Akamai

ホワイトペーパー

最新のエンタープライズ環境におけるネットワークセグメンテーションとマイクロセグメンテーション

概要

セグメンテーションでセキュリティを確保するという考え方は、今に始まったものではありません。境界ファイアウォールは、VLAN や ACL とともに、IT インフラをセグメント化したり保護したりするために、多くの企業が従来的に使用してきたものです。しかし、時代は変わりつつあります。コンテナ化の増加、ソフトウェア定義のネットワーク化、パブリックおよびマルチクラウドインフラの使用、インターネット接続デバイスの拡張により、新たなセキュリティ問題が生まれています。これに対処するためには、さまざまなセキュリティ要件を有する異種 IT 環境向けに構築されたソリューションが必要になります。さらに、ランサムウェアや国家ぐるみの攻撃者は、今やあらゆる企業にリスクをもたらします。また、攻撃者が高度化していく一方で、IT 環境を可視化して把握することが難しくなっています。従来の境界セキュリティ対策では、ディープ・パケット・インスペクションに基づく次世代ファイアウォールやシグニチャベースの検知と同様に、今日のエンタープライズデータセンターが抱えているトラフィック量に対応するのが難しくなっています。適切なマイクロセグメンテーション手法が、他のネットワーク・セグメンテーション・アプローチの欠点に対処するテクノロジーとして適切であることを紹介します。

ハイブリッドクラウド環境が標準となり、従来の境界セキュリティよりもはるかに厳しい要件が求められています

レガシーファイアウォールは水平方向（East/West）のトラフィックに適さない

IT 環境をセグメント化する際、エンタープライズでは従来型の境界セキュリティデバイスにまず目を向けてしまいがちです。残念ながらこれらのデバイスは、クライアントからサーバーへの縦方向のトラフィックを監視する仕様となります。これは外部ソースからデータセンターに送られるトラフィックです。最近は、データセンター内のサーバー間を移動するトラフィック（水平方向のトラフィック）の量が急増しています。これは主に、仮想化およびコンバージドインフラ（ハイパーバイザー、VPC、コンテナベースのコンピューティングなど）の普及が要因となっています。

従来のファイアウォールのような境界セキュリティ対策では、感染したデバイスからビジネスを保護したり、攻撃者が水平方向（East/West）のトラフィックで足掛かりを拡げるのを阻止したりすることができません。TLS 暗号化が増加し、オープンな正規のアプリケーションポートで悪質なトラフィックを隠蔽してピギーバッキングするのが簡単になり、ファイアウォールを横断しても、多くの攻撃が通過できてしまうようになっています。これにより、既存の侵害を特定して解決したり迂回したりすることができなくなります。また、ネットワーク上における攻撃者の滞留時間を制限するのも難しくなります。滞留時間が長いほど、侵害は壊滅的になります。Sophos の Active Adversary Playbook 2022 によると、平均滞留時間の中央値は 15 日でしたが、中小企業や特定の業界では最長 34 日と、平均滞留時間が長い傾向があることがわかりました。[1]攻撃者がネットワーク内で検知されない時間が長くなるほど、もたらされる被害も大きくなります。

数千にも及ぶアプリケーションやワークロードを保護するのに十分な数の仮想ファイアウォールを使用するのは、無理な話です。仮想ソリューションを作成できたとしても、現在の環境が変化し続けることを考えると、管理したり制御したりすることはできません。たとえば、ハイブリッドクラウドの場合、従来のファイアウォールの使用はさらに難しくなります。さまざまな環境で作業し、異なるクラウド間でワークロードを追跡するうえ、1 か所で制御する必要があるからです。これらの問題に対して解決を試みようと、ネットワーク・セグメンテーション・アプローチがいくつか生まれました。

3 つのセグメンテーションアプローチを検討

ファイアウォールは、仮想化されていてもハイブリッドクラウドデータセンターを十分に保護できないという認識の下、エンタープライズでは 3 つの基本的な方法で、水平方向のインフラでのセグメンテーションを適用することを検討しています。説明したように、ポートやサーバーは、強力なセグメンテーションポリシーやセキュリティ対策がなくても相互に通信ができます。つまり、サーバーのファイアウォールが侵害されると、攻撃者はネットワーク内のあらゆるポートやサーバーに容易に移動できることになります。サーバー間の接続を制限する最も効果的な方法は、ネットワークのセグメント化です。ネットワークのセグメント化には 3 つの基本タイプがあり、マイクロセグメンテーションを使用します。このテクノロジーにより、よりきめ細かなポリシーや制御を実施できるようになります。ユーザーは、以下に示す 3 タイプのセグメンテーションポリシーを組み合わせて、重要なアプリケーションやリスクの高いアプリケーションに対してきめ細かなポリシーを構築することができます。

環境のセグメンテーション

このアプローチでは、相互を異なる環境に分離します。これにより、たとえば、実稼働環境から会社の開発部門をセグメント化することができます。これは、セグメンテーション戦略における最初の重要な段階となります。そこから、きめ細かなポリシーを作成できるようになります。

アプリケーションのセグメンテーション

セグメンテーションをさらに進めて、高価値なアプリケーションの「リングフェンシング」では、各特定の重要アプリケーションを取り出し、ネットワークの他の部分から分離します。優れたマイクロセグメンテーションソリューションなら、これをプロセスレベルで制御することもできます。

階層のセグメンテーション

最も厳重なタイプのセグメンテーションは、アプリケーション内でのセグメント化です。ここでは、同じアプリケーションクラスター内の階層間で通信を管理する方法のポリシーを作成して、Web　サーバー間、アプリケーションサーバー間、データベースサーバー間のトラフィックを制御することができます。これは、プロセスレベルの実行を選択した場合でも制御できます。

ネットワークセグメンテーション手法：VLAN を介したネットワークセグメンテーション

ほとんどの企業では、VLAN を採用することから始めます。仮想ローカルエリアネットワークを使用すると、ルーター自体のファイアウォールやアクセス・コントロール・リスト（ACL）を介して、独自の通信パスで各セグメントを割り当てることができるようになります。ネットワークセグメンテーションに VLAN を使用するのは一般的ですが、水面下では多くの問題があります。今日のセキュリティニーズに対応するうえで、なぜ VLAN は標準的な選択肢となり得ないのか、詳しく説明します。

多くの企業がセグメンテーション手法として VLAN を選択する理由は簡単です。既存のアーキテクチャでできるからです。低コストで簡単に展開できる印象があります。しかし、このセグメンテーションアプローチは非常に厳密で複雑なものです。維持にコストがかかる可能性があり、実装するためにはダウンタイムが必要になります。

VLAN の使用を開始するためには、各セグメントのサーバーや依存関係を把握してから、セグメント化するネットワークスイッチに必要な設定を作成する必要があります。この作業はネットワークエンジニアが行い、複数の場所で行われることも少なくないため、何日も要することもあり、時間やコストがかかりすぎてしまう可能性があります。設定の際は、トラフィックが中断されたり、速度が低下したりする場合があります。

アジリティが重要な競争優位性となり、必須とさえ言われている今、変更に伴うコスト上昇やスピード低下は、最終収益に大きく響くことを意味します。Forbes によると、適応性は生き残るための鍵となると言われています。「中断は今に始まったことではありません。しかし、中断の速度、複雑さ、全体的な性質は、これまでにないレベルのものです。...規模が大きければ、または財政的に安定していれば生き残れるというわけではありません。急激な変化のペースに適応できるところが生き残れるのです」と、コメントしています。[2]

VLAN は、セグメンテーションを考慮して構築されたものではないことを認識することが重要です。本来、輻輳を軽減するために構築されたものであるため、通信を制御するために使用することは、既存のテクノロジーを活用する方法としてスマートではありません。これでは、さまざまな方法で悪用されてしまいます。このような観点から、VLAN を使用したセグメント化には制約が伴うのは当然のことと言えます。

- **クラウドテクノロジー**：VLAN などの従来のネットワーク・セグメンテーション・ポリシーをクラウドに拡張することはできません。内部セグメンテーションファイアウォール（ISFW）や ACL を使用して、ネットワークセグメントにアクセスできるユーザーを制御する場合、おそらくはクラウドの SDN（ソフトウェア定義ネットワーク）を利用しなければなりません。これは、仮想ファイアウォールまたはサブネットを使用する、サードパーティーのソフトウェアプロバイダーが行うのが一般的です。
- **コンテナ**：IT 環境でコンテナが広く採用されていることを考えると、セキュリティは依然として大きな懸念事項です。各コンテナが同じカーネル上で実行されるため、エクスプロイトによってすべてのコンテナが危険に晒される恐れがあります。分離が現行の大きな課題ですが、普通のネットワークセグメンテーション手法では解決できません。
- **プロトコル制限**：VLAN の上限は 4,096 セグメントです。これが制約となり、大規模データセンターでは十分にセグメンテーションを行うことができません。セグメンテーションをさらに細かく行うアプローチでは、このような制限はありません。

ネットワークセグメンテーションからアプリケーションセグメンテーションへ：レイヤー 4 制御の実装

これらの問題の多くは、クラウド環境内のセキュリティグループや、オンプレミス仮想環境用のハイパーバイザーベースのファイアウォールによるアプリケーションセグメンテーションを採用することで改善されています。従来のアプリケーションセグメンテーションでは、レイヤー 4 制御が実装されているため、サービス階層を分離でき、アプリケーションの境界でセキュリティを確保できるようになります。各階層は、完全な機能を提供するために必要なアクセスレベルに制限されますが、それ以上の制限はありません。個々のアプリケーションの階層間で明確に分離され、潜在的な侵害の脅威は最小限に抑えられます。

ロードバランサーやデータベースから、DMZ 内部または外部のアプリケーションサーバーまで、標準的なビジネスで見られる階層について考えてみましょう。これらの階層を分離させておくことで、それぞれに独自のセキュリティルールや機能を保持させることができます。アプリケーションセグメンテーションでは、各階層に適切な制御を提供し、機密情報や通信を制限しながら、必要に応じて幅広いユーザーアクセスを可能にして、企業をサポートすることができます。たとえば、特定のデータベースにおいてインターネット通信が一切できないようにしたり、単一のロードバランサーが侵害された場合に、攻撃者がデータベース階層にある機密性の高い情報に向かうことができないようにしたりすることができます。

ソリューションが細分化されると、アプリケーションセグメンテーションでは、ビジネスの他の領域からアプリケーションクラスター全体をセグメント化できるようになります。これにより、前述のとおり、アタックサーフェスの領域を削減し、攻撃者が階層間でラテラルムーブメントを行うことができないようにすることができます。

レイヤー 4 制御の限度

従来のアプリケーションセグメンテーションでは、深度が不足する場合があります。これは、可視化に直接影響します。ルーティングが行われるネットワーク層では、システム間でデータが移動し、IP　アドレスやプロトコルが割り当てられ、送信先向けのセグメント化で使用されるパスデータが細分化されます。アプリケーションセグメンテーションでは、多くの場合、レイヤー 4 のネットワーク制御が使用され、データ自体の配信方法に重点が置かれます。大規模なデータセグメントは、小さなセグメントやブロックに分割され、送信先で元通りにすることができるようになっています。情報を送受信するデバイスが必要な場合、フロー制御を使用すると、プロセスを動的に高速化したり減速したりすることができます。

今日の脅威の状況では、これらのレイヤーに対する制御が不可欠ですが、状況によっては、さらに細かいレベルでポリシーを設定したほうが良い場合もあります。攻撃者は、IP　アドレスをスプーフィングし、許可されたポートでピギーバッキング手法を用いてネットワークを侵害できることが確認されています。さらに、レイヤー　4　の保護では、アプリケーションや階層内でのラテラルムーブメントが制限されないため、アタックサーフェスが不必要に大きくなったままになっている可能性があります。

レイヤー 4 だけではなく、より細かい制御の必要性に関する最たる例の 1 つは、コンプライアンスイニシアチブにあります。企業では、従来のアプリケーションセグメンテーション手法で、PCI-DSS のために CDE を分離したり、HIPAA のために PHI を保護したりするなど、特定のコンプライアンス規制を満たすことがある程度可能でした。ところが、レイヤー 4 の手法は、コンプライアンスを示すための効果的な手段としてかつては受け入れられてきたものの、実情は十分でない可能性があることが判明しています。Verizon 2022 Payment Security Report によると、「完全に準拠している」と回答した企業はわずか 43% でした。[3]さらに悪いことに、コンプライアンスを 100% 確保しても、セキュリティが　100%　確保されているわけではないのです。レイヤー 4 の制御は、コンプライアンス面ではカバーされますが、セキュリティ確保において有意義な改善をもたらすほどアタックサーフェスが削減されるわけではないのです。それだけのことです。攻撃者は、単独のプロセス（レイヤー　7）を使用して 2 つの階層間でオープンなレイヤー 4 ポートを制圧して、必要なものをすべて取得することができます。

曖昧なセグメント化：ネットワークやアプリケーションにおけるセグメンテーションの可視性の欠如

アプリケーションセグメンテーションが正しい方向への一歩であることは、エンタープライズが認識しているとおり、間違いありません。しかし、セグメンテーションアプローチが大雑把だと、内在するあらゆる問題を解決することはできません。依然として対処が必要なもう 1 つの問題は、可視性です。セグメンテーションプロセスの各段階では、ネットワークの全体像を正確かつリアルタイムで確認できることが不可欠です。しかし、多くのセグメンテーションアプローチにおいてこれが欠如しています。

最初に、アプリケーションの依存関係を可視化する必要があります。そうすることで、正確なポリシールールが作成できるようになります。セグメンテーションができたら、セグメンテーションが意図したとおりに機能するかテストする必要があります。これは、セキュリティ体制が強力であることを確認するだけでなく、必要に応じて規制コンプライアンスのエビデンスを提示するためでもあります。

リアルタイムと過去の可視化がなければ、自分自身、サードパーティーのステークホルダー、規制機関に示せるエビデンスはありません。手作業でのエビデンス収集は、時間や管理コストがかかり、設定エラーやミスの可能性が常に伴うことになります。このような可視化ができなければ、セグメンテーションソリューションはまったく不十分です。

レイヤー 7（アプリケーションレイヤー）までのマイクロセグメンテーション

一方、アプリケーションレイヤー（レイヤー 7）でのセグメント化は、アプリケーションクラスター内であっても、ラテラルムーブメントを制限するうえで非常に効果的です。レイヤー 7 では、ネットワークサービスがオペレーティングシステムと統合されます。HTTP、FTP、TFTP、SMTP などのプロトコルはすべてレイヤー 7 のプロトコルです。マイクロセグメンテーションテクノロジーの最新の進歩により、他のソリューションよりもはるかに深く、このレイヤーでセグメント化できるようになり、従来のレイヤー 4 の場合と同様に、レイヤー 7 でアクティビティを可視化したり制御したりすることができます。つまり、企業でポリシーを設定するときに、IP　アドレスやポートに依存するのではなく、特定のプロセスやフローが使用できるようになります。これには、特定の階層やアプリケーションクラスターを凌駕するセグメンテーションのメリットがあります。また、不正ハッシュ程度の潜在的脅威も特定できるようになります。許可されたプロセスや経路を攻撃者がミラーリングしている場合でさえも特定可能です。

ポリシーの作成に関しては、レイヤー 7 に対してセグメント化することで、許可リストルールや例外を極めて具体的に設定できるようになり、完全に一致するプロセスやフローのみが許可され、他の通信はすべてデフォルトでブロックされるようになります。これにより、システム間のデータを強制的に分離できるようになりますが、必要なデータフローの場合やビジネスクリティカルなデータフローの場合は、通信を許可できます。

最も優れたマイクロセグメンテーションソリューションは、ビジネスがアジリティを得るために必要とする可視性をもたらす

ハイパーバイザーベースまたはVPCベース、コンテナ、ベアメタルサーバー、IoT/OTシステムなど、あらゆるワークロードのエージェントにおける包括的なマイクロセグメンテーションソリューションでは、IT インフラ全体の完全なビジュアルマップを企業に提供します。真のインテリジェントソリューションとなり、これにはデータセンター、クラウド、マルチクラウド、ハイブリッドクラウドの環境や、リモートデバイスなどが含まれます。従来のアプリケーション・セグメンテーション・ソリューションでは、ネットワーク中心のテクノロジーが混在して使用されているため、一元的に確認するのが困難です。

環境の包括的なビジュアルマップは、どのセキュリティポリシーが適用され、リアルタイムで実施されているのかが確認できるものでなければなりません。エンジニアやセキュリティ担当者が一目見ただけで、潜在的な欠陥を確認してポリシーの適用範囲を修正したり、新たに実装が必要なポリシーや、ゼロから新たに作成する必要があるポリシーを確認したりすることができなければなりません。

このように可視性を確保できると、更新されたアプリケーションや新規のアプリケーションのセグメント化に関するルールを事前に作成しておくことで、新規のソフトウェアや既存システムの更新に備えてから、展開できるようにしておくことができるようになります。更新がアクティブの状態になると、セキュリティチームは、異常なアプリケーションアクティビティを検知して解決に必要な情報をリアルタイムで入手できるようになるため、セキュリティリスクを見過ごしたり、アクティブなエクスプロイトが生じたりすることはありません。事後に、企業が保有するコンテキストツールでインシデントと履歴データを照合し、異常の発生を許した環境を正確に把握します。ポリシーを厳重化したり、セグメンテーションを調整したりすることもできます。さらに、コンプライアンス規制や後の調査に対してはインシデントを詳細に説明することができます。

ゼロトラスト・モデルの導入

マイクロセグメンテーションのもう 1 つのメリットは、ゼロトラスト・セキュリティ・モデルを採用できることです。ゼロトラストの概念は、2010 年に Forrester により生み出されたものですが、マイクロセグメンテーションなどのテクノロジーはこの概念の実現をサポートするものとなり、研究者やセキュリティ専門家がそのメリットを幅広く伝え続けています。[4]

考え方はシンプルです。信頼できることが証明されて承認されるまで、トラフィックやユーザーを信頼しないというものです。トラフィックのソースが外部であろうと内部であろうと関係なく、接続が試行されるたびに証明や承認が求められます。Forrester のゼロトラスト 3 大原則[5]はいずれも、強力できめ細かいマイクロセグメンテーションポリシーによりサポートされています。

- デフォルトの状態では、すべてのエンティティを信頼しない
- 包括的なセキュリティモニタリングが行われている
- 最小限の権限アクセスを適用する

ゼロトラストは、境界のみのセキュリティとはまさに正反対の位置付けになります。境界のみのセキュリティとは、深い堀で城の入口を保護し、内部にいる人は全員入場が認められていることを前提としています。ほとんどの企業は、封じ込められたネットワークやデータセンターをもはや保有していないため、「城」という考え方は時代遅れになっていると言えます。ゼロトラストのような最小権限戦略は、いつでも内部にいる人を把握して制御できる唯一の方法です。

マイクロセグメンテーションでビジネスの将来に備える

ネットワークセグメンテーションは、境界セキュリティを確実に凌ぎます。また、レイヤー 4 までの環境セグメンテーションとアプリケーションセグメンテーションは、セグメンテーション戦略を構築するうえで重要なステップとなります。しかし、IT 環境がますます複雑化するにつれ、階層のセグメンテーションでさらに細分化できるセグメンテーションソリューションや、アプリケーションおよび階層ステージのレイヤー 7 に対するプロセスレベルの適用の必要性を感じるかもしれません。

現代の企業は、自己完結型インフラの先を進んでいます。多くの場合、クラウド、コンテナ、ベアメタルハイパーバイザーの SDN などのテクノロジーに依存しています。これらは、さまざまな地域や物理的なデータセンターで機能します。

内外の脅威から自身を保護する唯一の方法は、水平方向や縦方向など、すべてのトラフィックを調査して制御し、重要なアプリケーションやリスクの高いアプリケーションに関しては、レイヤー 4 だけでの可視化にとどまらない、より多くの可視化を実現できるソリューションを採用することです。アプリケーションレベルまたは階層レベルとなるレイヤー 7 までのマイクロセグメンテーションにより、IT 環境全体を正確に把握し、ゼロトラスト・モデルに準拠したきめ細かなセキュリティポリシーを簡単に作成して適用できるようになります。優れたマイクロセグメンテーションソリューションなら、セキュリティやアジリティを選択する必要がありません。組織全体で最も強力なセキュリティ体制を実現できるものを選択してください。

その他の詳細については、
akamai.com/guardicore をご覧ください。

1 John Shier、2022 年、「The Active Adversary Playbook 2022（アクティブアドバーサリープレイブック 2022）」、Sophos、6 月 7 日。

2 Rob Gonda、2018 年、「Adaptability Is Key To Survival In The Age Of Digital Darwinism（デジタル自然淘汰の時代で生き残る鍵は適応力）」、Forbes、5 月 24 日。

3 https://www.verizon.com/business/reports/payment-security-report/

4 David Holmes、2022 年 6 月、「Best Practices For Zero Trust Microsegmentation（ゼロトラストマイクロセグメンテーションのベストプラクティス）」、Forrester、4 月。

5 David Holmes、Jess Burn、2022 年 1 月、「The Definition Of Modern Zero Trust（最新のゼロトラストの定義）」、Forrester、4 月。

Akamai は、お客様が生み出すもの全てにセキュリティを組み込む取り組みを支援することで、どこで構築しどこへ提供しようとも、顧客体験、従業員、システム、データを守ります。グローバルな脅威に対する可視性を備えた Akamai のプラットフォームは、セキュリティポスチャの適応と進化を後押しして、ゼロトラストの実現、ランサムウェアの阻止、アプリケーションと API のセキュリティの確保、DDoS 攻撃の撃退を支援します。これにより、お客様は自信を持って、継続して、イノベーションを起こし、可能性を広げ、新たな可能性を生み出すことができます。Akamai のセキュリティ、コンピューティング、デリバリーの各ソリューションの詳細については、akamai.com および akamai.com/blog をご覧いただくか、Twitter と LinkedIn で Akamai Technologies をフォローしてください。公開日：2023 年 5 月。