SOLUTION BRIEF

フォーティネットの Microsoft Azure 向けハイブリッドメッシュファイアウォールとセキュリティファブリック

エグゼクティブサマリー

Microsoft Azure は、世界中の何千社もの企業に選ばれているクラウドです。Microsoft Azure は、クラウド内のアプリケーションやデータを保護する、さまざまなセキュリティソリューションやテクノロジーに対応しています。しかし、エンタープライズネットワーク向けに完全なセキュリティを提供しているわけではありません。企業は、すべてのクラウドとデータセンター全体で一貫したセキュリティポリシーを適用するだけでなく、あらゆるコンピューティングを詳しく可視化し、細かく制御する必要があるのです。フォーティネットは、ファイアウォール管理とアナリティクスを一元化することで、クラウド、データセンター、支社などの場所を問わず一貫したセキュリティポリシーを適用し、セキュリティ管理の簡略化、セキュリティ担当者の負担軽減、アプリケーションの保護をサポートします。

「FortiGate は、世代を重ねるごとに性能を上げ、より高度な機能を搭載しています。また、Flex-VM（現 FortiFlex）という利用モデルは、当社のビジネスにとても有益です。状況に合わせてリソースの使用をスケーリングできるため、無駄なく効率的に運用できています。」

Lou Corriero
IT Vortex 社 ビジネス開発担当バイスプレジデント

クラウドがもたらす新たな機能と課題

大多数の企業は、すでに Microsoft Azure などのクラウドへ移行済みか、移行を検討しているところです。その目的は、コスト削減とビジネスアジリティの強化にあります。マイクロソフトはクラウド環境のセキュリティとしてファイアウォールを提供していますが、その機能は限定的で、他のクラウドやオンプレミスには適用されません。

ハイブリッドメッシュファイアウォールの構築

ハイブリッドメッシュファイアウォール（HMF）は、支社、キャンパス、データセンターなどの企業拠点、パブリッククラウドとプライベートクラウド、リモートワーカーなど、さまざまなエンタープライズ IT 領域に協調型の保護を提供する統合セキュリティプラットフォームです。HMF はこのような保護を実現するために、シャーシ、大小さまざまな拠点向けアプライアンス、仮想マシン、クラウドネイティブなファイアウォール、Firewall-as-a-Service（FWaaS）といったさまざまなフォームファクタで展開でき、他のテクノロジーを統合して、さまざまなセキュリティシグナルや自動化を共有できるようになっています。Fortinet FortiGate VM for Azure は、フォーティネットの HMF を含む、幅広いフォーティネットセキュリティファブリックに統合することができます。

さまざまな Microsoft Azure パブリッククラウド環境のセキュリティ

クラウドインフラストラクチャとして Microsoft Azure を採用する企業が増えるに伴い、そのハイブリッド IT インフラストラクチャ全体で一貫性のあるセキュリティを確保する必要性が高まっています。フォーティネットのソリューションは、フォーティネットセキュリティファブリックという統合アーキテクチャの一部として、Microsoft Azure パブリッククラウド環境を細かく可視化、保護、制御します。

1. セキュアなハイブリッドクラウド

FortiGate 次世代ファイアウォール（NGFW）とクラウドセキュリティソリューションによって、ハイブリッドクラウド環境に最も適したセキュアな接続、ネットワークセグメンテーション、アプリケーションセキュリティを実現します。FortiGate は、高速の VPN トンネル接続を使って、一元管理された、一貫性のあるセキュリティポリシーを適用します。パブリッククラウドに展開された FortiGate VM は、プライベートデータセンターに展開されるあらゆるフォームファクタの FortiGate と安全に通信し、一貫したポリシーを共有することができます。

2. クラウドインフラストラクチャの可視化と制御

フォーティネットのソリューションは、設定、ユーザー操作、トラフィックフローログなど、クラウドセキュリティに関わるすべての要素を監視および追跡します。また、コンプライアンスレポート要件にも対応します。

3. セキュアアクセス VPN

リモートアクセス用仮想プライベートネットワーク（VPN）によって、クラウドアプリケーションの利用を可能にします。フォーティネットセキュリティファブリックは、リモート地点から Microsoft Azure へのアクセス時にクラス最高の VPN トラフィック保護を提供します。Microsoft Azure のマルチリージョングローバルインフラストラクチャを利用することで、瞬時にサービスを拡張し、エンドユーザーの近くにリモートアクセス VPN の終端を設置できるようになります。

4. クラウドセキュリティサービスのハブ

フォーティネットのソリューションは、複数のネットワークとセキュリティサービスを世界中で共有することを可能にする Microsoft Azure のトランジット仮想ネットワーク（vNET）として展開できます。ネットワークの可視化、VPN 接続、NGFW、高度な Web アプリケーションファイアウォール（WAF）、サンドボックス機能、メールセキュリティを含むフォーティネットのソリューションがフル装備されたフォーティネットセキュリティファブリックを利用すれば、今までよりもはるかに多くのサービスを享受できると同時に、クラウドの弾力性、オンデマンドの拡張性、価格の最適化といったメリットも得られます。

5. Azure Virtual WAN の統合

フォーティネットのソリューションは Azure Virtual WAN と緊密に統合されているため、SD-WAN を Microsoft Azure クラウドに拡張すれば、vNET 間や Azure Virtual WAN ハブ間の内部通信（East-West トラフィック）が保護されます。

6. ゼロトラストの強制

FortiGate や FortiWeb といったフォーティネットのソリューションは、ゼロトラストポリシーを強制します。ゼロトラストネットワークアクセス（ZTNA）ソリューションは、必ずセッションごとにデバイスとユーザーを確認してから各アプリケーションへのアクセスを許可するため、アプリケーションアクセスを確認したユーザーとデバイスのみに制限することができます。

7. Web アプリケーションのセキュリティ

FortiWeb は、API だけでなくフロントエンドの Web アプリケーションも保護し、アプリケーションとデータのセキュリティを確保する専用 WAF を提供します。Web ベースのアプリケーションは、既知または未知を問わず、幅広い種類の攻撃に脆弱です。FortiWeb は、機械学習（ML）を活用してアプリケーション保護を自己最適化します。また、FortiWeb と連携できる FortiSandbox は、人工知能（AI）を利用してゼロデイ脅威を特定するなど、動的な分析を行います。

8. インテントベーストセグメンテーション

動的にプロビジョニングが行われるということは、IP アドレスが絶えず変わるということであり、クラウド環境のセグメンテーションが難しくなります。FortiGate VM は、ユーザー ID とビジネスロジックに基づいてルールとセグメントを構築する、インテントベーストセグメンテーションを行います。ルールは、継続的に行われる信頼性評価の結果に応じて動的に調節されます。そのため、FortiGate VM は、クラウド内外を問わず、ワークロードや他の要素がどのような通信を許可しているかを直感的に定義できるようになります。

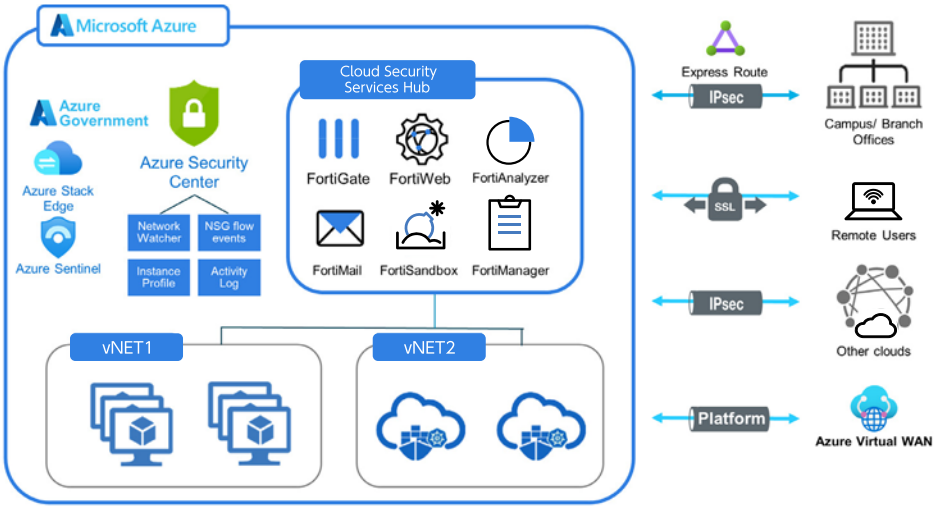

図 1: フォーティネットの Microsoft Azure 向けセキュア接続

フォーティネットセキュリティファブリックによる Microsoft Azure セキュリティの補完

Microsoft Azure の物理的なクラウドインフラストラクチャ（ネットワークやハイパーバイザなど）のセキュリティはマイクロソフトの責任ですが、通信、アクセス、アプリケーションなど、その他の要素のセキュリティとコンプライアンスは、利用者側の責任です。また、すべてのクラウドとデータセンター全体で一貫性のあるセキュリティポリシーを確保することも、利用者側の責任となります。
フォーティネットセキュリティファブリックは、Microsoft Azure のセキュリティソリューションを補完します。フォーティネットのソリューションが Microsoft Azure 内でシームレスに動作し、Microsoft Azure のセキュリティサービスと一体になって、そのクラウドインフラストラクチャ全域のセキュリティポリシーとイベントを透明化します。また、フォーティネットは大手クラウドプロバイダーと一体化されているため、各種クラウド全体でシームレスかつ自動的な一元管理が可能になります。このような一元管理により、可視化、制御、ポリシー管理が統一されるため、アプリケーションやユーザーの増加に合わせてセキュリティを拡張することができます。さらに、セキュリティギャップのリスクを軽減し、設定ミスを防ぎ、最先端のセキュリティによるインフラストラクチャ全域の保護を保証します。

すべての攻撃ステージに対応できる統合防御

フォーティネットセキュリティファブリックを構成するさまざまなソリューションは、クラウド環境に対するエンドユーザーの安心感を高めるために設計されました。Microsoft Azure 向けのフォーティネットセキュリティファブリックには、以下のソリューションが含まれています。

FortiGate VM：既知および未知の極めて高度なサイバー攻撃を防御する脅威保護を提供します。FortiGate VM は、ビジネスニーズの変化に応じてスケーリングできるだけでなく、多様なユースケースに合わせて、さまざまなサイズで取り入れることができます。

FortiWeb：既知および未知のエクスプロイトから Web アプリケーションを保護します。FortiWeb は、ML、AI、多層構造のセキュリティ、相関分析に基づく検出を利用して、既知の脆弱性やゼロデイ脅威からアプリケーションと API を保護します。FortiWeb は、PAYG（従量課金）や BYOL（Bring Your Own License；ライセンス持ち込み）プランを選択し、サービスとして利用することもできます。

FortiMail：フォーティネットのセキュアメールゲートウェイ（SEG）です。FortiGuard Labs の最新技術と脅威インテリジェンスサービスを利用し、一般的な脅威と高度な脅威に包括的な保護を提供するほか、堅牢なデータ保護機能を統合してデータ漏洩を防ぎます。

FortiSandbox：高度な検知、AI ベースの自動対応、実用的なインサイト、柔軟な展開のすべてに対応した強力なソリューションが、高度な脅威やゼロデイ脅威を阻止します。

FortiManager：拡張エンタープライズ全体で管理とポリシー制御を一元化し、ネットワークのあらゆる場所に潜むトラフィックベースの脅威を洞察します。FortiManager には、高度な攻撃を封じ込める機能だけでなく、最大 10,000 台のフォーティネットデバイスを管理できる拡張性も備わっています。

FortiAnalyzer：フォーティネット製品から収集したデータを分析し、それぞれの相関性を明らかにすることで、より詳しく環境を可視化し、確かなセキュリティアラート情報を提供します。また、FortiGuard Indicators of Compromise（IOC）サービスを併用すれば、侵害されたホスト一覧とその優先度を把握し、迅速に問題に対応できるようになります。

Fabric Connectors：フォーティネットのソリューションと、フォーティネットセキュリティファブリック内に展開されるサードパーティのセキュリティソリューションを、シームレスかつオープンに統合することを可能にします。これにより、既存のセキュリティエコシステムを構成するコンポーネントを使って、ファイアウォールの自動化や、動的なネットワークフローにネットワークセキュリティを挿入することが可能になります。

柔軟な利用モデル

フォーティネットの Microsoft Azure 向けソリューションは、長年、PAYG や BYOL などの料金モデルで利用されてきました。フォーティネットが新たに展開する FortiFlex プログラムでは、ポイントベースのアプローチでセキュリティソリューションの柔軟な拡張や、別のプラットフォームへの簡単な移行を可能にしました。また、これらのソリューションは、Microsoft Azure 消費コミットメント（Microsoft Azure Consumption Commitment；MACC）の対象です。

リスクを低減する多層構造の保護

Microsoft Azure 向けフォーティネットセキュリティファブリックを利用すれば、企業は責任共有モデルの枠組みに沿って、オンプレミスからクラウドまでの一貫したセキュリティ保護を適用することができます。Microsoft Azure を利用する企業では、包括的な多層構造のセキュリティと脅威防御が実現されます。同時に、運用、ポリシー管理、可視性を合理化し、セキュリティライフサイクル管理を強化することができます。

フォーティネットジャパン合同会社

〒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