FORTINET

DATA SHEET

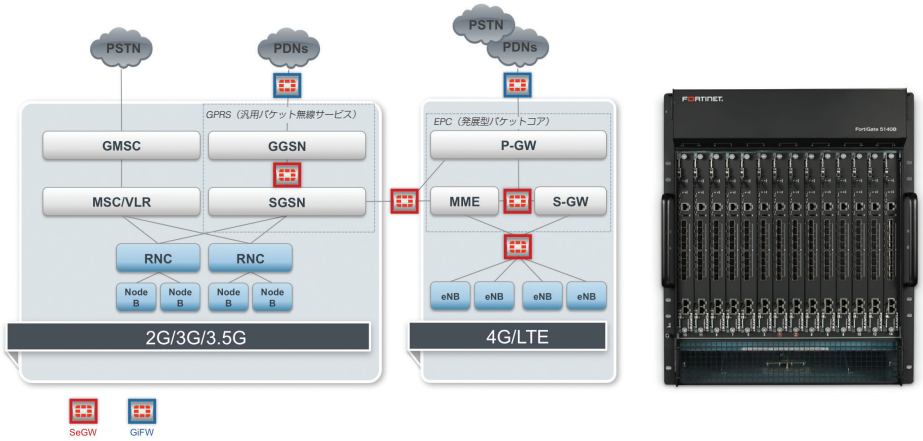
FortiCarrier
サービスプロバイダ向け
セキュリティプラットフォーム

FortiCarrier

サービスプロバイダ向けセキュリティプラットフォーム

FortiCarrier 5.0 – 通信事業者 / サービスプロバイダ向け統合セキュリティ

モバイルネットワークに追加されるデバイスやアプリケーションの爆発的な増加によって、通信事業者やサービスプロバイダは FortiCarrier OS が動作する FortiGate アプライアンスを採用し、高性能 / 大容量のセキュリティソリューションで長期にわたる拡張性と信頼性のニーズに対応するようになっています。



セキュリティゲートウェイ（SeGW）プラットフォーム

FortiCarrier OS は、GTP および SCTP のファイアウォール機能を備えており、従前の方式である 2G/3G GPRS コアモビリティネットワークと最新の LTE EPC（発展型パケットコア）のどちらのソフトウェアインタフェースも保護できます。マイクロセル方式での多数の発展型 NodeB（eNB）プラットフォームが拡大した場合でも、FortiCarrier OS の高性能 / 高密度 VPN サポートで対応できます。FortiCarrier OS 導入環境で仮想ドメイン（VDOM）を利用することで、SeGW 機能を 3GPP ソフトウェアインタフェースやデバイスのロールに簡単に分離させることができます。

FortiCarrier 5.0 セキュリティ機能

- IPv6 対応ステートフルファイアウォール
- 動的セキュリティプロファイル / グループ
- マネージドセキュリティ
- 音声通信のセキュリティ
- MMS のセキュリティ
- GPRS トンネリングプロトコル（GTP）
- SCTP ファイアウォール
- 高性能 / 高密度 VPN コンセントレータ – IPSec および SSL
- SSL 暗号化トラフィックインスペクション
- ウィルス対策 / スパイウェア対策とスパム対策
- 侵入防止システム（IPS）
- 情報漏えい対策（DLP）
- アプリケーション制御
- Web フィルタリング
- ボットネット対策
- クライアントレピュテーション追跡
- エンドポイントネットワークアクセス制御（NAC）
- 脆弱性管理
- WAN 最適化
- 無線コントローラ
- 監視、ログ、レポーティング
- 仮想ドメイン（VDOM）
- 高可用性
- レイヤー 2/3 ルーティングサービス
- FortiGuard セキュリティアップデート

Gi ファイアウォール（GiFW）プラットフォーム

インターネットにアクセスする BYOD デバイスの急増に加え、データセンターやクラウドベースのパケットデータネットワーク（PDN）が拡大し、HPSA+、LTE、LTE-Advanced などのハイパフォーマンスが要求されるネットワークが次々と登場していることで、GiFW ソリューションは数千人の同時実行ユーザーのセキュリティ要件への対応が求められるようになりました。FortiCarrier OS は、IPv4/IPv6 ネットワークでの NGFW および UTM をサポートし、加入者およびデバイスタイプによるポリシーの動的なコンテキスト化を可能にします。FortiOS Carrier には、MMS スキャンのサポートが組み込まれており、FortiOS のコンテンツフィルタリング、マルウェア対策、およびデータ漏えい防止（DLP）の機能を MMS ベースのサービスでも利用できます。

容易な管理

FortiCarrier OS では、GUI/CLI による豊富な管理機能のサポートに加えて、ログやレポートの機能も提供されており、デバイス管理用の FortiManager およびログ管理 / 分析用の FortiAnalyzer プラットフォームで完全にサポートされています。FortiCarrier OS または FortiOS が動作する FortiGate デバイスであれば、どちらも共通の管理環境で一元管理することができます。

FortiCarrier 5.0 – サービスプロバイダ向けのコンテンツとネットワークの完全な保護

FortiCarrier 5.0 には、MSSP、音声通信事業者、モバイル通信事業者などのサービスプロバイダにとって極めて有用な数百のセキュリティ関連機能が組み込まれています。ネットワークの IPv6 への移行に伴って、サービスプロバイダは自社のポートフォリオを拡大し新たなビジネスチャンスを獲得しようとしていますが、FortiCarrier OS が動作する FortiGate 統合セキュリティアプライアンスであれば、必要に応じて即座に導入配備や拡張に対応できます。FortiCarrier 5.0 には、FortiOS 5.0 が提供するすべてのセキュリティ機能（詳細は FortiOS 5.0 のカタログをご参照ください）に加えて、以下に挙げるサービスプロバイダ向けの機能も追加されています。

モバイルプロバイダのセキュリティ

FortiCarrier が動作する FortiGate アプライアンスは、GTPv2 のサポートを始めとする統合 GPRS トンネリングプロトコル（GTP）ファイアウォール機能によってモバイルネットワークインフラストラクチャを保護し、多様な導入環境での互換性を保証します。侵入防止機能の完全統合によって、さまざまな GTP 攻撃をブロックします。MMS スキャンでは、MM1/3/4/7 インタフェースのトラフィックを検査し、ウィルス対策、フラッド攻撃検知、電子メールのスパム対策、データ漏えい防止、およびモバイルコンテンツフィルタリングなどの機能によってフィッシング攻撃をブロックします。

動的コンテキスト

通信事業者やサービスプロバイダは、ユーザー数の拡大に伴って数百ものセキュリティポリシーと数えきれない程のエンドユーザーを管理するようになりました。動的コンテキスト機能を利用すれば、管理者がセキュリティポリシーを自動的にエンドユーザーへ提供できるため、手動によるプロビジョニングの必要性が著しく減少し、運用コストが大幅に削減されます。

音声通信のセキュリティ

FortiCarrier OS が動作する FortiGate アプライアンスに組み込まれた SIP（Session Initiation Protocol）シグナリングファイアウォールは、音声インフラストラクチャを不正アクセス、ピアネットワーク、およびトランキングネットワークから保護します。FortiCarrier プラットフォームは、IMS（IP マルチメディアサブシステム）や IMS 非対応の導入環境とも互換性があり、フラッドやネットワーク可用性を低下させる攻撃を防止することで、QoS（サービス品質）の保証を可能にします。SIP ファイアウォールと FortiCarrier 5.0 侵入防止システムのシームレスな統合によって、音声通信インフラストラクチャを DoS（Denial of Service）攻撃やその他のネットワーク関連の脅威から保護します。

FortiCarrier OS のライセンス体系

FortiOS 5.0 より前のバージョンでは、FortiCarrier OS を動作させるために下記の専用 FortiCarrier ハードウェアモデルを使用する必要がありました。

- FortiCarrier-3810A
- FortiCarrier-3950B
- FortiCarrier-5001A-DW

専用の FortiCarrier ハードウェアをご利用いただく場合は、継続してこれらのモデルをご購入いただき、FortiCarrier 5.0 にアップグレードしていただくことが可能です。また、FortiOS 5.0 のリリースに伴って、FortiOS 5.0 が動作する一部の FortiGate モデルでは、FortiCarrier アップグレードライセンスの適用によるアップグレードを利用して FortiCarrier 5.0 を動作させることもできます。これは 1 回限りのアップグレードであり、初期のアップグレード費用以外の追加サポートや定期コストは発生しません。現時点では、以下の FortiGate モデルが FortiCarrier アップグレードライセンスの対象となっています。

- FortiGate-3240C
- FortiGate-3600C
- FortiGate-3200D
- FortiGate-3700D
- FortiGate-3810D
- FortiGate-5001B/C/D
- FortiGate-5101C

主な機能

マネージドセキュリティ

動的コンテキスト

- ユーザー別のサービスポリシーの割り当て（最大 600,000 ユーザー）
- サービスポリシーでは FortiOS Carrier が提供するあらゆる高度なセキュリティサービスの設定を定義可能
- ペアレンタルコントロール / オプトアウトサービスに対応

仮想ドメイン（VDOM）

- 物理ブレード / アプライアンスあたり数百のエンタープライズユーザーをサポートし、シャーシあたり数千のエンタープライズユーザーまで拡張可能

統合セキュリティ

- ファイアウォール（ICSA Labs 認定）
- IPSec VPN（ICSA Labs 認定）
- SSL-VPN
- 侵入防止システム（ICSA Labs 認定）
- ゲートウェイアンチウイルス（ICSA Labs 認定）
- Web フィルタリング（20 億以上の URL をカテゴリ別に分類）
- アンチスパムフィルタリング
- アプリケーション制御（数千のアプリケーションをカテゴリ別に分類）
- データ漏えい対策（DLP）
- L2/L3 ルーティング（レートリミット）
- SSL ベースのトラフィックインスペクション

カテゴリ別ログ管理 / アラート機能

- FortiAnalyzer アプライアンスにより機能提供
- すべてのログ / アラート機能をユーザーごとに構成可能
- セキュリティ / システムイベントログを統合
- イベントの相関、グラフィカルなレポート、ネットワークデータ統計

一元管理

- FortiManager アプライアンスにより機能提供
- 導入環境の構成 / プロビジョニング
- リアルタイム監視
- デバイス / セキュリティポリシーの保守
- 各国語対応のセキュリティコンテンツアップデートサーバーとレーティングデータベースによるデバイスの管理

音声通信のセキュリティ

SIP シグナリングファイアウォール

- ステートフルで SIP プロトコル対応のファイアウォール
- ハードウェアによる高速 RTP 処理によるパケットロス、パケットレイテンシ、ジッターの軽減
- SIP トランスペアレント（検査のみ）モードと NAT（SIP ヘッダーの書き換え）モード
- プロキシモードまたはリダイレクトモードで SIP サーバーをサポート
- 構成可能な RTP ピンホールのサポート
- 複雑な送信元 / 送信先 SIP NAT 環境をサポート（SIP プロトコルと RTP プロトコル）
- NAT IP 保持により元の IP アドレスを管理目的（課金など）で維持
- セッション継続期間中の SIP 追跡
- SIP セッションフェイルオーバーによるアクティブ / パッシブモードの高可用性
- SIP セッションのロードバランシング（仮想 IP のロードバランシングによる）
- 地理的冗長性のサポート
- SIP レート制限による SIP サーバーフラッド / オーバーロードの防止
- SIP/RTP サーバーを隠避する IP トポロジ（NAT および NAPT による）
- 構成可能な SIP コマンドにより、未承認の SIP メソッドをブロック
- 構成可能な SIP ブロックにより、定義された最大ヘッダー長を超えるメッセージをブロック
- SIP 登録機関専用オプションにより、クライアントのスプーフィングを回避
- FortiAnalyzer アプライアンスへの SIP 通信のログ送信
- SIP 統計（アクティブセッション、合計通話数、失敗 / 切断した通話、成功した通話）

音声通信セキュリティ関連のその他のテクノロジ

- VoIP アノマリ /VoIP プロトコル対応、シグネチャベース検査機能付の侵入防止システム
- DOS（Denial of Service）センサーが信頼されたゾーンをフラッド攻撃から保護
- 統合 IPsec による信頼されたゾーン間のセキュアトンネル
- 仮想ドメイン（VDOM）のサポートにより、同一物理環境内でのインフラストラクチャの分離を強化

モバイル関連のセキュリティ

動的セキュリティプロファイル

- MSISDN 別のサービスポリシーの割り当て（モバイルステーション）
- サービスポリシーでは FortiOS Carrier が提供するあらゆる高度なセキュリティサービスの設定を定義可能
- ペアレンタルコントロール / オプトアウトサービスに対応

MMS 関連全般の機能

- 複数の MMS ポリシープロファイルで統合 /MVNO 導入環境をサポート
- カスタマイズ可能な通知メッセージ（MVNO ごと）
- MSISDN ヘッダーの解析（MM1/MM7 メッセージタイプでの Cookie の抽出と 16 進変換を含む）
- FortiAnalyzer アプライアンスへの MMS ファイルのインターセプトによるフォレンジック分析
- MMS コンテンツアーカイブ（HTTP/SMTP トランスポートヘッダーにより、MMS メッセージ全体を FortiAnalyzer アプライアンスにアーカイブ）
- FortiAnalyzer アプライアンスによる、MSISDN 別 / モバイルステーションタイプ別の悪意あるアクティビティのレポート

主な機能

MMS アンチウイルス
- 監視のみのモードとアクティブブロックモード（インタフェースタイプごと）
- MM1/MM3/MM4/MM7 メッセージタイプの同時マルウェアスキャン
- 悪意あるコンテンツのみを削除するオプション（メッセージトランザクションの完了が可能）
- 構成可能なブロックまたはインターセプトのアクションを利用してファイルタイプを分析（ファイル拡張子に依存しない分析）
- カスタマイズ可能な取得メッセージスキャン（MM1）で検査の冗長性を解消
- カスタマイズなブロック / アーカイブ / インターセプトアクションによる送信元別のスキャン
- MM1/MM7 のクライアント / サーバーの負荷軽減

MMS アンチスパム / 不正アクセス対策
- 個別の操作でカスタマイズ可能な 3 つのしきい値を駆使して MM1/MM4 フラッドを検知
- カスタマイズ可能なしきい値 / 操作で MM1/MM4 重複メッセージを検知
- スパム / 不正アクティビティを管理者に通知するアラートをカスタマイズ可能
- ブロック / パスの操作をカスタマイズ可能な MM1/MM7 有害ワードのスコア評価機能

GTP ファイアウォール
- GTP ペイロードの統合侵入防止用インスペクション
- Gn/Gp インタフェース（従来の 3GPP）、S11 および S5/S8 インタフェース（LTE）向け
  - GTP パケットサニティーチェック、長さによるフィルタリング、およびタイプによるスクリーニング
  - GSN トンネルリミット / レートリミット
  - GTP ステートフルインスペクション
  - ハング GTP トンネルのクリーンアップ
  - GTP トンネルフェイルオーバーによる高可用性
  - GTP IMSI プレフィックス（最大 1000）/APN（最大 2000）フィルタリング
  - GTP シーケンス番号検証
  - GTP メッセージの IP フラグメンテーション
  - GGSN/SGSN のリダイレクト
  - GTP-in-GTP パケットの検出
  - GTP トラフィックのカウント / ログ管理
  - Gi ファイアウォールとの併用による過大請求対策
  - スプーフィング対策機能によるカプセル化トラフィックフィルタリング
  - GTP プロトコルのアノマリ検出と攻撃防止
  - ハンドオーバー制御によるセッション乗っ取りの防止
- Gi インタフェース向け
  - Gn/Gp ファイアウォールとの併用による過大請求対策

FortiOS ネットワーキング

ネットワーキング / ルーティング
- 複数 WAN リンクのサポート
- PPPoE サポート
- DHCP クライアント / サーバー
- ポリシーに基づくルーティング
- IPv4 の動的ルーティング（RIP、OSPF、IS-IS、BGP、およびマルチキャストプロトコル）
- IPv6 の動的ルーティング（RIP、OSPF、および BGP）
- マルチゾーンサポート
- ゾーン間ルート
- 仮想 LAN（VLAN）間ルーティング
- マルチリンクアグリゲーション（802.3ad）
- IPv6 サポート（ファイアウォール、DNS、トランスペアレントモード、SIP、動的ルーティング、管理アクセス、管理）
- VRRP/ リンク障害の制御
- sFlow クライアント

トラフィックシェーピング
- ポリシーベースのトラフィックシェーピング
- アプリケーションベースの IP 別トラフィックシェーピング
- Differentiated Services（DiffServ）サポート
- 保証 / 最大 / 優先帯域幅
- アカウントによるシェーピング、トラフィッククオータ

仮想ドメイン（VDOM）
- ファイアウォール / ルーティングドメインの分離
- 管理ドメインの分離
- VLAN インタフェースの分離
- 10 VDOM の標準ライセンス（追加可能）

データセンター最適化
- Web サーバーキャッシング
- TCP マルチプレキシング
- HTTPS オフロード
- WCCP サポート

高可用性（HA）
- アクティブ / アクティブ、アクティブ / パッシブ
- ステートフルフェイルオーバー（FW と VPN）
- デバイス障害の検出および通知
- リンクステータスモニター
- リンクフェイルオーバー
- サーバーのロードバランシング

WAN 最適化
- 双方向 / ゲートウェイからクライアント / ゲートウェイ
- キャッシングとプロトコルの最適化を統合
- CIFS/FTP/MAPI/HTTP/HTTPS/ ジェネリック TCP を高速化
- ハードディスクドライブ内蔵の FortiGate デバイスが必要

主な機能

FortiOS 管理

管理オプション

- Web UI（HTTP/HTTPS）
- Telnet / SSH（セキュアコマンドシェル）、CLI（コマンドラインインタフェース）
- ロールベースの管理
- 多言語サポート：英語、日本語、韓国語、スペイン語、簡体字中国語、繁体字中国語、フランス語
- 複数の管理者 / ユーザーレベル
- システムソフトウェアロールバック
- カスタマイズ可能なパスワードポリシー
- カスタマイズ可能なダッシュボードウィジェット（Web UI）
- FortiManager による一元管理（オプション）

無線コントローラ

- WiFi とアクセスポイントの統一管理
- AP の自動プロビジョニング
- オンワイヤ検知と不正 AP のブロック
- 異なる SSID の仮想 AP
- 複数の認証方法に対応

ログ / 監視 / 脆弱性管理

- ネットワーク脆弱性スキャン
- グラフィカルなレポートのスケジュール機能をサポート
- リアルタイム / 履歴監視のグラフィカルな表示
- ローカルおよびリモートの Syslog/WELF サーバーのログ管理
- SNMP サポート
- 電子メールによるイベント通知
- VPN トンネルモニター
- FortiAnalyzer のログ管理機能（オプション、VDOM 別のログを含む）
- FortiGuard 分析 / 管理サービス（オプション）

ファイアウォールユーザー認証オプション

- ローカルデータベース
- Windows Active Directory（AD）の統合（FSAE による）
- 外部 RADIUS/LDAP/TACACS+ の統合
- RADIUS による IPSEC VPN の Xauth
- RSA SecurID サポート
- LDAP グループサポート
- FortiToken サポート

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 7-18-18
住友不動産六本木通ビル 8 階
www.fortinet.co.jp/contact

お問い合わせ