SOLUTION BRIEF

一元管理で SD-WAN の運用を簡素化する

概要

リモートオフィスや支社では、従来型のネットワーキングに代わってソフトウェア制御によるワイドエリアネットワーキング（SD-WAN）が急速に普及しています。SD-WAN ソリューションには、優れたパフォーマンスによって新たなデジタルトランスフォーメーションをサポートするというメリットがありますが、その一方で、ネットワーキング機能とセキュリティ機能が統合されていないソリューションが数多く存在します。その結果、ネットワークの管理と保護を行うさまざまなツールやソリューションを組み合わせる必要が生じ、SD-WAN 環境は複雑になっています。ネットワーク部門のリーダーが求めているのは、コスト削減、効率化、リスク軽減をシンプルに実現できるアプローチです。このような要件すべてに対応できるのが、FortiGate セキュア SD-WAN です。NGFW（次世代ファイアウォール）に管理 / 分析機能を統合することにより、SD-WAN の運用を簡素化します。

イノベーションの支援と成長するビジネスの保護を両立

拠点が分散する企業は、SaaS（サービスとしてのソフトウェア）アプリケーションや音声 / ビデオツールをはじめとするリアルタイムアプリケーションなどのデジタルトランスフォーメーションの採用を進め、生産性の向上、コミュニケーションの円滑化、急成長するビジネスをサポートしています。ところが、多くの支社やリモートオフィスにある従来の WAN アーキテクチャでは、このような新しいテクノロジーのトラフィック要件を満たすことはできません。これが、ダイレクトインターネットアクセスを低コストで実現できる SD-WAN アーキテクチャが普及する要因となっています。SD-WAN の市場規模は、2018 年に 7 億ドル以上と推定されており、2019 年から 2025 年に 58% の年平均成長率で成長すると予測されています [1]。

ところが SD-WAN には、ネットワーキング帯域幅を増加させる一方で、リスクが増大する側面もあります。ガートナーの調査では、企業は WAN のパフォーマンスと可視性の改善を図る取り組みを続けていますが、現在の WAN に関する最優先課題はセキュリティであることが明らかになっています [2]。

SD-WAN のセキュリティ要件に応えようと、多くの組織のネットワークエンジニアリング / オペレーションのリーダーは、脅威の減災やコンプライアンスを目的とした単機能のツールや製品を複数導入しています。このアプローチでは、インフラストラクチャが複雑になり管理が煩雑化するだけでなく、ネットワークエッジにセキュリティギャップが発生してしまいます。

フォーティネットが実現する SD-WAN 環境の簡素化とセキュリティ

セキュリティ ドリブン SD-WAN ソリューションに必要なネットワーキングとセキュリティツールを統合することで、寄せ集めされた支社インフラストラクチャの複雑さを軽減できます。その結果、攻撃対象領域が縮小し、デジタルトランスフォーメーションのイニシアチブを推進できるだけでなく、ネットワーキングチームの運用作業も簡素化されます。

フォーティネットのセキュア SD-WAN は、ファブリックマネジメントセンターの一部として統合されているため、FortiManager の一部として提供される SD-WAN オーケストレーターの一元管理コンソールを活用し、FortiAnalyzer の強力な分析とレポートの機能を利用できます。セキュア SD-WAN オーケストレーターは、一元的な展開、飛躍的に簡素化すると同時に、自動化を通じて時間を節約し、ビジネス中心のポリシーを提供します。

フォーティネット、ファブリックマネジメントセンターで SD-WAN の運用を簡素化

- ゼロタッチ展開
- 一元管理
- レポーティングと分析
- コンプライアンスレポート
- 統合と自動化

ガートナーは、「WAN における最大の懸念事項はセキュリティである」という回答が 72% にのぼっていると指摘しています [3]。

Gartner

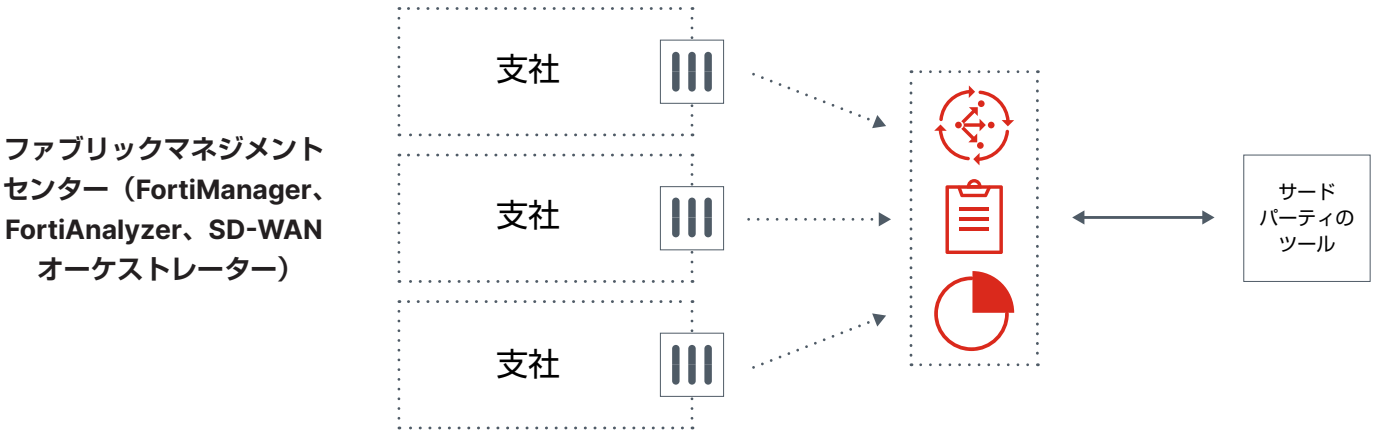


図 1：ファブリックマネジメントセンターを活用する SD-WAN のユースケース

ゼロタッチ展開

セキュア SD-WAN の導入では、ファブリックマネジメントセンターを使用することによって、作業に要する時間を数日からわずか数分に短縮できます。ファブリックマネジメントセンターのゼロタッチ展開機能では、支社オフィスで FortiGate デバイスを起動すると、本社の FortiManager がブロードバンド接続を介して自動設定が実行されます。これにより、現場に足を運ぶ時間とコストを節約できます。また、既存の SD-WAN 構成をテンプレートとして使用することで、新たな支社やリモートオフィスの大規模展開を短時間で実行可能になります。

拠点を分散する組織に適した一元管理

組織の分散ネットワーク全体を一元管理することで、サイバーリスクやネットワーク停止につながりかねない構成エラーが発生する確率を大幅に低減できます。

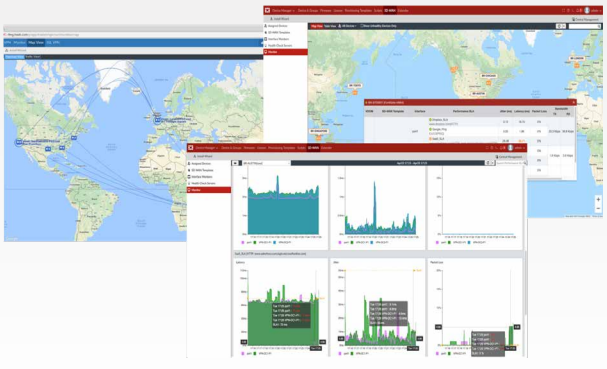
セキュア SD-WAN オーケストレーターは、ファブリックマネジメントセンターの一部として、一元的な展開、飛躍的に簡素化すると同時に、自動化を通じて時間を節約し、ビジネス中心のポリシーを提供します。フォーティネットの管理ツールは、競合他社のソリューションを大幅に上回る規模の環境をサポートでき、最大 10 万台の FortiGate デバイスの管理をサポートします。SD-WAN と NGFW のテンプレート、エンタープライズグレードの構成管理、ロールベースのアクセス制御といった機能は、ネットワークエンジニアリングおよびオペレーション部門で発生する人為的なミスの軽減に効果的です。

SD-WANのレポーティングと分析

WAN リンクの可用性、パフォーマンス SLA、実行時のアプリケーショントラフィックの分析と過去の統計情報の強化により、インフラストラクチャチームは、ネットワークの問題の迅速なトラブルシューティングと解決が可能になります。ファブリックマネジメントセンターは、アプリケーションの可視性とネットワークパフォーマンスの高度なテレメトリを提供することで、解決までの時間を短縮し、IT サポートチケットの数を削減します。オンデマンド SD-WAN レポートは、コンプライアンスで不可欠となる脅威の現状、信頼レベル、資産アクセスなどの実用的なインテリジェンスを提供します。

これには、SD-WAN 帯域幅監視レポートとデータセット、データセット / グラフ / レポートを使った SLA のロギングおよび履歴の監視、SLA アラートのカスタマイズ、アプリケーション使用状況レポート、そしてそれらを表示するダッシュボードが含まれます。また、SD-WAN イベントに対する適応型レスポンスハンドラー、アプリケーションとインタフェース全体の SLA に関するイベントのロギングとアーカイブも提供されます。

NSS Labs が実施したテストでは、FortiGate セキュア SD-WAN でゼロタッチ展開を使用することにより、支社をオンラインにする作業はわずか 6 分足らずで完了することが実証されています [4]。



コンプライアンスの徹底だけで、セキュリティは実現できません。コンプライアンスをベースラインと認識することで、サイバー攻撃への耐性を最大限に高めることができます[6]。

コンプライアンスレポート

監査でコンプライアンスを証明する作業では、カスタマイズ可能なレポートやツールが役立ちます。これまでのコンプライアンス管理は、ネットワークチームにとってコストと手間のかかるプロセスでした。フルタイムのスタッフ数人が何ヵ月もかけて複数の単機能ポイントセキュリティ製品からデータを収集し、正規化する作業が必要になることもあったのです。

フォーティネットは、セキュリティインフラストラクチャの簡素化と多くの手作業によるプロセスを排除することで、短時間でのコンプライアンスレポート作成を実現します。ファブリックマネジメントセンターには、準拠規格向けのカスタマイズ可能なテンプレートに加えて、PCI DSS（Payment Card Industry Data Security Standard）、SAR（Security Activity Report）、CIS（Center for Internet Security）、NIST（National Institute of Standards and Technology）をはじめとする標準向けのレポートが付属します。また、監査ログの作成や RBAC（ロールベースのアクセス制御）機能も提供しており、従業員のデータアクセスを業務上必要な情報のみに制限できます。

ファブリックマネジメントセンターでは、監査チェックを行う FortiGuard セキュリティレーティングサービスが拡張機能として提供されています。これにより、セキュリティ / ネットワーキングのチームは、セキュリティ ファブリックに存在する重大な脆弱性と構成上の弱点を特定し、ベストプラクティスに基づく推奨構成を実装することができます。また、このサービスでは、自社と業界内の他社のセキュリティ態勢を比較することも可能です[5]。

統合と自動化

セキュリティを効果的に実現するには、支社やリモートオフィスなど、分散した組織のあらゆる部分にセキュリティをシームレスに統合する必要があります。ネットワークエンジニアリングとオペレーションのリーダーは、攻撃対象領域全体を一元的に可視化しなければなりません。また、リソースの自動化により、リスクの検知から修正までに要する時間を短縮し、人手による作業負担を軽減することも重要です。

ファブリックマネジメントセンターは、フォーティネット セキュリティ ファブリック内の対応アクションをポリシーベースで自動化することにより、修正に要する時間を数ヵ月から数分へと短縮します。このファブリックは、セキュリティワークフローと脅威インテリジェンスの自動化を可能にする統合型のセキュリティアーキテクチャです。ある支社でインシデントが検知されると、コンテキストに基づく識別データがアラート送信されます。ネットワーク管理者は、この通知をもとに、組織全体を攻撃から保護するために必要な一連の対策を迅速に見極めることができます。また、一部のイベントにおいては、デバイス構成の自動変更をトリガーして反復的な攻撃を瞬時に阻止します。

さらに、FortiAnalyzer とファブリックマネジメントセンターは、SD-WAN タスクの多くを自動化することで、スタッフの負担を軽減します。いずれの製品も、SIEM（セキュリティ情報 / イベント管理）、ITSM（IT サービス管理）、DevOps（Ansible、Terraform）をはじめとするサードパーティ製ツールとも統合できるため、既存のワークフローを維持することが可能で、他のセキュリティ / ネットワーキングツールに対するこれまでの投資が無駄になることもありません。

価値、シンプルさ、セキュリティを実現

ファブリックマネジメントセンターは、エンタープライズクラスのセキュリティと支社のネットワーキング機能を提供し、次に示す業界トップクラスの優位性を実現します。

TCO の低減：セキュリティ ドリブン SD-WAN に向けたフォーティネットの統合アプローチは、ネットワーキング / セキュリティツールの統合によって CapEX（設備投資）を節約するとともに、シンプルな管理とワークフローの自動化を通じて OpEx（運用コスト）を抑えることにより、TCO（総所有コスト）を削減します。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（マルチプロトコルラベルスイッチング）による接続から、コスト効果に優れた接続への刷新を意味します。FortiGate 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[7]。

効率化：フォーティネットが SD-WAN 向けに提供するシンプルなインフラストラクチャは、支社レベルあるいは分散した組織全体のいずれにおいても、運用の複雑さを軽減します。FortiGate セキュア SD-WAN は、直感的な統合管理コンソールを使った一元管理が可能です。FortiManager を活用することで、FortiGate デバイスの本格的なプラグアンドプレイが可能になります。FortiManager では、一元的にポリシーやデバイス情報を構成し、FortiGate デバイスを最新のポリシー構成へと自動更新できます。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として、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。

リスク軽減：フォーティネットのトラッキングとレポート機能は、プライバシー保護法、セキュリティ関連の業界標準、業界の法規制へのコンプライアンスの確立はもちろん、ネットワーク侵害によって発生する罰金や訴訟費用といったリスクを軽減します。FortiAnalyzer は、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、問題の減災を支援する機能を備えています。FortiGate セキュア SD-WAN との緊密な統合を通じて、分散したビジネスインフラストラクチャ全体でファイアウォールポリシーを監視し、コンプライアンスに関する監査を自動実行します。

> データ侵害の平均コストは 392 万ドルに達しており、システムの複雑化に伴ってさらに 29 万ドルも増大します。コスト削減の方法として、インテリジェンスの共有（24 万ドル節減）とセキュリティアナリティクス（20 万ドル節減）を活用できます [8]。

フォーティネットが実現するセキュリティ ドリブン SD-WAN

セキュリティ ドリブン SD-WAN にはさまざまなユースケースがありますが、フォーティネットはあらゆるタイプの SD-WAN プロジェクトにおいて優れた効果を発揮するアプローチを採用しています。SD-WAN 運用の簡素化は、SD-WAN の実装と拡張を成功へと導く中心的な役割を果たし、デジタルイノベーションのイニシアチブを強力に支援します。フォーティネットセキュア SD-WAN とファブリックマネジメントセンターの組み合わせにより、トップクラスの SD-WAN 管理 / 分析機能が可能になり、運用コスト削減とネットワークエッジのリスク軽減をサポートします。

[1]「SD-WAN Infrastructure Market Poised to Reach $4.5 Billion in 2022」、IDC、2018 年 7 月（英語）

[2]「フォーティネット、2020 年 Gartner Peer Insights の WAN Edge インフラストラクチャ部門で Customers' Choice の 1 社に選出」、フォーティネット、2020 年 3 月 26 日：
https://www.fortinet.com/jp/corporate/about-us/newsroom/press-releases/2020/fortinet-recognized-as-2020-gartner-peer-insights-customers-choice-for-wan-edge-nfrastructure

[3]「Fortinet Secure SD-WAN: Best-of-Breed NGFW and SD-WAN in a Single Offering」、ガートナー、2018 年 11 月（英語）：
https://www.gartner.com/teamsiteanalytics/servePDF?g=/imagesrv/media-products/pdf/fortinet/fortinet-1-5VG5OU4.pdf

[4]「Software-Defined Wide Area Network Test Report: Fortinet FortiGate 61E」、Ahmed Basheer 著、NSS Labs、2019 年 6 月 19 日（英語）：
https://www.fortinet.com/content/dam/fortinet/assets/analyst-reports/ar-2019-nss-labs-sd-wan-test-report.pdf

[5]「Proactive, Actionable Risk Management with the Fortinet Security Rating Service」、フォーティネット、2019 年 4 月 5 日（英語）：
https://www.fortinet.com/content/dam/maindam/PUBLIC/02_MARKETING/02_Collateral/WhitePaper/wp-security-rating-service-solution.pdf

[6]「Compliance Is Not Security: Why You Need Cybersecurity Chops In The Boardroom」、Frances Dewing 著、Forbes、2019 年 8 月 15 日（英語）：
https://www.forbes.com/sites/theyec/2019/08/15/compliance-is-not-security-why-you-need-cybersecurity-chops-in-the-boardroom/#79c7fc2039b8

[7]「フォーティネット、2019 年のガートナー社 WAN エッジインフラストラクチャについてのマジック・クアドラントで、チャレンジャーの中で最も実行能力が高い位置づけと評価される」、フォーティネット、2019 年 12 月 4 日：
https://www.fortinet.com/jp/corporate/about-us/newsroom/press-releases/2019/challenger-with-highest-ability-to-execute-gartner-mq-wan-edge-infrastructure

[8]「2019 Cost of a Data Breach Report」、Ponemon Institute および IBM、2019 年 7 月（英語）：
https://securityintelligence.com/posts/whats-new-in-the-2019-cost-of-a-data-breach-report/

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-SD-WAN-Simplified-Operations-202109-R1