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。

A10 Harmony Controllerにより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ます。A10 Thunder ADCを通過するアプリケーショントラフィックを収集、分析してレポートを生成することができます。A10のSSLインサイト、CGNAT、Gi/SGiファイアウォール、そしてGTPファイアウォール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
ORACLE Cloud
vmware
NUTANIX
openstack.

お問い合わせ

Web
https://www.a10networks.co.jp/contact

機能と特長

Harmony Controllerはアプリケーションサービスの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、A10のセキュアアプリケーションサービスを集中管理するソリューションとしてDevOps/SecOpsのワークフローをサポートします。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統合のシングルポイントとして連携できます。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。

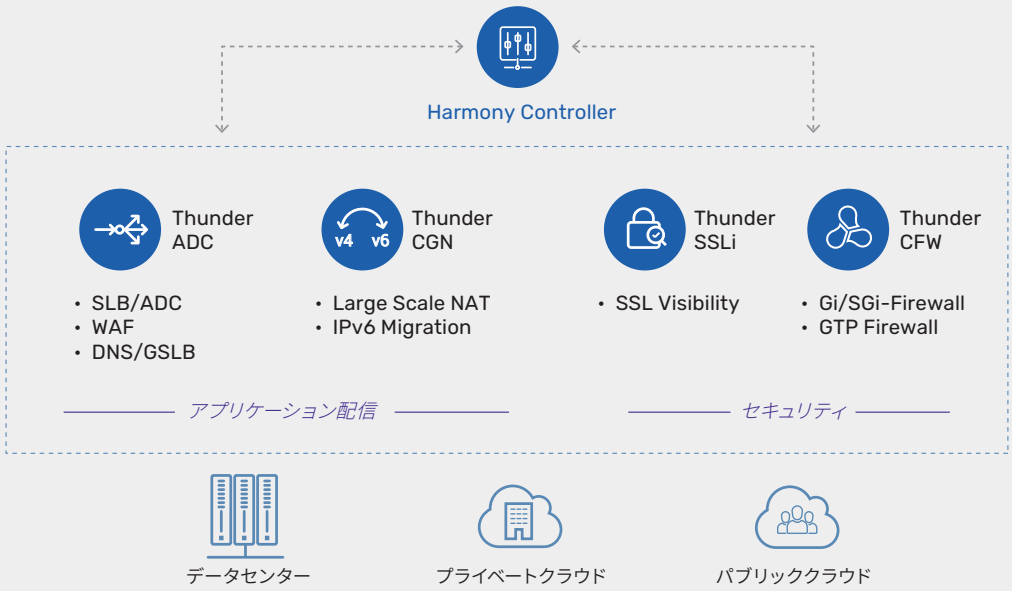

図1. Harmony Controllerを利用したマルチクラウド環境におけるA10製品の一元管理・自動化・可視化

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。

機能と特長

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。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 v RO/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、Linux ベースのベアメタル、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。

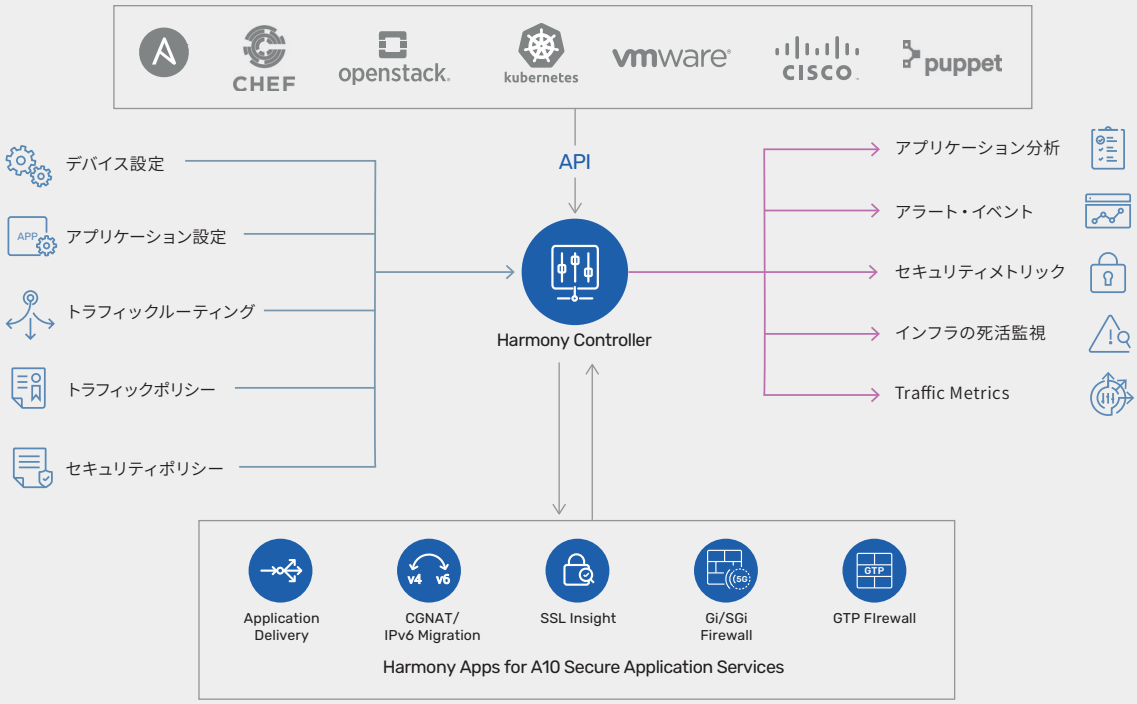

図 2. Harmony Controller は、あらゆるクラウド環境において、アプリケーションの管理と運用を簡素化・自動化します。

Harmony Controllerのインターフェイス

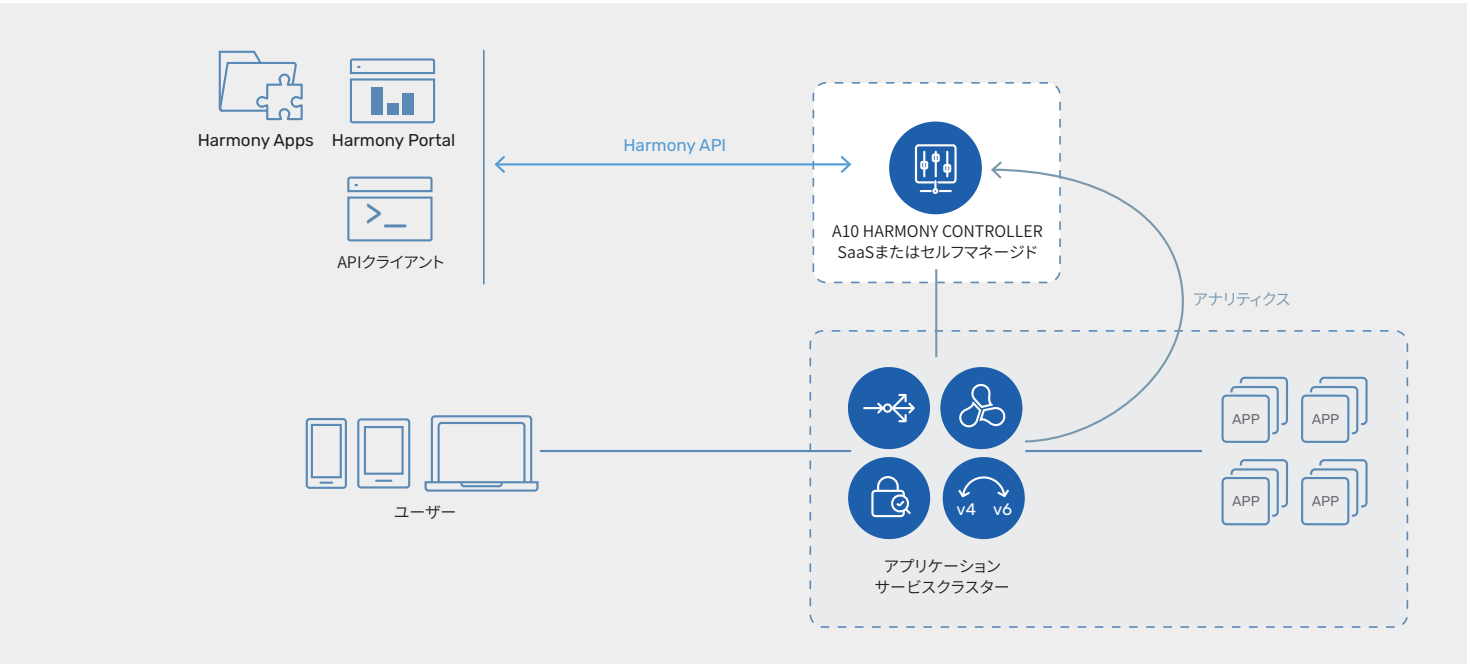

図3. Harmony Controller Harmony Controllerは、様々なアプリケーションサービス、クライアントAPI、管理機能を管理します。
この展開モデルでは、アプリケーションサービスがどこに展開されているかに関わらず、すべてのポリシーを一元的に設定することができます。

Harmony Portal

Harmony Portalは、セキュア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、ロールベースのアクセスコントロール(RBAC)を備えています。アプリケーションごとの可視性と洞察は、IT管理者がポータル上で有効化できるHarmony Appsを介して利用できます。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 APIs

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

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 TLS 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、TLS 通信でデータが保護されます。

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 ベースのハイパーバイザー、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 は、ベアメタル、ハイパーバイザー、クラウドなどの Linux マシン（CentOS または RHEL）に、スタンドアロンまたはハイアベイラビリティ（HA）でインストールすることができます。HA は、3 つのノード（仮想マシンまたはデバイス）の展開に対応しており、ノード障害時の回復力を提供します。マイクロサービスとコントローラーのデータストアは、この 3 つのノードに分散されます。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。Harmony Controller のインストールには、特別性能が高いハードウェアを用意する必要はなく、あらゆるスペックのサーバーを使用することができます。ストレージには、IOPS が高い SSD（ソリッドステートドライブ）が推奨されます。

Harmony Cotroller の導入に必要なシステム要件や前提条件の詳細については、最新の製品マニュアルを参照するか、A10 の営業担当者にお問い合わせください。

導入モデル

ライセンス

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。これらの帯域幅ユニットは、MBU（Managed Bandwidth Units）と呼ばれます。各 Thunder デバイスには、固定の MBU 値が設定されています。
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

A10 Thunder ADC

A10 Thunder® ADC は、アプリケーションの高可用性、高速性、安全性を実現する高性能な先進のロードバランシングソリューションです。

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）機能を提供しながら、ADC や CGN 機能を提供します。

A10 Thunder SSLi

A10 Thunder SSLi シリーズの SSL Insight® 機能により SSL/TLS 暗号化によって生まれる盲点を排除できます。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るため、コンプライアンスやプライバシーを確保し、ROI を向上させることができます。

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

Harmony Portal

デバイスインベントリー	デバイス毎、物理クラスタ毎、論理クラスタ毎などの様々なかたちでインベントリーを管理可能。
CLI コマンドユーティリティ	1 つの CLI コマンドまたはそのバッチを複数のデバイスパーティーションに同時にプッシュ可能。
デバイスのアップグレード	リモートから Thunder デバイスをアップグレード可能。
デバイスの死活監視	ダッシュボードでシステムの使用状況、デバイスの場所、イベント、アラートなどの情報をテナントサービス毎に提供。
デバイス設定のバックアップ / リストア	Thunder デバイスの設定バックアップ・リストアが可能。
マルチクラウドでのデバイス管理	あらゆるクラウド環境上にデプロイされた Thunder を一元管理。
一元化された設定ツール（Object Explorer）	Object Explorer により、接続されたデバイスの設定を読み込み、ADC、GSLB、CGNAT、Gi/SGi FW、WAF などのアプリケーションサービスレベルで設定可能。
クラウド上の A10 Thunder の自動プロビジョニング	AWS, Microsoft Azure, VMware ESXi, Kubernetes などのパブリック / プライベートクラウド上の仮想版 A10 Thunder を自動起動して管理可能。

オペレーション

RESTful API	外部連携や自動化、デバイス管理、アプリケーション設定、アナリティクスの取得などすべての操作は API 経由で可能。
マルチテナント対応	プロバイダ / テナントモデルの管理機能を採用。複数のプロバイダーをホスト可能で、各プロバイダーは複数のテナントと複数のユーザーをサポート。管理エンティティ（プロバイダー、テナント、ユーザー）の数による制限やライセンスは不要。500 以上の管理エンティティを作成可能。
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可能。複数のユーザーが同時にログインし、各自の領域を管理可能。
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を発信。 アラートは Slack や Microsoft Teams などのコラボレーションツールを使用して、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。
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可能。ローカルでのユーザー認証以外に、Google OAuth または任意の LDAP、Radius、TACACS ベースのサーバーも選択可能。
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可能。
レポートのスケジューリング	様々なレポート（PDF 形式）を定期的に IT 管理者に提供。任意の分析ページを PDF で印刷可能。

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	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可能。
セルフ・ヒーリング / マイクロサービスベースアーキテクチャ	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復旧可能。
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・変更可能。
災害対策	アクティブコントローラとパッシブコントローラを異なる地域に配置することで、災害などでプライマリロケーションが利用できなくなった場合でも、迅速に復旧可能。

機能一覧

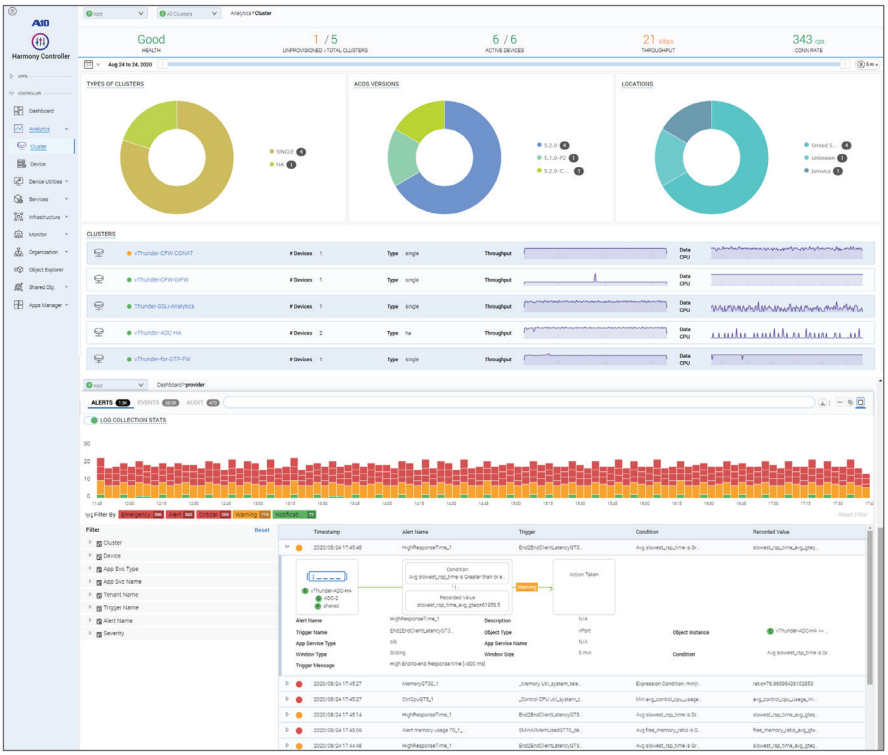

図4. Harmony Portalは、セキュアなアプリケーション・サービス・インフラストラクチャの健全性とイベントを示す包括的なダッシュボードと分析機能を提供します。サンプルでは、デバイスのステータスと詳細なアラートインサイトが表示されています。

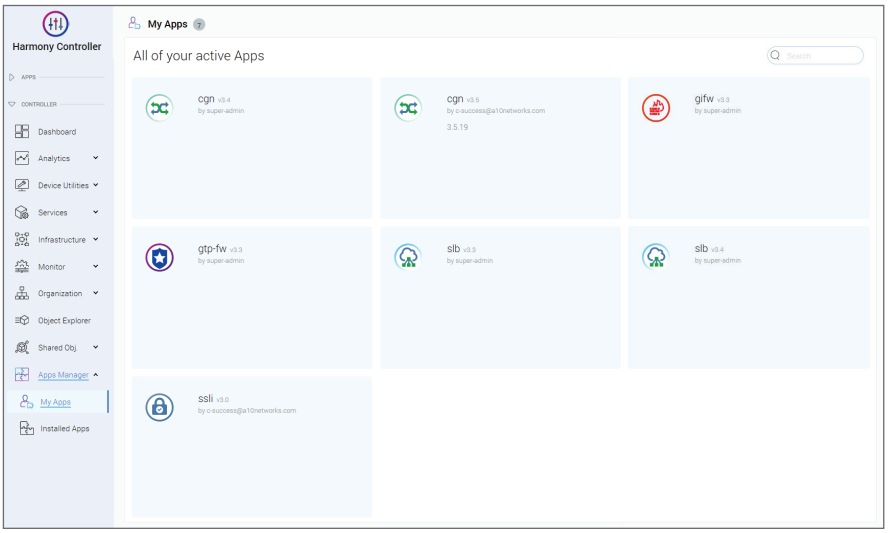

図5. Harmony Appsの一覧を表示しています。Harmony Appsは、アプリケーションごとに完全な可視性と分析を提供するもので、SLB/ADC、CGNAT、SSL Insight、Gi/SGi Firewall、GTP Firewallなどで利用可能です。

Harmony Appsの機能一覧

ADC/SLB App

アナリティクス&インサイト（サービスポートレベル）	クライアント	• ユーザーリクエストインサイト - リクエストメソッド、レスポンスコード、時系列のリクエスト統計情報 • 各セグメント（クライアント - ADC - アプリサーバー）でクライアントが体験している応答時間を示す平均エンドツーエンドレイテンシー • クライアントインサイト - 地理的分布、オペレーティングシステム、デバイス、ブラウザタイプなどのクライアントのプロパティ • リクエスト数とスループットの上位クライアント
	インターネット	• レイテンシー、リクエスト数（HTTP/HTTPS）、スループットなど、地理的な位置によるアプリケーション・トラフィックの分析
	WAF	• 違反タイプの分布、HTTP 閾値違反、プロトコル違反を含むWAFポリシー違反のインサイト • タイプ別の時系列のWAF違反統計 • 時系列のWAFリクエスト処理とイベント統計 • クッキーのセキュリティに関するインサイト • WAFポリシー違反のきっかけとなった受信リクエストの上位ソース
	ADC サービス	• アプリケーションサーバ間の接続数と応答数の時系列分布図 • アプリケーション・トラフィックのスループット（アップリンク／ダウンリンク）の時系列グラフ • リバースおよびフォワードの平均レイテンシーの時系列チャート • 応答コード3xx、4xx、5xxのエラートラフィック数の時系列チャート • HTTP2インサイト - プロキシ接続の統計、ボリューム、閉じたストリーム、クライアントに送信されたフレームタイプなどを含むHTTPSトラフィックの時系列グラフ • TLS/SSLインサイト - クライアント側とサーバー側の両方におけるTLS接続の時系列データ • RAMキャッシングの使用率や圧縮の使用率など、HTTPアクセラレーションに関するインサイト
	アプリケーションとサーバー	• 応答時間やエンドツーエンドのレイテンシーなど、時系列のアプリケーションパフォーマンス • アプリケーションサービスインサイト - アクセス数の多いURL/ドメイン、応答時間の長いURLなど • 時系列のバックエンドサーバーインサイト - サーバーの健全性、応答時間、新規接続、現在のコネクション数
	ADC クラスター	• ADCデバイス／クラスターのシステム使用率（CPU、メモリ）および帯域幅（ピーク時および平均時） • 世界地図上での導入位置 • スループットと両方向（入口と出口）のアクティブ・セッションに基づく時系列のクラスタ・トラフィック・チャート • 時系列のサービス・パーティション・レベルのレイテンシー・インサイト（フォワード、リバース、TTFB（time to first byte）、TTLB（time to last byte））
	レイテンシードリルダウン	• レイテンシー分析の概要 • 完全なリクエスト/レスポンス・サイクルの時系列平均エンド・ツー・エンド・レイテンシー
ADC サービスダッシュボード（グローバル）		• スループット、現在の接続数、接続率、エラートラフィック率を含むグローバルなリアルタイムADCトラフィック統計を含むADCサービスレベルKPI（重要業績評価指標）バー • サービスポートの統計とステータス、グローバルなデプロイメントロケーション、イベントログ、アラートを含むサービスインベントリ情報 • トラフィック・パターン、特性、平均エンド・ツー・エンド・レイテンシー、トップ10のアプリケーション・サービスを示すグローバル（テナント・レベル）ADCトラフィック・インサイト・ダッシュボード
一元化されたADC設定ツール		• ADCサービステンプレート、WAFルール、セキュリティポリシー、aFleXスクリプト、ヘルスモニターテンプレートなどのポリシーやテンプレートを一元管理し、複数のデバイスで共有・利用できるShared Objectの提供 • サービスオブジェクトは、共有オブジェクトで作成されたサービステンプレート、セキュリティポリシー、その他のオブジェクトを関連付けることで、直感的なADC仮想サーバー（VIP）設定ツールを提供 • 以前の設定バージョンと比較するための差分分析を備えたADCの設定リビジョン管理
セッションログ・ドリルダウン		• クライアント情報（IP、ロケーション、デバイスなど）、ADCサービス情報（VIP、サービスポート、プロトコルなど）、リクエストとレスポンスの詳細を含むトランザクション詳細を提供するADCトランザクションログ • リクエストおよびレスポンス・トランザクションの様々なフェーズにおけるセッション・レイテンシー（RTT）を表すレスポンス・タイム・ディストリビューション • 違反の詳細（タイプ、カテゴリー、WAFポリシー、アクション）を提供するWAFイベントの詳細なトランザクションログ • 使いやすい検索とフィルタリング機能により、ADCサービスの迅速なトラブルシューティングをサポート • ネットワーク層とアプリケーション層の両方で起こりうる問題やボトルネックをピンポイントで特定

Harmony Appsの機能一覧

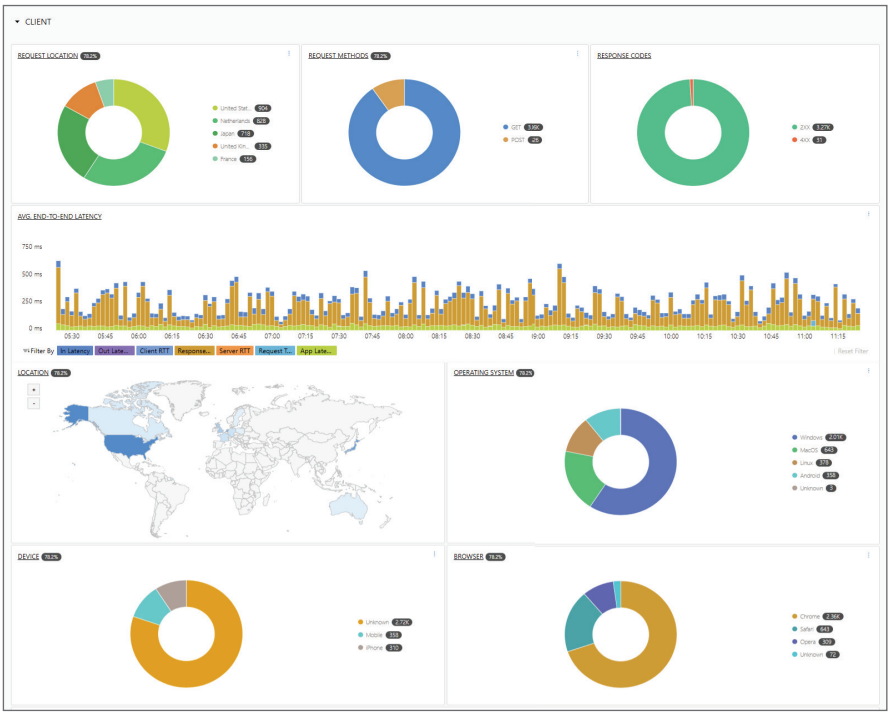

図6. ADC Harmony Appは、クライアント（サンプル）、インターネット、ADCサービス、アプリケーション、アプリサーバーなど、多方面からのアプリケーション分析とインサイトを提供します。

図7. レイテンシードリルダウンアナリティクスは、リクエスト - レスポンスの全サイクルにおける時系列の平均エンドツーエンドレイテンシーを提供します。
これは、応答時間の遅延に関連するアプリケーション・パフォーマンス問題のトラブルシューティングに大いに役立ちます。

Harmony Appsの機能一覧

SSL Insight App

アナリティクス&インサイト	トラフィックインサイト	• TLS検査の状況を、接続数やボリュームごとの総カウント数と時系列チャートで表示 • クライアントとサーバの接続に基づく、鍵交換方法、TLSバージョンに関するTLS暗号分析 • 接続数とボリュームに基づくプロトコルとセグメント別の時系列トラフィック分布 • 1秒あたりのTLS接続数とボリュームの時系列推移 • 接続数およびボリュームに基づく、TLS復号の上位ソースIP
	アプリケーション・インサイト	• 接続数およびボリュームに基づく上位アプリケーション • 接続数およびボリュームに基づく、上位のSaaSアプリケーション • 接続数およびボリュームに基づく、リスクの高いアプリケーションの上位 • アプリケーションのトラフィック分布 • アプリケーションとカテゴリの上位 • 観測されたすべてのアプリケーションプロトコルのリスト
	URLインサイト	• 接続数とボリュームに基づくURLカテゴリーの上位 • 生産性、機密性、ITリソース、プライバシーの各グループによるURLカテゴリーのインサイト • 接続数別の疑わしいURLカテゴリー - 疑わしいカテゴリーグループの時系列接続チャート • 上位5つのURLカテゴリーの時系列接続チャート
	ソース&デスティネーション	• 接続数とボリュームに基づいたSankeyダイアグラムによる送信元と送信先のIP分析 • 接続数とボリュームに基づいた送信元および送信先IPのパレート分析 • 接続数とボリュームに基づく送信先上位国
	スレット・インベスティゲーター	• IP、URL、ファイル、アプリケーションなど、インターネット上の個々のオブジェクトの潜在的なリスクを迅速に調べ、調査することができるスレットインテリジェンス調査・研究ツール
	ウォッチリスト	• URLとアプリケーションのカテゴリーに基づいてTLSトラフィックを監視 • アプリケーションのカスタムリストを作成し、ユーザーのトラフィックを時系列チャートで監視 • 時系列チャートでユーザートラフィックを監視するためのURLカテゴリのカスタムリストを作成
デバイス管理・設定ツール		• デバイスグループの健全性、リアルタイムのSSLiトラフィック統計、サービスの可用性、エラーレートなどを含む、SSL Insightのサービスレベルの KPI（主要業績評価指標）バー • 様々な導入オプション（シングルまたはデュアルアプライアンス、ハイアベイラビリティの有無、L2またはL3）と推奨されるセキュリティポリシーを直感的に設定可能な導入ウィザード • 多くの一般的な導入トポロジーをサポートするサイトグループとサイトトポロジー。同じサイトグループに新しいデバイスやサイトを追加することは、既存のサイトを複製するのと同じくらい容易に実現可能 • 一般的なシステム設定、インターフェースやネットワーク、アドオンのセキュリティライセンスなど、単一のデバイスレベルでの設定と管理をサポート • ポリシーマネージャーにより、デバイスグループ内のすべてのデバイスに対して、SSLインサイトサービスとポリシーの一元的な設定が可能 • 共有オブジェクトは、ACL、ポリシーテンプレート、SSLプロファイル、URLフィルタリング、ICAP、AAM、G-suites、Office 365など、様々なSSLiの設定を抽象化
セッションログ・ドリルダウン		• トラブルシューティングのために、アクセスログ、SSLi接続ログ、エラーログ、システムログの拡張表示と検索機能を提供するログビュー • 未分類のURLを含むセッションログの検索

Harmony Appsの機能一覧

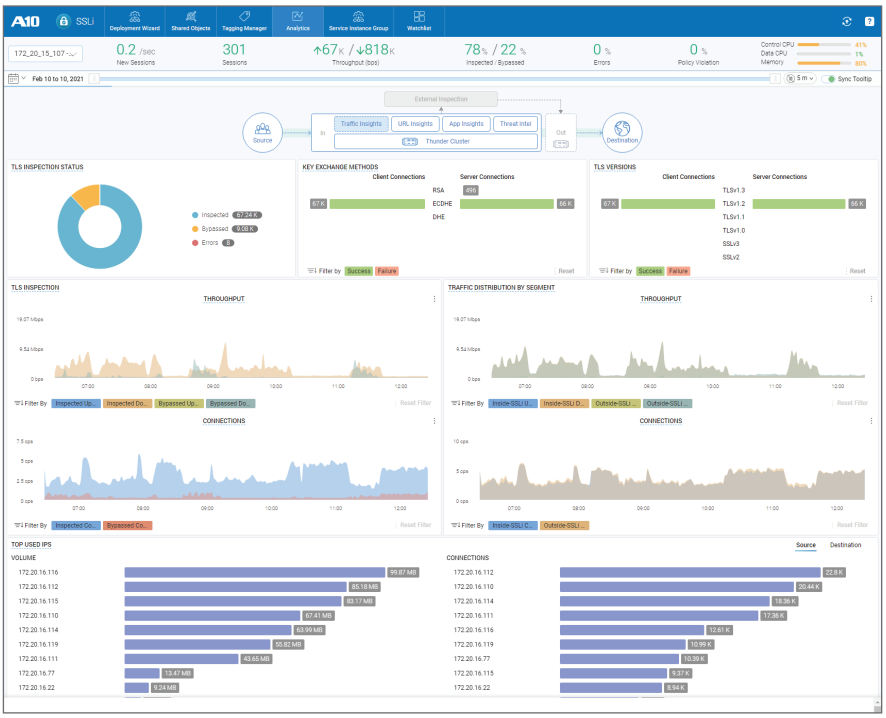

図8. SSL Insight Appは、TLS上のアプリケーション・トラフィックの包括的な分析、集中的なポリシー・コントロール、直感的なウィザードベースの設定ツールを提供します。

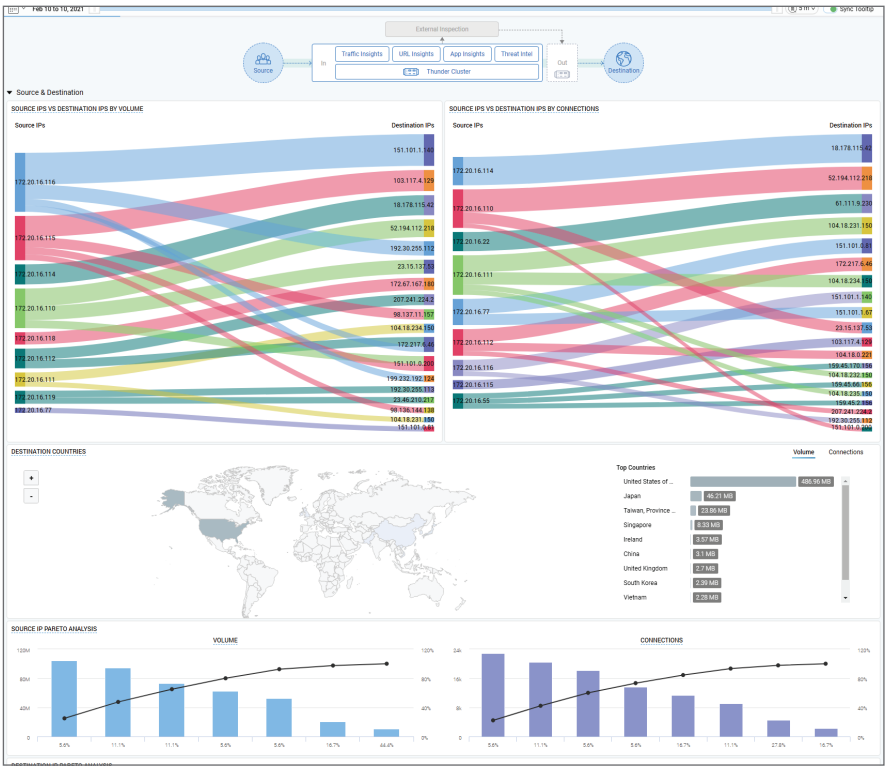

図9. SSL Insight アナリティクスは、IP、TLS トラフィックパターン、URL、アプリケーションカテゴリー、デバイスなどの側面からトラフィックのインサイトを視覚化します。

Harmony Appsの機能一覧

CGNAT App

アナリティクス&インサイト	トラフィック分析	• リアルタイムのサービストラフィック統計およびデバイスの健全性を含むCGNATサービスレベルKPI（主要業績評価指標）バー • 上位の加入者（IPv4/IPv6）と時系列の同時セッション数およびセッションレート • アップリンクおよびダウンリンクで測定された加入者側の時系列の総トラフィック（スループットおよびパケットレート） • CGNATサービス分析：ポートマッピング（プロトコル）、時系列のセッション統計（ユーザークォータ、フルコーンセッション、EIM/EIF、ヘアピン）、NATプール、ミスビヘイビア/エラー トラフィックの統計とインサイト • CGNデバイス/クラスタの統計、インターネット（アップリンク）側のトラフィック
	加入者のポート使用状況（固定NATの場合）	• 加入者のポート使用状況（TCP/UDP）の相関関係 • ポート範囲における加入者のトラフィックパターンのインサイト • アクティブな加入者
	アプリケーションの可視化	• トップアプリケーションチャート（ルールセット毎） • 接続数とボリュームに基づくアプリケーション・トラフィックの分布 • カテゴリ/ウォッチリスト別のアプリケーションのインサイト
	IPアノマリー	• 正常なパケットと異常なイベントを比較したインサイト • ダウンリンク、アップリンク、レイヤー3、レイヤー4によるフィルタリング • 異常のタイプとレイヤーの分布
ダッシュボード		• アラートやイベント、地理的な展開場所、CGNATサービスのKPIスコアカードを含む、CGNATサービス全体のテナントビュー • CGNサービスタイプビューでは、加入者のKPIスナップショットバーとドリルダウン統計、現在のセッション数とレート、スループット（bps）、パケットレート（pps）、NATプールの使用状況（TCP/UDP）、デバイスのステータス（データ/コントロールCPU、メモリ使用率）などを提供
トラブルシューティング		• 処理チェーンのどこでパケットドロップが発生しているかを可視化し、問題点や根本的な原因を迅速に特定するのに役立つドロップ分析 • アラートやイベントが時間軸上に重ねて表示されるため、パフォーマンスやエラーを簡単に相関させ、問題を迅速に特定することが可能な時系列チャート • あらゆる時系列データのスパイクを検知し、アラートを生成することが可能な異常検知機能
セッションログ・ドリルダウン		• 加入者情報（IP、MSISDN、IMEI、IMSI）、NATセッション、ポートマッピング、プロトコル、CGNポリシーなどを提供する詳細なCGNATトランザクションログ • 加入者情報、NATプール、プロトコル、理由/エラータイプを提供する詳細なエラートランザクションログ • セッションログとエラーログの両方に対して、使いやすい検索とフィルタリングのオプションを提供

図10. CGNAT Appは、CGNATサービスごとに、加入者のトラフィックを包括的に可視化し、インサイトを得ることができます。

Harmony Appsの機能一覧

GTP Firewall App

アナリティクス&インサイト	トラフィック・インサイト	• リアルタイムのサービストラフィック統計およびデバイスの健全性を含むGTP FWサービスレベルKPI（主要業績評価指標）バー • Roam-inおよびRoam-outの両方のGTPセッション数に基づくローミングの地理的表示 • GTPv0-C、GTPv1-C、GTPv2-C、GTP-U（アップリンク／ダウンリンク）に関する時系列のGTPトラフィックの把握 • 時系列のGTPトラフィックの分布と比較チャート — シグナリングゲートウェイ（SGW）およびシグナリングゲートウェイセキュアネットワーク（SGSN） — パケットデータネットワークゲートウェイ（PGW）およびゲートウェイGPRSサポートノード（GGSN） — アクセスポイント名（APN） • GTPセッションの時系列CFWクラスタ・トラフィック統計
	ポリシー違反	• GTPファイアウォールポリシーアクションの時系列統計および違反カテゴリに基づくポリシー違反のインサイト • 違反タイプの分布と比較を用いた、時系列のGTPファイアウォール・ポリシー違反分析 — シグナリング・ゲートウェイ（SGW）およびシグナリングゲートウェイセキュアネットワーク（SGSN） — パケットデータネットワークゲートウェイ（PGW）およびゲートウェイGPRSサポートノード（GGSN） — アクセスポイント名（APN） • ファイアウォール・ルールのパフォーマンス分析とステイル・ルール・インジケータ
	Roam-in	• 世界地図ビューでの発信国別GTP Roam-inセッション統計 • ログカウント、MMC、MNCに基づいたローミング元国のリストの表示
	Roam-out	• 世界地図ビューでのGTP Roam-outセッション統計（送信先国別） • ログカウント、MMC、MNCに基づいたローミング先の国の一覧
セッションログ・ドリルダウン		• 詳細なGTPファイアウォールセッションログ（送信元/オリジン、送信先、メッセージタイプ、セッションの詳細（プロトコル、ユーザーロケーション情報（LUI）、QoSなど）、ログの理由、ファイアウォールルール/アクション情報を提供 • GTPプロトコルタイプ、IP、TEID、その他を使用した使いやすい検索およびフィルタリングオプション

図 11. GTP Firewall Appは、時系列のGTPトラフィックインサイト、GTP FWサービスレベルKPI、ローミング（イン／アウト）セッション統計、詳細なセッションログなどを使用して、ローミングトラフィックの全体的なビューと分析を提供します。

Harmony Appsの機能一覧

Gi/SGi Firewall App

アナリティクス&インサイト	IPトラフィック	• リアルタイムのトラフィック統計、ファイアウォールルール統計、デバイスの健全性を含むCGNおよびGiFWのサービスレベルKPI（主要性能指標）バー • 総セッション数とレート • トータルの時系列トラフィック統計（スループットとパケットレート） • スループット、セッション、送信元と宛先のプロトコル（IPv4/IPv6）に基づいた上位K個のIPを使用したトラフィック分析
	ファイアウォール	• ファイアウォール・ルール・アクションに基づく時系列トラフィッ ク分析 • ルールにマッチしたトラフィックとドロップしたトラフィックに基づくトラフィックパターン統計 • 各アクションに対するファイアウォールルールのトラフィック分布 • ファイアーウォール・ルールのパフォーマンス・スコアカードとステイル・ルール・インジケータ • ボリューム、パケット、セッションに基づく上位加入者（IPv4/IPv6）
	CGN	• プロトコルベースのポートマッピングに関するインサイト • 時系列のポートマッピング統計 • 時系列のポートエラーおよびクォータ超過の統計情報 • 時系列のNATプール使用率（ポートベース、NAT IPベース、NAT IPごとの加入者）
	クラスター	• CFWデバイス／クラスターのシステム使用率（CPU、メモリ）と帯域幅 • 世界地図上の導入位置 • スループットとアクティブセッションに基づくクラスタートラフィックインサイト
セッションログ・ドリルダウン		• 加入者情報、NATセッション、ポートマッピング、CGNポリシーなどを提供する詳細なCGNATトランザクションログ • 加入者情報、ファイアウォールのルールとアクション、ゾーン、イン／アウトのインターフェイス、セッションのステータスを提供する詳細なファイアウォール／トランスペアレントセッションログ • NATとファイアウォールの両方のセッションログを対象とした、使いやすい検索および絞り込みオプション。

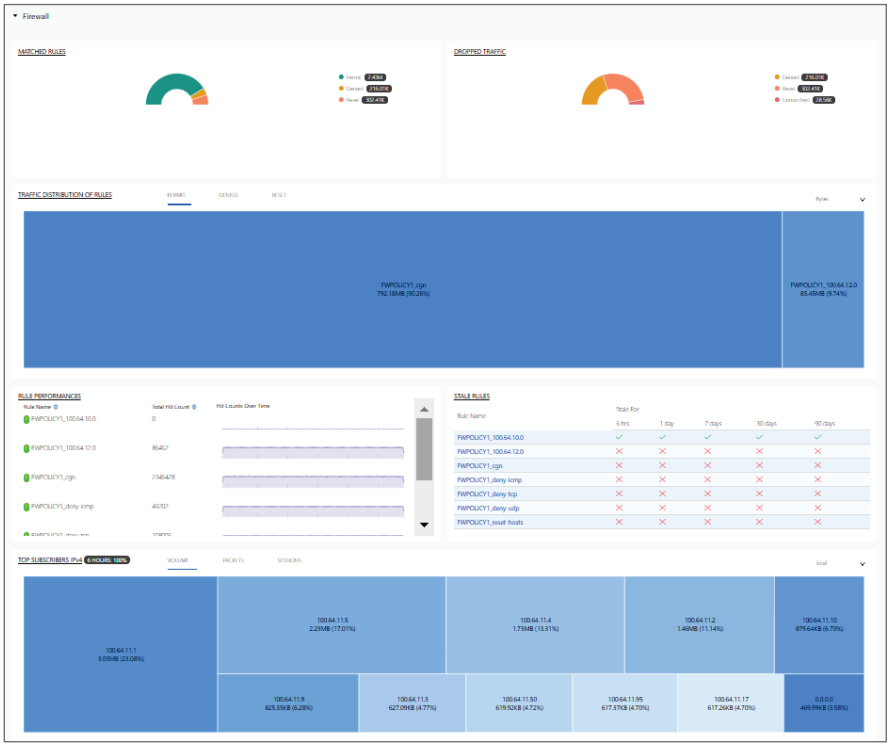

図12. Gi/SGi Firewall Appは、ユーザーのトラフィックの詳細な分析を行い、時系列のトラフィックのインサイト、ファイアウォールのルールの永続性、CGNとGiFWのサービスレベルKPIなどを提供します。

A10 Networks / A10 ネットワークス株式会社について

A10 Networks（NYSE: ATEN）は、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

Part Number: A10-DS-15122-JA-12　APR 2021