SOLUTION BRIEF

フォーティネットのゼロトラストネットワークアクセスによるアプリケーションのアクセスとセキュリティの向上

概要

仕事場がオフィスから自宅へと大きくシフトしたことで、セキュリティや接続性に関する多くの課題が浮き彫りになっています。また、今日のネットワークは、複数のデータセンターやマルチクラウド環境に広く分散しています。企業にとっては、一貫したセキュリティポリシーを適用しながら、あらゆる場所から多様なアプリケーションへのセキュアなアクセスを可能にすることが極めて重要です。だからこそ、今日の企業はリモートアクセスを従来の仮想プライベートネットワーク（VPN）からゼロトラストネットワークアクセス（ZTNA）ソリューションへと進化させる必要があります。

ガートナー社は、2023 年までに企業の 60% が従来の VPN を段階的に廃止し、ZTNA モデルを使用すると予測しています [1]。

フォーティネットの ZTNA を利用することで、セキュアな接続が簡素化され、攻撃対象領域が縮小します。ユーザーは、認証と検証を受けてからでないと、特定のアプリケーションへのアクセスは許可されません。本ソリューションには、フォーティネット セキュリティ ファブリックに統合される製品スイートが含まれており、管理のしやすさとエンドツーエンドの可視化を実現します。

フォーティネットの ZTNA の利点

ゼロトラストネットワークアクセスソリューションを構築するには、クライアント、プロキシ、認証、セキュリティなど、さまざまなコンポーネントが必要です。しかし、ほとんどの組織では、複数のベンダーのソリューションを利用しています。さらに、コンポーネントは各種のオペレーティングシステム上で動作し、管理や構成にも異なるコンソールが使用されることが多いため、ベンダーをまたいだゼロトラストモデルの確立はほぼ不可能です。

フォーティネットのソリューションを利用することで、1 社のベンダー、そして単一のオペレーティングシステムで、ゼロトラストアクセスを簡単に確立することが可能になります。FortiOS 7.0 のアップデートにより、既に使用されているフォーティネットのインフラストラクチャを、ゼロトラストアーキテクチャの一部として利用することができます。FortiGate 次世代ファイアウォール（NGFW）と FortiClient エンドポイント保護では、管理を簡素化した ZTNA 機能を採用しています。ユーザーがネットワーク内部 / 外部のどちらにいても、同じ適応型のアプリケーションアクセスポリシーが使用されます。また、ZTNA を FortiOS に組み込むことで、フォーティネット セキュリティ ファブリックに緊密に統合されるため、容易な管理と優れた可視性を実現しています。

フォーティネットは、アプリケーションへのリモートアクセスを制御することで、リモートユーザー、ホームオフィス、および小売店などに ZTNA を適用し、従来の VPN よりも簡単かつ迅速にリモートアクセスを実現することができます。これにより、いっそうきめ細かなセキュリティ保護を提供しながら、より優れたユーザーエクスペリエンスを提供できます。アプリケーションが置かれている場所がデータセンター、プライベートクラウド、パブリッククラウドであろうと関係ありません。ユーザーとアプリケーションが地理的に離れていても、セキュアで信頼性の高い接続を実現できます。

フォーティネットの ZTNA コンポーネント

フォーティネットの ZTNA ソリューションは、以下で構成されています。

FortiGate NGFW：これらのネットワークファイアウォールは、ZTNA のプロキシポイントおよびポリシー適用ポイントとして機能します。導入された FortiGate は、仮想マシン（VM）を含め、ZTNA ソリューションの FortiOS プロキシポイントとして利用できます。FortiGate は、暗号化されたトンネルターミネーションと、アプリケーションアクセスを提供します。また、FortiOS はアプリケーションのセッションごとにユーザー検証とデバイスリスク評価を実行し、オンプレミスまたはクラウドのアプリケーションへのセキュアな接続を行います。

FortiGate または FortiClient を既にお使いのお客様は、FortiOS 7.0 へのアップグレードと同時に ZTNA の使用が可能になり、追加のライセンス料は必要ありません。

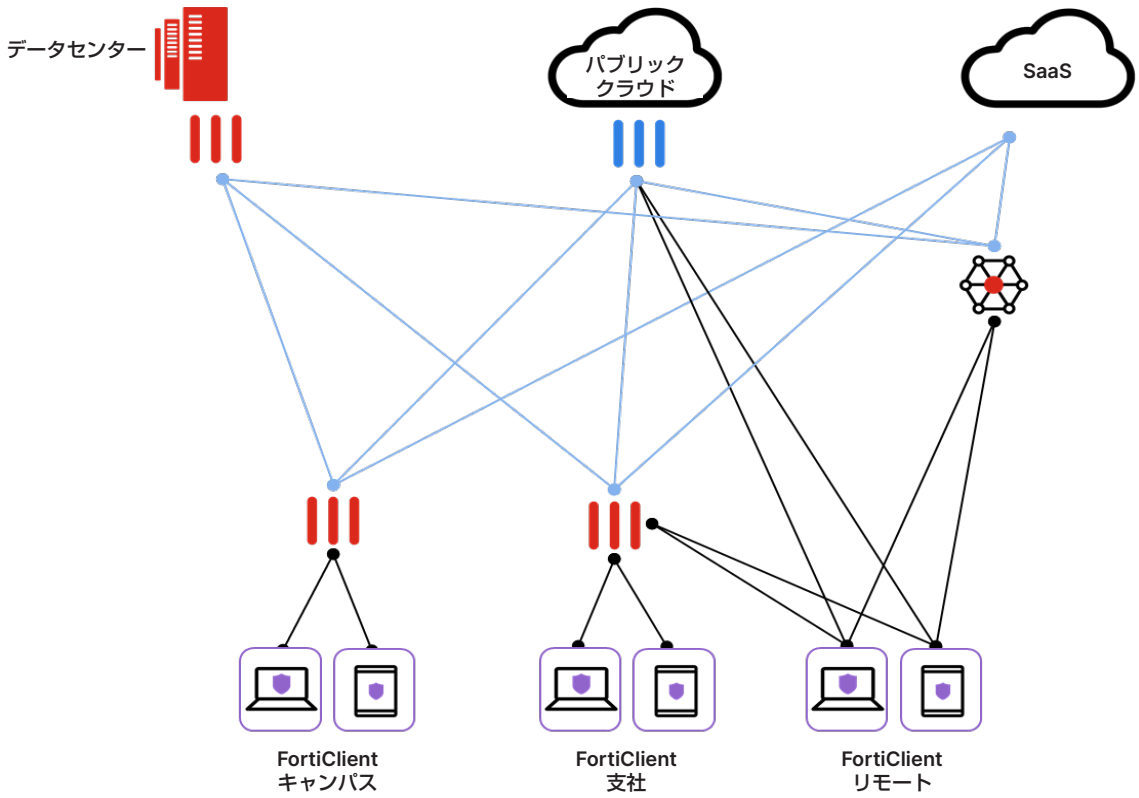
FortiManager 集中セキュリティ管理：セキュリティ ファブリック管理ソリューションにより、プロキシポイントの構成をすべての FortiGate に同時に適用することができます。

FortiClient エージェント：FortiClient は ZTNA エージェントとして機能し、エンドポイントデバイスにインストールされ、ZTNA 適用ポイント / プロキシポイント（FortiGate）への暗号化された ZTNA トンネルを自動的に作成します。

FortiClient Enterprise Management Server（EMS）：EMS は、ZTNA ソリューションを管理する ZTNA エージェントを構成し、非常に重要な役割を果たします。また、どの FortiOS プロキシポイントに接続すべきかをエージェントに知らせます。

フォーティネットの IAM（アイデンティティとアクセスの管理）：ネットワークにアクセスしようとするユーザーやデバイスのアイデンティティをセキュアで確実に検証するためのサービスを提供するもので、以下の製品が含まれます。

- **FortiAuthenticator：**シングルサインオン（SSO）などの一元認証サービスを提供します。
- **FortiToken：**二つ目の認証要素を追加し、ユーザーのアイデンティティを確認します（二要素認証）。



仕組み

フォーティネットのソリューションは、FortiOS 7.0 の新機能を活用し、ZTNA エージェントとして FortiClient を使用することにより、ZTNA 機能を実現しています。インターネット上のトラフィックを保護するために、デバイス上の FortiClient ZTNA エージェントは、デバイスから ZTNA 適用ポイント（FortiGate）まで、暗号化されたセキュアなトンネルを作成します。

このトンネルはオンデマンドで作成され、ユーザーには透過的であるため、VPN によるリモートアクセスで見られる主要な問題が解決されます。ネットワーク上のすべてのユーザーが機械的に信頼されているとはみなされなくなるため、ユーザーがネットワーク内部 / 外部のどちらにいても、同じトンネルが作成されます。

このアーキテクチャは、アプリケーションにもメリットをもたらします。ユーザーは FortiGate に接続した後、接続をアプリケーションにプロキシするため、アプリケーションの場所はオンプレミス、プライベートクラウド、パブリッククラウドのいずれであっても問題がない上に、インターネットからは見えない状態になっています。アプリケーションは FortiGate との接続を確立するだけでよく、執拗なハッカーやボットから身を隠すことができます。

分散したネットワークとユーザーのためのリモートアクセス保護

フォーティネットソリューションを使用することで、従来の VPN から ZTNA への移行が簡単に実現できます。FortiOS オペレーティングシステムに搭載されたテクノロジーにより、ユーザーやアプリケーションの場所に関係なく、セキュアで一貫したアクセスの提供が容易になりました。エンドユーザーエクスペリエンスは向上し、ネットワーク管理者にとっては管理が容易になります。さらに、継続的な検証とプロキシされたアプリケーションにより、攻撃対象領域が縮小します。フォーティネットの ZTNA ソリューションは、従来の VPN よりもセキュアなリモートアクセスを実現すると同時に、より優れたユーザーエクスペリエンスを可能にします。

フォーティネットの ZTNA は、SASE（セキュアアクセスサービスエッジ）サービスを必要としませんが、フォーティネットの SASE は、FortiOS 7.0 に移行する際に、FortiOS のプロキシポイントとして利用できます。SASE と ZTNA のサービスは、今後並行して提供できるようになります。

- ZTNA は、セキュアなアクセスとアプリケーションのアクセス制御を提供します。
- SASE は、ネットワークピアリングのほかに、FWaaS（Firewall-as-a-Service）、サンドボックス、データ漏えい対策（DLP）、セキュア Web ゲートウェイ（SWG）、マルウェア保護を提供します。

[1] 「Since Remote Work Isn't Going Away, Security Should Be the Focus」、Mike Wronski 著、Dark Reading、2020 年 9 月 24 日（英語）：https://www.darkreading.com/risk/since-remote-work-isnt-going-away-security-should-be-the-focus/a/d-id/1338848

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

SB-Zero-Trust-Network-Access-202107-R1