データシート

A10 Defend Orchestrator

DDoS 攻撃対策の監視・管理・オーケストレーション

A10 Defend Suite のソリューションの一つである A10 Defend Orchestrator（旧称 aGalaxy®）は、インテリジェントで自動化された DDoS 防御を行う A10 Defend Detector および Mitigator（旧称 Thunder TPS®）と連携し、DDoS 防御のマネジメントをシームレスに行う環境を提供します。

世界規模の DDoS 攻撃対策をリアルタイムで実現

今日、DDoS 攻撃は複雑さも規模も増大し、DDoS 防御も進化しています。総合的な DDoS 防御スイートが必要です。A10 Defend Suite は集中管理コンポーネントも有し、最新の DDoS 攻撃の把握や、最新の DDoS 防御アプライアンス利用に伴う管理を支援します。

企業、データセンタ、サービスプロバイダは、A10 Defend による DDoS 防御により DDoS 攻撃者と正常なユーザを正確に識別することができ、不要なトラフィックをブロックすることが可能になります。

業界をリードするスケーラビリティと最適化されたワークフローにより、組織の最前線に立つセキュリティ担当者は、より効果的な防御を実現できます。

A10 Defend Orchestrator は DDoS 防御環境をグローバルで監視できるため、攻撃を迅速に検出し、中央の管理ポイントから、攻撃防御のためのポリシーを確実に適用することができます。管理者は、Defend Detector および Defend Mitigator からのテレメトリデータを使用して設定変更やネットワークアクティビティの包括的な監視を行うことができます。DDoS 攻撃のリアルタイム監視や、DDoS 攻撃インシデントの詳細情報の把握が行えます。

Defend Orchestrator は、地理的に離れた場所にまたがる複数の Detector および Mitigator のデプロイを管理することができ、運用の合理化、IT 運用コストの削減を可能とします。

プラットフォーム

Virtual Appliance

関連製品

- A10 Defend Detector
- A10 Defend Mitigator
- A10 Defend Threat Control

お問い合わせ

https://info.a10networks.com/JP-WebContactUs.html

メリット

自動化

DDoS 防御を自動化。より強力な保護を実現

A10 Defend Orchestrator は DDoS 防御アーキテクチャの中心となります。DDoS 攻撃発生時、A10 Defend Detector および Mitigator と連携することで、インテリジェントな自動 DDoS 防御を可能にします。DDoS 検知、警告、疑わしいトラフィックのルート変更、DDoS トラフィックのスクラビング、攻撃が沈静化するまでの継続的な分析に加え、複数の対策を組み合わせることで攻撃を緩和します。この自動防御は、手動操作の場合に要する時間やエラーを大幅に軽減します。

DDoS インシデントが終了すると、Defend Orchestrator は電子メールで送信可能な DDoS インシデントレポートを自動的に生成します。セキュリティオペレータは、プロビジョニング、攻撃を受けている間の運用、インシデント報告ワークフローに至るまで、インテリジェントで自動化された DDoS 防御を利用できます。

加速

攻撃を受けている間の対応を加速

DDoS 攻撃への実際の対策として、訓練を受けた人員やリソースを無制限に備えている組織はありません。A10 Defend Suite の一つのソリューションである A10 Defend Detector はライブトラフィックのフロー分析を行います。DDoS 攻撃を監視し、動的に学習された検出しきい値に基づいて、保護対象のサービスや被害者のホストに向かうトラフィックの異常を検出します。

DDoS 攻撃が発生した場合、セキュリティオペレータは Defend Orchestrator の Mitigation Console と呼ばれるライブダッシュボードを通じてインシデントの状態をリアルタイムで監視することができ、必要に応じて DDoS 防御ポリシーの制御・管理が可能です。A10 Defend Mitigator は、DDoS 脅威インテリジェンスリストと攻撃フィルタリストベースの緩和、緩和の自動的なエスカレーション／デスカレーションを備えており、5 段階のアダプティブプロテクションや機械学習技術による自動化されたゼロデイ攻撃パターン認識などの複数の防御手法を組み合わせます。これにより、レスポンスタイムが大幅に改善され、時間のかかる手作業による変更や、攻撃を受けている間の緩和戦略の再評価の必要性が最小限に抑えられます。

最大化

アジリティとセキュリティの最大化

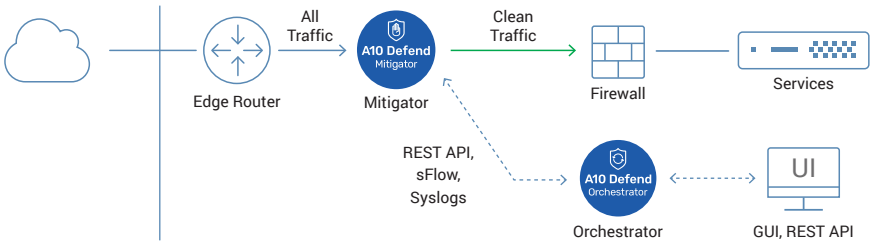
ネットワークオペレータは、Web スケール、SecOps/DevOps を採用するにつれ、変更を迅速にプロビジョニングし、問題を特定し、必要に応じて構成をロールバックする必要があります。A10 Defend Detector は、ネットワークトラフィックのパターンを容易に評価および学習することが可能です。A10 Defend Orchestrator によって、GUI または REST API(aGAPI) を介して複数の A10 Defend Mitigator の緩和ポリシーを一度に更新することができます。また、A10 Defend Orchestrator は、サードパーティの DDoS 検知システムや外部 SIEM、syslog サーバと容易に統合することができます。

削減

セキュリティの運用コストを削減

A10 Defend による DDoS 防御は非常に効果的です。A10 Defend Detector および Mitigator アプライアンスは、小型フォームファクタで高性能を実現し、電力使用量、ラックスペース、および冷却要件を大幅に削減して OPEX を削減します。A10 Defend Orchestrator は、インテリジェントで自動化された DDoS 防御を可能にし、運用の負荷および関連コストをさらに削減します。

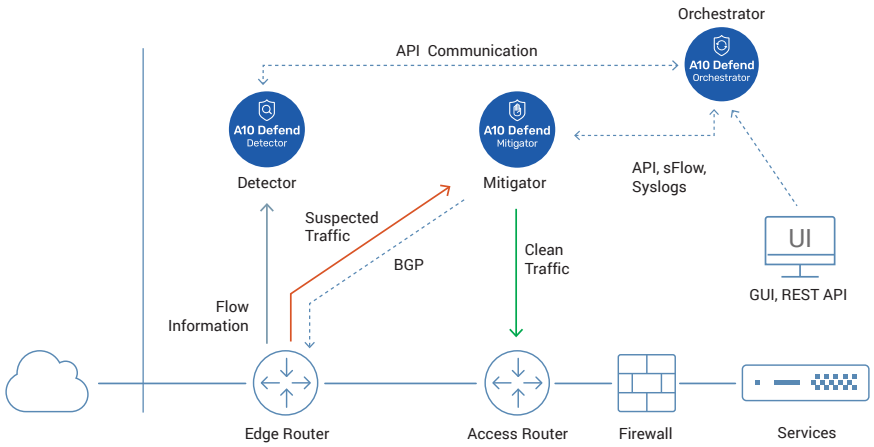
構成例



プロアクティブ構成

(非対称型または対称型)

プロアクティブ構成では、A10 Defend Mitigator による包括的な検知が継続的に行われ、迅速な防御が可能です。この構成は、ユーザエクスペリエンスが重要なゲームや DNS などのリアルタイムサービス、アプリケーション層の攻撃に対する保護に最も効果的です。A10 Defend Orchestrator は、トラフィックの可視性と DDoS 攻撃の緩和ダッシュボードとコンソールを提供します。

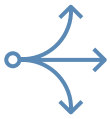


リアクティブ構成

大規模なネットワークでは、手動または DDoS 検知機能を搭載したフローコレクタのアラートをトリガーとするオンデマンドな攻撃緩和が有効です。A10 Defend Orchestrator は、グローバルに展開されている A10 Defend Detector および Mitigator とシームレスに統合し、トラフィックの異常検出時には自動化された DDoS 保護を有効にします。A10 Defend Suite は、オープン API や BGP FlowSpec により、他社製のフローコレクタとシームレスに連携可能です。不要な投資を抑え、DDoS 防御インフラストラクチャを強化することができます。

機能

防御サイクル全体にわたるインテリジェントな自動化



シンプル

自動オペレーションをシンプルに

A10 Defend は、防御サイクル全体を通じて、機械学習を活用した業界で最も高度な自動化機能を提供します。

オペレータが保護対象とするネットワークを定義すると、A10 Defend Orchestrator は、事前にオペレータが定義した検知および緩和ポリシーに基づいて残りの作業を実行します。これには、個別に学習した検出しきい値、自動トラフィック リダイレクト オーケストレーション、緩和とエスカレーションの開始、適応型保護ポリシーの適用、攻撃パターンフィルターを抽出して適用が含まれます。攻撃が沈静化すると、ネットワーク構成と防御態勢は平常に戻り、今後の分析のために詳細なインシデント レポートが生成されます。

一元管理

A10 Defend Orchestrator は、直感的なインターフェイスを備えています。複数の地理的な場所にまたがる、グローバルな DDoS 防御展開を管理することができ、ネットワークと DDoS インシデントの監視が行えます。オペレータは、1 か所からすべての A10 Defend アプライアンスを管理することができます。ヘルスチェック、バックアップ、更新、構成の変更、軽減テンプレートの適用、レポートの生成が実行可能です。

簡単かつ柔軟な統合

A10 Defend Orchestrator は、サードパーティ製の既存の DDoS 検知システムとシームレスに統合し、DDoS の兆候（プロトコルの異常、トラフィックの突然の急増、既知のボットからの大量のリクエストなど）を自動的に検知します。検知されると、REST API(aGAPI) を使用して DDoS 攻撃インシデント情報が動的に作成されます。インシデント管理では、重要な情報（攻撃の期間や種類など）を追跡するだけでなく、オペレータがインシデントデータに基づいて攻撃を直接軽減することもできます。

攻撃を受けている間のオペレーションとレポーティング

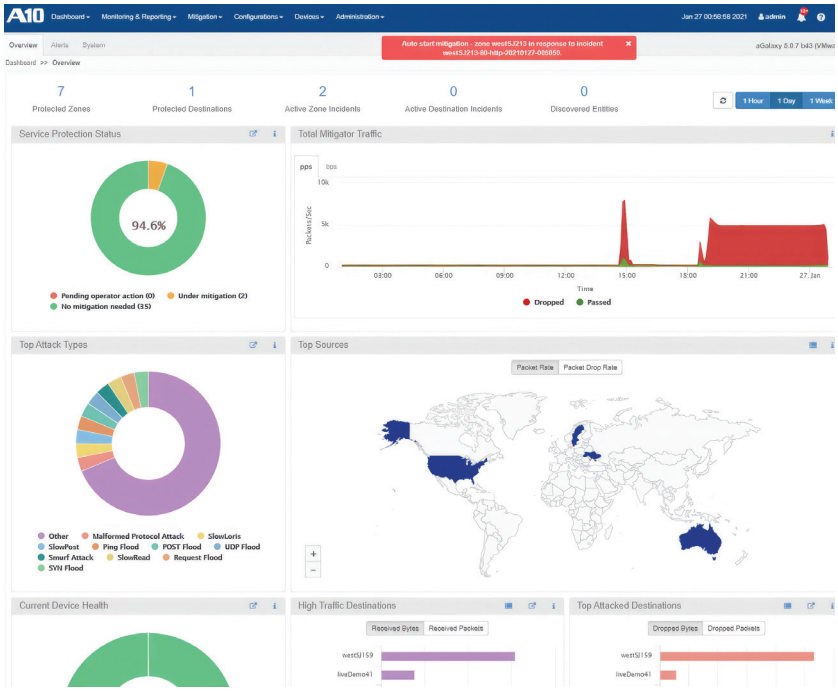
リアルタイム

緩和コンソール

A10 Defend Orchestrator の緩和コンソールから、セキュリティ オペレータはライブダッシュボードを通じてインシデントをリアルタイムで監視できます。DDoS 防御に特化したダッシュボードは、不審なトラフィック統計、適用された対策、緩和エスカレーション レベルを含むインシデントの詳細、Top-K 情報、アクティビティ ログを提供します。さらなるインシデント調査を支援するために、パケット キャプチャとデバッガをリモートで有効にし、必要に応じてカスタム対策を即座に作成することができます。

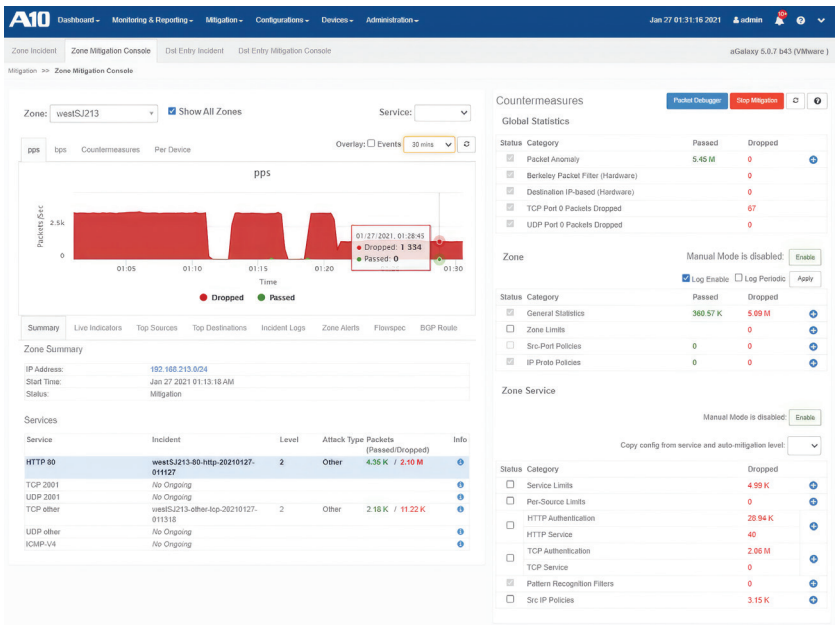
堅牢なレポート作成

A10 Defend Orchestrator は、管理対象の A10 Defend Detector および Mitigator デバイスから必要なデータを収集し、DF または CSV 形式でエクスポート可能な、読みやすいインシデントレポートを生成します。電子メールで即時送信したり、定期的または 1 回限りの通知としてスケジュールが可能です。DDoS 攻撃インシデントが終了すると、テレメトリ、カウンター、グラフ、イベント ログの豊富なセットを含む詳細なインシデントレポートが自動的に生成され、電子メール経由ですべての関係者と共有することができます。



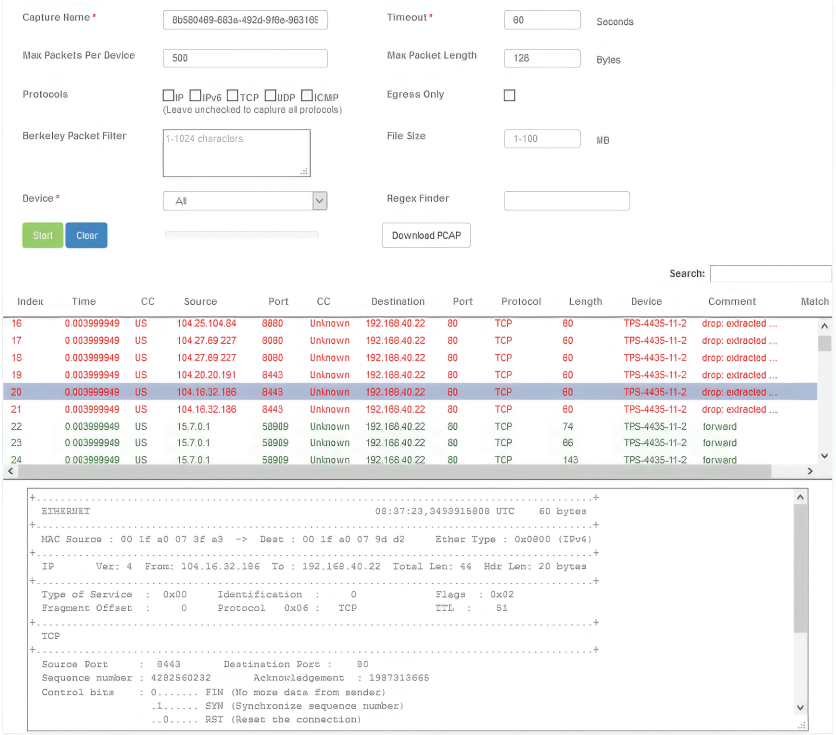
A10 Defend Orchestrator ダッシュボード

DDoS 防御に特化したダッシュボードは、不審なトラフィックのリアルタイムでの統計と DDoS インシデントのさまざまなサマリを提供します。組織がセキュリティイベントを追跡し、攻撃傾向を特定し、コンプライアンスのリスクに対処可能とします。



リアルタイム DDoS 緩和コンソール

セキュリティオペレータは、緩和コンソールから、攻撃のライブダッシュボードを表示し、緩和ステータスを確認し、必要に応じて高度な対策を即座に適用できます。緩和コンソールは、リアルタイムの統計情報と、緩和エスカレーションレベル、Top-K 情報、アクティビティログなどのインシデントの詳細を提供します。



リモート パケット キャプチャおよびデバッガツール

攻撃後または攻撃中のさらなるインシデント調査を支援するために、A10 Defend Orchestratorはパケットキャプチャとデバッガをリモートで有効にすることができます。これは、必要に応じてカスタム対策やフィルタを作成するのに役立ちます。

仕様

A10 Defend Orchestrator Virtual Appliance	
サポートするハイパーバイザ	VMware ESXi, KVM QEMU
ハードウェア要件	インストールガイドをご覧ください。

仮想アプライアンスの推奨サイジング

導入規模	100ゾーン／1,000サービス	1,000ゾーン／8,000サービス	3,000ゾーン／15,000サービス
vCPU	8	12	16
vRAM	24 GB	40 GB	96 GB
vDisk	500 GB	1 TB	1.5 TB

詳細機能一覧

シンプルな DDoS 防御管理

- プロビジョニング、攻撃を受けている間での運用、インシデント報告のための一元的な DDoS 防御オペレーションコンソール
- A10 Defend Detector および Mitigator アプライアンスの集中管理
- リアルタイム DDoS 防御ダッシュボードとコンソール
- 構成、バックアップ、復元、イメージ リポジトリのアップグレードの一元管理
- 再起動、シャットダウン、アップグレードのためのデバイスの一元管理
- 管理対象デバイスのヘルスモニタリング
- カスタマイズ可能なテンプレート内の事前定義された緩和ポリシーと構成プロファイル
- 攻撃を受けている間のリモートパケットキャプチャとデバッガ
- 検索可能な管理対象デバイスと A10 Defend Orchestrator 監査ログ
- オンボックス管理 GUI
- REST API (aGAPI)

イベント管理とレポート

- 攻撃の可視化と地理的位置の追跡
- ダッシュボードは、攻撃を受けたほとんどのサービスを継続的に監視可能
- 複数のアプライアンスにまたがるデータをリアルタイムでダッシュボードに統合
- 攻撃を受けている間のリアルタイム緩和コンソール
- オペレータの介入を最小限に抑え、完全に自動化された攻撃検知と緩和
- カスタマイズ可能なイベントアラート / アラーム
- 管理されたすべての A10 Defend Mitigator からの一元的なパケットキャプチャ
- オンデマンドあるいはスケジュール化されたレポーティング
- 電子メール経由で DDoS インシデントレポートを送付可能

アクセス管理

- ロール（役割）ベースのアクセス制御管理
- RADIUS および TACACS+ をサポートする外部認証

* ライセンスオプションによって機能が異なる場合があります。
オプションには、基本デバイス管理および A10 Defend（旧称 Thunder TPS）デバイス管理パックが含まれます。

A10 Networks / A10 ネットワークス株式会社について

A10 Networksは、オンプレミス、ハイブリッドクラウド、エッジクラウド環境における、セキュリティ、インフラストラクチャの課題を解決するソリューションを提供しています。大手グローバル企業や通信、クラウド、Webサービス事業者まで7000社以上のお客様に導入いただいており、ビジネスに不可欠なアプリケーションやネットワークの安全性、可用性、効率性を高めています。A10ネットワークスは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社を置き、世界中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。 詳しくはホームページをご覧ください。

- URL：https://www.a10networks.co.jp/
- X（旧Twitter）：https://twitter.com/a10networksjp
- Facebook：https://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-15137-JA-01 Mar 2024