシングのリンクやランディングページを通じて認証情報が盗まれたりすることで、ユーザーが意図せずに攻撃者になってしまうこともあります。これを防ぐにはどうすればよいのでしょうか。ここで重要になるのが Web トラフィックに対する防御と検知です。

1 つの方法として、Akamai Secure Internet Access などのクラウドベースの DNS ファイアウォールソリューションを展開することが挙げられます。この製品は、ユーザーが実行するあらゆる DNS リクエストを検査し、リアルタイムの脅威インテリジェンスを適用することにより、無害なリクエストは通常どおり解決され、悪性ドメインへのリクエストはプロアクティブにブロックされるようにします。これにより、従業員のデバイスがマルウェアやランサムウェアによって侵害されたり、フィッシング攻撃の被害に遭うリスクが減少します。

まとめ

従来のハブ・アンド・スポーク型ネットワーキングアーキテクチャと「堀と城」方式のセキュリティ境界を使用していたのでは、現在のようなクラウドとモバイルの世界に効果的にパフォーマンスとセキュリティを提供することはできません。これはすべての企業が着手しなければならない問題であり、そうでなければ企業は脆弱なままになってしまいます。今や、企業のセキュリティ侵害の原因の第 1 位は、安全なエンタープライズ・セキュリティ・アーキテクチャに移行していないことであり、侵害の件数は増加の一途をたどっています。簡単に言うと、境界の内側は安全ではないということです。なぜなら、境界自体がもはや存在しないからです。

次のステップ

ゼロトラスト・ネットワーク・アクセス（ZTNA）アーキテクチャへの移行に着手するためにはどうすればよいのでしょうか。

Akamai のクラウド・セキュリティ・サービスを組み合わせることで、包括的な ZTNA アーキテクチャを構築できます。これにより、マルチクラウドの世界で安全なアプリケーションアクセスを実現できるだけでなく、クラウドを活用して社内ネットワークの必要性をほぼ完全に排除することもできます。

Akamai の高度な分散 IAP ソリューション、フィッシング対抗の多要素認証、Akamai Connected Cloud の力を活用すれば、信じられないほど簡単な方法で、最終的に境界のない世界へと移行できます。アプリケーションを段階的に移行し、移行のリスクプロファイルをゼロに近づけ、長年にわたって実績を積み重ねてきた Akamai のパフォーマンスソリューションやセキュリティソリューションを活用できます。

お客様がゼロトラストへの移行を安心して進めていくことができるように、Akamai は移行の各段階でお客様をサポートします。アプリケーションとデータへのアクセスを提供するだけでなく、それを管理しやすい方法で実現し、高水準のセキュリティとパフォーマンスを維持できるアーキテクチャへとネットワークを移行するためのお手伝いをいたします。

Akamai ゼロトラスト・ポートフォリオでビジネスニーズに対応する方法をご確認ください。