DATA SHEET

FortiProxy

FortiProxy 400E、2000E、4000E、VM

FortiProxy は、Web フィルタリング、DNS フィルタリング、データ漏えい防止、アンチウイルス、不正侵入防止、高度な脅威保護などの複数の検知技術の採用によって、サイバー攻撃から従業員を保護する、セキュア Web プロキシです。きめ細かいアプリケーション制御の活用により、企業におけるインターネットコンプライアンスを支援します。高性能の物理アプライアンスと仮想アプライアンスをオンサイトに導入することで、あらゆる規模の企業に対応します。

SSL インスペクション

SSL インスペクションの実行が可能な強力なハードウェアが、パフォーマンスを低下することなく、暗号化されたトラフィックの死角を解消

高度な Web 攻撃からの保護

実証済みの FortiGuard 脅威インテリジェンスサービスと FortiSandbox Cloud との統合によって、最新の高度な脅威から企業を保護

認証に基づく Web アプリケーション制御

きめ細かいアプリケーション制御ポリシーによって、ソーシャル Web サイトへのアクセスをユーザーやグループの ID を使用して制限

ハイライト

- 脅威からの先進の防御機能
  - FortiGuard脅威インテリジェンスサービスとの統合
  - Web、DNSフィルタリング、およびアプリケーション制御
  - FortiSandbox Cloudとオンプレミスアプライアンスとの統合
  - AV、IPS、DLP、およびコンテンツ分析
- 高性能と拡張性
  - 独自設計のセキュリティ処理装置が高性能を実現
  - 小規模から大規模までのあらゆる組織に対応する拡張性
  - 冗長性を実現するHA（高可用性）構成
- コンテンツキャッシングとWAN最適化
  - 静的 / 動的コンテンツキャッシング
  - 複数のコンテンツデリバリネットワーク
  - ネットワークレイテンシを短縮
  - 帯域幅オーバーヘッドを削減

主な機能

多層型検知

FortiProxy は、レピュテーション検索、シグネチャベースの検知、サンドボックスの活用をはじめとする複数の検知方法を提供し、既知のマルウェア、新たな脅威、ゼロデイマルウェアからの保護を可能にします。

FortiGuard 脅威インテリジェンスとの統合

急速に進化する脅威に対抗するには、セキュリティチームが常に新しい脅威に注目し、監視する必要があります。FortiGuard 脅威インテリジェンスサービスは、FortiGuard Labs が提供し、変化し続ける脅威からの保護を実現する、一連のサービスです。31 カ国に 200 名を超える研究者が在籍する FortiGuard Labs は、常に新たな脅威を検知しており、15 以上の異なるセキュリティサービスを提供しています。FortiProxy によって提供される以下の保護サービスは、FortiGuard 脅威インテリジェンスの最新情報を活用して常に更新されます。

- **DNS と Web フィルタリング**
  FortiGuard 脅威インテリジェンスサービスの活用により、悪意のあるドメイン、疑わしいドメイン、新たに生成されたドメイン名が即座にブロックされます。毎分 150,000 以上の Web サイトが、FortiGuard Web フィルタリングによってブロックされています。動的なカテゴリベースの Web フィルタリングによって、従業員による会社の利用規定の遵守が担保されます。静的ホワイトリスト / ブラックリスト作成機能を利用して、特定の Web サイトの許可やブロックを設定することが可能です。
- **サンドボックスを使用した動的解析**
  トップクラスの評価を獲得している FortiSandbox を FortiProxy に連携させることで、高度な標的型攻撃からの保護も可能になります。不審なファイルやリスクの高いファイルは、FortiSandbox に自動的に送信されて、詳細に分析されます。サンプルは隔離された環境で分析され、システムの動作とコールバックの検知を使って攻撃のライフサイクル全体が明らかにされます。セキュリティ担当者は、レポートによって提供される豊富な実用的インテリジェンスを活用し、対策を行うことができます。
- **アンチウイルスと DLP**
  フォーティネットは、AV Comparatives や Virus Bulletin による業界テストにおいて、一貫して卓越した有効性評価を得ています。データ漏えい防止（DLP）機能により、外部への機密データの流出を防止します。機密ファイルにはフィンガープリントやウォーターマークを適用することができるため、発信トラフィックを検査してあらゆるデータ漏えいを特定可能です。
- **コンテンツ分析サービス**
  FortiProxy は、有害画像 / ビデオ検知に関する業界最先端のソリューションである Image Analyzer のコンテンツスキャンテクノロジーを採用しており、不適切なコンテンツへのアクセスを防止します。
- **IPS**
  FortiProxy は、シグネチャベース / シグネチャレス両方のエンジンを組み合わせて使用し、侵入を防止します。IPS シグネチャは、エクスプロイト、既知の脆弱性、またはアノマリパターンのいずれかに基づくものです。シグネチャレスの技術は、SQL インジェクション、ドメイン生成アルゴリズム攻撃、Java および Flash のエクスプロイトの検知に使用されます。FortiGuard Labs では、毎週 100 以上の IPS ルールが生成されており、400 万件を超えるネットワーク侵入の試行がブロックされています。

暗号化されたトラフィックのインスペクション

インターネットトラフィックの 60%以上が暗号化されるようになったことで、トラフィックの可視性が大きな課題となっています。FortiProxy では、SSL や SSH のディープインスペクション機能が提供されており、追加のライセンスやアプライアンスは必要ありません。FortiProxy が中間者として機能することで、暗号化されたトラフィックのインスペクションも可能になります。また、除外カテゴリを柔軟に追加できるため、金融機関、医療機関、その他のサイトを監視対象から除外することもできます。SSL ディープインスペクションが不可能な場合は、証明書ベースのインスペクションもサポートしています。

詳細なアプリケーション制御

ソーシャルアプリケーションの利用増加に伴い、多くの組織ではソーシャルアプリケーションへのアクセスは許可しつつ、投稿などの特定のアクションは禁止するといった、きめ細かい制御が必要とされるようになっています。FortiProxy は、すべての主要ソーシャル Web サイト（Facebook、LinkedIn、Twitter、Instagram を含む）をサポートしており、3,000 の以上のアプリケーションをサポートしています。さらには、FortiGuard が管理するクラウドデータベースを使用して SaaS アプリケーションを分類することもできます。

Web アクセスの認証

FortiProxy は、SAML、Kerberos、シングルサインオンなどの高度な認証方式をサポートしています。これらの機能はいずれも FortiProxy に内蔵されており、別のアプライアンスを追加する必要はありません。また、ユーザーやロールに基づいて管理者がポリシーを柔軟に構成することもできます。

WAN 最適化と高度キャッシング

多くの場所で帯域幅がボトルネックとなっている今日、運用コストの抑制と帯域幅の増強を両立させることは不可能のように思えます。FortiProxy のコンテンツキャッシングと WAN 最適化の機能を活用することで、このような環境においてもネットワークの最適化と大幅な高速化が実現します。

主な機能

セキュリティ ファブリック

フォーティネット セキュリティ ファブリックは、仮想、クラウド、オンプレミスのあらゆるネットワークセグメント、デバイス、アプライアンスの広範な保護と可視化を実現します。セキュリティリソースを自動的に同期させることで、ポリシーの適用のほか、ネットワークのあらゆる場所で検知される脅威への自動レスポンスが可能になると同時に、異なるセキュリティソリューションや製品を単一コンソールから簡単に管理できるようになります。FortiProxy は、FortiSandbox や FortiAnalyzer などのセキュリティ ファブリックの主要コンポーネントと統合されており、ICAP プロトコルや WCCP プロトコルを使用してサードパーティのセキュリティデバイスとの統合も可能です。

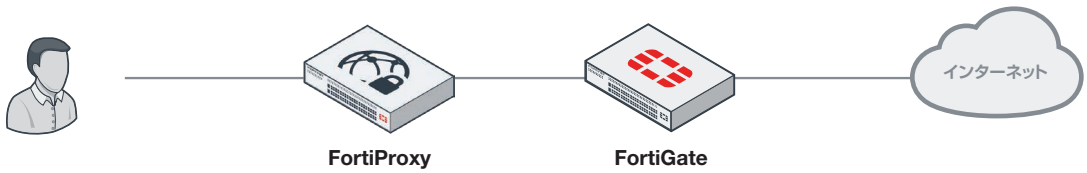
高い性能と拡張性、TCO 削減

FortiProxy は、専用の ASIC の採用によってネットワークモジュールやセキュリティモジュールのパフォーマンスを向上しています。FortiProxy は、最大 15 Gbps のプロキシ速度をサポートすると同時に、ユーザー数が 500 人程度から 50,000 人規模までのあらゆる規模の企業に対応する優れた拡張性も備えています。FortiProxy は、TCO を抑制しつつ、確かな価値をお客様に提供します。

導入例

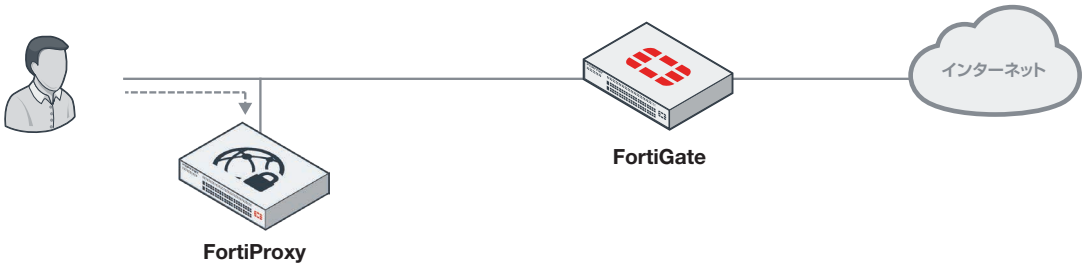
FortiProxy では、インフラストラクチャの変更やサービスの中断を最小限に留めながら、お客様の要件に合わせて 3 つの導入モードのいずれかを選択できます。

インライン導入



- 小規模企業に最適
- NGFW の背後に導入
- プロキシで構成されたトラフィックだけがインスペクションされ、それ以外のトラフィックは自動的に NGFW へとバイパスされます。

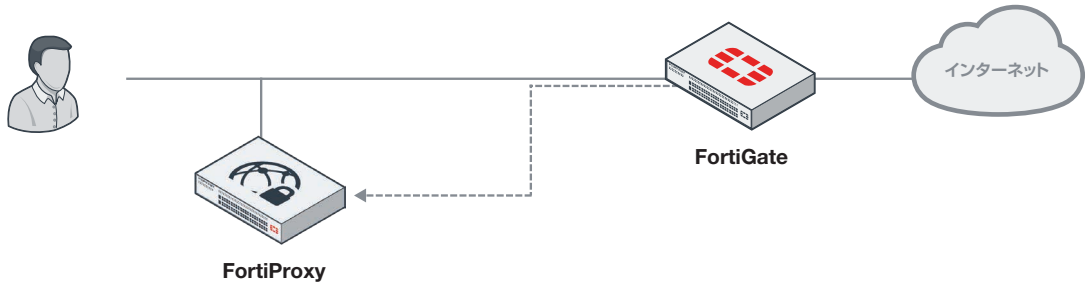
明示的導入



- 大規模企業向け
- エンタープライズ環境の任意の場所にプロキシを導入可能
- 複数の PAC ファイルをサポートし、柔軟な導入が可能

導入例

WCCP / PBR 導入



- 大規模導入環境に最適
- PAC ファイルの配布が困難な環境向けに、WCCP または PBR モードもサポート
- インスペクション対象のトラフィックをプロキシにルーティングするポリシーを NGFW / ルーター上で構成

主な機能と特長

システム

- 多様な導入オプション：
  – インライン、プロキシフォワーディング、明示的プロキシ、WCCP / PBR
  – ハードウェアまたは仮想アプライアンス
- IPv4、IPv6 アドレスのサポート
- HTTP / S を含むアプリケーションをサポート
- アクティブ - アクティブおよびアクティブ - バックアップ構成の HA によってセッションを同期

脅威保護

- FortiGuard 脅威インテリジェンスサービスとの統合により、リアルタイムで脅威情報のアップデートが可能
- クラウドサンドボックスとの統合によって高度な脅威を検知
- セキュリティサービスが付属、追加アプライアンスは不要
- DNS と Web フィルタリング
  – Web サイトの動的分類
  – 悪意のある怪しいドメイン / URL のブロック
  – 静的ブラックリスト / ホワイトリスト
- アプリケーション制御
  – ソーシャル Web サイトのきめ細かい Web アプリケーション制御
  – 3,000 以上のアプリケーションをサポート
- アンチウイルス、ボットネット、DLP
- コンテンツ分析
- 複数の ICAP サーバーをサポート
- IPS シグネチャとフィルター
- Web 評価のオーバーライド
- SSL / SSH インスペクション
- 独自のアプリケーションシグネチャ

認証

- Radius、SAML、LDAP、NTLM、Kerberos、FortiToken One-Time Password を含む各種認証モードをサポート
- 認証機能を内蔵し、追加デバイスは不要

高度なキャッシング

- Web とビデオのキャッシング
- リバース Web キャッシュ
- トラフィックシェーピングと QoS ポリシーによるアプリケーション優先度の設定
- HTTP 経由の動的アダプティブストリーミング
- RTP および RTMPT 経由の動的アダプティブストリーミング

WAN 最適化

- プロトコル最適化：HTTP、MAPI、CIFS、FTP、および TCP をサポート
- WAN のセキュアトンネル
- WAN 最適化ピア

管理 / レポート

- FortiView の統合
- FortiAnalyzer の統合
- Syslog サーバーのサポート
- きめ細かいロールベースのアクセス
- レポート作成とロギング
- 容易な導入を可能にするポリシーテスト

技術仕様

	FortiProxy 400E	FortiProxy 2000E	FortiProxy 4000E
システム情報			
対応ライセンス数	500 ～ 4,000 ユーザー	2,500 ～ 15,000 ユーザー	15,000 ～ 50,000 ユーザー
導入モード	インラインプロキシ、トランスペアレント / WCCP プロキシ、明示的プロキシ、プロキシルーティング		
ハードウェア仕様			
メモリ	8 GB	64 GB	128 GB
管理	HTTP / S、SSH、CLI、SNMP、シリアル管理コンソール（RJ45）	HTTP / S、SSH、CLI、SNMP、シリアル管理コンソール（DB9）	HTTP / S、SSH、CLI、SNMP、シリアル管理コンソール（DB9）
ネットワークインタフェース	4 x GbE RJ45	2 x 10 GbE SFP+、2 x GbE SFP、2 x GbE RJ45	4 x 10 GbE SFP+、2 x GbE SFP、4 x GbE RJ45
バイパスインタフェース	—	2 x GbE インタフェース（RJ45）	2 x GbE インタフェース（RJ45）
内蔵ストレージ	4 TB（2 TB x 2）ハードディスク	8 TB（2 TB x 4）ハードディスク	8 TB（2 TB x 4）ハードディスク
電源	単一（オプションで冗長化可能）	冗長	冗長
動作環境			
形状	1 U アプライアンス	2 U アプライアンス	2 U アプライアンス
AC 電源（入力電圧）	100 ～ 240 V AC、50 ～ 60 Hz	100 ～ 240 V AC、50 ～ 60 Hz	100 ～ 240 V AC、50 ～ 60 Hz
消費電力（平均 / 最大）	120 W / 151 W	244 W / 265 W	462 W / 493 W
最大電流	100 V / 5 A、240 V / 3 A	100 V / 10 A、240 V / 3.5 A	100 V / 9.8 A、240 V / 5 A
放熱	550 BTU/h	940 BTU/h	1,717 BTU/h
動作温度	0 ～ 40 ℃	10 ～ 35 ℃	10 ～ 35 ℃
保管温度	-25 ～ 70 ℃	-40 ～ 70 ℃	-40 ～ 70 ℃
湿度	5 ～ 95%（結露しないこと）	8 ～ 90%（結露しないこと）	8 ～ 90%（結露しないこと）
サイズ			
高さ x 幅 x 奥行	44 x 438 x 416 mm	89 x 437 x 647 mm	89 x 437 x 647 mm
重量	11 kg	14.5 kg	19.5 kg
準拠規格・認定			
準拠規格		FCC、ICES、CE、RCM、VCCI、BSMI（Class A）、UL / cUL、CB	

FortiProxy400E

FortiProxy 2000E

FortiProxy 4000E

仮想アプライアンス	FortiProxy VM01	FortiProxy VM02	FortiProxy VM04
システム情報			
サポートするハイパーバイザー	VMware ESX / ESXi、KVM プラットフォーム	VMware ESX / ESXi、KVM プラットフォーム	VMware ESX / ESXi、KVM プラットフォーム
対応ライセンス数	100 ユーザー	100 ～ 500 ユーザー	100 ～ 2,500 ユーザー
ハードウェア仕様			
ストレージ	2 CPU、RAM サイズ無制限、1 Disk	4 CPU、RAM サイズ無制限、2 Disk	8 CPU、RAM サイズ無制限、2 Disk
仮想 NIC 枚数（最大）	10	10	10
管理	HTTP / S、SSH、CLI、SNMP	HTTP / S、SSH、CLI、SNMP	HTTP / S、SSH、CLI、SNMP

仮想アプライアンス	FortiProxy VM08	FortiProxy VM16	FortiProxy VMUL
システム情報			
サポートするハイパーバイザー	VMware ESX / ESXi、KVM プラットフォーム	VMware ESX / ESXi、KVM プラットフォーム	VMware ESX / ESXi、KVM プラットフォーム
対応ライセンス数	100 ～ 10,000 ユーザー	100 ～ 25,000 ユーザー	100 ～ 50,000 ユーザー
ハードウェア仕様			
ストレージ	16 CPU、RAM サイズ無制限、4 Disk	32 CPU、RAM サイズ無制限、8 Disk	CPU 数無制限、RAM サイズ無制限、16 Disk
仮想 NIC 枚数（最大）	10	10	10
管理	HTTP / S、SSH、CLI、SNMP	HTTP / S、SSH、CLI、SNMP	HTTP / S、SSH、CLI、SNMP

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

DS-FPX-R6-202010-R1