データシート

aGALAXY FOR THUNDER TPS

DDoS攻撃対策管理システム

A10のaGalaxy®管理システムは、DDoS攻撃防御の専用アプライアンスであるA10のThunder TPS® (Threat Protection System) と連携し、世界規模のDDoS攻撃からシステムを防御するための監視機能や防御機能、攻撃検知、アラート、レポーティング機能を一元管理できる環境を提供します。

世界規模のDDoS攻撃対策をリアルタイムで実現

A10のDDoS攻撃対策ソリューションにより、企業やサービスプロバイダーは、正当なユーザーとDDoS攻撃者を正確に識別することが可能になります。セキュリティ担当者は、業界トップクラスの防御性能と、最適なワークフローにより、効果的にDDoS攻撃防御を実現できます。

A10のaGalaxy for Thunder TPSでは、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。

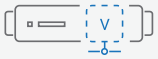
セキュリティ担当者は、防御環境に設置されたThunder TPSを設定、監視し、包括的な分析を行ってリアルタイムにDDoS攻撃を可視化できます。ドリルダウンして保護対象の各サービスによって処理された接続の詳細を確認することもできます。

aGalaxyは、各地域に分散配置された複数のThunder TPSを管理できるため、運用を効率化してIT運用コストを削減することができます。

aGalaxyは、フローベースのDDoS攻撃検知機能（Detectorモジュール）を搭載したモデルを選択して、Thunder TPSと連携させることにより、検知から防御までを完全に自動化した環境を構成することができます。

プラットフォーム

aGALAXY
ハードウェアアプライアンス



aGALAXY
仮想アプライアンス

プラットフォーム

THUNDER TPS
ハードウェアアプライアンス

vTHUNDER TPS
仮想アプライアンス

お問い合わせ

WEB
a10networks.co.jp/aGalaxy

連絡先
a10networks.co.jp/contact

メリット

ネットワーク全体を防御

セキュリティ担当者は、ダウンタイムを最小化するために、DDoS攻撃を素早く検出して防御しなければなりませんが、このような攻撃はさまざまな場所で発生します。

aGalaxyは、管理対象に設定された全てのThunder TPSからデータを収集し、DDoS攻撃の監視や防御に必要なデータをセキュリティ管理者に提供します。

セキュリティ担当者は、aGalaxy Mitigationコンソールのダッシュボード上で現在進行中の攻撃内容をリアルタイムで確認しながら、Thunder TPSに設定されている防御テンプレートを適用したり、独自の防御設定を作成して適用したりすることができます。

多様なポリシーと閾値を設定できるため、トラフィックをきめ細かく制御して不審な活動をブロックできます。ポリシーの適用後数秒以内に攻撃を軽減できたかどうかを確認できるため、必要に応じて対策内容を調整することができます。

DDoS攻撃防御管理

- 管理タスクを統合して運用コストを削減
- ダッシュボードを利用したリアルタイムのインシデント監視
- インシデントアラートを取得し、迅速に対策を適用
- 複数のThunder TPSアプライアンスを一元管理

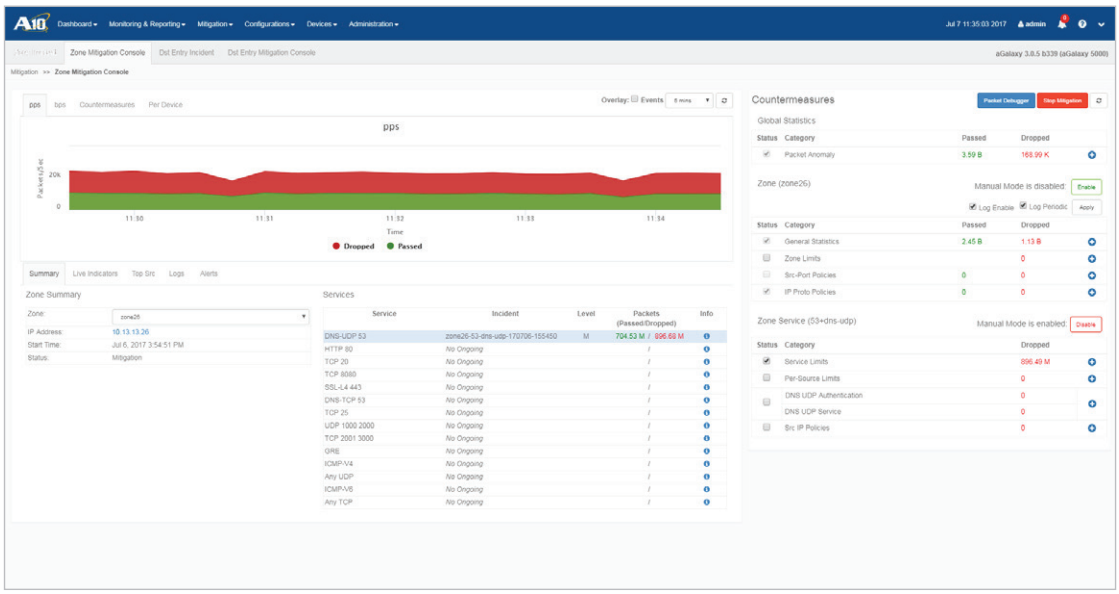


図1: aGalaxyのダッシュボード画面
ネットワーク状況をリアルタイムに確認しながら適切な攻撃防御ポリシーを適用できます。ポリシー適用後の防御状況も監視することができます。

シンプルな管理

aGalaxyを導入することにより、複数のThunder TPSアプライアンスを同時に管理できるため運用効率を向上させることができます。導入済みのすべてのアプライアンスのソフトウェアアップグレード、SSL証明書管理、設定ファイルのバックアップやリストアまで、aGalaxyがすべての管理タスクを一箇所に統合するため、管理者はすべてのデバイスに一貫したポリシーを容易に適用することができます。

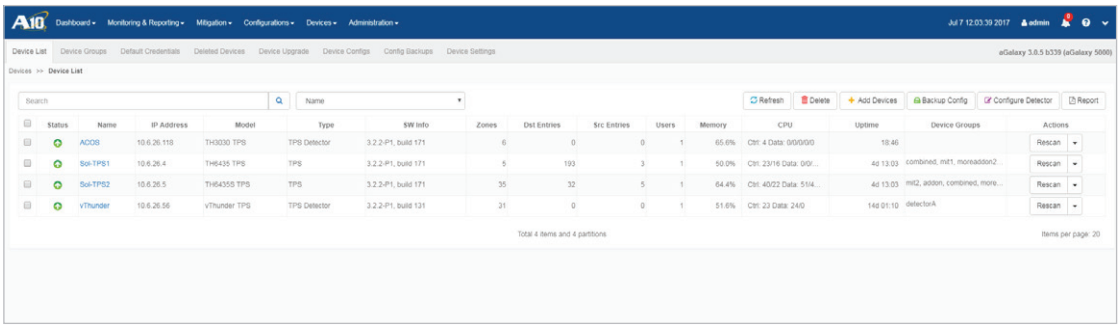


図2：aGalaxyのデバイス管理画面
管理対象のすべてのデバイスとバックアップ設定を表示できます。

アジリティの最大化

大規模にSecOps/DevOpsを採用したネットワークオペレータは、迅速に変更を行い、問題を特定し、必要なときに設定をロールバックする必要があります。aGalaxyを使用することにより、GUIまたは、RESTful API（aGAPI）を介して、複数のThunder TPSアプライアンスに対して、ポリシーを一括配信できます。

レポーティング

aGalaxyが提供するインシデントレポートやサマリー、リアルタイムダッシュボードを使用して、セキュリティイベントを追跡し、攻撃傾向を把握して、コンプライアンスリスクに対応することができます。aGalaxyのレポーティング機能では、全体のトラフィック状況やプロトコル別のブロックされた攻撃に関する情報などを得ることができます。レポートはすべて外部にエクスポート可能となっており、電子メールでの送信やファイルへの出力（PDF形式など）も可能です。

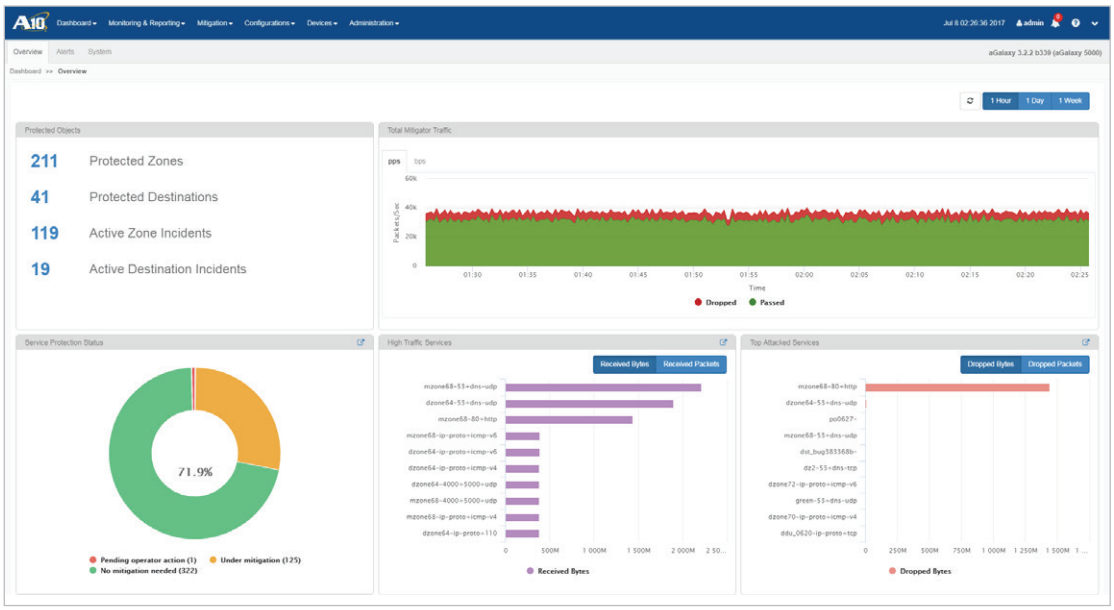
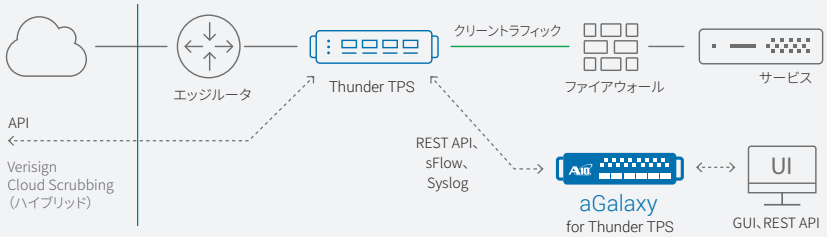


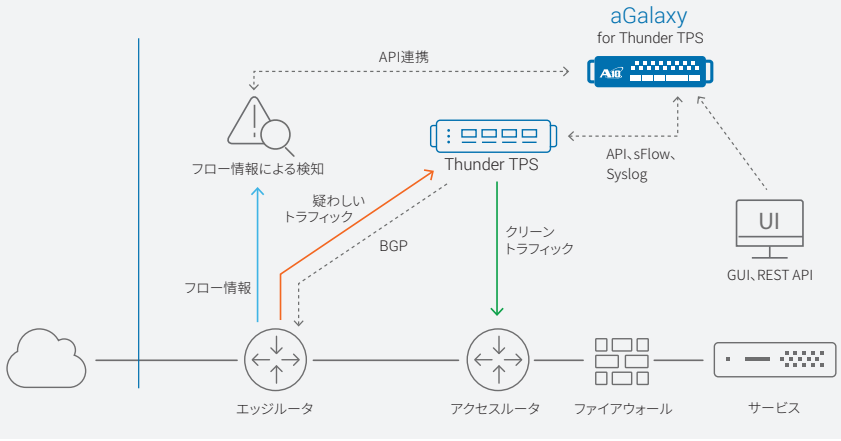
図3：aGalaxyのダッシュボード画面
直感的に操作できるダッシュボードでは、ネットワーク活動、レポート、ブロックされた攻撃を時系列で表示できます。

構成例



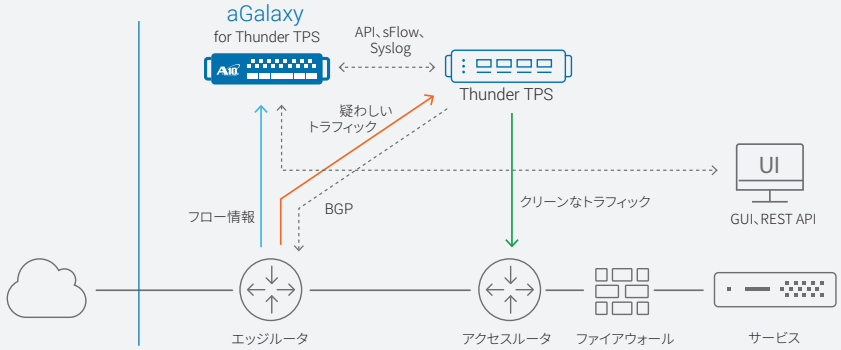
プロアクティブ構成
（非対称型または対称型）

プロアクティブ構成では、包括的な検知が継続的に行われ、迅速な防御が可能です。aGalaxyにより、導入されている複数のThunder TPSを統合管理することができます。この構成が最も効果的なのは、ユーザーエクスペリエンスを重要視するリアルタイム環境です。Thunder TPSは、L2またはL3のインライン構成をサポートします。L3構成であれば、インストール時のネットワーク中断やメンテナンス期間が不要になります。



リアクティブ構成

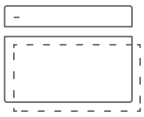
大規模なネットワークでは、手動またはDDoS検知機能を搭載したフローコレクタのアラートをトリガーとするオンデマンドな攻撃緩和が有効です。aGalaxyはグローバルに導入されたThunder TPSのオーケストレーションを行います。Thunder TPSは、BGPやその他のルーティングプロトコルを使用するあらゆるネットワークをサポートしています。そのため、追加の変更やルートを再度インジェクションするルータも必要ありません。オープンAPIにより、他社製のフローコレクタとシームレスに連携可能です。



aGalaxyとThunder TPSによるリアクティブ構成

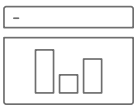
フローによるDDoS検知を可能にするDetectorモジュールを搭載したaGalaxyを利用し、Thunder TPSと連携させ、DDoS攻撃の検知から防御までを全てA10製品で構成することにより、迅速な防御と、統合された監視、レポーティング環境を実現できます。

機能



一元管理

直感的なインターフェイスを装備するaGalaxy一元管理システムは、広範囲にわたる不可欠なタスクを実行または自動化できる強力なネットワーク監視/管理ソリューションです。管理対象となるすべてのThunder TPSアプライアンスの死活監視から、防御テンプレートのバックアップ、更新、適用、レポートの生成までサポートしています。



リアルタイム ダッシュボード

使いやすいダッシュボードでは、システムの死活監視、アラート対応、保護対象オブジェクトとゾーンに対して発生しているインシデントの表示などを行うことができます。

レポーティング

aGalaxyは、管理対象のThunder TPSデバイスから必要なすべての情報を収集し、レポートを作成することができます。レポートは、PDF、またはCSV形式で生成可能となっとり、電子メールによる即時送信や、一定期間ごと、または一度のみ生成といったかたちでスケジューリングすることも可能です。

自動化

aGalaxyは、DDoS攻撃の兆候（プロトコル異常、突然のトラフィックサージ、既知のボットからの大量リクエストなど）を自動的に認識するサードパーティのDDoS検知システムと連携させて使用できます。攻撃を検知すると、RESTful API（aGAPI）を使用してDDoS攻撃インシデントデータを動的に生成します。インシデント管理機能では、攻撃の期間や攻撃の種類などの重要情報を追跡できるだけでなく、インシデントデータに基づいて攻撃を直接防御することができます。

フロー情報による DDOS検知

（特定モデルのみサポート）

リアクティブなDDoS検知は、ルータやスイッチからエクスポートされたIPv4、IPv6トラフィックのフローデータレコードを収集し、分析することによって効率化されます。フローベースのDDoS攻撃検知機能（Detectorモジュール）の動作学習モードでは、保護対象ゾーンの正常時トラフィックを分析し、自動的にプロファイルを作成します。監視モードでは、最大17のフロートラフィックインジケータを監視し、インバウンドトラフィックまたは双方向トラフィックの異常な動作を見つけ出します。

攻撃を検出すると、自動的にThunder TPSへ適切な防御テンプレートを適用し、BGPで不審なトラフィックのルートを変更します。その後、クリーンなトラフィックが目的の宛先に転送されます。

aGALAXYハードウェアアプライアンス

aGALAXY 5000

管理対象Thunder TPSデバイス数（推奨）	20台
管理対象バージョン（Thunder TPS）	ACOS 3.2.2以上
ブラウザー	Internet Explorer 8.x以上、Firefox 9.x以上
インターフェイス	1GEカッパー x 4 + 10GE SFP+ x 4、管理コンソールポート
プロセッサー	Intel Xeon 10-core x 2
メモリー	128 GB ECC RAM
外形寸法	8.89 cm（高さ）x 444.5 mm（幅）x 63.50 cm（奥行）
重量	16.78kg
ラックユニット（マウント可能）	2U
動作環境	温度：0°～40°C | 湿度：5%～95%
規格準拠	FCC Class A、UL、CE、TUV、CB、VCCI | RoHS

aGALAXY仮想アプライアンス

aGALAXY VA

管理対象Thunder TPSデバイス数（推奨）	20台
サポートハイパーバイザー	VMware ESXi 5.0以上 KVM version 0.14（qemu-kvm-0.14.0）以上
ハードウェア要件	インストールガイド参照

フローベースのDDoS検知機能

最大フロー処理数	500,000フロー/秒
最大管理台数　(Thunder TPSデバイス数)	4
最大対応ゾーン数	250

機能一覧

Thunder TPSデバイス管理

- ウィザードベースのシステム設定
- リアルタイムの集中管理
- 設定、バックアップ、リストア
- アップタイムステータス管理
- 管理対象デバイスのアップグレードとイメージアップグレードリポジトリの一元管理
- 管理対象デバイスのリブート/シャットダウン
- 管理対象デバイスのヘルスチェック
- 設定情報の投入と比較
- sFlowコレクター
- デバイス検索機能、監査ログ
- オンボックス管理GUI
- aGAPI REST API

イベント管理とレポーティング

- 攻撃の視覚化と地理情報追跡
- ダッシュボーによる攻撃対象サービスの監視
- 複数デバイスからのデータを統合してダッシュボードに表示
- リアルタイムで使用できる緩和コンソール
- 完全に自動化した攻撃検知(最小限の操作で攻撃を防御)
- カスタマイズ可能なイベントアラート/アラーム
- すべての管理対象Thunder TPSから一元的にパケットをキャプチャ
- オンデマンドレポートと定期レポート
- 帯域幅とアクセス制限に関するブラックリストとホワイトリスト

フローベースDDoS Detector

(特定モデルのみサポート)

- sFlow、NetFlow v5/v9、IPFIX/NetFlow v10
- IPv4/IPv6トラフィックのDDoS攻撃に対応
- 正常トラフィックの学習
- 17の動作インジケータを追跡したDDoS攻撃検知
- 双方向トラフィックの異常特定
- 迅速な攻撃検知時間(3秒)
- aGalaxy設定の制御

アクセス管理

- ロールベースのアクセス制御
- RADIUSとTACACS+をサポートした外部認証

機能はライセンスの種類によって異なります。

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-15125-JA-01 DEC 2017