THUNDER ADC WEB アプリケーションファイアウォール

Web攻撃を阻止し、大きな犠牲を伴うデータ侵害を防止

課題:

Webサイトに包囲網が敷かれている。脆弱性を見つけて悪用するために、悪質なユーザーとボットが絶えずWebサイトの調査を行い、攻撃を仕掛けている。

解決策:

A10 Thunder ADCに搭載された、ハイパフォーマンスかつ豊富な機能を提供するWebアプリケーションファイアウォールを利用して、攻撃からWebサイトを保護。

メリット:

- SQLインジェクション、クロスサイトスクリプティングなどの危険な攻撃と、OWASPの上位10位のリスクを阻止
- PCIコンプライアンス要件6.6に準拠
- 設定を簡素化するテンプレートと合理的な管理機能によって運用コストを削減
- A10のAdvanced Core Operating System（ACOS）を利用して、高トラフィックなWebサイトへの保護を拡張
- 攻撃からの保護、認証、アプリケーションデリバリーを単一のプラットフォームに統合

Webアプリケーションは今日のサイバー戦争の最大の戦場となりました。サイバー犯罪者、政治的ハッカー、国家による攻撃が、企業や政府機関に仕掛けられています。組織の防御における脆弱なリンクになることが多いために、アプリケーションはサイバー戦争の前線と化してしまったのです。実際、アプリケーションの96%が脆弱性を持っている[1]ことから、攻撃者は悪用できる弱点を探すため常にWebサイトを綿密に調査しています。

Webアプリケーションを保護するためには、正当なユーザーのブロックやアプリケーションのパフォーマンスの低下を伴わずに攻撃を緩和できるソリューションが必要です。このソリューションでは、設定が簡単で詳細なロギングやグラフィカルなレポートをサポートする必要があります。

アプリケーションデリバリーコントローラー（ADC）A10 Networks® Thunder®ADC製品ラインは、Webアプリケーションの攻撃、綿密な調査、偵察を阻止する強力で精度の高いWebアプリケーションファイアウォール（WAF）を提供します。複数の階層型防御を組み合わせたThunder ADCにより、サイバー犯罪者と政治的ハッカーを締め出し、機密情報の漏えいを防止することができます。ICSA Labsの認定を取得したThunder ADCは、OWASP（オープンWebアプリケーションセキュリティプロジェクト）の上位10位のセキュリティリスクを緩和し、アプリケーションの安全性を保持します。

Thunder ADCの機能：

- 合理化された管理機能と直感的に利用できるWAFテンプレート
- ホワイトリストとブラックリストを使用したセキュリティモデル
- A10 Networks Advanced Core Operating System（ACOS®）によって強化された高度なパフォーマンスと低遅延
- A10 Networks aFleX®ディープパケットインスペクション（DPI）スクリプトテクノロジーを活用した、プログラミングによるアプリケーショントラフィックの制御
- CEFに準拠した高速なロギングとグラフィカルなレポート
- PCI 6.6に準拠するICSA認定Webアプリケーションファイアウォール

アプリケーションの脅威の増大

攻撃者は、SQLインジェクション、クロスサイトスクリプティング（XSS）、クロスサイトリクエストフォージェリー（CSRF）などの攻撃を使用して24時間体制でWebサイトを攻撃しています。攻撃に対抗する専用の保護機能が導入されていなければ、ハッカーがWebサイトの脆弱性を悪用してデータを盗み出し、損害を伴うデータ侵害やブランドへの影響が発生する可能性があります。

パッケージアプリケーションへの最近の攻撃によって、セキュアコードを記述してアプリケーションをロックダウンする古い戦略の大きな欠陥が明らかになりました。パッケージアプリケーションは社内ではなく第三者によって開発されているため、組織はアプリケーション保護のためにセキュアコードを記述できないのです。2013年にWebアプリケーションに起因する侵害がすべての侵害の35%を占めたことを考えると[2]、組織にはWeb攻撃をブロックするプロアクティブな防御が必要です。

[1] Cenzicアプリケーションセキュリティトレンドレポート、2014年
[2] Verizon 2014データ侵害調査レポート

多くの組織のセキュリティ認識は誤っています。導入済みのネットワークファイアウォールと侵入防止システムで、アプリケーションレイヤーの脅威を阻止できると考えているのです。残念なことに、このような汎用セキュリティ製品は高度なWeb攻撃を阻止できるきめ細かい防御や専門的な防御を提供していません。

Thunder ADCが攻撃からWebアプリケーションを保護

Webアプリケーションを保護するためには、多数の脅威を緩和しながらも、卓越したアプリケーションパフォーマンスを提供できるWebアプリケーションファイアウォールを導入する必要があります。それを実現するのがA10 Thunder ADCです。Thunder ADCは、共有メモリーアーキテクチャーと64ビットの拡張性を駆使して高速で強靭な保護を提供します。

豊富な機能を備えICSAの認定を受けたThunder ADCのWAFは、Web攻撃が脆弱なアプリケーションに到達する前にブロックします。Webサーバーの前にリバースプロキシーとして導入されると、Thunder ADCはWeb要求および応答を検査してWeb攻撃をブロックするか攻撃の不適切な部分を削除し、アラートを送信できます。Thunder ADCは、複数の防御層を活用して幅広いWeb攻撃を緩和し、PCI 6.6コンプライアンスにも対応します。

Thunder ADC Webアプリケーションファイアウォールにより、以下のことが可能になります。

- **犠牲を伴うデータ侵害を阻止**
  – Thunder ADCは、OWASPの上位10位の脅威[3]を含むアプリケーションの脅威に対して強力な保護を提供するため、データの盗用と改ざんを防ぐことができます。自動的なアプリケーション学習機能やホワイトリスト・ブラックリストを活用するセキュリティを組み込んだThunder ADCは、攻撃を正確に特定できます。また不適切な部分を削除する機能によって、ユーザーのアプリケーションアクセスを妨害せず、問題も引き起こさずに攻撃を無害化できます。

- **PCI 6.6コンプライアンスを達成**
  – クレジットカード業界のセキュリティ基準（PCI DSS）は、カード所有者のデータを保護するために、加盟店、処理会社、その他の関係者向けに規定されているガイドラインです。Thunder ADCにはWAFが統合されているため、PCI要件6.6に準拠できます。

- **データ漏えいの防止によってデータとブランドを保護**
  – Thunder ADCは、送信トラフィックにクレジットカードや社会保障番号などの機密データが含まれていないかどうかを検査できます。定義しやすいPCRE（Perl Compatible Regular Expressions）マスクを利用することで、Webサイトフォーラムに表示される不快な単語などのカスタム文字列を難読化できます。

- **アプリケーションの脆弱性を緩和**
  – 導入後すぐにSQLインジェクションやクロスサイトスクリプティングなどのWeb攻撃から保護する機能を提供するThunder ADCは、ハッカーによるWebサイトの脆弱性の悪用を阻止できます。お客様は残りのすべての脆弱性に「仮想パッチ」を適用するようにカスタムaFleXスクリプティングポリシーを定義することで、アプリケーションを悪用から確実に保護できます。

- **セッションとCookieを保護**
  – Cookieの暗号化（オプション）機能を通じて、Thunder ADCはCookieポイズニング、Cookieインジェクション、セッションリプレイなどの脅威からアプリケーションを保護できます。Thunder ADCの管理者は、どのCookieを暗号化するかを定義できるので、セッションCookieのような機密性の高い読み取り専用Cookieのみに保護を限定できます。

- **自動化攻撃を阻止**
  – Thunder ADCは、既知のボットエージェントを認識しているため、ボットや自動化クライアントを検出します。また、要求レート制限とaFleXポリシーを備えるThunder ADCは、リクエストが多すぎるユーザーや、標準Webクライアントのようなふるまいをしないユーザーをブロックできます。Thunder ADCは、IP地理情報を活用して、特定の地域から発生した自動化攻撃をブロックすることも可能です。

- **攻撃者によるWeb防御回避を確実に阻止**
  – Thunder ADCは、検査前に各Web要求を正規化するので、攻撃者は難読化によってWebアプリケーションファイアウォールを迂回できなくなります。またThunder ADCは、HTTP要求に対してしきい値の上限を設定し、その上限を超える要求をブロックすることにより、バッファオーバーフローを阻止します。

- **サーバー情報を隠匿してWebサイト偵察を防止**
  – Thunder ADCは、HTTP応答ヘッダーを修正して、オペレーティングシステムやWebサーバーデータなどのサーバー情報を「隠匿」できます。攻撃の多くは、個別のサーバー、オペレーティングシステム、フレームワークに的を絞っているため、サーバー情報を隠匿することで、ハッカーによるアプリケーション脆弱性の悪用が非常に難しくなります。

- **検索エンジンによる機密データのインデックス化を防止**
  – Thunder ADCは、検索エンジンのIPアドレスやユーザーエージェントから保護対象Webサイトのパスワード保護セクションやプライベートセクションへの要求をブロックできます。管理者は、Thunder ADCのWebユーザーインターフェイスを利用して、特定のWebページへのアクセスや特定のユーザーエージェントをブロックするポリシーを定義できます。きめ細かい設定が可能なaFleXポリシーを通じて、Webサーバー応答、ソースIPアドレス、ユーザーエージェントなどのパターンに基づいてアクセスを制御する高度な相関付けポリシーを作成できます。

- **大きな被害をもたらすDDoS攻撃からWebアプリケーションを保護**
  – ネットワークレイヤーとアプリケーションレイヤー両方へのDDoS（分散型サービス拒否）攻撃を阻止できるThunder ADCは、中断のないアプリケーションアクセスを保証します。ハードウェアベースのFTA（Flexible Traffic Accelerator）テクノロジーを搭載するThunder ADCモデルを選択すると、一般的なDDoS攻撃を非常に高速に検知してブロックできます。

- **管理の効率化**
  – 直感的に利用できるWAFテンプレートと自動学習ポリシーにより、Thunder ADC Webアプリケーションファイアウォールは簡単に設定および導入できます。

Thunder ADCに統合されたWebアプリケーションファイアウォールは、ICSA LabsからWAF認定を取得しています。ICSA Labsのテストと認定によって、Thunder ADCは目的どおりに動作し、悪用と攻撃からアプリケーションサービスを保護できることが実証されています。

ICSA labs CERTIFIED WEB APPLICATION FIREWALL

[3] OWASP（オープンWebアプリケーションセキュリティプロジェクト）の上位10位とは、セキュリティ専門家の幅広いコンセンサスによって決定された最も重大なWebアプリケーションセキュリティの欠陥です。

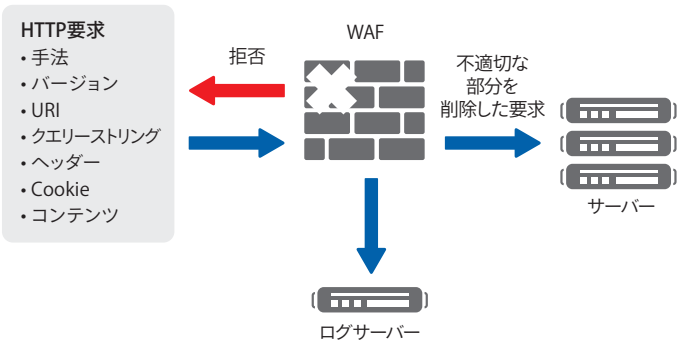

図1：Thunder ADCと、統合されたICSA認定のWAFによって、攻撃をブロックすることも、悪質なコンテンツやログアクティビティの要求の不適切な部分を削除することも可能

Webアプリケーションファイアウォールの機能

ホワイト/ブラックリストを使用したセキュリティと自動学習

WAFは、Web攻撃を阻止するために、既知の攻撃と同様に既知の正しい動作も見分けなければなりません。Thunder ADCのWAFは、保護対象アプリケーションの構造を自動的に学習し、異常な要求と攻撃を検知します。多数のWAFテンプレートを同時にサポートすることにより、Thunder ADCは新しいURLの学習とトラフィックの保護を同時に行うことができます。

既知の攻撃は、SQLインジェクション、クロスサイトスクリプティングなどの攻撃を定義するリストによって検知されます。管理者は、Webユーザーインターフェイスかcliからブラックリストもホワイトリストも簡単に表示および修正できます。

aFleXスクリプティングポリシーの統合

A10 Thunder ADC向けの高度なスクリプト言語であるaFleXは、アプリケーショントラフィックを完全に制御するために必要な柔軟性と強力な機能を管理者にもたらします。aFleXは容易に習得できるスクリプト言語、TCL（Tool Command Language）をベースに構築されており、トラフィックのブロック、トラフィックのリダイレクト、コンテンツの修正など多くのアクションを実行することができます。

WAFルールはaFleXポリシーに統合できるので、管理者はWAFの動作をきめ細かく制御できます。たとえば、ソースIPアドレスや宛先URLに基づいて特定の違反を無視する例外や、厳格なポリシーを適用する例外を作成できます。

またaFleXを利用することで、WAF管理者は、基盤アプリケーションにパッチが適用されるまで脆弱なWebアプリケーションに「仮想パッチをあてる」というカスタムルールを適用することも可能です。柔軟なaFleXスクリプト言語を利用すれば、数行のシンプルなスクリプトを作成するだけであらゆるタイプのWebアプリケーションのセキュリティの問題を解決できます。

地理情報を利用して国別にアクセスを監視またはブロック

政治的ハッカーとサイバースパイの台頭により、組織が地理情報に基づいてアクセスを抑制する必要性が高まっています。A10の地理情報ポリシーを利用すると、地理情報の制御が容易になります。A10のお客様は、ご利用の地理情報サービスからサードパーティの地理情報リストをインポートすることで、特定の地域から発生しているトラフィックを警告またはブロックできます。地理ベースの制御を通じて、特定の地域に由来するDDoS攻撃の阻止や、エクスポートコンプライアンス要件への対応が実現します。

XMLとJSONの保護

今日の主要なWebサイトは、XMLとJSON（JavaScript Object Notation）によって強化されています。動的でインタラクティブなアプリケーションの多くは、JSONを使用してほぼリアルタイムでWebデータを更新しています。Thunder ADCは、JSONトラフィックにSQLインジェクションやXSSなどの攻撃が含まれているかを検証できるほか、配列の長さや構造の深さなどのJSON要素も制限できます。また、XMLファイルを解析および検証し、WSDL（Web Services Description Language）スキーマを適用することで、XMLファイルが正しくフォーマットされていることも保証できます。

負荷分散、認証、DDoS防御の統合

Thunder ADCは、アプリケーションデリバリーとセキュリティの完全なソリューションの提供を通じて、お客様のネットワークアーキテクチャーの簡素化と統合を支援します。Thunder ADCは、Webトラフィックの負荷を分散し、高度なヘルスチェックによってサーバーの状態を監視し、キャッシング、圧縮、TCP最適化を通じてパフォーマンスを高速化します。また、アプリケーションアクセス管理（AAM）機能によって認証と許可を行い、DDoS防御機能によってアプリケーションへの帯域幅消費型の攻撃を阻止します。拡張によって単一デバイスで1秒当たり2億以上のSYNパケットのブロックが可能です。

包括的で拡張性の高い管理

管理の合理化と自動化のために、Thunder ADCは業界標準のCLI、Webベースユーザーインターフェイス、そしてサードパーティまたはカスタム管理コンソールと統合できるRESTful API（A10 Networks aXAPI® RESTベースのAPI）を備えています。大規模な導入では、A10 Networks® aGalaxy®一元管理システムによって、物理的な場所にかかわらず、複数のThunderアプライアンスでルーチンタスクを大規模に実行できます。

ロギングおよびレポーティング

Thunder ADCは、トラフィック分析のための高速syslogロギングに加え、電子メールアラートや、トラフィック分析のためのNetFlowとsFlowの統計情報をサポートしています。グラフィカルなレポートは、攻撃の分析とコンプライアンスのためにセキュリティトレンド情報を提供します。リアルタイムのダッシュボードには、システム情報、メモリーとCPUの使用率、ネットワークのステータスが表示されます。

ハードウェアと仮想アプライアンス

A10 ThunderシリーズのWAFは、幅広い導入ニーズに対応可能なハードウェア/ソフトウェアアプライアンスの製品ファミリーで提供されます。Thunderハードウェアアプライアンスは、最高レベルの信頼性とパフォーマンスを備えており、単一のアプライアンスで5～150Gbps以上のスループットまで拡張できます。仮想およびクラウドコンピューティング環境をサポートするために、A10は幅広いハイパーバイザー上で動作するvThunder® ADC仮想アプライアンス製品ラインを提供しています。一方A10 Networks Thunderハイブリッド仮想アプライアンス（HVA）は、仮想アプライアンスの柔軟性とパフォーマンスが最適化されたハードウェアアプライアンスの両方の利点を提供します。

Thunder ADCに搭載され、追加のライセンス料なしで使用できるA10のWebアプリケーションファイアウォールにより、迅速でコスト効率に優れたWebアプリケーション保護が可能になります。ACOSと高速共有メモリーアーキテクチャーによって強化されているThunder ADCは、独立したWebアプリケーションファイアウォールの購入や既存のロードバランサーのアップグレードを必要とせずに、大規模な負荷分散とアプリケーション保護を実現します。

Webアプリケーションファイアウォールの仕様

Webアプリケーション攻撃緩和

- SQLインジェクション攻撃からの保護
- クロスサイトスクリプティング攻撃からの保護
- クロスサイトリクエストフォージェリー（CSRF）攻撃からの保護
- オープンリダイレクト攻撃からの保護
- 既知のボットエージェントと要求頻度の検知によってボットから防御
- バッファオーバーフローの緩和
- トラフィックを正規化してプロトコル準拠を強制する攻撃回避技法

サポートするプロトコル

- HTML、DHTML、XML、SOAP、JSON、AJAX
- HTTP/1.0、HTTP/1.1

アプリケーション防御

- HTTPプロトコルへの準拠
- ホワイトリストによるセキュリティと自動学習
- ブラックリストによるセキュリティ
- 要求の正規化
- Cookieの暗号化、URIとフォームのリライトによるセッション保護
- クライアント側のキャッシングとSSLセキュリティの強化
- 地理情報によるブロック
- aFleXポリシーによるルールのカスタマイズとプログラムでの完全な制御

データ損失防止

- クレジットカード番号と社会保障番号のマスキング
- Perl互換正規表現（PCRE）のパターンマッチング
- 応答の隠匿

認証

- Basic
- Digest
- NTLM（NT LAN Manager）
- クライアントSSL証明書
- SAML（Security Assertion Markup Language）
- トークンベース認証

DDoSからの保護

- 帯域幅消費型DDoS攻撃 – SYNフラッド、ICMPフラッド、UDPフラッド、Ping of Death、Smurf攻撃、LAND攻撃、フラグメントパケット
- アプリケーションレイヤーDDoS攻撃 – HTTPフラッド、Slowloris、Slow POST、DNSフラッド、バックエンドデータベースリソースを枯渇させる標的型攻撃

Thunder ADCによるWebアプリケーションの保護

SQLインジェクション、XSS、アプリケーションレイヤーへのDDoS攻撃などの脅威への懸念が高まっている今、組織にはWebアプリケーションを保護できるソリューションが必要です。

組織は、Thunder ADCのICSA認定WAFを活用して、アプリケーションとデータを保護することができます。Thunder ADCは、Web攻撃に対する強力な防御を提供します。A10のACOS（Advanced Core Operating System）プラットフォームを基盤とするThunder ADCの卓越したパフォーマンスにより、お客様は将来も拡張性と機能の要件に対応することが可能になります。

統合されたWAF、高度なDDoSからの保護、DNSファイアウォール、SSL検査、認証機能を使用してアプリケーション保護という重要な役割を果たすThunder ADCは、データセンターのセキュリティプラットフォームの選択肢となっています。世界中の数千の組織に信頼されているA10 Thunder ADCは、アプリケーションの高可用性、高速化、保護を実現します。

A10 Networks / A10ネットワークス株式会社について

A10 Networks（NYSE: ATEN）はアプリケーションネットワーキング分野におけるリーダーとして、高性能なアプリケーションネットワーキングソリューション群を提供しています。世界中で数千社にのぼる大企業やサービスプロバイダー、大規模Webプロバイダーといったお客様のデータセンターに導入され、アプリケーションとネットワークを高速化し安全性を確保しています。A10 Networksは2004年に設立されました。米国カリフォルニア州サンノゼに本拠地を置き、世界各国の拠点からお客様をサポートしています。

A10ネットワークス株式会社はA10 Networksの日本子会社であり、お客様の意見や要望を積極的に取り入れ、革新的なアプリケーションネットワーキングソリューションをご提供することを使命としています。

詳しくはホームページをご覧ください。
www.a10networks.co.jp
Facebook：http://www.facebook.com/A10networksjapan

A10ネットワークス株式会社
〒105-0001
東京都港区虎ノ門4-3-20
神谷町MTビル16階
TEL：03-5777-1995
FAX: 03-5777-1997
jinfo@a10networks.com
www.a10networks.co.jp

海外拠点

北米（A10 Networks本社）
sales@a10networks.com
ヨーロッパ
emea_sales@a10networks.com
南米
latam_sales@a10networks.com
中国
china_sales@a10networks.com
香港
HongKong@a10networks.com
台湾
taiwan@a10networks.com
韓国
korea@a10networks.com
南アジア
SouthAsia@a10networks.com
オーストラリア/ニュージーランド
anz_sales@a10networks.com

お客様のビジネスを強化するA10のアプリケーションサービスゲートウェイ、Thunderの詳細は、A10ネットワークスのWebサイト**www.a10networks.co.jp**をご覧になるか、A10の営業担当者にご連絡ください。

Part Number: A10-SB-19128-JA-01
Mar 2015