Web アプリケーションファイアウォール

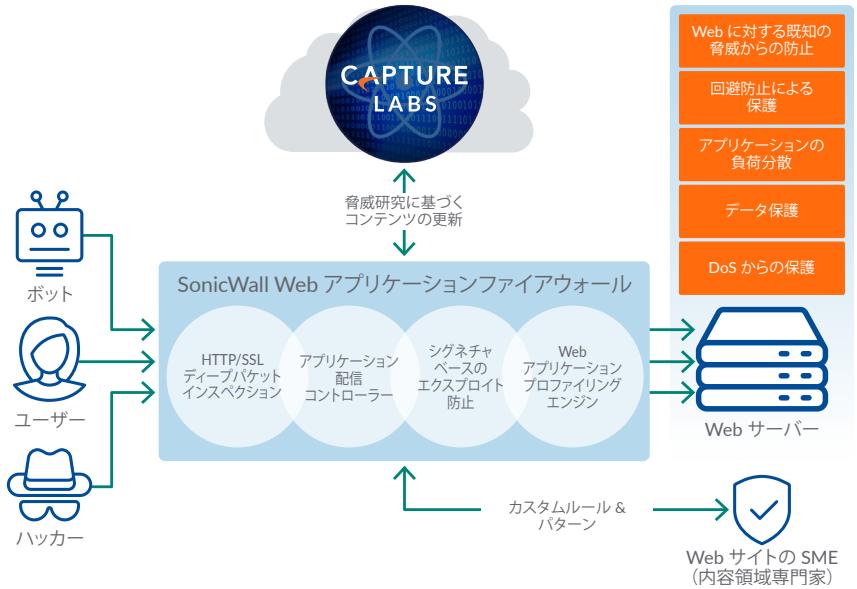
SonicWall Web アプリケーションファイアウォールは、Web アプリケーションのセキュリティ、データ漏洩防止、パフォーマンスに対する包括的な基盤を、オンプレミス、もしくはクラウド上で提供します。

SonicWall Web アプリケーションファイアウォール（WAF）ソリューションは、多層防御戦略を実現し、プライベート / パブリックもしくはハイブリッドのクラウド環境で実行される Web アプリケーションを保護します。 この製品は、すぐに使える、完全なコンプライアンスソリューションを組織に提供し、管理および導入が容易な、アプリケーション中心のセキュリティを実現します。

SonicWall WAF シリーズは、組織に高度な Web セキュリティツール / サービスを提供し、データと Web 資産を、Web をベースにした最新の脅威から保護する、フル機能の Web アプリケーションファイアウォールです。 この製品は、定期的に更新される既知のシグネチャのデータベースを参照して、レイヤ 7 の Web トラフィックにディープパケットインスペクションを実施し、Web アプリケーションへの脅威を検知すればアクセスを拒否し、ユーザーを説明付きのエラーページにリダイレクトします。 また、SonicWall WAF は Web アプリケーションの正規の利用 / 動作を規定し、アプリケーションの侵害、データ窃取、サービス妨害などの試みを示唆する異常を検知します。

WAF はシグネチャベースとアプリケーションプロファイリングのディープパケットインスペクションを組み合わせて用い、また、リアルタイムでハイパフォーマンスな侵入スキャンエンジンも採用しています。この製品は、そのためにイベントドリブンのアーキテクチャを使用し、Open Web Application Security Project（OWASP）が示したような進化する脅威、および Web アプリケーションに対するより高度な脅威、Denial of Service（DoS）攻撃、コンテキストに対応したエクスプロイトなどからの動的な防御を行います。 さらに、この製品は Web アプリケーションが正規に利用されているときの動作を学習、調査、基準化し、アプリケーションの侵害、データ窃取、サービス妨害などの試みを示唆する異常を検知します。

WAF は、仮想化によるスケールメリットの経済性を提供し、VMWare や Microsoft Hyper-V をベースにしたプライベートクラウ



メリット：

Web アプリケーションにおける脅威の管理

- Web アプリケーションのトラフィックを完全に管理および制御して攻撃される領域を縮小
- プロトコルごとのアクティビティに限らない、Web コミュニケーションの動作とロジックの検査
- Web アプリケーションの動作における異常を検出、警告

Web アプリケーションの保護

- 仮想パッチおよびカスタムルールを使用して、既知のゼロデイ脆弱性から保護
- OWASP Top 10 によって報告される、最新の脆弱性と脅威に対する防御
- アプリケーション Dos/DDoS 攻撃に対して Web サーバーの整合性とパフォーマンスを維持

データ漏洩防止（DLP）

- データマスキングおよびページブロック技術によりデータ盗難を防止
- 広範なアクセスセキュリティ制御により、攻撃者がユーザーのアカウントおよび Web サーバー上のすべてのアカウントにアクセスするのを阻止

アプリケーション配信を高速化

- キャッシング、圧縮、その他の HTTP/TCP 最適化を有効にしてアプリケーション配信を高速化
- SSL トランザクションのオフロードにより作業負荷を軽減し、パフォーマンスを向上させる
- レイヤ 7 ロードバランシングを実行して、クラスター化された Web サーバー間の負荷を分散

ド、あるいは、AWS や Microsoft Azure のようなパブリッククラウド環境に対し、仮想アプライアンスとして導入することができます。これによって組織には、物理的な WAF が持つセキュリティ上のメリットがすべて提供されると同時に、システム拡張性、俊敏性、システムプロビジョニングの速度、管理の容易性、コストの削減など、システム仮想化による運用上および経済上での利益ももたらされます。

負荷分散、コンテンツのキャッシング、圧縮、接続の多重化などのアクセラレーション機能により、保護された Web サイトのパフォーマンスが向上し、トランザクションに対するコストが大幅に削減されます。 堅牢なダッシュボードにより、シグネチャデータベースのステータス情報、起動後に検出・防止された脅威など、監視・ブロッキングに関わるすべてのアクティビティを概観可能なステータスページを備えた、使いやすい Web ベースの管理インターフェースが提供されます。

このシリーズでは 4 つのモデルが利用可能で、モデルの違いは検査能力の差を意味しています。このシリーズの製品は、広範囲にわたるパブリック / プライベートなクラウド / 仮想化導入ユースケースに対して、導入することができます。

導入オプション

SonicWall WAF は、仮想化・クラウド化された多様なプラットフォームにおける、さまざまなプライベート / パブリッククラウドセキュリティのユースケースに向けて導入することができます。WAF シリーズは以下のプラットフォームで導入可能です。

1. プライベートクラウド：
   - VMware ESXi
   - Microsoft Hyper-V
2. パブリッククラウド：
   - アマゾンウェブサービス（AWS）
   - Microsoft Azure

モデル	演算容量	推奨される AWS インスタンス	推奨される MS Azure インスタンス
WAF 200	2 vCPU	C5.large	Standard_F2s_v2
WAF 400	4 vCPU	C5.xlarge	Standard_F4s_v2
WAF 800	8 vCPU	C5.2xlarge	Standard_F8s_v2
WAF 1600	16 vCPU	C5.4xlarge	Standard_F16s_v2

*Intel Xeon E5-2600 など、サーバークラスのコンピューティングプロセッサーを前提としています

WAF の機能概要

Web アプリケーションセキュリティ

- OWASP Top 10 からの保護
- CSRF からの保護
- Cookie 改ざんからの保護
- Web サイトにおけるフィンガープリンティングの検知
- 機密データ保護 - マスキングおよびブロック
- 速度制限と DoS からの保護
- 回避手法に対応した検査
- シグネチャの自動更新
- Web アプリケーションプロファイリング & 自動ルール生成
- アクセスポリシー（地域 IP、URL、ユーザーに基づく）
- カスタムルール & ルールチェーン
- カスタマイズされたエラーレスポンス

ボットネットからの保護

- 地域 IP と脅威インテリジェンスをベースにした保護的フィルタリング
- ブラックリストとホワイトリスト
- ブロックと Captcha をベースにした復旧サポート

Web アプリケーションの安全な配信

- 安全な Web アプリオフロード
- SSL インスペクション & PFS
- スタック認証（2FA、OTP、Client-Cert、他）
- セッションのログアウト用タイマー
- レイヤ 7 の負荷分散
- Web アプリヘルスモニタリング
- Web アプリアクセラレーション - コンテンツのキャッシング、圧縮、TCP 最適化

管理

- CLI サポート付きのカスタマイズ可能な Web ポータル
- AD/LDAP、RADIUS、証明書による管理者認証
- ソフトウェアの自動更新

監視 & レポート

- SNMP のサポート
- イベント / 監査ログ & Syslog
- E メールによるアラート
- システムの監視 & 診断
- 脅威ダッシュボード
- ヘルスダッシュボード
- PDF レポートのエクスポート

プラットフォーム & ライセンス

- VMWare & MS Hyper-V、AWS & MS Azure（BYOL）
- 容量に基づくサブスクリプションライセンス

特徴

Web アプリケーションのセキュリティとボットからの保護	
OWASP Top 10 からの保護	SQL インジェクション、XSS/CSRF、Web フィンガープリンティング、その他を含む、Open Web Application Security Protection（OWASP）が公表する既知の攻撃トップ 10 から、Web アプリケーションを保護します。
機密データ保護	機密データを表示するページのブロック機能を用いて、機密データの流出を防止します。また、クレジットカード番号や社会保障番号などの個人情報（PII）をマスキングします。
セッション管理の制御	セッションの管理と認証に用いる強力な機能を提供して、ワンタイムパスワード、2 要素認証、シングルサインオン、クライアント証明書認証などの認証要件を厳格化します。
Web フォームへの入力の検証	クライアントからのリクエストに悪意あるコードが含まれている可能性を検査、検証し、バックエンドのサーバーを、ハッカーがセキュリティ防御の迂回を試みて送信したトランザクションから保護します。
セッションハイジャックの監視	盗聴、侵入、さらには Web セッションの窃取も検知し、攻撃者による悪意ある行動の防止に役立てます。
Perfect Forward Secrecy（PFS）による防御	過去のセッションを、未来における秘密鍵やパスワードの危殆化から保護します。
クロスサイトリクエストフォージェリ（CSRF）攻撃を拒否	ユーザーがあらかじめ認証を受けている Web アプリケーションに、悪意ある Web サイトが別の Web サイトから不正なリクエストを送るのを認識し、防止します。
コードインジェクション攻撃および遠隔コードインクルージョン攻撃のブロック	基礎となる OS に対する Web アプリケーションのインターフェースを悪用し、任意のコードや、悪意あるペイロードのダウンロードなど有害なコマンドを、意図せず実行させる攻撃を認識し、遮断します。
Cookie 改ざんからの保護と暗号化	暗号化と除外により、Cookie の窃取、ポイゾニング、不正確さ、クロスサイトクッキングから保護します。
カスタムルールに対する速度制限	カスタムルールやルールチェーンがマッチしている速度を追跡して、辞書攻撃やブルートフォース攻撃をブロックします。
Web サーバーのフィンガープリンティングからの保護	ハッカーが、Web アプリケーションソフトウェア、そのバージョン、プラットフォームを識別して、そのソフトウェアについて報告されている脆弱性を悪用するのに役立てる、Web サーバーへのフィンガープリンティング攻撃から保護します。
Web サービス/API の保護	Web サービスと API に含まれる重要な情報の露出を防止します。
CMS プラットフォームの保護	仮想パッチと共にカスタムルールを使用して、WordPress、Joomla、Documentum など、広く使用されている CMS ツールに見つかった新しい脆弱性を無効化します。
サービス妨害からの保護	Web アプリケーションに対するトラフィックについて、速度制限と帯域幅調整を実施し、アプリケーションをサービス妨害（DoS）から保護します。
シグネチャの自動更新	Web アプリケーションに関して新しく出現する脅威についての、Capture Labs による研究に基づいて、シグネチャを定期的に自動更新します。
Web アプリケーションプロファイリング	独自のプロファイリングエンジンが、Web アプリケーションに対する既知の正しいアクティビティを監視して、基準を確立し、そのアプリケーションに向けた WAF のルールを自動的に生成します。基準制定のために、信頼できる IP アドレスの利用をサポートします。
カスタムルール & エラーレスポンス	アプリケーション固有のロジックに基づいたカスタムルールと、シリアル化されたロジックに向けたルールチェーンを作成することができます。ルールにマッチした際のブロックページとエラーメッセージをカスタマイズすることができます。
ボットネットフィルタリング & 復旧	地域情報、明示的な IP アドレス/範囲、内蔵された脅威インテリジェンス統合の活用などに基づき、ボットネットフィルタリングを実現します。それぞれのタイプのボットネットフィルターに対し、Captcha による復旧をサポートします。また、ブラックリストとホワイトリストの作成もサポートします。

Web アプリケーションの安全な配信	
Web アプリケーションの安全なオフロード	アプリケーションのフロントエンドをオフロードするため、リバースプロキシとして導入されます。一定時間操作のないユーザーセッションを自動ログアウトする機能も搭載されています。
SSL インスペクション	HTTP と SSL/TLS 両方のトラフィックを内蔵サポートすると共に、SSL/TLS トラフィックを受信し、Web アプリケーションに HTTP トラフィックとして回送する機能も備えています。SSL 証明書をインポート、保存することができ、証明書署名要求（CSR）と CRL 検証のブローカーとなる機能もサポートしています。
スタック認証	保護された Web アプリケーションに対してスタック認証を適用し、サポート外の Web アプリケーションに対する多要素認証や認証の強制をサポートします。
レイヤ 7 の負荷分散	セッション持続性、カスタマイズ可能なロジック、フェイルオーバーへのサポートを備えた、使いやすい負荷分散機能が、Web アプリケーションに向けたヘルスモニタリングも提供します。
Web アプリケーションアクセラレーション	コンテンツのキャッシング、コンテンツの圧縮、ネットワーク帯域幅最適化を組み合わせて活用し、高速な Web 体験を提供します。

管理	
Web ポータル & コマンドラインインターフェース	ロゴを含むカスタマイズ可能なルックアンドフィールを備える、GUI ベースの管理に向けた親しみやすい Web ポータルを提供します（サービス事業者向け）。さらに、コマンドラインインターフェース（CLI）ベースの管理もサポートします。
管理者認証	MS Active Directory、LDAP、RADIUS、証明書ベースの認証など、多数の方式による管理者認証をサポートします。強力なパスワードの強制、およびロールベースの認証を含みます。
ソフトウェアの更新	SonicWall Cloud による自動化されたソフトウェア更新が、ライセンスされた WAF すべてに対し自動的にダウンロードされ、適用されます。

監視 & レポート	
ログ & アラート	セキュリティ、システム、監査イベントに対する精細なログは、ログレベルをコントロールし、SIEM プラットフォームのような外部システムに向け、Syslog 経由でログ転送するよう設定できる柔軟性を備えています。重大性に基づき、E メールでイベントに関するアラートを発します。
システム監視 & SNMP のサポート	デバッグモードと自動生成のテクニカルサポートレポート（TSR）を用いた広範なシステム診断を提供します。ダウンロードが容易な MIB を用いた SNMP で、サードパーティ製品を監視します。
ダッシュボード & レポート	Web セキュリティにおけるトップ事項 & ボットネットの脅威（Top Web Security & Botnet Threats）、最新の警告（Latest Alerts）、Web アプリケーションの状態とパフォーマンス（Web Application Health and Performance）などに向けた、直感的なダッシュボードを提供します。Capture Labs によるサポートを備えた、世界における脅威状況を参照可能なダッシュボードを提供します。PDF 形式のレポートがダウンロードできます。

プラットフォーム & ライセンス	
プラットフォーム	プライベートクラウドのハイパーバイザーである VMWare と MS Hyper-V、およびパブリッククラウドである AWS と MS Azure に導入可能な、仮想アプライアンスとして提供されます。AWS および Azure に対しては、ライセンス持ち込み（BYOL：Bring-Your-Own-License）モデルがサポートされます。
ライセンスモデル	期限付きの使用権が付与されたサブスクリプションライセンスとして調達され、24 時間体制のサポートサービスが含まれます。容量に基づくさまざまな「モデル」として、また、1 年もしくは複数年の SKU で利用可能です。

システム仕様

	WAF 200	WAF 400	WAF 800	WAF 1600
サポートされるプラットフォーム	VMware ESXi v6.5 Microsoft Hyper-V Manager 6.2 / 6.3 Amazon AWS Microsoft Azure			
WAF Tier	Tier 1	Tier 2	Tier 3	Tier 4
SSL トランザクション数/秒	6,000	12,000	24,000	48,000
SSL スループット	500 Mbps	1 Gbps	2 Gbps	4 Gbps
推奨される vCPU 数*	2	4	8	16
推奨されるメモリ	4 GB	8 GB	16 GB	32 GB
推奨されるストレージ	8 GB	8 GB	8 GB	8 GB
推奨される AWS インスタンス	c5.large	c5.xlarge	c5.2xlarge	c5.4xlarge
推奨される Azure インスタンス	Standard_F2s_v2	Standard_F4s_v2	Standard_F8s_v2	Standard_F16s_v2

* これは、企業クラスの典型的なサーバーシステムに基づくものです。詳細については、導入ガイド（Deployment Guide）をご覧ください。

当社について

創設後 25 年以上にわたり、SonicWall はこの業界の信頼できるセキュリティパートナーとして存在しています。ネットワークセキュリティから、アクセスセキュリティ、電子メールセキュリティまで、SonicWall は自社の製品ポートフォリオを継続的に進化させることで、組織の革新、促進、成長を可能にします。世界の約 200 の国と地域に 100 万台を超えるセキュリティデバイスを持つ SonicWall は、お客様が自信を持って未来を受け入れられるようにします。

SonicWall, Inc.
1033 McCarthy Boulevard | Milpitas, CA 95035
Refer to our website for additional information.
www.sonicwall.com

Datasheet-WebAppFirewall-US-KJ-MKTG2273

SONICWALL