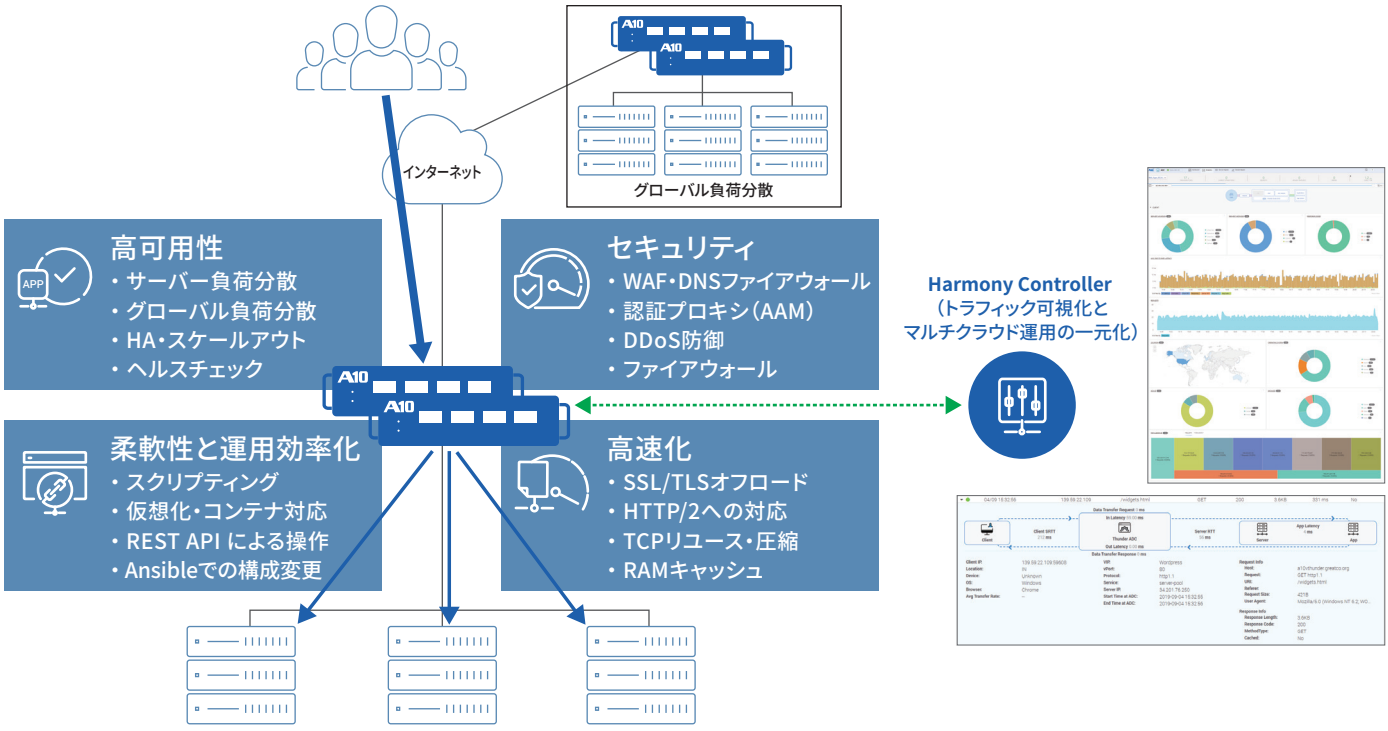
Always Secure. Always Available.

# Web 事業者様向けソリューション

## マルチクラウドでのアプリケーション配信の最適化とセキュリティ強化・運用の効率化

負荷分散と配信高速化、各種セキュリティ機能を集約。トラフィック可視化と運用自動化も実現

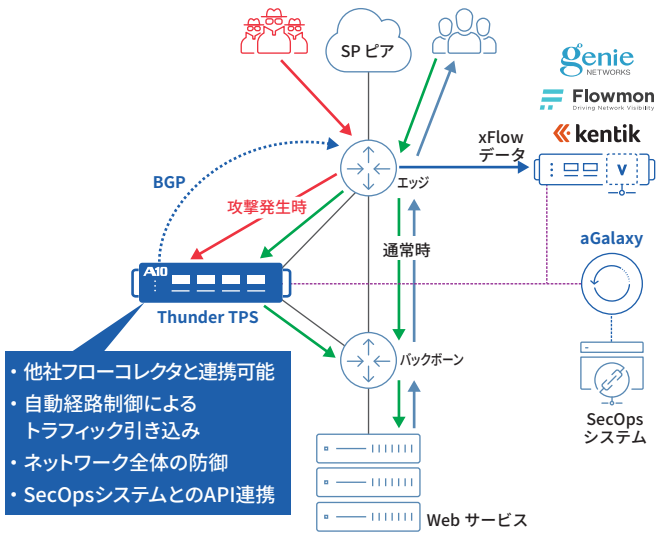



HTTP(S)/SMTP/IMAP/DNS/FTP/RADIUS/FIX/MQTT などあらゆるアプリケーション

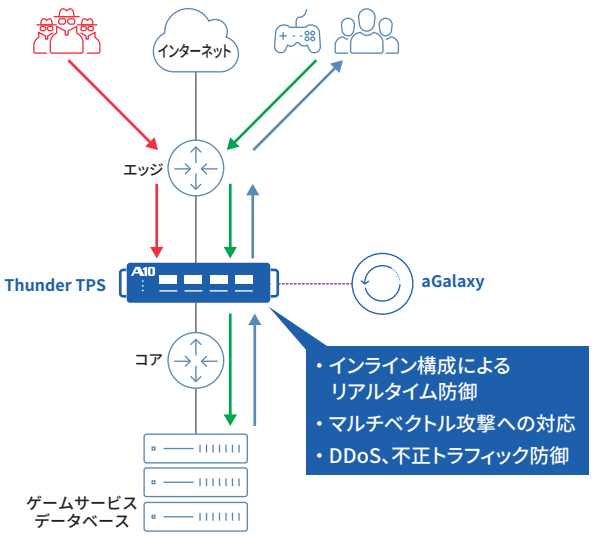
## DDoS 攻撃からの防御

多様なネットワークレイヤーでの攻撃から構成されるマルチベクトル DDoS 攻撃からネットワークを防御

### Web サービス：インフラの防御




### ゲーム：プレイヤー体験の向上



Always Secure. Always Available.

## アプリケーション配信の最適化とセキュリティ強化

Thunder ADC/CFW シリーズを利用することで、データセンター／プライベートクラウドやパブリッククラウド上の自社サービスのサーバー負荷分散や TLS オフロードなどのアプリケーション配信最適化を実現できます。1U の専用ハードウェアアプライアンス 1 台で最大 220Gbps のスループット、1,050 万秒間コネクション、2 億 5,600 万同時コネクションを処理できる高い性能を有します。Thunder そのものの冗長化やスケールアウトも可能です。

HTTP/2 のサーバー負荷分散や TLS1.3 のオフロードにも対応し、高速なアプリケーション配信を実現するとともに高いサービスの可用性を実現したり、Web アプリケーションファイアウォールや統合された L4 ファイアウォールによるセキュリティの強化を実現できます。

Thunder CFW シリーズではアプリケーション配信機能に L4 ファイアウォール機能が一元化されていることから、処理の高速化やラックスペースの効率的利用を実現します。

グローバル負荷分散の機能を標準で搭載しており、マルチクラウドに渡る災害対策やクライアントに最も近いサーバーからのコンテンツ配信なども可能です。サーバー負荷分散においてはスクリプティングにも対応し、トラフィックの中身に基づいたきめ細かなトラフィック制御を行えます。

DNS サーバーの前段に配置して DNS over HTTPS や DNS over TLS を容易に実現したり、DNS リクエストに対するアプリケーションファイアウォール機能によるセキュリティ強化も実現できます。

ユーザー認証プロキシとしては Active Directory や LDAP 等との連携による認証・認可だけでなく、SAML2.0 や OpenID Connect、OAuth2.0 に対応した認証・認可、CAPTCHA を利用した認証なども実現できます。アプリケーションレベルでの DDoS 攻撃に対する防御も実現できます。

## トラフィックの可視化と運用の効率化

管理ソリューションである Harmony Controller を用いることで、Thunder ADC/CFW を通過する Web サービスの利用状況やサーバー負荷分散を中心とした各トラフィックのレイテンシの詳細な内訳（クライアントと Thunder 間のレイテンシ、Thunder 内部の処理時間、Thunder とアプリケーションサーバー間のレイテンシ、アプリケーションサーバー内での処理時間など）を可視化でき、Web サービスの問題点に対する迅速で効率的な対処を可能にします。

Harmony Controller はマルチクラウドに対応しており、各種 IaaS や仮想化プラットフォーム、コンテナプラットフォームへの Thunder シリーズのデプロイやライセンスの割り当て、構成変更、トラフィック可視化とアラート設定を一元的に実施できます。アラートの設定は多様なメトリクスに基づき E メールや Web hook での通知が可能で、状況に応じて自動的に特定のスクリプトを実行する等、運用の自動化や効率化を行うことができます。

Thunder シリーズはフォームファクタに関わらず REST API によるほぼ全ての機能の設定が可能であり、各種の運用ツールに容易に組み込むことができます。Ansible のモジュールも多数提供しており、Ansible を利用した構成変更も行うことができます

## ネットワーク仮想化 / コンテナ化への対応

Thunder シリーズは専用ハードウェアアプライアンスだけでなく、サーバー仮想化プラットフォームでの利用やベアメタルでのインストール、コンテナプラットフォームでの利用、各種パブリッククラウドでの利用にも対応しています。仮想版でも 1 インスタンスあたり最大 100Gbps、コンテナ版では最大 180Gbps のスループットに対応します。また、必要な帯域をプールで購入し、通信トラフィックに応じて帯域を柔軟にインスタンスに割り当てることができるライセンス体系も提供しており、ネットワーク機能の配置を最適化できます。

また、アプリケーションを Kubernetes を利用したプラットフォームで提供する場合に、外部にある Thunder アプライアンスと連携するための A10 Kubernetes Connector のソリューションも提供しています。このソリューションを利用すると、A10 Kubernetes Connector が、Kubernetes Cluster 内のサービスを発見し、外部にある Thunder のサーバー負荷分散設定を自動的に更新することができます。

## DDoS 攻撃からの防御

Thunder TPS シリーズを利用することで、ネットワーク層からアプリケーション層までのマルチレイヤーに渡る DDoS 攻撃（マルチベクトル DDoS 攻撃）を検知・防御して正常通信のみを通すことができます。ネットワークの外部からの攻撃だけでなく、内部からの攻撃にも対応できます。管理ソリューションである aGalaxy と連携することで、フローデータから DDoS 攻撃を検知し、自動的に防御設定を変更できます。他社のフローコレクタとの連携も可能です。攻撃内容を分析するためのダッシュボードや高度なレポーティング機能も搭載されており、攻撃の状況を確認しながら対策を変更できます。

Thunder TPS は、機械学習を用いてボリューム型 DDoS 攻撃の内容を分析し、自動的に緩和フィルターを適用できる ZAP（Zero-day Automated Protection <ゼロデイ自動保護>）機能が搭載されており、手動での作業なく迅速な防御を実現できます。不正な IP アドレスからの攻撃を防ぐために、50 以上の提携セキュリティ機関から集めた 3,100 万以上の脅威 IP 情報を相関分析することにより、高い検知率でありながら誤検知が少なく、リアルタイムに更新される IP レピュテーション情報も利用できます。

## A10 Networks / A10 ネットワークス株式会社について

A10 Networks（NYSE: ATEN）は、サービス事業者やクラウド事業者および企業で利用される 5G ネットワークやマルチクラウドアプリケーションのセキュリティを確保します。高度な分析や機械学習、インテリジェントな自動化機能により、ミッションクリティカルなアプリケーションを保護し、信頼性と可用性を担保します。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 117 か国のお客様にサービスを提供しています。

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。
**www.a10networks.co.jp/**
**Facebook：http://www.facebook.com/A10networksjapan**

## Learn More

About A10 Networks

お問い合わせ
a10networks.co.jp/contact

**A10ネットワークス株式会社**
www.a10networks.co.jp
a10networks.co.jp/contact


Part Number: A10_SB_Solutions_for_WebServices APR 2021