DATA SHEET

FortiOS 7.0

提供形態：

フォーティネットのセキュリティオペレーティングシステム

FortiOS 7.0 のリリースでは、フォーティネット セキュリティ ファブリックの機能がさらに拡張され、すべてのネットワーク、エンドポイント、クラウドの一貫した保護が、SASE や ZTNA（ゼロトラストネットワークアクセス）によってさらに強化されました。

FortiOS 7.0 では可視性と制御が拡張され、セキュリティポリシーの一貫した展開と適用を確実に実現し、分散ネットワーク全体での一元管理が可能になりました。

パフォーマンスや保護に妥協を強いられることなくビジネスを遂行できるようになり、シームレスなスケーラビリティのサポートと革新的なテクノロジーの容易な利用が実現します。

一貫性のある動的なセキュリティ態勢の実現により、あらゆる場所に展開されたアプリケーション、リソース、データ、サービスに対して、ユーザーやデバイスが世界中のどこからでもアクセスし、リスクに合わせた自動的な評価と調整が可能になります。

FortiOS 7.0 によって実現されるフォーティネット セキュリティ ファブリックは、以下の機能を提供します。

セキュリティ ドリブン ネットワーキング

ネットワークとセキュリティのコンバージェンスにより、あらゆるエッジへの拡張が可能な単一の統合システムを提供

ゼロトラストアクセス

接続されているすべてのユーザーとデバイスの認識と制御

アダプティブクラウドセキュリティ

マルチクラウドインフラとアプリケーションの俊敏かつ自動的な保護と制御

ハイライト：新機能

ネットワーキング

- SD-WAN の高度なルーティングの強化

セキュリティ

- FortiGuard ビデオフィルタリングサービス
- DNS インスペクションによる ACME サポートの強化
- ゼロトラストネットワークアクセスの新しいソリューション
- AI ベースのマルウェア検知

管理

- マルチ VDOM モードでのセキュリティ ファブリックのサポート
- ファブリック デバイスによる自動化ルールのトリガー
- セキュリティレーティングオーバーレイ

概要

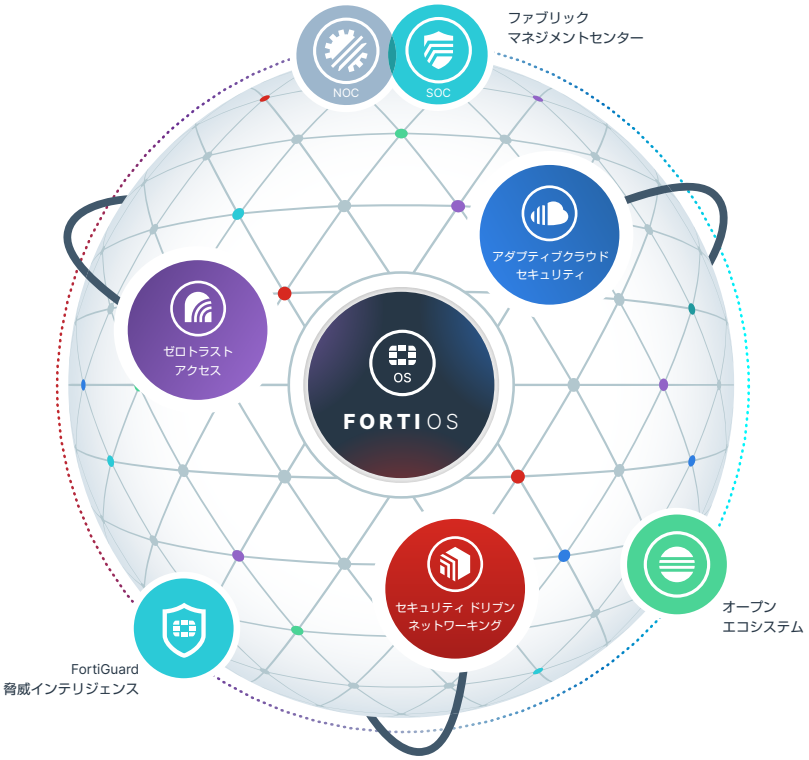
FortiOS 7.0 のご紹介

デジタルイノベーション

組織がデジタルイノベーションを加速させるには、自らのセキュリティが今日の複雑で急速に進化する脅威に確実に対応できるようにすることが極めて重要です。データセンター、WAN、LAN、LTE、オフネット、コンピューティング、OT 環境、CASB、SASE、インターネット、さらには、最近ではホームエッジなどにおいて、ネットワークエッジが爆発的に拡大したことで、インフラストラクチャの境界が曖昧になりました。

ネットワークエッジの急速な拡大によって多くのテクノロジーが必要とされるようになり、互いに連携して動作できなくなっています。デジタルイノベーションによる進化の多くは、統一されたセキュリティ戦略やフレームワークが存在しない、断片的な方法で進められてきました。ほとんどの組織で、ネットワークの 1 つの機能やセグメントを個別に保護することを前提に設計された、多種多様で分離されたセキュリティツールが利用されています。

ベンダーやソリューションが乱立しているため、ネットワーク全体の可視化や一貫したポリシーの適用の維持は極めて困難であり、ましてや、期待される高パフォーマンスのユーザーとアプリケーションの接続を目的に導入されたさまざまなセキュリティやネットワークのソリューションのメンテナンスや監視はほぼ不可能です。さらには、これまで以上に急速に形を変え、変化し、拡大する脅威に先行するのは不可能です。



このアプローチのスケーラビリティの欠如が、ビジネスを遅らせ、リスクと複雑さを増大させています。IT にも進化が求められています。

フォーティネットが開発した統合サイバーセキュリティプラットフォームであるフォーティネット セキュリティ ファブリックは、拡大するデジタル攻撃対象領域の保護をエコシステムを活用して可能にすることで、デバイス、データ、アプリケーションの広範で統合され、自動化されたセキュリティを実現します。

すべてのポートフォリオとソリューションピラーにわたって 300 以上の新機能が追加されたため、セキュリティ ファブリック、AI を活用した FortiGuard セキュリティサービス、および自動レスポンスの機能を利用し、ネットワーク、エンドポイント、マルチクラウドでのデータ、ユーザー、デバイス、アプリケーションの移動の継続的かつ脅威に先んじた保護が可能になります。フォーティネットのファブリックマネジメントセンターは、あらゆる規模の組織の SOC、NOC、IT インフラストラクチャの保護と簡素化を可能にします。また、新しい SOCaaS と Best Practice Service（BPS）は、包括的なセキュリティ態勢の最適化を支援します。

ハイライト

セキュリティ ファブリック

機能	ハイライト	フォーティネットの優位性
システム統合	▪ 迅速なセットアップ用の GUI コネクタを介したフォーティネット製品とのネイティブ統合 ▪ サードパーティソリューションサポートによる標準ベースのデータ交換 API のサポート ▪ 標準ベースのモニタリング出力：SNMP Netflow / sFlow および Syslog から外部 / サードパーティの SIEM、SOAR およびログ管理システムへの出力のサポート ▪ エンドポイント / アイデンティティインフラストラクチャの統合 ▪ 外部の脅威フィードの統合 ▪ **新機能：**複数の仮想ドメイン環境でのセキュリティ ファブリックのサポート	▪ 組織の既存のシステムを再利用可能なため、TCO を削減してプロセスを合理化できます。 ▪ 外部ソリューションとシームレスに統合することにより、セキュリティと運用の機能を拡張します。
管理とプロビジョニングの一元化	▪ API と CLI スクリプトによるフォーティネット / サードパーティの自動化およびポータルサービスのサポート ▪ クラウドベースのプロビジョニングソリューションを含む迅速な導入機能 ▪ 複雑な統合に対応する開発者コミュニティプラットフォームおよびプロフェッショナルサービスのオプション ▪ Ansible と Terraform 用の広範な統合リソース	▪ 包括的な API と CLI コマンドにより、豊富な機能を提供するサービスを強化します。 ▪ 迅速な包括的導入オプションにより、時間とコストの削減を可能にします。 ▪ Fortinet Developer Network（FNDN） が、大規模サービスプロバイダーおよびエンタープライズによる実装 / カスタマイズ / 統合に関する情報の共有を促進します。
クラウドと SDN の統合	▪ クラウドおよび SDN コネクタを使用したマルチクラウドのサポート：AWS、Microsoft Azure、GCP、OCI、AliCloud、VMware ESXi、NSX、OpenStack、Cisco ACI、Nuage Virtualized Service Platform ▪ プライベート / パブリッククラウド用 Kubernetes コネクタ ▪ **新機能：**特定の GUI アクションの背後にある REST API コマンドの表示	▪ 堅牢で包括的な SDN との統合機能により、俊敏性を損ねることなく確実にクラウドソリューションを実装できます。

ハイライト

機能	ハイライト	フォーティネットの優位性
可視性	▪ リアルタイム / 過去の脅威ステータスとネットワーク使用状況を、包括的なコンテキスト情報とともに表示するインタラクティブドリルダウンビューアーとトポロジービューアー ▪ ファブリックデバイスから提供される集約データビュー	▪ ワンクリックで改善を実行する機能により、脅威と悪用からの保護を正確かつ迅速に実現します。 ▪ 独自の脅威スコアシステムで重み付けされた脅威を特定ユーザーに相関させ、調査を優先付けします。 ▪ ファブリック全体ビューでは、単一セキュリティエンティティにとどまらない広範な可視化が可能であるため、問題を迅速に特定して解決できます。
自動化	▪ 定義されたトリガーに基づいてフォーティネット セキュリティ ファブリックで適切なアクションを実行する、ウィザードベースの自動化ワークフロー ▪ EMS 経由の FortiClient、または FortiSwitch / FortiAP 経由の接続を使用した、感染ホストの自動隔離 ▪ **新機能：**ファブリック デバイスによる自動化ルールのトリガー	▪ 侵害リスクを軽減し、人手によるセキュリティプロセスを自動化することで、予算の削減や人材不足の問題を解決できます。
NAC	▪ FortiAuthenticator および多様な外部 ID 管理システムのユーザー認証プロセス用インタフェース ▪ 多様なシングルサインオンの ID 取得方法（Windows AD、ターミナルサーバー、アクセスポータル、メールサーバーを含む） ▪ 組み込みトークンサーバーで、物理およびモバイルの両方のトークンを管理し、VPN アクセスや FortiGate の管理などの FortiOS の多様な認証のニーズに対応するために使用可能 ▪ **新機能：**モバイルエンドポイント向けに ZTNA（ゼロトラストネットワークアクセス）フレームワークを強化	▪ FortiOS は広範な AAA サービスと統合し、ユーザーアクセスの制御をさまざまなエントリーポイントから推進し、これによってユーザーの操作を簡素化しながらセキュリティを強化できます。 ▪ ユーザーおよび管理者のアクセス向けの二要素認証を、コストを抑えて簡単に導入できます。 ▪ ゲートウェイ保護との一貫性のあるクライアントのセキュリティプロファイルを簡単に配布してアップデートすることにより、モバイルユーザーに対するセキュリティの実施を簡素化します。
コンプライアンスとセキュリティレーティング	▪ 事前に定義したチェックリストを使用してファブリックデバイスのシステム構成を定期的にチェックし、セキュリティ態勢のステータスの変化の確認や保存したデータによる履歴トレンドチャートの作成が可能 ▪ PCI コンプライアンス要件に対する監査のセットアップ ▪ セキュリティレーティングランキングはピアに対するベンチマーク	▪ コンプライアンスの監査を自動化することにより、管理リソースを開放します。 ▪ ファブリック内の接続デバイスのステータスと状態をすばやく確認し、大きなリスクになる可能性があるギャップを特定します。
高度な脅威保護（ATP）	▪ ローカルファイルの隔離（ストレージ付きモデルの場合） ▪ 外部のフォーティネットファイル分析ソリューション（FortiSandbox）から、動的な修正（不正ファイルのチェックサムと URL）DB のアップデートと詳細な分析レポートを受信 ▪ 脆弱性の高いクライアントの詳細を提示するエンドポイント脆弱性ビュー ▪ IOC サービスの統合により、FortiAnalyzer の IOC 検知データを FortiView やトポロジーマップに表示	▪ 業界で実証された実績ある AV リサーチサービスによってサポートされます。 ▪ モバイルユーザーや支社も対象範囲に含む堅牢な ATP フレームワークを採用できます。これにより、暗号化ファイルを含む多様な経路からのファイルを評価し、従来の防御をバイパスする可能性のある高度な攻撃を検知して阻止します。 ▪ ファブリック内の脆弱性が存在するホストを容易に特定します。 ▪ 管理者が疑いのあるホストを容易に特定し、迅速または自動での隔離が可能になります。

ハイライト

機能	ハイライト	フォーティネットの優位性
無線 LAN コントローラ	▪ 室内、屋外、およびリモートモデルを含むフォーティネットの広範な AP フォームファクター向けに統合された無線 LAN コントローラ（ライセンスやコンポーネントの追加料金は不要） ▪ 不正 AP からの保護、無線セキュリティ、監視、およびレポート作成などのエンタープライズクラスの無線ネットワーク管理機能 ▪ 802.3ax AP をサポート	▪ 無線 LAN コントローラを FortiGate コンソールに統合することで、利便性と TCO 削減のメリットを提供する真の一元管理を実現します。
スイッチコントローラ	▪ フォーティネット製アクセススイッチ向けの統合スイッチコントローラ（追加のライセンスやコンポーネントは不要） ▪ NAC の展開を簡素化	▪ アクセスレベルのセキュリティの拡張によって、ターミナル間の脅威の阻止と保護を実現します。
WAN インタフェースマネージャ	▪ 統合されたモデム、USB ポート、または FortiExtender を介した LTE 接続をサポート	▪ WAN 向けに 3G / 4G 接続の使用や追加を可能にするとともに、アクセス制御を維持してこれらのリンクの使用を定義できます。

オペレーション

機能	ハイライト	フォーティネットの優位性
構成	▪ 多様な構成ツール：iOS アプリ、Web UI、CLI ▪ 直感的で使いやすい最先端の GUI とウィザード ▪ ログビューアー、ダッシュボードウィジェット、ポリシーテーブルなどの間でのワンクリック操作によるアクセスとアクション ▪ インテリジェントなオブジェクトパネルによるポリシーのセットアップと編集	▪ 管理者は独自の FortiExplorer 構成ツールを使用して、携帯電話やタブレットなどから構成に迅速にアクセスできます。 ▪ VPN ウィザードにより、一般的なモバイルクライアントや他のベンダーの VPN ゲートウェイのセットアップが容易になります。 ▪ 便利なワンクリックのアクセスとアクションにより、管理者は素早く正確に手続きを進めることができるので、脅威の減災や問題解決を迅速に実行できます。
ログおよびレポート	▪ コンプライアンス、監査、および診断に不可欠な詳細なログと、導入後すぐに利用可能なレポート ▪ FortiAnalyzer、FortiAnalyzer Cloud、および FortiGate Cloud へのリアルタイムのロギング ▪ CEF（共通イベント形式）のサポート ▪ セキュリティ ファブリック内のロギングの統合	▪ 送信元デバイスの詳細、強力な監査証跡を含む詳細なコンテキスト情報を提供します。 ▪ GUI レポートエディターにより、レポートを詳細にカスタマイズできます。 ▪ ログのホリスティック管理によって構成が簡素化され、すべての FortiGate の重要な情報を一元的に収集して分析に利用できるようになります。インテリジェンスのギャップが解消されます。
診断	▪ 診断用 CLI コマンド、セッショントレーサー、およびパケットキャプチャによるハードウェア、システム、およびネットワークのトラブルシューティング ▪ CLI のハードウェアテストスイート ▪ ポリシーとルーティングの GUI トレーサー	▪ 包括的な診断ツールが、迅速に問題を減災したり異常状態を調査したりする上で役立ちます。

ハイライト

機能	ハイライト	フォーティネットの優位性
監視	▪ リアルタイム監視 ▪ NOC ダッシュボード ▪ FortiExplorer アプリによる iOS プッシュ通知	▪ ダッシュボードの NOC ビューで、ミッションクリティカルな情報を常に表示できます。インタラクティブなドリルダウンウィジェットを利用することで、調査が行き詰まることなく迅速かつスムーズに分析を実行できます。

ポリシーおよび制御

機能	ハイライト	フォーティネットの優位性
ポリシーモード	▪ 独自のセクションまたはグローバルビューのオプションを含む、使いやすいポリシー管理 ▪ NGFW メモリベースモードとポリシーベースモード ▪ 統合された IPv4 および IPv6 ポリシー	▪ 多様な制御システムによる柔軟なポリシー設定を活用し、自社ネットワークに関連する効果的なネットワークセキュリティを実装できます。
デバイスの識別	▪ ネットワーク上のさまざまなタイプのデバイスの識別 ▪ MAC アドレスのポリシー送信元オブジェクト ▪ IoT セキュリティサービスにより、FortiGate による FortiGuard サーバーへのデバイスの詳細情報のクエリが可能	▪ 私物デバイスの識別により、今日の BYOD 環境に重要なセキュリティ機能を追加できるように企業を支援します。
SSL インスペクション	▪ AV やコンテンツフィルタリングなどのさまざまなセキュリティ制御機能を活用し、SSL 暗号化トラフィックを効果的に検証 ▪ コンテンツプロセッサによる高性能 SSL インスペクション ▪ 定評あるサイトのデータベースによる除外機能	▪ パフォーマンスに大きな影響を与えることなく、暗号化されたトラフィックに隠されている脅威を識別してブロックします。

セキュリティ

機能	ハイライト	フォーティネットの優位性
ファイアウォール	▪ SPU を搭載するアプライアンスによる高性能ファイアウォール ▪ 送信元のオブジェクト、IP、ユーザー、および / またはデバイスの組み合わせを使用するセキュリティポリシーの実装 ▪ ユーザー / 攻撃者の自動または手動の隔離 ▪ 登録された FortiClient にホストの隔離を指示	▪ 優れた費用対効果をもたらす、業界トップレベルのファイアウォールアプライアンス
VPN	▪ さまざまなタイプの VPN セットアップに対応する包括的なエンタープライズクラスの機能 ▪ 改善された SSL および IPsec VPN のウィザード ▪ フルメッシュ、ハブ & スポークトポロジーをサポートするクラウド活用型オーバーレイコントローラ VPN（ADVPN オプションが必要）	▪ FortiGate の比類ない VPN パフォーマンスによって、カスタムセキュリティプロセッサ（SPU）を活用してネットワークトラフィックの暗号化と復号を加速することで、複数のネットワークおよびホストの間で安全な通信を確立してデータの機密性を保持します。

ハイライト

機能	ハイライト	フォーティネットの優位性
IPS および DoS	▪ ゼロデイ攻撃の脅威保護と効果的な IPS の実装の研究に支えられた、通常のシグネチャとレートベースのシグネチャ ▪ DoS に対する統合保護機能による、異常なトラフィックの挙動からの防御 ▪ IPS シグネチャ向けの CVE の参照	▪ 卓越したカバレッジとコスト / パフォーマンスに対して NSS の「Recommended（推奨）」評価を獲得した、実証済みの高品質な保護を実現します。 ▪ コンテキストの可視性などの完全な IPS と NGIPS の機能により、エンタープライズのニーズに対応します。 ▪ スニファーモードなどの多様なネットワーク導入要件をサポートし、一部のモデルではアクティブバイパス機能を持つデバイスや内蔵バイパス機能を持つポートとの互換性を提供します。
Web およびビデオのフィルタリング	▪ クオータ、ユーザーオーバーライド、透過的セーフサーチ、サーチエンジンのキーワードのログ管理を含む、エンタープライズクラスの URL フィルタリングソリューションを提供 ▪ 広いカバレッジで 70 言語以上の URL レーティングを提供し、リダイレクト先（キャッシュおよび変換）サイトを識別 ▪ **新機能：** FortiGuard のカテゴリベースのフィルターや YouTube の API とパラメータを使用したビデオフィルタリング	▪ 統合アプリケーション制御および IPS による多層型のアンチプロキシ回避機能により、Web の使用状況に対する隙のない制御機能の実装が可能です。
E メールフィルタリング	▪ 誤検知率の低い効果的な多層型スパムフィルター	▪ 小規模組織および支社向けとして、追加システムへの投資を必要とせずにコスト効率の高いアンチスパムソリューションを提供します。
アプリケーション制御	▪ ネットワーク使用状況を可視化しながら、アプリケーションに基づいてトラフィックの異常を検知し、アクションを実行 ▪ SalesForce、Google Docs、Dropbox などの一般的なクラウドアプリケーションにおけるきめ細かな制御	▪ デスクトップおよびモバイルのアプリケーションの両方を含む広いカバレッジを対象として、ネットワークアクセスポリシーの管理を強化します。 ▪ パブリッククラウドサービスを利用するエンタープライズが増加する中、より詳細なアプリケーションのインスペクションを適用して制御と可視性を向上します。
アンチマルウェア	▪ フローベースおよびプロキシベースの AV オプションとして、保護機能やパフォーマンスを選択可能 ▪ IP レピュテーション DB を使用するアンチボット保護でボットと C&C サーバーの通信を切断 ▪ 外部のフォーティネットファイル分析ソリューション（FortiSandbox）から、動的な修正（不正ファイルのチェックサムと URL）DB のアップデートと詳細な分析レポートを受信 ▪ プロアクティブな保護レイヤーである Virus Outbreak Protection Service の追加により、リアルタイムの FortiGuard チェックサムデータベースを利用して脅威を比較、検知し、新たなマルウェアもブロック ▪ コンテンツ無害化（CDR）により、ユーザーにエクスプロイト可能なコンテンツが到達する前に除去 ▪ **新機能：** AI を活用したヒューリスティック検知エンジン	▪ 業界で実証された実績ある AV リサーチサービスによってサポートされます。 ▪ モバイルユーザーや支社も対象範囲に含む堅牢な ATP フレームワークを採用できます。これにより、暗号化ファイルを含む多様な経路からのファイルを評価し、従来の防御をバイパスする可能性のある高度な攻撃を検知して阻止します。
Protective DNS	▪ 既存の DNS プロトコルとアーキテクチャを使用して DNS クエリを分析し、脅威を減災	▪ ネットワークエクスプロイトのライフサイクルのさまざまなポイントでの防御により、フィッシング、マルウェアの拡散、コマンド＆コントロール、ドメイン生成アルゴリズム、コンテンツフィルタリングに対応します。

ハイライト

セキュリティ

機能	ハイライト	フォーティネットの優位性
SD-WAN	▪ インテリジェント WAN パス制御により、3,000 以上のアプリケーションおよびユーザー / ユーザーグループに基づいて WAN リンク間でトラフィックをダイレクト ▪ アプリケーショントランザクションの遅延、ジッター、パケットロスなどを測定し、自動フェイルオーバーの内蔵によって優先パスを判断することで、ビジネスクリティカルアプリケーションの最適なアプリケーションパフォーマンスを実現 ▪ QoS、トラフィックシェーピング、およびポリシールーティングを帯域幅管理に使用 ▪ ピアツーピアおよびリモートユーザーの WAN 最適化とバイトキャッシングのテクノロジー ▪ **新機能：**パッシブ WAN ヘルス測定	▪ 幅広いアプリケーション可視性と先頭パケット分類による効率的な SD-WAN を実現します。 ▪ NGFW と SD-WAN を同一アプライアンスに統合することで、TCO と複雑さのさらなる削減を可能にします。 ▪ WAN パスコントローラの自動化により、優れたアプリケーションパフォーマンスを持続します。 ▪ 業界トップクラスの IPsec VPN パフォーマンスを提供します。 ▪ SD-WAN エッジのゼロタッチ展開が可能です。
明示的プロキシ	▪ 1 つまたは複数のインタフェースでの IPv4 / IPv6 トラフィックの HTTP / HTTPS、FTP over HTTP、または SOCKS の明示的プロキシ ▪ トランスペアレント Web プロキシ	▪ エンタープライズクラスの統合された明示的 Web プロキシにより、HTTP および HTTPS のプロキシを提供し、UTM のセキュリティとユーザー識別のメリットが追加されます。
IPv6	▪ ルーティング、NAT、セキュリティポリシーなどの包括的な IPv6 サポート	▪ 既存のネットワークや重要ネットワークへの導入において柔軟な運用モードのオプションが選択可能で、ネットワーク変更の必要性を低減します。
高可用性	▪ 単一構成で複数の高可用性ソリューションの統合を実現し、業界標準の VRRP と多様な独自ソリューションをサポート	▪ 柔軟な高可用性機能により、ネットワーク環境と SLA の要件に基づいて最適なソリューションを選択できます。
ルーティング / NAT	▪ 包括的なルーティングプロトコルと NAT のサポート ▪ ICAP と WCCP のサポートによるトラフィックのリダイレクト	▪ 通信事業者やエンタープライズにおけるネットワークの耐障害性要件に対応する広範なルーティング機能を提供します。
L2 / スイッチング	▪ インタフェースからのソフトウェアスイッチの作成および VLAN スイッチのエミュレーション ▪ 複数のインタフェースによる SPAN ポートとポートアグリゲーションのサポート ▪ 802.1x やキャプティブポータルなどのインタフェースでのアクセス制御モードの実装 ▪ Wi-Fi および WAN インタフェースの包括的な構成オプション ▪ VXLAN および EMAC VLAN のサポート	▪ 柔軟なインタフェース構成により、組織のネットワーク要件に適した多様なセットアップオプションを採用でき、さらにアクセスセキュリティのオプションを利用できます。
オフライン インスペクション	▪ スニファーモードにより、ネットワークアクティビティの脅威と使用状況の監視をオフラインで実行	▪ 通信事業者やエンタープライズにおけるネットワークの耐障害性要件に対応する広範なルーティング機能を提供します。
基幹ネットワーク サービス	▪ DHCP、DNS サーバー、NTP サーバーなどの豊富なネットワークサービス	▪ 導入後すぐに使用可能な組み込みの機能により、必要なネットワークサービスの内部ターミナルに迅速な提供や、他のネットワークデバイスの統合も可能です。

ハイライト

サポートするプラットフォーム

機能	ハイライト	フォーティネットの優位性
物理アプライアンス（SPU 搭載）	▪ アクセラレーションコンポーネント（SPU）やマルチコアプロセッサをはじめとする独自のハードウェアアーキテクチャとの統合	▪ ソフトウェアおよびハードウェアの優れた統合機能がハードウェアコンポーネントの最適な利用を実現し、費用対効果を最大限に向上させます。
仮想システム	▪ 仮想ドメイン（VDOM）：仮想 FortiOS コンポーネントを単一の仮想または物理アプライアンス上の複数の論理システムに配置 ▪ グローバルセキュリティプロファイル ▪ ルーティングテーブルの複数のインスタンスが存在し同時に機能できるようにする、仮想ルーティングおよびフォワーディング（VRF）のサポート ▪ タスク分割をサポートする VDOM（仮想ドメイン）	▪ 導入後すぐに使用可能な組み込みの機能により、必要なネットワークサービスの内部ターミナルに迅速な提供や、他のネットワークデバイスの統合も可能です。
ハイパーバイザー	▪ VMware vSphere、Citrix、およびオープンソースの Xen、KVM、および MS Hyper-V を含む一般的なハイパーバイザープラットフォームのサポート	▪ 物理および仮想のアプライアンス間における一貫性のある管理と機能により、管理コストを削減して導入を簡素化します。
クラウド	▪ パブリッククラウドサービスのサポート：Amazon Web Services（AWS）、Microsoft Azure、Google Cloud Platform（GCP）、Oracle Cloud Infrastructure（OCI）、AliCloud	▪ 物理およびクラウドのプラットフォーム間における一貫性のある管理と機能により、管理コストを削減して導入を簡素化します。
ホスティング（FortiSASE SIA）	▪ **新機能：**FWaaS および FortiSASE SIA のホスティング型 SWG コンポーネントを活用	▪ SASE は、ネットワーキングやセキュリティの機能を通常の範囲を超えて拡張することで、あらゆる場所にいるユーザーが FWaaS（Firewall-as-a-Service）、SWG（セキュア Web ゲートウェイ）、ZTNA（ゼロトラストネットワークアクセス）などの脅威検知機能を利用可能になります。

技術仕様

セキュリティ ファブリック

システム統合

セキュリティ ファブリックのロギング :
- FortiAnalyzer 構成へのロギングを FortiGates 間で同期
- FortiAnalyzer とのデータ交換（トポロジーやデバイスのアセットタグなどの情報）

テクノロジーエコシステムはファイアウォール / ネットワークリスク管理、SDN / 仮想化、セキュリティ情報 / イベント管理（SIEM）、システム統合、テストとトレーニング、および無線の各市場をリードするパートナーを包含します。

FortiSandbox、FortiSandbox Cloud、FortiMail、FortiNAC、FortiMail Cloud、FortiProxy、FortiAI、FortiDeceptor、FortiTester、および FortiWeb とのネイティブ統合

管理とプロビジョニングの一元化

一元管理サポート : FortiManager、FortiCloud ホストサービス、Web サービス API

迅速な導入展開 : インストールウィザード、USB 自動インストール、ローカルおよびリモート環境でのスクリプト実行

クラウドと SDN の統合

コネクターを介した統合 :
- パブリッククラウド : AWS、MS Azure、GCP、OCI、AliCloud、IBM Cloud
- プライベート SDN : Kubernetes、VMware ESXi および NSX、OpenStack、Cisco ACI、Nuage Networks、Nutanix Prism

API プレビュー : 特定の GUI ページで使用されるすべての REST API リクエストを表示

可視性

ユーザー、デバイス、ネットワーク、およびセキュリティに関連するアクティビティ向けのインタラクティブでグラフィカルな可視化ツール（FortiView）:
- 「送信元」、「送信先」、「アプリケーション」、「脅威」などの異なる視点を使用して現在および過去のステータスを表示する多様な GUI コンソール
- 脅威 / VPN マップ
- データ表示オプション : テーブル、バブルチャート、または世界地図（該当する場合）
- 接続ファブリック対応デバイスに関する統計情報およびシステム情報
- セッション表示の高速化
- FortiView およびログテーブル内でのパブリック IP アドレスの WHOIS ルックアップ

物理 / 論理トポロジービューによる表示 :
- セキュリティ ファブリックネットワーク内のホストの場所
- ホストの隔離、IP 制限、アクセス詳細コンテキスト情報へのワンクリックアクセス
- セキュリティ ファブリックエンティティ間の接続
- リンク使用などの SD-WAN 関連情報

セキュリティ ファブリック内のダウンストリームの FortiGate による集約データビュー
- FortiView、トポロジー、モニターに表示

自動化

シンプルな if-then セットアップを使用して、セキュリティ ファブリック内に自動化を定義 :
- トリガー : 感染ホストの検知、システムステータス、構成変更、FortiAnalyzer イベントハンドラー、受信 Webhook およびスケジュール
- アクション : CLI スクリプト、E メール、iOS、MS Teams および Slack の通知、パブリッククラウドの機能、API コール / Web フック

FortiAP や FortiSwitch、または EMS 経由の FortiClient により、リモートホストをアクセスレイヤーで自動的に隔離

ネットワークアクセス制御（NAC）

サポートするローカルユーザーデータベースおよびリモートユーザー認証サービス : LDAP、Radius および TACACS+、ネイティブの FortiClient / FortiNAC のユーザーの統合と二要素認証

シングルサインオン : Windows AD、Microsoft Exchange Server、Novell eDirectory、FortiClient、Citrix およびターミナルサーバーエージェント、Radius（アカウンティングメッセージ）、POP3 / POP3S、ユーザーアクセス（802.1x、キャプティブポータル）による認証との統合

ファブリックのネットワーク内で SAML SSO がサポートされることで、管理者は再度ログインせずにファブリック対応デバイス間を移動可能

PKI および証明書 : X.509 証明書、SCEP サポート、署名要求（CSR）作成、証明書の失効前自動更新、OCSP サポート

物理、SMS およびソフトウェア OTP（ワンタイムパスワード）トークンのプロビジョニングを行う統合トークンサーバー

ZTNA フレームワーク : FortiClient EMS は、ゼロトラストタギングルールを使用して、FortiClient が検出したさまざまな属性に基づき、管理対象エンドポイントを自動的にタグ付けタグは FortiGate で動的アドレスオブジェクトとして同期

無線およびスイッチの統合コントローラによる NAC :
- NAC プロファイルをサポート（クライアントをデフォルト VLAN にオンボーディングし、デバイスのプロパティ、ユーザーグループ、または ZTNA タグに基づいて NAC ポリシーがクライアントをマッチングし、クライアントを特定の VLAN に割り当てる）

コンプライアンスとセキュリティレーティング

PCI 要件に対して一連のシステム構成コンプライアンスチェックを実行

セキュリティ ファブリックの評価 : ファブリック内のコンポーネントがベストプラクティスと照合されて監査されるため、ユーザーが一部のアイテムに修復手順を容易に適用可能

外部のクライアント管理システムから提供されるタグを使用した動的アクセス制御により、ネットワークデバイスのコンプライアンスを管理

高度な脅威保護（ATP）

脆弱性が存在するホストとその脆弱性のリストをテレメトリ経由で FortiClient を使って表示

感染したホストのリストを FortiAnalyzer から提供される情報を使って表示

外部のクラウドベースまたはオンプレミスのファイル分析（OS 非依存のサンドボックス）に統合:
- ファイル送信（タイプ選択オプションあり）
- ファイル分析レポートの受信
- ファイル分析システム（ファイルのチェックサムと不正 URL の DB）からの動的なシグネチャアップデートの受信

ドメイン名、Web フィルタリング URL、IP アドレス、マルウェアハッシュに関する外部のブロックリストのサポート

無線 LAN コントローラ

ローカルあるいはリモートのアクセスポイントの設定のプロビジョニングと管理

SSID 認証 :
- WPA2-Personal、WPA2-Enterprise
- WPA3（SAE、SAE Transition、Enterprise）
- 公開

統合された、あるいは外部のキャプティブポータル、802.1x、事前共有キーをサポート

SSID 毎のクライアントの制限、MAC フィルタリング、ブロードキャストの無効化、イントラトラフィックのブロック、ホスト隔離

WPA Personal の複数の PSK

ユーザーへの動的な VLAN の割り当て :
- RADIUS 属性を使用
- VLAN プーリングを使用（ラウンドロビン / ハッシュによるロードバランシング）

通信時間の公正化 : ネットワーク全体のパフォーマンスを向上するため、通信時間の公正化により複数のクライアントへのダウンリンクのリンクトラフィックを管理

CAPWAP データチャネルのセキュリティ : DTLS および IPsec VPN オプション

無線 LAN のセキュリティ : 不正なアクセスポイントの停止、無線 LAN IDS、フィッシング SSID の監視および停止

WiFi トラブルシューティングツール、スペクトル分析、およびロケーションマップ

Wi-Fi のトラブルシューティングを支援する、主要領域での広範なログ情報
- 関連付け、認証、DHCP、DNS

サポートする無線 LAN トポロジー : 高速ローミング、AP 負荷分散、無線 LAN メッシュおよびブリッジ

WiFi QoS WMM マーキング : アップストリーム転送時に DSCP 値に変換することにより、パケットの WiFi マルチメディア（WMM）QoS マーキングを保持（802.11ac-W2 AP のみ）

Wi-Fi Alliance Agile MBO（Multiband Operation）のサポート : ローミング決定時の Wi-Fi ネットワークリソースの有効活用と全体的なパフォーマンスの向上を支援

無線 LAN コントローラ間のフェイルオーバーの制御

スイッチコントローラ

フォーティネット製スイッチ（FortSwitch）を CAPWAP に類似する通信（FortiLink）によって管理することで、アクセス制御とセキュリティを有線デバイスに拡張

認証時のスイッチファームウェアの自動プロビジョニング

スイッチトポロジー :
- 単一 / スタックのスイッチユニット
- 単一 / スタックのスイッチユニットによる HA モード FortiGate
- 2 層スイッチユニットを備えた HA モードの FortiGate（オプション : アクセスリング付き）
- MCLAG を使用してスイッチユニットのペアに接続されたデュアルホームサーバー
- デュアルホームの FortiSwitch アクセスを備えたスタンドアロン / HA モードの FortiGate ユニット
- HA モード FortiGate ユニットによる多層型 MCLAG

スイッチポートの機能 :
- PoE 設定
- DHCP ブロッキングおよび IGMP スヌーピング
- STP（ステータス、BPDU、ルートガード）
- LLDP、IGMP、sFlow、動的 ARP 検証（DAI）
- ポートミラーリング

ポートセキュリティポリシー :
- 802.1x ポートベースモードおよび MAC ベースモード
- IEEE 802.1Q ポートを介して許可されるフレームのタイプを制限
- RADIUS アカウンティングのサポート
- MAC 認証のバイパス
- EAP パススルー

NAC ポリシーの適用 : ユーザーまたは検知されたデバイスの情報（デバイスタイプや OS など）を使用して、トラフィックを特定の VLAN に挿入または特定のポート設定を適用
- デバイス属性の条件 : MAC アドレス、ハードウェアベンダー、デバイスタイプ、オペレーティングシステム
- ユーザーベースの条件
- アクション : VLAN への割り当ておよびポート固有の設定の適用

ゲスト、認証失敗、隔離された VLAN のプロビジョニング

WAN インタフェースマネージャ

USB 3G / 4G 無線 WAN モデムおよびモデムエクステンダー（FortiExtender）のサポート

3G / 4G モデム設定 :
- スタンドアロンおよび冗長 WAN インタフェースモードのサポート
-「常時接続」および「オンデマンド」ダイアルモード
- リダイヤル制限を構成可能

一部のハードウェアでは内蔵 DSL モデムや 3G / 4G モデムをサポート

操作

構成

管理用アクセス : Web ブラウザ経由の HTTPS、SSH、telnet、コンソール

管理者ログイン :
- ACME 証明書のサポート
- パスワードポリシーの適用

FortiExplorer :
- iOS プラットフォームの管理クライアント
- USB 接続の使用による利便性
- モバイル通知を（自動化機能の一部として）提供

機能ストア : GUI コンポーネント表示の切り替え

GUI による構成 :
-「ワンクリック」アクセスにより、管理者が素早く手続きを進めることが可能
- 動的なオブジェクトセレクターと予測型の検索クエリ

サポートする管理用 Web UI 言語 : 英語、スペイン語、フランス語、ポルトガル語、日本語、簡体字中国語、繁体字中国語、韓国語

ログおよびレポート

サポートするログ用機器 : ローカルメモリおよびストレージ（利用可能な場合）、複数の syslog サーバー、FortiAnalyzer、WebTrends サーバー、FortiCloud ホステッドサービス

RFC 3195 / RFC6587 に基づく信頼性の高い syslog

FortiAnalyzer を利用するログの暗号化とログの整合性

スケジュールされたバッチログのアップロード、リアルタイムのロギング、または外部システムが利用可能になるまでローカルのキューを使用

詳細なトラフィックログ : フォワードされたトラフィック、侵害されたセッション、ローカルトラフィック、無効なパケット

総合的なイベントログ : システムおよび管理者のアクティビティ監査、ルーティングおよびネットワーク、VPN、ユーザー認証、無線関連イベント

トラフィックログの要約オプション

CEF（共通イベント形式）でログを syslog サーバーに送信

IP およびサービスポート名の解決オプション

診断

診断用 CLI コマンド、セッショントレーサー、およびパケットキャプチャによるハードウェア、システム、およびネットワークのトラブルシューティング

ポリシーとルーティングの GUI トレーサー

パケットフローの CLI トレーサー

CLI のハードウェアテストスイート

監視

SNMP システムモニタリング :
- SNMP v1 および v2c をサポート
- SNMP v3 を実装し、クエリ、トラップ、認証、およびプライバシーをサポート
- ログディスクが満杯の場合やウイルスの検知などのイベントのアラートを SNMP トラップが通知

トラフィックモニタリング :
- sFlow バージョン 5
- Netflow 9.0 および IPFIX（マネージド FortiSwitch に拡張可能）

グラフィカルモニター : リアルタイムのシステム、ネットワークサービス、およびユーザーに関するステータスビューアー

ダッシュボード : ウィジェットとレイアウトのカスタマイズが可能

ポリシーおよび制御

ポリシーモード

ポリシーオブジェクト : 事前定義、独自作成、オブジェクトグループ化

アドレスオブジェクト : サブネット、IP、IP レンジ、GeoIP（地域）、FQDN、動的（外部システムから受信したタグに基づく）、MAC アドレス

インターネットサービス DB : ポリシーのセットアップ、ルーティング、およびリンクのロードバランシング構成に使用可能な重要情報を一般的なクラウドアプリケーションに提供する DB を動的にアップデート

NGFW ポリシーモード : アプリケーションおよび URL をオブジェクトとして使用してポリシーをセットアップ

ユーザー通知 : ブロックサイトおよび添付ファイル向けのカスタマイズ可能な代替メッセージ

ユーザーの隔離 :
- 手動で永続またはカスタマイズ可能な期間を割り当て
- 自動構成のトリガーにより自動的に割り当て

デバイスの識別

デバイスの識別 : クラウドベースのクエリ DB サービス、デバイスおよび OS のフィンガープリント、自動分類、インベントリ管理

デバイスインベントリによる可視化

スイッチコントローラ LLDP-MED 音声検知

SSL インスペクション

IPS、アプリケーション制御、アンチウイルス、Web フィルタリングおよび DLP 向けの SSL 暗号化されたトラフィックの検査オプション

SSl MITM ミラーリング

SSL インスペクション方式のオプション : SSL 証明書インスペクションまたは SSL ディープインスペクション

サイトレピュテーション DB、Web カテゴリ、および / またはポリシーアドレスによる SSL インスペクションの除外

セキュリティ

アンチマルウェア

グローバル IP レピュテーションデータベースを活用するボットネットサーバーの IP ブロック

ネットワークとセキュリティのニーズに応じたアンチウイルスデータベースタイプの選択

VOR（Virus Outbreak Protection : ウイルスアウトブレイク防止）データベースのクエリ : AV シグネチャ公開前に新たに検知された脅威のリアルタイムチェックサム DB を使用

CDR（Content Disarm and Reconstruction : コンテンツ無害化）オプション :
- AV エンジンが、ユーザーに渡される前にすべてのアクティブコンテンツをリアルタイムで削除
- さらなる分析、隔離、または破棄の目的で、オリジナルファイルをサンドボックスに転送

AI ベースのマルウェア検知 : FortiGuard AV で多数のマルウェアサンプルと照合し、モジュールに学習させることで、マルウェアを構成するファイルの特徴を識別

AV 検査対象のプロトコルとファイルタイプ :
- HTTP、FTP、IMAP、POP3、SMTP、NNTP、MAPI、CIFS、SSH をサポート
- SSL インスペクションによる暗号化トラフィックのスキャン
-（パスワードで保護された）アーカイブファイル
- グレーウェアおよびモバイルマルウェア

E メール添付の Windows 実行ファイルをウイルスとして処理するオプション

ファイルの隔離（ローカルストレージが必要）と感染ホストの禁止

IPS および DoS

IPS エンジン : 11,000 以上の最新シグネチャ、プロトコルアノマリ型検知、レートベース検知、カスタムシグネチャ、マニュアルまたは自動のプル / プッシュ式シグネチャアップデート、脅威エンサイクロペディアの統合

IPS アクション : デフォルト、監視、ブロック、リセット、または攻撃者の IP を隔離（有効期限付き）

フィルターベースの選択 : 深刻度、標的、OS、アプリケーション、プロトコル

パケットのログ記録オプション

指定した IPS シグネチャからの IP 除外

IPv4 および IPv6 の TCP Syn フラッド、TCP / UDP / SCTP ポートスキャン、ICMP スイープ、TCP / UDP / SCTP / ICMP セッションフラッド（送信元 / 送信先）に対するしきい値設定が可能なレートベース DOS 検知（一部モデルを除く）

IDS スニファーモード

Protective DNS

DNS フィルター : DNS ベースの Web カテゴリフィルタリングとボットネットに対する保護
- DNS 変換、外部ブロックリスト、静的ドメインフィルターをサポート

アプリケーション制御

18 カテゴリにおよぶ数千規模のアプリケーションを検知：ビジネス、クラウド、IT、コラボレーション、E メール、ゲーム、一般向けアプリケーション、モバイル、ネットワークサービス、P2P、プロキシ、リモートアクセス、ソーシャルメディア、ストレージ / バックアップ、アップデート、ビデオ / オーディオ、VoIP、Web チャット、産業アプリケーション

独自のアプリケーションシグネチャをサポート

一部のシグネチャで複数のパラメータをサポート

HTTP / 2 プロトコルを使用するトラフィックの検知をサポートし、QUIC トラフィックをブロックできるため、ブラウザは自動的に HTTP / 2 + TLS 1.2 へフォールバック可能

フィルターベースのオーバーライド：挙動、カテゴリ、評判、テクノロジー、リスク、ベンダー、プロトコルによる

アクション：許可、ブロック、セッションのリセット（CLI のみ）、監視のみ、攻撃者の隔離

ポート適用チェック：デフォルト以外のポートで検知されたアプリケーションをブロック

プロトコル適用：定義されたポートにネットワークサービスを設定。違反した場合はブロックするように設定が可能

SSH インスペクション

SalesForce、Google Docs、Dropbox などの一般的なクラウドアプリケーションでのきめ細かなアプリケーション制御

Web およびビデオのフィルタリング

サポートする Web フィルタリング検査モード：プロキシベース、フローベース、および DNS

独自に定義した URL、Web コンテンツおよび MIME ヘッダーによる Web フィルタリング

クラウドベースのリアルタイム分類データベースによる動的 Web フィルタリング：
- 78 のカテゴリに評価分類された、70 の言語の 2 億 5 千件以上の URL データベース

構成済のカテゴリベースのフィルター：「G」、「PG-13」、「R」、カスタム

セーフサーチの適用：クエリに対して透過的にセーフサーチパラメータを挿入。Google、Yahoo!、Bing および Yandex、教育機関向けに定義可能な YouTube フィルターをサポート

プロキシ回避の禁止：プロキシサイトのカテゴリのブロック、ドメインおよび IP アドレスによる URL 評価、キャッシュおよび翻訳サイトからのリダイレクトのブロック、プロキシ回避アプリケーションのブロック（アプリケーション制御）、プロキシビヘイビアのブロック（IPS）

Web フィルタリングのローカルカテゴリおよびカテゴリ評価リストの上書き

Web フィルタリングプロファイルの上書き：管理者が特定のユーザー / ユーザーグループ / IP に対して異なるプロファイルを一時的に割り当て可能

複数の外部ブラックリストをサポート

Google コーポレートアカウントへのアクセスのみに制限

URL 証明書ブラックリスト：SSL を使用するボットネット通信のブロックに有効

プロキシベースの Web フィルタリングのその他の機能：
- Java アプレット、ActiveX、および / またはクッキーのフィルタリング
- HTTP POST 攻撃のブロック
- 検索キーワードのログ記録
- 評価に基づく HTTP リダイレクトのブロック
- プライバシー保護の目的で、特定のカテゴリの暗号化された接続をスキャン対象から除外
- カテゴリ別の Web ブラウジングクォータ設定

ビデオフィルタリング：
- クラウドベースのリアルタイム分類データベースによる動的ビデオフィルタリング
- YouTube ビデオをチャンネル ID でフィルタリング
-「YouTube アクセスを制限」および「Vimeo アクセス」の設定を適用

ファイアウォール

動作モード：NAT / ルートおよびトランスペアレント（ブリッジ）

スケジュール：ワンタイム、繰り返し

セッションヘルパーおよび ALG：DCE / RPC、DNS-TCP、DNS-UDP、FTP、H.245 I、H.245 0、H.323、MGCP、MMS、PMAP、PPTP、RAS、RSH、SIP、TFTP、TNS（Oracle）

VoIP トラフィックのサポート：SIP / H.323 / SCCP NAT トラバーサル、RTP ピンホーリング

サポートするプロトコル：SCTP、TCP、UDP、ICMP、IP

ユーザー / デバイス別のポリシー

ポリシー管理：セクション別 / グローバルのポリシー管理ビュー

統合された IPv4 および IPv6 ポリシーテーブル

VPN

カスタマイズ可能な SSL VPN ポータル：カラーのテーマ、レイアウト、ブックマーク、接続ツール、クライアントダウンロード

サポートする SSL VPN アドレス体系：ユーザーグループに関連付けられた複数のカスタム SSL VPN ログインが可能（URL パス、デザイン）

シングルサインオンブックマーク：以前のログインまたは事前定義された認証情報を再利用し、リソースへアクセス可能

パーソナルブックマークの管理：管理者がリモートクライアントのブックマークを参照および維持可能

SSL ポータルの同時ユーザー数制限

ユーザー別のワンタイムログインオプション：同じユーザー名を使用する同時ログインを禁止

SSL VPN Web モード：Web ブラウザのみを装備するシンリモートクライアント向け。
次のアプリケーションをサポート：HTTP / HTTPS Proxy、FTP、Telnet、SMB / CIFS、SSH、VNC、RDP、Citrix

SSL VPN トンネルモード：幅広いクライアント / サーバーアプリケーションを実行するリモートコンピュータ向け。SSL VPN クライアントは MAC OSX、Linux、Windows Vista および 64-bit の Windows オペレーティングシステムをサポート

SSL VPN ポートフォワーディングモード：ユーザーのコンピュータのローカルポートで接続を待受けする Java アプレットを使用。Java アプレットがクライアントアプリケーションからデータを受信すると、ポートフォワードモジュールがデータを暗号化して SSL VPN デバイスに送信し、続いてアプリケーションサーバーにトラフィックをフォワードします。

SSL トンネルモードの接続前のホスト整合性チェックおよび OS チェック（Windows ターミナル向け）

ポータル毎の MAC ホストチェック

SSL VPN セッション終了直前のキャッシュクリアオプション

IPsec VPN：
- サポートするリモートピア：IPsec 準拠ダイヤルアップクライアント、静的 IP / ダイナミック DNS のピア
- 認証メソッド：証明書、事前共有キー
- IPsec フェーズ 1 モード：アグレッシブモードおよびメイン（ID 保護）モード
- ピア受入れオプション：すべての ID、特定の ID、ダイヤルアップユーザーグループの ID
- IKEv1、IKEv2（RFC 4306）をサポート
- IKE モードの構成をサポート（サーバーまたはクライアントとして）、DHCP over IPsec
- 構成可能な IKE ポート
- フェーズ 1 / フェーズ 2 プロポーザル暗号化：DES、3DES、AES128、AES192、AES256、ARIA128、ARIA192 、ARIA256、SEED
- フェーズ 1 / フェーズ 2 プロポーザル認証：MD5、SHA1、SHA256、SHA384、SHA512
- サポートするフェーズ 1 / フェーズ 2 Diffie-Hellman Group 番号：1、2、5、14 ～ 21、27 ～ 32
- Suite-B のサポート：GCM128 および GCM256
- ChaCha20 / Poly1305 PRF のサポート：SHA1、SHA256、SHA384、SHA512
- クライアントまたはサーバーモードで XAuth をサポート
- ダイヤルアップユーザー向け XAuth：サーバータイプオプション（PAP、CHAP、Auto）、NAT トラバーサルオプション
- IKE 暗号キー有効期限、NAT トラバーサルのキープアライブ頻度を設定可能
- IPsec カプセル化の前後の IP フラグメンテーション
- デッドピアディテクション（DPD）
- リプレイ検知
- フェーズ 2 SA 向けの AutoKey キープアライブ

リモートゲートウェイ向け FQDN サポート

一般的なサードパーティ製デバイスによる終端を構成する IPsec 構成ウィザード

IPsec 集約トンネル：冗長性とトラフィックのロードバランシングのセットアップ
- パケット単位のロードバランシングアルゴリズム：IP アドレス、L4 情報、および（重み付け）ラウンドロビンによる

クラウド活用型ワンクリック VPN / VPN オーバーレイコントローラ：容易な構成
- ハブ & スポーク VPN（ADVPN オプションが必要）
- メッシュ VPN（ADVPN オプションが必要）
- SD-WAN 構成の統合
- ハブへの VPN クライアント接続をサポート

IPsec VPN 導入モード：ゲートウェイツーゲートウェイ、ハブ1& スポーク、フルメッシュ、冗長トンネル、トランスペアレントモードにおける VPN 終端

IPsec VPN 構成オプション：ルートベースまたはポリシーベース

ADVPN（自動検出 VPN）従来のハブ & スポークのアーキテクチャのスポーク間に直接トンネル（ショートカットと呼ばれる）を動的に確立
- NAT の背後のスポークに UDP ホールパンチング

VPN モニタリング：IPsec および SSL VPN 接続の詳細表示と管理が可能

サポートするその他の VPN：L2TP クライアント（一部のモデル）およびサーバーモード、L2TP over IPsec、PPTP、GRE over IPEC

E メールフィルタリング

メールプロトコルのサポート：IMAP（S）、POP3（S）、および SMTP（S）

アンチスパム DB のクエリ：IP アドレスチェック、URL チェック、E メールのチェックサム

ローカルのスパムフィルタリング：HELO DNS ルックアップ、返信メールの DNS チェック、およびブラックリスト / ホワイトリスト

ネットワーキング

ルーティング / NAT

静的ルーティングおよびポリシーベースのルーティング

動的ルーティングプロトコル：RIPv1 および v2、OSPF v2 および v3、ISIS、BGP4

コンテンツのルーティング：WCCP および ICAP

NAT 構成：ポリシーベース別および中央の NAT テーブル

サポートする NAT：NAT64、NAT46、静的 NAT、動的 NAT、PAT、フルコーン NAT、STUN

マルチキャストトラフィック：スパースモードおよびデンスモード、PIM 対応

L2 / スイッチング

レイヤー 2 のインタフェースモード：ポート集約、ループバック、VLAN（802.1Q およびトランキング）、仮想ハードウェア、ソフトウェアおよび VLAN スイッチ

EMAC-VLAN サポート：複数のレイヤー 2 アドレス（または Ethernet MAC アドレス）の単一物理インタフェースへの追加が可能

VXLAN のサポート：
- interVTEP（VXLAN トンネルエンドポイント）
- 複数のリモート IP（IPv4 ユニキャスト、IPv6 ユニキャスト、IPv4 マルチキャスト、または IPv6 ネットワークキャスト）をサポート

仮想ワイヤペア
- 同一ネットワークセグメントの指定された 2 つのインタフェース間でのみトラフィックを処理
- トランスペアレントおよび NAT / ルートの両モードで使用可能
- ワイルドカードによる VLAN のセットアップを実装するオプション

オフラインインスペクション

スニファーモード：専用のインタフェースで、そのインタフェースに入るすべての受信トラフィックをスニファーが処理

オフラインのセキュリティインスペクション：AV、Web フィルタリング、アプリケーション制御、IPS、およびアンチスパム

SD-WAN

WAN ロードバランシング（重み付け）のアルゴリズム：ボリューム、セッション、送信元 - 送信先 IP、送信元 IP、およびスピルオーバーによる

SLA のための WAN リンクのチェック：
- Ping または HTTP プローブ
- レイテンシ、ジッター、パケットロスなどのモニタリング基準
- チェック間隔、障害、フェイルバックのしきい値を構成可能
- クラウドベースの SD-WAN 帯域幅監視サービス

パッシブ WAN ヘルス測定：ファイアウォールポリシーで取得したセッション情報を使用してヘルスチェック測定を決定

以下の要素で定義したルールによるマルチパスインテリジェンス：
- 送信元アドレスやユーザーグループ
- 送信先アドレスや指定したアプリケーション（3,000 以上のアプリケーションから選択可能）
- 特定のリンク品質基準や SLA の定義を使用したパス選択

ポリシーまたはアプリケーション別のトラフィックシェーピングおよび QoS：共有ポリシーによるシェーピング、Per-IP シェーピング、インタフェースベースのトラフィックシェーピング、最大 / 保証帯域幅、IP 毎の最大同時接続、トラフィックの優先付け、Type of Service（TOS）、Differentiated Services（DiffServ）、および VPN サポート用の Forward Error Correction（FEC）

パケットの複製：
- パケットは SD-WAN ゾーン内の他の良好なリンクで複製され、送信先の FortiGate で重複排除される
- SD-WAN ルール、送信元、送信先、サービスパラメータによるトリガーが可能
- アグリゲーションされたダイアルアップ IPsec トンネルのサポート

分類されたトラフィック別にインタフェース帯域幅の割合を定義することでトラフィックシェーピングプロファイルを設定し、インタフェースにバインドするオプション

トラフィックシェーピングポリシー：送信元、送信先、サービス、アプリケーション、アプリケーションカテゴリ、および / または URL カテゴリに基づいて一致するポリシーによるトラフィックシェーピングプロファイルの割り当て

DSCP のサポート：
- SD-WAN ルールの DSCP 一致
- 特定されたアプリケーションに基づく、転送パケットの DSCP タグ設定

インラインおよびアウトオブパス型の WAN 最適化トポロジー、ピアツーピアおよびリモートクライアントをサポート

トランスペアレントモードオプション：パケットの本来の送信元アドレスを維持するため、サーバーはクライアントから直接トラフィックを受信しているように見える

WAN 最適化技術：プロトコル最適化およびバイトキャッシング

サポートする WAN 最適化プロトコル：CIFS、FTP、HTTP、HTTPS、MAPI、TCP

セキュアなトンネリングオプション：AES-128bit-CBC SSL を使用して、WAN 最適化トンネルのトラフィックを暗号化

トンネル共有オプション：複数の WAN 最適化セッション間で同じトンネルを共有

Web キャッシング：帯域幅使用量、サーバーの負荷およびユーザーが認識するレイテンシを低減することで、Web アプリケーションおよび Web サーバーの処理を高速化するオブジェクトキャッシング機能を提供。HTTP 1.0 および HTTP 1.1 の Web サイトのキャッシングをサポート

Web キャッシングによる SSL オフロード：
- フルモード：HTTPS トラフィックの暗号化と復号の両方を実行
- ハーフモード：暗号化または復号のいずれかのみを実行

URLパターンによって特定のWebサイトをWebキャッシング対象から除外するオプションを選択可能

高度な Web キャッシング構成とオプションをサポート：
- 常時再確認、キャッシュするオブジェクトの最大サイズ、否定応答持続時間、フレッシュファクター、最大 / 最小 / デフォルト TTL、プロキシ FQDN、最大 HTTP リクエスト / メッセージサイズ、無視オプション、キャッシュの有効期限切れオブジェクト、再確認された prama-no-cache

WAN 最適化および Web キャッシュの監視

明示的プロキシ

明示的 Web プロキシと FTP プロキシ：1 つ以上のインタフェースで FTP、HTTP および HTTPS プロキシを実行

プロキシ自動構成（PAC）：明示的 Web プロキシユーザー向けに自動的にプロキシを構成

プロキシチェーン：Web プロキシセッションを別のプロキシサーバーにリダイレクトする Web プロキシフォワーディング

Web プロキシフォワーディングサーバーの監視とヘルスチェック

IP リフレクト機能

プロキシフォワーディングおよびプロキシチェーンの負荷分散

明示的 Web プロキシ認証：IP ベース認証およびセッション毎認証

トランスペアレント Web プロキシ

SAML ユーザー認証のサポート

IPv6

IPv6 のサポート：IPv6 経由の管理、IPv6 ルーティングプロトコル、IPv6 トンネリング、IPv6 トラフィック向けファイアウォールと UTM、NAT46、NAT64、IPv6 IPsec VPN

IPv6 SD-WAN サポート：Ping6 リンクモニター、IPv6 送信元 / 送信先オブジェクト

トンネルおよびローカルブリッジモード SSID の両方からの無線クライアント IPv6 トラフィックを完全サポート

高可用性

高可用性モード：アクティブ / アクティブ、アクティブ / パッシブ、仮想クラスタ、VRRP、FortiGate 5000 シリーズのクラスタリング

冗長ハートビートインタフェース

HA 用予約済管理インタフェース

フェイルオーバー：
- ポート、ローカルおよびリモートのリンクモニタリング
- ステートフルフェイルオーバー
- 1 秒未満の即時フェイルオーバー
- 障害検知の通知
- メモリ使用率が一定時間にわたってしきい値を超えた場合

導入オプション：
- リンクアグリゲーションによる HA
- フルメッシュ接続による HA
- 地理的な分散による HA

スタンドアロンのセッション同期
- 非対称トラフィック、TCP、UDP、ICMP のセッションに加えて NAT のセッションのセキュリティインスペクションをサポート
- 類似する FortiGate 間での構成の同期

基幹ネットワークサービス

DHCP、NTP、DNS サーバー、DNS プロキシ内蔵

FortiGuard NTP、DDNS、およびDNSサービス

サポートするプラットフォーム

物理アプライアンス（SPU 搭載）

SPU コンポーネントとの統合によりトラフィック処理を加速

仮想システム

仮想システム（FortiOS 仮想ドメイン）は、単体の FortiGate ユニットを分割し、個別に機能し独立して管理可能な複数の仮想インスタンスまたは FortiOS を作成

「アクティブセッション」とログディスククオータの上限 / 保証など、構成可能な仮想システムリソースの制限と管理

VDOM（仮想ドメイン）の動作モード：NAT / ルートまたはトランスペアレント

タスク分割をサポートする仮想ドメイン：管理およびデータパス用に仮想ドメインを分離

仮想ルーティングおよびフォワーディング（VRF）：
- ローカルに定義された VRF（VRF-Lite）間のルートリーク機能
- 静的、OSPF、IBGP、EBGP をサポート

プライベートクラウド

VMware vSphere、Citrix、およびオープンソースの Xen、KVM、Nutanix、および MS Hyper-V を含む一般的なハイパーバイザープラットフォームのサポート

パブリッククラウド

Amazon AWS：自動スケーリング、ELB によるネイティブ HA、AZ をまたぐ HA、GuardDuty との統合；IAM、トポロジーおよび CVE の統合

Microsoft Azure：自動スケーリング、ネイティブ HA（Azure LB）、Azure Security Center との統合
Azure Stack：アクティブ - パッシブ HA

Google Cloud Platform：自動スケーリング、ゾーン間をまたぐ HA

Oracle Cloud Infrastructure：ネイティブおよび準仮想化モード、IAM の統合

AliCloud：自動スケーリング、ネイティブ HA

その他

その他

Web アプリケーションファイアウォール：
- シグネチャベース、URL 制限、および HTTP メソッドのポリシー

サーバーのロードバランシング：複数のバックエンドサーバー全体でトラフィックを分散
- 静的（フェイルオーバー）、ラウンドロビン、重み付けを含む複数の手法に基づく、またはラウンドトリップタイム、接続数に基づく
- HTTP、HTTPS、IMAPS、POP3S、SMTPS、SSL 、あるいは汎用 TCP / UDP または IP プロトコルをサポート
- セッションパーシステンスは、SSL セッション ID または挿入された HTTP Cookie に基づいてサポート

クレデンシャルスタッフィングディフェンス：外部 URL への送信トラフィックに含まれるユーザー名とパスワードをお客様のドメインコントローラに保存されている機密ネットワーククレデンシャルと照合してスキャン

DLP メッセージフィルター：
- サポートするプロトコル：HTTP-POST、SMTP、POP3、IMAP、MAPI、NNTP
- アクション：ログ記録のみ、ブロック、ユーザー / IP / インタフェースの隔離
- 事前定義済フィルター：クレジットカード番号、ソーシャルセキュリティ ID 番号

DLP ファイルフィルター：
- サポートするプロトコル：HTTP-POST、HTTP=-GET、SMTP、POP3、IMAP、MAPI、FTP、NNTP
- フィルターオプション：サイズ、ファイルタイプ、ウォーターマーク、コンテンツ、暗号化の有無

DLP ウォーターマーキング：FortiGate を通過し、ウォーターマーク内に隠された企業識別子（テキスト文字列）および重要度レベル（クリティカル、プライベートおよび警告）を含んでいるファイルのフィルタリングが可能。Windows および Linux 向けの無償ウォーターマーキングツールをサポート

DLP フィンガープリンティング：捕捉されたファイルからチェックサムフィンガープリントを生成し、フィンガープリントデータベースと比較

DLP アーカイビング：E メール、FTP、IM、NNTP および Web トラフィックのコンテンツすべてを記録

PRP（Parallel Redundancy Protocol）のサポート：パケットの FortiOS による処理で、PRP の RCT（Redundancy Control Trailer）を保持

注：FortiOS7.0 の機能を紹介しており、一部の機能はすべてのモデルに該当しない場合があります。機能の提供状況については、docs.fortinet.com でソフトウェア機能一覧をご覧ください。

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