FORTINET

WHITE PAPER

インテント ベースト セグメンテーションのための ネットワーク運用ガイド

攻撃対象領域全体でのリスク軽減と コンプライアンス実現に不可欠なプラクティス

要約

ネットワーク、デバイス、ユーザー、アプリケーションのセグメンテーションは、エッジセキュリティを補完し、フラットな内部ネットワークを分割するベストプラクティスとして長年にわたって活用されてきました。ところが、ネットワークエンジニアリングとオペレーションのリーダーが、リスクの軽減、コンプライアンスの実現、効果的なセキュリティ管理を優先事項として位置付けるようになると、このようなセグメンテーションのアプローチでは不十分です。

従来のアプローチでは、アクセス制御の粒度が粗すぎて、ビジネス要件を満たすことはできませんでした。また、基盤となる信頼（トラスト）評価情報は、すぐに古くなってしまいます。このアプローチでは脅威保護の実装が前提となりますが、攻撃対象領域の拡大と伴にセキュリティホールも広がっています。このような環境でプロアクティブなセキュリティ管理を行うことは不可能であり、組織を深刻なセキュリティリスクにさらすことになってしまいます。

マルチクラウド、モバイルファースト、モノのインターネット（IoT）をはじめとするデジタルトランスフォーメーションイニシアティブによって攻撃対象領域が拡大する今、重要なアプローチとして新たに登場したのが、インテント ベースト セグメンテーションです。セグメンテーションの弱点を解消するこのアプローチは、幅広いアクセス制御シナリオに適用することができます。

企業が導入しているセキュリティツールは、平均で 75 種類にも達します。このような環境で、透明性に優れたエンドツーエンドの可視化は実現できるでしょうか。[1]

効果的なセグメンテーションを行うには、ビジネスの意図（インテント）に基づいて、セグメンテーションの適用範囲、監視の方法、セキュリティの実行対象を確立する必要があります。

インテント ベースト セグメンテーションの基本

インテント ベースト セグメンテーションとは、ネットワークリーダーのビジネス意図（インテント）を、セキュリティセグメンテーションの「適用範囲（Where）」、「方法（How）」、「内容（What）」へと効率的に変換するものです。

- **「適用範囲（Where）」：**セグメントの場所と、IT 資産をセグメント化するためのロジックを確立します。
- **「方法（How）」：**ビジネス意図を粒度の高いアクセス制御に適用し、継続的でアダプティブ（適応型）の信頼に基づいて維持します。
- **「内容（What）」：**高性能で高度な（レイヤー 7）セキュリティをネットワーク全体に適用することで、アクセス制御を行います。

上記の 3 つの要素は、セキュリティコンポーネントが統合されたファブリック内で動作し、このコンポーネントは他のネットワークやインフラストラクチャデバイスと通信します。したがって、セキュリティ対策の強化、リスク軽減、コンプライアンスや運用効率のサポートを全社的に実現でき、ネットワークアーキテクチャを変更する必要もありません。

ビジネスの意図を満たすセグメンテーション

インテント ベースト セグメンテーションは、一般的な**マクロやミクロのセグメンテーションアーキテクチャ**はもちろん、**アプリケーション、プロセス、エンドポイントのレベルでのセグメンテーション**にも対応します。このようなセグメンテーション手法のいずれかでフラットなネットワークをセグメント化すると、攻撃対象領域が縮小されて管理しやすくなり、高性能で高度な（レイヤー 7）セキュリティによる保護をさらに強化できます。

インテント ベースト セグメンテーションでは、ビジネス意図に沿ってセキュリティドメインやセグメントを作成することが可能です。ただし、ビジネス意図の実現には、**ユーザーアイデンティティやビジネスロジック**に基づいた粒度の高いアクセス制御が必須です。また、信頼評価情報が継続的に収集されている外部信頼データベースに対してクエリを実行し、最新の信頼情報に基づいてアクセス制御を調整する必要もあります。

情報に基づいたリスク管理を実現するアダプティブな信頼

これまでのアクセス制御は、「ユーザー、デバイス、アプリケーションの信頼性は不変である」という前提に基づいていました。ところが実際には、一般的な業務の変化や新たな脅威の登場により、信頼性は常に変化しています。信頼レベルの変化は企業のセキュリティ環境とネットワーク固有のリスクに非常に大きな影響を及ぼすため、静的な信頼に基づくアプローチでは十分な情報を得ることはできません。

この問題を解決するため、インテント ベースト セグメンテーションでは、継続的に更新される信頼レベルへとアクセス制御をリンクします。より包括的なソリューションを実現するために、信頼情報は社内外のデータソースから取得されます。

また、ネットワーク固有のリスクを正確に把握するために、セキュリティの状態を継続的に評価する機能を搭載しています。**セキュリティレーティングサービス**は、ネットワークのセキュリティ設定の評価、リスクや脆弱性に関する実用的インテリジェンスの提供、設定の不具合を修正するベストプラクティスの提示といった機能を備えています。また、セキュリティ状態を時系列で追跡し、全体的なセキュリティ状態を自社と類の組織と比較し、セキュリティ標準に基づいて測定することも可能です。ここで重要なのは、セキュリティをリアルタイムで評価する機能を備えた脅威インテリジェンスソリューションを選定することです。このようなソリューションがあれば、攻撃対象領域全体に存在する脆弱性を完全に把握し、一元的な可視化が可能になります。さらに、セキュリティレーティング機能があれば、脆弱性のパッチ適用に優先順位を付け、新たに発生した脅威を素早く検知するなど、ネットワーク内外で対策を講じることができます。

現在、インターネットトラフィックの72% が暗号化されていますが、サーバー犯罪者によるネットワークへの侵入とデータ流出は後を絶ちません。

脅威は巧妙化しているため、ネットワークエンジニアリングとオペレーションの責任者は、ネットワークセキュリティ環境の評価を継続的に行う必要があります。

強力な脅威保護を広範囲に適用

多くの組織がアクセス制御を実装していますが、その適用に必要なセキュリティコンポーネントが導入されているとは限りません。また、コンポーネントが導入されていたとしても、有効に統合されていないケースもあります。このような場合、新たに出現する脅威をネットワークエンジニアリングやオペレーションのリーダーが検知し、攻撃を未然に防ぎ、ネットワーク全体への感染拡大を回避することは難しくなります。

ネットワーク全体に SSL を常時適用:アクセスポリシーを適用して攻撃対象領域全体を保護するために、インテント ベースト セグメンテーションでは、コスト効率とパフォーマンスに優れた高度な（レイヤー 7）脅威保護を次世代ファイアウォール（NGFW）に実装しています。これによって提供される SSL（Secure Sockets Layer）インスペクションは、セキュリティに不可欠なコンポーネントです。

インターネットトラフィックの 72% が暗号化される今、SSL や TLS（トランスポートレイヤーセキュリティ）で暗号化されたトラフィックのインスペクションは、もはや必須要件であるといえます[2]。Heartbleed、Poodle、Zeus といったマルウェアの登場は、暗号化標準が脆弱であり、攻撃の標的になり得ることを示しています[3]。ところが、ネットワークスループットやユーザーエクスペリエンスへの影響という点で、現状では多くの組織が SSL インスペクションの全面的な適用に消極的になっています。この問題を解決するために、インテント ベースト セグメンテーションで使用される NGFW には、スループット低下を最小限に抑える**専用設計の高性能セキュリティプロセッサ**が搭載されています。これにより、すべての NGFW において SSL インスペクション機能が常に有効な状態になります。

インテント ベースト セグメンテーションの重要な原則の 1 つに、オンプレミスとクラウドのいずれにおいても、脅威保護を必要に応じて導入できるという点が挙げられます。このようなポリシーの実装にコストを掛けたくないと考えるネットワークエンジニアリングやオペレーションの責任者も存在しますが、物理および仮想の幅広いフォームファクターと多様なポート密度の製品を展開するベンダーの NGFW を選択することで、TCO（総所有コスト）を最小限に抑え、広範囲での導入が可能になります。

エンドツーエンドの管理：ネットワーク全体に多様な脅威保護ソリューションを導入するには、効果的なエンドツーエンドの可視性と管理機能が不可欠です。あらゆる経路で侵入する脅威からネットワーク全体をプロアクティブに保護するには、統合型のセキュリティ ファブリックの一部として、インテント ベースト セグメンテーションによるソリューションを導入する必要があります。このソリューションは、包括的でエンドツーエンドの可視性と一貫したポリシー制御を、あらゆるセキュリティ適用ポイントに提供する必要があります。

ユースケース

インテント ベースト セグメンテーションは、幅広いアクセス制御のシナリオに適用できます。ここでは、ネットワークワークエンジニアリングやオペレーションの責任者向けに、適切なアクセス制御の分類と高性能で高度な脅威保護が、セキュリティアーキテクチャの的確な制御と効果的なリスク軽減に役立つ事例を 2 つご紹介します。

ユースケース：攻撃対象領域の縮小

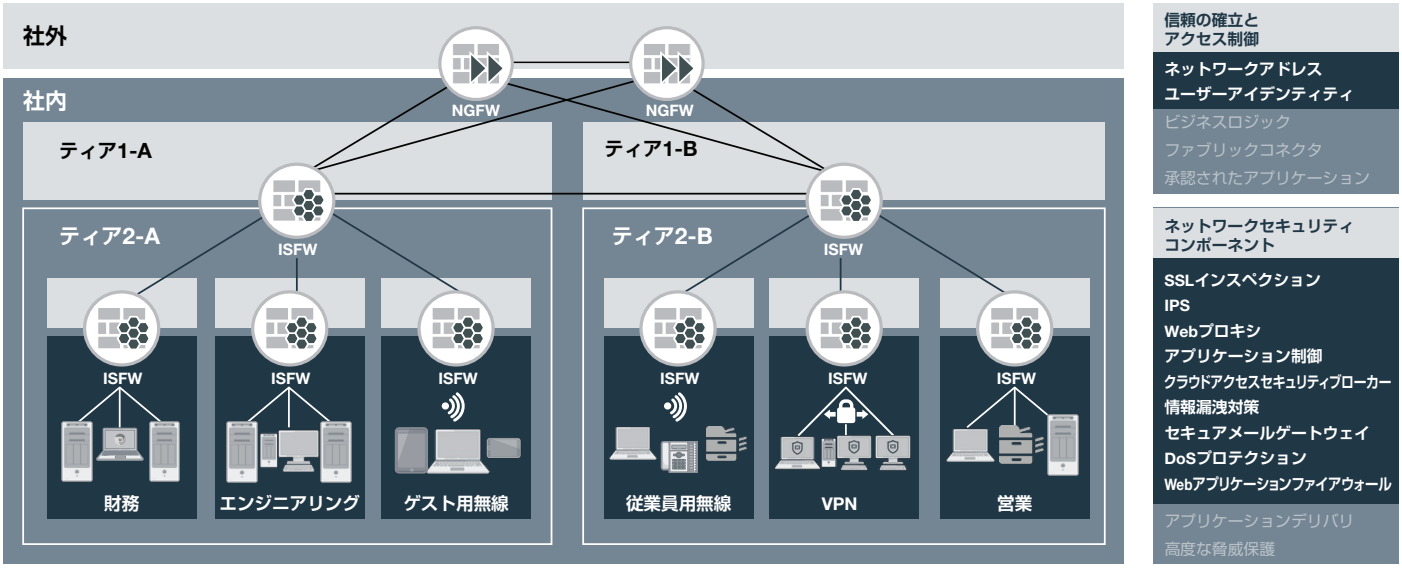

図 1：ユースケース：攻撃対象領域を縮小することでリスクを軽減

ほとんどの企業では、境界の防御だけではネットワーク資産を保護できません。不適切な設定、社内ネットワークに接続したデバイスの侵害、セキュリティ制御を迂回したゼロデイ攻撃などが原因でセキュリティ侵害が発生した場合、これに対抗するには、**多層型の防御**が必要です（図 1 では、ティア 1 とティア 2 の間にある境界と、ティア 2 内にある境界）。

このように内部セグメンテーションファイアウォールを追加することで、さまざまなセキュリティ制御を適用し、保護対象のゾーン内で発生した悪意のある活動を封じ込めることができます。この場合、資産 ID（ネットワークアドレス）やユーザーアイデンティティに基づく認証を使用するのが一般的です。セキュリティセグメンテーションの追加には、ネットワークアーキテクチャ自体を変更する必要はありません。

すべてのファイアウォールは相互に通信すると同時に、一元管理システムとも通信するため、ネットワークトラフィックをエンドツーエンドに可視化できます。ファブリックベースの管理システムは、あらゆるセキュリティコンポーネントの脅威保護活動を統合し、完全な監査証跡を作成します。

ユースケース：コンプライアンスの達成

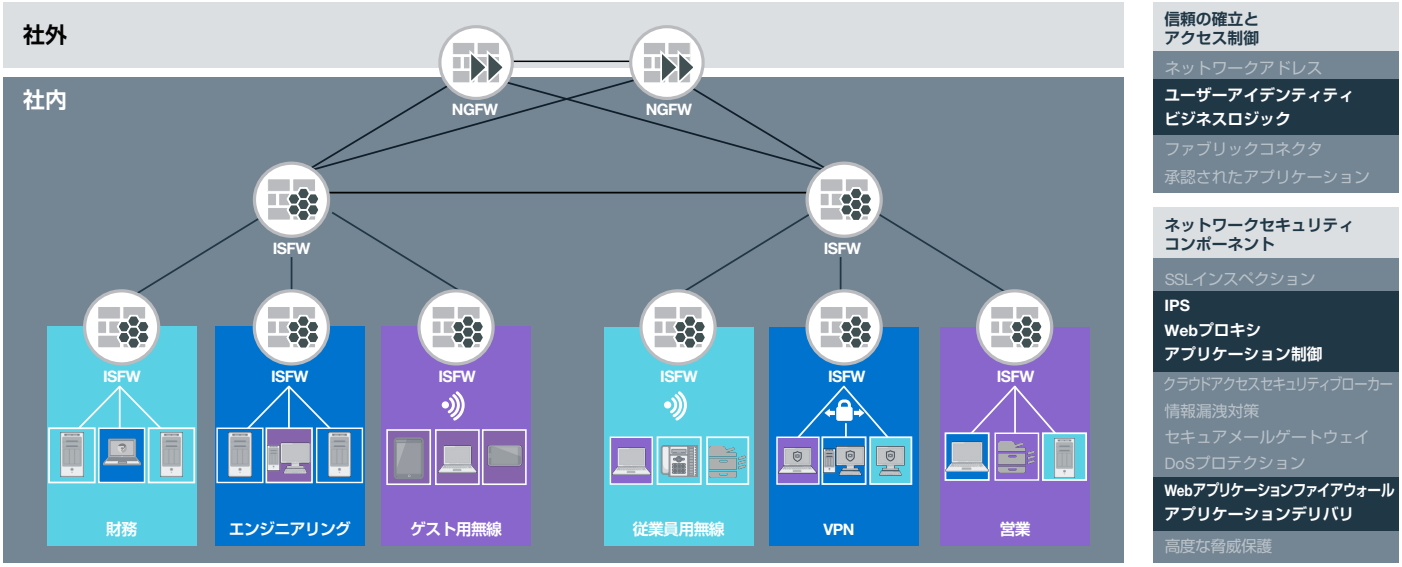

図 2：ユースケース：複雑なコンプライアンス要件への対応

ガバナンスや業界規制へのコンプライアンスは、ほぼすべての組織に求められる必須要件です。ただし、コンプライアンスの規則変更や新たな法規制の施行の際に毎回ネットワークを構成し直すことは、現実的ではありません。

たとえば、図 2 で示すように財務部門用サブネットを隔離するだけでは、PCI DSS（Payment Card Industry Data Security Standard）に準拠する資産のセグメント化は極めて困難だといえます。実際には、財務部門用サブネット内のデバイスすべてが PCI コンプライアンス対象になるとは限りません。また、PCI コンプライアンスの対象となるデバイスが別のサブネット上にある場合や、リモート環境に存在する可能性もあります。

インテント ベースト セグメンテーションでは、アクセスポリシーを定義し、ファブリック接続されたセキュリティコンポーネントを介して適用することが可能です。資産とユーザーには、ネットワーク上の場所、他のコンプライアンス要件、アクセスポリシーに関係なく、PCI コンプライアンスの対象であることを示すタグを付けることができます。

まとめ

インテント ベースト セグメンテーションは新しいアプローチですが、すぐに本番環境での稼働が可能なソリューションです。その実装に必要な製品とサービスは数多く存在し、ファブリック接続型の脅威保護コンポーネントも着実に増加しています。

ネットワークエンジニアリングとオペレーションの責任者の皆様には、本資料で紹介したユースケースや現在のビジネス要件に沿って、インテント ベースト セグメンテーションの概念実証を行うことをお勧めします。フォーティネットのデモンストレーションでは、中核的なコンポーネントを実装して既存のネットワーキングテクノロジーに接続することにより、インテント ベースト セグメンテーションを段階的かつ確実に導入する方法をご紹介します。詳しくは、営業窓口までお問合せください。

[1] Kacy Zurkus 氏、「Defense in depth: Stop spending, start consolidating（英文）」、CSO Online（2016 年 3 月 14 日時点の情報）：https://www.csoonline.com/article/3042601/security/defense-in-depth-stop-spending-start-consolidating.html

[2]「フォーティネット脅威レポート 2018 年第 3 四半期版」（2018 年 11 月公開）：https://www.fortinet.com/content/dam/fortinet/assets/threat-reports/ja_jp/TR-18Q3.pdf

[3] Ananda Rajagopal 氏、「How SSL encryption gives a false sense of security（英文）」、CSO Online（2019 年 2 月 4 日時点の情報）：https://www.cso.com.au/article/569409/how-ssl-encryption-gives-false-sense-security/

FORTINET
フォーティネットジャパン株式会社

〒106-0032
東京都港区六本木 7-7-7
Tri-Seven Roppongi 9 階
www.fortinet.com/jp/contact

お問い合わせ

WP-Network-Intent-based-Segmentation-201907-R1