データシート

A10 HARMONY CONTROLLER

マルチクラウド環境にアジャイルな管理、自動化、分析機能を提供

A10 Harmony™ Controllerは、データセンターやプライベートクラウド、パブリッククラウド、ハイブリッドクラウドなどのあらゆるインフラストラクチャに導入されたA10製品の一元管理、自動化、分析機能を提供します。

あらゆるアプリケーション環境にアジャイルな管理機能と分析機能を提供

A10 Harmony Controllerは、Thunder® ADC、SSLi、CFW、CGNなどのA10製品に対して、アプリケーションの設定やポリシー管理を実現する一元管理機能と分析機能を提供します。

アプリケーション配信とセキュリティソリューションが統合されたA10のThunderシリーズ及びLightningシリーズを利用することにより、これらを通過するトラフィックフローを収集、分析してレポートを生成することができます。A10のSSLi、CGN、CFW上のトラフィックを統合して一元的にダッシュボードで分析することにより、セキュリティの状態を視覚的に把握することが可能となり、運用の効率化に役立てることができます。

Harmony Controllerを利用することにより、アプリケーションサービスの導入と運用を効率的に自動化し、運用の効率とアジャイル性を高めるとともに、エンドユーザーのセキュリティエクスペリエンスを向上させ、TCOを削減することができます。さらに、分散しているアプリケーションサービス管理をシンプルにすることにより、トラブルシューティングにかかる時間を大幅に短縮、パフォーマンスやセキュリティの異常に関するアラートを受信できるようになるため、容量設計を改善し、ITインフラとクラウド環境の最適化も可能になります。

プラットフォーム

aws
vmware
NUTANIX
openstack.

お問い合わせ

WEB
a10networks.co.jp/controller

連絡先
a10networks.co.jp/contact

機能と特長

Harmony Controllerは、運用をシンプル化して、運用チームのアジリティを向上させます。インフラチームやアプリケーション運用チームは、インフラの設定と、A10のThunderシリーズやLightningシリーズで構成しているアプリケーションサービスのポリシー設定を一元管理することができます。このアプリケーションサービスには、ロードバランシングやアプリケーション配信、Webアプリケーションファイアウォールなどが含まれています。設定と制御は、APIを通じて自動化可能で、組織で使用しているオーケストレーションシステムとも連携できます。さらに、包括的なインフラや、アプリケーション単位でのメトリックと分析にも対応するため、パフォーマンスとセキュリティの監視、異常の検知、トラブルシューティングにかかる時間の短縮に役立ちます。

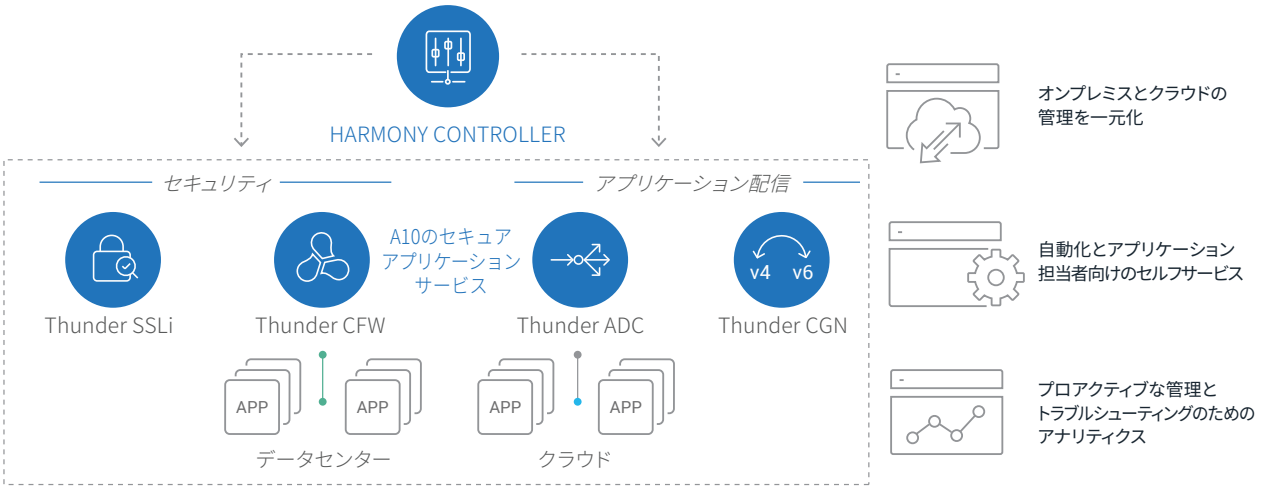


図1. Harmony Controllerを利用したマルチクラウド環境におけるA10製品の一元管理・自動化・可視化

一元管理

ADC、SSLi、CFW、CGNを含むA10の幅広い製品ポートフォリオのセキュアアプリケーションサービスを一元管理できます。データセンター、プライベートクラウド、パブリッククラウドにわたって導入されているアプリケーション全体に対して、容易にポリシーを設定して管理することができます。

トラフィックとセキュリティのアナリティクス

可視化を通じてアプリケーショントラフィックに関する実用的な情報を取得できます。さらにコンテキスト化されたデータとログを利用することで、トラブルシューティングが容易になります。また、収集したデータを分析して異常なトレンドを検知できます。アラートは、さまざまなメトリックとカスタマイズ可能なフィールドに基づいて取得可能です。アラートは電子メールまたはWebhook URLで配信され、自動化されたアクションを迅速に実行できます。

マルチテナント・セルフサービス

階層型のテナントモデルによって、インフラ全体のガバナンスに影響を与えずにアジリティが強化されます。アプリケーションチームとサービス担当者をテナントとして作成すると、各テナントが自身のインフラとアプリケーションポリシーを個別に管理することができます。

デバイスのライフサイクル管理

A10のハードウェアアプライアンスおよび仮想インスタンスのライフサイクルを一元的に管理できます。デバイスをグループ化して共通のテンプレートを適用することにより、多数のデバイスの管理も簡単に行えます。設定のバックアップとリストアや、定期的なソフトウェア更新も実行できます。

APIによる自動化

アプリケーション設定やデバイス操作、分析データの収集には、RESTベースのAPIが利用可能です。このAPIを利用することにより、Ansible、Chef、JenkinsなどのDevOpsツールや、VMware vRO/vRA、Cisco Cloud Center、Microsoft Azure、Google Cloud Platform、Amazon Web Servicesをはじめとする多くのオーケストレーションシステムと連携することができます。

プラットフォームに依存しない高い拡張性

Harmony Controllerはコンテナベースのマイクロサービスアーキテクチャを採用しているため、運用を中断せずにコントローラーの容量を拡張できます。ベアメタル、仮想サーバー、パブリッククラウド、またはプライベートクラウドへの導入が可能です。

Kubernetes向けIngressコントローラー

Kubernetesクラスター上で実行されているコンテナベースのアプリケーションに対してロードバランス機能やサービスディスカバリー機能、セキュリティ、アナリティクス機能を提供します。

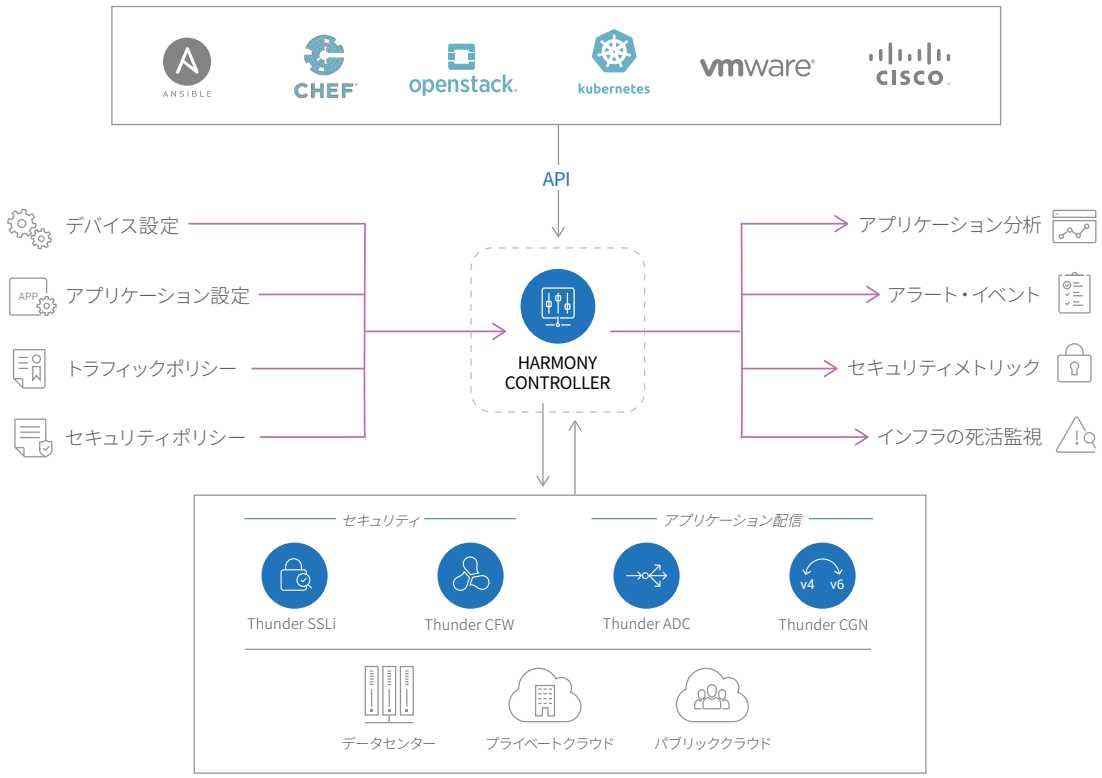


図2. Harmony Controllerの機能とAPIによる連携

HARMONY CONTROLLERのインターフェイス

Harmony Controllerを利用すると、A10のアプリケーションサービスやさまざまなポリシーの管理とコントロールを一元化し、分析機能とアラート機能によるリアルタイムな可視化を実現できます。管理者は、Harmony Portalを利用してコントローラーに接続して設定を行います。Harmony Portalは、さまざまなアプリケーションサービスを管理するためのHarmony APIを使用します。

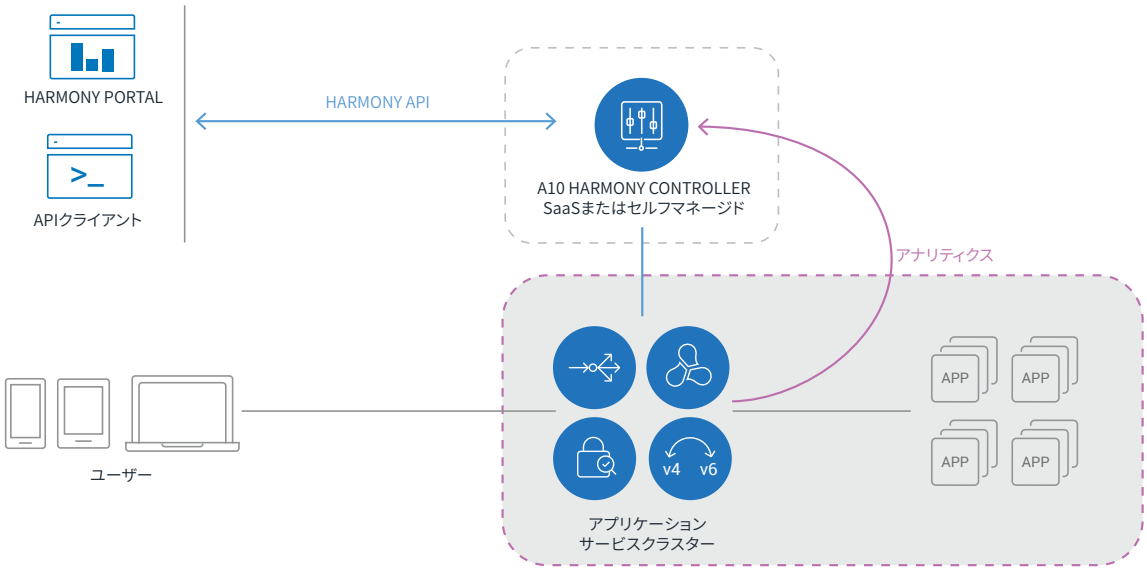


図3. Harmony Portalによる制御と分析の一元化

HARMONY PORTAL

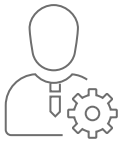
Harmony Portalは、アプリケーション配信と関連するポリシーをアプリケーション単位で管理できる、直感的に利用可能なグラフィカルユーザーインターフェイスです。セルフサービス機能により、IT管理者がアプリケーションごとにすべてのインフラを設定する必要がなくなるため、アジリティが向上し、運用コストを削減しながら複数のアプリケーションチームをサポートできるようになります。

HARMONY API

Harmony APIにより、すべてのアプリケーションサービス機能は、RESTベースのインターフェイスを介して利用することができます。APIは、Chef、Puppet、Ansibleなどの自動化ツール、およびJenkinsなどのCI/CDツールと連携して使用することができます。Analytics APIを利用することにより、各アプリケーションのメトリクスとログへのアクセスも可能です。これらのAPIは、サードパーティのツールと連携する場合や、カスタムダッシュボードを作成する場合に便利です。

導入モデル

A10 Harmony Controllerは、A10が提供するSaaS型と、オンプレミスに導入して使用できるセルフマネージド型の2つの導入モデルがあります。SaaS型は、サービスとして利用できるため、手軽に導入可能で、しかもコスト効率良く運用することができます。



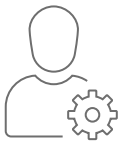
SaaS型モデル

サービスとして利用できるクラウドベースのHarmony Controllerは、A10によって完全に管理、監視されています。アプリケーションチームは、SaaS型のHarmony Controller上で「テナント」アカウントを直接取得できます。またITチームは、「プロバイダー」アカウントを取得することにより、内部や外部テナントを管理できます。

コントローラーとサービスインスタンス間では、制御に関するメッセージ、統計情報およびテレメトリデータのみがSSLで暗号化されて送信されます。アプリケーションデータは、クライアント側のネットワーク内のみで処理されるため、コントローラー側に送信されることはありません。

コントローラーは、パブリッククラウド上にホストされており、強化されたオペレーティングシステム上で構成することによって高い可用性を実現しています。複数レイヤで構成されたコントローラーのセキュリティは、定期的にスキャンと脆弱性の監査を実施することにより、コンプライアンスを確保しています。

SaaSコントローラーは、ネットワーク的に隔離された環境に配置されており、権限のある担当者にのみアクセスが許可されています。コントローラー内でのデータの交換には強力な暗号を使用しています。パスワードやSSL秘密鍵などの機密データに対しても強力な暗号方式を採用して、データベースに格納しています。外部からのアクセスは、SSL通信でデータが保護されます。Harmony Controllerは、AWS MarketplaceおよびAWS GovCloudで、Lightning ADCとともにSaaSとして入手できます。



セルフマネージド型

オンプレミスで利用できるセルフマネージド型のコントローラーは、ユーザー自身のクラウド環境内に設置し、ユーザーによる管理と拡張が可能なソフトウェアソリューションまたはハードウェアアプライアンスとして導入できます。これにより、データセンター内、もしくはベアメタルサーバー、VMwareベースのクラウド、Amazon Web Services、Google Cloud Platform、Microsoft Azureなどで利用可能です。

セルフマネージド型コントローラーは、CentOSまたはRHEL 7.4以上のオペレーティングシステムを実行しているあらゆるサーバーまたは仮想マシンインスタンスにインストールできます。コントローラー内部のマイクロサービスアーキテクチャにより、コントローラーの可用性が最大限に高められます。またこのアーキテクチャによって、コントローラーとアプリケーションサーバー間の接続がダウンした場合でもトラフィックの中断が発生しないことが保証されます。

システム要件

Harmony Controllerソフトウェアは、奇数台のマシンにインストールできます。本番環境では、クラスター内の3つのノードへのインストールが適しています。実際のリソースの要件は、管理対象デバイスの数と必要なアナリティクスに応じて異なります。コントローラーのマイクロサービスは、これらの3つのインスタンスに分散されます。データストレージもこれら3つのインスタンスに分散されます。

ノード構成	説明
1ノード構成	16 CPU、64 GB RAM、1.2 TBストレージ（SSD推奨）
3ノード構成	各ノード: 8 CPU、32 GB RAM、500 MBストレージ（SSD推奨）

ハードウェアアプライアンスモデル

Harmony Controllerは、専用のハードウェアアプライアンスとして利用可能です。
これらのアプライアンスは、セルフマネージド型コントローラーとして使用できます。

モデル	HC8000	HC2000
ラックサイズ	2U	1U
CPU	Intel Xeon	Intel Communication Processor SoC
	20コア（40 HT）	16コア（16 HT）
メモリー（RAM）	128 GB	64 GB
ストレージ：リムーバブルディスクドライブ	4 x 3.5”	1 x 3.5”
	4 x 6 TB HDD	6 TB HDD
	ブランクベイなし	ブランクベイなし
電源	デュアル500W RPS	デュアル750W RPS DCオプション
	80 PLUS「Silver」	80 PLUS「Platinum」

プライシングモデル

コントローラーソフトウェアサブスクリプションの価格は、管理対象デバイスで消費される帯域幅ユニット値に基づいています。帯域幅ユニット値のプールは、異なる帯域幅ユニット値をもつさまざまなデバイスで柔軟に利用できます。サブスクリプションは、1年または3年から選択できます。
すべてのソフトウェアサブスクリプションにGoldサポートが含まれていますが、デバイスのライセンスは、別途購入する必要があります。

管理対象製品

Harmony Controllerは、次のようなA10製品とサードパーティのソリューションに対応しています。

A10 THUNDER ADC
（アプライアンス、仮想ソフトウェア、ベアメタル）

A10のADC製品は、アプライアンス、仮想ソフトウェア、またはベアメタルサーバー用のマシンイメージとして提供されています。

A10 LIGHTNING ADC

A10 Lightning ADCは、ロードバランス機能とセキュリティ機能が統合されたライトウェイトなADC製品です。パブリッククラウド、プライベートクラウド、およびコンテナ環境向けに提供されています。

A10 THUNDER SSLi

A10 Thunder SSLiシリーズのSSL Insight®機能により、SSL暗号化によって生まれる盲点を排除できます。CPUリソースを集中的に消費するSSL復号処理がセキュリティ機器からオフロードされるため、セキュリティ機器は暗号化されたトラフィックをより効率的に検査できるようになります。

A10 THUNDER CFW

A10 Thunder CFWは、サービスプロバイダーや大企業向けに、データセンターファイアウォールやサイト間IPsec VPN、Gi/SGiファイアウォール、セキュアWebゲートウェイ（クラウドプロキシ）機能を提供します。

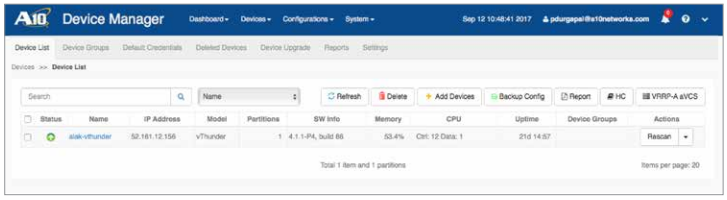
A10 THUNDER CGN

A10 Thunder® CGNは、パフォーマンスに優れた透過性の高いIPアドレス、プロトコル変換を可能にします。これにより、サービスプロバイダーや企業は、IPv4ネットワークの接続性を拡張しながらIPv6への移行を進めることができます。

機能一覧

デバイス管理の一元化

デバイスグループ	複数の Thunder ADC を論理グループにグループ化し、同じ操作を一度にすべてのグループメンバーに対して実行できます。
デバイスでのコマンド実行	1 つの CLI コマンドまたはそのバッチを個々のデバイスまたはグループにプッシュできます。
デバイスのアップグレード	Thunder ADC のアップグレードは、Harmony Portal を使用してリモートから実行できます。
デバイスの死活監視	Lightning ADC と Thunder ADC の両方を監視して適切なアクションを実行できます。
デバイス設定のバックアップ / リストア	デバイスの設定をバックアップして外部のデバイスにコピーを保存できます。
オーケストレーションと ADC のオートスケール	設定に従って Lightning ADC を起動し、トラフィックの要求に合わせてインスタンスのスケールアップ / ダウンを自動的に実行します。
マルチクラウド ADC 管理	マルチクラウド環境に導入されている Thunder ADC と Lightning ADC を一元的に管理することができます。
Kubernetes クラスターでの Lightning ADC の自動化	Ingress リソースと統合し、ルーティングの設定やオンデマンドでの Lightning ADC の動的な構成に対応します。



オペレーション

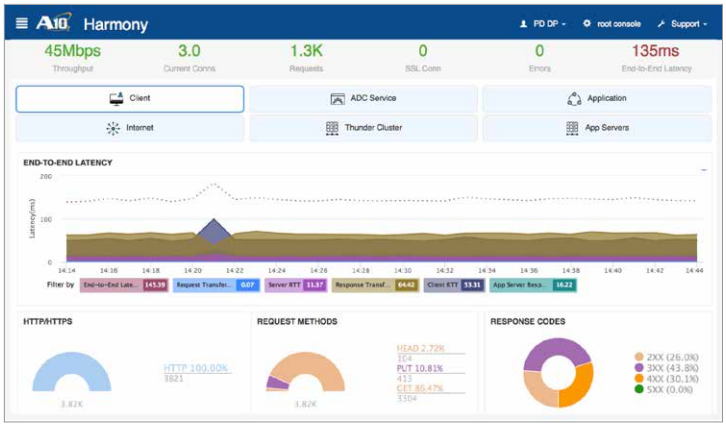
REST API	デバイス管理、アプリケーション設定、分析データの確認を含むすべての操作は、Harmony API を使用して実行できます。あらゆる連携や自動化も API を介して実行可能です。
プロバイダーテナントモデルによるマルチテナンシー	管理機能はプロバイダーとテナント間で分割されます。Harmony Controller は複数のプロバイダーをホストでき、各プロバイダーは複数のテナントと複数のユーザーを持つことができます。管理エンティティ（プロバイダー、テナント、ユーザー）の数に課させる制限やライセンスはありません。必要に応じて、500 以上の管理エンティティを作成できます。
ロールベースのアクセス制御	ユーザーは、プロバイダー、テナント、またはデバイスレベルで適切なパーミッションが付与されており、許可されている領域にのみアクセスできます。複数のユーザーが同時にログインし、各自の領域を管理できます。
アラート	ADC から収集されたメトリックは、ユーザー定義のルールに従って評価されアラートが発信されます。アラートは、手動による運用に適した電子メールによる送信やオートメーションに適した Webhook による送信が可能です。
セキュリティデータの定期更新	A10 は、リサーチャーによって定期的にリリースされるセキュリティ更新をサブスクライブしています。 A10 のセキュリティチームは、更新を監視し、重要な更新を定期的に発行しています。このコントローラーにより、中央のリポジトリから Lightning ADC への脅威インテリジェンスの更新を実行できます。
外部認証	プロバイダーは、ユーザーの認証プロバイダーを選択できます。ローカルでのユーザー認証以外に、Google OAuth または任意の LDAP ベースサーバーも選択可能です。
設定バックアップ	Harmony Controller の設定は、コピーして外部に保存することによってバックアップできます。

インストールとメンテナンス

あらゆるプラットフォームに対応	Harmony Controllerソフトウェアは、あらゆる環境の物理または仮想Linuxマシンにインストールできます。
高い拡張性とセルフヒーリング	コントローラーは、複数のマイクロサービスで構成されており、マイクロサービスが停止しても自動的に回復させます。コントローラーの容量は、トラフィックに影響を与えずに稼働中に追加できます。
API経由の設定	コントローラー自体の設定はAPIを介して監視・変更できます。

アナリティクス

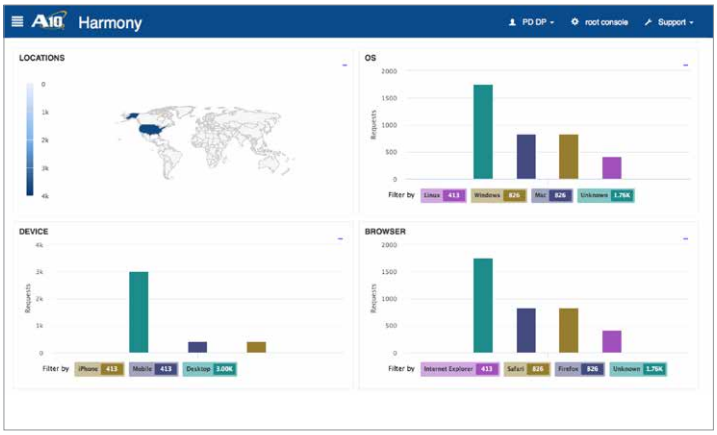
レスポンスタイム監視	クライアントとサーバー間のエンドツーエンドのレスポンスタイムはレポートされ、ドリルダウンして特定の領域を確認することができます。
トラフィックインサイトと分析機能	トラフィック情報はアカウントレベルで集約され、アプリケーション毎、またはリクエストレベル毎でドリルダウンできます。
セキュリティインサイト	ADCを通過するトラフィックは、セキュリティ脅威が含まれているかどうかの検査が行われ、保護の強化に役立つレポートが作成されます。
サーバーの死活管理	ADCから収集されるサーバーの監視情報とトラフィック情報によりサーバーの状態に関する予測が可能です。
リクエストごとの分析/アプリケーションアクセスログ	リクエストごとのアプリケーションアクセスログを基に分析可能となっており、トラブルシューティングの効率化に活用できます。



チャート

クライアントチャート

エンドツーエンドの遅延	クライアントが体験しているアプリケーショントラフィックのレスポンス時間と遅延の要素を示します。
リクエストレート HTTP / HTTPS リクエストメソッド	リクエスト送信レート、SSL を使用しているリクエストの数、使用されている HTTP メソッドを示します。
レスポンスコード	クライアントが正常なレスポンスを取得しているか、エラーを取得しているかを示します。
ロケーション	世界地図上でのクライアントのリクエスト、帯域幅、遅延状況の地理的な分布
OS デバイス ブラウザー	クライアントの情報（クライアントのオペレーティングシステム、デバイスタイプ（電話、タブレットまたはデスクトップ）、使用されている Web ブラウザー）の分布
トップクライアント	最も多くのリクエストを送信しているクライアントの IP アドレス



ADC サービス

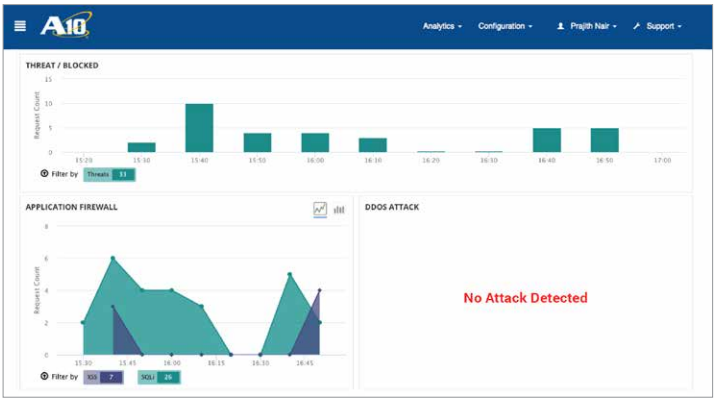
キャッシュヒット数 キャッシュ使用率 キャッシュされているエントリ	キャッシュで処理されているリクエスト数と帯域幅
スループット	スループットの合計と時系列分布
クライアント SSL コネクション	クライアントによる SSL 接続の合計と時系列分布
負荷分散	異なるアプリケーションサーバーへのリクエスト分散
CPU 使用率 メモリー使用率 帯域幅	ADC クラスターのヘルスパラメーター

アプリケーション

レスポンスタイム	サーバーレスポンスタイムの時系列情報
トップ URL トップドメイン トップサービス トップポート	トラフィックが最も多い URL、ドメイン、サービス、ポートを示すグラフ
サーバーヘルス	さまざまなヘルスパラメーターから算出されたサーバーヘルス指標
コネクション数	ADC からサーバーへのコネクション数の時系列グラフ

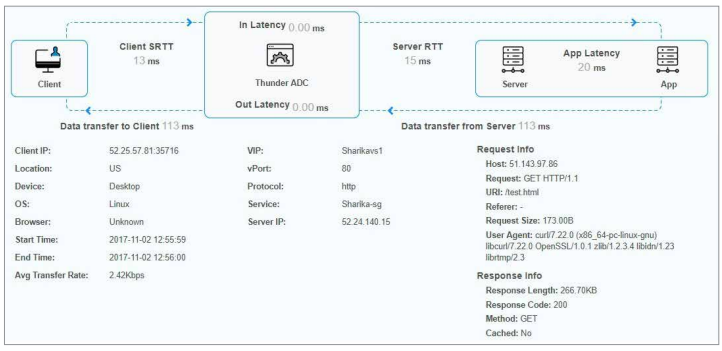
セキュリティ（Lightning ADC）

脅威の検出 / ブロック	さまざまな時間帯に検出 / ブロックされた脅威のサマリー
アプリケーションファイアウォール	タイプごとの攻撃の時系列分布
ブラックリスト / 低いレピュテーション	クライアントがブラックリストに含まれているか、レピュテーションが悪いためにブロックされたリクエストの情報
DDoS 攻撃の緩和	大量のアプリケーションレイヤー DDoS 攻撃を緩和するためにブロックされたリクエスト / セッション



トランザクションごとのログ

レスポンス時間の分布	リクエストとレスポンスのさまざまなフェーズで消費された時間のグラフ
クライアント情報	クライアント IP アドレス、デバイスタイプ、オペレーティングシステム、ブラウザー
サーバー情報	サーバー IP アドレス、ポート、リクエストに対応したマイクロサービス
リクエスト / レスポンス情報	リクエストのメソッド、プロトコル、URL、レスポンスデータサイズ
セキュリティ情報	リクエストまたはレスポンスで検出された脅威の詳細とその OWASP 分類



SSLiアナリティクス*

SSLステータス&レポート	• 検査の詳細 • バイパスされたカテゴリー • 鍵交換の詳細 • アクセスの詳細
システムヘルスのステータス&レポート	• システムステータス • キャッシュされた証明書 • CPS、セッション、トラフィック

*GI-FW アナリティクス **

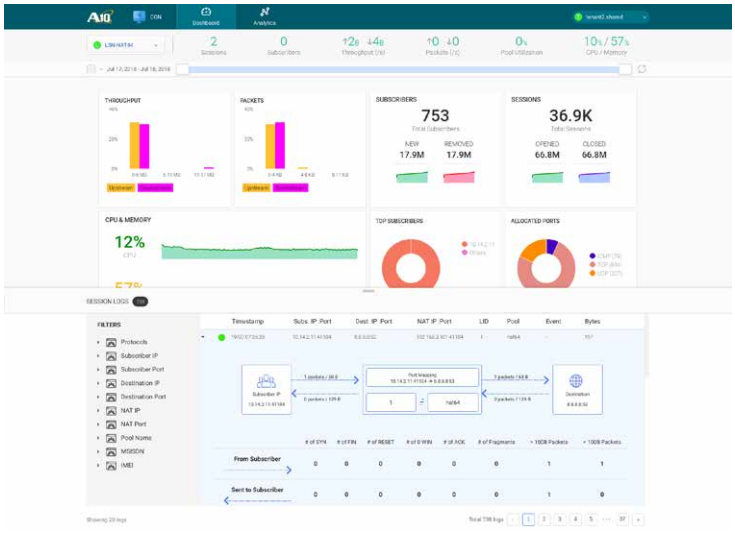
加入者セッションインサイト	• セッションオープン / クローズレート （潜在する DDoS 攻撃の指標） • 帯域幅 / フローを最も消費している加入者 （潜在するネットワーク悪用の指標）
CGN リソーストラッキング	• プロトコル & テクノロジーごとのマッピング （潜在するボットネット DDoS 攻撃の指標） • NAT IP プール使用率 （NAT IP プールへの攻撃指標）
トラフィック分布アラート	• 加入者割り当て帯域利用状況のアラート
ファイアウォール分析	• ファイアウォールルールのパフォーマンスとプロトコル毎のルール分布 • 状態ごとのトップファイアウォールルール – 許可、拒否 • 可視性の向上とトラブルシューティングの高速化に利用できる、送信元 / 宛先 IP、ポート、ファイアウォールアクションを含む完全なログ
アプリケーションの可視性	• カテゴリー毎のアプリケーション分布 • アプリケーション分布毎のトップ宛先 IP • アプリケーションカテゴリー別の消費バイト数

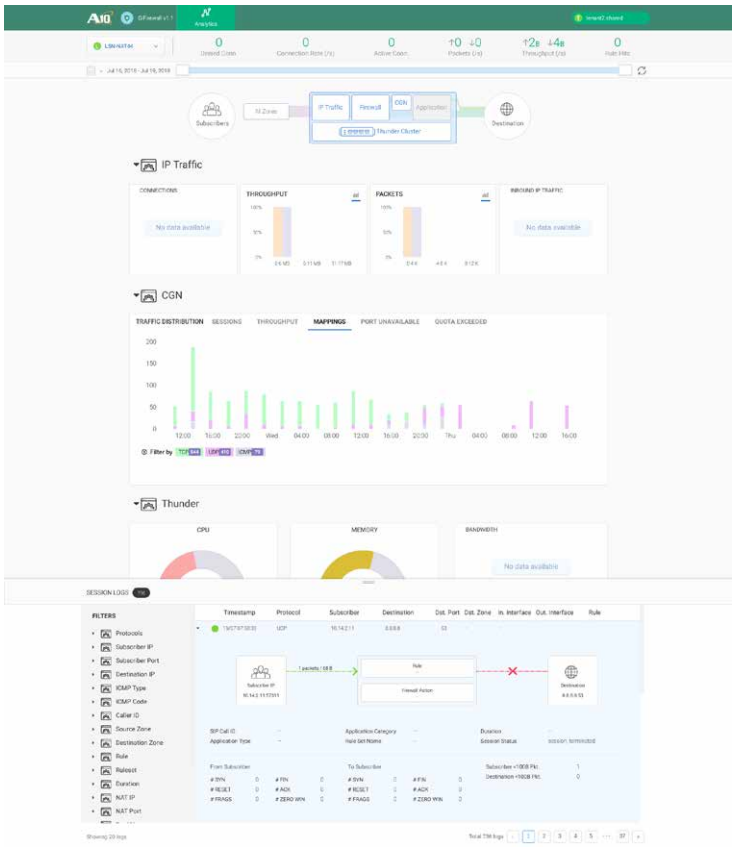
*CGN アナリティクス **

加入者情報	• 使用された合計スループットと加入者割当帯域アラート • 加入者別のオープン / クローズセッション • 消費スループット別のトップ加入者
CGN サービス	• プロトコル別のポート割当 • マッピングエラー • トップポート消費統計情報 • Full Cone セッション分布
宛先	• 全体のパケットレート • フラグメントされた / 不正なトラフィックの分析 • インターネットからのフローオープンの試行
加入者セッションインサイト	• セッションオープン / クローズレート （潜在する DDoS 攻撃の指標） • 帯域幅 / フローを最も消費している加入者 （潜在するネットワーク悪用の指標）
CGN リソーストラッキング	• プロトコル & テクノロジーごとのマッピング （潜在するボットネット DDoS 攻撃の指標） • NAT IP プール使用率 （NAT IP プールへの攻撃指標）
トラフィック分布アラート	• 加入者割り当て帯域利用状況のアラート
不正な行動	• ユーザー割当アラート – 超過セッション、超過接続レートなど • セッション作成失敗 • ヘアピニング、EIM/EIF 失敗
統合ログ	• トラブルシューティングの高速化に役立つきめ細かいログメッセージ • 加入者情報 • プロトコル • MSISDN • IMEI/IMSI • 無線アクセスタイプなど

*2018 年第 4 四半期に提供予定

CGN 分析





*2018 年第 4 四半期に提供予定

A10 Networks / A10 ネットワークス株式会社について

A10 Networks（NYSE: ATEN）はセキュアアプリケーションサービスにおけるリーディングカンパニーとして、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。お客様のデータセンターにおいて、アプリケーションとネットワークを高速化し可用性と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。

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

LEARN MORE
ABOUT THE 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

Part Number: A10-DS-15122-JA-09　Oct 2018