境界防御型ファイアウォールの5大リスク＋それらを克服する1つの方法

ファイアウォールは、これまでの長い間企業のネットワークアーキテクチャに不可欠な要素でした。しかし、デジタルビジネスモデルへと移行するに伴い、セキュリティの定番と考えられ強固だったファイアウォールが、セキュリティリスクへと変わろうとしています。その理由は以下の通りです。

ファイアウォールとVPNを活用する従来の境界ベースのセキュリティアーキテクチャでは、セキュリティは境界または信頼ゾーンに限定されていました。境界または信頼ゾーン内のユーザまたはアプリケーションは良い性質を持つと見なされ、外部のユーザーまたはアプリケーションは悪い性質を持つと見なされます。このような仕組みは、ほとんどのユーザーとアプリケーションが境界の内側にある場合にはうまく機能していました。境界の外側にいるユーザーは、境界を自身の側まで拡張してネットワークに参加する必要があり、これは、信頼ゾーンに含まれる例外として扱われました。

ファイアウォールが導入されて以来、ビジネスは大きく変化しました。今日では、企業に勤める社員は、インターネット接続と電源さえあれば、ホームオフィスでも、共有ワークスペースでも、ブランチオフィスでも、どこからでも仕事ができるようになりました。分散したユーザやアプリケーションという例外が当たり前になった現在、リモートユーザごとに境界を拡張することは、もはや有効な方法ではありません。アプリケーションやユーザがどこにでも存在するようになった今、信頼ゾーンという概念はもはや意味を持たなくなり、ゼロトラストモデルに切り替える必要がでてきました。真のゼロトラストはファイアウォールやVPNでは実現できず、それでも実現しようとするといくつかのリスクが生じます。

このホワイトペーパーでは、クラウドやモバイルの世界で従来型のファイアウォールがもたらす5つの主なリスクと、最新のゼロトラストアプローチを用いてそれらの過去の手法を置き換える方法について詳しく説明します。

リスク#1

広範な攻撃対象領域

攻撃対象領域とは、攻撃者が脆弱性を発見し、そこへ入り込み、悪用してシステムにアクセスし、貴重なデータを盗み出すことを可能にさせうる、IPアドレスなどの公開されているあらゆるポイントの総称です。端的に言えば攻撃対象領域が小さければ小さいほど、攻撃者がアクセスしにくくなります。しかし、クラウドでのアプリケーションの配布やモバイルワーカーが増えたことで、攻撃対象領域が飛躍的に拡大し、組織はかつてないほどに脆弱な状態になっています。境界ベースの物理ファイアウォールや仮想ファイアウォールを使うと、この問題を解決できないばかりでなく、組織の攻撃対象領域を拡大し、サイバー犯罪者がネットワークやクラウドインスタンスへの足がかりを得ることを可能にし、事態を悪化させることになります。

これはどのような仕組みになっているのでしょうか。ファイアウォールは、サーバやアプリケーションを社員やパートナーが見つけられるように、それらのIPアドレスをインターネットに公開しますが、裏を返すとそれらが攻撃者にも発見される可能性につながります。インターネットに接続されたすべてのファイアウォールは、データセンタ、クラウド、ブランチオフィスのいずれにあっても、検出され、攻撃され、悪用される可能性があるのです。仮想ファイアウォールも物理ファイアウォールと同様に、IPをインターネットに公開します。多くの場合、その数は物理ファイアウォールよりはるかに多いため、リスクがさらに高まります。

ゼロトラストで攻撃対象領域をなくす方法

ネットワーク、アプリケーション、そして最も重要なデータを保護するための秘訣は、攻撃対象領域をうまく排除することです。真のゼロトラスト機能は、アプリケーションを潜在的な攻撃者から見えないルーティング不可能なエンティティにすることで、インターネット上でリソースを発見できないようにします。真のゼロトラストプラットフォームは、ユーザとアプリケーションの間に配置されるため、すべての通信がプラットフォームを経由し、プラットフォームの許可なしではアプリケーションには何も到達しません。

これらに対して、これからご紹介アプローチは、従来のファイアウォールとは根本的に異なります。従来のアウトサイドインのアプローチでは、アドレスを公開する必要があったのに対し、このアプローチではインサイドアウトの接続のみが許可されることによります。アプリケーションを攻撃者から見えないようにし、許可されたユーザーのみがアクセスできるようにすることで、攻撃対象領域が実質的に排除され、インターネット、SaaS、パブリックまたはプライベートクラウドのアプリケーションへのアクセスが常に安全に保護されます。

攻撃対象領域の検出

攻撃対象領域を手動で見つけるのは困難ですが、インターネット攻撃対象領域分析などのサービスにより、攻撃対象領域全体を可視化し、現在インターネット上で見えるサーバ、名前空間、脆弱性、クラウドインスタンスを明確にできます。この分析では、公開されているソースを照会し、危険にさらされている領域を明らかにします。このようにして、組織は攻撃対象領域を評価し、分析し、ゼロトラストによって排除できます。

リスク#2

アプリケーションパフォーマンスの制限

ユーザは、プライベートで利用するクラウドアプリケーションに対し、一定水準のレスポンスとアップタイムを求めるようになりました。しかし、社員が会社のネットワークアクセスを使用して自社のアプリケーションにアクセスすれば、クラウドアプリケーションには高速で直接アクセスできなくなるため、ユーザエクスペリエンスが大幅に低下する事態が多発します。実際、アプリケーションのパフォーマンスが低下すると、ユーザは生産性を落とし、他との効率的なコラボレーションできなくなります。このため、多くのユーザはセキュリティ管理を回避しがちになります。特に管理外のデバイス、またはセキュリティ保護されていないWi-Fiやホームネットワークを使用している場合は、リスクが高くなります。また、エンドユーザのパフォーマンスの問題は、SaaSやクラウドアプリケーションの可用性、デバイスの容量、ネットワークパスの停止、ネットワークの混雑など、オペレーターが容易に切り分けて診断できない原因として発生します。

上記の問題はなぜ発生するのでしょうか。「ハブアンドスポーク」ネットワークアーキテクチャでは、リモートオフィスやブランチオフィスは、MPLSを使用したファイアウォール経由で中央オフィス（データセンター）に接続し、リモートユーザーはVPNで接続する必要があります。私たちのアーキテクチャでは、すべての拠点に広がるフラットなネットワークが構築され、すべてのネットワークトラフィックが中央のセキュリティスタックに流れる仕組みになります。リモートユーザーからデータセンターを経由してクラウドに送信されたトラフィックがユーザに戻り、同じパスを逆方向にたどると、遅延が大幅に増加し、ユーザエクスペリエンスを損ねエしまいます。クラウド上の仮想ファイアウォールも、アプリケーションサーバとインラインで接続されていないため、物理データセンターと同じようにトラフィックをリダイレクトしなければならず、その意味で同じ運命をたどることになります。

クラウドアプリケーションは、パフォーマンスを最大化するために、できるだけ少ないホップ数で直接アクセスできるように設計されています。そのため、多くのSaaSアプリケーションベンダー（Microsoft 365など）は、全面的にサポートを受けるにはパス上にファイアウォールを置かないようにと明言しています。

ゼロトラストでパフォーマンスの問題を解決する方法

ゼロトラストアーキテクチャは、従来のハブアンドスポークネットワークやキャッスルアンドモート（城を掘で囲む型）セキュリティから脱却します。アプリケーションとの直接接続を実現し、リスクを軽減しながら、より良いユーザエクスペリエンスを提供します。

効果的なゼロトラストプラットフォームは、エッジでインラインにポリシーを適用するため、余分なホップは不要で、さらに、アプリケーション企業との直接ピアリングにより、可用性とキャパシティに基づいた直接接続が可能になります。ゼロトラストプラットフォームはデータパスで動作するので、すべての接続を監視し、パフォーマンスの問題を自動的に特定して修正することもできます。この機能は、Microsoft TeamsやZoomなどのUCaaS（Unified Communications as a Service）アプリケーションなどの低遅延のアプリケーションにとって不可欠です。デジタルエクスペリエンス監視（DEM）機能により、これらのアプリケーションを監視して問題を迅速に修正することで、組織はユーザが気付く前に問題を特定して解決できるため、社員のコラボレーションと生産性が向上します。

ユーザエクスペリエンスの測定

監視ツールを使用して測定できます。このツールは、組織内のユーザエクスペリエンスの問題を理解、診断、改善するためのデジタルエクスペリエンスに関するインサイトを提供します。スコアは、機械学習を使用してパフォーマンスの異常を特定し、実用的なアラートを受け取るのに役立ちます。

リスク#3

運用の複雑化と高コスト

ゼロトラストを実現するために従来のファイアウォール、MPLS、VPNS、または仮想アプライアンスを活用することは、現実的とは言えません。境界ファイアウォールを管理および導入し、すべてのユーザー、すべてのアプリケーション、すべてのデバイス、すべての場所に一貫したセキュリティを提供する方法は、運用上あまりにも複雑でコストがかかりすぎるからです。境界ポリシーの展開、アップデート、パッチを管理するために同じスケールで人員を追加することは現実的ではありません。ハードウェアと仮想ファイアウォールを、最悪の事態に備えて購入し、導入する必要性が生じます。また、単一のセキュリティスタックにトラフィックをバックホールすると、不要な帯域幅とセキュリティ容量を利用することになります。

キャパシティプランニングでは、CIOとCISOが将来を正確に予測し、ハードウェアの要件と、すべてのトラフィックをMPLSでデータセンタに送信して検査する際の帯域幅消費コストを計画する必要があります。ネットワークのニーズを過小評価するとパフォーマンスが低下し、逆に過大評価すると、コストが必要以上に高くなり、機器がアイドル状態になってしまいます。言うまでもなく、すべての場所にまったく同等のアプライアンススタックを導入するのは現実的ではなく、その結果、インフラ全体にさまざまな製品が分散配置されることになります。さらにもう1つの課題として、これだけ多数あるデバイスのログを収集管理しなければならなくなるため、運用者は重要なログを見落としがちになり、潜在的なセキュリティリスクにつながる可能性があります。ファイアウォールのハードウェア、アップグレード、デプロイメントの管理は困難であると、75%もの運用担当者が認めています。[2]

これは課題のほんの一部に過ぎません。このような断片化されたアプローチでは、セキュリティ担当者は別々のサブスクリプションと管理プラットフォームを使用して、異なるポリシーを実装し、ネットワークセグメンテーションを使用して異なるゾーンを管理する必要があります。さらに、ユーザ別、アプリケーション別、場所別の可視性をまとめる作業も必要です。社員は、一致しないファイアウォールやセキュリティアプライアンスのコレクション全体にわたって、パッチ、セキュリティ更新、ハードウェアのリフレッシュを実施し、ポリシーを管理することにフルタイムで作業することを求められます。その結果、資金調達や生産性が低下し、維持できなくなります。

ゼロトラストで複雑化を回避する方法

統合されたゼロトラストソリューションは、管理と維持が困難な複数のハードウェアベースのソリューションやポイント製品のクラウドソリューションとは異なり、単一のプラットフォームですべてのSaaS、インターネット、プライベートアプリケーションを保護します。ゼロトラストは、高速で安全なダイレクトトゥクラウドアクセス、安全なクラウド間接続により、複雑なルーティング、スイッチング、ネットワークセグメンテーションなどを必要とするコストの高いMPLSネットワークを不要にします。基本的に、インスペクションのためにデータセンタにトラフィックをバックホールする必要がなくなります。単一の管理コンソールを備えた統合ゼロトラストプラットフォームは、従来の境界セキュリティよりもはるかに迅速に構成が可能で、管理が容易であり、ポリシーが簡素化され、セキュリティが強化されています。

クラウドベースのゼロトラストソリューションは、ユーザーとアプリケーションが存在する場所、つまりクラウド上にセキュリティコントロールを配置します。ゼロトラストは、すべてのユーザー、クラウド、ワークロードを可視化できるため、運用とトラブルシューティング作業を簡素化します。クラウドへの移行により、ファイアウォールなどのセキュリティハードウェアの購入、管理、保守、監視など、ITチームの負担が軽減され、他のプロジェクトに集中するための時間を捻出できます。さらに重要なのは、クラウドベースのゼロトラストソリューションでは、ユーザーやアプリケーションの数が増えても、すばやく簡単に拡張できる点です。

コスト意識

2021 VPNリスクレポートの調査では、セキュリティアプライアンスやインフラの高コストが、企業がリモートアクセスソリューションで直面する2番目に大きな課題であると結論づけています。Zero Trust Exchangeを通じてゼロトラストを採用した組織は、生産性の向上、インシデントの減少、アプライアンスの削減により、平均で139%のROIと、410万ドルの利益を達成しています。[3]

リスク#4

脅威の水平方向への移動

攻撃者は、フィッシング攻撃やマルウェア感染など、さまざまな手段で組織のネットワークに侵入します。攻撃者の目的は、ネットワークに侵入した後、機密データへのアクセスを求めて組織内を水平方向に移動し、データを持ち出したり、身代金目的で暗号化したり、その他の混乱を引き起こしたりすることです。攻撃者は水平方向に移動することで、最初に感染したマシンで発見されたとしても、検知を回避し、アクセスを維持できてしまいます。また、滞留時間が長いため、データの漏洩が発生するのは、最初の侵入から数週間後、あるいは数か月後になる可能性があります。

組織は、悪意のある攻撃からデータを保護するために、「キャッスルアンドモート（城を掘で囲む型）」セキュリティアプローチ（「境界セキュリティ」とも呼ばれる）に依存してきました。石垣、堀、門で守られた中世の城のように、境界セキュリティは、ファイアウォールや他のツールでネットワークの境界を強化することに多額の投資を行います。境界セキュリティは、組織のネットワークに出入りするデータパケットとユーザの身元を確認することによって、ネットワークの入口と出口を警備し、強化された境界内部のアクティビティは比較的安全であると想定しています。

従来のセキュリティアーキテクチャでは、善悪にかかわらず、ユーザーがいったん「セキュリティ保護された」ネットワークに侵入すると信頼されたユーザーとなり、本来はそうでなくても、すべてのアプリケーションに水平方向からアクセスできるようになってしまうため、こうした巧妙な攻撃を阻止することはできません。従来の境界ベースのアーキテクチャで末端間の水平方向の移動を抑えるには、ネットワークのセグメント化（内部境界化）が必要ですが、これは根本的な問題を適切に解決せずに、より多くのポリシーとファイアウォールを導入し管理する必要があるため、運用上、非常に難しい事態となります。

ゼロトラストで水平方向の移動を阻止する方法

ゼロトラストは、ユーザとワークロードを企業ネットワークにではなくアプリケーションに直接接続するため、水平方向への移動を防止します。つまり、複雑なネットワークセグメンテーションがなくても、脅威が水平方向に伝播して他のデバイスやアプリケーションに感染することができなくなります。これは、アプリケーションにアクセスするユーザだけに適用されるのではなく、IoTマシンから互いに通信するアプリケーションに至るまで、組織内のあらゆる接続に適用できます。そのようなアプリケーション間では、クラウドまたはデータセンタなどに存在するアプリケーションが、別のアプリケーションに、その存在場所を問わず安全に接続できます。このような安全な1対1の接続のおかげで、水平方向への移動のリスクがなくなります。

ゼロトラストモデルは、全てのアクセスは信頼できないという前提仮定からスタートし、アイデンティティとコンテキストに基づいてのみ信頼を確立します。このアプローチでは、接続するエンティティおよびその接続のコンテキストに関する知識に基づいて接続を許可するため、アクセスは常に必要なものだけに制限されます。これは自動的に実施され、そのようなエンティティやその接続の条件が変化すると動的に変化するため、セキュリティチームやITチームにかかる大きな負担を軽減できます。

最後に指摘したいのは、ゼロトラストは、条件付きアクセスによるきめ細かい制御を提供するという点です。管理者は、トラフィックが企業ネットワークなどの信頼できる場所から発信され、ユーザが多要素認証にパスした場合にのみ、ユーザが特定のアプリケーションにアクセスできるようにポリシーを設定できます。また、管理者は、特定の場所や地域、さらには信頼されていないデバイスからのユーザトラフィックをブロックしたり、要求されたデータがユーザの特定のアクセス権限を越えている場合にブロックしたりできます。すべての接続はコンテキストに基づいて許可され、コンテキストの変化に応じて信頼度が再評価されます。

新しいセグメンテーション

従来の仮想ファイアウォールを使用したネットワークのセグメンテーションは複雑でコストや運用時間がかかり、こうした欠点はセキュリティ上のメリットを上回ってしまいます。これに対して**ワークロードセグメンテーション**は、アプリケーションのワークロードをセグメント化する新たな方法です。ネットワークに変更を加えることなく、ワークロードのセグメンテーションによりリスクを明らかにし、アイデンティティベースの保護をワークロードに適用できるため、ワンクリックでセキュリティを強化できます。アイデンティティベースのワークロードセグメンテーションテクノロジーは、環境の変化に自動的に適応するポリシーにより、間隙のない保護を提供します。

リスク#5

データ損失

データは、特に戦略、財務、セキュリティ上の理由から、組織にとって極めて重要です。場合によっては国家の安全保障にとって重要になることもあります。ネットワークセキュリティの境界が設定されていても、認識不足、ユーザの意図しない操作、システムの不具合、巧妙化する悪意のある行為などによって、データ漏洩が発生する可能性があります。その結果、罰金、顧客喪失、法的措置、規制違反、ブランドの毀損など、さまざまな問題が発生する可能性があります。ここでは、さまざまな種類のデータについて、どのようなリスクにさらされる可能性があるのか見ていきましょう。

- **移動中のデータ:** アプリケーションが主にWeb経由でアクセスされるようになった現在、インターネット経由で転送されるデータが、移動中のデータの大部分を占めるようになりました。このことは、SaaSアプリケーション、データセンター内のアプリケーション、パブリッククラウド内のアプリケーションに当てはまります。ユーザーがインターネットにアクセスし、機密情報が流出する可能性のある危険な宛先にアクセスすることは、企業のデータに対する脅威となります。従来のファイアウォールでは、ネットワーク外のユーザを追跡したり、移動中の重要なウェブトラフィックを保護したりすることはできません。エンドポイントに残るデータとアプリケーションの数が減少しているため、移動中のデータソリューションを使用して、エンドポイント、クラウドアプリケーション、ストレージ間を流れるデータを保護することがより重要になっています。
- **保存データ:** 保存データの大部分を占めるのは、データセンター、SaaSアプリケーション、パブリッククラウドに存在するデータです。特に、SaaSアプリケーションに保存されているデータをセキュリティで保護することは、セキュリティにとって非常に重要です。たとえファイアウォールで保護されていても、Microsoft OneDriveなどのアプリケーションでは、わずか数クリックだで不正なユーザーとデータを共有することができてしまうからです。さらに、クラウドへの侵入は、危険な設定ミスやアクセス権限によって引き起こされる可能性があります。SaaSやIaaSは非常に動的で、セキュリティを専門としない個人が設定することが多いため、このような間隙がしばしば見過ごされ、悪用されることがよくあります。

セキュリティテクノロジの最終的な目標は機密データを保護することですが、ファイアウォールは移動中または保存されているデータを効率的に識別し、制御することができないため、組織のデータを危険にさらしています。最も重要なのは、暗号化されたトラフィック（全トラフィックの90%以上[1]）を効率的にインスペクションできないため、SSL/TLSで暗号化されたトラフィックが検査されずに通過してしまうということです。

ゼロトラストでデータ損失を回避する方法

真のゼロトラストプラットフォームは、暗号化されたトラフィックも含め、ネットワーク上とネットワーク外のすべてのトラフィックを検査することができます。可視化とインスペクションの間隙を埋めることで、効果的なデータ損失防止（DLP）とサイバー脅威の防御を実現します。すべてのデータを復号化し、データの健全性を判断した上で、ユーザー、ジオロケーション、IPアドレス、デバイスポスチャ、時間帯などのコンテキストを使用して接続を承認することができます。ゼロトラストソリューションのDLPポリシーは、移動中のデータを保護し、どこにいるユーザーも高速で一貫したセキュリティを獲得することができます。

インラインのゼロトラストソリューションは、シャドーITの完全な検出とコントロールを実現します。ブラウザの分離により、Webベースの脅威とデータを保護し、パフォーマンス上の問題を生じることなく、アンマネージドデバイスにアクセスできます。ブラウザの分離は、コンテナ化された環境で分離されたセッションからピクセルとしてデータをストリーミングすることで機能し、BYODを可能にすると同時に、ダウンロード、コピー、貼り付け、印刷によるデータ損失を防止できます。アウトオブバンドDLPと高度な脅威保護（ATP）により、クラウド内に存在する危険なファイル共有やマルウェアを修復できます。また、クラウドのデータを保護するために、致命的な設定ミス、コンプライアンス違反、アクセス権限、エンタイトルメントを修正することも可能です。

つまり、ゼロトラストは、インターネット、SaaS、パブリッククラウドのアプリケーション全体で、ユーザのデバイスに関係なく、暗号化されたトラフィックを含む、保存中のデータと移動中のデータに対して一貫した統合セキュリティを提供します。

Webブラウザの脆弱性

インターネット上の暗号化されたWebトラフィックの割合は、2014年の50%から今日では驚異的な95%まで着実に増加しています[1]。それでも、Gartnerの調査によると、攻撃の98%はパブリックインターネット上で実行され、そのうちの80%がブラウザを通じてエンドユーザーをターゲットにしていることから、ウェブブラウザが攻撃者の最大の標的となっています。Cloud Browser Isolationのようなブラウザ分離ツールは、これらの脆弱性を緩和するのに役立ちます。特に、クライアント側にソフトウェアをインストールせずに導入できるため、企業のITリソースにアクセスするアンマネージドデバイスに適しています。

ゼットスケーラーで真のゼロトラストを実現

Zscalerは、世界中にある150のデータセンターで稼働するクラウドネイティブなプラットフォーム Zscaler Zero Trust Exchangeを使用してゼロトラストを実現します。同プラットフォームは、世界最大のセキュリティクラウドを活用して高速かつ安全な接続を提供し、これにより社員がインターネットを企業ネットワークとして使用して、どこからでも、どんなデバイスからでも安全に仕事でいるようになります。Zero Trust Exchangeは、従来のファイアウォールやVPNとは異なり、最小特権アクセスの原則と、本質的にユーザーやアプリケーションは信頼できないという考えに基づいています。その代わりに、ユーザーの位置情報、デバイスのセキュリティ状態、アクセスするアプリケーション、やりとりするコンテンツなど、ユーザーのアイデンティティとコンテキストに基づいて接続が承認されます。

これはどのような仕組みなのでしょうか。Zero Trust Exchangeは、まず接続を終了させ、暗号化トラフィック、詳細データ、脅威分析などの詳細なコンテンツのインスペクションを実施します。その後、ユーザ、デバイス、要求されたアプリケーション、コンテンツの種類などのコンテキストに基づき、IDとデバイスを特定し、ビジネスポリシーを使用してアクセス権を検証します。ビジネスポリシーが検証され、実施されると、Zero Trust Exchangeは目的のリソース間の接続を仲介します。ユーザとデバイスはアプリケーションに直接接続され、企業ネットワークには接続されません。

詳細情報

ゼロトラストの詳細とゼットスケーラーのサポート内容については、**Zero Trust Exchange**のページをご覧ください。

出典

[1] *Google Transparency Report https://transparencyreport.google.com/https/overview?hl=en*
[2] *Zscaler Networks Security Survey 2020*
[3] *ESG Economic Validation Study 2021*

Zscalerについて

Zscalerは、モバイル対応、クラウドファーストの環境へのセキュアトランスフォーメーションを可能にします。Zscalerは、デバイス、場所、あるいはネットワークの区別なく、ユーザをアプリケーションやクラウドサービスに接続し、それと同時に、包括的セキュリティと高速のユーザエクスペリエンスを提供します。高価で複雑なゲートウェイアプライアンスは、もう必要ありません。

zscaler™