SOLUTION BRIEF

フォーティネットのセキュア SD-WAN による支社インフラストラクチャのアップグレード

エグゼクティブの皆様へ

ビジネスクリティカルなクラウドベースのアプリケーションやツールの使用が増加を続けています。これを背景に、複数のリモートオフィスを展開する分散型の企業は、パフォーマンスの低いワイドエリアネットワーク（WAN）から、ソフトウェア制御による WAN（SD-WAN）アーキテクチャへと移行しています。SD-WAN は、サービスとしてのソフトウェア（SaaS）ソリューションはもちろん、デジタル音声やビデオサービスにおいても、高速な接続、コストの削減、そして優れたパフォーマンスを実現します。しかしながら、SD-WAN には欠点もあります。特に、セキュリティは大きな課題となっています。

SD-WAN のグローバル市場では 40% を上回る年平均成長率（CAGR）が予測され、2022 年までに 45 億ドルに達すると見込まれています [4]。

フォーティネットの FortiGate 次世代ファイアウォール（NGFW）は、セキュリティ ドリブン ネットワーキングを実現するセキュア SD-WAN 機能を備えており、統合ソリューションとして提供しています。フォーティネットのソリューションは、瞬時の識別とインテリジェントなルーティングによってアプリケーションパフォーマンスを大幅に向上します。また、支社のネットワークパフォーマンス向上、セキュリティやコンプライアンスのリスク管理ワークフローの簡素化を両立します。

事業拠点の分散するエンタープライズは、SaaS アプリケーションや IP ベースの音声 / ビデオツールをはじめとするデジタルトランスフォーメーション（DX）テクノロジーの採用を推進し、生産性の向上、コミュニケーションの改善、急速なビジネスの成長をサポートしています。しかし、クラウドベースのツールやサービスはレガシーな WAN インフラストラクチャに大きな負担となっており、企業が求める極めて高いレベルのパフォーマンスを実現できません。

成長を続ける企業にとって、この問題はますます深刻になっています。先頃発表されたある報告書によると、SaaS アプリケーションを 1 つでも導入している企業は、全体の 60% を占めています [1]。その導入率も急速に上昇しており、全世界の SaaS 市場は 2018 年から 2023 年の間に 21.2% の年平均成長率（CAGR）で拡大するものと見込まれています [2]。その一方で、企業の IT 意思決定を行う担当者の 64% は、SaaS の導入にセキュリティ対応が追い付いていないと考えています [3]。

従来の WAN は、マルチプロトコルラベルスイッチング（MPLS）リンクを使用します。MPLS は接続のコストが高額であると指摘されますが、コスト以上に重要な点として、生産性についても考慮しなければなりません。従来の WAN のほとんどが「ハブ & スポーク」アーキテクチャを採用し、支社ネットワークのトラフィックをメインのデータセンターへと送信して、フィルタリングとセキュリティチェックを行います。

このアーキテクチャでは、保護を一元化できるもののレイテンシーが増大し、ネットワークパフォーマンスは低下することになります。この影響は、特に VoIP（Voice over IP）やビデオ会議テクノロジーのようなクラウドベースのツールで大きな問題になります。音声やビデオは大量のネットワークリソースを要するサービスであり、企業の従業員は高品質のパフォーマンスを期待しています。

これこそ、分散した事業拠点を持つ多くの企業が、古くなった WAN インフラストラクチャ刷新する DX イニシアチブに取り組んでいる最大の理由です。分散型の企業には、大幅な簡素化、優れたコスト効率、クラウド導入のサポート機能を備えた支社ネットワーキングというニーズが存在します。SD-WAN テクノロジーは、帯域幅コストやトラフィックレイテンシーといった問題の解決にその威力を発揮します。この結果、MPLS から、パブリックブロードバンド接続はもちろん、4G / LTE や 5G 無線接続への移行が可能になるのです。SD-WAN は、クラウドアプリケーションやサービスへの直接アクセスを可能にすることで、支社からクラウド、本社、他の支社へとネットワークトラフィックをルーティングします。これは、デジタルトランスフォーメーションを推進する企業が SD-WAN を選択する理由のひとつになっています。

SD-WAN の成功に不可欠なセキュリティ

SD-WANは、従来のWANに比べてより広範な接続オプション、パフォーマンス、そしてコスト面のメリットがあるものの、次のような欠点もあります。

- **複雑性：**SD-WAN アーキテクチャはトラブルシューティングが難しく、すべての支社の一元管理が困難だという特性があります。その結果、限られた人数の IT 担当者の負荷がさらに増加し、脅威防御にギャップが生じる原因になります。
- **セキュリティ：**インターネットを介した直接的なブロードバンドリンクへの移行は、データセンターを介したトラフィックのバックホールによる一元管理ができなくなるため、新たなリスクが生じます。SD-WAN を効果的に実装するには、エンタープライズインフラストラクチャ内にセキュリティ機能を追加して接続を保護し、大量のトラフィックのインスペクションを実行する必要があります。しかも、ネットワークパフォーマンスを犠牲にすることはできません。
- **暗号化されたトラフィックのインスペクション：**今日のネットワークトラフィックの 72% は SSL（Secure Sockets Layer）/ TLS（Transport Layer Security）によって暗号化されているにもかかわらず、SD-WAN ソリューションの大半はこのようなトラフィックのインスペクション機能を備えていません[5]。特に、サイバー犯罪者はマルウェアをネットワークに感染させてデータを窃取しようとしているため、このようなリスクに直面する企業は、暗号化されたトラフィックのインスペクションをネットワークエッジで実行するために、アプライアンスの追加購入を余儀なくされています。

高度なネットワーキングとセキュリティを融合したフォーティネットのセキュア SD-WAN

FortiGate 次世代ファイアウォール（NGFW）は、セキュア SD-WAN 機能を搭載しており、SD-WAN を採用する支社ネットワークに最適なネットワーキングとセキュリティの機能を単一のソリューションで提供します。一貫したポリシーの適用と一元管理により、すべての支社を効率的に保護します。また、DX の推進に伴うリスクを緩和することも可能です。

NSS Labs が初めて実施した、「ソフトウェア制御による WAN テストレポート」において、フォーティネットは「Recommended（推奨）」の評価を獲得し、唯一セキュリティ機能を提供できる SD-WAN ベンダーです[6]。また、FortiGate NGFW は、セキュリティ製品の出荷台数において世界第 1 位の実績を誇ります[7]。FortiGate は、NGFW と SD-WAN 機能を 1 つに融合することで、WAN の効率性向上とセキュリティの強化を実現します。

フォーティネットのセキュア SD-WAN は、次のような機能と特長を備えています。

アプリケーション識別とインテリジェントなパス自動制御

従来の WAN では、ユーザーエクスペリエンスの品質をアプリケーション毎に管理することは困難でした。その理由は、パケットルーティングを採用しているためアプリケーションを十分に可視化できない点にあります。

フォーティネットのセキュア SD-WAN は、「ファーストパケット識別」機能を活用し、データトラフィックの最初のパケットでアプリケーションを確実に識別します。この包括的な**アプリケーション識別**機能によって、社内全体でどのようなアプリケーションが使用されているか特定できるため、豊富な情報に基づいた SD-WAN ポリシー設定が可能になります。フォーティネットのセキュア SD-WAN は、5,000 種類を超えるアプリケーションが登録されているアプリケーション制御データベースを参照します。登録アプリケーションは、脅威のトレンドやデジタルネットワークの進化に伴って拡充され続けています。

アプリケーションの識別によって、**インテリジェントなパス自動制御**が可能になります。これは、特定のアプリケーションやユーザーに基づいて、ネットワーク帯域幅全体でアプリケーションルーティングの優先度を決定する機能です。セキュア SD-WAN のインテリジェントなパス自動制御は、状況に応じて最適な WAN リンク / 接続を動的に選択することにより、アプリケーション別のレベルで SLA を実現します。SoC4 ASIC を搭載する FortiGate NGFW は、業界最速のアプリケーションステアリングを実現し、比類ないアプリケーション識別パフォーマンスを発揮します。また、パフォーマンス低下を最小限に抑えながら詳細な SSL / TLS インスペクションも実行できます。フォーティネットのセキュア SD-WAN は、次のような関連機能を備えています。

- **WAN パス修復：**FEC（前方誤り訂正）により、リンクの劣化やノイズといった WAN の問題を解消します。これにより、データの信頼性が強化され、音声やビデオサービスをはじめとするアプリケーションのユーザーエクスペリエンスを改善します。FEC は、エラー訂正データをアウトバウンドトラフィックに付加することで、転送時に発生するパケットロスなどのエラーを受信側で修復できます。この機能は、リアルタイムアプリケーションの品質向上に役立ちます。
- **トンネル帯域幅集約：**アプリケーションの帯域幅要件が増大した場合、2 つのオーバーレイトンネルを統合することでパケット単位のロードバランシングとデリバリを行い、ネットワーク性能を最大限に高めます。
- **自動フェイルオーバー機能：**プライマリの WAN パスのパフォーマンスが低下した場合には、使用可能なリンクの中から最適なものに自動的にフェイルオーバーされます。自動フェイルオーバーを FortiGate NGFW に組み込むことで、エンドユーザーの設定を簡素化するだけでなく、エクスペリエンスと生産性を向上します。

NGFW のセキュリティとコンプライアンス

フォーティネットのセキュア SD-WAN は、エンタープライズクラスのセキュリティ機能と支社ネットワーキング機能を、FortiGate NGFW という 1 つのソリューションで提供します。下記の重要なセキュリティ機能が装備されています。

インターネットベース VPN の優れたコストパフォーマンスと、MPLS VPN のパフォーマンスと俊敏性は、SD-WAN の重要なメリットの 1 つです [8]。

- **SSL / TLS インスペクションと脅威保護：**マルウェアの可視化と侵入防御機能を備えているため、暗号化トラフィックのインスペクション用アプライアンスを別途追加する必要はありません。
- **Web フィルタリングサービス：**インターネットセキュリティを適用することで複雑さを軽減できるため、SWG（セキュア Web ゲートウェイ）デバイスを追加する必要はありません。
- **完全な脅威保護：**サンドボックス、マルウェア対策、侵入防止システム（IPS）を装備しています。
- **拡張性に優れたオーバーレイ VPN トンネル：**トラフィックの常時暗号化と機密性保持を、優れたスループットで実行します。
- **きめ細かい SLA 分析：**アプリケーショントランザクションの分析により、SLA の修正にかかる時間を短縮します。

セキュア SD-WAN によって実現するトラッキングとレポート機能は、ネットワーク侵害が発生した場合の罰金や訴訟費用といった副次的リスクを低減すると同時に、プライバシー保護法、セキュリティ関連の標準、業界の法規制への確実なコンプライアンスに役立ちます。このような機能を活用することで、脅威アクティビティのリアルタイム追跡、リスク評価、潜在的な問題の検知、問題の軽減が可能になります。また、ファイアウォールポリシーを監視し、コンプライアンス監査の自動化を推進することもできます。

フォーティネットの**セキュリティレーティングサービス**は、PCI-DSS（Payment Card Industry Data Security Standard：ペイメントカード業界データセキュリティ標準）をはじめとする法規制遵守のベストプラクティス、NIST（米国国立標準技術研究所）や CIS（Center for Internet Security）などのセキュリティ標準に対応する、リアルタイムのトラッキングとレポーティング機能を提供します。また、セキュリティ対策の評価を受けることができるため、同業他社との比較も可能です。

シンプルな管理、オーケストレーション、オーバーレイコントロール

SD-WAN の導入に際しては、広く分散したインフラストラクチャ全体でシームレスな導入と管理を可能にするツールが必要です。フォーティネットのセキュア SD-WAN は、直感的な統合管理コンソールを備えた FortiManager による管理が可能です。クラウドベースソリューションやホスト型ソリューション向けのオプションを備えているため、数千単位の分散拠点のリモート制御やオーケストレーションに対応します。FortiManager を活用することで、まさにプラグアンドプレイで FortiGate デバイスを機能させることが可能になります。FortiManager から一元的にポリシーやデイバス情報を構成することで、FortiGate デバイスを最新のポリシー構成へ自動更新できます。

SoC4 ASIC 搭載の FortiGate NGFW は、業界最速の SD-WAN セキュリティを提供します。これにより、**オーバーレイ VPN** の高速化や、WAN の包括的なユーザーエクスペリエンス向上が実現します。**クラウドオーバーレイコントローラー**オーケストレーションは、360 Protection Bundle サブスクリプションサービスで提供され、クラウドベースの自動プロビジョニングによってオーバーレイ VPN の導入を簡素化します。また、柔軟な一元管理機能も備えているため、すべての支社や拠点を対象にクラウドから拡張性のあるリモートセキュリティやネットワーク制御を実行できます。

総所有コスト

パブリックブロードバンドへの移行は、高額なコストの掛かる MPLS 接続を最もコスト効果に優れた接続へと刷新することを意味します。トランスポートに依存しないフォーティネットのソリューションは、アクティブ - アクティブモードで接続を使用することで、利用可能な帯域幅全体の効率的な活用が可能になります。フォーティネットのセキュア SD-WAN は、他社製品の 10 分の 1 という、業界で最も優れた TCO を実現します [9]。

セキュリティ ドリブン ネットワーキング

市場でさまざまな SD-WAN が提供されている現在、IT 部門の VP には慎重なソリューションの選択が求められています。フォーティネットのセキュア SD-WAN は、高度な SD-WAN 機能とその有効性が実証されている優れたセキュリティを融合することで、保護機能を損なうことなく支社オペレーションを効率化する、セキュリティ ドリブン ネットワーキングを実現します。

[1]「SaaS Adoption Rising（急増する SaaS の導入）」、Computer Economics、2018 年 11 月発行（英語）：
https://www.computereconomics.com/article.cfm?id=2253

[2]「Global Software-as-a-Service (SaaS) Market Outlook（2018-2023）（2018 ～ 2023 年の国際的な SaaS 市場に関する展望）」、Business Wire、2018 年 11 月 14 日発行（英語）：
https://www.businesswire.com/news/home/20181114005369/en/Global-Software-as-a-Service-SaaS-Market-Outlook-2018-2023-Expected

[3]「Businesses are adopting SaaS too fast to properly secure it（適切なセキュリティ対策なく SaaS の導入を急ぐ企業）」、Conner Forrest 著、TechRepublic、
2018 年 4 月 10 日発行（英語）：https://www.techrepublic.com/article/businesses-are-adopting-saas-too-fast-to-properly-secure-it/

[4]「SD-WAN Infrastructure Market Poised to Reach $4.5 Billion in 2022（SD-WAN 市場は 2022 年には 45 億ドル規模に拡大）」、IDC、2018 年 8 月 7 日発行（英語）：
https://www.idc.com/getdoc.jsp?containerId=prUS44203118

[5]「More Encrypted Traffic Than Ever（これまで以上に増加する暗号化トラフィック）」、John Maddison 著、フォーティネットセキュリティブログ、
2018 年 12 月 10 日発行（英語）：https://www.fortinet.com/blog/industry-trends/more-encrypted-traffic-than-ever.html

[6]「Fortinet SD-WAN gives the performance of a lifetime（最高レベルのパフォーマンスを提供するフォーティネットのセキュア SD-WAN）」、フォーティネット、
2018 年 8 月 9 日発行（英語）：https://www.fortinet.com/products/sd-wan/nss-2018.html

[7]「IDC Worldwide Security Appliances Tracker」、IDC、2018 年 4 月（年間出荷台数に基づく）（英語）：
https://www.idc.com/tracker/showproductinfo.jsp?prod_id=38

[8]「Understanding Virtual Private Networks (and why VPNs are important to SD-WAN)（VPN に関する基礎知識（および SD-WAN にとって VPN が重要な理由））」、
Zeus Kerravala 著、Network World、2018 年 4 月 13 日発行（英語）：
https://www.networkworld.com/article/3268744/internet-of-things/understanding-virtual-private-networks-and-why-vpns-are-important-to-sd-wan.html

[9]「Fortinet SD-WAN gives the performance of a lifetime（最高レベルのパフォーマンスを提供するフォーティネットのセキュア SD-WAN）」、フォーティネット、
2018 年 8 月 9 日発行（英語）：https://www.fortinet.com/products/sd-wan/nss-2018.html

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

SB-Upgrade-Branch-Infra-SD-WAN-201908-R1