

FortiWeb™

Webアプリケーション/XML統合ファイアウォール

迫られるPCI DSSコンプライアンスへの対応

ネットワークセキュリティの脅威は、バックエンド データベースに保存されている機密情報への入り口であるWebベース アプリケーションを攻撃の標的とするように、巧妙に変化し続けています。そうした深刻なセキュリティ侵害や情報/ID/データの漏洩に対処するべく、PCI標準が制定されました。しかし、Webアプリケーションの脆弱性を解消するための作業は、新たな脆弱性の継続的な発見によるパッチ開発、コード改訂、市場投入までの時間との競争、さらに脆弱性の特定やアプリケーションコードへのアクセスが本質的に難しいことなど、様々な要因で複雑化しているのが現状です。

Webアプリケーションに対する比類ないプロテクション

Webアプリケーション ファイアウォールであるFortiWebファミリは、中大規模エンタープライズ、アプリケーション サービス プロバイダ、およびSaaSプロバイダ向けに、アプリケーション脅威に対する専用の多層プロテクションを提供します。FortiWebのWebアプリケーション/XML統合ファイアウォールは、Webベース アプリケーションとインターネットに接続されるデータを攻撃や漏洩から保護します。SQLインジェクションやクロスサイト スクリプティングのような巧妙な脅威に対する双方向プロテクションを提供する先進の技術を用いて、FortiWebプラットフォームは個人情報漏洩や金融詐欺、企業スパイ活動からの保護に貢献します。FortiWebは、法令や業界のベストプラクティス、社内ポリシーへの準拠状況を監視し、これを施行するために必要なテクノロジーを提供します。

導入に要する時間の短縮とコスト削減を実現

FortiWebでは、Webアプリケーション ファイアウォール、XMLフィルタリング、Webトラフィック高速化、およびアプリケーション トラフィック ロードバランシング機能が1台の機器に統合されるとともに、ユーザ単位の価格設定ではないため、導入コストを大幅に削減することができます。これによって、インターネットでやりとりされる規制対象のデータを保護するために必要な時間が劇的に短縮され、ポリシー施行や法令順守に伴う課題の解決も容易になります。アプリケーションを認識するそのインテリジェントなロードバランシング エンジンによって、アプリケーション パフォーマンスの向上、リソース利用の効率アップ、アプリケーションの安定度の強化、サービスの応答時間の短縮などが実現します。



Webアプリケーションに 対する比類ないプロテクション

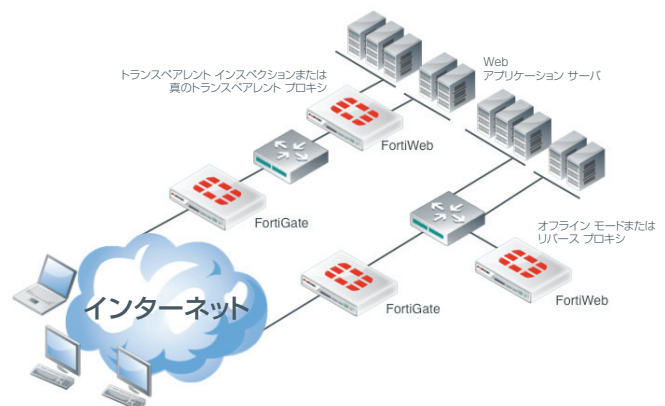
- ✓ ICSA WAF認定
- ✓ WebアプリケーションとXMLの各ファイアウォールを統合
- ✓ 柔軟な導入とシンプルな管理
- ✓ 自動学習ベースのプロファイリング
- ✓ PCI 6.6への準拠を支援するWAFおよび統合スキャナ
- ✓ FortiGuardからの定期更新



FortiWebの導入

FortiWeb導入オプション

- インライン トランスパレント - ネットワーク レベルでの再設計が不要なレイヤ2ブリッジ
- 真のトランスパレント プロキシ - ネットワーク レベルでの再設計が不要。トラフィックを終端させて、単なるインスペクションにとどまらない機能を提供
- リバース プロキシ - URLリライトや高度なルーティング機能といった追加機能を提供
- オフライン スニフing - ネットワークに影響をおよぼしたりレイテンシを発生させたりすることなく環境を監視



柔軟な導入と効率的な管理

- **さまざまな導入オプション**
FortiWebは、トランスペアレント インспекション、真のトランスペアレント プロキシ、リバース プロキシ、およびオフライン スニフィングの各構成に対応することで、あらゆる環境に適合できます。
- **自動学習セキュリティ プロファイリング**
間断なくリアルタイムでユーザ活動を監視することで、保護対象のアプリケーションのセキュリティ モデルを自動かつ動的に構築します。セキュリティ プロファイルを手作業で設定する必要はありません。
- **認証の負荷を軽減**
Webサーバ認証をFortiWebプラットフォームに移すことで負荷を軽減できるとともに、ローカル、LDAP、NTLMなど各種の認証スキームもサポートします。
- **ウィザードおよび定義済みポリシー**
ウィザードを使用した設定作業によりワンクリックで導入できるとともに、ポリシーの作成手順も極めて容易です。
- **ハイパフォーマンス**
受賞実績を誇るFortiASIC™ テクノロジーを搭載するFortiWebは、何万にのぼるWebトランザクションを処理することができ、ハードウェアによる高速化SSLオフロードと先進のロードバランシング機能を提供します。
- **高可用性**
設定を同期化するHA（高可用性）モードでは、不慮の障害が発生したときにネットワーク レベルでのフェイルオーバーを可能にします。
- **ロギングおよびレポーティング**
FortiWebにはすぐに利用可能な数百種類のレポートが装備されているため、管理者や監査役は法令順守を目的とした攻撃、イベント、トラフィックの分析が行えます。

究極のプロテクションとモニタリング

- **情報漏洩防止**
すべての送信トラフィックを厳重に監視することで、クレジットカード情報の漏洩やアプリケーション情報の開示を防止する強力なモニタリングおよびプロテクション機能を提供します。あらゆる種類のイベントに対応する定義済みのルールに加えて、ユーザ自身できめ細かいシグネチャやDLPパターンを作成できます。
- **Web改ざん防止**
何らかの改ざんがなされていないか保護対象のアプリケーションを監視するユニークな機能が搭載され、保存されているバージョンのWEBコンテンツに自動かつ迅速に復元できます。
- **HTTP RFCコンプライアンス準拠検査**
FortiWebは、厳密なRFC基準を保全してエンコーディング攻撃やバッファ オーバーフローをはじめとするアプリケーション固有の攻撃を防止することで、HTTPプロトコルを操作するあらゆる攻撃をブロックします。
- **脆弱性評価**
保護対象のWebアプリケーションを自動的にスキャンおよび分析し、セキュリティ上の弱点や潜在的なアプリケーションの既知および未知の脆弱性を検出することで、PCI DSSに対する包括的なソリューションを完成させます。
- **XMLファイアウォール**
スキーマ検証、IPS、およびルーティング機能とともに、XMLファイアウォールを提供します。
- **アプリケーション層脆弱性プロテクション**
SQLインジェクションやクロスサイト スクリプティングといった極めて複雑な多数の攻撃に対するプロテクション機能を即座に発揮します。自動学習プロファイリング システムと先進の機能を装備するFortiWebは、1つのアプリケーション エレメントまで落とし込んだ細かいルールを作成できます。

コンプライアンスへの準拠支援

- **PCI DSSコンプライアンス**
FortiWebは、PCI DSS規定6.6を満たした包括的なソリューションを構築するWebアプリケーション ファイアウォールに脆弱性スキャナ モジュールを搭載する唯一の製品です。
- **OWASPトップ10の脅威からの保護**
FortiWebは、双方向トラフィック分析と組込み型行動ベース異常検出エンジンに基づくポジティブおよびネガティブ セキュリティ モジュールを実装することで、OWASPトップ10の脅威から保護します。
- **FortiGuard**
FortiWebユーザは、高い評価を獲得しているフォーティネットのFortiGuardサービスを通じて、既知や潜在的なアプリケーション セキュリティ脅威に対抗するプロテクションを研究開発しているFortinet® グローバル セキュリティ リサーチ チームから最新のプロテクションを入手できます。

幅広い攻撃から保護できるFortiWeb

クロスサイト スクリプティング
 SQLインジェクション
 セッション ハイジャック
 Cookie変更/ポイズニング
 クロスサイト リクエスト
 フォージェリ (CSRF)
 コマンド インジェクション
 リモートファイル インクルージョン
 形状変更
 Hiddenフィールド操作

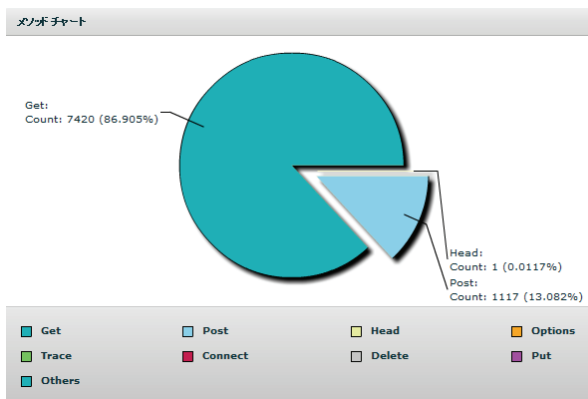
アウトバウンドデータ漏洩
 HTTPリクエスト スマグリング
 リモートファイル インクルージョン
 エンコーディング攻撃
 アクセス制御破壊
 強制ブラウズ
 ディレクトリ トラバーサル
 サイト偵察
 検索エンジン ハッキング
 ブルートフォース ログイン

アクセス レート コントロール
 スキーマ ポイズニング
 XMLパラメータ改変
 XML不正侵入防御
 WSDLスキャン
 再帰ペイロード
 外部エンティティ攻撃
 バッファオーバーフロー
 DoS

FortiWeb自動学習プロファイリング

自動学習プロファイリング機能は完全にトランスペアレントであり、アプリケーションやネットワーク アーキテクチャに一切変更を施す必要がありません。FortiWebは、プロファイルを構築するためにアプリケーションをスキャンするのではなく、アプリケーションが受信する際にトラフィックを分析します。アプリケーションの包括的なセキュリティ モデルを構築することで、FortiWebは任意の既知または未知の脆弱性およびゼロデイ攻撃から保護できるようになっています。

Webアプリケーション ファイアウォールの導入を定めるPCI 1.2セクション6.6の一部として、継続的に脆弱性評価を実行（年1回、変更後に脆弱性修正および再スキャン）することにより、新たな脆弱性に対処することも選択肢の一つです。FortiWebは、WebアプリケーションファイアウォールとWebアプリケーション スキャナの両方を提供し、組織を支援します。



FortiWeb脆弱性スキャナ

アプリケーション全体に定期スキャンやオンデマンド スキャンを実行してWeb脆弱性を検査します。PCI DSS 6.6を満たすようWAFを補完します。

http://192.168.150.174:81
印刷可能 クローズ

概要

- スキャンサマリー
- 見つかった警告
- 影響を受けるページ

アプリケーション脆弱性

- Cross-Site Scripting (28)

一般的な脆弱性

- Information (15)

サーバ情報

- ウェブサーバー
- 見つかったURL/ページ
- 入力があるURL
- 外部のリンク

スキャンサマリー

Target	http://192.168.150.174:81
Server	Microsoft-IIS/5.1
Scan Start Time	Thu Aug 19 12:36:35 2010
Scan End Time	Thu Aug 19 12:36:40 2010
Scan Mode	Normal Checking Mode
Scan For	Common Vulnerability, Cross-Site Scripting, SQL Injection, Source Disclosure, OS Commands
Total URLs and Forms Found	2 (1 Pages/Applications, 2 URLs with Inputs)
Total External Hyperlinks	0 (0 email links)
Total Alerts Found	43

見つかった警告

重要度	Count
High Severity	28
Medium Severity	0
Low Severity	0
Information	15

カテゴリ

カテゴリ	Count
Common Vulnerability	15
Cross-Site Scripting	28

影響を受けるページ/アプリケーション

ページ/アプリケーション	Count
1 /test/rdpassnext.asp	1

技術仕様	FortiWeb-400C	FortiWeb-1000C	FortiWeb-3000C	FortiWeb-4000C
インタフェースとモジュール				
10/100/1000 インタフェース	4	4	6	6
1000 Base-SX バイパスインタフェース	-	-	2 ペア*	2 ペア
USBインタフェース (A端子)	-	2	4	4
内蔵ストレージ	1 TB	1 TB	2 TB	2 TB
増設ストレージ	-	-	1 TB x 4	1 TB x 4
システム性能				
HTTPスループット	100 Mbps	500 Mbps	1 Gbps	2 Gbps
最大HTTPトランザクション/秒	10,000	27,000	40,000	70,000
レイテンシ	ミリ秒未満			
ユーザ数無制限ライセンス	○			
ハードウェア仕様				
高さ	4.4 cm	4.3 cm	8.9 cm	8.9 cm
幅	43.5 cm	43.4 cm	44.5 cm	44.5 cm
奥行	36.4 cm	62.71 cm	73.7 cm	73.7 cm
重量	6.42 kg	11 kg	28.6 kg	28.6 kg
ラック マウント	○			
AC電源	100 - 240 VAC、 50 - 60 Hz、4 A (最大)	100 - 240 VAC、 50 - 60 Hz、7 A (最大)	100 - 240 VAC、 50 - 60 Hz、9 A (最大)	100 - 240 VAC、 50 - 60 Hz、9 A (最大)
消費電力 (平均)	181 W	189 W	200 W	200W
冗長電源 (ホットスワップ対応)	-	-	○	○
動作環境				
動作温度	0 ~ 40°C		0 ~ 40°C	
保管温度	-25 ~ 70°C		-40 ~ 65°C	
湿度	10 ~ 90% (結露しないこと)		5 ~ 95% (結露しないこと)	
準拠規格・認定				
準拠規格	FCC Class A Part 15, C Tick, VCCI, CE, UL/cUL, CB			

*FortiWeb-3000C-FSX

FortiWeb仮想アプライアンス	FortiWeb-VM02	FortiWeb-VM04	FortiWeb-VM08
技術仕様			
ハイパーバイザ	VMware ESXi / ESX v3.5, v4.0, v4.1		
仮想CPU数(最大)	2	4	8
メモリ(最小)	1024 MB	1024 MB	1024 MB
仮想NIC枚数(最小/最大)	2 / 4	2 / 4	2 / 4
ストレージ容量(最小)	40 GB	40 GB	40 GB
システム性能			
HTTPスループット	100 Mbps	500 Mbps	1 Gbps
最大HTTPトランザクション/秒	8,000	24,000	36,000
ユーザ数無制限ライセンス	○		

数値はネットワークトラフィックとシステム構成によって異なります。

測定条件: Dell PowerEdge R710 サーバ (2 x Intel Xeon E5504 2.0 GHz 4MBCache)、VMware ESXi 4.1

FortiWeb-VM02は1G vRAM、FortiWeb-VM04およびFortiWeb-VM08は3G vRAM

FortiCareサポートサービス: 全てのフォーティネット製品においてグローバルサポートを提供するサービスです。FortiCareサポートによりフォーティネット製品を最適にご利用いただくことが可能になります。サポートプランには、Technical Assistant Center (TAC)を通じて、製品サポート(ソフトウェア、ハードウェア)を当社の1次代理店様にご提供します。また、万一のハードウェア不良時に備え、センドバック方式によるハードウェアRMA交換サービス(良品、後出し)を含む平日の9時間サポートから、オプションとして、プレミアムサポート、プレミアムRMA交換サービス、プロフェッショナルサービス等もごございます。 *FortiCareサポートサービスは、当社の1次代理店様経由でご提供させていただきます。

FortiGuardサブスクリプションサービス: フォーティネット製品に対して、動的な自動セキュリティアップデート配信を提供するサービスです。フォーティネットのグローバルセキュリティ研究チームが開発するこれらのセキュリティアップデートにより、巧妙な脅威に対する最新のプロテクションが確保できます。サブスクリプションには、アンチウイルス、不正侵入検知/防御Webコンテンツフィルタリング、アンチスパム、脆弱性/コンプライアンス管理、アプリケーション制御、Webアプリケーションファイアウォール、データベースセキュリティサービスなどが含まれます。

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

TEL:03-6434-8531/8533

www.fortinet.co.jp

お問い合わせ